Nano Security:
From Nano-Electronics to Secure Systems

Ilia Polian[1], Frank Altmann[2], Tolga Arul[3], Christian Boit[4], Ralf Brederlow[5], Lucas Davi[6], Rolf Drechsler[7], Nan Du[8], Thomas Eisenbarth[9], Tim Güneysu[10], Sascha Hermann[11], Matthias Hiller[12], Rainer Leupers[13], Farhad Merchant[13], Thomas Mussenbrock[14], Stefan Katzenbeisser[3], Akash Kumar[15], Wolfgang Kunz[16], Thomas Mikolajick[17], Vivek Pachauri[18], Jean-Pierre Seifert[19], Frank Sill Torres[20], Jens Trommer[17]

[1]Institute of Computer Engineering and Computer Architecture, University of Stuttgart, [4]Fraunhofer Institute for Microstructure of Materials and Systems (IMWS), Halle, [3]Chair of Computer Engineering, University of Passau, [4]Institute for Radio-Frequency and Semiconductor Technologies, TU Berlin, [5]Chair for Circuit Design, TU Munich, [6]Secure Software Systems Group, University Duisburg-Essen, [7]Computer Architecture Group, University of Bremen, [8]Material Systems and Nanoelectronics Group, TU Chemnitz, [9]Institute for IT Security, University of Lübeck, [10]Secure Hardware Group, Ruhr-University of Bochum, [11]Center for Microtechnologies, TU Chemnitz, [12]Fraunhofer Institute for Applied and Integrated Security, [13]Institute for Communication Technologies and Embedded Systems, RWTH Aachen University, [14]Chair of Plasma Technology, Ruhr University Bochum, [15]Chair for Processor Design, TU Dresden, [16]Chair for Electronic Design Automation, TU Kaiserslautern, [17]NamLab gGmbH, Dresden, [18]Institute of Materials in Electrical Engineering 1, RWTH Aachen University, [19]Chair for Security in Telecommunications, TU Berlin, [20]Department for Resilience of Maritime Systems, DLR Bremerhaven (all affiliations are in Germany)

***Abstract*—The field of computer hardware stands at the verge of a revolution driven by recent breakthroughs in emerging nano-devices. "Nano Security" is a new Priority Program recently approved by DFG, the German Research Council. This initial-stage project initiative at the crossroads of nano-electronics and hardware-oriented security includes 11 projects with a total of 23 Principal Investigators from 18 German institutions. It considers the interplay between security and nano-electronics, focusing on a dichotomy which emerging nano-devices (and their architectural implications) have on system security. The projects within the Priority Program consider both: potential security threats and vulnerabilities stemming from novel nano-electronics, and innovative approaches to establishing and improving system security based on nano-electronics. This paper provides an overview of the Priority Program's overall philosophy and discusses the scientific objectives of its individual projects.**

I. Introduction

Recent spectacular cyber-attacks have shown the vulnerability of many electronic systems today's societies are relying on. While the need to protect existing and upcoming systems against such attacks is clear, most of the available cyber-defenses focus on their software part or communication links. However, an increasing number of reported attacks target the system's hardware modules directly, thus outmaneuvering software-level security mechanisms [1]. With the ongoing change from the conventional nanoscale CMOS technology to radically new emerging nano-devices, completely new and little-understood security challenges arise [2]. Among such devices are memristors, spintronics and carbon nanotubes. Their new properties, such as hysteresis and non-volatility, improve energy efficiency, computing power and performance of such devices. They keep the exponential scaling of integration density intact and give rise to novel neuromorphic, approximate, in- and near-memory computer architectures. The same features that create new possibilities to improve security (e.g., by straightforward implementations of stateful cryptographic functions [3] or neuromorphic anomaly-detection modules) also raise doubts about new types of hardware-related attacks.

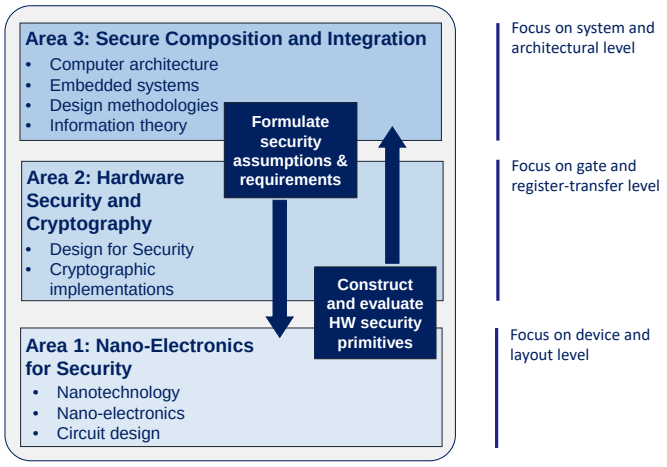

Fig. 1: Overview of the Priority Program *Nano Security*.

