Charge Sensing
– A Key to Improving Sensitivity in Integrated Circuit Analysis –

vorgelegt von
M. Sc. EE
Clemens Helfmeier
geb. in Berlin

von der Fakultät IV – Elektrotechnik und Informatik
der Technischen Universität Berlin
zur Erlangung des akademischen Grades

Doktor der Ingenieurwissenschaften
– Dr.-Ing. –

genehmigte Dissertation

Promotionsausschuss:
Vorsitzender: Prof. Dr. Klaus Petermann
Gutachter: Prof. Dr. Christian Boit
Gutachter: Prof. Dr. Heinrich Neitzert
Gutachter: Prof. Dr. Roland Thewes

Tag der wissenschaftlichen Aussprache: 16. April 2015

Berlin 2015
D 83

Eidesstattliche Erklärung

Hiermit versichere ich an Eides statt die eigenhändige Anfertigung dieser Arbeit. Soweit andere Werke genutzt oder zitiert wurden, sind diese entsprechend mit Angabe der Quelle gekennzeichnet.

Berlin, den

Datum Unterschrift

To my parents

Abstract

This work analyzes very low currents by investigation of charge amounts. A system capable of measuring charges down to femto-coulomb range (10^{-15} C) is discussed and implemented in an integrated circuit (IC) technology ("charge sensor"). The system is fully compliant with complementary metal oxide semiconductor (CMOS) technology, and can be applied to a wide range of IC related investigations. With the capability of measuring charge, impacts on many different areas of electronic circuits are identified, including failure analysis (FA) and security ICs. These exemplary situations are part of the impact assessment: 1. dielectric leakage behavior characterization of different kinds of dielectrics, 2. analysis of charging from focused ion beam (FIB) irradiation during circuit edit (CE) tasks in FA, and 3. security evaluation of IC hardware by consideration of charge.

Dielectric characterization is conventionally done by stress-, breakdown- or leakage current analysis and possibly integration of the current for modeling based on charge dependent behavior. This work extends the dielectric characterization to charge measurements. Measurement results from two different dielectrics are presented. The characterization of the leakage behavior is possible with noise currents below 1 aA. This sensitivity is not achievable with conventional current measurement systems.

FIB irradiation of insulating IC surfaces is analyzed using the charge sensor. Measurements show that 2.2 secondary electrons (SEs) are emitted per incident ion from the neutral insulating IC surface. Charging of the IC surface reduces this to 0.8 SEs during continuous irradiation. The electronically blanked ion beam causes the observation of a parameter-dependent charging current of 0.01 fA…10 fA.

A FIB detector circuit is implemented by using the charge sensor to identify the surface charging of the ion beam. The aspects for integrating the charge sensor into a security IC are discussed. Commonalities and differences to current suggestions for physically unclonable function (PUF) circuits are identified.

An implementation of fuse bits is analyzed with the FIB showing severe vulnerabilities of this security feature due to charge investigations. Different aspects of IC hardware, wiretapping of on-die signals and semi-invasive analysis techniques are discussed. Results show that consideration of charge is an important factor when new PUF implementations are suggested.

Charge analysis allows for matched and to date unrivaled sensitivity in IC analysis.

Zusammenfassung

Die vorliegende Arbeit analysiert besonders niedrige Stromstärken mithilfe von Ladungen. Die Konstruktion einer Ladungsmessschaltung mit Femtocoulomb Empfindlichkeit wird für die Verwendung in einem CMOS (complementary metal oxide semiconductor) integrierten Schaltkreis (IC) gezeigt. Durch die Messbarkeit kleiner Ladungsmengen ergeben sich weitreichende Möglichkeiten in der Fehleranalyse und Sicherheit von ICs, die an Beispielen analysiert werden: 1. Charakterisierung von Dielektrika, 2. Aufladung durch Ionenbestrahlung (FIB) von isolierenden Proben, sowie 3. Schutz und Angriff von Sicherheitsschaltkreisen auf Grundlage von Ladungen.

Die Charakterisierung von Dielektrika wird konventionell mit Stress-, Leck- und Durchbruch-Verhaltensanalyse durch den Strom ausgedrückt und nur auf Basis von Modellbildungen auf Ladungsmengen übertragen. In dieser Arbeit wird das Verhalten von zwei verschiedenen Dielektrika bei Strömen im Bereich von 1 aA analysiert. Die Ladungsmessung ist gegenüber konventionellen Methoden etwa 1000× empfindlicher.

Die Aufladung der isolierenden IC-Oberfläche durch die Bestrahlung mit einem FIB wird ermittelt. Ein Sekundärelektronenemissionskoeffizient von 2.2 Elektronen pro initial eintreffendem Ion, sowie von 0.8 Elektronen pro eintreffendem Ion für kontinuierliche Bestrahlung wird bestimmt. Nebeneffekte des FIB Systems im Bereich von 0.01 fA…10 fA äquivalentem Strom können beobachtet werden.

Durch die Aufladungserscheinungen im FIB kann ein FIB Angriff durch die Zielschaltung erkannt werden. Eine entsprechende Schaltung wird konstruiert und Aspekte für die Implementierung in einen Sicherheitsschaltkreis werden diskutiert. Anhand dieser Ergebnisse können neue Erkenntnisse über die Implementierung und Verwundbarkeit von Sicherheitsschaltkreisen gewonnen werden. Die Zusammenhänge verschiedener Analyseaspekte von PUF (physically unclonable function) Schaltungen werden dargestellt.

Ladungsmessung und -analyse erlauben bisher unerreichte Empfindlichkeit in unterschiedlichen Bereichen der integrierten Schaltungen.

Contents

Abstract **7**

Zusammenfassung **9**

Chronological List of Publications **13**

1 Introduction **15**

2 Context of Charge **19**
2.1 Focused Ion Beam 19
2.1.1 FIB Technology 19
2.1.2 FIB Applications 22
2.2 Manufacturing of Insulators 23
2.3 Semiconductor Manufacturing Technology 25
2.4 Semiconductor 26
2.5 Tunneling Currents in Insulators 27
2.6 Security of Electronic Hardware 28

3 Ultra Low Current Measurements **33**
3.1 Practical System Setups 33
3.2 Origin of Current 35
3.3 Quantization of Charge 36
3.3.1 Shot Noise 36
3.3.2 Thermal Noise 37
3.3.3 $1/f$ Noise 37
3.3.4 Summary of Noise 38
3.3.5 Nyquist Theorem 39

4 DC Charge Measurement Concept Selection **41**
4.1 Basic Electrometer Designs 41
4.1.1 Electroscope 42
4.1.2 Field Mill 44
4.1.3 Solid State Devices 45
4.1.4 Secondary Electron Emission Yield as Field Indicator 46

4.2 Feedback construction 48
4.3 Antenna design 50
4.4 Tunneling Current in Capacitive Voltage Divider 53
4.5 Summary 56

5 Charge Measurement Construction **57**
5.1 Closed Loop Feedback Principle 58
5.2 Systematic Measurement Limitations 59
5.2.1 Static Measurement Errors 61
5.2.2 Transient Measurement Errors 62
5.3 Noise 64
5.4 Measurement Speed 66
5.5 Offline Charge Detection Principle 67
5.6 Realizations 70
5.6.1 Closed-Loop Feedback Implementation 71
5.6.2 Offline Charge Detector Implementation 79

6 Results on Application Scenarios **85**
6.1 Dielectric Characterization 87
6.1.1 On-die Dielectric Characterization 87
6.1.2 Off-die Dielectric Characterization 92
6.2 Charging by FIB 98
6.3 Focused Ion Beam Detector 109
6.4 Charges in Security 114
6.5 Charges in PUF Characterization 118

7 Conclusion and Summary **123**

A IHP Technology Tunneling Properties **127**

B Tunneling Current Simulation Script **129**

C Noise of LMS Derived Current Value **137**
C.1 Numerical Verification 138

Acronyms **147**

Mathematical Symbols **151**

Bibliography **155**

Chronological List of Publications

This work is part of my fellowship in the Helmholtz Research School on Security Technologies (HRS-ST). Parts of this work have already been published in one or more of the following publications:

[1] A. Glowacki, **C. Helfmeier**, U. Kerst, and C. Boit. "Improvement of optical resolution through chip backside using FIB trenches". In: *Proceedings of the 36th International Symposium for Testing and Failure Analysis (ISTFA 2010)*. Vol. 36. ASM International, 2010, pp. 176–180.

[2] **C. Helfmeier**, C. Boit, and U. Kerst. "On charge sensors for FIB attack detection". In: *Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on*. 2012, pp. 128–133. DOI: 10.1109/HST.2012.6224332.

[3] **C. Helfmeier**, C. Boit, D. Nedospasov, and J.-P. Seifert. "Cloning Physically Unclonable Functions". In: *Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on*. 2013, pp. 1–6. DOI: 10.1109/HST.2013.6581556.

[4] **C. Helfmeier**, D. Nedospasov, C. Tarnovsky, J. Krissler, C. Boit, and J.-P. Seifert. "Breaking and Entering through the Silicon". In: *CCS '13: Proceedings of the 20th ACM conference on Computer and communications security*. 2013. DOI: 10.1145/2508859.2516717.

[5] C. Boit, **C. Helfmeier**, D. Nedospasov, and A. Fox. "Ultra high precision circuit diagnosis through Seebeck generation and charge monitoring". In: *Physical and Failure Analysis of Integrated Circuits (IPFA), 2013 20th IEEE International Symposium on the*. 2013, pp. 17–21. DOI: 10.1109/IPFA.2013.6599119.

[6] C. Boit, **C. Helfmeier**, and U. Kerst. "Security Risks Posed By Modern IC Debug & Diagnosis Tools". Invited Paper. In: *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on*. 2013, pp. 3–11. DOI: 10.1109/FDTC.2013.13.

[7] C. Boit, **C. Helfmeier**, and D. Nedospasov. "Feasibly Clonable Functions". Invited Paper. In: *TrustED '13: Trustworthy Embedded Devices, International Workshop on*. 2013. DOI: 10.1145/2517300.2528523.

[8] D. Nedospasov, **C. Helfmeier**, J.-P. Seifert, and C. Boit. "Invasive PUF Analysis". In: *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on*. 2013, pp. 30–38. DOI: 10.1109/FDTC.2013.19.

[9] **C. Helfmeier**, C. Boit, D. Nedospasov, S. Tajik, and J.-P. Seifert. "Physical vulnerabilities of Physically Unclonable Functions". In: *Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014*. 2014, pp. 1–4. DOI: 10.7873/DATE.2014.363.

[10] **C. Helfmeier**, R. Schlangen, and C. Boit. "Focused ion beam contact to non-volatile memory cells". In: *Microelectronics Reliability* 54.9–10 (2014). ESREF 2014, pp. 1798–1801. ISSN: 0026-2714. DOI: 10.1016/j.microrel.2014.07.017.

[11] C. Boit, N. Schäfer, D. Abou-Ras, **C. Helfmeier**, A. Glowacki, and U. Kerst. "Backside failure analysis techniques: What's the gain of silicon getting thinner?" In: *Physical and Failure Analysis of Integrated Circuits (IPFA), 2014 IEEE 21st International Symposium on the*. 2014, pp. 17–21. DOI: 10.1109/IPFA.2014.6898203.

[12] S. Tajik, D. Nedospasov, **C. Helfmeier**, J.-P. Seifert, and C. Boit. "Emission Analysis of Hardware Implementations". In: *Digital System Design (DSD), 2014 17th Euromicro Conference on*. 2014, pp. 528–534. DOI: 10.1109/DSD.2014.64.

[13] S. Tajik, E. Dietz, S. Frohmann, J.-P. Seifert, D. Nedospasov, **C. Helfmeier**, C. Boit, and H. Dittrich. "Physical Characterization of Arbiter PUFs". In: *Cryptographic Hardware and Embedded Systems – CHES 2014*. Ed. by L. Batina and M. Robshaw. Vol. 8731. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2014, pp. 493–509. ISBN: 978-3-662-44708-6. DOI: 10.1007/978-3-662-44709-3_27.

[14] S. Tajik, E. Dietz, S. Frohmann, H. Dittrich, D. Nedospasov, **C. Helfmeier**, J.-P. Seifert, C. Boit, and H.-W. Hübers. "A Complete and Linear Physical Characterization Methodology for the Arbiter PUF Family". In: *Journal of Cryptography* (2015). in press.

Chapter 1

Introduction

Electricity has been a topic of curious interest ever since the discovery. Miletus was among the first to discover charge, the very basic of electricity, already in 600 BC. Though, the nature of charge was not yet understood, it was this quantity that was the first within electronics discoveries. It lasted until the experiments of Volta in AD 1800 [3] that current becomes available for inspection. The voltaic pile allowed for the continuous support of charge over a long time, though the initial understanding was incorrect at that time [50]. Nowadays, charge has vanished from the usual understanding of general electronics into a corner existence. Only when special circuits are discussed, that require charge or work with charge, for example charge coupled device (CCD) or capacitors, charge is considered. Today, the understanding of electronic circuits is based on current and voltage, often neglecting charge for simplification.

Current is related to the movement of charge. As such, it does not resemble a new basic phenomenon but is mere a reformulation of the nature of charge with respect to time. With the Maxwell equations [6], current (density) can be formulated as the movement of charge:

$$\nabla \times \vec{H} = \vec{J} + \frac{\partial \vec{D}}{\partial t} \qquad \text{Maxwell I} \tag{1.1}$$

$$\nabla \times \vec{E} = -\frac{\partial \vec{B}}{\partial t}$$

$$\nabla \cdot \vec{D} = q_\mathrm{v} \qquad \text{Maxwell III} \tag{1.2}$$

$$\nabla \cdot \vec{B} = 0$$

Applying the divergence to (1.1), interchanging the derivations and substituting (1.2) gives:

$$\nabla \cdot \vec{J} = -\frac{\partial q_\mathrm{v}}{\partial t} \tag{1.3}$$

Considering $\nabla \cdot \vec{J}$ at a cross section of a conductor (i.e. no closed surface) leads to the fact that the amount of passing charge per time resembles the current. In this sense, charge is the integral of current with respect to time. The physical dimension of the setup does not play a role in this description. The movement of charge over time is integrated into the concept of current in the conductor.

Voltage, in contrast, is related to the field strength resulting from the existence of charge. In this context, the electrical field is the basis for the description of voltage: Integrating the field over any path between two points $\vec{A}$ and $\vec{B}$ results in the potential difference between these two points. The potential difference is called "voltage" in electronic systems. The third Maxwell equation (1.2) states that the sources of the electrical field is charge. Accordingly, due to the integration path between the two points to derive the *voltage* from charge, the physical dimension of the setup is of importance for the result. Voltage thus combines the existence of charge with the physical location of the charge into a single quantity. For the understanding or design of electronic circuits, this is an important factor.

Describing a circuit using current and voltage abstracts from the physical extension of the locations containing charge and from the time dependent position of charge. Instead, the physical dimensions are integrated into the voltage and the time dependence of charge locations into the current. The resulting rules to describe, analyze or understand an electronic circuit thus are using discrete components, reducing the physical circuit onto a netlist with only discrete coordinates. These rules are the Kirchhoff rules [5].

The limitations of using current and voltage can be derived from the ways they are defined. The physical dimensions of the system are neglected and the description is reduced to a netlist. Assuming ideal correspondences between physical devices and netlist models, only the system structure is reduced. But already this simplification is only valid for certain situations. The connections between the circuit components exhibit resistive, capacitive and inductive behavior in reality. The difference between idealized and real behavior can be severe. If direct currents (DC) in the circuit create significant voltage drops across the interconnect resistances, the netlist is imprecise. Neglecting the differences results in errors for the description of the circuit by a netlist instead of by a complete physical model. In case the field in an insulator results in significant current (compared to the DC purposely involved in the circuit), again the netlist would not describe the circuit well. Similarly, if the alternating current (AC) parameters of the circuit are significantly altering the circuit response due to the capacitive or inductive behavior of the interconnect system, this would also create mismatch between real physical model and netlist. In the circuit design process, this has been addressed with post layout simulations, where the interconnect system is integrated into the netlist using additional resistors, capacitors and sometimes inductances. These limitations become significant when adjacent wire distances reduce, wire aspect ratios increase (length to cross section) and when the circuit operation frequency increases. As this is the case for modern semiconductor

technologies, the netlist description of a circuit becomes more and more challenging to match to reality.

Instead of using current and voltage, an equivalent method would be to describe a circuit with the physical dimensions, charge and time. Listing "time" is important since current and voltage allow for the full description of any circuit with constant input quantities (when currents and voltages are independent of time, e.g. the direct current (DC) operating point). Yet for the same circuit, using charge requires the time aspects for dissipative elements (e.g. resistors) as they require a certain amount of charge to continuously flow. Efforts have been invested into the restructuring of electronic thinking with respect to charge. For example in [52], a simulation model based on charge and voltage is suggested, with appropriate correspondent circuits between the two domains. The improvement in simulation accuracy and speed is significant, even though the simulation has been carried out for relatively old technologies. Several concepts for circuit design build on the basis of charge. For example CCDs [24], switched capacitor (SC) circuits [25] or charge domain devices (CDDs) [36] are implementations of circuits that are described using charge and voltage. In order to match the common understanding of circuits, which is based on current and voltage, these devices are used within a time discrete context. The time discrete circuits (e.g. switched capacitor circuits) forbid the use of dissipative components. This simplification is similar to neglecting physical dimensions when considering voltage. With these circuits, the charge is transferred continuously in terms of the sampling character, and it again allows for the established understanding by current and voltage.

Charge within complementary metal oxide semiconductor (CMOS) circuits is dissipated due to the charging and discharging of capacitors. During a rising edge switching event in conventional CMOS logic, charge is transferred from the power supply to the gate output connection and further to ground once the falling edge follows. The total amount of charge stored in the output capacitor is lost during charging and discharging phase. Adiabatic circuits are a special construction of digital circuits using CMOS components that allow to circumvent this limitation [140]. These devices use a four-phase clock system that allows to recover charge during alternating clock phases [46]. A drawback from this approach is the reduced switching speed as circuits must operate at least four times slower than conventional CMOS designs. To allow for efficient charge recovery, the speed must be at least ten times less [93] than the maximum switching speed.

Apart from the circuit designer's point of view, charge is also considered highly important in other areas of electronic circuits. These areas include the technology design and verification (e.g. dielectric characterization and non-volatile memory design) and many techniques for physical failure analysis (including for example scanning electron microscopy (SEM) and derivatives, capacitive atomic force microscopy (AFM) and photoelectric laser stimulation (PLS)).

In this work, exemplary results are presented by the use of charge and voltage instead of current and voltage. It is shown, that from considering charge, currents

down to atto amperes can be measured while the dynamic response of the measurement system to the current is directly connected to the level of current involved. The examples given to show these powerful properties of charge investigation include the characterization of dielectrics, the investigation of focused ion beam (FIB) influence on insulating targets and finally questions related to security integrated circuit (IC) devices.

The next chapter introduces techniques used within this work and gives a very brief overview on topics investigated. Subsequently, in Chapter 3, different techniques for measuring low currents and limitations for the measurement of low currents are presented. Instead of measuring current, charge can describe certain effects under the above outlined circumstances better. Chapter 4 discusses different concepts that allow for the measurement of charge by example and by a conceptual view allowing for direct deduction of a possible approach to an implementation. Finally, Chapters 5 and 6 document the implementation and application of a charge measurement device for different use cases, respectively. The work is concluded by a summarizing remark with an outlook to future research work in Chapter 7.

Chapter 2

Context of Charge

This chapter aims at supplying a basis for the discussion during the later parts of this work. As a consequence, only those charge related topics in electronics are presented and shortly summarized that are actually part of the experiments. These are the application of FIB, dielectrics as insulators and semiconductor behavior. In Section 2.5 the behavior and analysis of capacitor divider circuits with tunneling currents is introduced and in Section 2.6 aspects of security ICs that become important in the context of charge are considered. This chapter can be skipped if the reader is familiar with the presented techniques.

2.1 Focused Ion Beam

Focused ion beam (FIB) technology is widely established in semiconductor manufacturing industry. Even though the applications are so ubiquitous, the precise control of the system on arbitrary samples is challenging. In the following subsections, the functionality of the FIB system is explained along with a brief summary of its use today.

2.1.1 FIB Technology

A FIB is very similar to a scanning electron microscopy (SEM) setup. A good review on the setup of a FIB system is given by [39], and [111] summarizes the physical effects. There exist numerous books on the topic of FIB, for example [76, 90]. Figure 2.1 shows a rough schematic of a usual circuit edit (CE) FIB system. A FIB consists at a minimum of an ion source, a beam forming unit and a secondary electron (SE) detector all enclosed in a vacuum chamber. Common specimens for the ions in a FIB system include gallium ions (Ga^+) [39], xenon ions (Xe^+) [131] and recently also helium ions (He^+) [102, 154]. The ion source is conditioned by the suppressor and extractor to supply a continuous flow of ions from a relatively small spot. The beam forming unit (here consisting of lenses, quadrupoles and octopoles) can target the beam such that all ions from the source, that reach through the aperture, impinge

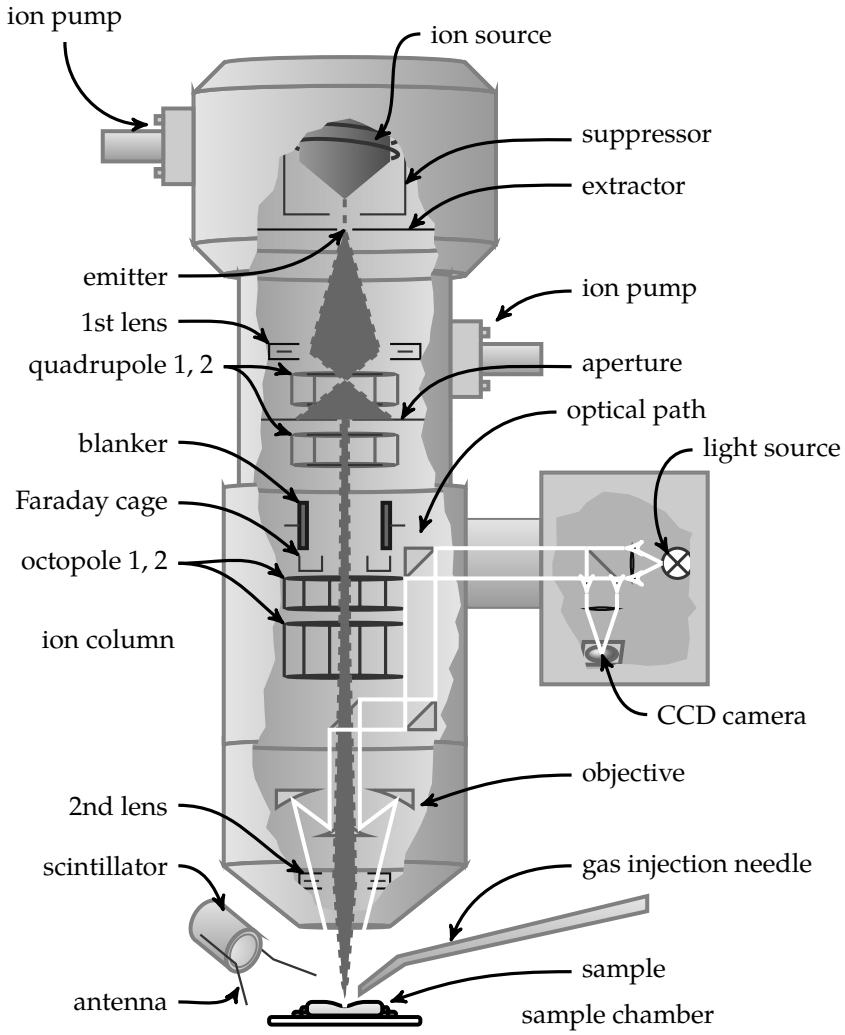


Figure 2.1: Schematic of the FIB system used throughout this work [117]: an OptiFIB from DCG Systems. The individual components roughly correspond to any CE FIB system. The optical system is special to the OptiFIB.

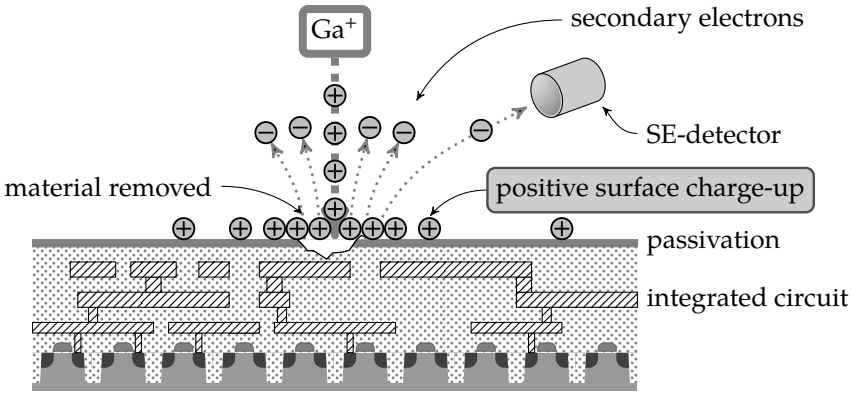


Figure 2.2: Surface charging model from FIB irradiation: Due to the incident ions and the emitted SE, the insulating surface charges up when irradiated by the FIB. The charge stays localized at the incident spot due to the insulating nature of the IC surface.

on a small spot on the target. The resulting spot size can be relatively small, in the range of single nanometers [76], though the destructive nature limits the resolution [53]. Often, a beam blanker allows to stop the beam from reaching the sample at all, bringing the interaction and destruction to a halt. In this work, the OptiFIB from DCG Systems is used, which includes a coaxial optical system into the ion column. This allows for in-situ optical monitoring of the sample, for example using near infrared (NIR) light. In backside FIB processes on silicon ICs, the silicon is transparent for NIR light allowing for navigation by metal structures on the opposite side of the sample.

Due to collision of the ions with the target, electrons with low energies (below 50 eV) are emitted, so called secondary electrons (SEs), and subsequently captured by the scintillator. Using the scintillator as an SE detector and the common technique of scanning, an image is formed, just like in an SEM. In order to allow the destructive and constructive work of a CE FIB system, a gas injection needle is used to target a precursor gas directly onto the surface of the sample. The ion beam then activates the reaction of the gas with the sample locally at the incident spot and thus enables the nano machining capabilities of a FIB [111]. By the use of the gas, the material removal is sped up significantly, up to a factor of 10 to 20, for the selected material [39, 72].

Figure 2.2 shows a schematic view on the interaction between the ion beam and the device if an IC is targeted. The impinging ions remove or add material, depending on the precursor gas used (not shown), allowing to reach buried layers or add new electrical connections between interconnects. Furthermore, the emitted SE are captured by the SE detector to image the device allowing for navigation. Yet, this SE emission, and additionally the neutralization of impinging ions cause deposition of a positive charge on the device surface. The insulating passivation of any IC does not allow for the conductive removal of this surface charge, introducing multiple problems. Emitted SE are re-captured by the Coulomb attraction to the positive surface charge, reducing the available amount of SE for imaging. This hinders proper

navigation on the sample, making CE imprecise in location. Once the surface charge is sufficiently high, electrostatic discharge (ESD) can happen into adjacent nodes of the IC device, irrevocably damaging it. Consequently, preventing ESD from happening is a major goal of every FIB operator. These facts make up for an increased interest into the charging dynamics during FIB tasks on insulating targets. Investigation of the charging in FIB columns is part of the discussion of this work, see Section 6.2.

2.1.2 FIB Applications

Material analysis Due to the high mass and large diameter of ions, their penetration depth is limited to tens of nanometers [55, 72], allowing for surface analysis. Using the destructive property of the ions, a cross section can be created with nanometer precision in positioning [89, 111]. This is useful for material analysis, as the tedious and imprecise mechanical polishing for the creation of a cross section can be replaced with an adequate FIB procedure. The creation of transmission electron microscopy (TEM) lamellas is improved in time and precision by using a FIB significantly [60] as it is a similar process as that of creating cross sections.

IC technology laboratories Apart from cross sectioning, circuit edit (CE) is a very important application. Using different precursor gases in a CE FIB system allows to selectively remove material or add insulating or conductive material. Thus, IC hardware can be modified on a nanometer scale, allowing to restructure modern IC devices destructively and constructively [69, 74]. Especially with the optical system incorporated into the FIB column, backside circuit edit and debugging [62] is made possible by the transparency of silicon for the NIR light.

Gases used in CE FIB systems include precursor gases based on tungsten (W), platinum (Pt) or molybdenum (Mo) to allow for the creation of conductors. Precursor gases that deposit insulating material are also available, though the resulting material properties are far from ideal. Still, their applicability to IC restructuring is very useful [37].

IC design process is significantly sped up if a FIB is used for debugging. Though vendors try to get the design of a new IC right in the first place, this is seldom achieved. Due to the high complexity of IC devices today, their fault-free implementation and construction is very difficult – if not impossible! Using a FIB system, the process of correcting the design is improved. Figure 2.3 shows rough phases of the design process of a new IC, though this might depend on the actual manufacturer work flow. Yet, the manufacturing of IC samples from the design data set (i.e. “mask production” and “silicon production”) is always in the range of several months in duration. This directly limits the lower bound in time required to create a new product. FIB technology allows to restructure a circuit on a nanometer scale within a few hours of work time. Individual samples of the IC (i.e. engineering samples) can be created and subsequently verified quickly allowing for a faster rework of faults in

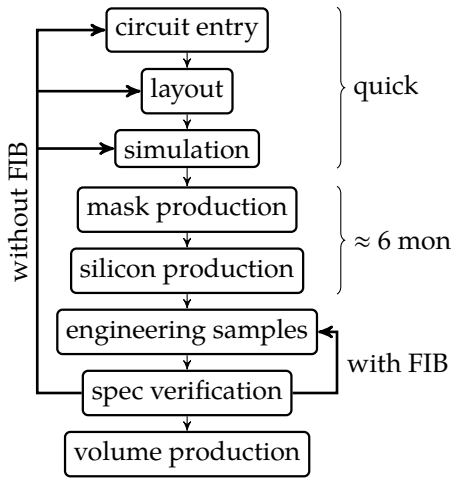


Figure 2.3: Usage of the FIB service during the development of an IC. The main advantage arises from the reduced cost compared to device manufacturing (masks and first silicon production) and the shortened round-trip-time between subsequent engineering sample verifications.

the design of the IC. Verification and debugging now can be done on the first version of an IC and allow to produce a working version of the same IC with the second version.

The ease of application of the FIB system makes the use in very many different fields of technology highly attractive. Consequently, the number of different applications of FIB tools increases continuously [72, 147]. Yet, the current driver for FIB technology remains the semiconductor industry, leaping towards ever smaller dimensions. As the time to market is a key factor for successful product placement, the FIB technology is driven by direct economical decisions.

2.2 Manufacturing of Insulators

Insulator manufacturing has evolved into one of the most difficult tasks in IC technology design. The first successful production of metal oxide semiconductor (MOS) based circuits happened when the gate oxide was sufficiently reliable in volume production. Only by the use of the compound of silicon and silicon dioxide, this condition could be met. Today, silicon dioxide is vanishing more and more from the system as new insulators with better properties are developed. Their contribution to state of the art devices is very important. Shrinking device sizes and increased signal speed requirements lead to the development of high-k dielectrics for gate oxides and low-k dielectrics for inter level dielectric (ILD) usage. Using high-k dielectrics as gate oxide increases the amount of charge in the channel of the transistor, allowing for higher conductivity when the transistor is “on” [146]. Reducing the dielectric thickness instead is not possible due to increased leakage currents. Thus, signal transition increases in speed and allows for higher clock rates through this mechanism,

just as shrinking gate length would do, too. At the same time, signal speed can be accomplished by reducing the wire capacitances, as those are dominant in modern circuits [146]. This is improved when the dielectric constant is decreased in the ILD. Yet, using vacuum (k = 1) is impossible as ILD because of missing mechanical stability. Modern low-k dielectrics instead build not only on a material with lower dielectric constant but also on "including" vacuum in their structure [123, 146]. Yet, the problems when using such material are numerous [159] making good electrical measurement capabilities required.

For investigation of dielectrics, the properties are evaluated in a relatively short time-frame during the technology design, but the results should be valid for the whole lifetime of the final circuit produced with the technology. To overcome this limitation, different methods are used to extrapolate the behavior to the device lifetime. The methods include increasing temperature, voltage or current, though the precise mechanisms are of much debate. All methods build on the precise measurement of the characteristics of the dielectric. The characteristics are mainly the insulation behavior (e.g. leakage current), the breakdown behavior and probably mechanical, physical or chemical alteration of the dielectric structure by aging. As the physical mechanisms of oxide stress changes fundamentally with the type of dielectric [12, 15] and even the dielectric thickness [59], the methods of investigation were altered and adjusted frequently. A full review would lead too far for the purpose of this work. Earlier methods of investigation were mainly based on the breakdown behavior of dielectrics but recent studies evaluate the pre-breakdown behavior (e.g. leakage currents) [123, 134, 135]. Especially the leakage current evaluation requires the measurement of very low currents. A common way to implement such measurements is to increase the cross sectional area of the dielectric to a value that allows for a sufficiently high measurable absolute current [92]. This method does not allow for the separation of intrinsic behavior from defect originating behavior as such structures are very unlikely to be defect free. Furthermore, the post-electrical characterization of the actual stress impact is difficult if the location of stress is unknown [135]. Instead, using very small areas to investigate the intrinsic behavior of a dielectric requires current measurements well below the pico ampere range. For example, increasing the voltage across such dielectrics and measuring the current during this voltage ramp would allow for the measurement of hundreds of femto amperes, yet take a very long time of stressing the dielectrics of around 5 min [135].

One of the earlier techniques for dielectric analysis is the measurement of injection charge or "charge to breakdown", Q_{inj} [59] and Q_{bd} [66], respectively. The value for Q_{bd} is derived by integrating the current through the dielectric until the breakdown occurs, usually done by conventional measurement means. Other methods include the analysis of interface traps [80] or the time dependent dielectric breakdown (TDDB) [65]. Modern dielectrics do not exhibit a sharp breakdown anymore, instead they increase in conductivity but stay (partially) insulating [94, 98]. When observing this process carefully, the difference between direct tunneling current as leakage and trap assisted leakage can be used to predict the breakdown behavior, which is called stress

induced leakage current (SILC) [73]. As the investigation of dielectrics is a very vivid topic in semiconductor industry, the amount of information is close to unlimited and growing. A summary of different physical effects is given in [94] and a good review from the IC perspective is for example [98]. Many of the characterization methods for dielectrics consider the amount of charge traversed through the dielectric during characterization. Yet, measurements are often done by integrating the current which yields a bad measurement performance. This work applies the presented charge measurement methodology to the evaluation of pre-breakdown behavior of dielectrics. Because charge is measured directly, the measurement precision is improved and the benefits are shown in Section 6.1.

2.3 Semiconductor Manufacturing Technology

The manufacturing of ICs not only requires to fabricate insulators but also the implantation of dopants into the semiconductor base material. The processes involved during manufacturing have many different influences, some of which can severely affect the functionality and reliability of the end product. For example ion implantation, chemical mechanical polishing and wafer handling are intrinsically dangerous production steps for ICs. These processes deposit varying amounts of charges onto the device surface which can degrade the performance, possibly rendering the device faulty before manufacturing is finished. For example, surface charging during the different steps of film application and delamination for wafer thinning in post production steps can cause electrostatic discharge (ESD) events to occur, damaging the device. As a consequence different control methods have been used in the past, that allow for monitoring of these types of failures.

Once the device is finished in fabrication, ESD protection circuits allow for safe handling. Before such structures are functional on the affected nodes of a circuit, this approach is not possible. For example when the implantation of dopants for diffusions and polysilicon gate layer is done through an ion implanter, the introduced charge damages the already produced gate oxide, below the polysilicon structures. To prevent against severe charging during such a process careful process control mechanisms and strict design rules during the construction of the circuit layout are necessary. “Antenna” structures and antenna rules are used for this purpose.

Small transistors are fabricated that have large areas of gate layer connected to their gate terminal. During processing, the large area collects effects from the process, for example the ion implanter process. This influence is then concentrated on the relatively small transistor. Measurement of the transistor parameters after production allows to estimate the influence from the process. For example the gate current or the breakdown behavior of the transistor can be used for this purpose. As the large collection area works as an “antenna”, the design rules stemming from this analysis are often called “antenna rules”. They force an upper limit of the amount of polysilicon area and metal area that is allowed to be connected to a transistor gate. In this sense, the “antenna” test structures violate this requirement in order to control

the process for the antenna rules.

2.4 Semiconductor

The physics of semiconductors can be regarded on many different levels of abstraction. In order to keep the involved models targeted to the topic of this work, only a very basic model is discussed. A textbooks on this topic which covers semiconductor physics is [26, 84, 85, 96]. The present text is inspired by the way of explanation also found in [85, 105]. The metal oxide semiconductor field effect transistor (MOSFET) is the most frequently produced part on the basis of semiconductor physics these days. It will be considered in Section 4.1.3 as it is actually a charge detection device. The semiconductor basics for the MOSFET functionality are summarized here.

The Poisson equation describes the relation between electrical field $\vec{E}$ and net charge density ρ:

$$\nabla \cdot \varepsilon \vec{E} = \rho$$

In 1-dimensional situations the potential Φ can be described as:

$$\frac{\partial^2 \Phi}{\partial x^2} = -\frac{\partial E}{\partial x} = \frac{\rho}{\varepsilon} \tag{2.1}$$

with E as the field in x-direction and ε as the dielectric constant. In semiconductors, the net charge density consists of mobile carriers and fixed dopant atoms. The mobile carrier concentration can be approximated by the Boltzmann statistics [105]:

$$n\,, p = n_\mathrm{i} \exp\left(\frac{\pm\Phi}{\mathrm{k_B} T_\mathrm{abs}}\right)$$

Here, n_i is the intrinsic carrier concentration which is material and temperature dependent (${n_\mathrm{i}}^2 = N_\mathrm{C} N_\mathrm{V} \exp\left(\frac{-W_\mathrm{G}}{\mathrm{k_B} T_\mathrm{abs}}\right)$) and which stems from the assumption of equal carrier densities $n = p$ for semiconductors without impurities. Φ is the difference between Fermi energy and intrinsic Fermi energy $\Phi = W_\mathrm{F} - W_\mathrm{i}$, which is proportional to the potential from the Poisson Equation 2.1. Fixed dopant atoms are impurities that change the value of W_F and accordingly also of Φ. The net charge density can then be written as

$$\rho \frac{1}{\mathrm{e}} = p + {N_\mathrm{D}}^+ - n - {N_\mathrm{A}}^- \tag{2.2}$$

where e is the charge of a single carrier in Coulomb and ${N_\mathrm{D}}^+$ and ${N_\mathrm{A}}^-$ are the concentrations of ionized impurities of donor type (positively charged) and acceptor type (negatively charged), also called dopants. At room temperature and with common material impurities, ${N_\mathrm{D}}^+$ and ${N_\mathrm{A}}^-$ can be set equal to the designed dopant concentrations of N_D and N_A (fully ionized semiconductor). For a semiconductor without field, ρ becomes zero and Equation 2.2 allows to determine Φ, which is called Φ_B

(bulk potential) in this case.

If a semiconductor surface is subject to an impinging electrical field, two different situations can be distinguished in Equation 2.2. The potential at the surface is called Φ_S (surface potential) in all cases. Either the exponential functions of n or p dominate the behavior of ρ in Equation 2.2 if $|\Phi_S| > |\Phi_B|$, or, if $|\Phi_S| < |\Phi_B|$, the fixed dopant concentrations ${N_D}^+$ or ${N_A}^-$ dominate ρ. For the latter case, the impinging field is absorbed (described through Equation 2.1) by the fixed dopant concentrations, resulting in a penetration depth of the field proportional to the square root of the surface impinging field ($x \sim \sqrt{E_S}$). The region of non-zero electrical field inside the semiconductor is called space charge region (SCR). In this case, the mobile carrier concentrations are small compared to the dopant concentration. This condition contains the following states of the semiconductor: flat band ($\Phi_S = \Phi_B$), depletion ($0 < \frac{\Phi_S}{\Phi_B} < 1$), mid-gap ($\Phi_S = 0$) and inversion ($0 > \frac{\Phi_S}{\Phi_B} > -1$).

For the other case ($|\Phi_S| > |\Phi_B|$), the impinging field is absorbed by mobile carriers in the first place. Due to the exponential dependence of n, p on Φ_S, arbitrary carrier densities can be created without severely affecting Φ_S. These carriers distribute according to the Debye length at the very close proximity to the surface, allowing approximation as surface charge, which is normally only found in conductors. This means that the amount of field absorbed within the semiconductor does not change and any additional impinging field is absorbed by the (mobile) surface charge density. This situation is called either accumulation ($\frac{\Phi_S}{\Phi_B} > 1$) or strong inversion ($\frac{\Phi_S}{\Phi_B} < -1$), depending on the sign of Φ_S.

According to this argument, the charge densities of a semiconductor are subject to the electrical field strength within the semiconductor material. As the mobile carrier density allows for current transport by movement, this behavior can be used to measure field (or charge) with the conductivity of the underlying semiconductor material. As is presented in section 4.1.3, the MOSFET builds onto this characteristic.

2.5 Tunneling Currents in Insulators

Tunneling is the phenomenon that charge carriers can penetrate through an energy barrier which is higher than the energy of the carrier. Multiple different kinds of tunneling have been investigated in literature, for example Fowler-Nordheim (FN) tunneling [12], Poole-Frenkel (PF) tunneling [15], and direct tunneling [48]. Classical mechanics do not allow for these phenomena to happen, quantum mechanic theory is required. In this work, tunneling is a source for error in measurement results in one part and a requirement for successful operation in other parts. The model of FN and PF tunneling are summarized as their behavior is used for simulation later on. In this sense, the present section highlights two types of tunneling which are present in the materials used within the scope of this work.

Fowler-Nordheim tunneling [12] builds on a triangular barrier, which is modulated through an externally applied electrical field. The barrier modulation in turn alters the probability of carriers tunneling through it. Many improvements of this

model were suggested, for example the barrier form and temperature dependence were adjusted [23]. FN tunneling limits the entering of carriers into the insulator through the conductor-insulator interface at the emitting side. Once the carriers have tunneled through this barrier, they are conducted in the insulator (i.e. in the conduction band) and accordingly FN tunneling is an emission mechanism and limited by the conductor-insulator interface. Poole-Frenkel tunneling, in contrast, assumes a concentration of trap centers, where carriers can tunnel from one trap center to the next [15]. Accordingly PF tunneling is a transport mechanism inside the insulator and is thus limited by the insulator bulk material. Depending on the type of insulator and amount and character of trap centers, either PF or FN tunneling dominates.

Tunneling currents with known tunneling characteristic are plotted according to the characteristic to yield a straight line. The characteristics of tunneling are

$$J = aE^2 \exp\left(-\frac{b}{E}\right)$$

for FN tunneling, and

$$J = cE \exp\left(d\sqrt{E}\right) \tag{2.3}$$

for PF tunneling. The coefficients of the two tunneling mechanisms can be expressed in terms of material properties [15, 23]. As no sufficiently precise data is available for the materials used in the course of this work, only experimental data is used to fit the coefficients. Appendix A contains the measurement results and tunneling characteristic coefficients a, b or c and d for the corresponding materials. Accordingly, FN tunneling is plotted as $\frac{J}{E^2}$ against $\frac{1}{E}$ in a semilogarithmic scale to yield a straight line. For PF tunneling the plot is $\frac{J}{E}$ against $\sqrt{E}$ in a semilogarithmic scale for a straight line. Using this representation, the coefficients can be easily calculated from the slope and offset of the linear approximation. The tunneling coefficients are derived in Appendix A for the materials used as insulators in the technology of this work.

2.6 Security of Electronic Hardware

In the present economy, the process of revenue for a specific service is often not obvious. Especially in the market of software (apps, games and the like) and consumer products (smart phones, tablets, etc.), the price for a given item is in no correlation to the manufacturing and distribution costs. In such a case, vendors are interested in keeping the control over the product to support the process of revenue during use time. Often, the revenue is based on the use of the vendor's infrastructure (like in telephone companies "locking" the device to the use with their own infrastructure, only) or through the distribution of advertisement and data collection (similar to the way Google supplies it's devices through it's software structure). Similar to

this, pay-TV providers want to ensure that a given customer can only watch the provider's content in well-defined circumstances. Specifically, recording, duplication or redistribution of the contents should be avoided, for example. In all these scenarios, strong encryption algorithms are employed that protect the specified good in such a way that the customer can only use it in the desired ways. The encryption protects the contents because the customer does not have the key material to decipher the information. Instead he is only in possession of a special device which can perform the decryption. This device acts according to the control of the vendor and thus enforces the desired usage scenarios. The confidentiality of the secret key material is the basis for a successful implementation. Often, the devices given to the customer contain an IC which fulfills this function. Such IC devices are equally often called "smart cards" within the security community and will be labeled "security IC" here.

A security IC can be defined as an IC which *stores* (and possibly protects) sensitive information. "Sensitive information" can resemble secrets (i.e. user supplied material not to be disclosed to third parties) or secret key material, which allows to decipher secrets. As such, an IC containing a block cipher algorithm in hardware (e.g. advanced encryption standard (AES)) is *not* a security IC because the secret key material must be supplied to such a device. In contrast, a memory device can be a security IC as it can store secret data or secret key material. In security ICs today, multiple functions are implemented, for example storing, encrypting and decrypting secret information together with authentication procedures. This improves the control of the IC over the usage of the secret information.

As the most challenging task with cryptography in systems that are given away to possible adversaries (like mobile phones, bank cards, pay-TV systems, etc. are physically in control of the customer) is secret key storage [51, 99], this is the core functionality of a security IC. Often, the algorithm employed for encryption is easily reverse engineered or even part of the public domain (e.g. AES), thus offering no protection. As many of the mentioned services require the use of private keys directly within the product, the duplication of theses keys is the only part protecting the contents from being used outside the product. Due to the nature of information distribution in such systems, the loss of private key material is a scenario that should never become true. Subsequently, vendors of conditional access systems have improved the security of systems significantly over the last tens of years.