Nano Security is a national Priority Program funded by the DFG (German Research Council). A Priority Program is a coordinated multi-partner initiative where individual research projects are selected based on a topic-specific call by an independent panel for the duration of three years, with a possibility of extension for further three years. Priority Programs focus on fundamental scientific research; therefore, most participants are usually in Universities and other academic institutions. Priority Programs are selected by the DFG Senate from a set initiatives proposed by researchers.

The cornerstone of the Priority Program's philosophy is to achieve interdisciplinary collaboration among the researchers who work across traditional levels of abstraction. To this end, *Nano Security* is organized in a matrix structure with three areas and three interdisciplinary groups (IGs). The three areas, shown in Figure 1, bundle scientists from disciplines with a focus on a certain abstraction level. Area 1 "Nano-

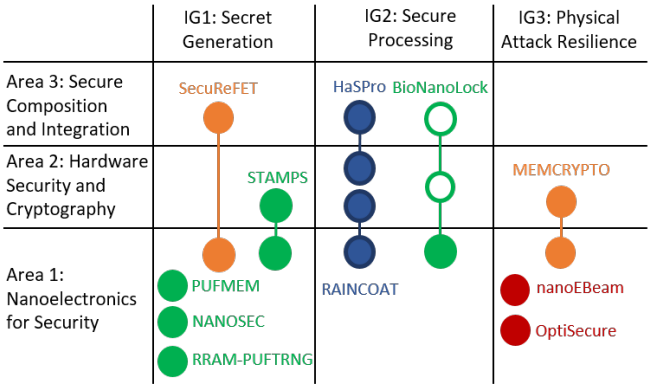

Fig. 2: Attribution of projects to areas and interdisciplinary groups (yellow: technology-oriented; red: attack-oriented; green: primitive-oriented; blue: architecture-oriented projects).

electronics for Security" focuses on developing and analyzing nano-electronic security primitives. Area 2 "Hardware Security and Cryptography" assesses and systematically improves the security of both: hardware primitives originating from Area 1 and architectures, protocols and design methods coming from Area 3; it serves as an intermediary between the other two areas. Finally, Area 3 "Secure Composition and Integration" deals with the integration of secure primitives into larger systems and architectures. It aims at answering the question under which circumstances the security guarantees defined and validated for lower-level primitives translate in higher-order, system- and architecture-level security properties.

The main mode of collaboration across the abstraction levels is indicated in the Figure 1: The joint activities in the Areas 1 and 2 will result in *hardware security primitives* with well-characterized security properties, which can be used to obtain security guarantees for systems and architectures in Area 3. When doing this, Area 3, together with Area 2, will formulate *security requirements,* which the hardware primitives should ideally fulfill. Area 1 will create such primitives and, together with Area 2, assess their real properties; the collaborative task consists of bringing these lower-level properties together with higher-level requirements from Area 3. To achieve this vertical integration, the SPP includes *Interdisciplinary Groups* (IGs) defined across the main challenges for hardware trust anchors, i.e. secure secret key storage, secure information processing, and physical attack resistance.

Figure 2 shows the 11 projects of the Priority Program attributed to areas and IGs. Many of the projects are *tandem projects* where two (or more) partners from different areas work together on an interdisciplinary research topic.

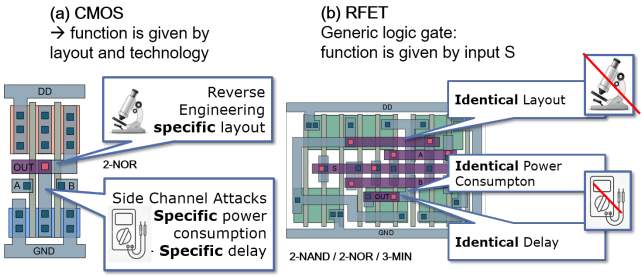

Fig. 3: (a) Attack modes in CMOS technology and (b) safety features in RFET technology.