Many different ways exist to read out private information from physical devices. Basically, the methods can be categorized in different ways. For the purpose of this text, the *invasiveness* of the approach is a practical choice for categorization of attacks. This categorization has already been suggested in literature [83]. Three different categories can be distinguished: non-invasive, semi-invasive and fully-invasive.

- Non-invasive attacks for data ex-filtration act on the targeted IC in a way, that internal signals are not recorded individually. Instead, only the system can be observed as a whole. Measuring the power consumption or the time for signal

processing [61] would be such examples. Many of the attacks in this category are side channel analysis (SCA) attacks.

- Semi-invasive attacks allow for certain, system level modifications to the attacked device. For example opening the housing of a device chemically [51] or mechanically [139] would be such an approach. Subsequently, interaction between an arbitrary analysis system and the attacked device can be carried out. Instead of measuring the response from the whole circuit, individual parts of the circuit are analyzed separately. For example using electron beam probing (EBP) [32, 43, 109], individual top layer metal lines can be probed and subsequently data can be reconstructed. Using a NIR optical system for frontside or backside analysis, individual circuit blocks or transistors can be targeted [120, 151]. It is important to note, that the system level modification is not necessary for this attack class since individual circuit components can already be measured on packaged samples. For example using an electro magnetic (EM) probe on a packaged device yields information about specific parts of the circuit [71, 78, 113]. Due to the nature of the attack, the circuit is sound and operates as the manufacturer intended it to do.

- In contrast to semi-invasive attacks, fully-invasive attacks also allow for the modification of the circuit itself. Fully invasive attacks are the most powerful but also most expensive attacks. This class includes using a laser to disable certain parts of the system, using a focused ion beam (FIB) system to access or modify transistors or interconnects [127]. The special difficulty with this type of attack is within the manufacturer not knowing what part of a system the adversary might remove or modify. For example, using a FIB system, an attacker can act on any circuit node or transistor inside the IC [126, 141].

The categorization of attacks on secure ICs is without doubt of much debate in the scientific community [51, 122]. It is obvious that the given categorization is by far not a standard. As the present text is based on the physical nature of systems, the use of a physical categorization seems appropriate.

Means and methods to thwart non-invasive attacks have been long proposed on software and hardware level. The research into different CMOS design techniques to thwart power leakage is extensive [138]. To thwart semi-invasive attacks is more difficult and thus not as thoroughly based today. Yet, means exist to counteract semi-invasive attackers, too. For example the semi-invasive attacker can often be thwarted by implementing operation counters and preventing certain operations or erasing secret data if the counter reaches a certain critical value. Other means including the use of redundant logic have been suggested to prevent the different fault-induction attacks [83]. Light sensors are used to detect the malicious application of laser scanning to security devices [121, 156]. Modern smart cards route sensitive signals only on lower metal layers and place additional shields on top to prevent the read out using needles [127] or EBP techniques.

The most difficult task in attack prevention is with the fully invasive attacks as the fully invasive attacker is capable of reading any signal available on an IC. This would allow wiretapping onto all data processed by or stored on the IC. If such a technique is applied to a security IC, the secret data would be disclosed, even if the manufacturer implemented "sensors" that are capable of detecting the invasive attack: The invasive attacker would simply disable the sensor and still read out the secret information [127]. Encapsulating the sensitive parts into meshes with integrity checks has been used in products [121] but proven inapplicable to fully-invasive attacks [127, 142]. Thus, the IC must not only detect the invasive attack but also, at the same time, disable access to the secret information permanently — in the most physical sense of data destruction.

Memory reading techniques have been shown for various applications. For example chemical removal of the bulk silicon material (this is termed "backside access" in failure analysis (FA)) can allow for the reading of the state of non-volatile memory (NVM) cells [101]. In Section 6.4, the reading of fuse bit state is shown using a FIB system [142]. Consequently, storing secret data unencrypted in NVM is considered insecure today. A promising alternative is the use of physically unclonable function (PUF) for the storage of secret key material. The original concept of a PUF was a means of authentication in a special protocol [77]. The PUF maps specific input challenges (i.e. input data, originally the incident angle of a laser beam onto the PUF) to specific output responses (i.e. output data, originally the optical speckle resulting from the laser beam interacting with the PUF). The key feature is, that the PUF response can not be predicted for an unknown input challenge, even if many challenge response pairs (CPRs) are known for a PUF instance. Thus, only the actual PUF instance can respond to the challenge correctly, allowing for an authentication procedure. If furthermore the challenge space is large (i.e. the PUF can not be characterized physically or through the CRP interface with sufficient detail in a certain time), this property effectively prohibits to clone the PUF instance.

Recent implementations of PUF concepts into IC products do not use this approach. Instead, the PUF is used to protect ICs from invasive analysis techniques [106, 107]. In order to do so, the response of the PUF is used as encryption key for secret data [110]. Without the specific PUF instance, the secret data can not be deciphered, effectively making the PUF to a secret key storage. The fundamental difference of this context to the initial PUF idea is, that the PUF is used to always generate the *same* secret key. Accordingly, the challenge response behavior is reduced to only a single challenge and a single response. Many different attempts were made to formalize the properties of a PUF in this use scenario [107, 119, 124, 129, 137, 152]. Without going into too much detail, it is clear that, on a given deterministic system (e.g. an encryption device), the output can be mathematically reconstructed if all input quantities are known. Thus, hardware analysis techniques allowing to wiretap on all signals on a device allow for the extraction of all information, including the encrypted information. In order to prevent against this analysis by the use of a PUF, the whole circuit must be built such, that when performing the analysis technique on any part of the system, the behavior

of the PUF substantially changes. In this case, the analysis technique can only be able to wiretap on the altered behavior, which must be uncorrelated to the initial behavior of the device containing the secret information.

The IC analysis can be conducted in many different ways making the implementation of a PUF challenging. Even with respect to charges, the PUF concept and implementation can take many different characters. As PUFs are built to keep information from being analyzed from the outside and at the same time to be very sensitive to invasive modifications, the use of (very few) charges seems promising: Already small changes can cause a severe alteration and analyzing few charges with outside equipment is complex. In Section 6.3, a circuit is shown to be tamper evident to the application of a FIB attack allowing for a successful PUF construction with respect to FIB modification attacks. Section 6.4 will finally discuss alternative approaches to the problems involved with respect to security IC hardware. Especially the properties of the most frequently used PUF implementation – a static random access memory (SRAM) PUF – are shown to be inadequate for the use as secret key storage [148] or to prevent duplication [141], see Section 6.5.

Chapter 3

Ultra Low Current Measurements

Measuring low currents is identified in the introduction as an important part of circuit and technology design. Often, very complex devices are used to acquire these measurements with highly sophisticated means of improving the sensitivity. This chapter summarizes limitations that result from the character of charge or the character of most measurement setups.

The first section starts with a practical example of a current measurement system that can measure down to single digit femto amperes. It is shown that measuring such low currents is intrinsically connected to long measurement times. Subsequently, this is supported by analyzing the way such a current is generated on a discrete circuit basis, independent of the actual process or means of acquiring the ultra low current measurement. Finally, the character of current also places limitations on the achievable precision for a current measurement. These limitations lead to the analysis of charge, which is the topic of Chapter 4.

3.1 Practical System Setups

Current measurement systems are available off-the-shelf with capabilities extending down into the pico-ampere regime. For example, Keithley Instruments Inc. provides a semiconductor characterization system for measuring down to several tens of femto ampere (SCS4200) and Agilent Technologies Inc. has a similar system (B1500A). Though the vendors state that a resolution down to 0.1 fA [128, 143] is possible, the noise floor will be in the range of several femto amperes limiting the minimal current observable, stated in the same documents. Though these products are specialized high performance equipments, their limits are of significant magnitude.

Figure 3.1 shows an exemplary measurement with the Keithley Instruments Inc. SCS4200 Semiconductor Characterization system. To identify the measurement capabilities, a simple voltage step is applied to the unconnected terminals of the specific

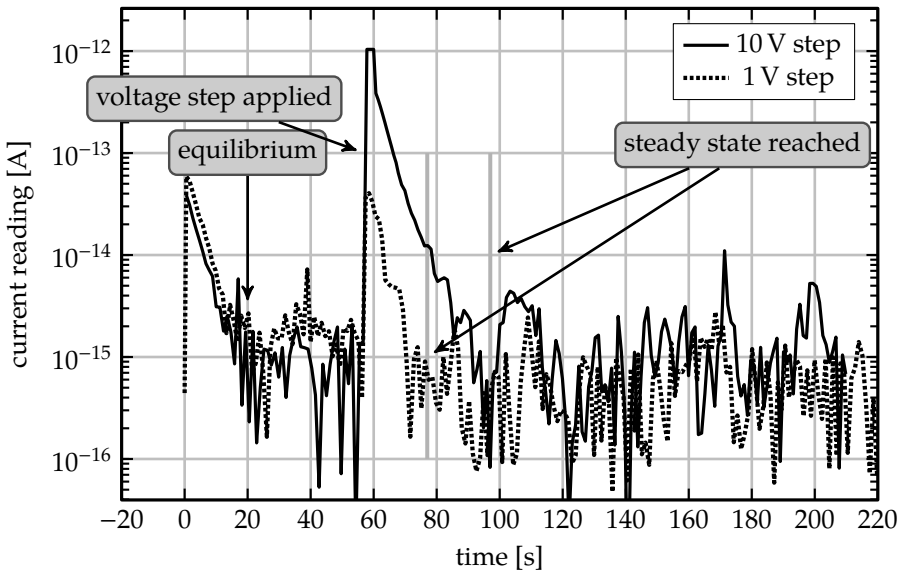


Figure 3.1: The Keithley Instruments SCS4200 system equipped with preamplifier SMU is subject to a low pass behavior.

source and measurement unit (SMU). The measurement system is set up to record the measured current over time. The current is expected to be zero after a specific setup time. The setup time is required to charge parasitic capacitances and let the voltage source of the SMU settle. Figure 3.1 shows a specific slope in current after initial setup and after the step is applied suggesting an exponential decay of remaining current. Obviously after starting the measurement, the system requires approximately 20 seconds to reach equilibrium. When the step is applied, the steady state is reached with the same slope for both step voltages. When applying a 10 V step, the time for settling to the remaining noise current of 2 fA…4 fA takes roughly 40 seconds, for a 1 V step, it takes 20 seconds. Both situations represent an estimated slope of 25 s per decade. The leakage current within the cable (10 fA in case of the 10 V step) do not show up with unconnected (triaxial) cables but the time constant is equal. To acquire the measured traces, special care has been taken to configure the system for continuous sampling at the specified sensitivity level and the leakage current in the cable is compensated for in the results figure.

As can be seen from Figure 3.1, the noise floor for the measurement is in the range of 2 fA…4 fA under steady state conditions without post processing. To measure a current of 1 fA, an average of 50 measurements could be applied (noise is then 0.28 fA…0.57 fA, acquisition of 50 measurements takes 50 s in this configuration). Furthermore, to settle to this level of current would require 40 s after each 1 V step, making for a slow measurement of only one measured point every 90 s.

Many measurement setups require a faster measurement acquisition. For example, the leakage current through dielectrics stresses the insulation barrier significantly. Once the stress voltage is applied to the dielectric, a current reading should be ac-

quired as fast as possible. Furthermore, if the leakage current is higher than expected, the measurement could be carried out faster than for very low leakage currents (according to the settling behavior of the measurement system). Still, measurement systems have fixed measurement ranges and timing setups that do not allow for such a flexible measurement setup. The method of using a standard high performance measurement system to measure in such a situation does not fulfill all requirements.

This setup already shows the difficulty of ultra low current measurements. Yet, an easy model can be analyzed resulting in exactly the same parameters for measurement timing. The next section will discuss this setup simplified on a discrete circuit basis and also derive parameters for the available timing.

3.2 Origin of Current

The measurement setup similar to the one used in the previous setup is schematically drafted in Figure 3.2. The device under test (DUT) is for example a dielectric test structure exhibiting a very low current conduction. Triaxial or coaxial cables connect the SMU to the DUT. The SMU applies a certain voltage to the setup and measures the current drawn from the DUT. The equivalent circuit is depicted next to the physical setup, showing the high-ohmic DUT resistance, the wire capacitances and the SMU voltage source with inner resistance. In order to attain a good voltage accuracy, the SMU output resistance must be less than the DUT resistance.

This is a first order low pass filter. The current at the voltage source (as measured over r_{SMU}) after the application of a voltage step ΔV_{SMU} can be expressed as

$$\mathbf{i}_{\mathrm{SMU}}(t) = \mathbf{I}_{\mathrm{SMU}}(t) - \mathbf{I}_{\mathrm{SMU}}(t \to \infty) = \frac{\Delta V_{\mathrm{SMU}}}{r_{\mathrm{SMU}}} \exp\left(-t \frac{r_{\mathrm{SMU}} + r_{\mathrm{DUT}}}{r_{\mathrm{SMU}} r_{\mathrm{DUT}} c_{\mathrm{wire}}}\right)$$

If $r_{\mathrm{SMU}} \ll r_{\mathrm{DUT}}$ holds, this equation only depends on the SMU, not on the DUT any more.

$$\mathbf{i}_{\mathrm{SMU}}(t) = \frac{\Delta V_{\mathrm{SMU}}}{r_{\mathrm{SMU}}} \exp\left(-\frac{t}{r_{\mathrm{SMU}} c_{\mathrm{wire}}}\right)$$

Accordingly, the measurement system limits the achievable bandwidth, depending on the voltage source output resistance.

As the exponential decay equals a first order low pass, the circuit from Figure 3.2 is

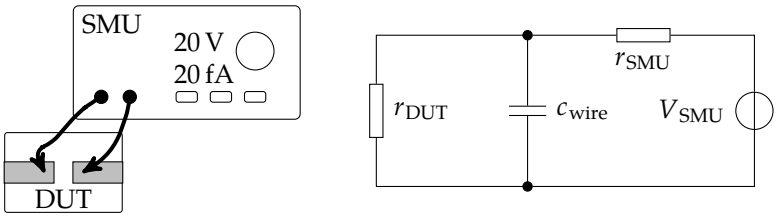


Figure 3.2: Model and equivalent small signal circuit of a DUT connected to an SMU

a valid model for the Keithley Instruments SCS4200 System. The slope from Figure 3.1 equals a $\frac{1}{e}$ decay after 10.9 s. Accordingly, the 3 dB frequency limit for measurement in the most sensitive measurement range is the reciprocal slope, roughly 0.1 Hz. From these parameters, an equivalent output resistance can be derived. For typical cable capacitances of 54 pF/m and the used cable lengths of 1.5 m the theoretically resulting equivalent small signal output resistance of the SMU is approx. $1.45 \cdot 10^{11}\,\Omega$. This is only the equivalent value, which does not necessarily resemble the real output resistance of the SMU.

The limited bandwidth of such a (high performance) measurement system is found in many commercial current amplifier and measurement systems [158], though they might change with specific purpose. Yet, the limited bandwidth directly limits the available acquisition speed that can be achieved with the system. Basically, this means that measuring low currents in the fA-range is speed limited by the measurement equipment for these setups.

3.3 Quantization of Charge

Not only the measurement equipment limits the available measurement speed for ultra low currents. A fundamental limit to any signal processing in electronic circuits is electronic noise. "Noise" incorporates effects of very different origins, for example thermal noise, the discrete nature of charge and memory effects. The thermal noise effect originates from the non-zero energy of the physical system processing the electrical signals. It was first theoretically described by Schottky [8] building on Einstein's observations about thermal equilibrium and natural oscillations. Later, Johnson measured this type of noise attributed to the thermal conditions of resistances and resistive conductors [11, 13]. The noise from the discrete nature of charge was observed in junction devices and termed shot noise [8, 9]. In this section, a brief description of three different noise phenomena is given: thermal (or Johnson) noise, shot noise and $\frac{1}{f}$-noise. The last part within this section deals with the Nyquist theorem and the therefrom resulting minimum amount of current per bandwidth.

3.3.1 Shot Noise

Shot noise [8, 10] is present in all electronic devices where charge passes through a relatively thin barrier. Examples of such electronic devices are pn-junctions, bipolar transistors (e.g. space charge region (SCR), tunneling mechanisms constitute the barrier). Due to the quantization of charge and from the fact that the passing charge transits through the layer on a discrete basis, the current is not continuous with the thermal movement of the carriers but has a burst character. The noise spectral density of shot noise is given by

$$s_{\mathrm{n,sh}} = 2eI$$

and for a given frequency band f_B, the root mean square (RMS) noise voltage gives:

$$i_{n,sh} = \sqrt{2eIf_B}$$

In order to measure I (i.e. a unity signal to noise ratio (SNR), $i_{n,sh} = I$), the bandwidth must be at most

$$f_B \leq I\frac{1}{2e} \tag{3.1}$$

From this point of view, a measurement bandwidth of 0.1 Hz allows for a current measurement down to $3.2 \cdot 10^{-20}$ A. This limit only applies if the current results from a barrier, according to the shot noise source.

3.3.2 Thermal Noise

If thermal noise [11, 13] is considered, a limit in the measurable current can be derived, too. The deduction needs a source of the current that exhibits thermal noise. To allow for thermal noise, a resistive characteristic is required, modeled by r_{src}. With the absolute temperature T_{abs} and Boltzmann's constant k_B, the noise spectral density from this resistance is, according to thermal noise:

$$s_{n,th} = 4k_B T_{abs}\frac{1}{r_{src}}$$

and the resulting RMS noise current in an observation bandwidth f_B is:

$$i_{n,th} = \sqrt{\frac{4k_B T_{abs} f_B}{r_{src}}}$$

For a resistive element, the current (measurement) is proportional to applied voltage, and the maximum bandwidth for unity SNR gives:

$$f_B \leq I\frac{V}{4k_B T_{abs}}$$

Note that the source resistance has been replaced by the applied voltage source.

Here, a measurement bandwidth of 0.1 Hz allows for current measurements down to $1.67 \cdot 10^{-18}$ A, if the voltage drop across the resistive current sinking element (noise source) is 1 mV. Note, that this also means that the resistance would be as high as $6 \cdot 10^{14}\,\Omega$.

3.3.3 $1/f$ Noise

The observation of a $\frac{1}{f}$ spectral power density from noise is called flicker noise. The actual source of flicker noise can be from many effects and science still lacks

a comprehensive uniform explanation [27, 31, 41]. To achieve a $\frac{1}{f}$ spectral density, the auto correlation function must be unity for all values [114]. According to this explanation, flicker noise would originate from the fact, that the behavior of the observed signal correlates well with the same signal at any given time. Thus, a simply put explanation could be, that the signal has a long "memory" since it is similar to itself at any given time. Many techniques work on "resetting" or subtracting this memory from the signal to remove flicker noise [114].

The total RMS voltage from flicker noise can be calculated by integrating the power spectral density over the acquired frequency bandwidth between f_1 and f_2:

$$\mathbf{s}_{\mathrm{n,flr}} = s_{0,\mathrm{flr}} \frac{1}{f}$$
$$i_{\mathrm{flr}}{}^2 = \int_{f_1}^{f_2} \mathbf{s}_{\mathrm{n,flr}}(f)\ \mathrm{d}f = s_{0,\mathrm{flr}} \log \frac{f_2}{f_1}$$

As the flicker noise coefficient $s_{0,\mathrm{flr}}$ depends on the physical properties of the system exhibiting the flicker noise, an easy maximum bandwidth specification similar to the equations given for thermal or shot noise is not possible. Flicker noise limits the available dynamic bandwidth $\frac{f_2}{f_1}$, not the absolute bandwidth $f_2 - f_1$. The maximum observable bandwidth would then be

$$\log \frac{f_2}{f_1} \leq \frac{I^2}{s_{0,\mathrm{flr}}}$$
$$f_2 - f_1 \leq f_1 \left(\exp\left(\frac{I^2}{s_{0,\mathrm{flr}}} \right) - 1 \right)$$

As I^2 is always positive, the exponential can not be neglected in any case. Once I^2 exceeds $s_{0,\mathrm{flr}}$, the bandwidth becomes exponential in I^2 while neglecting the –1. Below this point, the bandwidth is relatively limited: Taylor approximation of the exponential gives $1 + \frac{I^2}{s_{0,\mathrm{flr}}}$ for small values of $\frac{I^2}{s_{0,\mathrm{flr}}}$. Accordingly, the representation of the flicker noise at low current values has twice the slope as the other noise types, see Figure 3.3. In all cases, the bandwidth scales with the minimum observable frequency f_1. A direct comparison to the other two noise sources is difficult due to this dependence. Hence only exemplary relations can be given.

3.3.4 Summary of Noise

The previous analysis of different noise sources leads to the conclusion that low currents have a very limited bandwidth. The only directly available hard limit is the shot noise, which is independent of the actual source of the current, as long as the current originates from a barrier. Many low current measurements, like dielectric stress characterization, leakage characterization and others, are of such a nature and thus, the shot noise limit is applicable. As the numbers of the thermal noise example suggest, resistive elements exhibiting such low currents that the previous analysis gains impact, are hard to achieve on a technical basis. Yet, it must be kept in mind,

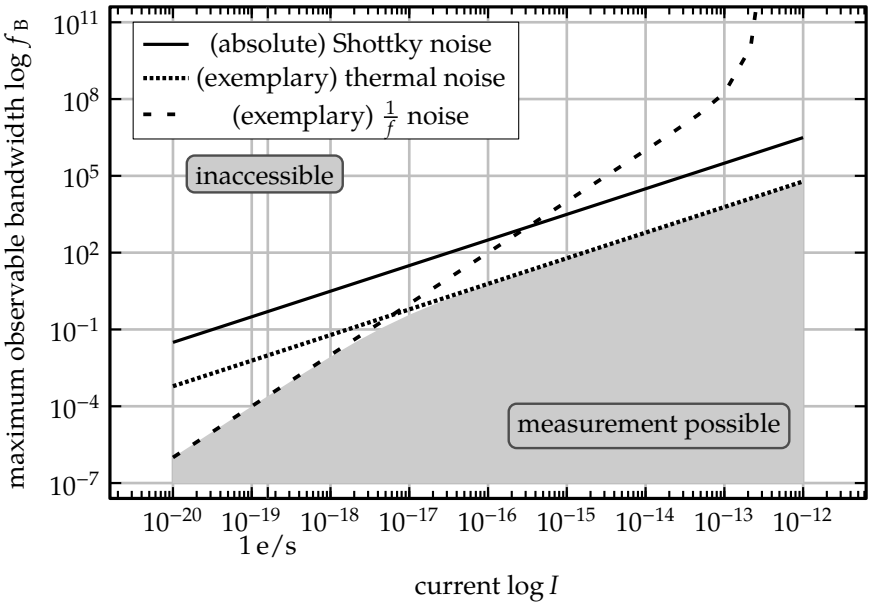


Figure 3.3: Limits to low current measurement from noise. The actual values for current and frequency of $\frac{1}{f}$ noise and thermal noise are setup dependent.

that resistive paths could be formed, for example during the analysis of dielectrics, which exhibit this noise. A small current can also exhibit $\frac{1}{f}$ noise, though the actual amount of noise power is a matter of signal source and can not be easily compared. $\frac{1}{f}$ noise can have very different origins and a general analysis of this noise source for low currents is difficult. The comparison of the noise sources in terms of current dependence (see Figure 3.3), shows that at low frequencies, the $\frac{1}{f}$ noise will dominate, though the precise point of crossing between this noise and the other noises is setup dependent. The previous discussion shows that a small current requires a small measurement bandwidth, independent of the specific noise a DUT exhibits. The actual noise characteristic only reflects the precise bandwidth to be expected usable.

3.3.5 Nyquist Theorem

The Nyquist theorem states, that for a given signal $\mathbf{V}$ with bandwidth f_B, a minimum of $2f_B$ instantaneous measurements of the signal value $\mathbf{V}(t_i)$, $i \in [1, 2f_B]$ allow the exact reconstruction of the original signal. In this sense, a time discrete signal can be exactly reconstructed when the signal bandwidth criterion is met. A very similar statement has been derived for the quantization of the amplitude [20], again stating that the continuous character can be reconstructed from quantized values under certain circumstances.

Putting this idea further into the quantized character of charge leads to the following arguments. An arbitrary signal of bandwidth f_B needs $2f_B$ readings. Such a signal is periodic. Thus, with $2f_B$ readings of a signal, a bandwidth of f_B is specified.

The nature of "readings" is open within this context. If considering a (relatively low) current of limited bandwidth, the current has a periodic character. Electrons pass through the measurement apparatus at certain times, one at a time, repeating the pattern according to the periodicity. If now, the times of electron passage are recorded within one period, resulting in $2f_B$ readings, the signal can be reconstructed precisely. According to the Nyquist theorem, the bandwidth of the signal is then limited to f_B.

As such, it could be safe to formulate, that the minimum observable current would be resembled, if for each "instantaneous measurement", a single electron is "measured". Accordingly, the minimum observable current by a bandwidth f_B is given by $I_{min} = 2ef_B$. This is exactly the same limit as given by shot noise, see Section 3.3.1.

Chapter 4

DC Charge Measurement Concept Selection

Many techniques are available which allow to measure charge. This section is devoted to give a brief overview. Different setups from earlier works are presented in section 4.1. Emphasis is put on the physical means of measurement. A good summary of techniques available for the investigations of electrostatic measurements is given by [19, 64] in form of a textbook and by [35] in form of a review article. Section 4.2 then discusses how to enable all of the presented methods to measure charge quantitatively.

Electrostatic measurements involve in the static measurement of charge or field. Both physical quantities are connected by the Maxwell equations 1.1 and 1.2 on page 15. The measurement equipments available to measure either of them can be used to measure the other through these correspondences. This is possible by using an antenna, which is the subject of Section 4.3.

As electrostatic measurements are capable of measuring static charge or fields, a common property of all systems is a high impedance probe. A potential applied to the high impedance probe does not draw a direct current from the signal source. Only capacitive charging of the probe is permissible in such a setup. Deviations from these ideal probe properties are often referred to as leakage and constrain the measurement time. The higher the leakage, the shorter the allowable measurement time. The leakage within capacitive voltage dividers is considered in Section 4.4. This not only limits the measurement capabilities but also enables certain use cases (Section 5.5).

4.1 Basic Electrometer Designs

Possible realizations of the charge or field sensitive measurement apparatus are briefly presented. The list is not exhaustive but should give an overview of currently available techniques and their properties. Charge measurements divide into four groups:

- Chemical charge meters measure a passed charge through the measurement of the amount of material deposited or absorbed during a chemical process such as electrolysis. The charge measurement is indirect through the particles carrying the charge. As the amount of material required for a precise measurement is large (in terms of number of elementary particles), the sensitivity of this technique is limited and will not be further discussed in the present work.

- The Coulomb force allows to observe a mechanical displacement or force alteration due to the presence or absence of a charge. The most obvious representation of this technique is the gold leaf electroscope.

- Another method is to use the capacitance as translator between charge and voltage. This group of charge meters includes the field mill, the vibrating reed electrometer and other integrated solutions like varactor based modulators.

- The fourth group of electric charge sensors is composed of semiconductor devices. These setups use the intrinsic property of semiconductors to build up a field dependent conductivity.

The first three groups allow for a mechanical or electrical realization of the setup, making measurements in normal workshop scale (say: millimeter) available with sensitivity down to atto-coulomb scale. Though, the measurement of atto-coulomb is a high achievement, the actual implementations often suffer from poor measurement bandwidth if in a workshop scale design. Some types for charge measurements can also be realized in a microscopic scale using IC technology. In the following text, the last three groups are briefly presented and their functional principle is explained.

4.1.1 Electroscope

The electroscope works on the principle of the Coulomb force. This force was discovered by Coulomb in 1785 as the force to a charge in an electrical field [1, 2]. Already Coulomb himself described the most simple voltage meter based on this force resulting from the charge. The application as "voltmeter" did not occur to him due to the lack of precise measurement of the applied voltage or charge, presumably. Later the method of using the Coulomb force to measure voltages was improved by numerous inventors [7].

The basic principle is to charge two parts of the electroscope with the same type of charges [54]. Due to the repelling Coulomb force between even polarized charges, these two parts of the electroscope will retract from each other. If now the construction allows for a derivation of the force from the retracted distance, the charge can be estimated. The gold leaf electroscope (see Figure 4.1) is the most simple form where a single electrically conductive film is bent down to yield two leafs. This film is then charged, resulting in a repelling force between the two leafs, working against the gravitational force. Accordingly, the absence or presence of charge, field or voltage can be derived.

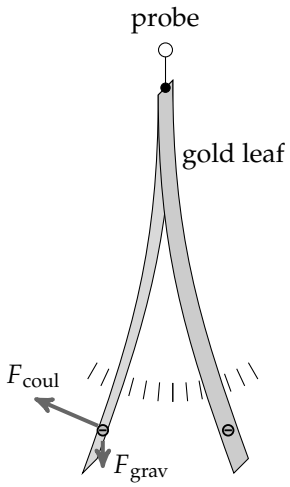


Figure 4.1: Gold leaf electrometer. The charges on the leafs repel the leafs against the gravitational force. From the reading on the scale, the Coulomb force and applied voltage can reconstructed.

Measuring small amounts of charge or low voltages using a mechanical electroscope is a difficult task. Devices detecting down to 10 V have been built [19]. Yet, due to the reciprocal dependence of the Coulomb force on the distance of the charges, small geometries ease the task of detecting smaller amounts of charge. This fact is used by electrostatic force microscopy (EFM) [40, 56, 68, 70], which is a derivative of atomic force microscopy (AFM). In this mode, the distance between the charge under test and the sensitive probe is just a few nanometer, making large Coulomb forces available for detection. The detection takes place by modification of the operating point of a mechanically oscillating cantilever. As the cantilever is relatively small and oscillates with a high quality factor, the detectable force is small. Charge amounts as small as a couple of electrons should be detectable [44].

An IC version of the electroscope would be similar to the work published in [58]: The electrostatic force on a body is observed through the movement and quantitatively investigated to allow for a calculation of the applied charge. The IC in [58] operates a mechanical paddle in resonance. Due to the Coulomb force imposed on the paddle by presence or absence of charge, the resonance frequency shifts and can be detected. As the Coulomb force exhibited by a small amount of charge (say a couple of pico Coulomb), is really weak, a large scale apparatus is difficult to design. With the micro-version of the electroscope [58], already small charges can be detected. It is unknown whether such a result is achievable on a millimeter scale.

Though the electroscope principle does not require an alternating current (AC) design, most implemented systems that are capable of detecting low amounts of charge work on a lock-in or non-DC technique. This directly affects the measurement input, as the actual force is modulated by a high frequency. Due to the principle of operation, this modulation of the force transfers into a modulation of the input

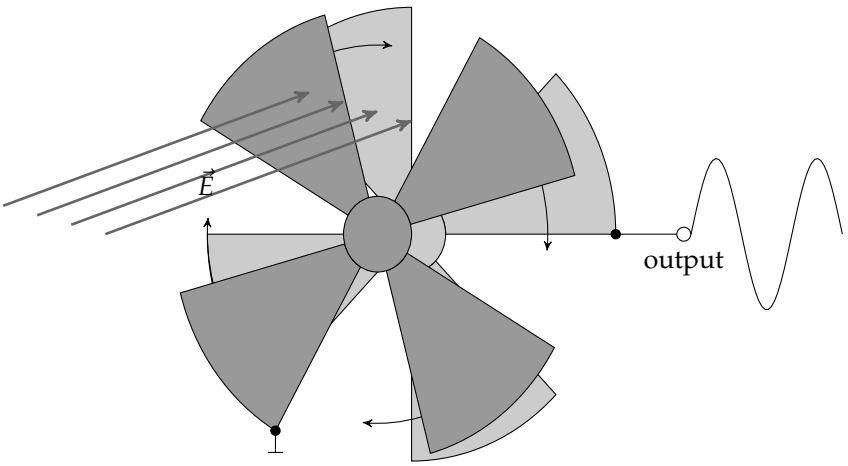


Figure 4.2: The sensitive plate is subjected to a time varying capacitive coupling to the target charge. According to the rotating cover, this setup is termed "field mill".

potential, originating from the measurement equipment. This technique forces a certain amount of AC signal onto the measured signal source, which could potentially alter the source characteristic.

4.1.2 Field Mill

The field mill is an electronic measurement device allowing to measure an electrical field. It works on the principle of periodically exposing and covering a sensitive plate to the field. Figure 4.2 shows the basic setup of a field mill. The rotating cover for the sensitive plate results in a periodic change of the capacitive coupling of the field to the sensitive plate. From the very weak output amplitude (voltage or current depending on implementation), the field strength can be determined. Due to the periodicity, the response from the sensitive plate is also repetitive and can be demodulated synchronously. The method is different from the electroscope described before, as it does not require a Coulomb force. The functionality is based on the capacitive coupling of the target charge to the sensing electrode. Other examples for the use of such an approach are vibrating plate electrometers [18, 22, 108, 150]. Since the electrical signal can, in nearly all cases, be read out through a lock-in technique, these methods allow for the detection of very weak fields and very small amounts of charge.

Using IC technology, the same principle can be carried out on two different ways. A simple air gap capacitor can be implemented in microelectromechanical system (MEMS) technology and a mechanical movement of the plates can be achieved on a micrometer scale [82, 116]. This would be a direct pendant to the mechanical means of the field mill or vibrating reed electrometer. Alternatively, a variable capacitor (varactor) can be used to achieve the same effect but without the need for moving components [42]. This would be a solid state electronics approach and is for example available as the Hewlett Packard 4145 Electrometer or using different techniques like capacitive diodes or metal oxide semiconductor (MOS) varactors [30, 125].

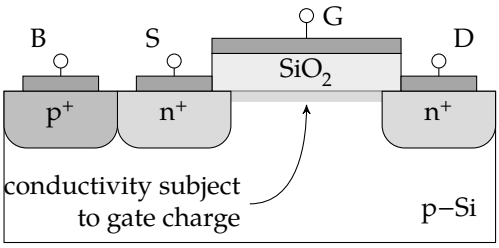


Figure 4.3: Cross sectional schematic of a MOSFET. The diffusions are (B)ulk, (S)ource and (D)rain. The amount of charge on the (G)ate conductor controls the conductivity in the active area of the substrate.

The method of detecting charge based on a periodically altering capacitor forces a non-constant potential to the input terminal of the charge meter. As already with many of the mechanical electroscope designs, this poses a limitation on the usage with certain signal sources. The fact that the measurement equipment creates a variable input potential is often undesirable because it could potentially influence the behavior of the signal source and make a clear measurement difficult. For example tunneling characteristics are relatively steep in their response to a voltage change, possibly changing the tunneling current significantly by such voltage alterations.

Another drawback from the capacitive coupling method is the requirement for synchronous demodulation. The very weak signals that are present at the capacitor for low amounts of charge need to be analyzed by a lock-in amplifier. Lock-in amplifiers are part of everyday analysis techniques but require special considerations when integrated into an IC. Consequently, this technique is complex to use for implementation in total onto an IC.

4.1.3 Solid State Devices

Due to an impinging field, the carrier density in the semiconductor material changes and thus the conductivity is altered, see Equation 2.2 on page 26. As the mobile carriers can be of either polarity, independent of semiconductor doping and only depending on the field direction, an inversion layer can be formed. The metal oxide semiconductor field effect transistor (MOSFET) uses this inversion layer to transport current. For the inversion layer in the MOSFET, the surface potential must be inverted to the bulk potential and at least as strong as the same: $\frac{\Phi_S}{\Phi_B} < -1$. Figure 4.3 shows the cross section through a device that can work with this principle. Two diffusions, drain and source, are placed next to an "active area". The active area semiconductor is coated with an insulation layer (e.g. silicon dioxide for silicon MOSFET) and a conductive gate layer (poly-Si or metals, e.g. aluminum).

Application of a voltage to the gate material subjects the underlying semiconductor material to the aforementioned electrical field. This electrical field can be made large enough for the semiconductor to accumulate significant mobile carrier concentrations at the semiconductor surface, see Section 2.4. If this mobile carrier concentration

is of same type as the two diffusions drain and source next to the active area, a current can flow between them. The resulting conducting surface is called "channel". In this case, the vertical field is absorbed by the mobile carrier concentration and a proportionality between the applied charge to the gate and the resulting charge available for conduction in the inversion layer is present. Accordingly, the conductivity between drain and source is a direct measure for the amount of charge on the gate layer which can be reconstructed from the conductivity.

The current conduction of the MOSFET depends on the voltage applied to the gate and to the drain with respect to source. In source mode operation, these two voltages depict input and output voltage respectively. The charge sheet model [105] is a very simple description of the MOSFET functionality for the parabolic and saturation region. All devices within this work are operated in one of these two regions. The output current for the charge sheet model is given by:

$$\mathbf{I}_{\mathrm{D}}(V_{\mathrm{GS}}, V_{\mathrm{DS}}) = \mu C_{\mathrm{ox}} \frac{W}{L} \begin{cases} 0 & V_{\mathrm{GS}} < V_{\mathrm{TH}} \\ (V_{\mathrm{GS}} - V_{\mathrm{TH}})\, V_{\mathrm{DS}} - \frac{1}{2} {V_{\mathrm{DS}}}^2 & V_{\mathrm{GS}} - V_{\mathrm{TH}} > V_{\mathrm{DS}} \\ \frac{1}{2} (V_{\mathrm{GS}} - V_{\mathrm{TH}})^2 & V_{\mathrm{GS}} - V_{\mathrm{TH}} < V_{\mathrm{DS}} \end{cases} \tag{4.1}$$

The cases in Equation 4.1 are off ($V_{\mathrm{GS}} < V_{\mathrm{TH}}$), linear/parabolic region ($V_{\mathrm{GS}} - V_{\mathrm{TH}} > V_{\mathrm{DS}}$) and saturation region ($V_{\mathrm{GS}} - V_{\mathrm{TH}} < V_{\mathrm{DS}}$). μ is the mobility of the carriers in the channel, C_{ox} the oxide-semiconductor area capacitance, W the width and L the length of the transistor. V_{TH} is the threshold voltage from which on the inversion layer (channel) is considered to be formed. This characteristic has been significantly extended and modified to represent modern transistors. Due to various effects when small geometries are used, the electrical behavior is altering. The principle of influencing a mobile charge concentration and using this mobile charge concentration as output conductivity, is still the same.

Semiconductor electrometers based on the functionality of the MOS transistor had been proposed already. For example in [33], the MOSFET principle is used to measure the current of a reversely biased pn-junction. This method has also been used to measure the leakage currents through gate dielectrics directly through the transfer of the MOS transistor [45] or through a feedback configuration [97], see Section 4.2. Previous works have also demonstrated [112] that this method is capable of detecting single electrons at room temperature.

4.1.4 Secondary Electron Emission Yield as Field Indicator

Using a scanning electron microscopy (SEM) or a focused ion beam (FIB) system to bombard a sample with ions or electrons causes the sample to emit secondary electrons (SEs), see also Section 2.1. The emitted SEs can have a wide range of energies, though many have energies below 5 eV. These electrons are influenced already by low electric fields. For example, the emitted electrons can be recollected if the potential of the emitting sample spot is larger than their energy. Normally, the amount of emitted

Setup / Component	Key Features / Occurrences	Limitations
Electroscope	coulomb force to mechanical movement + very simple setup − low sensitivity − lock-in required for better sensitivity	EFM, gold leaf electroscope, MEMS based oscillators
Field mill	capacitive coupling / mirror charges + pure electrical signal path + high sensitivity − lock-in required	Field mill, Vibrating Reed Electrometer, MEMS based capacitors, MOS varactor based electrometer
Solid State Devices	capacitive coupling / mirror charges + pure electrical signal path + high sensitivity + **static operation**	MOSFET
SE emission yield	displacement of probe charges + **spatially resolved result** − complex vacuum setup − possible influence to investigated charge	SEM, FIB

Table 4.1: Tabular summary of the presented charge measurement methods. The key features of the MOSFET and the SE yield based charge detection are highlighted in bold.

electrons is used as imaging means through an SE detector. If the amount of emitted SEs changes due to the field, the SE detector will reflect this change. By this means, charge can be detected, though quantitative evaluation remains difficult.

In contrast to the other techniques mentioned above, this technique introduces the electron beam or ion beam current into the sample. This current causes a charging of the sample, which can also be observed by the SE detector, see Section 6.2. Accordingly, it is important that the targeted material is not carrying the charge of interest. An alteration of the measured charge would be the result in this case. It is important to separate the (conductive) sample which is targeted by the beam and the part which carries the charges. As will be shown in Section 6.4, this can be achieved by targeting the beam to a semiconductor material which has the node with charge buried below. The charge results in a space charge region (SCR) in the semiconductor which can cause a field on the surface, see Section 2.4. This field can affect the SE emission and allow for a field or charge measurement through the ion or electron irradiation.

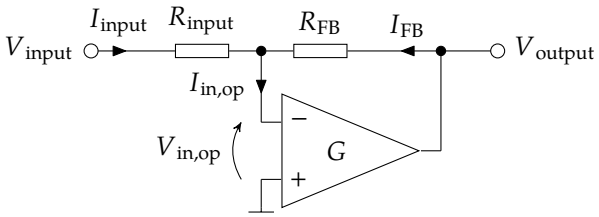


Figure 4.4: An inverting amplifier with resistive feedback elements.

4.2 Feedback construction

All available electrostatic measurement principles can be extended by the use of a feedback loop. Once the electrostatic quantity (field or charge) is converted to a somehow discernible signal (electronic, mechanical, optical, …), the implementation of a feedback loop using a capacitor can derive a quantitative value if the capacitor properties are known. The following example will motivate the use and functionality of the feedback loop.

Figure 4.4 shows the common circuit of an inverting amplifier with an operational amplifier as core device. The basic circuit is a common implementation using board level devices [29] which integrates a feedback loop [28]. It is governed by the equations:

$$V_{\text{output}} = G V_{\text{op,in}}$$

where G is the operational amplifier gain, and

$$I_{\text{input}} = \frac{V_{\text{input}} + V_{\text{in,op}}}{R_{\text{input}}}$$
$$I_{\text{FB}} = \frac{V_{\text{output}} + V_{\text{in,op}}}{R_{\text{FB}}}$$

At the inverting input of the amplifier, three currents sum according to Kirchhoff's laws

$$I_{\text{in,op}} = I_{\text{input}} + I_{\text{FB}}$$

And the dependence of output to input can be derived:

$$V_{\text{output}} = -\frac{1}{\frac{R_{\text{FB}}}{G R_{\text{input}}} + \frac{1}{G} + 1} \frac{R_{\text{FB}}}{R_{\text{input}}} \left(V_{\text{input}} - I_{\text{in,op}} R_{\text{input}} \right)$$

Obviously, this is an ideal inverting amplifier with gain $\frac{R_{\text{FB}}}{R_{\text{input}}}$ if two conditions are met:

- $G \gg 1$, a high amplification gain, and

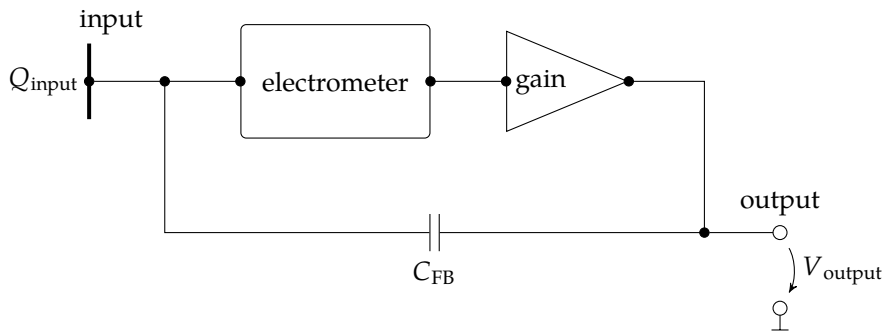


Figure 4.5: Capacitor feedback design usable with any of the available electrometer measurement setups.

- $I_{\text{in,op}} \approx 0\,\text{A}$, the amplifier draws no current.

The second requirement can be relaxed to $I_{\text{in,op}} = \text{const}$, if changes matter, only.

$$V_{\text{output}} = -\frac{R_{\text{FB}}}{R_{\text{input}}} V_{\text{input}} \tag{4.2}$$

The feedback causes the operational amplifier to control the voltage at the inverting input terminal to zero. Often this configuration is called "virtual ground".

Expressing the output current in terms of the input current, Equation 4.2 becomes

$$V_{\text{output}} = -R_{\text{FB}} I_{\text{input}}$$

Accordingly, the input resistor can be removed if the signal source connected to the amplifier behaves like a current source (high output resistance). The function of the feedback resistor R_{FB} becomes obvious in this situation: it transfers the input quantity (I_{input}) to the output quantity (V_{output}), in this case current to voltage.

The resistor R_{FB}, which connects *current* to voltage, is now replaced by a capacitor, which connects *charge* to voltage. The circuit from Figure 4.5 is achieved. The capacitor connects *charge* to voltage which requires reformulation of the equations governing the new circuit. With the resistor circuit from Figure 4.4, Ohm's law is considered ($V = IR$). The circuit with feedback capacitor builds on the capacitance instead of the resistor, which follows $V = Q\frac{1}{C_{\text{FB}}}$. Accordingly, R_{FB} is replaced with $\frac{1}{C_{\text{FB}}}$ in the equations for the capacitor circuit:

$$V_{\text{output}} = -\frac{1}{C_{\text{FB}}} Q_{\text{input}} \tag{4.3}$$

The previous requirements now change "charge" for "current" and give

- $G \gg 1$, as before and
- $Q_{\text{in,op}} \approx 0\,\text{C}$, or $Q_{\text{in,op}} = \text{const}$.

The first requirement is equal as before. The second requirement is that the amount

of charge stored in the amplifier input stays constant (i.e. independent of input or output voltage). Accordingly, the electrometer input must not draw a leakage current. The amplifier must operate as an electrometer. The previously summarized electrometer setups can be dropped into this circuit, possibly equipped with an additional amplification stage to address the first requirement. In this case, the output depends on the input charge and the feedback capacitor, only. In order to address parasitic elements and non-ideal behavior, the mathematical description for the circuit is re-evaluated in Chapter 5.

Application of charge to the input can be done through two different means. The first way is to conductively connect the input of the charge sensor to the charge source. For example, a MOS transistor gate can be connected to the input and charge that tunnels through the MOS transistors gate dielectric reaches the input of the charge sensor. The charge sensor would measure the oxide leaked charge. Alternatively, the charge to be measured can be coupled to the charge sensor through an insulator and a structure labeled "antenna". The construction and functionality of the antenna is the topic of the next Section 4.3.