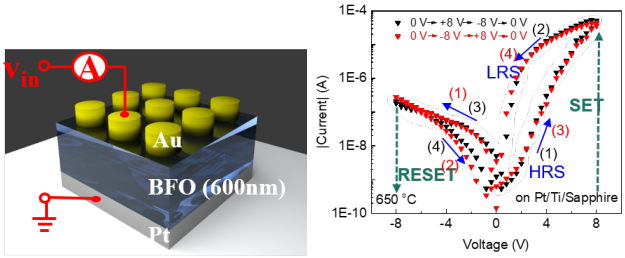

Fig. 4: BFO memristive device and its electrical behavior

In the following, the individual projects are described in more detail. While a project can be attributed to multiple areas and IGs, the following sections structure the project portfolio based on whether a project is mainly driven by a certain nano-technology, by a specific attack scenario, by a concrete hardware security primitive, or by architectural questions (color coded in Figure 2).

II. Technology-oriented Projects

A. SecuReFET: Secure Circuits through inherent Reconfigurable Field Effect Transistors

Reconfigurable Field Effect Transistors (RFETs) are a new class of device, which merge the functionality of classical p-type and n-type MOSFETs in a single element [4]. The runtime-reconfigurable nature of those nanoelectronic devices yields an inherent polymorphic functionality at the logic gate level [5]. As a result, circuits made of regular RFET blocks are able to provide a large number of possible functional combinations based on the apparently same circuit representation. The manufacturers, therefore, are able to program the desired functionality after chip production. The actual circuit or function remains hidden since they cannot be differentiated from other possible combinations by physical reverse engineering. In addition the inherent symmetry of their underlying device characteristics [6] will prevent electrical monitoring of the circuit, i.e. side-channel attacks (Figure 3). RFETs thus provide a promising option to fight against hardware-level attacks in future electronic system, by applying them to camouflage integrated circuit designs or provide Physically Unclonable Functions (PUFs) and encryption shemes [7]. In turn, there are also potential security threats stemming from the reconfigurable nature of the technology, such as hardware Trojans. Measures to mitigate those vulnerabilities by the circuit as well as device design have to be established.

SecuReFET approaches these questions by lab scale logic cell fabrication as well as analysis regarding their security benefits and vulnerabilities. Further, it aims at providing an automated design-synthesis environment (EDA) for logic and physical design of RFET circuits based on modified modern design rules. This should pave the way for the application of this emerging nanotechnology in hardware security.

B. MemCrypto: Towards Secure Electroforming-free Memristive Cryptographic Implementations

Memristive devices have attracted large interest for construction of non-volatile memories [8] and neuromorphic primitives [9], but also for security. MemCrypto aims at pushing the use of memristive technologies beyond the ongoing work on

physical unclonable functions [10], [11] and random number generators [12], namely to realization of complete cryptographic circuits. It has three main goals: physical realization of simplified cryptographic circuits; protection of such circuits against physical attacks; and development of simulation models and procedures for pre-fabrication security analysis.

For the first goal, novel electroforming-free $BeFeO_3$ (or BFO) memristive devices [13] (Figure 4) will be fabricated using pulse laser deposition and connected to form cryptographic primitives. The consideration of physical attacks will focus on identifying side-channel [14] and fault-injection [15] attack mechanisms that are not present in the traditional CMOS technology, e.g., new channels of information leakage based on effects of memristance and non-volatility. A central question is whether such attacks necessitate new types of countermeasures beyond the ones used in conventional CMOS. With regard to simulation, MemCrypto aims at improving electrical-level models to accurately assess security of a memristive component, but also to develop mixed-level simulation procedures [16] that can be applied to medium-size cryptographic circuit.

III. Attack-oriented Projects

A. nanoEBeam: E Beam Probing for backside attacks against nanoscale ICs

The extraction of data from integrated circuits (ICs) can pose a serious threat to the secrets and intellectual property (IP) used within. This access allows the attacker to reverse-engineer the design and thus counterfeit and overbuild the target products, or misuse sensitive information. Currently, the most successful attacks are performed through optical techniques for IC signal tracking and defect localization, which are strongly challenged by the miniaturization of technology nodes below 10nm. They require complex access strategies such as sophisticated chip substrate thinning down to the μm range [17].

In this project, novel physical side-channel attack strategies based on electron beams via E-Beam Probing from the chip backside are to be tested on appropriate highly integrated modern circuits. E-Beam probing enables the imaging of electrical potentials via the potential contrast of the detected secondary electrons in the scanning electron microscope (SEM). E-Beam probing through the silicon substrate from the chip backside has already been demonstrated for 120nm technologies [18]. In addition, the successful application for fault localization has recently been demonstrated on a 10nm-node FinFET technology [19].

Conduction of fundamental research of this approach as a potential IC attack technique particularly to nanotechnology is therefore urgently required. Due to the achievable local resolution in the nanometer range, which is considerably improved compared to existing optical techniques, the risk of novel attack scenarios arises. In this research, e-beam-based attack strategies in combination with novel FIB preparation strategies for precise backside access to functional IC structures on modern 10nm chip technologies will be investigated and compared with previously established optical methods. IC attacks with these techniques are currently unknown.

B. OptiSecure: Securing Nano-Circuits against Optical Probing

Optical probing techniques like Laser Voltage Imaging (LVI) and Laser Voltage Probing (LVP) enable the localization

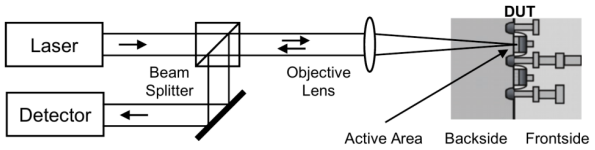

Fig. 5: Optical probing signal acquisition (simplified)

of transistors switching with a specific frequency as well as probing the state of transistors. In both cases, photons from a laser probing source enter the backside of the silicon backside of the device under test (DUT) (Figure 5). The light is partially absorbed in the silicon and partially reflected at, for instance, the lowest metal layer. Phase and amplitude of the reflected light are modulated by the electrical signal at a node, which can be measured at a detector.

Consequently, optical probing enables the contactless extraction of information from integrated nano-circuits, which also includes secure applications as has been shown in several works [20]. For example, Tajik et al. reported in [21] an attack on the bitstream encryption scheme of a FPGA manufactured in 28nm technology, where the authors could show that the plaintext data containing sensitive design information and intellectual property can be extracted. Despite the severe implications of this type of passive attack, no relevant countermeasures are being deployed so far. This shortcoming forms the motivation of this project, which aims at investigating methods that enable the protection of future integrated nano-circuits against optical probing attacks.

To this end, a technology model for the exploration of the relation between geometrical characteristics of the integrated devices and its susceptibility to optical probing attacks shall be derived [22], [23]. At the same time, it shall be investigated how alternative logic styles and design methodologies can contribute as countermeasures against this kind of passive attack [24]. Furthermore, new kinds of similar optical attacks shall be developed and evaluated in terms of its threat potential. Finally, several test structures and its hardened counterparts shall be integrated in a physical circuit and extensively tested.

IV. Security Primitive-oriented Projects

A. STAMPS: From Strain to Trust: tAMper aware silicon PufS

Integrated circuits have a unique internal and external physical state. While PUFs on circuit level typically address the intrinsic variation, STAMPS evaluates the physical strain as immediate surrounding of an IC. This allows to detect physical tampering which is necessary beforehand to perform invasive and semi-invasive attacks, such as localized EM attack [25] or laser fault injection, as shown in Figure 6. In addition, the soldering process leaves a unique thermal fingerprint that could allow to detect if a chips was removed and reapplied.

An often underestimated problem with analog performance of circuits is related to the mechanical deformation of the silicon circuit in a package [26]. It is to be expected that deformation is another dimension of challenges for the physical state of the integrated circuit – similar in effect to what we already know from supply voltage and temperature related shifts in physical properties of the integrated circuit. Applying techniques for measuring strain [27] and temperature to make use of this information in an analog PUF generation circuit

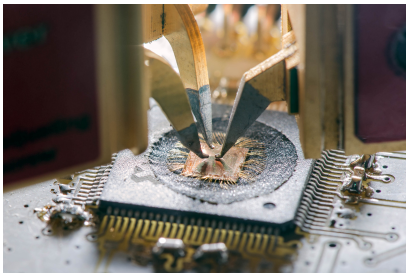

Fig. 6: Localized EM attack on a decapsulated IC

may allow a better reliability of the secret with respect to the security application needs.