4.3 Antenna design

The antenna rules as presented in Section 2.3 are similar to the antenna principle presented in this section. The principle from this section can be used in an additional, electrostatic influencing way. The antenna structures are targeted to "collect" charges during the application of a process step. Their collected charge is then transferred to a (small) test transistor which is measured afterwards for certain parameters. Within this work, charge is also collected through such an "antenna" structure and is conducted to the charge sensor. Additionally, the charge sensor is very sensitive and can detect image charges already. This is not the case with the conventional "antenna rule" verification structures from technology design from Section 2.3. As a consequence, the influence from charges near to the antenna is discussed in this section. Those charges that are collected by the antenna are conducted through the terminal and do not need further consideration.

Charge can be detected through the presence of electrical field. Obviously this would also allow to measure the electrical field itself if no charge is present. In order

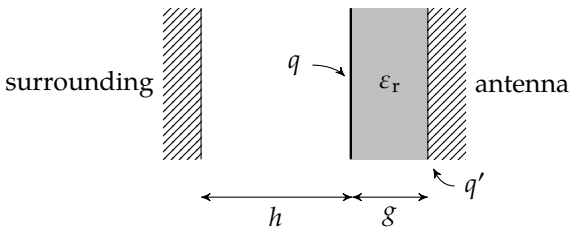


Figure 4.6: One dimensional problem for the explanation of mirror charge in the antenna charge measurement setup.

to do so, the following simplified (one dimensional) setup is discussed, see Figure 4.6. A conductor is connected to the charge sensor input and is placed at a distance g apart from a charge q. This conductor is called "antenna" in this work. The term "antenna" stems from the fact that the conductor receives the electrical field of nearby charge, as laid out in the following. There is no connection to radio frequency (RF) signal reception, despite the name similarity.

The space between the charge and the antenna is filled with a dielectric with constant ε_r. The remaining space is filled with air or vacuum ($\varepsilon_\mathrm{r} \approx 1$) and at a distance h, the surrounding enclosure is again a conductor with connection to "ground". The setup is unbound in two dimensions making for a one dimensional electrostatic problem, where the field is along this dimension. Within this setup, the integral form of the third Maxwell equation, Equation 1.2, allows to calculate the field strength from the charge amounts. With the area A of the setup in the two homogeneous dimensions, the third Maxwell equation is evaluated "around" the charge q:

$$\begin{aligned} A\frac{\partial D}{\partial x} &= A q_\mathrm{V} \\ A\,\varepsilon_\mathrm{r}\,\varepsilon_0 E_\mathrm{insulator} + A\,\varepsilon_0 E_\mathrm{vacuum} &= A q \end{aligned} \tag{4.4}$$

The antenna is connected to the charge sensor input, which resembles a virtual ground. As both, the antenna and the surrounding conductor are at ground potential, the integral of E must zero out if going from surrounding to the antenna:

$$h E_\mathrm{vacuum} = g E_\mathrm{insulator}$$

Due to the presence of the electric field in the insulator $E_\mathrm{insulator}$, a mirror charge q' builds up on the antenna surface. This mirror charge must be conductively supplied by the charge sensor. The mirror charge q' is again calculated using Maxwell's equation, where $E_\mathrm{insulator}$ is negative due to the inverted direction of the setup compared to the previous case of q. The divergence is evaluated at the antenna surface (around q'):

$$-A\,\varepsilon_\mathrm{r}\,\varepsilon_0 E_\mathrm{insulator} = A q' \tag{4.5}$$

Substitution into Equation 4.4 yields

$$-A q' - A\,\varepsilon_0 \frac{g}{h}\frac{q'}{\varepsilon_\mathrm{r}\,\varepsilon_0} = A q$$

The amount of charge loss $1 - \frac{-q'}{q}$ specifies how good $-q'$ approximates q and is calculated as:

$$1 + \frac{q'}{q} = \frac{g}{h\,\varepsilon_\mathrm{r} + g} \tag{4.6}$$

In order to measure q with low charge loss (i.e. $-q' \approx q$), ε_r and h should be large and g should be small. Once $\varepsilon_r h \gg g$ is satisfied[1], the error is negligible and the charge measurement resembles q even though no conductive connection between charge and charge sensor is established.

The simple one dimensional setup represents a real physical setup with limited extension into all directions, too. Except for the simple requirement for h and d, the requirement is extended into three dimensions: For all objects close to the charge, the direct distance between the charge and the object must be significantly larger than the direct distance to the conductor connected to the charge sensor. If this is still fulfilled, the charge measurement of the charge sensor output resembles the negative amount of charge under investigation: $-q$.

The Shockley-Ramo theorem [16, 17] was developed to ease the complex analysis of image charges in real physical setups to yield the current value from moving of such charges. A means to calculate the current I in the case that the charge e moves ($\vec{v}$) relative to a conductor (e.g. the antenna) is, according to [17, equation (1)]:

$$I = \mathrm{e}\vec{E}_\mathrm{v} \cdot \vec{v} \tag{4.7}$$

The field $\vec{E}_\mathrm{v}$ in this equation contains the information on the physical setup. It is the field at the position of e if the antenna is at unit potential and all other conductors are set to zero potential. The scalar product of $\vec{E}_\mathrm{v}$ and $\vec{v}$ resembles the influence of the field from the charge onto the antenna. In this theorem, the *current* in the antenna terminal resulting from the charge movement in vicinity of the antenna is expressed. If the charge reaches the antenna, the conduction of charge must be applied, Equation 1.3, if the charge does not reach the antenna but settles to a steady position (i.e. stops moving), the previous considerations about the image charge have to be applied. The Shockley-Ramo theorem affects the current *before* the charge reaches a steady position in relation to the antenna (i.e. a displacement current). In all subsequent analyses where current is derived, the observation of current according to the Shockley-Ramo theorem can be neglected. The time-frame from the point where the charge influences the antenna (i.e. the $\vec{E}_\mathrm{v}$ term from Equation 4.7 becomes significant) up to the time when the charge reaches a steady position in relation to the antenna is small compared to the sampling time of the measurement recording. This is applicable to all measurements conducted within this work. As a consequence, the current can be simply calculated as derivative of the charge amount on the antenna, according to the image charge analysis from this section.

With an antenna, "remote" charge sensing can be implemented, independent of the type of material that contains the charge. This can be an insulator (see Section 6.2 for results) or a conductor, such as a needle (see Section 5.6 for examples). In all cases, charge can be transferred to field once the setup is known sufficiently well, by the Maxwell equations. As discussed in Section 4.2, charge can be directly applied to the charge sensor through a conductor. This allows the usage as very sensitive

[1] Note the opposite sign of q' and q, which requires Equation 4.6 to go to zero, hence the inequality.

charge or current sensor as laid out in Section 6.1. In any case, field and charge, conductively transported or remotely coupled through a field to the charge sensor, is always brought back to the measurement of a (mirror) charge in the capacitor of the charge sensor. This principle is implemented within Chapter 5.

4.4 Tunneling Current in Capacitive Voltage Divider

As will be shown later, a non-linear behavior can improve the capabilities of charge measurement systems. This non-linearity will be used to alter charge on an otherwise floating circuit node, the output of a capacitive voltage divider. For such a setup, the tunneling characteristic of dielectrics is a usable non-linearity, see also Section 2.5 for two different tunneling methods. In this section, the resulting voltage traces and charge amounts for a tunneling capacitive voltage divider are analyzed. The tunneling current through dielectrics is a means to enforce a diode-like threshold behavior of the output voltage of a capacitive voltage divider. By this means, the charge detector from Section 5.5 allows to measure charge without the requirement of a power supply.

A capacitive voltage divider subject to a high voltage can show tunneling currents through the capacitances dielectrics. Depending on the type of dielectric, thickness and capacitance ratio, different scenarios are considered. For all subsequent discussions, the nomenclature from Figure 4.7 is used to specify input, output voltage and capacitance values accordingly. In this voltage divider configuration, the nominal output voltage without tunneling is given by

$$V_{\text{output}} = \frac{C_2 V_{\text{input}} + Q_0}{C_1 + C_2} \tag{4.8}$$

Here, Q_0 specifies the amount of charge that is on the output node if the input is 0 V. In the following it is assumed, that $Q_0 = 0\,\text{C}$ holds. If tunneling is considered, a steady state would be reached if the tunneling currents through both capacitors are equal:

$$A_1\,\mathbf{J}_1(V_{\text{output}}) = A_2\,\mathbf{J}_2(V_{\text{input}} - V_{\text{output}}) \tag{4.9}$$

$\mathbf{J}_1$ and $\mathbf{J}_2$ are the tunneling current densities within the two capacitors and A_1 and A_2 are the areas of the tunneling cross sections. The script in Appendix B solves this equation numerically by two ways with the coefficients for the technology used in this

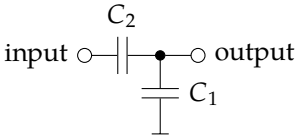


Figure 4.7: Capacitive voltage divider and nomenclature.

work. It can either be solved to target the steady state voltage (i.e. exactly Equation 4.9), or with regard to time while also considering the current used to charge/discharge the capacitances. The latter case solves the circuit by the Kirchhoff laws resembled in Equation 4.10 for a constant input voltage V_{input} and time dependent output voltage $\mathbf{V}_{\text{output}}(t)$.

$$0 = A_2\,\mathbf{J}_2(V_{\text{input}} - \mathbf{V}_{\text{output}}(t)\,) - A_1\,\mathbf{J}_1(V_{\text{output}}) - (C_1 + C_2)\frac{\partial\,\mathbf{V}_{\text{output}}(t)}{\partial t} \tag{4.10}$$

Two setups are analyzed in more detail:

- C_1 is a MOS transistor (Fowler-Nordheim (FN) tunneling) with an area of $0.4\,\mu\text{m}^2$ and C_2 is a capacitor ($A = 18\,\mu\text{m} \times 18\,\mu\text{m}$, $d_{\text{ins}} = 1.2\,\mu\text{m}$, $\varepsilon_{\text{r}} = 5.1$) without tunneling current, which resembles the capacitive coupling over a large distance when neglecting tunneling is appropriate, and
- C_1 is a MOS transistor (FN tunneling) with a different area of $15\,\mu\text{m}^2$ and C_2 is a capacitor with a larger area ($A = 1000\,\mu\text{m}^2$) and tunneling current of FN type, which corresponds to a poly insulator poly (PIP) capacitor in the used technology.

The steady state result from the first case is $V_{\text{output}} = 0\,\text{V}$ due to $\mathbf{J}_2 = 0\,\text{A/m}^2$ in Equation 4.9. Yet, the steep reduction of the tunneling current with decreasing field causes the time to reach this steady state to be infinite.

If conducting a transient simulation of both setups using Equation 4.10, the resulting output voltage starts at the value given by the capacitance ratio, Equation 4.8. For both cases it quickly decays to a quasi-fixed voltage as can be seen in the simulation results in Figure 4.8. Increasing the applied input voltage results in a decreasing ratio between output and input voltage and a constant output voltage. Figure 4.9 shows the corresponding plot of quasi-static output voltage V_{output} against applied input voltage V_{input}. The quasi-static value has been taken at 1 s after the application. Accordingly, for both setups, the tunneling properties of capacitor C_1 cause a constant output voltage, independent of input voltage up to a certain maximum. Once the tunneling current in the second capacitor becomes significant, the output voltage will increase again, as marked in Figure 4.9. Using this fact, the voltage divider can be set to an arbitrary charge setting by applying an according input voltage and leaving the current settle to quasi-static level. After setting the input voltage to 0 V again, the output changes by the initial voltage step from Equation 4.8 and stays at a non-zero level. This is a manifestation of the changed charge on the capacitive voltage divider during the tunneling, as described by Q_0 in Equation 4.8. As can be seen in Figure 4.8, the exact time for the removal of the input voltage is not important. The amount of transferred charge can be controlled via the applied input voltage.

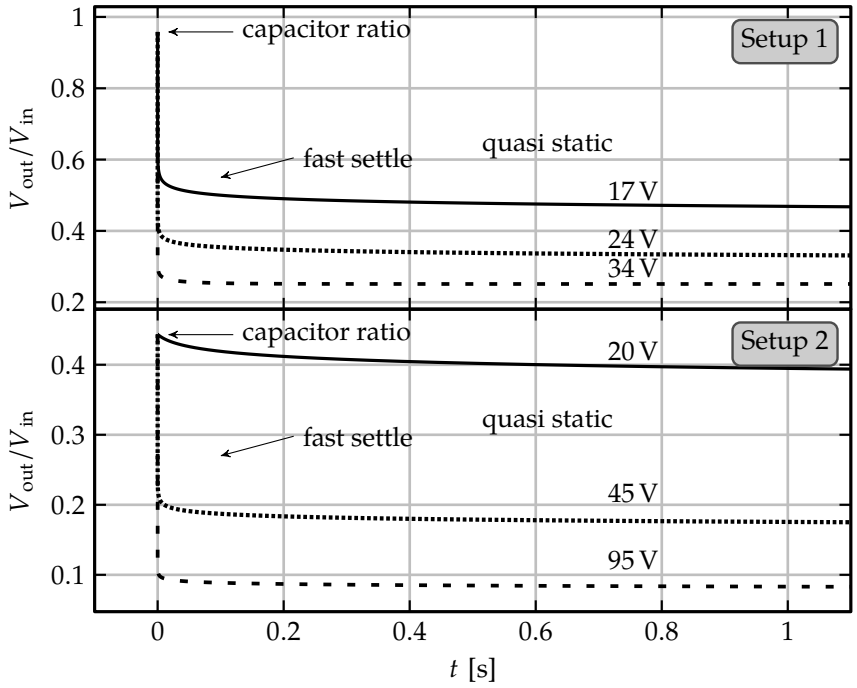


Figure 4.8: Voltage trace of the capacitive voltage divider simulated with the script from Appendix B.

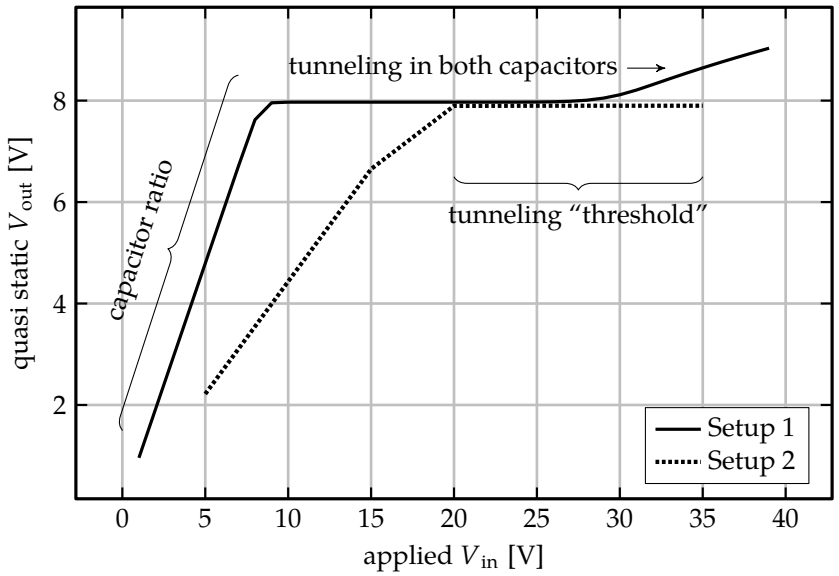


Figure 4.9: Simulated quasi-static output voltage after 1 s delay, depending on the applied input voltage.

4.5 Summary

A charge measurement is possible by many different means. Various setups for detecting charge are laid out and a feedback construction is motivated to allow a quantitative analysis of the measurement result. Coupling of the charge between the analyzed object and the charge measurement system can be realized by a conductive connection or by using image charges. Finally, the (absolute) charge transfer function of such a setup (Equation 4.3 contains the absolute input charge Q_{input} and not a charge difference) requires possibilities to alter the charge. This is possible by using a capacitive voltage divider. Consequently a measurement system for charge analysis can be realized in many different ways.

The next chapter deals with the implementation of a charge measurement system based on a MOSFET as charge detection device. This enables the use in every modern complementary metal oxide semiconductor (CMOS) circuit. As it allows for a very universal and widespread application, it is the preferred way of implementing a charge measurement system for IC analysis. Even though other implementations can be integrated into an IC, their implementation requires special technological features, for example MEMS or silicon on insulator (SOI) structures. For example the techniques building on the Coulomb force require a MEMS process to allow for movable micromechanical components integrated into the circuit. This limits their application to a very small range of technologies and would not allow for a widespread usage.

Chapter 5

Charge Measurement Construction

The feedback circuitry is shown for resistive circuits in Chapter 4. Replacing the resistor by a capacitor is motivated and the ideal description is already given: $V_{\text{output}} = -\frac{1}{C_{\text{FB}}} Q_{\text{input}}$. Here, this equation is revised with respect to non-ideal components and parasitics and subsequently the limitations imposed by the realization are discussed. In order to support this discussion, the measurement principle is formulated such that the limitations can be expressed with respect to the actual procedure. Finally, in Section 5.6, the individual implementations realized throughout this work are presented and the validity of their functionality is discussed.

The key features of the MOSFET make the use as a charge measurement means outstanding. All other presented techniques would require the use of lock-in or non-DC technology and special processing features during production to evaluate charge on a very sensitive scale. Accordingly, the charge measurement constructed throughout this work is built on the means of a MOSFET as electrometer.

A very similar setup has been suggested in [97], though the use case differs from the usage in this work. In [38] and [45], a floating gate transistor has been used to measure hot carrier injection and tunneling current in a MOS transistor with

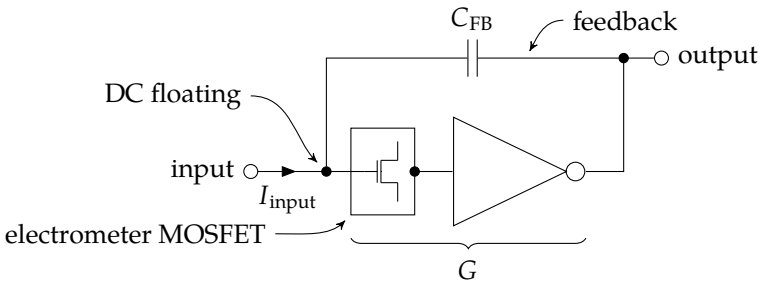


Figure 5.1: Simplified schematic circuit of the capacitive charge measurement setup.

high sensitivity, yet the universality of the circuit has not been pointed out. The circuit implemented throughout this work is very similar to the feedback circuit from Figure 4.5 and can be seen in Figure 5.1. It contains the closed loop feedback as described earlier in Section 4.2 with a MOSFET as electrometer device, according to Section 4.1.3. The high gain is achieved through an amplifier, as required by Section 4.2. The amplification from the MOSFET and the amplifier in Figure 5.1 is considered together. An alternative implementation would be to use an amplifier with a field effect transistor (FET) as input transistor.

As shown in Section 4.2, the amplifier G implements a virtual ground at its input due to the negative feedback loop with the capacitor C_{FB}. This setup can also be described in terms of charge, where Q_{input} is the charge on the input node:

$$Q_{\mathrm{input}} = C_{\mathrm{FB}} \left(V_{\mathrm{input}} - V_{\mathrm{output}} \right) + V_{\mathrm{input}} C_{\mathrm{op,in}}$$

and again with the amplifying behavior $V_{\mathrm{output}} = G V_{\mathrm{input}}$, this yields:

$$Q_{\mathrm{input}} = C_{\mathrm{FB}} \left(\frac{1}{G} - 1 \right) V_{\mathrm{output}} + C_{\mathrm{op,in}} \frac{1}{G} V_{\mathrm{output}}$$

which follows the already known relation between input and output for unlimited gain. The precise dependence for a limited gain of the amplifier is:

$$\frac{1}{C_{\mathrm{FB}}} Q_{\mathrm{input}} = - \left(1 - \frac{1}{G} (1 + \frac{C_{\mathrm{op,in}}}{C_{\mathrm{FB}}}) \right) V_{\mathrm{output}} \tag{5.1}$$

For unlimited G, this gives the relation from Equation 4.3. The role of $C_{\mathrm{op,in}}$ will be the subject of Section 5.2. As this circuit implements a feedback loop, it is labeled "closed loop feedback" setup or implementation in the following text. In Section 5.5, a second charge measurement setup is suggested, which is labeled differently.

5.1 Measurement Principle for the Closed Loop Feedback Implementation

The measurement is conducted in a three steps process. The amplifier is powered up and the circuit settles to equilibrium conditions. With the initial condition of Q_{input}, the initial output voltage is generated according to Equation 5.1.

1. The initial output voltage of the amplifier is measured,
2. the charge to be measured is applied to the input of the circuit,
3. the output voltage is measured again.

To obtain the amount of charge applied to the circuit in step 2, the resulting value of the output voltage is subtracted from the initial output voltage, yielding $\Delta V_{\mathrm{output}}$.

This output voltage change is multiplied by the size of the capacitor C_{FB}. The change in charge in the circuit input is labeled $\Delta Q_{\mathrm{input}}$ and for the ideal case, this gives:

$$\Delta Q_{\mathrm{input}} = -C_{\mathrm{FB}} \Delta V_{\mathrm{output}} \tag{5.2}$$

If consecutive measurements are performed, the initial step 1 can be skipped on subsequent iterations, and the process is reduced to consist of two steps. In this case, it is beneficial to subtract the same initial output voltage from all subsequent output voltages, giving a result for the change in charge with respect to the start.

With the closed-loop feedback implementation, application of charge to the input terminal is equivalent to the application of electrostatic field to an electrode connected to the input terminal, as laid out in Section 4.3. In this situation, both original quantities (charge and field) are reflected by a certain amount of mirror charge in the feedback capacitor, which is then measured by the charge sensor. With Equation 4.5 on page 51, the measured charge could be transferred into a field strength. Only for very simple physical dimensions, this can be done on an analytical basis. For more complex designed antennas and charge distributions, numerical methods could be used up to certain limitations.

Once $\Delta Q_{\mathrm{input}}$ has been measured, it can be used in various ways: The charge itself can be used as output of an experiment, for example as observable from charged particle beam irradiation as presented in Section 6.2. Taking the time development of the charge $\Delta \mathbf{Q}_{\mathrm{input}}(t)$ into account, a current can be derived from the observed charge value by differentiation or least mean square (LMS) approximation. This could be used to derive leakage behavior of dielectrics, as presented in Section 6.1. The charge measurement principle allows for in-situ charge monitoring or sensitive current measurement. In-situ capability allows for a direct replacement of certain workshop scale measurement units, like pico-ampere meters.

5.2 Systematic Measurement Limitations

If the amplification of G is finite the output voltage is different from the ideal form given by Equation 5.2. Taking a limited amplification factor into account also requires to consider parasitic input capacitances. Furthermore, leakage currents and source resistances can degrade the circuit performance. For the following calculation, the circuit is extended to include parasitic and non-ideal devices. Figure 5.2 shows the adapted circuit. The amplifier is replaced by a differential amplifier (operational amplifier) and the MOSFET input has been removed from the schematic for clarity. Yet, for the desired performance the amplifier must have a MOSFET input.

The circuit in Figure 5.2 assumes that any node can have a parasitic cross-capacitance to any other node. The feedback loop is assumed to be stable with a fast settling time, compared to the observation time during the experiment. Then, the only node that might be influenced by parasitic capacitances is the input node and only capacitances for this node need to be considered. The only non-fixed signals in this circuit are

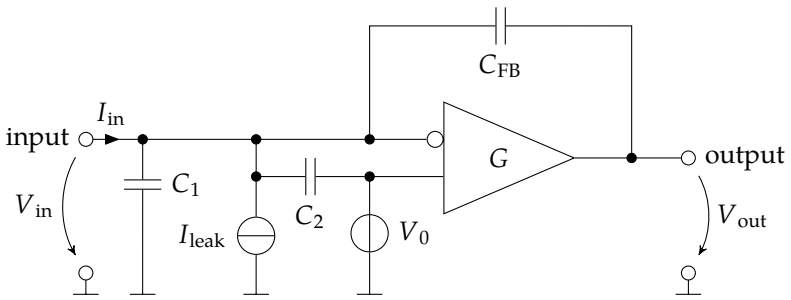


Figure 5.2: Capacitive measurement setup circuit with real devices and parasitics. Load circuit (e.g. A-to-D-converter) is not shown as the amplifier output resistance is considered to be zero.

the output node and the positive input to the inverter. Three parasitic capacitance exist: C_1, C_2 and a parasitic part of C_{FB}. The parasitic part of C_{FB} is not considered separately in the following text. Other parasitic parameters of the circuit are leakage currents on the sensitive input node denoted by I_{leak}, limited amplification of the amplifier denoted by G. The output resistance of the amplifier can be neglected as typical measurement circuits (e.g. A-to-D converter) easily have input resistance of several tens of kilo ohms. In the following text, each of these parameters is discussed appropriately.

The following calculation is based on the charge Q_{input} present on the input node. This can be done because the two capacitors C_1 and C_2 represent all parasitic capacitances available on this node. As a result, the charge can be transformed to a voltage and vice versa. Q_{input} can be expressed as:

$$Q_{input} = V_{in} C_1 + (V_{in} - V_0) C_2 + (V_{in} - V_{out}) C_{FB}$$

The amplifier connects input voltage V_{in} to output voltage V_{out} with

$$V_{in} = V_0 - \frac{1}{G} V_{out}$$

The above equation transforms then to:

$$\begin{aligned} Q_{input} = &\left(V_0 - \frac{1}{G} V_{out}\right) C_1 \\ &+ \left(V_0 - \frac{1}{G} V_{out} - V_0\right) C_2 \\ &+ \left(V_0 - \frac{1}{G} V_{out} - V_{out}\right) C_{FB} \end{aligned}$$

$$Q_{input} = V_0 (C_1 + C_{FB}) - V_{out} \left(C_{FB} + \frac{C_1 + C_2 + C_{FB}}{G}\right) \tag{5.3}$$

Reordering Equation 5.3 yields offset and gain separately:

$$V_{\text{out}} \left(C_{\text{FB}} + \frac{C_1 + C_2 + C_{\text{FB}}}{G} \right) = V_0 \left(C_1 + C_{\text{FB}} \right) - Q_{\text{input}} \tag{5.4}$$

Here, $\frac{1}{\left(C_{\text{FB}} + \frac{C_1 + C_2 + C_{\text{FB}}}{G} \right)}$ denotes the amplification factor and $V_0 \left(C_1 + C_{\text{FB}} \right)$ represents an input offset charge. In order to design the circuit successfully, the individual parts of the circuit are analyzed for their influence onto the measurement signal.

5.2.1 Static Measurement Errors

Limited Amplifier Gain G: The value of V_0 is considered to be fixed, adding a constant offset to the output voltage. To investigate the gain of the circuit this offset can be neglected and $V_0 = 0\,\text{V}$ can be substituted, as also shown in the next paragraph. Obviously, the combination of all capacitors divided by the amplification factor G in Equation 5.4 diverts the gain of the circuit from its nominal value of $-\frac{1}{C_{\text{FB}}}$. Thus, this term will be introduced as $C_{\text{err,g}} = C_1 + C_2 + C_{\text{FB}}$ and the resulting dependence between input and output gives:

$$\left(C_{\text{FB}} + \frac{C_{\text{err,g}}}{G} \right) V_{\text{out}} \sim -Q_{\text{input}}$$

The error from insufficient gain can be expressed relatively as $\epsilon_{\text{out,g}} = \left| \frac{\Delta V_{\text{out}}}{V_{\text{out}}} \right|$. Rewriting $\epsilon_{\text{out,g}}$ yields:

$$\frac{1}{\epsilon_{\text{out,g}}} = \left| 1 + \frac{C_{\text{FB}}}{C_{\text{err,g}}} G \right| \tag{5.5}$$

$\epsilon_{\text{out,g}}$ diminishes for high values of G, as expected.

Equation 5.5 points out that a high gain can allow for the feedback capacitor to be smaller than the parasitic capacitance. The overall circuit gain error would still be small. For example, an operational amplifier gain of $G = 120\,\text{dB} = 1 \cdot 10^6$ reduces the gain error to below 0.1 % even if the parasitic capacitances are 1000 times as large as the feedback capacitor. As the design of the implemented circuit has very high gain amplification stages the error from the gain is neglected.

Parasitic Capacitances on Input Node: The parasitic capacitances on the input node collect charge in case the input node voltage changes. Two reasons can cause a shift of the input voltage:

1. due to limited gain, a change of the output voltage requires a change of the input voltage altering the charge on the parasitic input node capacitances, and

2. a variation of V_0 directly translates into a variation of the input voltage due to the virtual ground configuration of the amplifier feedback.

The resulting error from the first point (1.) transforms into the same error $\epsilon_{\text{out,g}}$ as in Equation 5.5, with the same deduction. For investigation of 2., the amplifier gain is considered to be large and the resulting gain error is low. In this case, Equation 5.4 can be simplified as

$$V_{\text{out}} C_{\text{FB}} = V_0 \left(C_1 + C_{\text{FB}}\right) - Q_{\text{input}} \tag{5.6}$$

Equation 5.6 suggests to take the difference $V_{\text{out}} - V_0$ as representation for the input charge instead of only V_{out}:

$$V_{\text{out},0} = V_{\text{out}} - V_0 = -\frac{1}{C_{\text{FB}}} \left(Q_{\text{input}} - V_0 C_1\right) \tag{5.7}$$

The full value of $V_0 C_1$ does not lead to errors due to the consideration of the initial conditions of the circuit, see Section 5.1. Still, a variation of V_0 during the measurement itself, denoted by ΔV_0, leads to an error equivalent input charge of $-\Delta V_0 C_1$. The relative error can then be expressed as:

$$\epsilon_{\text{out},0} = \left| \frac{\Delta V_0 C_1}{Q_{\text{input}}} \right|$$

Or in terms of output voltage as:

$$\frac{1}{\epsilon_{\text{out},0}} = \left| \frac{V_{\text{out}}}{\Delta V_0} - 1 \right| \frac{C_{\text{FB}}}{C_1}$$

Reducing the size of C_1 or ΔV_0 also reduces the error introduced by the parasitic capacitance on the input node. It should also be noted, that the parasitic capacitance between the input node and the virtual ground C_2 does not have an influence on this behavior. C_2 only shows up in the gain error in Equation 5.5.

Unfortunately, the requirement $C_1 \ll C_{\text{FB}}$ is hard to achieve. Large feedback capacitors reduce the gain of the transfer function (i.e. the output would not react as sensitive to input charge) and a small parasitic capacitance – which would mainly result from the input transistor of the amplifier – makes the amplifier input offset large. The input offset of the amplifier can be considered as being part of V_0, making an amplifier input offset drift also influence $\epsilon_{\text{out},0}$ through ΔV_0. For the present design, the requirement $C_1 < C_{\text{FB}}$ will be met in most cases and the drift of offset voltage and V_0 is kept low by keeping the temperature constant. Yet, when increasing the sensitivity, this must be kept in mind.

5.2.2 Transient Measurement Errors

The following section discusses different transient effects that influence the measurement result. Transient effects with regard to the measurement process as described in section 5.1 are those that apply in between step 1 and 3 on page 58.

Leakage Current on Input Node: The leakage current on the sensitive node causes the measurement value to drift. As this is an effect that is only visible over time, static conditions are not sufficient to describe it. Taking into account the effect of leakage current through I_{leak} and integrating it over the measurement period T to yield Q_{input} gives:

$$Q_{\text{input}} = Q_0 + \int_0^T \mathbf{I}_{\text{in}}(t) \; - I_{\text{leak}} \, \mathrm{d}t$$

If the leakage current is relatively constant, this can be divided into two terms:

$$Q_{\text{input}} = Q_0 - T I_{\text{leak}} + \int_0^T \mathbf{I}_{\text{in}}(t) \; \mathrm{d}t$$

Furthermore, for measurements as described in section 5.1, the difference in charge matters, giving

$$\Delta Q_{\text{input}} = -T I_{\text{leak}} + \int_0^T \mathbf{I}_{\text{in}}(t) \; \mathrm{d}t$$

And the measurement error from leakage current can be expressed relative to the measured value as

$$\epsilon_{\text{out,l}} = \frac{T I_{\text{leak}}}{\int_0^T \mathbf{I}_{\text{in}}(t) \; \mathrm{d}t} = \frac{\overline{I_{\text{leak}}}}{\overline{\mathbf{I}_{\text{in}}}} \tag{5.8}$$

Equation 5.8 specifies that the measured current must exceed the leakage current significantly for a small $\epsilon_{\text{out,l}}$ and good measurement results. This requirement applies to all high ohmic, electrostatic probe methods and places a fundamental limit to the measurement principle of measuring static charge.

The voltage at the sensitive node is constant, according to the feedback loop. The leakage currents to other nodes with fixed potential could – under certain idealized circumstances – be considered constant. Thus, their influence on the charge measurement result is proportional to the measurement time T and independent of the actual measured amount of charge. After initial determination of this leakage behavior, it could be mathematically subtracted from the measurement result and, by this means, the precision can be significantly improved. The feedback capacitor C_{FB} does not fulfill this requirement as the voltage across this capacitor is not fixed but proportional to the input charge. Accordingly, the leakage through the feedback capacitor must be kept to a minimum.

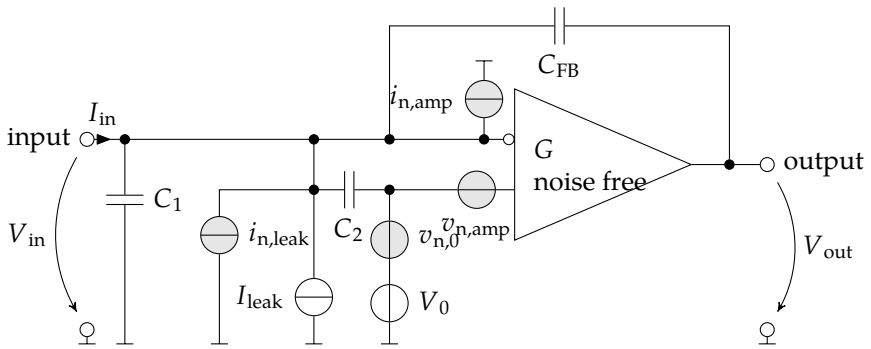


Figure 5.3: Equivalent noise circuit for the specified noise sources. The only contributing noise sources are the input noise sources for the amplifier $i_{n,amp}$ and $v_{n,amp}$, the noise from the reference voltage $v_{n,0}$ and the current noise from leakage current in connections and capacitors $i_{n,leak}$.

5.3 Noise

Circuit noise is a fundamental effect present in all conventional circuits. Different physical interpretations are available from literature attributed to different kinds of noise. As noise is a statistical process, descriptions are formulated on the population in total, not on individual "readings". These range from probability distribution functions describing the likeliness to read a certain specific value to power spectral densities describing the amount of energy in the noise signal at a specific frequency. The noise section tries to abstract from these statistical values wherever possible and discusses the noise on a qualitative basis. Accordingly, its not always possible to formulate the resulting quantities numerically but with respect to their dependence on certain system variables and properties.

The circuit from Figure 5.3 shows the charge measurement circuit equipped with noise sources for the amplifier and reference voltage. The input voltage noise on the positive terminal of the amplifier and the noise of the reference voltage add together. A signal source would also be connected to the input (not shown in Figure 5.3) but as the output resistance of the amplifier is small compared to the output resistance of the signal source, the input current noise of the amplifier can be simplified without considering the signal source output resistance. The cables and capacitors are leaking some amount of current which also exhibits noise.

The noise sources $i_{n,leak}$, $v_{n,0}$, $v_{n,amp}$ and $i_{n,amp}$ represent the noise from possible leakage currents, from the reference voltage and from the amplifier. As the positive input to the amplifier is fed by a low impedance voltage source, its noise current can be neglected (already omitted in Figure 5.3). Though the input voltage noise of the amplifier is in series with the reference voltage, it can not be combined into a single reference noise voltage. $v_{n,0}$ feeds through to the output according to the transfer of V_0 described by Equation 5.7. For $v_{n,amp}$, the capacitance C_2 is connected to the fixed potential of V_0 and thus in parallel with C_1. Here, the transfer to the output can be

derived from Equation 5.7 as:

$$v_{\mathrm{n,out,a}}{}^2 = \left(\frac{C_1 + C_2}{C_{\mathrm{FB}}}\right)^2 v_{\mathrm{n,amp}}{}^2$$

The total output equivalent noise from V_0 and $v_{\mathrm{n,amp}}$ yields:

$$v_{\mathrm{n,out}}{}^2 = \left(\frac{C_1}{C_{\mathrm{FB}}}\right)^2 v_{\mathrm{n,0}}{}^2 + \left(\frac{C_1 + C_2}{C_{\mathrm{FB}}}\right)^2 v_{\mathrm{n,amp}}{}^2$$

For sufficient gain G, this term can be rewritten as an equivalent input noise charge using Equation 5.7:

$$q_{\mathrm{n,in}}{}^2 = C_1{}^2 v_{\mathrm{n,0}}{}^2 + (C_1 + C_2)^2 \, v_{\mathrm{n,amp}}{}^2 \tag{5.9}$$

The input noise source for this equation would be a pure charge source which alters the charge on the input node. Equation 5.9 specifies that for high values for C_2, the amplifier input voltage noise $v_{\mathrm{n,amp}}$ dominates the input noise charge. This is important to remember when designing the interface between the charge measurement and the target device. Triaxial cables could be used and the inner mantle could be connected to V_0 for reduced leakage, at the same time increasing C_2 by the capacitance of the cable. This could make the measurement very sensitive to noise and care needs to be taken. Yet, for the intended application of the implemented charge meter, the capacitance C_2 can be kept low easily.

The noise current from sources $i_{\mathrm{n,amp}}$ and $i_{\mathrm{n,leak}}$ directly apply to the input current. Accordingly, these noise sources can not be distinguished from an input current and directly reflect the amount of input current required for detection. From Equation 5.8, the input current must be larger than the part of leakage current that is not compensated. As the noise current from leakage ($i_{\mathrm{n,leak}}$) is derived from the leakage current (for example as shot noise, see section 3.3.1), the noise amplitude is smaller for the most applicable measurement cases. According to Equation 3.1 on page 37, this is given for a measurement bandwidth of 1 Hz by $1.6 \cdot 10^{-19}$ A. Thus, the leakage noise current does not need additional considerations. The input current noise from the amplifier is in part also a leakage current through the gate dielectric of the MOSFET. Another part is constituted from the capacitive coupling through the gate-drain capacitance. As the latter is a simple capacitive coupled voltage source, it can be regarded as part of the voltage noise $v_{\mathrm{n,amp}}$.

Measuring current with the charge sensor can be implemented by various methods. As the derivation of the input current from the measured amount of charge is a major application of the charge sensor, the influence of the equivalent input charge noise source $q_{\mathrm{n,in}}$ onto the derived current value I'_{in} is analyzed. In most experiments conducted throughout this work, the current is calculated after the measurement phase is finished. A constant current is assumed during the measurement time, where

the current controls the slope of the charge measurement. If this was not the case, a subset of the measurement recordings of charge could be used, that resembles constant current. To calculate the slope, the LMS algorithm is used.

Deriving the current as a simple linear fit by using only the start time and charge and the end time and charge is suboptimal. In all measurements of this work, intermediate points are recorded, which can also be used for deriving the current. The LMS approximations takes the intermediate points into account, too. In this case, N readings are used for the LMS approximation. The resulting noise in the calculated current value $i'_{\mathrm{n,in}}$ then scales as if all N readings were fully independent. For N equidistant measurements between $x = -\frac{T}{2} \ldots \frac{T}{2}$, this yields:

$$i'^{\,2}_{\mathrm{n,in}} = 12 \frac{q_{\mathrm{n,in}}{}^2}{T^2} \frac{1}{N} \frac{N-1}{N+1} \tag{5.10}$$

See Appendix C for the calculation of this result. For increasing N, the input current noise $i'_{\mathrm{n,in}}$ goes to zero with $\frac{1}{N}$, as if N distinct measurements were taken.

In order to achieve a measurement performance comparable to the results of the conventional measurement system from Section 3.1, an input current noise RMS value of 4 fA must not be exceeded for a 1 Hz bandwidth. Accordingly, the equivalent input RMS charge noise must be less than 5.66 fC. With Equation 5.9, this limits the values for the parasitic capacitances, the voltage reference and the amplifier offset voltage. Typical parasitic capacitances are in the range of 100 fF, requiring a voltage noise of less than 56.6 mV in total. This voltage noise can be achieved without further efforts, yet simple methods can reduce the voltage noise significantly below 5 mV, promising enormous improvements possible by the use of a charge measurement system for low current derivation.

5.4 Measurement Speed

Limiting factors for the measurement speed of the charge measurement system are the amplifier and the capacitors. The polarization process of the capacitances (including parasitics) can limit the measurement speed. Theoretical approaches to the dielectric polarization with time dependent fields (dispersion) is discussed in [34] for example. With a time dependent polarization, the output voltage will gradually approach the final value in this case, causing a slow measurement. Different effects of polarization contribute to the dielectric constant [21] with varying relaxation behaviors. The polarizability is usually fast compared to the timescale of charge measurements conducted throughout this work in the range of seconds. As a consequence, the speed of the charge measurement system is only limited by the amplifier. Operational amplifiers are available for a variety of unity gain frequencies, including devices with values far in the megahertz regime. Implementation of a stable amplifier into an IC is feasible for unity gain frequencies of 1 MHz at minimum. The speed of the charge measurement can thus be easily adjusted to the needs of the specific application and

does not need further consideration.

The current measurement using conventional techniques can be replaced by a charge measurement, as is part of section 6.1. The main drawback from the conventional current measurement system is the speed of acquisition, yet the speed of acquisition using a charge measurement requires some attention. With a conventional setup, the delay time after application of a voltage step is required to charge the capacitive parts of the connections between the measurement equipment and the target device. As a consequence, the behavior of a first order low pass filter is observed, see Figure 3.1 on page 34. This limits the speed for the measurement significantly. With a charge measurement system, this limitation is lifted. A capacitive connection between the target device and the charge measurement would be part of the parasitic capacitance. Accordingly, care must be taken to avoid excessive error through this parasitic capacitance, but the speed is not degraded. Only when the parasitic capacitance is exhibiting a slow polarization process, a speed limit can occur, see above. The limiting factor for conducting of a current measurement using the charge measurement system stems from the current derivation, see Section 5.3 and Chapter 6.

5.5 Offline Charge Detection Principle

A drawback of the closed loop feedback implementation as laid out in Section 5.1 is the requirement for a power supply. With this power supply, the feedback implementation compensates introduced charge by a voltage across the feedback capacitance. By this means, the input terminal is kept at a constant potential. In order to allow for an offline charge detection system, the constant input potential can not be sustained. Instead, a capacitive voltage divider, as discussed in Section 4.4, exhibiting a non-linearity, is used. The non-linearity in the capacitive voltage divider is not directly reversible allowing for a hysteresis behavior. Because the power supply is not required for this to work, the charge measurement result is not available in-situ. It must be determined at a later point in time. The following structure does not require a power supply for sensing charge, it is labeled “offline charge detection” circuit or implementation.

The tunneling behavior of dielectrics is a strongly non-linear characteristic. Section 2.5 summarizes two basic tunneling mechanisms, the Fowler-Nordheim (FN) and the Poole-Frenkel (PF) tunneling. Also, this characteristic is not directly reversible as the physical influence to the dielectric allowing the reversal of the tunneling effect must be large. Approximately the same electrical field strength must be applied for the same time in order to reverse the amount of tunneled charge in a symmetric structure. If only one direction of field is available, reversal of the tunneling effect is not possible. The offline charge detection circuit builds on the tunneling effect in capacitive voltage divider from Section 4.4.

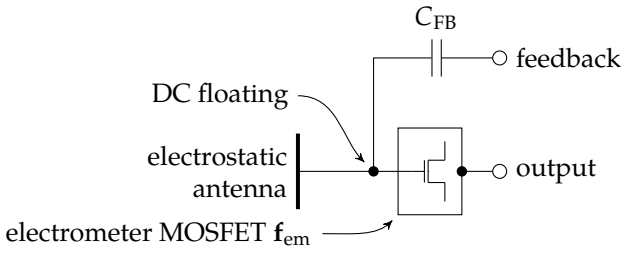


Figure 5.4: Circuit of a offline charge detection implementation.

The principle of the capacitive voltage divider paired with a tunneling characteristic is used within multiple technologies. For example non-volatile memories (NVMs) work with this principle if the cells are programmed or erased by FN tunneling. Process monitoring has also been suggested for analysis by this means [49, 75] and multiple patents are found [47, 63]. This work extends the use of this structure to a more general scope of applications. Whenever the charge monitoring has to be conducted without a proper power supply, the offline charge detection can be used. This section presents the circuit used for the experiments throughout this work. In Section 6.3, the application of the offline charge detector to the surface charging of a FIB is presented showing that the use scenarios of this structure can be extended.

Figure 5.4 shows the principle operation of the offline charge detection circuit. The circuit is a simplified version of the closed loop feedback implementation from Figure 5.1. The feedback loop has been opened and the feedback terminal is separated from the electrometer output. As input probe, an electrostatic antenna is depicted according to Section 4.3 and discussed below. Application of a voltage to the feedback terminal allows for the determination of the charge amount on the input node and for the purposeful modification of this charge amount, according to Section 4.4.

The principle of measurement for this structure is then conducted in a similar way as for the closed loop feedback implementation described in Section 5.1. Yet, this structure does not allow to derive the charge amount in-situ during the application but only after the charge has been removed again and the power supply has been restored. Accordingly, the principle is:

1. Measure the amount of charge on the input Q_{input}, possibly alter this charge via V_{feedback} as noted below.

2. Remove the supply voltage of the device, apply the charge or field of interest to the antenna and/or input node and remove the charge or field again.

3. Measure the charge again and determine ΔQ_{input} from this and the initial measurement.

To initially alter the charge during step 1, the voltage at the feedback input V_{feedback} can be used according to Section 4.4. This causes the capacitive voltage divider to alter the charge as desired. In order for this charge alteration (and also the charge alteration

during the measurement phase, step 2), to stay permanently, the input node must not be connected conductively to any other structure exhibiting leakage behavior. This requires the use of an electrostatic antenna, see Section 4.3. Accordingly, connection of resistive elements between the input and ground is not permissible for this structure. This is in contrast to the closed loop feedback implementation, which would allow such a construction.

The determination of charge on the input Q_{input} is also done by the feedback terminal. If $\mathbf{F}_{\text{em}}(V_{\text{input}})$ is the transfer characteristic of the electrometer and if the electrometer has a constant (or determined) input capacitance, then the transfer function between the feedback terminal and the output terminal can be analyzed through the charge present on the input node Q_{input}:

$$Q_{\text{input}} = C_{\text{FB}}(V_{\text{input}} - V_{\text{feedback}}) + C_{\text{em}} V_{\text{input}}$$

Where C_{em} depicts the electrometer input capacitance and V_{input} the electrometer input potential.

$$V_{\text{input}} = \frac{Q_{\text{input}} + V_{\text{feedback}} C_{\text{FB}}}{C_{\text{FB}} + C_{\text{em}}}$$

Depending on the type of electrometer circuit, V_{output} might also be implemented as a current instead. Without limiting the applicability, this work assumes the output to be a voltage and labels it V_{output}.

$$V_{\text{output}} = \mathbf{F}_{\text{em}}(Q_{\text{input}} \frac{1}{C_{\text{FB}} + C_{\text{em}}} + V_{\text{feedback}} \frac{C_{\text{FB}}}{C_{\text{FB}} + C_{\text{em}}}) \tag{5.11}$$

The implemented design uses a MOSFET as electrometer – again based on the same reasoning as before for the closed loop feedback implementation, making $\mathbf{F}_{\text{em}}$ well known, see Equation 4.1 on page 46. Equation 5.11 allows the operation of this circuit as charge detector. Once sufficiently many pairs $(V_{\text{feedback}}; V_{\text{output}})$ are measured, the point where $Q_{\text{input}} 1/(C_{\text{FB}} + C_{\text{em}}) + V_{\text{feedback}} C_{\text{FB}}/(C_{\text{FB}} + C_{\text{em}}) = 0$ holds can be determined mathematically. $\mathbf{F}_{\text{em}}$ must be continuous for this, which is the case for the transfer characteristic of the MOSFET if operated above threshold voltage.

Even if $\mathbf{F}_{\text{em}}$ were unknown, the input to $\mathbf{F}_{\text{em}}$ can be compensated for, by using the feedback input, to yield a constant value, allowing for direct derivation of Q_{input} from the setting of V_{feedback}.

$$\begin{aligned} 0 &= Q_{\text{input}} \frac{1}{C_{\text{FB}} + C_{\text{em}}} + V_{\text{feedback}} \frac{C_{\text{FB}}}{C_{\text{FB}} + C_{\text{em}}} \\ Q_{\text{input}} &= -V_{\text{feedback}} C_{\text{FB}} \end{aligned} \tag{5.12}$$

This offline charge detection circuit is limited by the leakage behavior in the first place. Measurement of the input charge through the aforementioned procedure can

for example be conducted through determination of the threshold voltage of the MOS transistor. As this is possible without much error using conventional measurement equipment, it is not discussed here. The leakage current possibly present on the input node is important. If the leakage current is present during all the time between steps 1 and 3, then it will sum up for an error in charge reading:

$$Q_{\text{input,leak}} = \int_{t_{\text{initial}}}^{t_{\text{final}}} \mathbf{I}_{\text{leak}}(t)\ \mathrm{d}t$$

For a constant leakage current, this can be simplified to

$$Q_{\text{input,leak}} = I_{\text{leak}}\ (t_{\text{final}} - t_{\text{initial}})$$

The amount of charge to be measured Q_{input} would then have to be significantly larger than the charge from leakage: $Q_{\text{input}} \ll Q_{\text{input,leak}}$. This requirement is much stronger as the actual measurement time is only part of the time-frame valid for the leakage behavior. Accordingly, for the successful implementation of this principle of operation, care must be taken to keep the leakage low.

5.6 Realizations

Both types of implementations are realized in this work. The feedback implementation is constructed with an off-die amplifier in a first revision and with a built-in amplifier and voltage reference in a second revision ("fully integrated"). The open loop implementation is built for the evaluation of FIB attacks on ICs (FIB detector). Both types of realizations are described in this section, whereas the closed loop feedback implementation is discussed with respect to the version with external amplifier. The fully integrated realization has significantly reduced costs and complexity, yet most of the results achieved throughout this work are done with the external amplifier version. The fully integrated version allows a production integrated analysis using the charge sensor, without additional equipment. This makes fast and low cost solutions to high precision measurements available for in-line testing of ICs during manufacturing.

All IC hardware is designed, simulated and fabricated in the 0.25 µm bipolar complementary metal oxide semiconductor (BiCMOS) technology from IHP Microelectronics / Frankfurt Oder. This technology is optimized for high performance bipolar components and has MOS devices for supplementary logic including two polysilicon layers for non-volatile memory (NVM) blocks. The bipolar part of the technology is neither required nor used. Only standard CMOS devices are instantiated plus capacitors made up of the two polysilicon layers and the available metal insulator metal (MIM) capacitor module. The use of two polysilicon layers can also be substituted by MOS varactors. The technology is chosen due to ease of integration and availability.

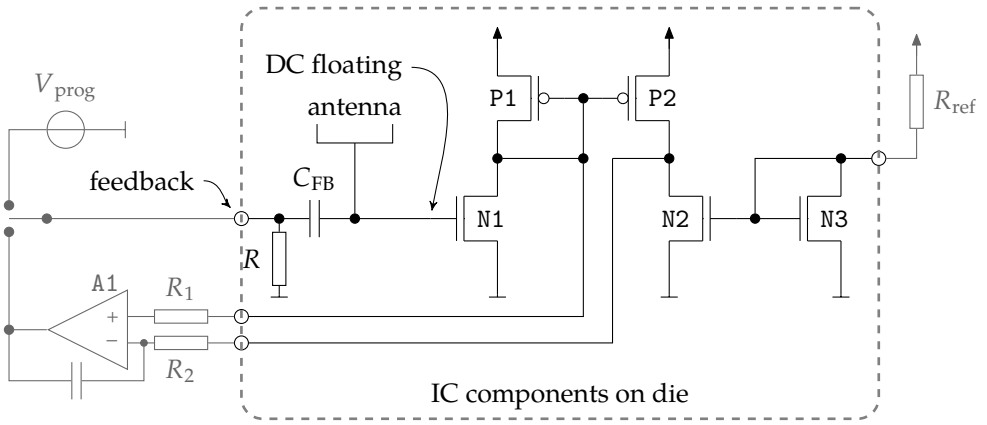


Figure 5.5: Schematic circuit of the implemented closed loop feedback design. Gray parts of this schematic are implemented as discrete components, black parts are implemented on die. The amplifier G is compensated for stability by the capacitor. The voltage source V_{prog} enables the purposeful modification of the charge on the DC floating node, see Section 4.4. For the charge sensor application, the switch would be placed in the lower position.

This section addresses the implementations, the limitations and discusses the methods that are used to verify the functionality of the circuit. The limitations as pointed out in the previous sections are part of this discussions, too. These are: parasitic capacitance, limited gain, leakage current and output noise.

5.6.1 Closed-Loop Feedback Implementation

The closed-loop feedback implementation is realized by the use of matched current mirrors on die and by an external operational amplifier. Figure 5.5 shows the circuit of the first version, where the gray parts are external components and the black parts are on-die components.

The closed loop feedback implementation electrometer device is the MOS transistor `N1`. The drain current of `N1` is compared to the reference current I_{ref} at the drains of `N2` and `P2`. The external amplifier then contributes as amplification stage and closes the feedback loop through the feedback capacitor C_{FB}. This setup is a straight forward realization of the suggested implementation from Section 5.1. For the layout construction, matching rules are considered to make the properties of `P1` and `P2` as well as the properties of `N1` and `N2` as equal as possible. Furthermore, the external amplifier is fed with both drain voltages in order to operate both transistor pairs in equal conditions. This helps to suppress the supply voltage feed through. In the fully integrated realization of the closed loop feedback implementation, the gate voltage of `N2` is derived through a proportional to absolute temperature (PTAT) voltage reference to further suppress supply voltage variations.

As the charge sensor is not only sensitive to introduced charge but also to fields reaching the input node, additional steps are taken to allow a robust operation. In

order to improve the resistance against surrounding fields, a cover is created above the whole active cell area. This shield is grounded and thus provided for a fixed reference field around all capacitive nodes. It is made from nontransparent metal, incident light is not able to reach the active devices. The circuit works reliably with external fields and external light. The measurement is only influenced by the external field or charge if it is applied to the antenna.

The technology supply voltage for the IC is specified at 2.5 V. This allows for proper operation of the current mirrors. To allow sufficient voltage for the feedback terminal, an external amplifier with a higher supply voltage is chosen. Typical supply voltages for the external amplifier are 10 V…20 V. This ensures two important points at the same time: The maximum applicable voltage to the capacitor C_{FB} directly translates to the maximum operation range for the collected charge and a high supply voltage for the amplifier enables a valid operation point after production independent of the initial charge on the capacitor C_{FB}. The application of such a high voltage to the capacitor C_{FB} is not without problems. If driving the feedback voltage above the critical tunneling voltage, a current flows through the capacitor, degrading the measurement. See section 2.5 and 4.4 for an analysis of this behavior. As laid out in Section 4.4, this effect allows for the purposeful modification of the absolute charge on the input node, also supporting to reach a valid operating point

Application of the charge is possible to a number of different tasks, see Chapter 2 for a motivation. In order to evaluate the charge measurement for these different tasks, the charge sensor is instantiated multiple times with varying input configurations and sensitivity settings. These instances are chosen such that a verification of the charge sensor can be carried out and the charge sensor can be used to measure charge in one of the application cases. The verification of the charge sensor is done in a way to proof the sensitivity of the sensor to field or charge applied to the antenna and to proof the robustness of the charge sensor circuit itself against these influences. Accordingly, instances without input connection and with a capacitor and a resistor are created. The instances of the charge sensor usable for measurements are designed for both, conductive connections, charge collections and field sensing:

- To verify the functionality of the charge sensor circuit, the input of one instance is connected to a bond-pad through a large resistor. This allows for the application of a small voltage across the resistor to cause a current into the input node of the charge sensor. This charge sensor sensitivity is chosen to be very *insensitive* in order to allow for a successful application of a small voltage.

- Another sensor input is connected to a bond-pad via a capacitor. Using the (known) dielectric displacement charge across this capacitor when applying a voltage, the functionality of the charge sensor can be verified.

- The immunity of the charge sensor circuit itself is verified through the use of an unconnected charge sensor. Applying charge or field to this charge sensor instance (it does not have an input connection!) should not result in a measurement signal.

- To investigate static fields and surface charges, an antenna structure as described in Section 4.3 is connected to the input. This antenna structure is designed from a rectangular, buried metal structure. The metal structure is covered by inter level dielectric (ILD) and passivation and so does not allow a conductive introduction of charge.

- A conductive introduction of charge is possible if the input connection of the charge sensor is exposed at the surface. This is realized as a second antenna type, which consists of a rectangular metal structure not covered with insulating material.

- A second version of the previous antenna is made large enough to allow for a permanent connection of external components by wire bonding. This input connection is similar to a bond-pad. As the charge sensor input is an electrometer input, it is put in danger from ESD events. Consequently, bonding has to be performed carefully.

The feedback capacitor sets the sensitivity of the cell according to Equation 5.2. Different sizes are employed, ranging from a total of 10 μm^2 (equals roughly 13.7 fF) up to 100 000 μm^2 (i.e. 137 pF). The capacitor sizes are additionally matched to the expected behavior of the cell such that the resulting current and voltage characteristics are within measurable and controllable regions. Two technologies are used for the feedback capacitor: PIP and MIM capacitors. The large range of capacitances allows for a successful investigation of the cells functionality.

Simulations of the charge sensor are carried out using Cadence Spectre analog simulation. In order to ensure correct working of the circuit components, temperature, supply voltage and process parameters are varied into different corners of the technology. The circuit is adapted slightly to ensure the proper functioning of all devices. The simulation includes external components by implementing the required design models for the external amplifier into the Cadence Spectre system. Parts of the simulations are again carried out after the layout had been finished in order to ensure a post layout simulation. Parasitic components do not have a significant effect on the design due to the low frequency requirements. The external feedback amplifier is frequency compensated externally (integrator configuration) as high speed measurements are not desired, see Figure 5.5.

The layout has been arranged in a way such that the transistors in current mirror configuration match each other, except `N2` and `N3`. `N3` is implemented only once for the whole circuit including low pass filtering of the incoming reference current. Furthermore, the pad constraints driven by the available wafer level tester needle mask limited the amount of usable pads such that this measure had to be taken. The points are made equal by matching and consequently, high performance can be expected. The process design rules are fulfilled, making the charge sensors conform

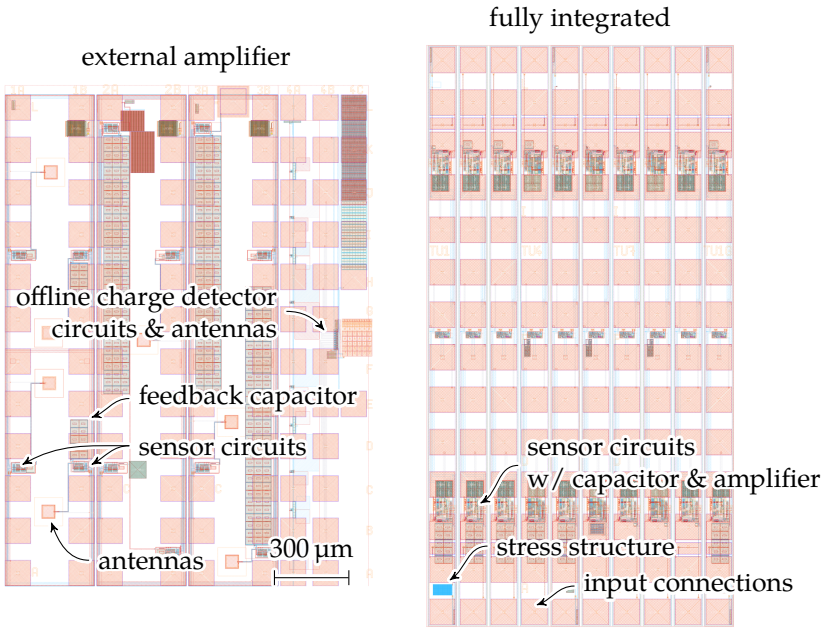


Figure 5.6: Layout of the charge sensor chip to be used with an external amplifier (left) and with on-die amplifier (right).

to standard circuit design requirements. A layout versus schematic (LVS) check is performed to ensure the correct transfer between simulated design and produced layout. Figure 5.6 shows the layout for the implemented circuits (including the offline-charge detection) for the device fabricated in this work: the closed-loop feedback implementation for external amplifier use (left) and including the internal feedback amplifier (right). The later discussed offline charge detector is also integrated into the left layout. After production of the IC hardware, the design is verified and tested against the specification as described here.

The verification of the correct functionality of the charge sensor is required in order to allow performing measurements successfully. The verification is performed, to show, that

1. the applied charge, field or current causes the correct amount of output change, and

2. all other possible influences to the charge sensor do not contribute to this output.

These two requirements can be described as sensitivity (1) and selectivity (2). The limitations to the functionality of the design are identified in Section 5.2 and 5.3. Leakage current would contribute to item 1 and parasitic capacitances would contribute to a violation of item 2. A limited amplifier gain would mainly cause and incorrect but linear charge reading, as would an incorrectly designed capacitor size.

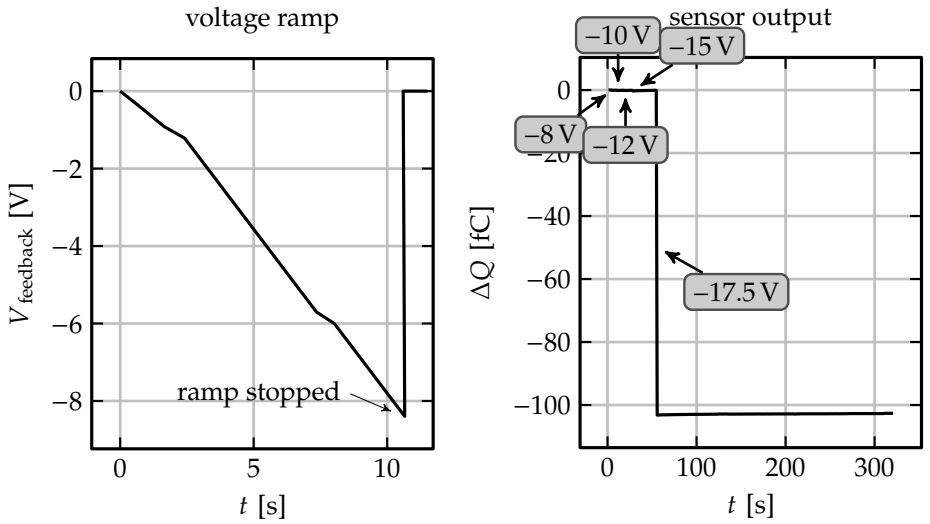


Figure 5.7: Verification process of the floating gate functionality, $C_{\text{FB}} = 137\,\text{fF}$. In between normal operation recordings (right), a voltage ramp is applied to the capacitive voltage divider of feedback capacitor and MOSFET gate (left). The voltage ramp is stopped at increasingly high voltages while observing the output value of the closed loop feedback operation At −17.5 V in this case, the capacitive voltage divider caused a change in output charge.

No precise information on the area capacitance for the PIP capacitor is available, making a precise quantitative measurement only possible by comparing it to a known capacitor. This is done by comparing it to the PIP capacitance, not shown in these verification results.

To show that the sensitivity requirement (1) is fulfilled, the floating gate behavior needs to be analyzed. It must be floating and only pinned to a fixed value by the feedback operation of the amplifier. This is basically resembled by two properties:

a) Charge stored on the floating gate is stored for a long time, giving a constant output (i.e. no leakage current), and

b) alteration of the charge on the floating gate is observed at the output terminal (i.e. no short).

Especially the last point is important as a shorted floating gate would fulfill the first point. To validate the effect from alteration of the charge on the floating gate (item b) a high voltage can be applied to the feedback node of the circuit while the remaining parts of the circuit are unpowered. This allows for a tunneling current between the floating gate and the transistor bulk according to the capacitive voltage divider, see Section 4.4. By this tunneling current, the charge on the floating node is altered and subsequent startups of the feedback loop result in different operating points. With a shorted floating gate node, the tunneling process as described in Section 4.4 would reverse itself after removal, causing no shift in the output for subsequent startups. As this is a generic approach, the additional voltage source V_{feedback} in Figure 5.5 is

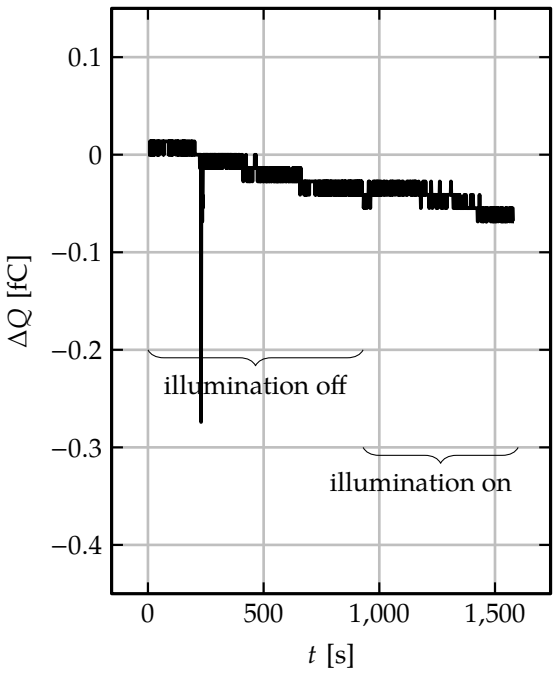


Figure 5.8: Verification of low leakage behavior and effectiveness of shield against incident light, $C_{\mathrm{FB}} = 137\,\mathrm{fF}$.

used to allow for this test on every used cell, independent of antenna configuration. Figure 5.7 shows a sample trace used for this test on the left. A slow voltage ramp is applied to the feedback input of the cell and stopped at the target voltage. The cell is subsequently powered up again in closed-loop feedback mode and the feedback voltage is analyzed with respect to an influence from the voltage ramp. These two steps are repeated for increasing target voltages until the desired influence happens, verifying the cells floating gate functionality. Figure 5.7 (right) shows the so recorded output values combined into a single trace. The applied voltage ramp targets are noted, showing that the voltage ramp of 17.5 V caused the alteration of the charge sensor input charge.

To verify the absence of leakage currents (item a from above), a long time measurement is conducted that covers a total of 1600 s. During this time, the circuit is operated as normal and the output is recorded. Figure 5.8 shows the resulting behavior: a nearly constant output value with only an equivalent current of a single electron every three seconds. Accordingly, the cell does not loose charge in significant amounts. As the time of most experiments is limited to not more than 160 s, this verification is carried out for most of the charge sensor instances using a shorter observation time, as can be seen also in the right plot of Figure 5.7.

These results show that the circuit is working with respect to the feedback loop (item 1 on page 74) and leakage current does not degrade the measurement. For the verification of the circuit functionality with respect to the measurement application, the selectivity needs to be provided (item 2 on page 74). The circuit design is made

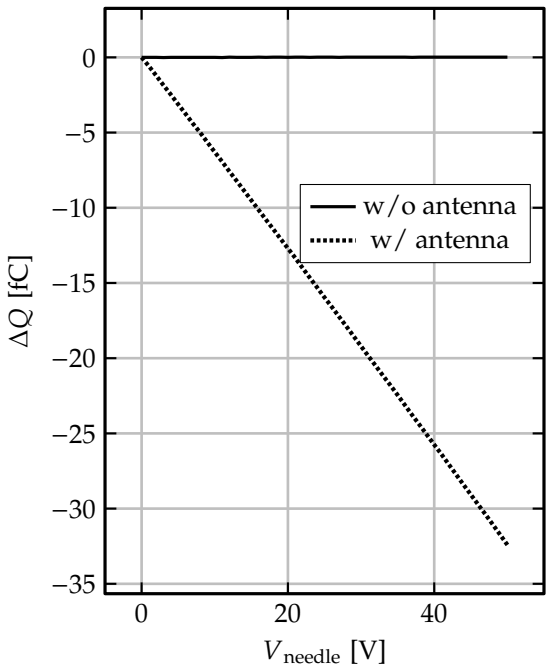


Figure 5.9: External fields (i.e. voltage at needle) do only influence those cells which have an antenna connected to the input, $C_{\text{FB}} = 137\,\text{fF}$.

such that external fields, applied charge and incident light do not modify the output value. Only charge and field applied to the antenna and/or input connection are to be reflected by the output. Consequently, two requirements are tested:

c) Application of any field/charge or light to the charge sensor circuit itself does not vary the output, and

d) charge/field brought into the input of the charge sensor directly or through an antenna structure is reflected by the output.

The requirement from item c is tested for electrical field by use of an instance which does not have an input connection. The circuit is operated as in a normal measurement and a prober needle is placed above the circuit instance. This needle is then subject to a high potential creating a field between the needle's tip and the charge sensor circuit. The resulting dependence is shown as solid graph in Figure 5.9. Clearly, the resulting charge is independent of the voltage applied to the needle. External fields do not influence the circuit measurement output.

Verifying item c for light is conducted by observing the output of a charge sensor instance while altering the illumination of the device. Figure 5.8 shows not only the observed output for a long measurement but also for an illumination change. Parts of the trace are captured with illumination turned on, yet the output voltage does not change nor does the slope. Accordingly, neither the charge sensor operating point nor the charge sensor floating gate functionality (i.e. leakage currents) are influence by an

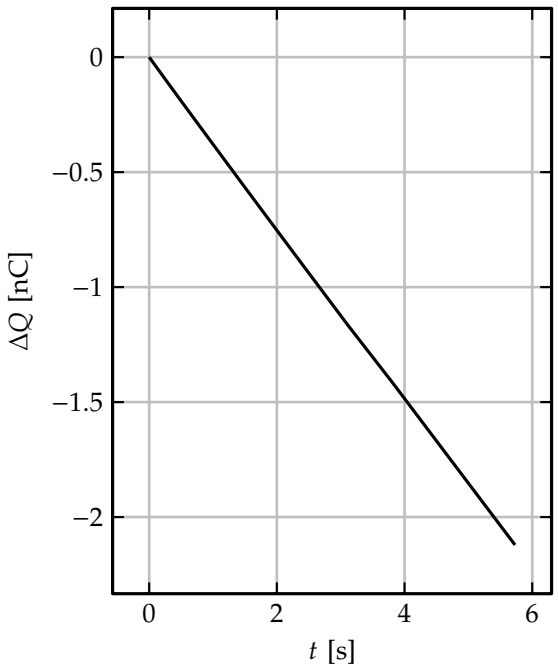


Figure 5.10: A resistor conducts a current into the charge sensor input causing a linear accumulation of charge in the charge sensor, $C_{FB} = 137\,pF$

illumination in this case. This is different for a cell, where no shield is implemented: the output performs a step when altering the illumination. In this case, reverting the illumination back to the initial level also caused the output voltage to revert back to the initial value, proving that the DC operating point of the circuit is affected. The charge sensor functionality is not affected if the illumination is kept constant in this case.

As a last verification requirement, item d needs to be tested. The sensitivity of the circuit to an external field or charge applied to the antenna or input node is analyzed. Application of an external field is done in Figure 5.9, again by a prober needle. A charge sensor instance with an antenna is chosen for this experiment and the needle is brought in place above the antenna structure. The voltage applied to the prober needle is then varied and the sensor output is observed. Figure 5.9 shows the resulting plot (dotted). As the output value depends linearly on the applied prober needle voltage, the charge sensor obviously reacts to a field impinging on the antenna. The linear dependence between voltage at the needle and influenced charge also shows that the feedback capacitance in the charge sensor is constant if a constant capacitance is assumed between needle and antenna. This verifies the sensitivity by capacitive coupling.

Transferring known amounts of charge onto the antenna to verify the selectivity can also be done through a high resistance connected to the input node. According to ohms law, a current flows proportional to the voltage drop across the resistor. A $120\,M\Omega$ resistor is connected to the input of one instance of the charge sensor for

this purpose. The charge sensor circuit is then powered up and the voltage drop across the resistor is adjusted to allow for a small current into the charge sensor input node. Figure 5.10 shows the resulting output trace. As the voltage across the resistor is kept constant for the measurement time, the slope of the output is constant. Thus, the charge sensor is also capable of measuring charge introduced into the input connection correctly.

The verification of the charge sensor circuit has shown that the electrometer and setup choice in Chapter 4 and the subsequent implementation in Section 5.1 works as expected. In order to ensure that the performed charge measurements are valid, the verification of item 1 to prove the sensitivity of the charge sensor is carried out on every instance prior to using the circuit. The other verifications shown in this section deal with the principle and do not have to be tested for every instance.

5.6.2 Offline Charge Detector Implementation

The offline charge detection circuit is implemented according to the principle from Section 5.5, Figure 5.4 on page 68. Again, the MOSFET is used as electrometer device. To ensure a valid operating point at low voltages, the feedback capacitor C_{FB} is chosen larger than the transistor. Yet, this does not degrade the performance severely. As the cell is very small, multiple instances are placed. To cope with the limited number of bond-pads, two cells are connected to one bond-pad with a multiplex transistor each. By this means, the number of cells is doubled, allowing for 18 cells with the 12 available bond-pads. Figure 5.11 shows the schematic of the implemented circuit. The antenna structures are created from quadratic metal structures of varying sizes between 2 µm × 2 µm and 14 µm × 14 µm. Grounded metal wiring is placed surrounding the antennas and the distance between antenna and charge detector circuit is varied. Openings in the grounded metal wiring are between 8 µm × 8 µm and 18 µm × 18 µm in size. The goal of the implementation is to show the validity of the approach with respect to FIB irradiation. The amount of charge stored on the

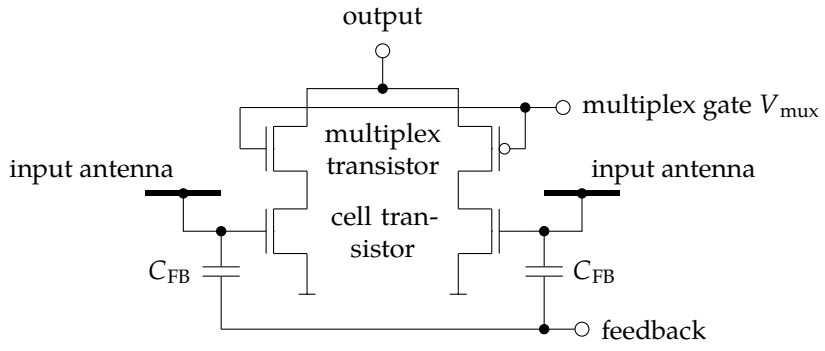


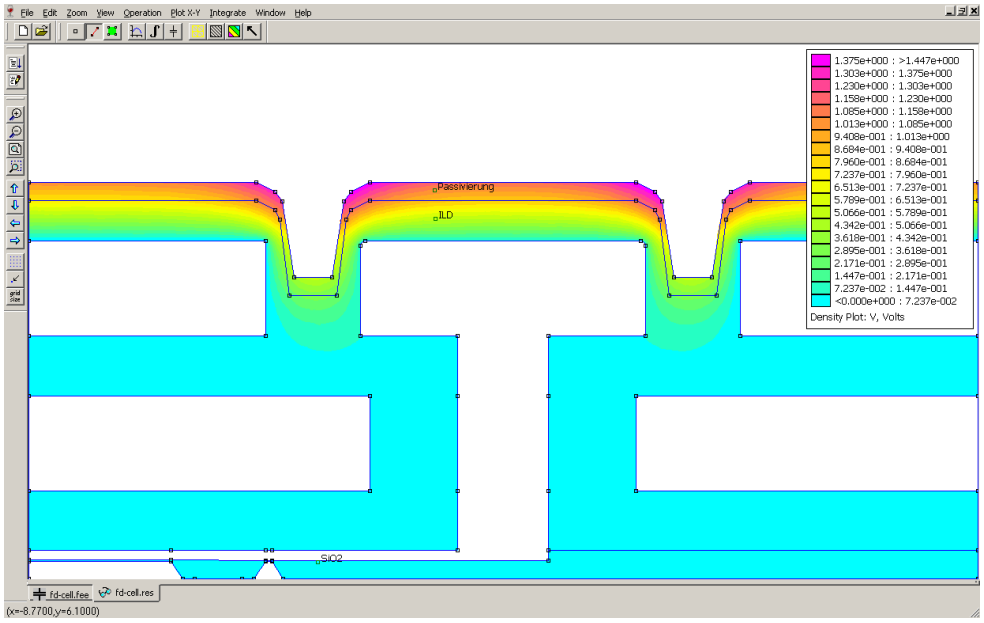
Figure 5.11: Schematic of the implemented offline charge detection circuit. The multiplex transistor enables implementation of two cells per external connection (output).

antenna should be influence by the FIB surface charging as discussed in Section 2.1. In order to validate the approach, simulations are carried out based on the principle of the circuit and finally the hardware devices are subjected to the experiment in Section 6.3.

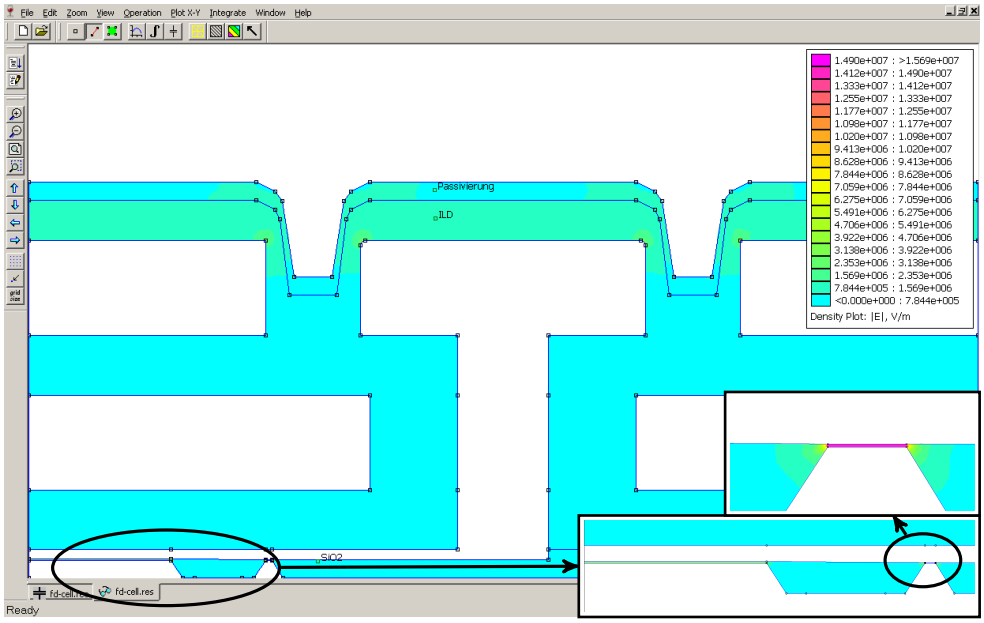
Different simulations are performed to validate the approach and functionality of the designed circuits. A finite-element simulation is conducted with the 2D-simulation software "FEMM" in a Cartesian setup, similar to the antenna-surrounding structure. This simulation aims at determining the amount of influence to be expected from the FIB surface charge on the capacitive structure of the offline charge detection circuit. A second simulation is done by an "octave" program (see Appendix B for the program code), which simulates the tunneling behavior of the capacitive voltage divider, in accordance with Section 4.4. The octave program simulation uses the simulated charge amounts from the first simulation to estimate the influence to the offline charge detection circuit behavior.

Figure 5.12 shows the simulation results from the 2D simulation software. The model consists of a 26 µm long and 6 µm wide (orthogonal to visible plane) area comprising the antenna (center), transistor and capacitor of the offline charge detection circuit, see Figure 5.4. The antenna is simulated with 6 µm × 6 µm embedded in surrounding grounded metal wires. The transistor and capacitor are approximated with constant capacitance. A surface charge density comparable to the influence from a FIB surface scan (20 pA on 355 µm × 355 µm yields ≈ 33.3 aC/µm^2 of ions) is assumed over the whole simulated area of 26 µm × 6 µm (5.19 fC of ions). Integrating the dielectric flux in the capacitor and transistor gives a total mirror charge of 2.53 fC. Accordingly, for this antenna configuration, half the surface charge is mirrored onto the capacitor and transistor. The "effective" antenna size is thus 13 µm wide instead of the model parameter of 6 µm and this effective size parameter is used in subsequent experiments for the derivation of the mirror charge.

The tunneling behavior of the MOS transistor gate is simulated with the octave program from Appendix B. As the mirror charge on the capacitor and transistor are already known from the 2D-simulation result, the remaining problem is reduced to the capacitance and the transistor. A charge on a capacitor with tunneling properties reduces in quantity in the same way as the voltage of the capacitive voltage divider, see Section 4.4. As the offline charge detection circuit is exposed to the charge for a longer time-frame, the quasi-static case is considered at 20 s settling time. The amount of charge remaining after 20 s delay is calculated depending on the initially available amount of charge on the capacitor. Figure 5.13 shows the resulting quasi-static charge for varying initial charge amounts. Any charge applied to the capacitor and transistor in excess of this limit will tunnel through the oxide of the transistor when applied (second graph). In order to allow for the detection of the surface charge placed by the FIB, the charge limit for the capacitor and transistor must be less than the actual amount of charge mirrored into the antenna from the FIB irradiation. According to this simulation, a total charge amount of 0.125 pC is required on the capacitor



(a) Electrical potential



(b) Electrical field strength

Figure 5.12: Simulation of the electrostatic potential and electrical field strength (with detailed views as inlets). A constant surface charge is used as a simplifier FIB influence model. This simulation is used to derive the capacitive coupling model between surface and antenna.

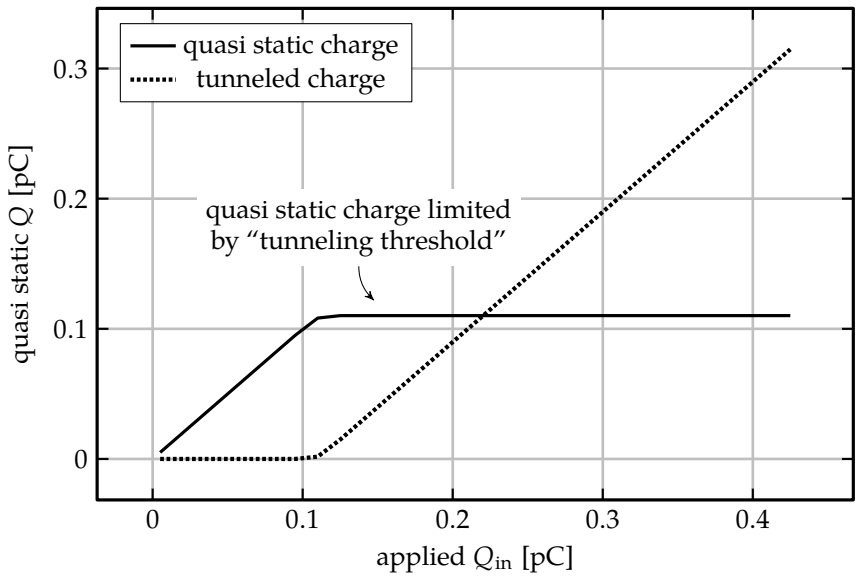


Figure 5.13: Simulation of the tunneled charge amount from the applied surface voltage based on the capacitive voltage divider simulations.

and transistor to enable the charge measurement through tunneling with the offline charge detector circuit. The charge amount presented to the antenna in excess of this will cause a detectable signal.

Three possibilities exist to control the sensitivity of the circuit. The capacitor and transistor size can be reduced to allow for the tunneling at a lower charge amount; the parts of the charge required for tunneling can be placed onto the device prior to the experiment; or the size of the antenna can be increased, improving the charge collection. All realized instances have a capacitor of approximately 13.7 fF and a transistor of 0.4 µm × 1 µm. These devices give the simulated result from the tunneling properties as noted above. The antenna area and the antenna opening in the grounded metal wiring are varied as stated above. After successful verification of the properties, a suitable version of the antenna and opening can be chosen.

The circuit layout is made compact to validate a low cost integration into existing designs based on the area requirement. For a single instance excluding external connections, the required area is 18 µm × 9.1 µm. This circuit is already equipped with the additional transistor and connections to ensure a reliable handling for later experiments. ESD protection of the circuit connections are implemented using resistors. Though, this does not prevent damage, it helps in reducing problems with ESD. The layout of the offline charge detector is integrated into the layout of the closed-loop feedback implementation, see Figure 5.6 on page 74.

Verification of the offline charge detection circuit is carried out through electrical characterization of the transfer function between feedback voltage input and tran-

sistor output current. A scaled MOS transistor transfer function is expected. If the floating gate is shorted to a fixed potential (e.g. transistor oxide short), the transfer characteristic would be constant. If the feedback capacitor is shorted instead, the transfer characteristic would only be scaled, thus detection could be potentially difficult. For this case, a similar verification procedure can be carried out as is done for the closed loop feedback circuits: Applying a voltage ramp to the feedback input, a tunneling current can alter the charge on the floating gate, shifting the transfer characteristic. In this case, the detection of a short in the feedback capacitor would not cause a shift in transfer function. Additionally, observing the faint drain current in sub-threshold region allows for detection of malicious cells, too. Though some cells are found exhibiting a bad sub threshold behavior, these are attributed to damaged select transistors as the floating gate behavior is still intact.

The function of the antenna structure and the capacitive coupling to the floating node is not verified. Still, the experiments suggest that the applied structures are capable of detecting charge as can be seen from the usage scenarios presented in section 6.3.

Chapter 6

Results on Application Scenarios

The charge measurement realization as presented in the previous chapter allows to observe effects, that were previously impossible to analyze. The improvement in sensitivity and new possibilities for analyses is shown with three examples. The first application is the characterization of a dielectric where the charge sensor is externally connected to the dielectric test structure. Previous measurements of dielectrics allowed for current values of tens of femto amperes to be measured. The charge sensor improves this value down to below 1 fA. If the charge sensor and the dielectric test structure are placed onto the same IC, the measurement is easier to conduct because complex device preparation can be skipped. Additional external measurement equipment does not need special requirements making it ideal for characterization of dielectrics in a routine way, previously impossible. As a third application of charge measurements, the charging in a focused ion beam (FIB) circuit edit (CE) procedure is considered. The charging from FIB irradiation is shown with the closed loop feedback implementation and with the offline charge detection circuit. The charging from the FIB is measured down to 0.2 pC and further effects show equivalent currents into the charge sensor below 0.1 fA. These measurements are made possible due to the low noise current values below 10 aA allowed by the charge measurement implementation. The final two sections within this chapter show results of charge analysis with respect to security ICs.

The closed loop feedback implementation is in all measurements assembled on a printed circuit board (PCB). This PCB contains the additional components required to operate the charge sensor, see Figure 5.5. In order to power the PCB and device and to record the resulting output voltage of the charge sensor, the Keithley Instruments Semiconductor Characterization System SCS-4200 is used in sampling mode. This system is equipped with 5 source and measurement units (SMUs) and one ground unit. The SMUs are used to supply the negative and positive power supply voltages, the voltage to control the switch (see Figure 5.5 on page 71) and the programming

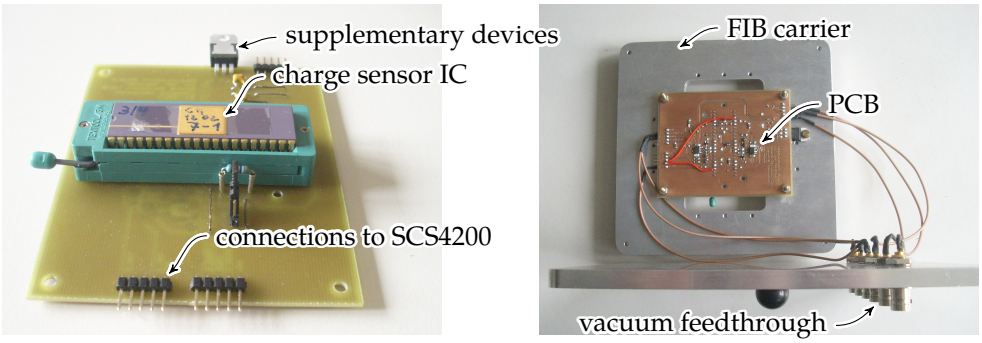


Figure 6.1: Photograph of the measurement setup for the closed loop feedback implementation. The charge sensor device is placed into the socket on the PCB (left) and connected to the SCS4200 (not shown) through the terminals (right). The setup is either placed into the FIB or into a needle prober station. To allow using the setup inside the FIB, the connection and setup is made vacuum proof with feed-through connections (right).

voltage. One SMU is used to record the output voltage. The output voltage recording is done with a resolution of 20 µV according to the specification of the system [128]. Figure 6.1 shows a photograph of the charge sensor circuit, the supporting PCB and the connections for interfacing to the SCS-4200. The setup is made capable of operating in vacuum to be able to do in-situ measurements within the FIB. For non-FIB measurements, the setup is operated on a needle prober (at ambient pressure) with the same connectors.

According to Equation 5.2, the feedback capacitor C_{FB} determines the sensitivity of the charge sensor. Some results presented within this section are charge measurements which are converted to current values. Especially for dielectric characterization discussions, this is the prevailing method in the scientific community. The current measurement sensitivity depends on the charge sensitivity and the period used to derive the current value, see Section 5.3. Thus, the charge sensor sensitivity and the period for current determination are given for all presented results. The derivation of the current values are performed by using a least mean square (LMS) approximation on the recorded charge values. The LMS calculates from charge amounts q_i at times t_i the linear approximation between q_i and t_i which gives the minimum square errors from the measured values. In the case of a constant current I, this gives an approximation current I', where the difference depends on the measurement noise. See Appendix C for a calculation of the noise. If the current is constant, I' is calculated with LMS by:

$$I' = \frac{(\sum_i t_i)(\sum_i q_i) - N \sum_i t_i q_i}{(\sum_i t_i)(\sum_i t_i) - N \sum_i t_i^2}$$

where the sums over i are considered for all measured tuples $(t_i; q_i)$. If the current is not constant within the period of measurement, the approximation will not be correct accordingly. The use of LMS reduces the noise power by the number of measurement

points. In cases, where the current is plotted over time, the current determination has also been done using LMS on a limited subset of adjacent measurement points. The number of measurement points used for this calculation are given accordingly and make up for the period as before.

In a later section of this chapter, the offline charge detection circuit will be used. This circuit is not connected to external components during application of the charge. Only during the measurement phase, the circuit is connected to the SCS-4200 system without additional components and a simply sweep test program available for device characterization in the SCS-4200 is used to characterize the offline charge detection circuit. More information on the evaluation of the data is given in Section 6.3.

The last sections within this chapter is fundamentally different. Instead of analyzing charge quantitatively, it only does a qualitative analysis. Again, it is shown that using charge or analyzing charge can yield information that is previously not available. The secondary electron (SE) emission is used to analyze the surface potential of an integrated circuit silicon backside and different aspects of PUF characterization are identified that relate to charge.

6.1 Dielectric Characterization

6.1.1 On-die Dielectric Characterization

The charge sensor measurement is applied to dielectric characterization. Conventional means to measure dielectric behavior is capable of performing measurements with 2 fA…4 fA of noise when a single measurement point takes 50 s, see Section 3.1. This can be improved by a factor of 10 to 1000 when the charge sensor is employed. Two such measurements will be presented that enable the characterization of dielectrics down to below 1 aA of noise current. The first setup will include both the charge sensor and the dielectric test structure into a single die by design. The second setup will use a dedicated charge sensor instance which is connected through a bond-wire to a target dielectric test structure.