The physical fingerprint of the strain sensor will be evaluated as PUF to protect the secrets inside a system, and the tampering will destroy this secret. This requires an analog and a system design tailored to the approach [28]. A tamper-sensitive error correction scheme, building upon [29], will be designed and the quality of the fingerprint will be assessed.

B. PUFMem: Intrinsic Physical Unclonable Functions from Emerging Non-Volatile Memories

The integration density of circuits is approaching a scaling limit, where structures become so small that the saved information are hard to retrieve. This development brings novel non-volatile memory (NVM) types such magnetoresistive (MRAM), resistive (ReRAM) and ferroelectric (FRAM) random access memory to the scene. PUFMem investigates the realization and characterization of intrinsic PUFs on the aforementioned NVM types in a systematic manner.

As PUFs from conventional memories are susceptible to varying environmental conditions such as temperature, supply voltage, etc., PUF instances on NVMs will additionally be characterized while subject to these conditions. To counteract undesired effects, advanced techniques such as protocols, error correcting codes, stochastic models etc. will be applied, to improve PUF quality and resilience to influences from the environment. In particular when used as random access memory in present-day computers, credentials and results of cryptographic operations are directly accessible on NVMs due to their inherent storage properties. PUFMem plans to overcome this drawback by employing self-encryption, where the same NVM is used for two different purposes: as a memory to store data and as a PUF for retrieving the key to encrypt the same data.

C. NANOSEC: Tamper-Evident PUFs based on Nanostructures for Secure and Robust Hardware Security Primitives

Carbon nanotubes (CNT) and concomitant integration technologies provide a promising alternative for PUF realization. Nondeterministic nanodevice properties, high sensitivity to environmental changes as well as additive technologies give new degrees of freedom for device design and security. With respect to compatibility with CMOS technology, a high maturity level on nanotechnology boast with CNT-based energy efficient sub-10 nm transistors [30], record speed NRAM storage devices [31] or analog high performance RF transistors [32]. Thus, a combination of outstanding properties and post-CMOS integration capabilities prospect low-footprint, low-cost, low-energy security primitives [33], [34] as well as additional functionality with the same technology.

In NanoSec CNT-based PUFs are investigated targeting primitives that feature high entropy and robustness along with inherent tamper-evidence capabilities. By further exploring important security characteristics like error correction, reliability, and tamper-evidence mechanisms of CNT-based PUFs, novel insights regarding the applicability for forthcoming system integration technologies are sought to be achieved. Different device designs which internalize multibit functionality as well as tamper-evidence are pursued. The realized PUFs will be subjected to an in depth analysis exposing suitable error correction models to enable the extraction of stable PUF responses. Further studies will explore inherent tamper-evidence features of the CNTs, resulting in an increased security against invasive and noninvasive attacks.

D. RRAM-PUFTRNG: CMOS-compatible RRAM-based structures for the implementation of Physical Unclonable Functions (PUF) and True Random Number Generators (TRNG)

Resistive Random Access Memories (RRAM) have emerged in the last years as promising candidates in the field of Non-Volatile Memories (NVM). The mechanisms behind switching operations in RRAM devices are intrinsically stochastic. Therefore, RRAM technology has started recently to be considered as a suitable solution to implement the Physical Unclonable Functions (PUF) and True Random Number Generators (TRNG), which are are two components widely used nowadays to generate random bit streams in security applications.

The study proposed in this project involves interdisciplinary research in order to achieve three main targets: i) studying in detail the statistical distributions of the electrical parameters involved in RRAM switching, which have been typically identified as a source of randomness, ii) figuring out how the correlations which avoid the true randomness emerge from fundamental physical and chemical processes, and iii) development of an appropriate operative algorithm able to overcome the correlations found on the electrical parameters of RRAM devices providing the true random digital outputs required for both TRNG and PUF applications.

E. BioNanoLock: Bio-Nanoelectronic based Logic Locking for Secure Systems

The new age processor is going to require hardware-oriented solutions as a primary design criterion for the security against threats [35] [36]. Alternative computational architectures proposed in recent years drive this idea by the inclusion of multi-value logic operations. The realization of multi-value logic gates and testing the advantages of polymorphic inputs and outputs of a circuit, however, remains elusive due to the technology gap. In this project, we put forward a new logic-locking framework that will allow us incorporating multi-value and multi-layer logic with existing CMOS based logic-locking architectures. An encoded DNA sequence acts as a secret 'biological activation-key' which is molecularly recognized at a unique and secret pattern of key-gates called biological key-gates and activates them [37]. This, in turn, enables the CMOS based key-gates in logic-locked circuit with the appropriate key value [38]. Different voltage-levels in the multi-valued logic define "on" or "off" state of the key-gates adding another level of ambiguity for an attacker and making it impossible for

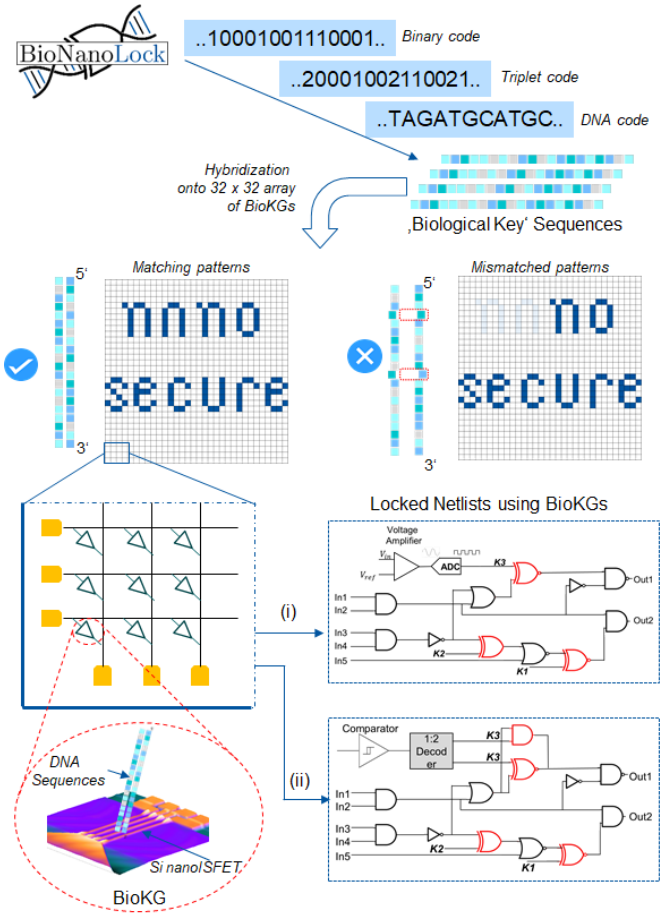

Fig. 7: BioNanoLock: a multi-layer, multi-value logic-locking by the combination of molecular level locking (biological key), device-level locking and gate-level locking.

the attacker to unlock the circuit (see Fig. 7). Enabling future-generation processors with BioNanoLock is the prime target of the project with small (10-100 logic gates) to medium-sized (100-10000 logic gates) circuits as an intermediate goal. We also envision developing heterogeneous integrated systems for secure information processing in the long-term.

V. Architecture-oriented Projects

A. RAINCOAT: Randomization in Secure Nano-Scale Microarchitectures

A large number of security problems in digital systems arise from the interfaces between hardware and software [39], [40], [41], [42]. During the last few years, attacks targeting these interfaces rapidly gained popularity and thus pose a continuously growing threat by undermining higher level security assumptions, in many cases bypassing also applied countermeasures. With increasing integration density on the hardware level and exacerbating security policies on the software level, the era of nano technology will open up new options for hardware-based attacks in the ongoing arms race between researchers and attackers.

The goal of the RAINCOAT project is the development, security analysis and evaluation of a novel randomization-augmented microarchitecture with respect to the technological challenges in nano-scale technology, including the efficient

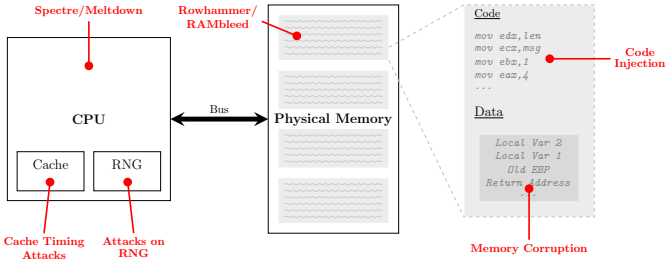

Fig. 8: Simplified overview of core components and corresponding attacks in project RAINCOAT.

generation, sharing and distribution of randomness. We therefore analyze current microarchitectural attacks such as Spectre, Meltdown and Rowhammer and port them onto emerging nano scale architectures. Figure 8 depicts the main points of interest for this project.