On-die dielectric characterization is performed on the MIM capacitors available in the BiCMOS technology used for fabricating the charge sensor [145]. For this purpose, the closed loop feedback charge sensor circuit is instantiated on a dedicated test chip. The input of the charge sensor is connected by design to a MIM capacitor as dielectric stress test structure. This charge sensor is then capable to measure the charge leaked through the MIM capacitor dielectric. Thus, the MIM capacitor implements a dielectric stress test structure in this situation. As the connection and instantiation is done by design at the layout phase of the test chip, the device is functional once all required metal layers have been manufactured. Thus, the charge sensor measurement could be performed on a wafer level already.

The second terminal of the stress test structure (i.e. the MIM capacitor) is wired to a pad which is contacted through a needle probe during measurement. In order to

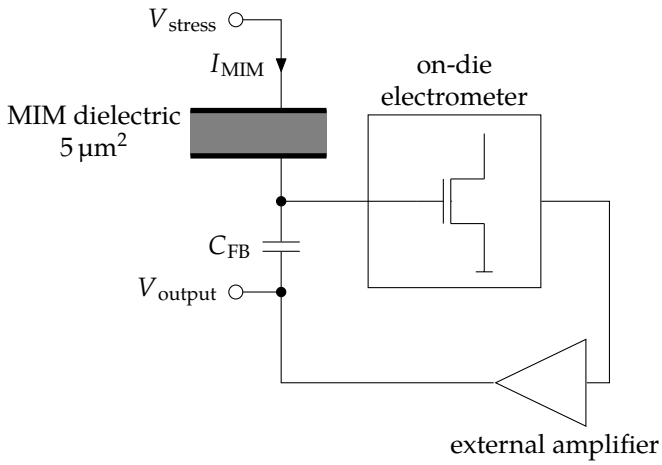


Figure 6.2: Schematic of the implemented charge measurement circuit including the attached stress test structure. The dielectric test structure is a MIM capacitor available in the technology of the charge sensor. [145]

minimize potential damage to the structure during production, the test structure bond-pad is additionally equipped with a resistor to substrate in the layout. Charging effects during manufacturing do not generate severe damage through the huge antenna area of the bond-pad. Figure 6.2 shows the resulting circuit schematically. The voltage at the bond-pad of the test structure is labeled V_{stress} as it relates to the voltage across the dielectric.

In order to facilitate the experiments in this work, the test circuits are wire bonded into a 40-pin ceramic dual in line (DIL) package. This package has a removable lid which is opened to allow the contacting of the stress test structure bond-pad with a needle for the application of V_{stress}. The electrical power supply is powered up and the device starts operation with a constant voltage V_{stress}. The resulting output voltage of the charge sensor is recorded for a time of 150 s and the experiment is stopped again by removing the power supply voltage. This procedure is repeated for different voltage settings of V_{stress}. The resulting voltage traces are scaled by the sensitivity of the charge sensor, in this case $C_{\text{FB}} = 1.37\,\text{pF}$, to yield the charge leaked through the stress test structure. Some of the resulting traces are shown in Figure 6.3.

Using the LMS approximation, the measured charge trace is converted to a linear function, which is shown for 23.1 V and 24.1 V of V_{stress} in gray in Figure 6.3. Assuming a constant leakage current through the dielectric test structure, the linear approximation would ideally be equal to the measured charge trace. Only noise would make the measurement differ from the approximation from time to time. Yet, when considering the graphs from Figure 6.3, a systematic difference between the measurement and the approximation is apparent. The measurements do not show noise on this scale but are curved. This means that the charge accumulation speed differs between beginning (fast accumulation) and end (slower accumulation) of the measurement. As the charge accumulation speed is equal to the leakage current

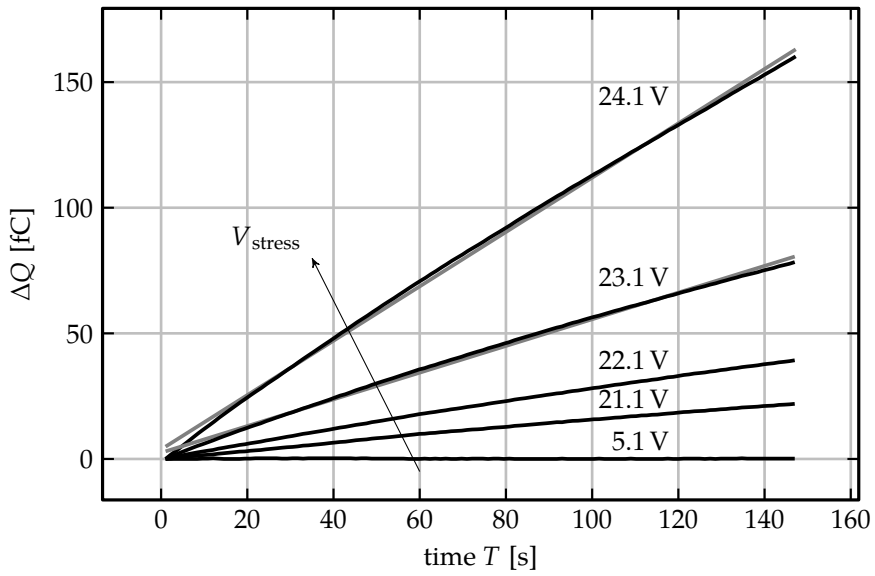


Figure 6.3: A MIM stress test structure is exposed to an increasing stress voltage V_{stress}. Subsequently, the leaked charge is recorded using the charge sensor ($C_{\text{FB}} = 1.37\,\text{pF}$) [145]. As a result, different levels of leaked charge are observed. The gray plots are the approximations as derived from the LMS algorithm.

through the dielectric, this suggests that the leakage current is not constant over the whole measurement period of one trace. Instead, the leakage current decays with the measurement time.

Many reasons can cause the observed behavior with varying origins. The most important differentiation between all possible reasons is the point of origin. If the behavior is originating from the charge sensor circuit, the measurement benefits would reduce severely. Assuming the measurement circuit does not work as expected and the decay of current is a side effect of the charge measurement is possible. Such effects could for example originate from operating point drift of the whole circuit. For example temperature change originating from the electronic power dissipation could result in this effect. Yet, temperature effects would be observed independent of the actual leakage current as the power consumption of the measurement circuit is approximately independent of the actual charge readings. Accordingly, all traces would have to show the same temperature behavior (i.e. time dependent slope). This is obviously not the case as for example the charge trace for $V_{\text{stress}} = 5.1\,\text{V}$ is very linear (i.e. constant level zero). This supports the assumption that the charge measurement circuit works as designed but the leakage behavior of the dielectric test structure has a non-constant leakage current. In order to verify this, the same type of structure, but with sufficiently large area, is measured multiple times with conventional means. The resulting current traces show a similar decay of current over time. This also manifests in difficulties of measuring the dielectric leakage behavior of the MIM dielectric with conventional means. Recording the same measurement trace multiple times results

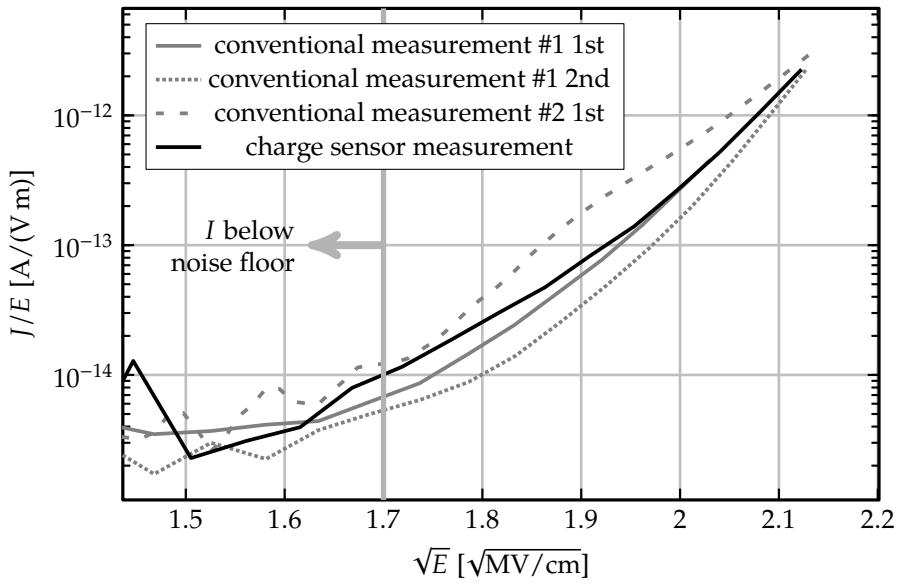


Figure 6.4: Comparing the leakage current of the MIM stress test structures from different measurement techniques. Two conventional measurements consecutively acquired with the SCS4200 on two 5625 µm^2 large stress test structure and a charge sensor measurement (C_{FB} = 1.37 pF, N = 120, T = 150 s) on a 5 µm^2 large stress test structure derived from the charge traces from Figure 6.3 by LMS approximation.

in decreasing current values, see for example Figure 6.4.

All recorded charge traces are analyzed with the LMS algorithm to obtain the slope, regardless of the curving observed already (this is neglected for performing the LMS approximation). This slope of the charge trace is the average current during the charge measurement for a single trace. The MIM stress test structure exhibits Poole-Frankel tunneling [15], which is modeled with a characteristic according to Equation 2.3 on page 28. Plotting the characteristic function **J** divided by E in a semilogarithmic scale against $\sqrt{E}$ yields a straight line. Figure 6.4 shows this kind of plot for the charge measurement values (solid black graph). A comparison to a known working setup is desired, yet is not completely possible to achieve. The same MIM dielectric is measured with a much larger area (1000 fold and 2000 fold) on two different test structures using a conventional measurement system. The measurements differ significantly and even measuring the same structure twice in direct succession does not show equal traces. This supports the assumption, that the leakage characteristic of the MIM dielectric alters significantly even during the short period of measurement. The charge measurement trace as shown in Figure 6.4 is likely to reflect the actual leakage behavior of the analyzed structure. Additionally to this, the time dependent characteristic alteration of the MIM dielectric is already apparent from the charge traces. With the conventional measurement system, this information is only available after performing specific steps for it – repeating the measurement for example. Derivation of the characteristic coefficients in the PF tunneling Equation 2.3

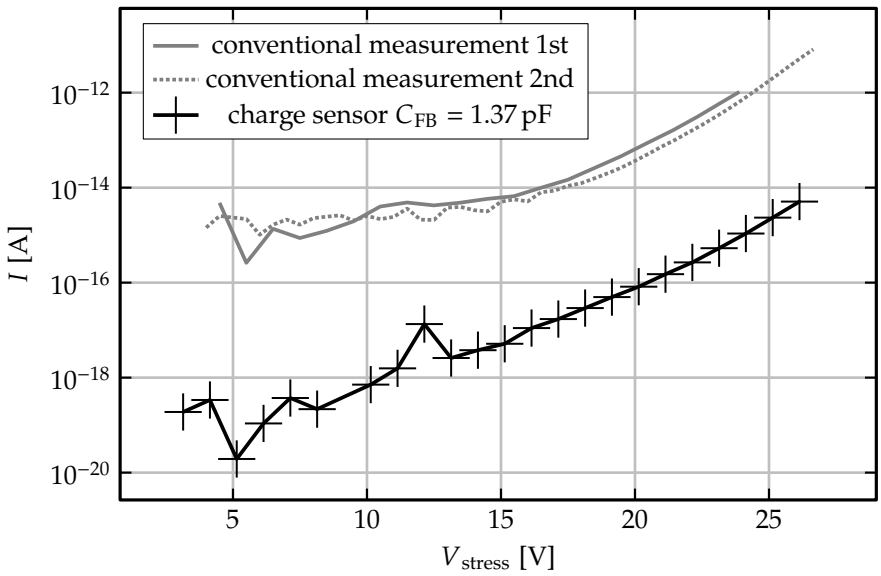


Figure 6.5: Absolute current values for the two measurements from Figure 6.4. The noise floor for the charge measurement is roughly 1000 times less than that for the conventional measurement, opening up multiple possibilities for this measurement techniques.

is hindered by the characteristic alteration. The current traces from Figure 6.4 are not linear as supposed from the PF model. Yet, without further investigations into the tunneling behavior of the stress test dielectric, no explanation can be provided for the observed effect.

The charge measurement system enables the measurement of very low absolute currents. In the previous graphs, all currents are converted to current densities according to the designed stress test structure area. As the current densities are comparable, the absolute current values scale with the area of the dielectric. In this case, the dielectric area is 1000 times larger with the conventional measurement than with the charge sensor measurement. Accordingly, the charge sensor measurement is required to be 1000 times more sensitive than the conventional setup. Figure 6.5 shows the same measurement values but within a simple voltage-current semilogarithmic plot. The noisy readings at the lower bound of the capabilities of the respective measurement setups are included to show the performance difference between the two measurement types. Accordingly, the charge sensor measurement is performing approximately 1000 times more sensitive than the conventional setup. The conventional measurement system shows a noise level of several femto amperes where the charge sensor measurement reaches down to below atto amperes. The measurement time is comparable for both measurements: 3450 s for the charge sensor and 1730 s for the conventional setup.

Using Equation 5.10 on page 66 to determine the resulting current sensitivity from a single charge trace supports this assumption. A charge trace with negligible leakage

current, for example for $V_{\text{stress}} < 7\,\text{V}$ gives RMS voltage readings at the charge sensor output of approximately $50\,\mu\text{V}\ldots80\,\mu\text{V}$. With 120 readings of the charge value within the 150 s period of observation, the equivalent resulting current noise would be

$$\begin{aligned}\sqrt{{i_{\text{n,in}}}^2} &= \frac{C_{\text{FB}}}{T}\sqrt{12\frac{{v_{\text{n,output}}}^2}{N}\frac{N-1}{N+1}} \\ &= 0.23\cdot10^{-18}\,\text{A}\end{aligned}$$

As can be seen in Figure 6.5, this value is a reasonable approximation of the resulting current noise. Achieving such a current noise reading with conventional measurement means can be considered impossible: Assuming a noise floor of 0.23 fA with a conventional measurement system (Keithley Instruments SCS-4200 gives roughly 1 fA at best), averaging of a total of $1\cdot10^6$ readings would be required to achieve a 0.23 aA noise floor. Apart from the enormous measurement time required to achieve such a result (roughly one *year* per measurement point), the stress structure would most likely not survive such a long time under elevated stress levels.

Numerous benefits arise when such small absolute currents are detectable. Instead of using large areas to characterize a dielectric, significantly smaller structures can be used. This is important as large areas are less likely defect free. Accordingly, using a measurement on a large area test structure will probably show the behavior of the defects, not of the dielectric. Acquiring the intrinsic properties of the dielectric is enabled by sensitive means such as the charge sensor measurement. The amount of information available from the charge measurement traces is obviously more than the information available from the conventional measurement. The charge measurement trace already shows that the leakage current is not constant for the whole measurement time. This effect of the charge sensor measurement principle will be of even greater interest with the measurement of a different dielectric discussed as next experiment.

6.1.2 Off-die Dielectric Characterization

If the dielectric to investigate is not available in the charge sensor technology – or if the means to construct the charge sensor circuit are not available in the technology of the dielectric – an off-die dielectric measurement is required. In order to conduct this measurement, a bond-wire is used to connect a charge sensor die to the die containing the dielectric test structure. The bonding process is performed with great care to preserve the charge sensor functionality and prevent ESD damage. With this setup, the measurement during the regular wafer level testing would not be possible. Yet if the power of the charge sensor is required, the costs of a specialized setup are often justified. Using a printed circuit board (PCB) to create the connection between the charge sensor and the dielectric test structure could introduce numerous problems. For example leakage currents through the PCB or the PCB surface from impurities can be present. Also, electro magnetic (EM) or noise reception through the larger

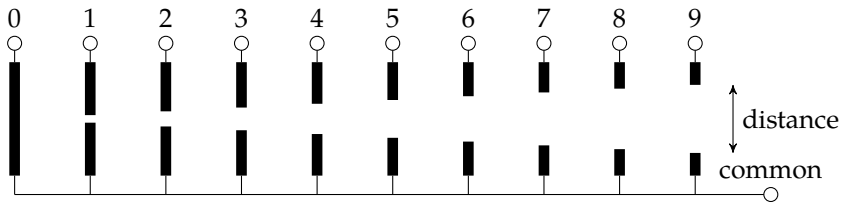


Figure 6.6: The tip-to-tip stress test structures with varying distances used to evaluate the charge sensor, according to [135]. Each terminal has a bondpad to contact the specific tip.

physical setup could be problematic if the sensitive input of the charge sensor would be routed over the PCB. Using the bond-wire connection directly between two dies (chip-to-chip bond-wire) makes the measurement resistant against many of such problems.

Many different kinds of stress test structures have been used to study dielectric behavior, for example comb structures [81] where the dielectric is between adjacent metal wires routed in serpentines. One of the main purposes of these structures is to elevate the absolute current to a level where the (conventional) measurement equipment employed for characterization is capable of performing measurements above noise level. This usually involves relatively large areas (e.g. long wires routed in serpentines) where the averaged current through the whole structure is analyzed. These structures do not allow to measure individual, localized sites. A conceptual different dielectric test structure has been proposed in [135], where the dielectric to investigate is only subjected to the stress at a very small area. These structures are built from opposing tips of metal wires with dielectric in between. Using these structures, the stressed dielectric volume and cross section are relatively small allowing for an in-depth analysis with physical methods [135]. Figure 6.6 shows a schematic view of such stress test structures.

The test structures used to obtain the results from this section are similar tip-to-tip structures where the stress test structure is a low-k dielectric. Different distances between two neighboring peaks are realized. The cross sectional area of the tips is very small and stressing the structures yields a very low total current value. Using conventional means to measure such structures, the investigation of pre-breakdown behavior faces severe problems as the degradation of the structures is already advanced when the measurement system measures currents above noise level [135]. Using the charge sensor promises significant improvements as the absolute current measurable with the charge sensor is multiple orders of magnitude lower than with conventional setups.

Figure 6.7 shows the setup used for these measurements. The charge sensor (C_{FB} = 137 pF) is bonded to the DIL package as before in order to allow the normal operation. The stress test structure is placed inside the same cavity of the package next to the charge sensor. A bond-wire is placed between the charge sensor input and the stress test structures common terminal. The package is again supported by

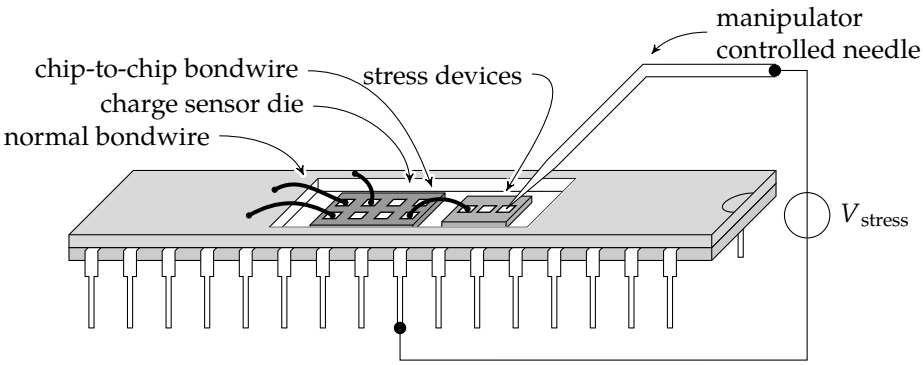


Figure 6.7: Small geometries are mandatory for ultra low current measurements. The stress voltage is applied by a probing needle to a bond-pad, allowing to measure multiple test structures (see Figure 6.6) with a single charge sensor.

a PCB with additional components required to operate the charge sensor, see the photograph in Figure 6.1. The individual terminal of the desired stress test structure is then connected to the stress voltage source using a prober needle. Again, the setup is supplied with power and measured through the Keithley Semiconductor Characterization System SCS4200 as before. Also, the measurement procedure is kept the same, applying different stress voltages V_{stress} to the stress test structure and recording the sensor output for a certain time, repeating the procedure for increasing stress voltages.

The resulting charge traces are shown for two stress peaks in Figure 6.8. As the applied stress voltage is relatively low and constant over time, a constant leakage current would be expected. Again, the LMS approximation for the exemplary traces is shown in gray plot. The type 1 structure shows a linear charge accumulation apart from added noise. No systematic difference between the charge trace and the approximation is evident. This supports the assumption that the leakage current through this structure is constant for the measurement time. It also supports the assumed functionality of the charge sensor. In contrast, the stress test structure type 2 shows systematic differences between the linear approximation and the charge trace. Here, the charge traces show discrete steps suggesting spikes in current conduction. These results will be discussed in two ways: At first, the mean current (i.e. slope of the charge traces) is – as before – plotted and discussed with respect to the applied stress voltage. Again, this result is compared to possible acquisition by conventional means, showing the performance increase by the use of the charge sensor. The second discussion will focus on the charge traces from the dielectric test structure type 2. These traces are also taken individually and a time dependent current value is derived. As a consequence, the leakage current value shows these spikes, which is not observable by conventional means.

The slope of all charge traces is approximated by the LMS method, as drawn in gray for the exemplary traces in Figure 6.8. Subsequently, the current resulting from each charge trace is plotted into a current-voltage plot. Figure 6.9 shows the resulting

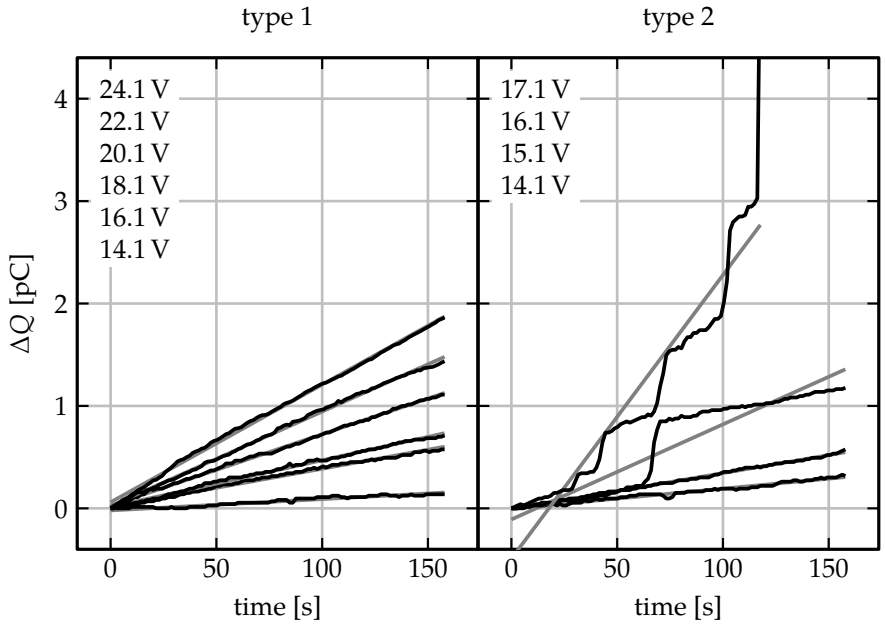


Figure 6.8: Charge traces for different applied stress voltages of the comb structures for two individual peaks located in vicinity to each other, $C_{FB} = 137\,pF$.

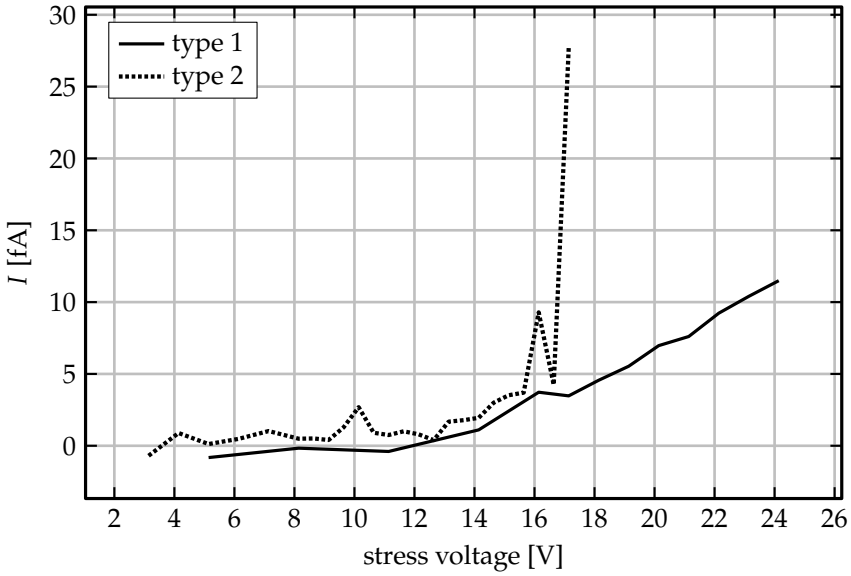


Figure 6.9: Leakage current behavior derived by LMS from the charge traces for the off-die dielectric characterization, $C_{FB} = 137\,pF$, $N = 110$, $T = 160\,s$.

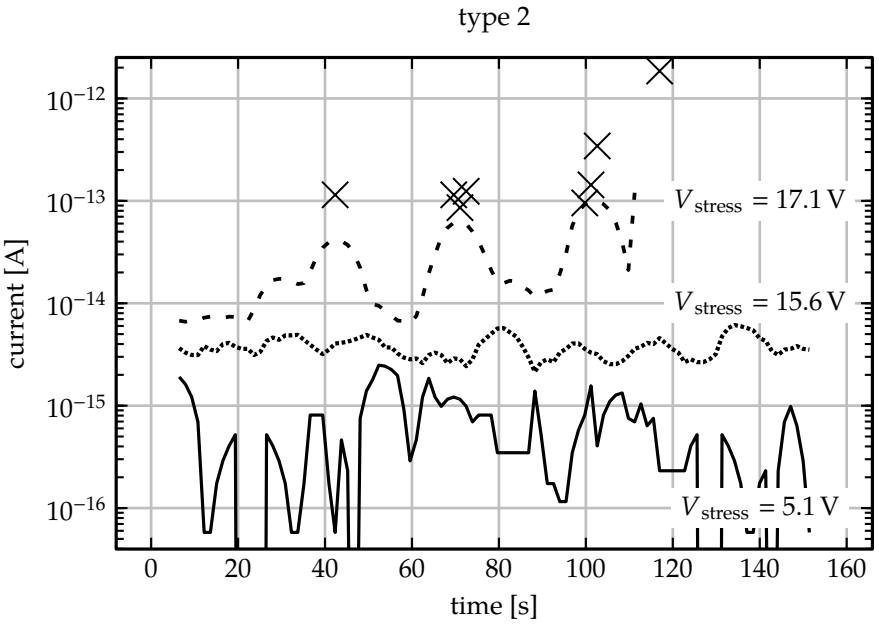


Figure 6.10: Current derived from a subset of points from three exemplary charge measurements showing the time resolved behavior of the leakage current (C_{FB} = 137 pF, N = 10, T = 15 s). The cross marks are the values achieved if instead of ten charge readings only three charge readings are used for LMS approximation at the charge steps of the 17.1 V trace.

current traces for both dielectric stress test structure instances. As can be seen, the noise current is again below femto ampere allowing for very sensitive measurements. This is also supported by the calculation through the noise from the charge trace. The variance in output voltage of the charge sensor output for a low stress voltage (i.e. below 10 V, see Figure 6.9) is substituted in Equation 5.10 on page 66. A variance of 0.1 mV…0.4 mV (type 1) is observed, resulting in an expected RMS current noise (using Equation 5.10, T = 160 s, N = 110) of 28 aA…84 aA for this charge sensor setup, supporting the low noise level of the charge sensor measurement. Yet, the noise is larger with this structure in comparison to the previous on-die measurements, as the feedback capacitor is significantly larger. Additionally, higher voltage noise of the charge sensor output is observed, which is possibly attributed to the large physical size (i.e. bond-wire) and additional influences from surroundings (i.e. free air, etc) in comparison to the on-die implementation. Such effects can not have an influence on the previously shown on-die measurements as in that case the sensitive node is very small and not exposed to the surface. The noise level of the charge sensor measurement is still lower than with a conventional setup.

The dielectric stress structures type 1 and type 2 differ only in tip-to-tip distance. They are located in direct vicinity suggesting that process variations should still be small. Yet, their current-voltage characteristics differ significantly. A clear explanation is not possible from the simple current-voltage measurements. Thus, if a

conventional means with appropriate sensitivity would have been used, explanation of the difference would be very limited. If using the charge sensor this difference can be analyzed in greater detail. Apart from the analysis of the mean current values, the charge traces can also be analyzed with respect to time.

Figure 6.10 shows three exemplary traces of current converted from the charge trace from the type 2 dielectric test structure with respect to time. The LMS algorithm has been applied to only a subset of all measurement points ($N = 10$, $T = 15\,\mathrm{s}$) in order to allow for investigating the current at different points in time during the measurement of a single trace. This allows to improve the bandwidth of the result mathematically interchangably for increased noise level of the current. When using multiple points to derive the current, as done in Figure 6.10, a step in the charge trace as seen in Figure 6.8 results in a wider current spike, see the plot for $V_{\mathrm{stress}} = 17.1\,\mathrm{V}$. The maximum of this current trace than does not show the actual maximum value. Reducing the number of charge readings used for the LMS approximation allows to compensate for this while at the same time increasing the current noise. Yet, if the current spike is large, an increase in current noise does not degrade the result significantly. The cross marks in Figure 6.10 have been placed at the positions of the steps in the charge trace for the stress voltage of 17.1 V. The magnitude at these points has been calculated by using only three charge readings. The increase in noise is less than the current readings from Figure 6.10 (theoretical $i_{\mathrm{n,in}} = 70\,\mathrm{fA}$ for the worst case charge sensor output voltage noise). Yet, due to the fact that only a single point resembles the steps in the charge traces, the maximum bandwidth of the measurement still does not catch the signal correctly. Also, the maximum current value in the current spike is not determined correctly. In order to achieve these two results, the charge readings must be conducted significantly more often, which was not possible with the SCS4200 system.

Performing physical analysis (e.g. TEM investigations) of breakdown behavior or pre-breakdown behavior makes the use of localized structures mandatory [135]. Measuring these small structures with conventional measurement means poses severe limitations on the observable effects. Using a charge measurement setup allows measurement of significantly less absolute current values. Degradation can be easier detected with such a setup. Additionally, the charge measurement system allows for an in-situ adaption of the measurement time to the current observed. For example the charge trace for the 17.1 V stress voltage is stopped prior to reaching the 160 s measurement time because significant charge steps are observed. At this point, the stress to the structure already shows electronic alteration of the behavior (i.e. steps in charge readings) and could be analyzed through additional physical means. Using a conventional setup, this would not have been possible to detect.

Summarizing the dielectric characterizations performed with the charge sensor circuit shows the huge potential of this technique. The absolute current value detectable is lowered to single digit atto amperes. With such low currents, structures to be analyzed can be decreased in size significantly. Even tip-to-tip structures can

be analyzed on a current level significantly below conventional means. With small structures, the degradation is localized and can be analyzed with physical techniques. Also, defects are less likely present in small structures, enabling the analysis of intrinsic device and material properties. If stress structures exhibit varying currents, the charge sensor measurement allows for in-situ detection of this behavior during the measurement. Thus, the measurement time can be adapted to the observed current value, without requiring to restart the measurement (e.g. within different measurement range). Applying the charge measurement method to dielectrics will allow for previously unknown analysis means, precision and speed.

6.2 Charging by FIB

Focused ion beam (FIB) systems are employed for micro-manipulation of semiconductor devices on a regular basis. A significant drawback of this technique is the charging effect of insulating targets. The incident ions and the emitted secondary electrons (SEs) cause a positive surface charge deposited on the insulating surface of the IC. This charging can be lethal for sensitive circuits. Electrostatic discharge (ESD) can happen between the surface and underlying metal lines, destroying gate oxides of transistors connected to the affected metal line. During such ESD events, very high voltages and currents are present within the IC. The surface charging is the driving force for ESD and thus it is beneficial to know about the surface charge during FIB processing. Using the charge sensor, this surface charging and other effects originating from the FIB can be analyzed with high precision for the first time. This section will cover sample measurement results obtained while operating the charge sensor inside the FIB.

In a FIB system, the incident ions and emitted electrons cause a net positive charge on the insulating surface of an IC. Figure 6.11 shows an idealized model of the ion-solid interaction effects most important within a FIB system when a charge sensor (or any other insulating surface) is targeted. In order to observe the positive surface charging effect, a charge sensor with an antenna structure connected at the input as described in Section 4.3 is used. The charge sensor and the antenna are fabricated on the same die and the connection is placed during the design phase. A simple rectangle of metal at a layer which is covered by insulating material on top resembles the antenna.

Apart from the physical interaction between ion and surface, electrical effects become apparent. Incident ions are either neutralized or remain on the surface of the device. During the stopping of the ions, SE can be generated and either be emitted into the sample or into the vacuum chamber. These SE also cause a positive surface charging. The positive surface charging and the emission of SE into the sample material are the main effects that can have an influence on the charge sensor antenna. Direct influence from incident ions onto the antenna structure (and thus the charge sensor) is not possible because of the insulating layer on top of the antenna. The penetration depth of ions with $W_{\mathrm{kin}} = 30\,\mathrm{keV}$ is limited to tens of nanometers [55,

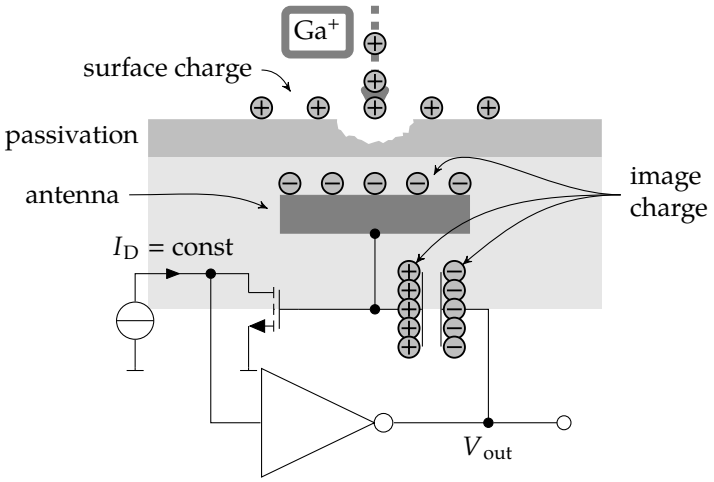


Figure 6.11: Surface charging model and resulting mirror charges in the charge sensor

72] not allowing for ions to reach the significantly deeper buried antenna structure. If SE are emitted into the sample material, their final location will determine the influence to the antenna. Electrons can "get stuck" within the material between surface and antenna. Electrons emitted into the insulator leave a positive charge of same amount on the surface behind. As a result, the mirror charge on the antenna is not altered as long as the electron does not reach beyond the antenna. It merely is a superposition of the antenna functionality with two opposite charges, see Section 4.3. The requirement for this approximation is again that the distances between (all) charges and antenna are small compared to the distances to surroundings. This means, that any charge between antenna and surface is not reflected by the charge sensor reading. If, instead electrons reach beyond the antenna, the influence gradually increases with the distance between the electrons and the antenna. Once the electrons reach a connected metal line or the conductive substrate, they can not compensate for their positive charge left behind on the surface. Accordingly, the electron would be measured only then in total by the charge sensor. With this in mind, the charge sensor reading basically resembles the surface charge, except for charge displaced within the sample between surface and antenna.

The ion beam inside a FIB system is scanned over the surface only when absolutely required. The impinging ions damage the surface and remove material, which has to be kept at a minimum. Thus, only during processing of CE procedures or during imaging of the surface, the ion beam is supposed to reach the target. At all other times, the ion beam is blanked electronically, collecting the ions prior to their exit of the ion column into the sample chamber, see Figure 2.1 on page 20. Consequently, in order to observe the interaction between ions and charge sensor, the beam must be scanned on purpose – for example by acquisition of an image. The image is acquired by scanning the field of view (FOV) with the ion beam. As a first experiment, this

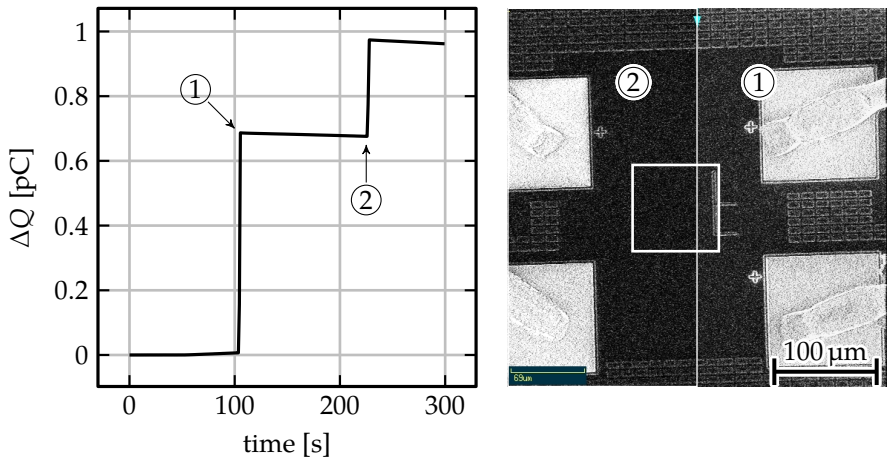


Figure 6.12: Irradiating a charge sensor (C_{FB} = 1.37 pF) with a 30 keV Ga^+ ion beam of 20 picoA. The two halves of the right image are acquired at positions 1 and 2 as marked in the graph [132].

interaction is investigated using the charge sensor. The charge sensor is operated continuously, allowing for an in-situ measurement and the ion beam is scanned on purpose at specific times over the charge sensor antenna. It is expected that the output value of the charge sensor changes during the scan.

For the experiment on the insulating target surface, a beam current of 5 pA is chosen. Figure 6.12 shows a trace of the charge sensor output value over the experiment duration. The ion beam is directed to the charge sensor surface and scanned two times, as indicated at locations 1 and 2. During each scan, the ion beam is rastered over the surface according to the image acquisition procedure common in scanning applications. A simplified calculation of the theoretically deposited charge is done by neglecting the charge displacement within the volume between antenna and surface, as stated before. The resulting charge of the ion beam within the FOV is calculated using the resolution of $N_{\text{pixel}} = 512 \times 512$ pixel, the number of frames $N_{\text{frames}} = 4$, the dwell time for each pixel of $t_{\text{dwell}} = 200$ ns and the beam current of $I_{\text{beam}} = 5$ pA:

$$\begin{aligned} Q_{\text{FOV}} &= N_{\text{pixel}} N_{\text{frames}} t_{\text{dwell}} I_{\text{beam}} \\ &= 4.1\,\text{pC} \end{aligned}$$

In this case, the FOV is 355 µm × 355 µm while the charge sensor antenna area is only 80 µm × 80 µm.

According to the charge step 1 in Figure 6.12, the measured amount of charge is 0.69 pC. As the antenna structure is smaller than the irradiated area, the deposited charge above the antenna is reduced by this ratio. In this case, the antenna area is only 0.052 times the scan area, resulting in a total deposited amount of charge subject to the antenna sensitivity of approximately 0.22 pC. Because border effects of the antenna are not considered, the deposited charge is only an approximation. This

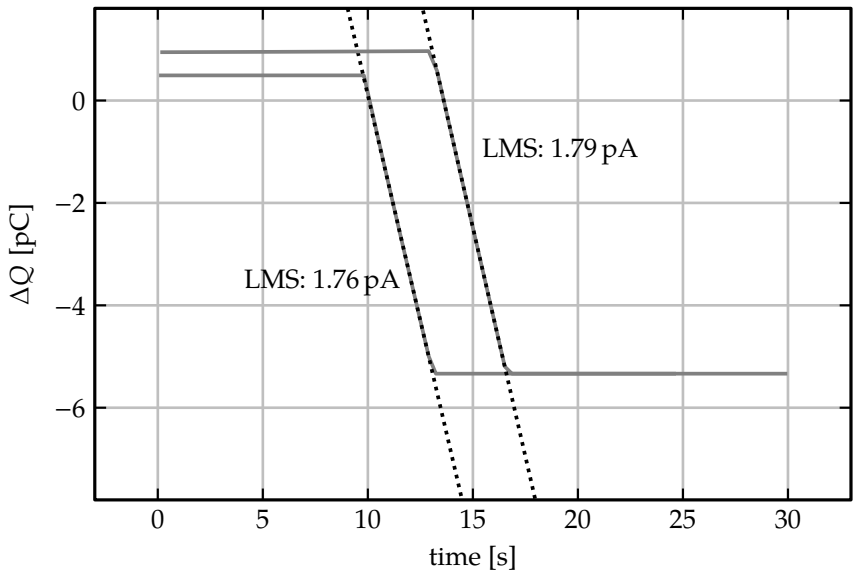


Figure 6.13: The charge sensor (C_{FB} = 1 pF) is irradiated continuously. The charge accumulation does not saturate within the observation band of this figure. The dotted traces are linear approximations using the LMS algorithm of the time-frame of irradiation.

figure is smaller than the measured charge and the difference is due to the emission of SE. The SE emission can be calculated from the measured charge amount: roughly 2.2 electrons leave the device surface per incident ion, making for a total measured charge of 3.2 times the incident beam charge. This is in agreement with emission coefficients from literature for different materials [39].

In a second scan performed with equal scan settings, at position 2 in Figure 6.12, the measured charge reduces due to the already charged surface. For surfaces of higher potential, parts of the emitted SE can be re-captured by Coulomb attraction. The recollected SE do not contribute to charging any more and thus, the effect of charging is reduced. FIB operators fear this effect due to the reduced signal strength when insulating surfaces are to be imaged, as can be seen in the right half of Figure 6.12: reduced brightness is apparent.

Before a FIB CE can be performed on an arbitrary sample, the position of the CE must be located. During this navigation step, the ion beam scans very often (close to continuous) on the surface, depositing large amounts of charge. In order to analyze the effect from such a procedure, the charge sensor is subjected to continuous irradiation from the ions. Figure 6.13 shows two traces where a nominal beam current of 1 pA is used to target the charge sensor surface. In this experiment the sensitive antenna area of the charge sensor is larger than the FOV of the ion beam and as a consequence the charge reading resembles the total effect from the ion beam. With the selected charge sensor sensitivity, it is possible to observe the surface charge for a time of 8 s as from then on, the charge sensor output saturates. The linear accumulation

of charge over this time suggests that the surface charge does not saturate within the period of the experiment. The linear behavior is approximated with the LMS algorithm and plotted as dotted graph, also in Figure 6.13. The dotted graphs suggest that the actual measurement of charge accumulation is linear in time, suggesting a constant equivalent current. The slope of the approximated charge trace describes an equivalent current of 1.76 pA and 1.79 pA, respectively. For a single impinging ion on the target, roughly 0.8 electrons are permanently emitted from the surface. This suggests, that the previously estimated value of 2.2 emitted electrons per incident ion during a single scan is reduced quickly. The graphs do not show a steeper slope when the experiment started. This could be hidden by the relatively slow acquisition speed of the charge readings in this experiment. It could show up if a higher time resolution was chosen. As the emission yield of SEs reduces from charging within a few frames of irradiation (see previous paragraph), the time resolution of the measurement from Figure 6.13 does not allow to identify this effect: Roughly 19 frames are scanned per second in the experiment. Instead, the continuous irradiation with the ion beam suggests that even when the surface is charged, certain amounts of electrons are emitted. These electrons could for example have higher energies than those electrons used for imaging (i.e. SEs of 0 eV…50 eV). Further experiments could allow for a better insight into these effects.

In this manner, the charge sensor can be used for multiple purposes. Analyzing the SE emission coefficient for insulating materials as shown is one valuable application. By the very high sensitivity of the charge sensor, very small amounts of charge already allow to determine the insulator properties. The information on SE emission can also be used in failure analysis (FA). For example, the construction of a specially crafted FIB CE procedure to reliably connect floating gate structures is possible once the induced stress from the ion beam is known. In this manner, the floating gate of non-volatile memory (NVM) cells are contacted and subsequently measured [153]. Without properly analyzing the influences from charging, such an approach would likely fail.

The extraordinary performance of the implemented charge sensor is presented within the verification experiments of Chapter 5. The output voltage of the charge sensor is in fact constant, even if the experiment time is on the order of hundreds of seconds. Yet, the experiments conducted with the FIB system showed, that even though the ion beam is blanked electronically (e.g. between the steps in Figure 6.12), an influence causes a change in the charge sensor output voltage. A quick analysis showed that the ion column must be part of the reason for this effect. The following experiments are not capable of identifying the exact source and connection between ion column and charge sensor output in this situation. Yet, their analysis shows how the charge sensor function could affect the measurement – and interpretation. With a new measurement method or implementation the interpretation of results requires special attention.

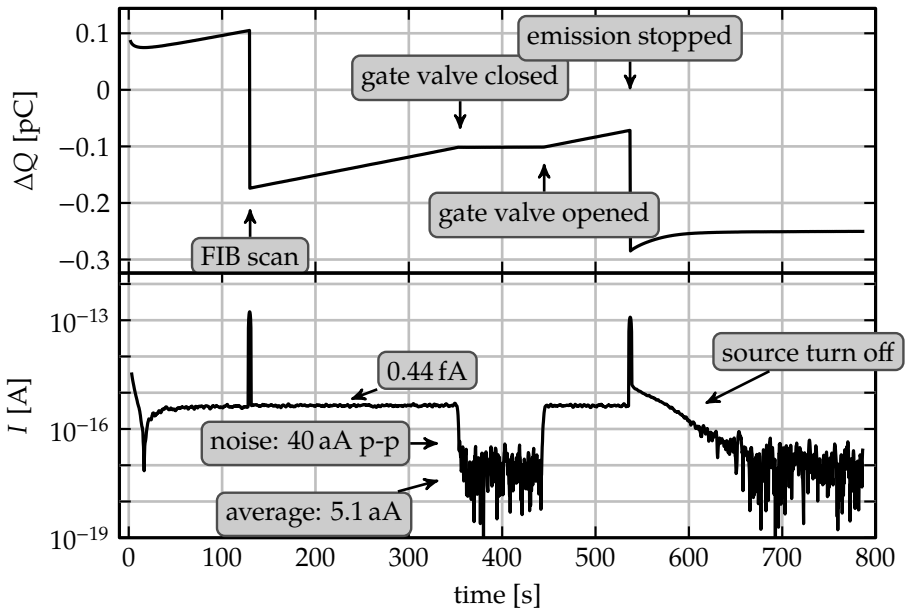


Figure 6.14: Charge and current observation from the electronically blanked FIB. Closing the metal lid (gate valve) of the column, stops the effect, $C_{\mathrm{FB}} = 1.37\,\mathrm{pF}$ PIP, $N = 10$, $T = 30\,\mathrm{s}$.