B. HaSPro: Verifiable Hardware Security for Out-of-Order Processors

Processor designers have started to integrate security-specific hardware (HW) features such as HW-based stack protection, execution prevention, memory encryption, cryptographic engines, and trusted execution environments (TEE) into modern processors. Processor hardware was considered a performant and reliable root-of-trust for the entire system. This changed dramatically in January 2018 when a new class of attacks known under the names of Spectre and Meltdown. These *transient execution attacks* have been particularly devastating for hardware-supported security mechanisms, that is, TEEs such as Intel SGX and ARM Trustzone. TEEs enable *secure enclaves* that are protected via additional hardware-enforced isolation—even against system-level adversaries with superuser privileges, e.g., a compromised OS. Yet, transient execution attacks have been shown to circumvent even these stronger hardware-based isolation mechanisms in current CPUs, rendering enclaves vulnerable to attacks [43], [44].

HaSPro works towards a systematic approach to detect and protect against attacks already at design time and at the HW level: by providing (I) a secure enclave environment to isolate sensitive processes from system vulnerabilities and (II) a verifiably side-channel-free processor to ensure that the logic

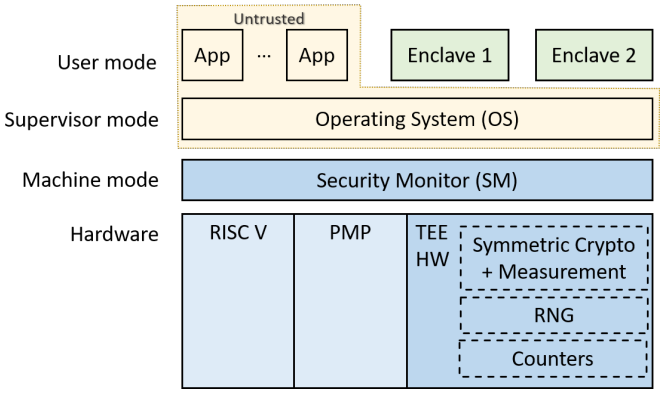

Fig. 9: Trusted execution environment (TEE) consisting of lean security monitor (in software) and verified TEE hardware

isolation of the CPU is actually effective and not undermined by HW design flaws.

The new TEE architecture, as depicted in Figure 9, will consist of a hardware layer that offers several performance-critical basic services; on top of that the security monitor, a shallow machine-mode firmware layer, will implement higher-level functionality and provide interaction with the RISC-V ISA. HW vulnerabilities will be detected systematically by a new formal approach based on Unique Program Execution Checking (UPEC) [45]. Joint research is conducted to support a compositional approach which closes security gaps by measures both at the HW and at the SW level.

VI. Conclusions

The researchers in the Priority Program "Nano Security" have identified a number of relevant scientific questions. After its start in late 2020, the program aims at making new contributions on the frontier between material science, security / cryptography, and design automation.

Acknowledgment

This work was supported by the DFG Priority Program SPP 2253 Nano Security.

References

[1] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1283–1295, 2014.

[2] J. Rajendran *et al.*, "Nano meets security: Exploring nanoelectronic devices for security applications," *Proceedings of the IEEE*, vol. 103, no. 5, pp. 829–849, 2015.

[3] Y. Zhou, Y. Li, L. Xu, S. Zhong, R. Xu, and X. Miao, "A hybrid memristor-CMOS XOR gate for nonvolatile logic computation," *Physica Status Solidi A*, vol. 213, pp. 1050–1054, 2016.

[4] T. Mikolajick, A. Heinzig, J. Trommer, T. Baldauf, and W. Weber, "The RFET—a reconfigurable nanowire transistor and its application to novel electronic circuits and systems," *Semiconductor Science and Technology*, vol. 32, no. 4, p. 043001, 2017.

[5] S. Rai, J. Trommer, M. Raitza, T. Mikolajick, W. M. Weber, and A. Kumar, "Designing efficient circuits based on runtime-reconfigurable field-effect transistors," *IEEE Trans. VLSI*, vol. 27, pp. 560–572, 2018.

[6] J. Trommer, A. Heinzig, T. Baldauf, S. Slesazeck, T. Mikolajick, and W. M. Weber, "Functionality-enhanced logic gate design enabled by symmetrical reconfigurable silicon nanowire transistors," *IEEE Transactions on Nanotechnology*, vol. 14, no. 4, pp. 689–698, 2015.