The FIB column used throughout this work also affects the measurement of the charge sensor in other ways. The primary effect of surface charging from the positive ions and negative electrons are already discussed, yet the charge sensor is so sensitive, that other effects can be observed, too. Figure 6.14 shows a trace recorded during conduction of multiple different actions with the ion beam column. The top graph shows the recorded amount of charge relatively to the start of the experiment. The lower graph shows the least mean square (LMS) calculated current. In order to perform the LMS algorithm, a subset of adjacent measurement points is used – assuming a constant current within the time-frame of this subset of measurement points.

At $t = 130\,\mathrm{s}$, a single ion beam scan is performed on the device surface. As before, charge is deposited on the surface above the antenna resulting in a net charge measurement of the sensor. Before and after the scan, the charge sensor shows a linear slope in opposite direction. The linear slope is equivalent to a constant current and is from the same effect as already seen very weakly in Figure 6.12. As the direction of charging (positive slope) is opposite to that from the ion beam scan (negative slope/step), this signal is unlikely to originate from ions hitting the device surface. If ions were the reason, the charging would be in negative direction, as with the step when a scan is performed. No action with the ion beam is performed, the beam is electronically blanked. Ions are supposed not to reach the device surface in this situation. Yet, if the ion column is closed by a mechanical metal lid (the gate valve, i.e. at $t = 350\,\mathrm{s}$ in Figure 6.14), the slope vanishes, leaving the charge sensor output

constant again. The low leakage current of the charge sensor of only 5.1 aA in this case can be identified. Obviously, the ion column must be connected to the observed effect. When the gate valve is closed, the observed slope vanishes. Thus, the charge sensor operation within the vacuum and in direct vicinity to the SE detector (see Figure 2.1 on page 20) is not the reason for the slope.

In order to isolate the source for this signal, various different actions are performed with the ion beam column. Very many different physical effects can show the observed behavior, making a directed approach difficult to conduct. Also, there is no means to conduct measurements within the vacuum of the FIB system, that could identify such effects on a different physical interaction. For example it is not possible to measure the radioactive radiation in the situation of the charge sensor with external means due to the lack of suitable equipment. The approach identifies the dependencies of the slope to the different ion column parameters, for example the beam current and blanker voltage. This does help to understand the connections but can not explain the effect in all details. The FIB system has very many parameters making a choice for parameters to be analyzed difficult.

The influence from the ion column can be from different sources. Beside the electrical field from the ion column lenses, also radiation emitted through the ion column could be the reason for the slope. The SE detector has attached “antennas”, which are on a high potential, see Figure 2.1 on page 20. The SE detector antennas are part of the FIB system and are not correlated to the charge sensor antenna. The charge sensor output slope is removed even if the voltage at the SE detector antennas stays constant, see Figure 6.14 at $t = 350\,\mathrm{s}$. This supports the assumption, that the electrostatic lenses of the ion column, are also not the source for the signal. To verify this, the gate valve was re-opened and the emission of ions was stopped without changing the high voltages and lens settings. By this means, the electrical field from the ion column should stay constant and only the radiative nature of ions (or other particles, secondaries, etc.) is stopped. During the ion source emission turn off in Figure 6.14, the FIB system performed a single image update scan, which results in the step at $t = 540\,\mathrm{s}$. Subsequently, the charge slope reduced exponentially down to the before mentioned noise level. Due to the decay of the observed current, the slope must be connected to the ion emission and not the electrical field present in the ion column. Also, the exponential decay suggests a diffusive behavior of the effect once the ion emission has come to a halt.

Radiative sources for the slope could be secondary particles, optical light (high energy) or even x-ray. Optical light would also influence the DC operating point of the circuit and cause a step if turned on or off. It is unlikely present as there is no step in the operating point of the circuit when the gate valve is opened, only the slope changes. Secondary particles like low energy SE or x-ray could be created for example during the extraction of ions from the source or during the beam blanking process. The exponential decay does not go with the arguments of x-ray being created during extraction as in this case a possible x-ray emission would stop immediately after source turn off but the decay in Figure 6.14 shows exponential behavior. Two

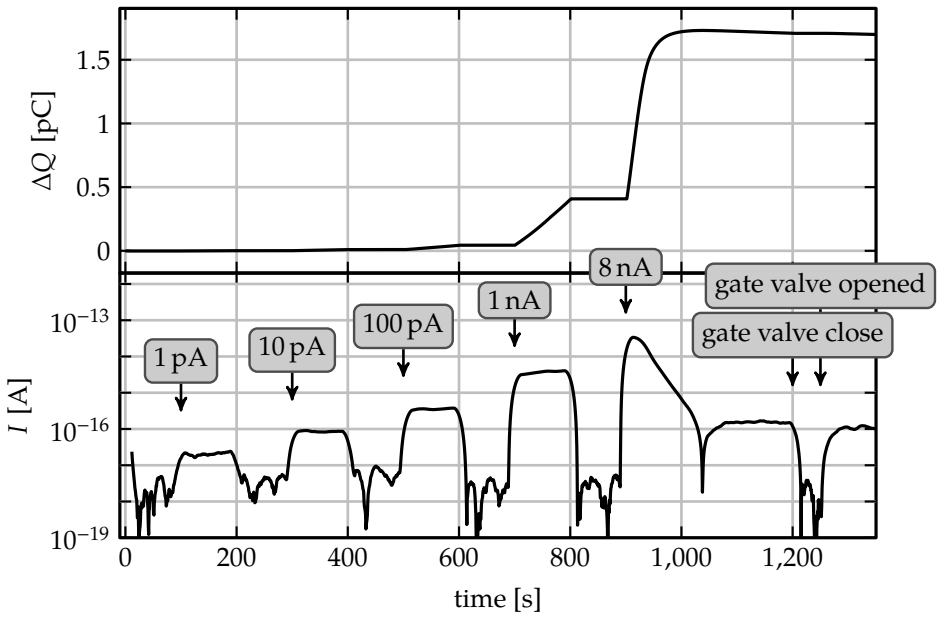


Figure 6.15: Charging and current observation dependence of the electronically blanked FIB from the beam current setting. Saturation of the accumulated charge ΔQ during the 8 nA beam current setting can be from different effects, see text. (C_{FB} = 1.37 pF, PIP, N = 70, T = 23 s)

parameters are analyzed to further clarify the possible origin of the slope of the charge sensor: the beam blanker operation and the beam current setting. The beam blanker works by deflecting the ion beam off the device into a Faraday cage with the help of the beam blanker voltage. Varying this voltage alters the beam blanking process. The beam current setting is controlled by a mechanical aperture and by varying the beam cross section at the aperture. This "electronically variable aperture" mode allows for a continuous beam current setting although desired beam current settings are pre-configured within the used system. Thus, by varying the beam current, both, the aperture and the lens settings vary.

Figure 6.15 shows the charge trace for varying beam current settings. Here, the beam current of 1 pA and 10 pA uses a 20 µm aperture, the 100 pA beam current a 100 µm aperture and the final two values of 1 nA and 8 nA work with a 200 µm aperture. Obviously, the slope observed with the charge sensor does not depend on the aperture diameter only. The lens configuration for the beam cross section size at the aperture does matter, too. The source for the slope must follow the same optic rules as the ion beam does, when reaching the aperture. Accordingly, x-ray and electrons generated before the aperture can be precluded. Electrons have opposite charge polarity and would not follow the same path as the ions. Also, from the specific working of the ion beam column, it is very likely that only those ions that normally target the sample (i.e. Ga^+ ions), can follow the optic rules that make up the ion beam path prior to reaching the aperture. It follows, that the slope must come

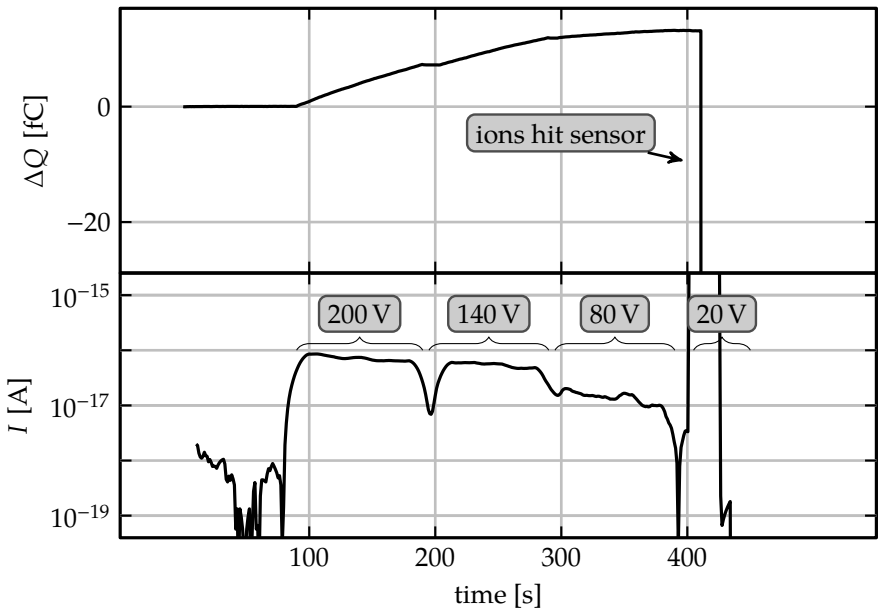


Figure 6.16: The charging is influenced by the beam blanker deflection voltage. For the voltage of $V_{\text{blank}} = 20\,\text{V}$, ions can reach the charge sensor surface. ($C_{\text{FB}} = 137\,\text{fF}$, $N = 20$, $T = 20\,\text{s}$)

from ions that traverse through the aperture. Yet, it is still possible that those ions do not cause the slope by themselves.

Selection of the 8 nA beam current setting causes the charge sensor to saturate and even reverse the direction of slope, see Figure 6.15. This suggests, that the interaction of the (unknown) radiation with the charge sensor is not an ion interaction at the charge sensor surface. With ion interaction, the slope would become less but not reverse, because the ions can reach the sample independent of surface charging due to their high acceleration energy.

Once the beam leaves the aperture, it is either blanked by the beam blanker or targeted at the sample. As the beam blanker is active during the whole time-frame of this experiment showing the slope, the beam blanker voltage dependence is analyzed. Figure 6.16 shows the resulting charge trace from varying the beam blanker voltage. At a voltage of 20 V, the beam blanker does not successfully blank the beam any more and ions reach the charge sensor surface, causing the already analyzed surface charging. This can be seen from the step at $t = 410\,\text{s}$ in Figure 6.16. For the other three settings, only 80 V shows a significant dependence of the slope on the beam blanker voltage. This allows for different possible interpretations:

- The beam blanker voltage setting does not influence the primary origin of the slope in the charge detection. Instead, the variation of the beam blanker voltage causes the blanking process to be insufficient. Subsequently, the slope continues but is compensated in parts by a few ions that are not blanked electronically and can reach the target. Finally, at a very low beam blanking voltage (e.g. 20 V),

the beam is not blanked at all any more and the significantly stronger effect from the ion irradiation overlap the actually still present slope.

- Alternatively, the slope originates from within the beam blanking process. For example SE are generated within the beam blanker during the ion stopping process. These SE then get accelerated towards the sample by the lens voltages, the beam blanker voltage and other effects. Yet the acceleration must be low enough for the electrons hitting the sample surface to have an SE emission yield less than one on the sample surface, roughly below 1 keV. This results then in a positive slope for the charge. Depending on the beam blanker voltage, the same arguments as before hold true. Additionally, the directing of SE from the beam blanker onto the charge sensor is likely influence by the beam blanker voltage, which could be seen at a setting of 80 V.

- Another plausible explanation would be, that with the ion stopping process in the beam blanker, high energy photons (x-ray or UV-light) are generated and reach the charge sensor. Inside the charge sensor, the photons could cause an internal emission from the charge sensor antenna node, which could result in the observed slope. Incident photons would not only cause a slope but also change the DC operating point of the whole circuit, very likely causing a (reversible) step in the charge trace. Such a step in the traces is not observed at the point of closing and opening the gate valve (see Figure 6.14), making at least photons as explanation unlikely.

Without further experiments, the precise origin of the slope remains unknown. Yet, multiple possibilities are considered, including effects that originate from the charge sensor itself. These examples show that even though the charge sensor functionality is clear and can be verified within the FIB, still multiple effects can cause the change of the charge amount measured with the sensor. If care is taken, the charge sensor can enable for very weak effects to be observed.

As a conclusion, it is not clear from where the observed slope is originating. Yet, the charge sensor, the vacuum chamber and possible electrical fields as well as the ion source of the FIB can be excluded as origin. Furthermore, the blanking process can play a role but is not necessarily the origin. As the slope changes with beam current and decays for emission stop, it is likely to originate between the ion column aperture and the sample/charge sensor. A precise deduction could be conducted in future works when more experimental data is acquired.

Gas presence can affect the charge sensor measurement, too. Previous publications show, that a chemical sensor could be built using the field effect principle [57, 67, 79]. It is expected that using the gas injection system of the FIB influences the charge measurements of the charge sensor. Figure 6.17 shows a trace recorded while subjecting the charge sensor to a gas flow. Before the charge measurement is started, the charge sensor is set into the vacuum chamber and the chamber is evacuated. The

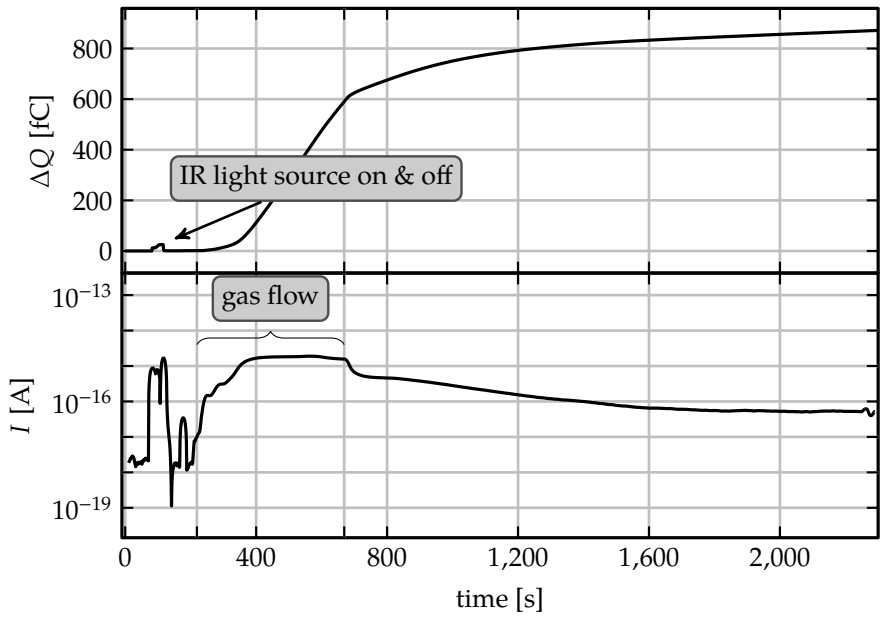


Figure 6.17: Charge traces as observed during the entry of process gases into the FIB system. No ion beam scan is performed after evacuation, the gas flow is permitted as indicated by the graph text. ($C_{\mathrm{FB}} = 1.37\,\mathrm{pF}$, $N = 20$, $T = 20\,\mathrm{s}$)

ion beam is not targeted towards the sample during the whole time period of the experiment. To navigate, the optical system is used and the gas injection needle is positioned in vicinity of the charge sensor structure. Subsequently, the charge sensor output is recorded while the gas entry is admitted. In this case, xenon difluoride (XeF_2) is chosen as gas which is usually employed when dielectrics or silicon bulk material is etched. After a time of 450 s ($t = 670\,\mathrm{s}$), the gas entry is stopped. As can be seen from Figure 6.17, the gas entry has an influence on the charge sensor output.

The charge trace is accumulating charges in a continuous fashion. Xenon difluoride targeted at the sample is considered to adsorb at the surface in parts. The superfluous gas amounts are removed from the vicinity by the vacuum pump of the FIB chamber. Thus, after an initial settling time, the adsorbed gas on the surface is fixed in amount and the gas flow will be constant. Once the gas inlet is closed, the flow will decay to a stop and the adsorbed gas molecules will be re-evaporated into the vacuum gradually. With this very simple gas model in mind, the charge sensor result can be interpreted. The adsorption process is reverted after the gas inlet is closed, but as can be seen from the charge trace in Figure 6.17, the charge amount does not revert back to the initial value. Instead, the charge accumulation continues even after the gas inlet is closed. These results support the assumption, that the change in charge does not exclusively stem from the adsorption of gas molecules on the surface as these would gradually remove from the surface once the gas flow is stopped. It suggests that the gas itself transports charge, even though the gas molecules are not initially ionized. They could become ionized by electrical fields present within the vacuum chamber

or charges present on the charge sensor surface could be picked up by individual gas molecules. If radiation is present on the charge sensor in the FIB chamber during this situation (as laid out in the previous paragraph), the gas molecules could also be ionized. Without further investigations, a clear explanation of these effects can not be given.

Summarizing the charge measurements of the FIB system. The experiments show the extraordinary potential of the charge sensor technique. The results not only represent the charging from the ion beam itself according to the prevailing model but also show the very faint influences from a blanked ion beam or injected gas. Though no severe thread arises from the measured quantities, the ion beam obviously has more effects than presently considered. Once charge can be detected sensitively with a charge sensor, the processes within a FIB system can be analyzed. If investigated further, this can potentially lead to significant improvements of FIB processing in CE tasks.

6.3 Focused Ion Beam Detector

Usage of the offline charge detection circuit is shown as a FIB detector. The purpose of this circuit is to prevent unauthorized access to internal signals carrying sensitive information using a FIB tool. The main application is in security sensitive IC design where the information on internal signals are confidential. They should also remain confidential if the circuit is analyzed using FA equipment, for example by a FIB. As the offline charge detection does not require a power supply to detect charge, it is a promising approach for this task.

Integrating the offline charge detection circuit with a security sensitive IC is not possible within this work. Security sensitive IC hardware is designed and fabricated with very strict limitations on the amount of information available to the public. Even for non-security hardware, integration of a system critical part into existing concepts is only performed if sufficient economical motivation is present. The present work is in a research state and consequently, vendors are skeptic about the economical benefits. Even though vendors signaled interest it was not possible to implement the charge detection within a functional security IC. Instead, the implementation of the offline charge detection circuit is performed on a simple test chip without security relevant functions. Aspects of combining the presented design with cryptographic functionality is accounted for.

Figure 6.18 shows two exemplary transfer characteristics of the offline charge detection circuit. The transfer characteristics is used to derive the threshold voltage V_{TH} of the transistor (see Equation 4.1 on page 46) as shown in the figure. First, the point of maximum transconductance g_{m} is determined. The characteristic at this point is extrapolated linearly to $I_{\mathrm{D}} = 0\,\mathrm{A}$, which is taken as threshold voltage. Other means of threshold voltage determination are possible but are not employed in this work. The threshold voltage is a measure for the amount of charge on the floating

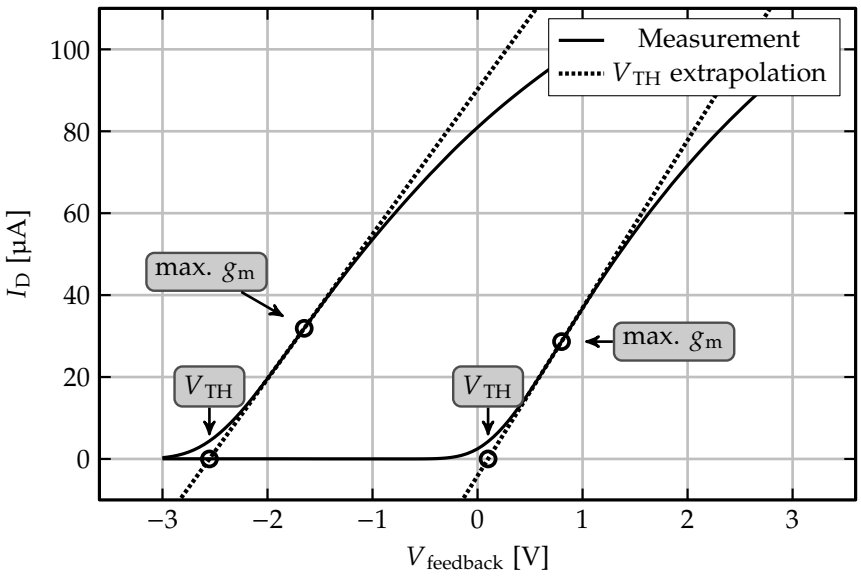


Figure 6.18: Transfer characteristics from two different cells of the offline charge detection circuit.

gate. It is transformed into the amount of changed charge using Equation 5.12 on page 69. As the initial amount of charge on a freshly fabricated cell is determined by process parameters and is at least in part random, the relative value should be considered. For this purpose, the charge amounts for different cells are compared before and after the experiment.

The experiment is designed similar to the way a potential attacker would compromise an IC. A normal FIB work flow integrates the preparation, the navigation and the CE phases. An attacker would follow this procedure, at least in parts, too. Figure 6.19 shows the three steps with correlating influences. Decapsulation usually works on the whole die area, often with chemical or mechanical means. The navigation phase starts by placing the circuit into the vacuum chamber and using the ion beam to navigate to the site of interest. During this step, the ion beam only scans parts of the die, though the scanned area usually is as large as several hundred micro meters in diameter. The influence from the ion beam is kept low in this phase to prevent too much degradation of the sample. Once the site of interest is localized, the ion beam performs the desired operation on very small areas. This last step has the highest influence on the target device but is targeted to the smallest area.

Two possible approaches to detecting the attacker in this work flow are: 1. during navigation with a few very sensitive charge detectors, or 2. during CE with very many distributed charge detectors. The charge detector must be integrated into the cryptographic chain of the secret information to be effective, see Section 2.6 and also 6.5 for a discussion. Accordingly, the infrastructure to accommodate this is relatively complex and much larger than the charge sensor itself. Placing many distributed charge sensors on an integrated circuit might become ineffective due to

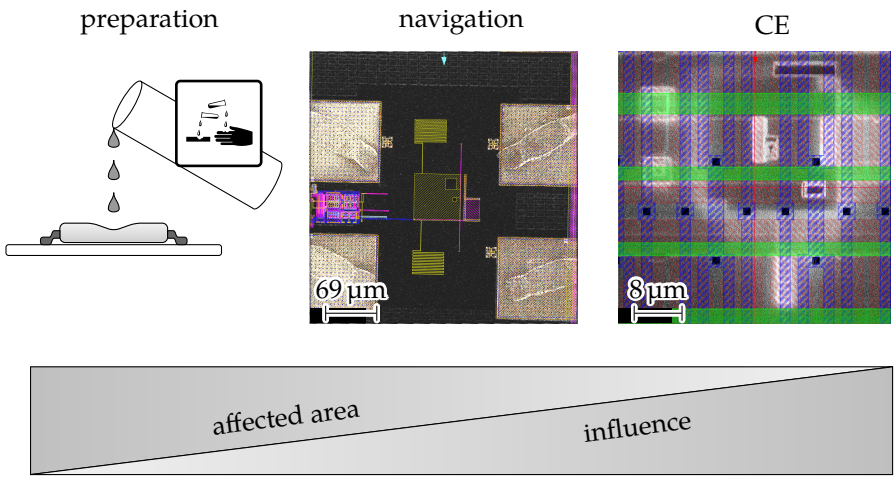


Figure 6.19: Influences from a possible FIB attack on an IC with correspondingly affected die area. The actual CE task only applies the FIB influence to a very small area whereas the navigation task uses the FIB on a larger area with much less intense beam settings. [117] The electronic version of this document contains colored layout information.

this infrastructure requirement. The detection of FIB application to the IC is best accomplished with a few sensitive charge detectors distributed equally across the die. By this, the attacker will very likely hit the charge detectors sensitive area during the navigation phase and render the secret information irrecoverable.

To show the effectiveness of the charge detector circuit, the FIB is applied to the test structure in a way similar to the process of navigation. A single scan of the ion beam with relatively large area (355 µm × 355 µm) and low beam density (20 pA), just enough for navigation, is performed. The amount of charge stored in the charge sensor is then compared before the FIB scan and after the FIB scan, both times outside of the vacuum chamber, see Figure 6.20. Additionally to the FIB irradiation (top left graph), the device is heated to 200 °C for two hours (top center graph) and stored at room temperature for eleven days (top right graph). These additional steps are performed to evaluate the resistance of the FIB detector against such measures as an attacker would try to circumvent the protection. As charge trapped in solid materials can be removed at elevated temperatures, the attacker could wish to reset the device to the original state by heating.

The charge amounts of the 18 realized cells of varying configuration are shown in Figure 6.20 for the three steps of the experiment. Two devices are shown: the upper three plots are from a device subject to FIB irradiation and the lower two plots are from a reference device which is not exposed to FIB irradiation. All charge amounts are recorded relative to the *initial* charge amount as measured on the fresh device. For a reliable function as a FIB detector, the upper row of graphs should always show a significant value, corresponding to a permanent and safe detection of the application of the FIB tool. The device shown on the lower row of graphs is not exposed to FIB

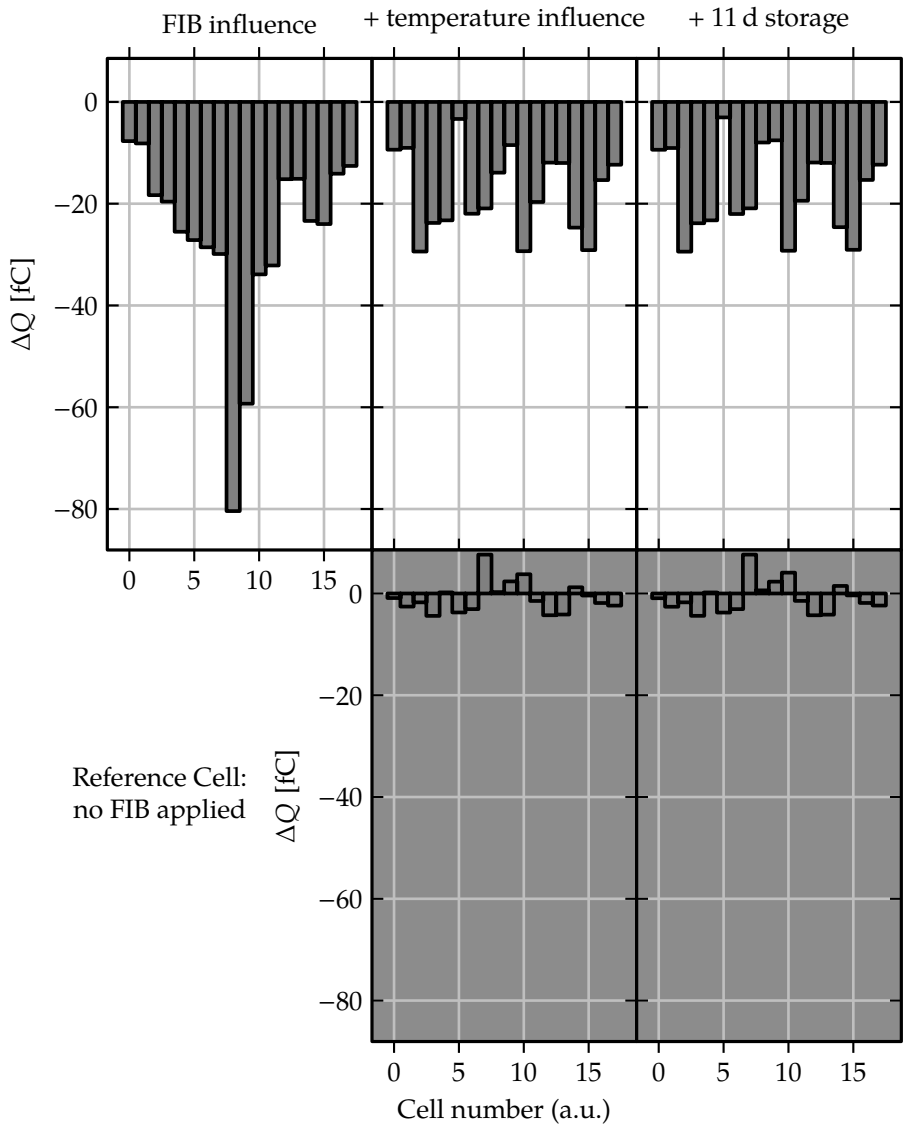


Figure 6.20: Influence of the FIB to the state of the offline charge detection. One device is subjected to FIB irradiation (top graphs), another is not (bottom graphs). For a next design step, a suitable cell type can be chosen and implemented into a security IC.

irradiation and thus should not show a signal. Cells with a change of charge in the lower row would be equal to false positives where the FIB detector renders the secret information unusable even though no FIB is applied. As can be seen in Figure 6.20, the application of the FIB is possible with a low false positive rate. According to the graphs, the results from cells 2, 10, 14 or 15 suggest that they fulfill the requirements: The irradiated device shows a strong signal, which can not be recovered with the approach of heating and, at the same time, the signal from a cells of a non-irradiated device is very weak.

From these results, the utilization of the offline charge sensor as a FIB detector is possible. As the integration into an IC work flow is impossible, the experiments can only suggest directions for further research. For a system integration, additional points must be considered. The placement of charge sensors and antennas should be equally distributed around the nodes requiring protection. Integrating this placement procedure into an existing (automated) design flow would be required for successful roll out of this sensor. Furthermore, the secret information (e.g. encryption key) must be intrinsically connected to the amount of charge on the FIB detector. This could be achieved by deriving the secret key from the charge amount and then using this secret key for encrypting the data stored in a NVM. Once the charge amount changes, the secret key would be irrevocably lost. This functionality is similar to that of a physically unclonable function (PUF), where secret key material is derived from material and instance properties [110, 119, 144].

An important aspect for PUF implementations is the inability of the attacker to predict the PUF characteristic. Analysis of the PUF should be impossible without destroying the PUF's characteristic, i.e. no non-destructive analysis means exist for an attacker. With the charge sensor, the same must hold true. Thus, the precise information about the amount of charge in the sensors must not be detectable without using a FIB. If a FIB is required for this task, the information would again be lost once the attacker tries to figure out the charge states. Careful designing the antenna structures in a way that does not allow external measurement of the charge amount with sufficient detail, e.g. by capacitive AFM, would be required.

The suggested charge sensor implementation and the shown results on the offline charge sensor as a FIB detector have been discussed for frontside attacks, only. Yet, in recent years, backside approaches – as are part of every day FA tasks – are also coming into reach for attacks on security relevant ICs [120, 141, 148]. In order to conduct probing attacks from the backside, a FIB work flow is required [142]. It has not been tested within the course of this work, if the suggested charge sensor design is capable of detecting backside FIB applications. As the sensitivity of the charge sensor is so enormous, chances are that careful design can allow for a backside FIB detector. In the next section, a backside approach to attacking security relevant ICs is presented which uses a FIB tool. Though the charge sensor itself is not in connection with that, charges still play an important role within the shown experiments.

6.4 Charges in Security

The nature of charge can not only be used to prevent access to the secret information inside an IC (see Section 6.3) but can also be used to gain this information. For example, NVM devices can be read out using a charge sensitive technique [100, 101]. This is done by backside preparation of the IC [86]: The silicon semiconductor bulk material is removed in large parts, leaving only a very thin layer of active devices. As the access is done from the backside, the interconnect metal stack stays intact. This makes preparation possible for allowing access to every circuit node [104] while the device is kept fully intact and functional. In order to read NVM data from the backside, capacitive AFM can be used on the thinned sample as for example shown in [101]: Using chemical etchants, the silicon is removed and subsequently, the AFM analysis is carried out. Due to difficult process control of this approach, the location where the final thickness is satisfying and the analysis can be done, is not under control of the operator, according to [101]. If, in contrast a FIB system is used to remove the silicon from the backside, localized thin trenches can be created with only several tens or hundreds of nanometers of silicon left [95] and with precise control of their location. In both cases, the charge on the floating gate of the flash cells is reflected by the semiconductor field on the back surface, see also Section 2.4. Accordingly, the (possibly secret) data can be read using a field probe, for example capacitive AFM [101] or electron beam prober [109]. The same effect can also be evaluated using a FIB tool, allowing for in-situ monitoring [142]: The SE emission yield, as already pointed out in Section 6.2, depends on the surface potential of the targeted material. As the surface potential of both, insulator and semiconductor, reflects the electrical potential of near-by conductors, the FIB image brightness contains the data stored in the NVM cells. The results from [142] are presented.

A proof-of-concept device is chosen to analyze the attack performance, in this case an `ATMega328p` from Atmel Corporation [133]. “Fuse bits” are individual, non-volatile configuration storage cells that are often used for enabling certain functions or storing device configuration data. The fuse bits within this device are implemented to protect the reading of the on-die flash and electrically erasable programmable read only memory (EEPROM) through the debugging and programming interface of the device. A device or assembly vendor would program the fuse bits accordingly after the NVM has been configured. This protects the program code from analysis and read out through the normal programming interface. The logic of the device ensures that the protection fuse bits are only cleared (to again allow reading of memories) if the memories were previously erased safely. Thus, the memory contents are protected from simple readout through the debugging and programming interface. An alternative implementation could store secret key material in the fuse bits and accordingly encrypt all memories with this key. Again, reading the memory contents would yield the contained data only encrypted (i.e. useless to the attacker). The fuse bits would then also require protection. In both cases, the situation for an attacker equipped with a FIB is “beneficial” as the backside observation and editing of ICs

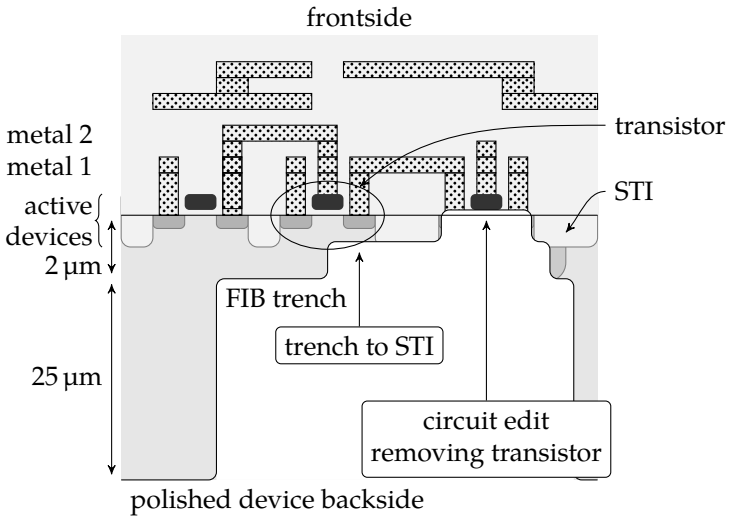


Figure 6.21: Backside circuit access is performed by a number of different polishing steps, mechanically to 25 µm and with a FIB to 2 µm remaining silicon thickness. The CE tasks are then performed on locally thinned area with only several hundreds of nanometers left.

enables to access data from such an implementation.

The device is globally thinned using chemical and mechanical means down to approximately 25 µm of remaining silicon. A second polishing step is performed with the FIB system on parts of the device using xenon difluoride (XeF_2) support. The concept of backside preparation using a FIB is shown in Figure 6.21. The FIB polishing (trenching) is stopped once the wells are identified in the SE image ("FIB trench"). Often, the size of the FIB trench is in the order of 100 µm × 100 µm to 300 µm × 300 µm, allowing for access to many nearby circuit nodes [104]. At this stage, the remaining silicon thickness is below 2 µm in the FIB trench. Figure 6.21 shows a schematic view on the individual polishing steps. Two situations are discussed within this section: performing CE on this backside with respect to security ICs and data ex-filtration by the back-surface potential. For CE operations, the device is locally further thinned to shallow trench isolation (STI), which leaves 200 nm…300 nm remaining silicon thickness, depending on technology. On this "trench to STI", every circuit node can be accessed [126]. Logical waveform data can then be obtained for example by probing transistors or metal lines. If the signal is sufficiently strong, it can also be picked up earlier in the preparation process. As the semiconductor permits the entry of electrical field to a certain degree (see Section 2.4), the potential is not only visible on the STI backside [103] but also on the backside silicon, which is shown here.

Figure 6.22 shows the image acquired on the FIB trench of roughly 2 µm remaining silicon thickness. The area in the image consists of the fuse bit circuitry, where 8 such fuse bits are within the FOV. The left image is acquired as the wells became apparent (i.e. the preparation endpoint condition), the middle image is a contrast

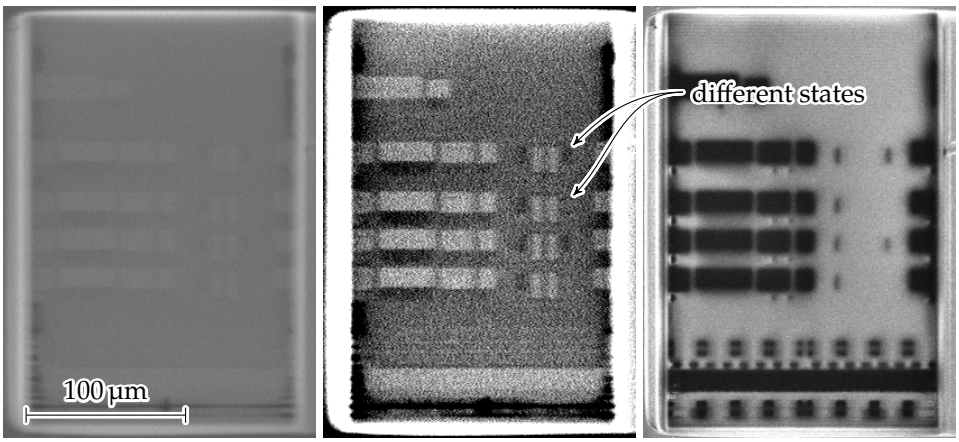


Figure 6.22: Observed fuse bit state using the FIB SE image [142], unpowered device (left), enhanced contrast version (middle) and on the powered-up device (right).

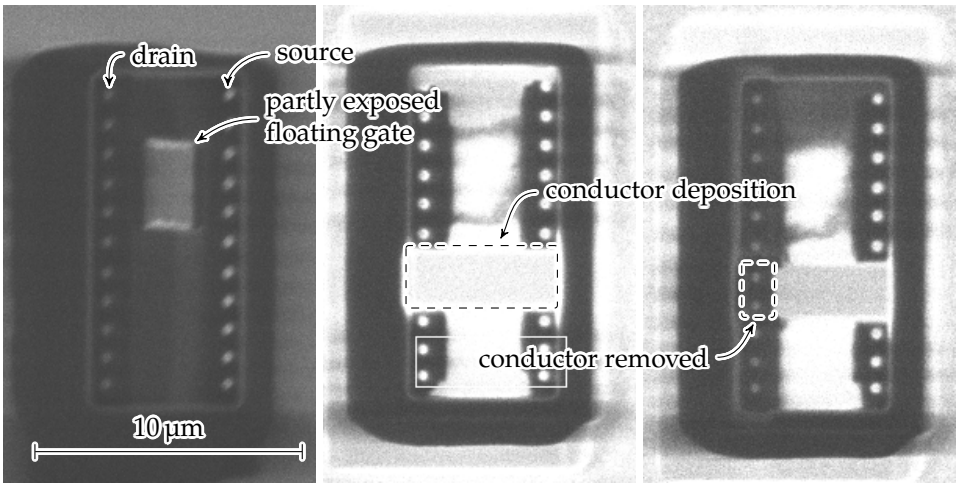


Figure 6.23: Performing a FIB CE on the backside prepared fuse bit structure, setting it to arbitrary values. [142]

enhanced version of the left image. The right image finally shows the same trench at the same preparation thickness but when the device is powered with nominal supply voltage. With the power supply voltage turned on, the well contrast becomes significantly stronger as the potential difference is increased by the power supply. Yet, already with the left and middle images, the wells are clearly visible and they even show irregularities. As all fuse bits are likely of the exact same layout (optical images of the devices support this assumption), the different gray values in the irregular structure from Figure 6.22 must be attributed to the data stored within the fuse bit. The SEs emitted from the surface on the incident ion beam are partially recollected, depending on the surface potential of the device. Accordingly, the fuse bit state, which is propagated to the surface is reflected by the image brightness.

Reading the fuse bit is only helpful if the data stored contains secret material

(e.g. private key material). If instead, the fuse bit is used to configure the device for access restriction on a logical level, the attacker needs to *change* the fuse bit state. In order to achieve this, the attacker first identifies the fuse bits (e.g. from the pattern of the data) using the FIB. The transistor storing the information (i.e. the one with data dependent back-surface contrast) is selected and milled away until the drain and source contacts are visible. This roughly corresponds to the "removed transistor" from the schematic view in Figure 6.21. At this stage, the fuse bit is set or cleared, depending on implementation, see the left image in Figure 6.23. The device is powered up during the acquisition of this image. The two contact rows for drain and source of the transistor are differing in brightness significantly, showing that the connection from the fuse bit transistor is broken up. To enforce the opposite state, the transistor is replaced by a conductor deposited by the FIB (middle image of Figure 6.23), resulting in equal brightnesses for the contacts of drain and source. The procedure of setting and resetting the fuse bit state by adding and removing the conductor can be carried out multiple times (right image). If the edited fuse bit controls the access methods through the normal device programming interface, the attacker can read-out all memories after using the FIB.

The two possible fuse bit usages must both be considered insecure. An attacker equipped with a FIB system is enabled to read secret key material if the fuse bits store these data, and to modify the state of any transistor if the transistor protects against attacks. In the same way, also the contents of other memory types can be configured permanently. For example the contents stored in an SRAM is normally configured by software (i.e. as temporary data storage). Yet, by removing individual transistors, the contents can be fixed to represent a certain state, as has been shown in [141]. The next section will discuss the SRAM in more detail, where the free configuration possibilities of an SRAM are fatal, too.

The specialty of the presented approach is the detection of faint signals through the use of a field sensitive measurement using charge and the precise modification of a device on a small scale. Both applications of charge result in a disastrous situation for the security of possible hardware implemented security ICs. A need for improving this situation is addressed by physically unclonable function (PUF). These circuit building blocks promise device individual keys that can not be characterized from the outside. Thus, secret data encrypted with these keys can not be reconstructed without co-operation of the circuit, see also the discussion in Section 2.6. Accordingly, "perfect secrecy" seems reachable. Unfortunately, to date, there is no such thing as a physically *unclonable* function. Instead, many very sensitive techniques exist for the characterization of circuit building blocks resembling a PUF, practically allowing to clone any PUF. The next section will show, that also during the characterization of PUFs, charges play a significant role.

6.5 Charges in PUF Characterization

The security of ICs significantly depends on the capabilities of the individual device to protect against outside analysis attacks, see Section 2.6. Many attacks show, that wiretapping on data is possible through different channels [78, 83, 127]. This directly limits the implementation capabilities of security devices [88, 106]. Consequently, new ideas about protection are suggested, for example different constructions using shields and meshes, placing transistors carrying sensitive information at special locations or different types of coatings or sensors to detect the application of malicious techniques. Section 6.3 already shows a means to successfully protect against focused ion beam (FIB) attacks. The principle is a sensor design which is implemented into the data flow of the cryptographic operation. At least parts of the secret key used for encryption must be derived from the (analog) sensor state. The sensor is required for operation and disabling it makes the device non-functional. Altering the sensor state alters the secret key data, making the encrypted data irrecoverable.

Section 6.4 shows that data stored in NVM requires additional protection means. A FIB can be used to analyze the data through the back-surface potential or modify it through the alteration of the circuit. Accordingly, this situation has been addressed by a number of concepts, where the concept of the physically unclonable function (PUF) is discussed here. A PUF connects the physical instance of a device to the logical behavior through using suitable circuit blocks.

An example of a circuit often used as a PUF is the static random access memory (SRAM) [107, 118]. The state of the bits after powering up an SRAM depends on the specific process variations during production. The actual pattern that is present as data is device dependent. SRAMs are implemented into every logic device for temporary data storage. This property makes the application of the SRAM as a PUF economically attractive. Different vendors use such a PUF today [149, 157]. This chapter describes the means that allow to characterize an SRAM PUF and subsequently to duplicate this type of PUF. Characterization builds on the Seebeck effect, and duplication on the modification of a circuit by a FIB, similar to Section 6.4.

A conductor subject to a temperature gradient causes the transportation of charge carriers along this gradient. The transport of the carriers yields a current which charges up the two ends of the conductor. The resistive conductivity of the conductor limits the maximum voltage that is achieved between the two conductors. A static condition between charge displacement from the temperature gradient and the resistive conduction according to Ohm's law is established. This effect is known as the "thermo-electric effect" or "Seebeck effect" [4, 14, 130]. The static voltage V_{Seebeck} can be modeled proportionally to the temperature difference ΔT_{abs}, i.e.

$$V_{\text{Seebeck}} = \Delta T_{\text{abs}} \alpha_{\text{Seebeck}} \tag{6.1}$$

with α_{Seebeck} as the Seebeck coefficient. As the measurement equipment to observe such a voltage must form a closed electrical loop between the two points of measure-

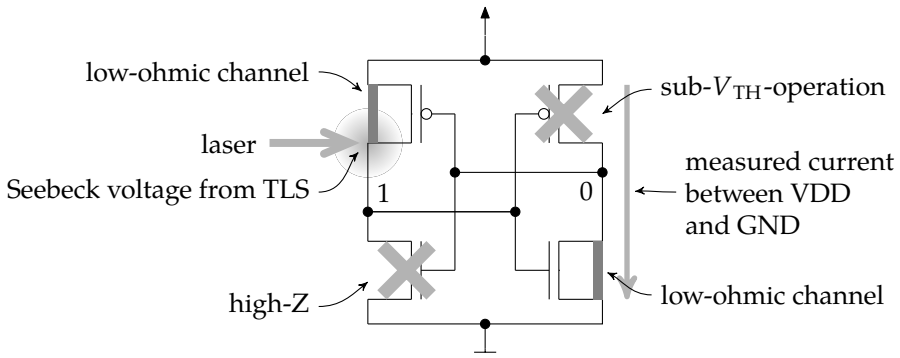


Figure 6.24: Schematic of an SRAM cell subject to a Seebeck voltage generated by a temperature gradient [145].

ment, the temperature gradient compensates within all conductors. Only if different types of conductors are used, a net voltage is observed. In a closed loop, Equation 6.1 causes the Seebeck voltage to compensate if α_{Seebeck} is equal for all conductive parts of the loop. For different α_{Seebeck} coefficients, the closed loop allows to observe a voltage proportional to the difference between the Seebeck coefficients.

In an IC, the transport of carriers causes a current. Additionally, if the carrier concentration varies, electrical fields are generated. The semiconductor material can exhibit changes in conductivity, see Section 2.4 and 4.1.3. If the carrier transport is directed to or from a MOS transistor gate, the mirror charge in the channel is varied and can cause additional current – an amplification is observed.

The temperature gradient can be created in an IC by the use of a laser beam. This technique is called thermal laser stimulation (TLS) in failure analysis (FA) [87, 91]. The laser spot is directed towards the sample from frontside or backside of the IC. A terminal of the IC is measured for varying voltage or current. If the temperature gradient is part of this measurement loop and the Seebeck voltages do not compensate, the measurement equipment shows a voltage or current amplitude. The laser spot is scanned over the device. The position is translated to an image position and the amplitude recording is translated to the brightness of the image at that location. This scanning technique results in an image where bright and dark spots correspond to positive or negative amplitude of the device if heated by the laser at the specific position.

The TLS technique allows for data ex-filtration by observing the power supply current of the IC. In order to observe the charge transportation from the temperature gradient on the power supply terminal, additional conditions must be met. The Seebeck effect must cause charge alteration on the gate of MOS transistors, as pointed out above, to alter the current consumption of the affected transistor. In order for this charge alteration to be effective, the Seebeck voltage has to be introduced into terminals of transistors that are in on state. Increased or decreased power consumption can then be analyzed from the power supply current. The construction of complementary metal oxide semiconductor (CMOS) circuits intrinsically provides for this behavior:

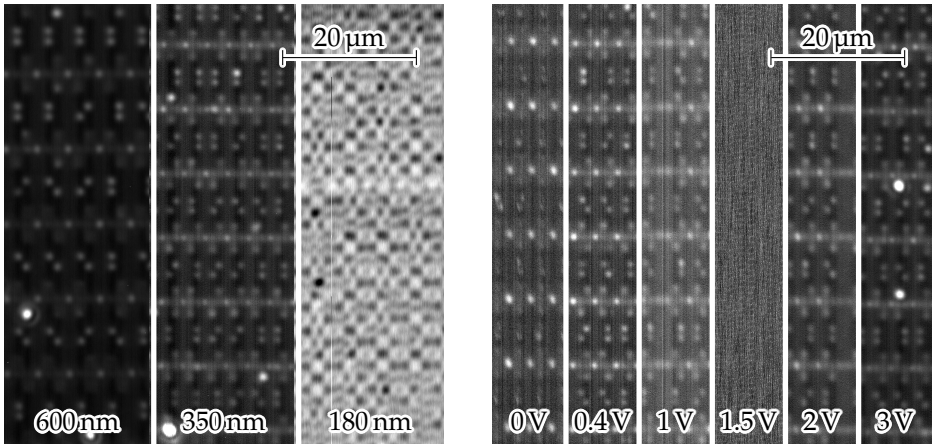


Figure 6.25: Supply current intensity pattern observed from TLS on a powered up SRAM device [145].

Considering an inverter, only a single transistor in the direct path between power supply and ground is in off state. If the charge on the gate terminal of this transistor is varied, the transistor drain current (i.e. the current in the channel) will vary weakly, too. Accordingly, this variation is reflected by the power supply current of the IC. This principle holds for all types of CMOS gates at least in a subset of possible input states.

Figure 6.24 shows a 6-T SRAM cell, where the effect from a Seebeck voltage generation is illustrated in more detail. If the circuit is supplied with a power supply, the output voltage of the two inverters are of opposite value and the circuit is stable. Accordingly, either one transistor of the two transistor pairs is on, the other is off, as marked in Figure 6.24. Localized heating of individual parts of the device can cause the generation of Seebeck voltages in the corresponding device terminal. The generated Seebeck voltage applies the charges to the gate of subsequent transistors if the transistor subject to heating is in the on state. In subsequent transistors in off state, the presented Seebeck voltage changes the current conducted by this transistor and the whole circuit in general. By this path, the effect of the Seebeck voltage from localized heating of the device can be transported to the terminals of the IC. This path is only available at locations, where the heated transistor is in the “on” state, allowing to derive the state if the presence of a transistor is given.

Figure 6.25 shows the resulting power consumption pattern obtained from different SRAM devices and at varying supply voltages. The layout of the SRAM is a very regular structure. The pattern from the results show a clear irregularity, which is dependent on the data stored in the SRAM. Reconstructing the data is possible from within the analysis result, at all voltages, even down to significantly below the supply voltage, see for example the part of 0.4 V.

As the alteration of the supply current (which is monitored) from the Seebeck voltage is very weak, a high amplification is required. Consequently, distortions of the

supply current by running logic hinders the measurement of this signal, see the 1.5 V part of Figure 6.25. Yet, it is possible to operate security ICs on such a low voltage, that the CMOS logic can not perform switching but the SRAM state is observable through the TLS approach [148]. This allows for an easy and full characterization of SRAM PUFs. The device is powered up to a voltage where the CMOS logic is non-functional but the SRAM already settles into the startup state. Subsequently, the data stored in the SRAM is the PUF response and can be analyzed by the TLS technique. The PUF behavior can be mathematically modeled or physically programmed into a second instance of the PUF [141]. Limitations to this technique are imposed if the SRAM is separated from the power supply by an additional transistor or when the heating by the laser beam does not allow for individually creating Seebeck voltages in the transistors. The latter is the case for too small dimensions of the SRAM cells. Using modern laser FA techniques such as solid immersion lens (SIL) imaging, the resolution limit for this attack should not prevent success above 60 nm of technology design size.

Creating physical clones of SRAM PUFs in the same form factor as the original is a valid attack scenario. By duplicating the physical behavior of the SRAM, an attacker is not required to understand (i.e. reverse engineer) the encryption algorithm and functionality of the circuit in total. Instead, it suffices to duplicate the SRAM behavior into a second instance of the same IC. The modification of fuse bits as shown in Section 6.4 can also be applied to SRAMs, enabling this procedure. In [141], the SRAM is successfully trimmed to show the programmed startup state and can still hold both states during normal operation.

Analyzing these results is possible with respect to charge. The Seebeck effect is exploited, which causes a charge *movement*. Due to the temperature difference, the charge carriers within the conductor are transported. As the conductor has a high carrier concentration, there is no limit at which the transportation stops, except for the, reversely directed, electronic conduction. The result is a steady voltage across the conductor, according to the ohmic law. The attacker has an unlimited supply of carriers to analyze the PUF with the laser technique, making the analysis successful in all situations. In order to prevent against an attacker, different suggestions are given: Stopping the SRAM supply current from reaching the attacker through the power terminals of the IC can be performed by a transistor integrated into the power supply path [115]. Alternatively, the response information of the PUF can be determined on a different way. For example comparing individual cells within an SRAM with respect to their drive strength allows for such an approach [155]. In the latter case, to acquire the response requires the successful coordination of the various signals within the SRAM: In order to compare two cells, their output signals must be connected together, for example through the simultaneous assertion of both of their wordlines. In this case, the amount of charge available to the attacker for analysis would be limited by the capacitances of the bitlines during the operation.

Even with the previous improvement in mind, the realization of a PUF by use of an SRAM is impossible. Though characterization using various semi-invasive

means can be made impractical, the PUF characteristic can be analyzed with fully-invasive attacks. This is possible, because the SRAM PUF response is a result of the static properties of the physical circuit. In the case of the SRAM, the threshold voltages of the individual transistors and the capacitive loads of the gates determine the startup value. Consequently, the main goal for an invasive attacker is to preserve these properties while still wiretapping on the PUF response, possibly by driving the SRAM interface bus directly. In order to improve this situation, a very sensitive property must also influence the PUF response, very similar to the charge amount in the FIB detector from Section 6.3. Yet, this property must be well hidden from the outside attacker and must not be characterizable, as identified in Section 6.3 already.

Charge can be used for this purpose. Sensitive charge measurement is available on CMOS devices in form of a FET. The influence from various interaction media also affects charge: FIB irradiation, scanning electron microscopy (SEM) irradiation and ultra violet (UV) light all can cause charges to alter the logical states. Future concepts for PUF design must consider the nature of their connections and interaction with the surrounding. The concept could build on very small amounts of charge that are severely altered by any of the various invasive and semi-invasive analysis techniques. Limiting the amount of information an attacker has for analysis is a key task in PUF design. Charge can resemble a promising way in this context.

Chapter 7

Conclusion and Summary

Failure analysis (FA) and security analysis of integrated circuits (ICs) are regularly confronted with the analysis of very weak electrical signals. A number of techniques exist that allow for this analysis, for example frequency analysis, lock-in amplification of signals and preamplifier circuits for pico-ampere meters. This work investigates the use of charge measurement techniques to improve the sensitivity in IC analysis in the contexts of FA and security ICs.

A charge measurement device ("charge sensor") is constructed and fabricated in a 0.25 µm bipolar complementary metal oxide semiconductor (BiCMOS) technology in two variations: A closed loop feedback implementation allows for in-situ monitoring of charges. An offline charge detection circuit can observe charges applied during unpowered periods of the charge sensor. The functionality of the charge sensor is derived theoretically and the corresponding implementations are verified by showing the designed behavior in practice. This includes the verification of the charge measurement itself as well as the coupling of the desired charges to the charge sensor through adequate probes. The closed loop feedback circuit is implemented for measuring charges with a sensitivity of 137 aC/mV to 137 fC/mV whereas the offline charge detection circuit can analyze charges from 125 fC upwards.

The closed loop feedback implementation is used to in-situ monitor the charging in focused ion beam (FIB) processes on ICs during circuit edit (CE) tasks. The FIB is shown to exhibit positive surface charging by ion neutralization. An emission of 2.2 secondary electrons (SEs) per incident ion is measured for the insulating surface of the charge sensor IC. Additional charging effects of the FIB column in the range of tens of atto amperes are observed while the ion beam is blanked. High voltages in the FIB chamber and the extraction process of ions are investigated, yet a definite source for these charging effects can not be finally isolated. The charge sensor allows for analysis of very weak charging currents: A noise floor of 40 aA root mean square (RMS) and 5.1 aA offset is observed.

Two different dielectric test structures are connected to the closed loop feedback implementation of the charge sensor. Different setups are presented to connect the test structures to the charge sensor: by design placing both parts onto the same IC and

after manufacturing by bonding the test structure IC to the charge sensor IC. The stress test structures show a leakage behavior that amounts to a charge accumulation in the charge sensor device. Equivalent currents are derived from the charge measurements, with a noise level as low as 0.23 aA RMS in one case and 84 aA in the other case. Not all investigated dielectrics exhibit a constant leakage current during the recording of the charge traces: One dielectric has a slightly decaying current, another dielectric showed steps in the charge, suggesting current spikes, a third dielectric showed a constant equivalent current. With the charge sensor measurement, the current value observed during measurement can directly scale the sensitivity of the charge measurement. This allows for a very flexible analysis even when the precise current level to be expected is unknown. The mechanism for the dielectric behavior could be investigated with the charge sensor in future researches.

A FIB detection circuit is presented that can protect an IC from unauthorized access using a FIB. The implemented circuit requires a small die area of only 18 µm × 9.1 µm and between 6 µm × 6 µm and 18 µm × 18 µm of top metal area for the antenna. Irradiation of the device with a FIB already shows a severe alteration of the device state when only navigational steps are performed: Between 30 fC…80 fC of charge are measured with the offline charge detector. This allows for protecting the circuit by placing a limited amount of such detectors distributed over the whole IC already. The design and implementation are shown such that disabling the circuit renders the contained information unrecoverable. An attacker can not revert the state to the initial value even when heating the device. The measured results suggest that implementing the FIB detector into a security IC is feasible and beneficial.

The presented offline charge detector protects an IC against frontside FIB modifications, yet backside FIB preparations are an increasingly dangerous attack vector. It is shown that using a FIB for investigating the passive and active voltage contrast of the silicon back-surface on a security IC can severely affect the robustness of the implementation against fully invasive attackers. The analysis techniques available can be better understood if circuits are analyzed on a basis of charge. It is shown that an attacker can observe charges and yield useful information but also that the IC designer can use charge as a means to protect the circuit.

The presentation of the charge investigations in this work show that IC analysis can significantly be improved when considering charges. Once the measurement system is setup for extending the sensitivity by charge sensing, new opportunities for investigations are opened up. Future research can build on the results of this work to improve the analysis capabilities in IC FA and security IC design.

Acknowledgment

I want to thank my supervisor, Prof. Dr. Christian Boit, for his continuous support and encouragement. The fruitful discussions we had over the last five years always were a source of new insights and ideas to me, and your open mindedness in our conversations made the work as a PhD student very enjoyable.

It was always a pleasure to discuss various topics with Prof. Dr. Roland Thewes. Thank you for helpful ideas and suggestions regarding possible enhancements. I would like to thank Prof. Dr. Heinrich Neitzert for the chats we had over the years and for being part of my examination committee. Prof. Peter Jacob bestowed on me further insights into the various natures of charge, especially at high voltages.

Without the support from Alexander Fox and Prof. Dr. Bernd Tillack (both IHP, Frankfurt/Oder), the present work could not have been realized. Thanks to Ulrike Kindereit for initiating this connection. I enjoyed many productive discussions with Dr. Ted Lundquist from DCG Systems, Inc., about focused ion beam (FIB) topics. DCG Systems' support for our FIB system is gratefully acknowledged.

It was a pleasure to be part of the team of the Semiconductor Devices group at TU Berlin. Thanks to Andreas Eckert for the many samples you prepared for me and to Helmut Wegner for the help with experimental setups. René Hartman bonded my device into whatever package I gave him, thank you! Thanks to Rudolf Schlangen for introducing me into failure analysis (FA) and FIB work, which led to the conduction of this work. It was always a pleasure to coordinate and teach students together with Philipp Scholz, Norbert Herfurth and Anne Beyreuther. Thanks to the support of the whole group, I was finally able to take the time at the library and write up this thesis. We will have to celebrate this with another round of ice skating!

My fellowship in the Helmholtz Research School on Security Technologies was initiated thanks to Christian Boit. This allowed me to network with researchers of different disciplines, resulting in the interdisciplinary character of this thesis. Prof. Dr. Jean-Pierre Seifert and his PhD students Dmitry Nedospasov and Shahin Tajik were a significant support to me by motivation, good criticism and co-operation – at day and during nights before paper submission!

The investigative attitude towards many problems is a gift of education. I want to say, "Thank you," to my parents Dr. Angelika and Dr. Heinrich Helfmeier for raising me the way they did. You were never tired in devotedly supporting me and in making me to what I am – even in contemplation of death. A PhD thesis is taking lots of room in ones life, and I am happy to have met my girlfriend Sarah Fügener, who supported my in all aspects of living and working.

Appendix A

IHP Technology Tunneling Properties

Test structures are available to derive the tunneling properties from the technology. Using these measurements, the creation of a tunneling model according to the parameters is possible. The properties for the gate dielectric and the insulator between the two polysilicon layers (poly insulator poly (PIP) capacitance) as well as the metal insulator metal (MIM) capacitor insulator are measured. Figure A.1a shows the resulting traces for the gate dielectric and dielectric between the two polysilicon layer in a Fowler Nordheim plot and Figure A.1b shows the corresponding plot for the MIM capacitor using the reverse of the Poole Frenkel tunneling characteristic. All tunneling currents are approximated by a least mean square (LMS) algorithm and shown dotted in the graphs. The resulting coefficients are shown in Table A.1.

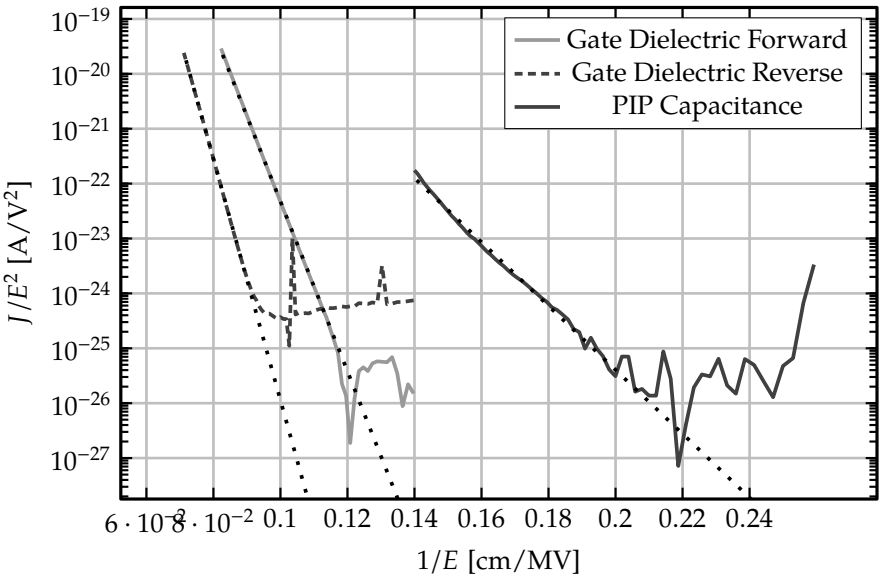
Fowler Nordheim: $J = aE^2 \exp\left(-\frac{b}{E}\right)$

Dielectric	a [A/V^2]	b [V/m]
Gate Dielectric Forward	$1.07 \cdot 10^{-4}$	$5.06 \cdot 10^{10}$
Gate Dielectric Reverse	$1.41 \cdot 10^{-7}$	$3.56 \cdot 10^{10}$
PIP	$1.78 \cdot 10^{-14}$	$1.34 \cdot 10^{10}$

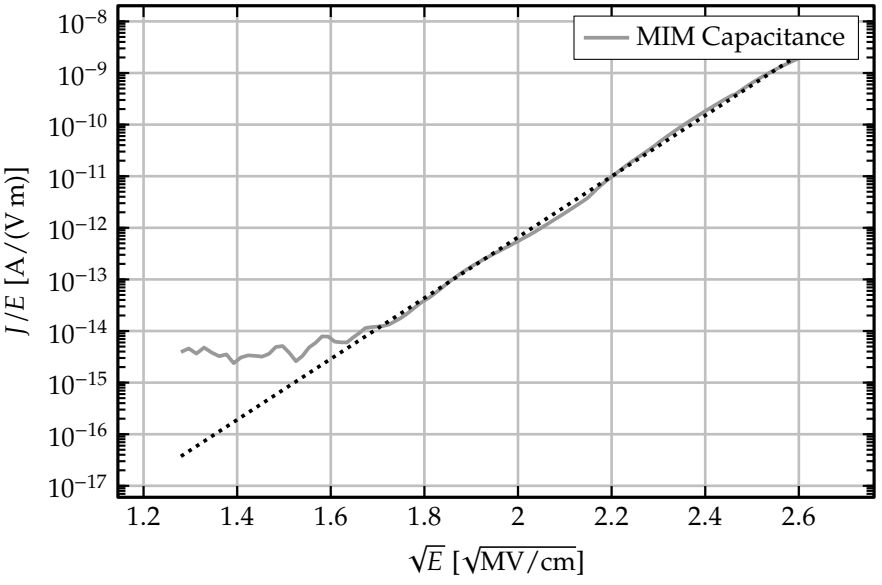
Poole Frankel: $J = cE \exp\left(d\sqrt{E}\right)$

Dielectric	c [A m/V]	d [$\sqrt{\text{m/V}}$]
MIM	$1.06 \cdot 10^{-24}$	$1.36 \cdot 10^{-3}$

Table A.1: Tunneling model coefficients derived by LMS approximation for gate, PIP and MIM dielectrics of the BiCMOS technology used for simulations.



(a) Fowler Nordheim Tunneling



(b) Poole Frankel Tunneling

Figure A.1: The tunneling behavior of the gate and PIP dielectric are measured with conventional means and plotted here according to the Fowler-Nordheim (FN) tunneling (Figure A.1a). The MIM dielectric is plotted according to Poole-Frenkel (PF) tunneling (Figure A.1b). LMS approximations are shown in dotted with the coefficients from Table A.1.

Appendix B

Octave Script for Simulation of Tunneling Current in Capacitive Voltage Dividers

For FN tunneling, the following function is used:

```
% Units: [A/m^2] = [V/m] [A/V^2] [V/m]
function J = fn(E, a, b)
 J = a.*E.^2.*exp(-b./E);
end
```

For the MIM capacitance, the function implements the PF tunneling characteristic:

```
% Units: [A/m^2] = [V/m] [Am/V] [sqrt(V/m)]
function J = pf(E, a, b)
 J = a.*E.*exp(b.*sqrt(E));
end
```

The tunneling functions are used in simulating the behavior of a capacitive voltage divider in the `timed_simulation` function:

```
% Units: [s] [] = [V] [F] [F] [s] [C]
function [t, v] = timed_simulation( V, C1, C2, tend=1e2, qinitial=0 )
  % Calculate the resulting voltage traces when capacitive
  % voltage divider with C1 and C2 is subject to input
  % voltage V.
  % Returns time samples t and
  % resulting voltage ratio v [0...1]
  % Implicitly given: tun1 and tun2 as absolute tunneling
  % current values, returning current I [A] from voltage
  % V [V]
  %
```

```
% calculate the initial voltage ratio
v(1,:) = C2 ./ (C1+C2) .* ones( 1, length(V) ) ...
  + qinitial / (C1+C2) ./ V;
t(1) = 0;
t0 = zeros( 1, length(V) );
% the precision to achieve in each timestep
% [relative in terms of ratio]
eps = 1e-4;

% a vector of eps
dv = eps .* ones( 1, length(V) );

% number of steps to calculate at maximum
n = 1e6;

% walk in eps steps through v from start to stationary
% value, each time calculating the time required to
% reach that, based on the current difference,
% and capacitance.
% to determine ts we reverse-calculate the
% time required to transfer eps of voltage
% desired change
qdes = 0.5 * (C1 + C2) .* V .* eps;
for i = [2:n]
  % calculate the amount of current now
  i1 = tun1( V .* (v(i-1,:))); % tun1, tun2 implicitly given
  i2 = tun2( V .* (1 - v(i-1,:)));
  % difference in current
  di = i2 - i1;
  % and calculate the timestep
  % keep in mind:
  %  for multiple input voltages, this is as slow as the
  %  slowest calculation!
  ts = min(qdes ./ abs(di));
  % calculate difference in charge
  dq = di .* ts;
  % the resulting voltage change (relative) is calculated
  % this yields eps at least at one instance of dv
  dv = dq ./ (C1 + C2) ./ V;
  % remember the timestep
  t(i) = t(i-1) + ts;
  % apply the voltage change
  v(i,:) = v(i-1,:) + dv;
  % break conditions
  if (t(i) > tend)
    printf( "Operation stopped because end of time reached.\n" );
    break;
```

```
    end
  end
end
```

Finally, to find the steady state voltage (direct current (DC) operating point), the same function for tunneling characteristic is used but with a different simulation procedure:

```
% Units: [] = [V]
function v = stationary( V )
  % Calculate the stationary ratio of voltage from two
  % capacitors when applying voltage V [V]
  %
  % implicitly given: tun1 and tun2 as tunneling
  % characteristics, functions of V returning I
  % in [V] and [A]
  %

  v = 0.5 * ones( 1, length(V) );
  % as we use bi-section here starting with v=.5
  % we need only log2(1/p) steps to achieve
  % precision p. Every step makes the result
  % twice as precise.
  % using n = 20 gives roughly 1e-6 as precision
  n = 20;

  % iterate through all steps
  for i = [2:n]
    % calculate the currents under the current v
    % condition
    i1 = tun1( V .* (v) );
    i2 = tun2( V .* (1-v) );
    % difference
    di = i2 - i1;
    % determine which way to go and change
    % v according to the current step number
    % as v is initially .5 and i is 2, we
    % get 0.25 as the very first step size,
    % which is just what we want.
    v = v + 1./(2.^i) .* (di > 0) - 1./(2.^i) .* (di < 0);
  end
  % done
end
```

For the calculation of the charge decay on a capacitor, the following `timed_charge` function is used:

```
% Units: [s] [C] = [C] [F] [s]
```

```
function [t, Q] = timed_charge( Q1, C1, tend=1e2)
  % Calculate the resulting charge traces when capacitor C1
  % with tunneling characteristic tun1 is subject to charge Q1.
  % Returns time samples t and
  % resulting charge trace Q
  % Implicitly given: tun1 as absolute tunneling
  % current values, returning current I [A] from voltage
  % V [V]
  %

  % number of steps to calculate at maximum
  n = 1e6;

  % initialize t and Q variables
  Q = zeros(n, length(Q1));
  t = zeros(n, 1);
  % calculate the initial charge
  Q(1,:) = Q1;
  t(1) = 0;

  % the precision to achieve in each timestep
  % relative in terms of charge Q(t)
  eps = 1e-3;

  % walk in eps steps through v from start to stationary
  % value, each time calculating the time required to
  % reach that, based on the current difference,
  % and capacitance.
  for i = [2:n]
    % calculate the current
    i1 = tun1( Q(i-1,:) ./ C1 );
    % and calculate timestep
    % keep in mind:
    %  for multiple input voltages, this is as slow as the
    %  slowest calculation!
    ts = min( Q(i-1,:) .* eps ./ i1 );
    % break condition 1
    if (ts > tend)
      printf( "Simulation finished, no significant change.\n" );
      break;
    end
    % calculate difference in charge
    dq = i1 .* ts;
    % remember the timestep
    t(i) = t(i-1) + ts;
    % apply the charge change
    Q(i,:) = Q(i-1,:) - dq;
```

```
    % additional break conditions
    if (t(i) > tend)
      printf( "Operation stopped because end of time reached.\n" );
      break;
    end
  end
end
```

The graphs in this work are created using the following script. It contains the appropriate constants for the tunneling behavior and the sizes of the capacitances.

```
% the coefficients as derived from
% the measurements, table from Appendix B
x = [
   1.070082e-04 5.059905e+10 5.8e-9
   1.411857e-07 3.562635e+10 5.8e-9
   1.782027e-14 1.340438e+10 21e-9
   1.061053e-24 1.357643e-03 58e-9
];
global a
a = x(:, 1);
global b
b = x(:, 2);
% oxide thicknesses: required due
% to the fact that we have voltage as input
global d
d = x(:, 3);

% define corresponding functions for the
% three tunneling characteristics using these
% coefficients taking V as returning J
% in V and A/m^2
function J = tun_MOS( V )
  global a, global b, global d
  J = sign(V) .* fn( abs(V) / d(2), a(1) .* (V > 0) ...
    + a(2) .* (V < 0), b(1) );
end
function J = tun_PIP( V )
  global a, global b, global d
  J = sign(V) .* fn( abs(V) / d(3), a(3), b(3) );
end
function J = tun_MIM( V )
  global a, global b, global d
  J = sign(V) .* pf( abs(V) / d(4), a(4), b(4) );
end
% for dielectrics between surface and actives,
% there is no current
```

```
function J = tun_NON( V )
  J = 0;
end

%% Setup 1:
%%  C2 PIP (1kum^2) + C1 MOS (15um^2)
% MOS:
function I = tun1( V )
  I = tun_MOS( V ) * 15e-12;
end
% estimate of MOS capacitance
C1 = 15*4e-15;
% PIP:
function I = tun2( V )
  I = tun_PIP( V ) * 10*1e-12;
end
C2 = 1e3*1.37e-15;
% voltages to examine:
V = [1:1:40];
% simulate
v1 = stationary( V );
[t1, vv1] = timed_simulation( V, C1, C2 );
dlmwrite( 'setup-1-s.result.knl', [V' v1'] );
dlmwrite( 'setup-1-t.result.knl', [0, V; t1', vv1] );

%% Setup 2:
%%  C2 ILD + C1 MOS (0.4um^2)
% MOS tunneling: only through transistor
function I = tun1( V )
  I = sign(V) .* tun_MOS( abs(V) ) * 0.4e-12;
end
% MOS capacitance: transistor and additional capacitor
C1 = 0.4*4e-15 + 10*1.37e-15;
% ILD
function I = tun2( V )
  I = sign(V) .* tun_NON( abs(V) );
end
% ILD capacitor
% Eps_r = 5.1, d=1.2um, A=6x6um
C2 = 18*18e-12*8.85e-12*5.1/1.2e-6;
% voltages to examine:
V = [5:5:200];
% simulate
v2 = stationary( V );
[t2, vv2 ] = timed_simulation( V, C1, C2, 1e2, 0 );
dlmwrite( 'setup-2-s.result.knl', [V' v2'] );
dlmwrite( 'setup-2-t.result.knl', [0, V; t2', vv2] );
```

```
%% Setup 3:
%%   Charge simulation of decay on tunneling capacitor
%%  C1: MOS (0.4*1um^2) + PIP (10um^2)
% tunneling only through the transistor
function I = tun1( V )
  I = sign(V) .* tun_MOS( abs(V) ) * 0.4e-12;
end
% capacitance is sum from transistor and PIP capacitor
C1 = 0.4*4e-15 + 10*1.37e-15;
% Charge amounts to simulate
Q = [5e-15:1.5e-14:5e-13];
% stationary simulation is no use: it will return Q=0 for all cases
% time simulation
[t3, q3] = timed_charge( Q, C1 );
dlmwrite( 'setup-3-t.result.knl', [0, Q; t3, q3] );
```

Appendix C

Noise of LMS Derived Current Value

In order to calculate the resulting current noise from noisy charge readings of the charge sensor, the following notation is used: The charge sensor is operated in the time-frame between $-\frac{T}{2} \ldots \frac{T}{2}$, giving noisy charge readings q_i at N equidistant times t_i with $i = -\frac{N-1}{2} \ldots \frac{N-1}{2}$, where $N = 2n + 1$ with $n \in \mathbb{N}$. Also $t_\mathrm{i} = i\frac{T}{N-1}$ describes the points in time for measurement. This yields $\overline{t_\mathrm{i}} = 0$. The noisy readings q_i are described by $q_\mathrm{i} = I t_\mathrm{i} + e$ with e as mean free normal distributed random variable ($\overline{e} = 0$ and $\mathrm{Var}\, e = {\sigma_\mathrm{e}}^2$), and subsequently $\overline{q_\mathrm{i}} = 0$ holds.

The approximation now derives I' from the $(t_\mathrm{i}; q_\mathrm{i})$-tuples such that the quadratic error of the resulting approximation to the measured values is minimal.

$$I' = \frac{\left(\sum_i t_\mathrm{i}\right)\left(\sum_i q_\mathrm{i}\right) - N \sum_i t_\mathrm{i} q_\mathrm{i}}{\left(\sum_i t_\mathrm{i}\right)\left(\sum_i t_\mathrm{i}\right) - N \sum_i {t_\mathrm{i}}^2}$$

If not noted otherwise, i iterates over all tuples, that is $i = -\frac{N-1}{2} \ldots \frac{N-1}{2}$. Replacing q_i accordingly and separating the deterministic part:

$$I' = \frac{\left(\sum_i t_\mathrm{i}\right)\left(\sum_i I t_\mathrm{i} + \sum_i e\right) - N\left(\sum_i I {t_\mathrm{i}}^2 + \sum_i t_\mathrm{i} e\right)}{\left(\sum_i t_\mathrm{i}\right)\left(\sum_i t_\mathrm{i}\right) - N \sum_i {t_\mathrm{i}}^2}$$

As t_i is constructed with mean zero ($\overline{t_\mathrm{i}} = 0$), the first terms are zero, too:

$$I' = \frac{-N\left(I \sum_i {t_\mathrm{i}}^2 + \sum_i t_\mathrm{i} e\right)}{-N \sum_i {t_\mathrm{i}}^2}$$

The deterministic part is I, which is the purpose of the least mean square (LMS) algorithm:

$$I' = I + \frac{1}{\sum_i {t_\mathrm{i}}^2} \sum_i e\, t_\mathrm{i}$$

The sum over the squares can be transformed[1] and results in:

$$I' = I + \frac{12}{T^2 N} \frac{N-1}{N+1} \sum_i e\, t_\mathrm{i} \tag{C.1}$$

Still, the determined value of current is affected by the noise term e. When this experiment is repeated multiple times with the same value for I, the variance from e is reflected within each individual instance of I', labeled I'_k.

To further characterize the noise of the resulting current values, the term from Equation C.1 is analyzed with respect to the distribution. The sum term sums scaled versions of Gaussian random variables e. e is characterized by $\overline{e} = 0$ and $\mathrm{Var}\, e = {\sigma_\mathrm{e}}^2$ entirely. Scaling of the Gaussian random variable by t_i causes the mean and variance to scale alike. Summing then causes the variances and means to sum, too. The variance of I' is not affected by the value of I. As initially the mean is zero, it will stay zero, $\overline{I'_\mathrm{k}} = 0$. The sum then transfers to the variance as

$$\mathrm{Var}\, I'_\mathrm{k} = \left(\frac{12}{T^2 N} \frac{N-1}{N+1}\right)^2 \sum_i {\sigma_\mathrm{e}}^2 {t_\mathrm{i}}^2$$

where the sum can again be calculated as ${\sigma_\mathrm{e}}^2$ is fixed with respect to i:

$$\mathrm{Var}\, I'_\mathrm{k} = {\sigma_\mathrm{e}}^2 \frac{12}{T^2 N} \frac{N-1}{N+1}$$

C.1 Numerical Verification

The mathematical model for the resulting variance in the approximated current value can be simulated on a Monte-Carlo basis. This is done using an "octave" program. The simulation and the theoretical value match, as can be seen in Figure C.1. The program for simulation used is:

[1] The sum of the squares can be expressed as [136, p. 19, 1.59]:

$$\begin{aligned}\sum_{i=-\frac{N-1}{2}\ldots\frac{N-1}{2}} {t_\mathrm{i}}^2 &= 2 \sum_{i=1\ldots\frac{N-1}{2}} \left(i \frac{T}{N-1}\right)^2 \\ &= 2\left(\frac{T}{N-1}\right)^2 \frac{N-1}{2} \left(\frac{N-1}{2}+1\right)\left(2\frac{N-1}{2}+1\right) \\ &= \frac{1}{12} T^2 N \frac{N+1}{N-1}\end{aligned}$$

```
% octave script to test if the regression
% follows the given behavior
%
% idea: create sample traces of charge q over time t
% where charge q is affected from noisy measurement,
% derive the current value II through LMS approximation
% collect multiple of these current values II for
% - different number of measurement points within T
% - different current values I
% and calculate mean and variance from the resulting
% collection.

T = 10;        % measurement time [s]
N = [3:4:50]; % number of measurements within T for each experiment
sigma = 10e-3; % deviation of measured value r.m.s. voltage [V]
M = 1000;      % number of experiments to try per current value
Cfb = 100e-15; % feedback capacitor size [F]
I = [0:1e-15:1e-14]; % measured current [A]

mI=[];
vI=[];
II=[];

% 1) go through all numbers of N
for i = 1:length(N)
  % N(i) measurements at time t [0...T]
  t = ([0:N(i)-1] ./ (N(i)-1) .* T)';
  % go through all current values
  for j = 1:length(I)
    % theoretical charge q
    q = (I(j) .* ones( length(t), M )) .* t;
    % add noise (independent of I and t)
    q += Cfb .* sigma .* stdnormal_rnd(rows(q), columns(q));
    % now do LMS on q and t
    for n = 1:columns(q)
      y=q(:,n); x=t;
      II(j,i,n)=sum((x-mean(x)).*(y-mean(y)))/sum((x-mean(x)).^2);
    end
    % and calculate mean and variance
    mI(j,i) = mean(II(j,i,:));
    vI(j,i) = var(II(j,i,:));
  end
end

% calculate theoretical value according to formula
tvI = 12 .* ((Cfb .* sigma ./ T) .^ 2) .* (N-1) ./ (N .* (N+1));
```

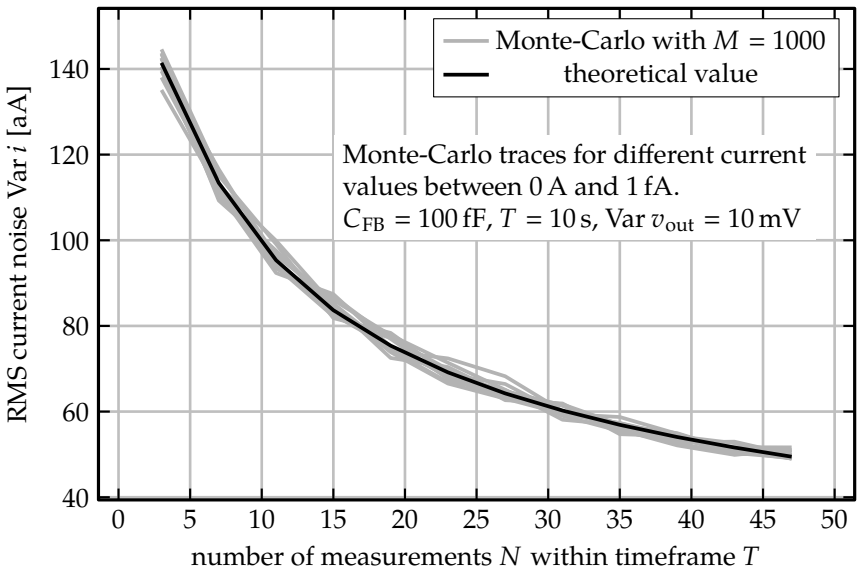


Figure C.1: Verification of the theoretical calculation with a Monte-Carlo simulation using the octave program.

```
% and plot the results
figure();
plot(N,sqrt(vI),'',N,sqrt(tvI),'linewidth',3)
ylabel('r.m.s. current noise');
xlabel('number of measurements');
title(sprintf(['%i Experiments per point, feedback capacitor %1.2e F', ...
  ', voltage r.m.s. noise %1.2e V'], M, Cfb, sigma));

% save results
dlmwrite( 'noise-simulation.result.knl', [sprintf( ...
  'Simulation: %i experiments per point; Cfb=%1.2e F; sigma=%1.2e V', ...
  M, Cfb, sigma) ; 'I,Points'], '');
dlmwrite( 'noise-simulation.result.knl', ...
  [0, N; 0, tvI; I', vI], '-append' );
```

List of Figures

2.1 Focused ion beam schematic 20
2.2 Surface charging model from FIB irradiation 21
2.3 Manufacturing process improvement from FIB usage 23

3.1 The Keithley Instruments SCS4200 system equipped with preamplifier SMU is subject to a low pass behavior. 34
3.2 Model and equivalent small signal circuit of a DUT connected to an SMU 35
3.3 Limits to low current measurement from noise 39

4.1 Gold leaf electrometer 43
4.2 Field mill electrometer 44
4.3 Cross sectional schematic of a MOSFET 45
4.4 An inverting amplifier with resistive feedback elements. 48
4.5 Capacitor feedback design usable with any of the available electrometer measurement setups. 49
4.6 One dimensional problem for the explanation of mirror charge in the antenna charge measurement setup. 50
4.7 Capacitive voltage divider and nomenclature. 53
4.8 Voltage trace of the capacitive voltage divider simulated with the script from Appendix B. 55
4.9 Simulated quasi-static output voltage after 1 s delay, depending on the applied input voltage. 55

5.1 Simplified schematic circuit of the capacitive charge measurement setup. 57
5.2 Capacitive measurement setup with non-ideal devices and parasitics 60
5.3 Capacitive charge measurement circuit including noise sources . . . 64
5.4 Circuit of a offline charge detection implementation. 68
5.5 Schematic circuit of the implemented closed loop feedback design . . 71
5.6 Layout of the charge sensor chip to be used with an external amplifier (left) and with on-die amplifier (right). 74
5.7 Verification process of the floating gate functionality 75
5.8 Verification of low leakage behavior and effectiveness of shield against incident light, C_{FB} = 137 fF. 76
5.9 External fields (i.e. voltage at needle) do only influence those cells which have an antenna connected to the input, C_{FB} = 137 fF. 77
5.10 A resistor conducts a current into the charge sensor input causing a linear accumulation of charge in the charge sensor, C_{FB} = 137 pF . . . 78
5.11 Schematic of the implemented offline charge detection circuit 79
5.12 FEM simulation model for antenna functionality 81

5.13 Simulation of the tunneled charge amount from the applied surface voltage based on the capacitive voltage divider simulations. 82

6.1 Photograph of the measurement setup for the closed loop feedback implementation 86
6.2 Schematic for the characterization of dielectrics with the closed loop feedback implementation 88
6.3 Recorded charge traces for the MIM dielectric leakage behavior . . . 89
6.4 Derived current value for the MIM dielectric test structure and comparison with conventional measurement 90
6.5 Sensitivity improvement from using the charge sensor for dielectric characterization 91
6.6 The tip-to-tip stress test structures with varying distances used to evaluate the charge sensor, according to [135]. Each terminal has a bondpad to contact the specific tip. 93
6.7 Schematic setup for off-die dielectric characterization by bonding and needle probing 94
6.8 Charge traces for different applied stress voltages of the comb structures for two individual peaks located in vicinity to each other, C_{FB} = 137 pF. 95
6.9 Leakage current behavior derived by LMS from the charge traces for the off-die dielectric characterization, $C_{FB} = 137\,\text{pF}$, $N = 110$, $T = 160\,\text{s}$. 95
6.10 Current derived from a subset of points from three exemplary charge measurements showing the time resolved behavior of the leakage current 96
6.11 Surface charging model and resulting mirror charges in the charge sensor 99
6.12 Surface charge from FIB irradiation and resulting SE image 100
6.13 Surface charge accumulation for continuous FIB irradiation 101
6.14 Charge and current observation from the electronically blanked FIB. Closing the metal lid (gate valve) of the column, stops the effect, C_{FB} = 1.37 pF poly insulator poly (PIP), $N = 10$, $T = 30\,\text{s}$. 103
6.15 Charging and current observation dependence of the electronically blanked FIB from the beam current setting 105
6.16 Beam blanker voltage influence on the charging during blanked ion beam 106
6.17 Charge observation from the entry of process gases into the FIB system 108
6.18 Transfer characteristics from two different cells of the offline charge detection circuit. 110
6.19 Influences from typical FIB CE steps to the IC 111
6.20 Influence of the FIB to the state of the offline charge detection 112
6.21 Schematic of backside CE using a FIB 115
6.22 Observed fuse bit state using the FIB SE image [142], unpowered device (left), enhanced contrast version (middle) and on the powered-up device (right). 116
6.23 Performing a FIB CE on the backside prepared fuse bit structure, setting it to arbitrary values. [142] 116
6.24 Schematic of an SRAM cell subject to a Seebeck voltage generated by a temperature gradient [145]. 119
6.25 Supply current intensity pattern observed from TLS on a powered up SRAM device [145]. 120

A.1 Tunneling current characteristics and approximation of model parameters 128

C.1 Verification of the theoretical calculation with a Monte-Carlo simulation using the octave program. 140

List of Tables

4.1 Summary of charge measurement methods 47

A.1 Tunneling model coefficients derived by LMS approximation for gate, PIP and MIM dielectrics of the BiCMOS technology used for simulations. 127

Acronyms

AC alternating current. 16, 43, 44

AES advanced encryption standard. 29

AFM atomic force microscopy. 17, 43, 113, 114

BiCMOS bipolar complementary metal oxide semiconductor. 70, 87, 123

CCD charge coupled device. 15, 17

CDD charge domain device. 17

CE circuit edit. 7, 19, 21, 22, 85, 99, 101, 102, 109, 110, 115, 123

CMOS complementary metal oxide semiconductor. 7, 17, 56, 70, 119–122

CRP challenge response pair. 31

DC direct current. 16, 17, 57, 78, 104, 107, 131

DIL dual in line. 88, 93

DUT device under test. 35, 39

EBP electron beam probing. 30

EEPROM electrically erasable programmable read only memory. 114

EFM electrostatic force microscopy. 43

EM electro magnetic. 30, 92

ESD electrostatic discharge. 22, 25, 73, 82, 92, 98

FA failure analysis. 7, 31, 102, 109, 113, 119, 121, 123–125

FET field effect transistor. 58, 122

FIB focused ion beam. 7, 18, 19, 21–23, 30–32, 46, 68, 70, 79, 80, 85, 86, 98, 99, 101–104, 107–111, 113–115, 117, 118, 122–125

FN Fowler-Nordheim. 27, 28, 54, 67, 68, 128, 129

FOV field of view. 99–101, 115

IC integrated circuit. 7, 18, 19, 21–23, 25, 29–32, 42–45, 56, 66, 70, 72, 74, 85, 98, 109–111, 113–115, 117–121, 123, 124

ILD inter level dielectric. 23, 24, 73

LMS least mean square. 59, 66, 86–88, 90, 94, 97, 102, 103, 127, 128, 138

LVS layout versus schematic. 74

MEMS microelectromechanical system. 44, 56

MIM metal insulator metal. 70, 73, 87, 89, 90, 127–129

MOS metal oxide semiconductor. 23, 44, 46, 50, 54, 70, 71, 80, 83, 119

MOSFET metal oxide semiconductor field effect transistor. 26, 27, 45–47, 56–59, 65, 69, 79

NIR near infrared. 21, 22, 30

NVM non-volatile memory. 31, 68, 70, 102, 113, 114, 118

PCB printed circuit board. 85, 86, 92–94

PF Poole-Frenkel. 27, 28, 67, 90, 91, 128, 129

PIP poly insulator poly. 54, 73, 75, 103, 105, 127, 128, 142

PLS photoelectric laser stimulation. 17

PTAT proportional to absolute temperature. 71

PUF physically unclonable function. 7, 31, 32, 87, 113, 117, 118, 121, 122

RF radio frequency. 51

RMS root mean square. 37, 38, 66, 92, 96, 123, 124

SC switched capacitor. 17

SCA side channel analysis. 30

SCR space charge region. 27, 36, 47

SE secondary electron. 7, 19, 21, 46, 47, 87, 98, 99, 101, 102, 104, 107, 114–116, 123

SEM scanning electron microscopy. 17, 19, 21, 46, 122

SIL solid immersion lens. 121

SILC stress induced leakage current. 24

SMU source and measurement unit. 34–36, 85, 86

SNR signal to noise ratio. 37

SOI silicon on insulator. 56

SRAM static random access memory. 32, 117, 118, 120–122

STI shallow trench isolation. 115

TDDB time dependent dielectric breakdown. 24

TEM transmission electron microscopy. 22, 97

TLS thermal laser stimulation. 119, 121

UV ultra violet. 122

Mathematical Symbols

A	area. 51, 53, 54
α_{Seebeck}	Seebeck coefficient. 118, 119
$\vec{B}$	magnetic induction. 15, 16
C	capacitance. 46, 53, 54, 58, 60–62, 64, 65, 69
C_{FB}	feedback capacitor. 49, 57–63, 65, 69, 71, 72, 79, 86, 88, 92, 93, 141, 142
c_{wire}	small signal wire capacitance. 35
$\vec{D}$	electric displacement field. 15, 51
$\vec{E}$	electric field. 15, 26–28, 51, 52, 90, 127
e	absolute electron charge. 26, 36, 37, 40, 52
e	error part of measurement amplitude. 137, 138
ε	permittivity. 26
ϵ	relative error. 54, 61–63
ε_0	vacuum permittivity. 51
ε_{r}	relative permittivity. 51, 52
$\mathbf{F}$	arbitrary transfer function. 69
f	frequency. 36–39
f_{B}	bandwidth. 37, 39, 40
G	gain. 48, 49, 58–61, 65
g	distance. 51, 52
g_{m}	transconductance of metal oxide semiconductor field effect transistor (MOSFET). 109
$\vec{H}$	magnetic field. 15
h	distance. 51, 52

$\mathbf{I}'$ current value derived from least mean square (LMS) approximation. 65, 86, 137, 138

$\mathbf{I}$ absolute current. 35–38, 40, 46, 48, 49, 52, 60, 63, 70, 71, 86, 100, 109, 137, 138

$\mathbf{i}$ relative current, small signal current. 35, 37–39, 64, 65, 86, 92, 97, 137, 138

$\vec{J}$ current density. 15, 16, 28, 53, 54, 90, 127

k_B Boltzmann's constant. 26, 37

L transistor channel length. 46

$\mathbf{n}$ electron density in conduction band. 26, 27, 137

N natural number, counts. 26, 66, 86, 92, 96, 97, 100, 137, 138, 142

N_A Acceptor density. 26, 27

N_D Donor density. 26, 27

n_i intrinsic carrier density. 26

$\mathbf{p}$ hole density in valence band. 26, 27

$\mathbf{\Phi}$ electrostatic potential. 26

Φ_B bulk potential. 26, 27, 45

Φ_S surface potential. 27, 45

q' mirror charge density. 51, 52

$\mathbf{Q}$ charge. 24, 49, 53, 54, 56–63, 68–70, 100

q charge density. 51, 52, 65, 66, 86, 137

q_v volume charge density. 15

R resistance. 48, 49

r small signal resistance. 35, 37

R_{FB} feedback resistor. 48, 49

ρ space charge density. 26, 27

$s_{0,flr}$ flicker noise proportionality coefficient. 38

$\mathbf{s}_{n,flr}$ flicker noise power. 38

$\mathbf{s}_{n,sh}$ Shottky noise power. 36

$\mathbf{s}_{n,th}$ Shottky noise power. 37

σ standard deviation. 137, 138

T period. 63, 66, 92, 96, 97, 137, 138, 142

t time. 15, 35, 39, 54, 59, 63, 70, 86, 100, 103, 104, 106, 108, 137, 138

T_{abs} absolute temperature. 26, 37, 118

μ mobility. 46

$\mathbf{V}$ absolute voltage. 35, 37, 39, 46, 48, 49, 53, 54, 57–62, 64, 65, 68, 69, 75, 88, 89, 92, 94, 97, 109, 118

$\mathbf{v}$ relative voltage, small signal voltage. 52, 64, 65, 92

W transistor width. 46

W_{F} Fermi level. 26

W_{G} band gap. 26

W_{i} Fermi level for an intrinsic semiconductor. 26

W_{kin} kinetic energy. 98

x location. 26, 27, 51, 66

Bibliography

[1] M. Coulomb. "Premier mémoire sur l'électricité et le magnétisme". In: *Histoire de l'Académie Royale des Sciences*. 1785, pp. 569–577.

[2] M. Coulomb. "Second mémoire sur l'électricité et le magnétisme". In: *Histoire de l'Académie Royale des Sciences*. 1785, pp. 578–611.

[3] A. Volta. "On the Electricity Excited by the Mere Contact of Conducting Substances of Different Kinds. In a Letter from Mr. Alexander Volta, F. R. S. Professor of Natural Philosophy in the University of Pavia, to the Rt. Hon. Sir Joseph Banks, Bart. K. B. P. R. S." In: *Philosophical Transactions of the Royal Society of London* 90 (1800), pp. 403–431. DOI: 10.1098/rstl.1800.0018.

[4] T. J. Seebeck. *Magnetische Polarisation der Metalle und Erze durch Temperatur-Differenz*. Ed. by A. J. v. Oettingen. 1895th ed. Verlag von Wilhelm Engelmann, Leipzig, 1822.

[5] G. Kirchhoff. "Ueber eine Ableitung der Ohm'schen Gesetze, welche sich an die Theorie der Elektrostatik anschliesst". In: *Annalen der Physik* 154.12 (1849), pp. 506–513. ISSN: 1521-3889. DOI: 10.1002/andp.18491541206.

[6] J. C. Maxwell. "A Dynamical Theory of the Electromagnetic Field". In: *Philosophical Transactions of the Royal Society of London* 155 (1865), pp. 459–512. DOI: 10.1098/rstl.1865.0008.

[7] O. Weston. *Electrometer*. US Patent 530,145. 1894. URL: https://www.google.com/patents/US530145.

[8] W. Schottky. "Über spontane Stromschwankungen in verschiedenen Elektrizitätsleitern". In: *Annalen der Physik* 362.23 (1918), pp. 541–567. ISSN: 1521-3889. DOI: 10.1002/andp.19183622304.

[9] J. B. Johnson. "The Schottky Effect in Low Frequency Circuits". In: *Phys. Rev.* 26 (1 1925), pp. 71–85. DOI: 10.1103/PhysRev.26.71.

[10] W. Schottky. "Small-Shot Effect and Flicker Effect". In: *Phys. Rev.* 28 (1 1926), pp. 74–103. DOI: 10.1103/PhysRev.28.74.

[11] J. B. Johnson. "Thermal agitation of electricity in conductors". In: *Nature* 119.2984 (1927), pp. 50–51.

[12] R. H. Fowler and L. Nordheim. "Electron Emission in Intense Electric Fields". In: *Proceedings of the Royal Society of London*. Vol. 117. 1928, pp. 173–181. DOI: 10.1098/rspa.1928.0091.

[13] J. B. Johnson. "Thermal agitation of electricity in conductors". In: *Physical Review* 32.1 (1928), p. 97.

[14] L. Onsager. "Reciprocal Relations in Irreversible Processes. I." In: *Phys. Rev.* 37 (4 1931), pp. 405–426. DOI: 10.1103/PhysRev.37.405.

[15] J. Frenkel. "On Pre-Breakdown Phenomena in Insulators and Electronic Semi-Conductors". In: *Phys. Rev.* 54 (8 1938), pp. 647–648. DOI: 10.1103/PhysRev.54.647.

[16] W. Shockley. "Currents to Conductors Induced by a Moving Point Charge". In: *Journal of Applied Physics* 9.10 (1938), pp. 635–636. DOI: 10.1063/1.1710367.

[17] S. Ramo. "Currents Induced by Electron Motion". In: *Proceedings of the IRE* 27.9 (1939), pp. 584–585. ISSN: 0096-8390. DOI: 10.1109/JRPROC.1939.228757.

[18] H. Palevsky, R. K. Swank, and R. Grenchik. "Design of Dynamic Condenser Electrometers". In: *Review of Scientific Instruments* 18.5 (1947), pp. 298–314. ISSN: 0034-6748. DOI: 10.1063/1.1740941.

[19] A. Palm. "Elektrostatische Meßgeräte". In: *Elektrische Meßgeräte und Meßeinrichtungen*. Springer Berlin Heidelberg, 1948, pp. 101–115. ISBN: 978-3-662-01407-3. DOI: 10.1007/978-3-662-01406-6_8.

[20] B. Widrow. "A Study of Rough Amplitude Quantization by Means of Nyquist Sampling Theory". In: *Circuit Theory, IRE Transactions on* 3.4 (1956), pp. 266–276. ISSN: 0096-2007. DOI: 10.1109/TCT.1956.1086334.

[21] W. R. Beam. *Electronics of Solids*. Physical and Quantum Electronics Series. McGraw-Hill, 1965.

[22] E. Tudor. "The dynamic capacitor electrometer". In: *Radio and Electronic Engineer* 30.1 (1965), pp. 37–45. ISSN: 0033-7722. DOI: 10.1049/ree.1965.0075.

[23] M. Lenzlinger and E. H. Snow. "Fowler-Nordheim Tunneling into Thermally Grown SiO_2". In: *Journal of Applied Physics* 40.1 (1969), pp. 278–283. DOI: 10.1063/1.1657043.

[24] W. S. Boyle and G. E. Smith. "Charge Coupled Semiconductor Devices". In: *Bell System Technical Journal* 49.4 (1970), pp. 587–593. ISSN: 1538-7305. DOI: 10.1002/j.1538-7305.1970.tb01790.x.

[25] D. Fried. "Analog sample-data filters". In: *Solid-State Circuits, IEEE Journal of* 7.4 (1972), pp. 302–304. ISSN: 0018-9200. DOI: 10.1109/JSSC.1972.1050305.

[26] R. Paul. *Halbleiterphysik*. Elektronische Festkörperbauelemente. VEB Verlag Technik, 1974. ISBN: 9783778503355. URL: http://books.google.de/books?id=FCjnGwAACAAJ.

[27] D. Allan. "A Review of Flicker Noise Frequency Instabilities in Precision Frequency Standards". In: *Proceedings of the Symposium on 1/f Fluctuation* (1977). BIN 634, pp. 158–172.

[28] P. M. Pflier, H. Jahn, and G. Jentsch. *Elektrische Meßgeräte und Meßverfahren*. 4th ed. Springer-Verlag Berlin Heidelberg, 1978. ISBN: 3-540-08601-3.

[29] U. Tietze and C. Schenk. *Halbleiter-Schaltungstechnik*. 4th ed. Springer-Verlag, 1978.

[30] H. Herscovici. "Input Offset Voltage and Current in Varicap Diode Modulators". In: *Instrumentation and Measurement, IEEE Transactions on* 28.1 (1979), pp. 36–41. ISSN: 0018-9456. DOI: 10.1109/TIM.1979.4314757.

[31] R. Voss. "1/f (Flicker) Noise: A Brief Review". In: *33rd Annual Symposium on Frequency Control. 1979*. 1979, pp. 40–46. DOI: 10.1109/FREQ.1979.200297.

[32] E. Wolfgang, P. Fazekas, H.-P. Feuerbaum, and R. Lindner. "Electron-beam testing of VLSI circuits". In: *Solid-State Circuits, IEEE Journal of* 14.2 (1979), pp. 471–481. ISSN: 0018-9200. DOI: 10.1109/JSSC.1979.1051199.

[33] G. Carver and M. Buehler. "An analytical expression for the evaluation of leakage current in the integrated gated-diode electrometer". In: *Electron Devices, IEEE Transactions on* 27.12 (1980), pp. 2245–2252. ISSN: 0018-9383. DOI: 10.1109/T-ED.1980.20259.

[34] A. K. Jonscher. *Dielectric Relaxation in Solids*. Chelsea Dielectrics Press, London, 1983.

[35] P. Secker and J. Chubb. "Instrumentation for electrostatic measurements". In: *Journal of Electrostatics* 16.1 (1984), pp. 1–19. ISSN: 0304-3886. DOI: 10.1016/0304-3886(84)90015-9.

[36] T. L. Vogelsong, J. Tiemann, and A. Steckl. "Charge-domain integrated circuits for signal processing". In: *Solid-State Circuits, IEEE Journal of* 20.2 (1985), pp. 562–570.

[37] J. Melngailis, C. R. Musil, E. H. Stevens, M. Utlaut, E. M. Kellogg, R. T. Post, M. W. Geis, and R. W. Mountain. "The focused ion beam as an integrated circuit restructuring tool". In: *Journal of Vacuum Science & Technology B* 4.1 (1986), pp. 176–180. DOI: 10.1116/1.583373.

[38] Y. Nissan-Cohen. "A novel floating-gate method for measurement of ultra-low hole and electron gate currents in MOS transistors". In: *Electron Device Letters, IEEE* 7.10 (1986), pp. 561–563. ISSN: 0741-3106. DOI: 10.1109/EDL.1986.26474.

[39] J. Melngailis. "Focused ion beam technology and applications". In: *Journal of Vacuum Science & Technology B* 5.2 (1987), pp. 469–495. DOI: 10.1116/1.583937.

[40] J. E. Stern, B. D. Terris, H. J. Mamin, and D. Rugar. "Deposition and imaging of localized charge on insulator surfaces using a force microscope". In: *Applied Physics Letters* 53.26 (1988), pp. 2717–2719. DOI: 10.1063/1.100162.

[41] A. van der Ziel. "Unified presentation of 1/f noise in electron devices: fundamental 1/f noise sources". In: *Proceedings of the IEEE* 76.3 (1988), pp. 233–258. ISSN: 0018-9219. DOI: 10.1109/5.4401.

[42] K. S. Cover. "Construction of a prototype MOS electrometer". In: *Review of Scientific Instruments* 60.8 (1989), pp. 2733–2739. DOI: 10.1063/1.1140650.

[43] W. Lee. "Engineering a device for electron-beam probing". In: *Design Test of Computers, IEEE* 6.3 (1989), pp. 36–42. ISSN: 0740-7475. DOI: 10.1109/54.32411.

[44] B. D. Terris, J. E. Stern, D. Rugar, and H. J. Mamin. "Contact electrification using force microscopy". In: *Phys. Rev. Lett.* 63 (24 1989), pp. 2669–2672. DOI: 10.1103/PhysRevLett.63.2669.

[45] B. Fishbein, D. Krakauer, and B. Doyle. "Measurement of very low tunneling current density in SiO_2 using the floating-gate technique". In: *Electron Device Letters, IEEE* 12.12 (1991), pp. 713–715. ISSN: 0741-3106. DOI: 10.1109/55.116965.

[46] J. Koller and W. Athas. "Adiabatic Switching, Low Energy Computing, And The Physics Of Storing And Erasing Information". In: *Physics and Computation, 1992. PhysComp '92., Workshop on*. 1992, pp. 267–270. DOI: 10.1109/PHYCMP.1992.615554.

[47] W. Lukaszek. *Charge monitoring device for use in semiconductor wafer fabrication for unipolar operation and charge monitoring*. US Patent 5,315,145. 1994. URL: https://www.google.com.ar/patents/US5315145.

[48] K. Schuegraf, D. Park, and C. Hu. "Reliability of thin SiO/sub 2/ at direct-tunneling voltages". In: *Electron Devices Meeting, 1994. IEDM '94. Technical Digest., International*. 1994, pp. 609–612. DOI: 10.1109/IEDM.1994.383336.

[49] R. Bammi and S. Reno. "Using CHARM-2 wafers to increase reliability in ion implant processing". In: *Integrated Reliability Workshop, 1995. Final Report., International*. 1995, pp. 11–17. DOI: 10.1109/IRWS.1995.493568.

[50] P. Cotti. "The discovery of the electric current". In: *Physica B: Condensed Matter* 204.1–4 (1995), pp. 367–369. ISSN: 0921-4526. DOI: 10.1016/0921-4526(94)00289-8.

[51] R. Anderson and M. Kuhn. "Tamper resistance: a cautionary note". In: *Proceedings of the 2nd conference on Proceedings of the Second USENIX Workshop on Electronic Commerce-Volume 2* (1996).

[52] A. Devgan. "Transient simulation of integrated circuits in the charge-voltage plane". In: *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on* 15.11 (1996), pp. 1379–1390. ISSN: 0278-0070. DOI: 10.1109/43.543770.

[53] J. Orloff, L. Swanson, and M. Utlaut. "Fundamental limits to imaging resolution for focused ion beams". In: *Journal of Vacuum Science & Technology B: Microelectronics and Nanometer Structures* 14.6 (1996), pp. 3759–3763.

[54] S. Brandt and H. D. Dahmen. *Elektrodynamik. Eine Einführung in Experiment und Theorie*. 3rd ed. Springer-Verlag Berlin Heidelberg, 1997. ISBN: 3-540-61911-9.

[55] A. Campbell, K. Peterson, D. Fleetwood, and J. Soden. "Effects on focused ion beam irradiation on MOS transistors". In: 1997. URL: http://www.osti.gov/scitech/servlets/purl/456309.

[56] R. M. Nyffenegger, R. M. Penner, and R. Schierle. "Electrostatic force microscopy of silver nanocrystals with nanometer-scale resolution". In: *Applied Physics Letters* 71.13 (1997), pp. 1878–1880. DOI: 10.1063/1.119425.

[57] P. Bergveld, J. Hendrikse, and W. Olthuis. "Theory and application of the material work function for chemical sensors based on the field effect principle". In: *Measurement Science and Technology* 9.11 (1998), p. 1801. URL: http://stacks.iop.org/0957-0233/9/i=11/a=003.

[58] A. N. Cleland and M. L. Roukes. "A nanometre-scale mechanical electrometer". In: *Nature* 392.6672 (12, 1998), pp. 160–162. ISSN: 0028-0836. DOI: 10.1038/32373.

[59] Y.-B. Park and D. Schroder. "Degradation of thin tunnel gate oxide under constant Fowler-Nordheim current stress for a flash EEPROM". In: *Electron Devices, IEEE Transactions on* 45.6 (1998), pp. 1361–1368. ISSN: 0018-9383. DOI: 10.1109/16.678579.

[60] L. Giannuzzi and F. Stevie. "A review of focused ion beam milling techniques for TEM specimen preparation". In: *Micron* 30.3 (1999), pp. 197–204. ISSN: 0968-4328. DOI: 10.1016/S0968-4328(99)00005-0.

[61] P. C. Kocher, J. Jaffe, and B. Jun. "Differential Power Analysis". In: *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*. CRYPTO '99. London, UK, UK: Springer-Verlag, 1999, pp. 388–397. ISBN: 3-540-66347-9. URL: http://dl.acm.org/citation.cfm?id=646764.703989.

[62] R. H. Livengood, P. Winer, and V. R. Rao. "Application of advanced micromachining techniques for the characterization and debug of high performance microprocessors". In: *Journal of Vacuum Science Technology B: Microelectronics and Nanometer Structures* 17.1 (1999), pp. 40–43. ISSN: 1071-1023. DOI: 10.1116/1.590514.

[63] W. Lukaszek. *Method of reducing charging damage to integrated circuits in ion implant and plasma-based integrated circuit process equipment*. US Patent 5,998,282. 1999. URL: https://www.google.com/patents/US5998282.

[64] T. J. Sumner, J. Mester, and S. Buchman. "Chapter 44: Charge Measurement". In: *The Measurement, Instrumentation and Sensors Handbook*. CRC Press, 26, 1999. Chap. Charge Measurement. ISBN: 978-0-8493-8347-2. DOI: 10.1201/9780415876179.ch44.

[65] J. Suehle, E. M. Vogel, B. Wang, and J. Bernstein. "Temperature dependence of soft breakdown and wear-out in sub-3 nm SiO2 films". In: *Reliability Physics Symposium, 2000. Proceedings. 38th Annual 2000 IEEE International*. 2000, pp. 33–39. DOI: 10.1109/RELPHY.2000.843888.

[66] E. M. Vogel, J. Suehle, M. D. Edelstein, B. Wang, Y. Chen, and J. Bernstein. "Reliability of ultrathin silicon dioxide under combined substrate hot-electron and constant voltage tunneling stress". In: *Electron Devices, IEEE Transactions on* 47.6 (2000), pp. 1183–1191. ISSN: 0018-9383. DOI: 10.1109/16.842960.

[67] I. Eisele, T. Doll, and M. Burgmair. "Low power gas detection with FET sensors". In: *Sensors and Actuators B: Chemical* 78.1–3 (2001). Selected Papers from Eurosensors XIV, pp. 19–25. ISSN: 0925-4005. DOI: 10.1016/S0925-4005(01)00786-9.

[68] P. Girard. "Electrostatic force microscopy: principles and some applications to semiconductors". In: *Nanotechnology* 12.4 (2001), p. 485. URL: http://stacks.iop.org/0957-4484/12/i=4/a=321.

[69] J. C. Gonzalez, D. P. Griffis, T. T. Miau, and P. E. Russell. "Chemically enhanced focused ion beam micromachining of copper". In: *Journal of Vacuum Science & Technology B* 19.6 (2001), pp. 2539–2542. DOI: 10.1116/1.1418406.

[70] S. W. Howell. "Electrostatic Force Microscopy Studies of Nanomscale Systems". PhD thesis. Purdue University, May 2001.

[71] J.-J. Quisquater and D. Samyde. "ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards". In: *Smart Card Programming and Security*. Ed. by I. Attali and T. Jensen. Vol. 2140. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2001, pp. 200–210. ISBN: 978-3-540-42610-3. DOI: 10.1007/3-540-45418-7_17.

[72] S. Reyntjens and R. Puers. "A review of focused ion beam applications in microsystem technology". In: *Journal of Micromechanics and Microengineering* 11.4 (2001), p. 287. URL: http://stacks.iop.org/0960-1317/11/i=4/a=301.

[73] M. Alam. "SILC as a measure of trap generation and predictor of TBD in ultrathin oxides". In: *Electron Devices, IEEE Transactions on* 49.2 (2002), pp. 226–231. ISSN: 0018-9383. DOI: 10.1109/16.981211.

[74] J. D. Casey, M. Phaneuf, C. Chandler, M. Megorden, K. E. Noll, R. Schuman, T. J. Gannon, A. Krechmer, D. Monforte, N. Antoniou, N. Bassom, J. Li, P. Carleson, and C. Huynh. "Copper device editing: Strategy for focused ion beam milling of copper". In: *Journal of Vacuum Science & Technology B* 20.6 (2002), pp. 2682–2685. DOI: 10.1116/1.1521736.

[75] W. Lukaszek. "Use of EEPROM-based sensors in investigating physical mechanisms responsible for charging damage". In: *Reliability Physics Symposium Proceedings, 2002. 40th Annual*. 2002, pp. 346–353. DOI: 10.1109/RELPHY.2002.996658.

[76] J. Orloff, L. Swanson, and M. Utlaut. *High Resolution Focused Ion Beams: FIB and its Applications*. Springer, 2002, p. 304. ISBN: 978-1-4615-0765-9.

[77] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld. "Physical one-way functions". In: *Science* 297.5589 (2002), pp. 2026–2030.

[78] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi. "The EM Side-Channel(s)". In: *Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems*. CHES '02. London, UK, UK: Springer-Verlag, 2003, pp. 29–45. ISBN: 3-540-00409-2. URL: http://dl.acm.org/citation.cfm?id=648255.752713.

[79] M. Burgmair, H.-P. Frerichs, M. Zimmer, M. Lehmann, and I. Eisele. "Field effect transducers for work function gas measurements: device improvements and comparison of performance". In: *Sensors and Actuators B: Chemical* 95.1–3 (2003). Selected Papers from Eurosensors {XVI}, pp. 183–188. ISSN: 0925-4005. DOI: 10.1016/S0925-4005(03)00412-X.

[80] J.-D. Lee, J.-H. Choi, D. Park, and K. Kim. "Degradation of tunnel oxide by FN current stress and its effects on data retention characteristics of 90 nm NAND flash memory cells". In: *Reliability Physics Symposium Proceedings, 2003. 41st Annual. 2003 IEEE International*. 2003, pp. 497–501. DOI: 10.1109/RELPHY.2003.1197798.

[81] E. Ogawa, J. Kim, G. Haase, H. Mogul, and J. McPherson. "Leakage, breakdown, and TDDB characteristics of porous low-k silica-based interconnect dielectrics". In: *Reliability Physics Symposium Proceedings, 2003. 41st Annual. 2003 IEEE International*. 2003, pp. 166–172. DOI: 10.1109/RELPHY.2003.1197739.

[82] P. Riehl, K. Scott, R. Muller, R. Howe, and J. Yasaitis. "Electrostatic charge and field sensors based on micromechanical resonators". In: *Microelectromechanical Systems, Journal of* 12.5 (2003), pp. 577–589. ISSN: 1057-7157. DOI: 10.1109/JMEMS.2003.818066.

[83] S. P. Skorobogatov and R. J. Anderson. "Optical Fault Induction Attacks". In: *Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems*. CHES '02. London, UK, UK: Springer-Verlag, 2003, pp. 2–12. ISBN: 3-540-00409-2.

[84] Y. Tsividis. *Operation and Modeling of the MOS Transistor*. 2nd. Oxford University Press, 2003. ISBN: 0195170148.

[85] H.-G. Wagemann and T. Schönauer. *Silizium-Planartechnologie*. Teubner, 2003. ISBN: 978-3519004677.

[86] D. Barton, E. Cole Jr., and K. Bernhard-Höfer. "Flip Chip and 'Backside' Sample Preparation Techniques". In: *Microelectronics Failure Analysis - Desk Reference Fifth Edition*. ASM International, 2004, pp. 42–48.

[87] F. Beaudoin, R. Desplates, P. Perdu, and C. Boit. "Principles of Thermal Laser Stimulation Techniques". In: *Microelectronics Failure Analysis - Desk Reference Fifth Edition*. ASM International, 2004, pp. 417–425.

[88] R. Gennaro, A. Lysyanskaya, T. Malkin, S. Micali, and T. Rabin. "Algorithmic Tamper-Proof (ATP) Security: Theoretical Foundations for Security against Hardware Tampering". In: *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*. Vol. 2951. Lecture Notes in Computer Science. Springer, 2004, pp. 258–277. DOI: 10.1007/978-3-540-24638-1_15.

[89] K. Hooghan. "Focused Ion Beam (FIB) Systems: A Brief Overview". In: *Microelectronics Failure Analysis: Desk Reference*. 5th ed. ASM International, 2004. ISBN: 0-87179-804-3.

[90] L. A. Giannuzzi, B. I. Prenitzer, and B. W. Kempshall. *Introduction to Focused Ion Beams. Instrumentation, Theory, Techniques and Practice*. Ed. by L. A. Giannuzzi and F. A. Stevie. 2005. Chap. 2 Ion-Solid Interactions. DOI: 10.1007/b101190.

[91] A. Glowacki and C. Boit. "Characterization of thermoelectric devices in ICs as stimulated by a scanning laser beam". In: *Reliability Physics Symposium, 2005. Proceedings. 43rd Annual. 2005 IEEE International*. 2005, pp. 450–457. DOI: 10.1109/RELPHY.2005.1493127.

[92] G. S. Haase, E. T. Ogawa, and J. W. McPherson. "Reliability analysis method for low-k interconnect dielectrics breakdown in integrated circuits". In: *Journal of Applied Physics* 98.3, 034503 (2005). DOI: 10.1063/1.1999028.

[93] S. Henzler, T. Nirschl, M. Eireiner, E. Amirante, and D. Schmitt-Landsiedel. "Making Adiabatic Circuits Attractive for Todays VLSI Industry by Multimode Operation-adiabatic Mode Circuits". In: *Proceedings of the 2Nd Conference on Computing Frontiers*. CF '05. Ischia, Italy: ACM, 2005, pp. 414–420. ISBN: 1-59593-019-1. DOI: 10.1145/1062261.1062331.

[94] S. Lombardo, J. Stathis, B. Linder, K. L. Pey, F. Palumbo, and C.-H. Tung. "Dielectric breakdown mechanisms in gate oxides". In: *Journal of Applied Physics* 98.12 (2005). DOI: 10.1063/1.2147714.

[95] R. Schlangen, U. Kerst, A. Kabakow, and C. Boit. "Electrical Performance Evaluation of FIB Edited Circuits through Chip Backside Exposing Shallow Trench Isolations". In: *Microelectronics Reliability* 45.9-11 (2005), pp. 1544–1549.

[96] T. Tille and D. Schmitt-Landsiedel. *Mikroelektronik. Halbleiterbauelemente und deren Anwendung in elektronischen Schaltungen*. Springer, 2005. ISBN: 3-540-20422-9.

[97] B. Wang, Y. Ma, R. Paulsen, C. Diorio, and T. Humes. "Measurement of ultralow gate tunneling currents using floating-gate integrator technique". In: *Electron Device Letters, IEEE* 26.5 (2005), pp. 329–331. ISSN: 0741-3106. DOI: 10.1109/LED.2005.846588.

[98] M. Alam. "A Review of New Characterization Methodologies of Gate Dielectric Breakdown and Negative Bias Temperature Instability". In: *Physical and Failure Analysis of Integrated Circuits, 2006. 13th International Symposium on the*. 2006, pp. 25–32. DOI: 10.1109/IPFA.2006.250990.

[99] R. Anderson, M. Bond, J. Clulow, and S. Skorobogatov. "Cryptographic Processors-A Survey". In: *Proceedings of the IEEE* 94.2 (2006), pp. 357–369. ISSN: 0018-9219. DOI: 10.1109/JPROC.2005.862423.

[100] C. DeNardi, R. Desplats, and P. Perdu. "Direct Measurements of Charge in Floating Gate Transistor Channels of Flash Memories Using Scanning Capacitance Microscopy". In: *Proceedings of the 32nd International Symposium for Testing and Failure Analysis (ISTFA 2006)*. ASM International, 2006, pp. 86–93.

[101] C. DeNardi, R. Desplats, P. Perdu, J.-L. Gauffier, and C. Guérin. "Descrambling and data reading techniques for flash-EEPROM memories. Application to smart cards". In: *Microelectronics Reliability* 46.9–11 (2006). Proceedings of the 17th European Symposium on Reliability of Electron Devices, Failure Physics and Analysis. Wuppertal, Germany 3rd–6th October 2006, pp. 1569–1574. ISSN: 0026-2714. DOI: 10.1016/j.microrel.2006.07.022.

[102] J. Morgan, J. Notte, R. Hill, and B. Ward. "An Introduction to the Helium Ion Miscroscope". In: *Microscopy Today* 14 (4 2006), p. 24.

[103] R. Schlangen, R. Leihkauf, U. Kerst, and C. Boit. "Functional IC Analysis Through Chip Backside With Nano Scale Resolution - E-Beam Probing in FIB Trenches to STI Level". In: *Proceedings of the 32nd International Symposium for Testing and Failure Analysis (ISTFA 2006)*. ASM International, 2006, pp. 376–381.

[104] R. Schlangen, P. Sadewater, U. Kerst, and C. Boit. "Contact to contacts or silicide by use of backside FIB circuit edit allowing to approach every active circuit node". In: *Microelectronics Reliability* 46.9–11 (2006), pp. 1498–1503. ISSN: 0026-2714. DOI: 10.1016/j.microrel.2006.07.025.

[105] S. M. Sze and K. K. Ng. *Physics of Semiconductor Devices*. Wiley-Interscience, 2006.

[106] P. Tuyls, G.-J. Schrijen, B. Škorić, J. Geloven, N. Verhaegh, and R. Wolters. "Read-Proof Hardware from Protective Coatings". In: *Cryptographic Hardware and Embedded Systems - CHES 2006*. Ed. by L. Goubin and M. Matsui. Vol. 4249. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2006, pp. 369–383. ISBN: 978-3-540-46559-1. DOI: 10.1007/11894063_29.

[107] J. Guajardo, S. Kumar, G. J. Schrijen, and P. Tuyls. "FPGA intrinsic PUFs and their use for IP protection". In: *Cryptographic Hardware and Embedded Systems – CHES 2007* (2007), pp. 63–80. DOI: 10.1007/978-3-540-74735-2_5.

[108] G. Rietveld and H. van den Brom. "Vibration Reed Electrometer for Accurate Measurement of Electrical Currents Below 10 pA". In: *Instrumentation and Measurement, IEEE Transactions on* 56.2 (2007), pp. 559–563. ISSN: 0018-9456. DOI: 10.1109/TIM.2007.890792.

[109] R. Schlangen, R. Leihkauf, U. Kerst, C. Boit, R. Jain, T. Malik, K. Wilsher, T. Lundquist, and B. Kruger. "Backside E-Beam Probing on Nano scale devices". In: *Test Conference, 2007. ITC 2007. IEEE International*. 2007, pp. 1–9. DOI: 10.1109/TEST.2007.4437627.

[110] G. E. Suh and S. Devadas. "Physical unclonable functions for device authentication and secret key generation". In: *Proceedings of the 44th annual Design Automation Conference*. DAC '07. San Diego, California: ACM, 2007, pp. 9–14. ISBN: 978-1-59593-627-1. DOI: 10.1145/1278480.1278484.

[111] C. A. Volkert and A. M. Minor. "Focused Ion Beam Microscopy and Micromachining". In: *MRS Bulletin* 32 (05 2007), pp. 389–399. ISSN: 1938-1425. DOI: 10.1557/mrs2007.62.

[112] K. Nishiguchi, C. Koechlin, Y. Ono, A. Fujiwara, H. Inokawa, and H. Yamaguchi. "Single-Electron-Resolution Electrometer Based on Field-Effect Transistor". In: *Japanese Journal of Applied Physics* 47.11R (2008), p. 8305. URL: http://stacks.iop.org/1347-4065/47/i=11R/a=8305.

[113] L. Sauvage, S. Guilley, J.-L. Danger, Y. Mathieu, and M. Nassar. "Successful Attack on an FPGA-based Automatically Placed and Routed WDDL+ Crypto Processor." 2008. URL: https://hal.archives-ouvertes.fr/hal-00339858.

[114] H. Schmid. In: CRC Press, 9, 2008. Chap. Offset, Flicker Noise, andWays to Deal with Them, pp. 95–115. ISBN: 978-1-4200-7062-0. DOI: 10.1201/9781420070637.pt2.

[115] Y. Su, J. Holleman, and B. Otis. "A Digital 1.6 pJ/bit Chip Identification Circuit Using Process Variations". In: *Solid-State Circuits, IEEE Journal of* 43.1 (2008), pp. 69–77. ISSN: 0018-9200. DOI: 10.1109/JSSC.2007.910961.

[116] Y. Zhu, J. E. .-.-Y. Lee, and A. Seshia. "A Resonant Micromachined Electrostatic Charge Sensor". In: *Sensors Journal, IEEE* 8.9 (2008), pp. 1499–1505. ISSN: 1530-437X. DOI: 10.1109/JSEN.2008.923597.

[117] C. Helfmeier. "Entwicklung und Optimierung einer Vorgehensweise, um mittels eines "Focused Ion Beam"-Gerätes auf "Floating Gate"-Technologie basierende Permanent-Speicherzellen vollständig und zerstörungsfrei zu kontaktieren." MA thesis. Technische Universität Berlin, FG Halbleiterbauelemente, Aug. 6, 2009.

[118] D. Holcomb, W. Burleson, and K. Fu. "Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers". In: *Computers, IEEE Transactions on* 58.9 (2009), pp. 1198–1210. ISSN: 0018-9340. DOI: 10.1109/TC.2008.212.

[119] U. Rührmair, J. Sölter, and F. Sehnke. *On the Foundations of Physical Unclonable Functions*. 10, 2009.

[120] S. Skorobogatov. "Using Optical Emission Analysis for Estimating Contribution to Power Analysis". In: *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2009 Workshop on*. 2009, pp. 111–119. DOI: 10.1109/FDTC.2009.39.

[121] *SLE 66CLX126 PE (M/S) – 8/16-bit High Security Dual Interface Controller for Contact based and Contactless Applications in* 0.22 µm *CMOS Technology*. Infineon. Mar. 2009. URL: http://www.infineon.com/dgdl?folderId=db3a30431b3e89eb011bdf5adad97c2d&fileId=db3a30431f848401011ff02a5549492d (visited on 04/29/2014).

[122] R. J. Anderson. "Security Engineering". In: *A Guide to Building Dependable Distributed Systems*. Wiley, 2010, p. 1080.

[123] T. Breuer, U. Kerst, C. Boit, E. Langer, and H. Ruelke. "Ultra-low-κ porous SiCOH dielectric degradation process before breakdown". In: *Physical and Failure Analysis of Integrated Circuits (IPFA), 2010 17th IEEE International Symposium on the*. 2010, pp. 1–6. DOI: 10.1109/IPFA.2010.5532240.

[124] H. Busch, M. Sotáková, S. Katzenbeisser, and R. Sion. "The PUF Promise". In: *Trust and Trustworthy Computing*. Ed. by A. Acquisti, S. Smith, and A.-R. Sadeghi. Vol. 6101. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2010, pp. 290–297. ISBN: 978-3-642-13868-3. DOI: 10.1007/978-3-642-13869-0_21.

[125] M. Noras. "Electric Field Sensor Based on a Varactor Diode/MIS/MOS Structure". In: *Industry Applications Society Annual Meeting (IAS), 2010 IEEE*. 2010, pp. 1–3. DOI: 10.1109/IAS.2010.5614485.

[126] R. Schlangen. "Development and Evaluation of Novel Chip Modification- and Analysis-Techniques, based on Backside Focused Ion Beam Preparation". PhD thesis. 2010.

[127] C. Tarnovsky. "Hacking the Smartcard Chip". In: *Blackhat DC 2010*. Arlington, VA, 2010.

[128] *4200-SCS Semiconductor Characterization System Technical Data*. Rev M. Keithley Instruments Inc. 2011.

[129] F. Armknecht, R. Maes, A. Sadeghi, F.-X. Standaert, and C. Wachsmann. "A Formalization of the Security Features of Physical Functions". In: *Security and Privacy (SP), 2011 IEEE Symposium on*. 2011, pp. 397–412. DOI: 10.1109/SP.2011.10.

[130] C. Goupil, W. Seifert, K. Zabrocki, E. Müller, and G. J. Snyder. "Thermodynamics of Thermoelectric Phenomena and Applications". In: *Entropy* 13.8 (2011), pp. 1481–1517. ISSN: 1099-4300. DOI: 10.3390/e13081481.

[131] R. Young, C. Rue, S. Randolph, C. Chandler, G. Franz, R. Schampers, A. Klumpp, and L. Kwakman. "A Comparison of Xenon Plasma FIB Technology with Conventional Gallium LMIS FIB: Imaging, Milling, and Gas-Assisted Applications". In: *Microscopy and Microanalysis* 17 (Supplement S2 2011), pp. 652–653. ISSN: 1435-8115. DOI: 10.1017/S1431927611004132.

[132] C. Helfmeier, C. Boit, and U. Kerst. "On charge sensors for FIB attack detection". In: *Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on*. 2012, pp. 128–133. DOI: 10.1109/HST.2012.6224332.

[133] *ATMega328p Datasheet*. Atmel Corporation. 2012.

[134] T. Breuer, U. Kerst, C. Boit, E. Langer, H. Ruelke, and A. Fissel. "Conduction and material transport phenomena of degradation in electrically stressed ultra low-k dielectric before breakdown". In: *Journal of Applied Physics* 112.12, 124103 (2012), p. 124103. DOI: 10.1063/1.4768918.

[135] T. Breuer. *Untersuchung der Degradation von elektrisch gestresstem nano- porösem ultra low-k Dielektrikum vor dem elektrischen Durchschlag*. 2012.

[136] I. N. Bronstein, K. A. Semedjajew, G. Musiol, and H. Mühlig. *Taschenbuch der Mathematik*. 8th ed. 2012. ISBN: 978-3-8171-2008-6. URL: http://d-nb.info/1024545725.

[137] S. Katzenbeisser, Ü. Kocabaş, V. Rožić, A. Sadeghi, I. Verbauwhede, and C. Wachsmann. "PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon". In: *Cryptographic Hardware and Embedded Systems–CHES 2012* (2012), pp. 283–301.

[138] H. Kim, V. Rozic, and I. Verbauwhede. "Three Phase Dynamic Current Mode Logic: A More Secure DyCML to Achieve a More Balanced Power Consumption". In: *Information Security Applications - 13th International Workshop, WISA 2012, Jeju Island, Korea, August 16-18, 2012, Revised Selected Papers*. Ed. by D. H. Lee and M. Yung. Vol. 7690. Lecture Notes in Computer Science. Springer, 2012, pp. 68–81. ISBN: 978-3-642-35415-1. DOI: 10.1007/978-3-642-35416-8_6.

[139] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J.-P. Seifert. "Simple Photonic Emission Analysis of AES". In: *Cryptographic Hardware and Embedded Systems – CHES 2012*. Ed. by E. Prouff and P. Schaumont. Vol. 7428. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2012, pp. 41–57. ISBN: 978-3-642-33026-1. DOI: 10.1007/978-3-642-33027-8_3.

[140] P. Teichmann. *Adiabatic Logic. Future Trend and System Level Perspective*. 34 vols. Springer Series in Advanced Microelectronics. Future Trend and System Level Perspective Series: Springer Series in Advanced Microelectronics, Vol. 34, 2012.

[141] C. Helfmeier, C. Boit, D. Nedospasov, and J.-P. Seifert. "Cloning Physically Unclonable Functions". In: *Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on*. 2013, pp. 1–6. DOI: 10.1109/HST.2013.6581556.

[142] C. Helfmeier, D. Nedospasov, C. Tarnovsky, J. Krissler, C. Boit, and J.-P. Seifert. "Breaking and Entering through the Silicon". In: *CCS '13: Proceedings of the 20th ACM conference on Computer and communications security*. 2013. DOI: 10.1145/2508859.2516717.

[143] *B1500A Semiconductor Device Analyzer Manual*. Agilent Technologies. Oct. 13, 2013.

[144] C. Böhm and M. Hofer. *Physical Unclonable Functions in Theory and Practice*. Springer Berlin Heidelberg, 2013. ISBN: 978-1-4614-5039-9.

[145] C. Boit, C. Helfmeier, D. Nedospasov, and A. Fox. "Ultra high precision circuit diagnosis through Seebeck generation and charge monitoring". In: *Physical and Failure Analysis of Integrated Circuits (IPFA), 2013 20th IEEE International Symposium on the*. 2013, pp. 17–21. DOI: 10.1109/IPFA.2013.6599119.

[146] *International Technology Roadmap for Semiconductors 2013*. Tech. rep. ITRS, 2013.

[147] M. S. Joens, C. Huynh, J. M. Kasuboski, D. Ferranti, Y. J. Sigal, F. Zeitvogel, M. Obst, C. J. Burkhardt, K. P. Curran, S. H. Chalasani, L. A. Stern, B. Goetze, and J. A. J. Fitzpatrick. "Helium Ion Microscopy (HIM) for the imaging of biological samples at sub-nanometer resolution". In: *Sci. Rep.* 3 (17, 2013). Article. DOI: 10.1038/srep03514.

[148] D. Nedospasov, C. Helfmeier, J.-P. Seifert, and C. Boit. "Invasive PUF Analysis". In: *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on*. 2013, pp. 30–38. DOI: 10.1109/FDTC.2013.19.

[149] *NXP Strengthens SmartMX2 Security Chips with PUF Anti-Cloning Technology*. NXP Semiconductors N.V. 2013.

[150] G. Rietveld. "Vibrating Reed Electrometer With Attocoulomb Charge Resolution and Subattoampere Current Resolution". In: *Instrumentation and Measurement, IEEE Transactions on* 62.1 (2013), pp. 192–198. ISSN: 0018-9456. DOI: 10.1109/TIM.2012.2212509.

[151] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J.-P. Seifert. "Simple photonic emission analysis of AES". In: *Journal of Cryptographic Engineering* 3.1 (2013), pp. 3–15. ISSN: 2190-8508. DOI: 10.1007/s13389-013-0053-7.

[152] C. Helfmeier, C. Boit, D. Nedospasov, S. Tajik, and J.-P. Seifert. "Physical vulnerabilities of Physically Unclonable Functions". In: *Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014*. 2014, pp. 1–4. DOI: 10.7873/DATE.2014.363.

[153] C. Helfmeier, R. Schlangen, and C. Boit. "Focused ion beam contact to non-volatile memory cells". In: *Microelectronics Reliability* 54.9–10 (2014). ESREF 2014, pp. 1798–1801. ISSN: 0026-2714. DOI: 10.1016/j.microrel.2014.07.017.

[154] G. Hlawacek, V. Veligura, R. van Gastel, and B. Poelsema. "Helium ion microscopy". In: *Journal of Vacuum Science & Technology B* 32.2, 020801 (2014). DOI: 10.1116/1.4863676.

[155] D. Holcomb and K. Fu. "Bitline PUF: Building Native Challenge-Response PUF Capability into Any SRAM". In: *Cryptographic Hardware and Embedded Systems – CHES 2014*. Ed. by L. Batina and M. Robshaw. Vol. 8731. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2014, pp. 510–526. ISBN: 978-3-662-44708-6. DOI: 10.1007/978-3-662-44709-3_28.

[156] N. Semiconductors. *SmartMX2 P40 family P40C012/040/072 Secure smart card controller*. http://www.nxp.com/documents/short_data_sheet/P40C040_C072_SMX2_FAM_SDS.pdf. Datasheet. 2014.

[157] I. I. B. V. *Intrinsic ID – Solutions to Secure Your Digital Life*. Product Brochure. 2014.

[158] S. Research. *SR570 Low-Noise Current Preamplifier*.

[159] J. Lloyd, M. Lane, X.-H. Liu, E. Liniger, T. Shaw, C.-K. Hu, and R. Rosenberg. "Reliability Challenges with Ultra-Low k Interlevel Dielectrics". In: *Microelectronics Reliability* 44.9–11 (2004). 15th European Symposium on Reliability of Electron Devices, Failure Physics and Analysis, pp. 1835–1841. ISSN: 0026-2714. DOI: 10.1016/j.microrel.2004.07.094.