[7] A. Rupani, S. Rai, and A. Kumar, "Exploiting emerging reconfigurable technologies for secure devices," in *Euromicro DSD*, 2019, pp. 668–671.

[8] M. Chang *et al.*, "Challenges and circuit techniques for energy-efficient on-chip nonvolatile memory using memristive devices," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 5, no. 2, pp. 183–193, 2015.

[9] X. Wang, S. Joshi, S. Savel'ev *et al.*, "Fully memristive neural networks for pattern classification with unsupervised learning," *Nature Electronics*, vol. 1, no. 2, pp. 137–145, 2018.

[10] J. Rajendran, G. S. Rose, R. Karri, and M. Potkonjak, "Nano-PPUF: A memristor-based security primitive," in *ISVLSI*, 2012, pp. 84–87.

[11] G. S. Rose *et al.*, "Foundations of memristor based PUF architectures," in *IEEE/ACM Int'l Symp. Nanoscale Architectures*, 2013, pp. 52–57.

[12] H. Jiang *et al.*, "A novel true random number generator based on a stochastic diffusive memristor," *Nature Comm.*, vol. 8, no. 882, 2017.

[13] T. You, Y. Shuai, W. Luo, N. Du *et al.*, "Exploiting memristive BiFeO3 bilayer structures for compact sequential logics," *Adv. Funct. Mater.*, vol. 24, no. 3357, 2014.

[14] J. Doget *et al.*, "Univariate side channel attacks and leakage modeling," *J. Cryptogr. Eng.*, vol. 1, no. 2, pp. 123–144, 2011.

[15] I. Polian and F. Regazzoni, "Counteracting malicious faults in cryptographic circuits," in *ETS*. IEEE, 2017, pp. 1–10.

[16] J. Jiang, M. Aparicio, M. Comte, F. Azaïs, M. Renovell, and I. Polian, "MIRID: mixed-mode IR-drop induced delay simulator," in *Asian Test Symposium*. IEEE Computer Society, 2013, pp. 177–182.

[17] H. Lohrke *et al.*, "Contactless fault isolation for FinFET technologies with visible light and GaP SIL," in *ISTFA*, 2016.

[18] R. Schlangen *et al.*, "Functional IC analysis through chip backside with nano scale resolution e-beam probing in FIB trenches to STI level," in *IPFA*, 2007.

[19] T. Tong *et al.*, "Electron beam probing of active advanced FinFET circuit with fin level resolution," in *ISTFA*, 2019, pp. 753–768.

[20] H. Lohrke, S. Tajik, C. Boit, and J.-P. Seifert, "No place to hide: Contactless probing of secret data on FPGAs," in *Cryptographic Hardware and Embedded Systems*, 2016, pp. 147–167.

[21] S. Tajik, H. Lohrke, J.-P. Seifert, and C. Boit, "On the power of optical contactless probing: Attacking bitstream encryption of fpgas," in *ACM SIGSAC CCS*, 2017, p. 1661–1674.

[22] R. F. R. Soares, F. Sill Torres, and D. Timmermann, "Exploration of technology parameter values of integrated circuit technologies," in *Int. W. on Power & Timing Modeling, Optimiz. & Simul.*, 2015, pp. 118–125.

[23] F. Bache, C. Plump, J. Wloka, T. Güneysu, and R. Drechsler, "Evaluation of (power) side-channels in cryptographic implementations," *it - Information Technology*, vol. 61, no. 1, pp. 15–28, 2019.

[24] M. V. Guimarães and F. Sill Torres, "Automatic layout integration of bulk built-in current sensors for detection of soft errors," in *Symp. Integrated Circuits and Systems Design*, 2016, pp. 1–6.

[25] J. Heyszl, S. Mangard, B. Heinz, F. Stumpf, and G. Sigl, "Localized electromagnetic analysis of cryptographic implementations," in *CT-RSA*, ser. LNCS, vol. 7178. Springer, 2012, pp. 231–244.

[26] M. Motz and U. Ausserlechner, "Electrical compensation of mechanical stress drift in precision analog circuits," in *Wideband Continuous-time ADCs, Automotive Electronics, and Power Management*. Springer International Publishing Switzerland, 2017, pp. 296–397.

[27] U. Nurmetov, T. Fritz, E. Müllner, C. M. Dougherty, M. Szelong, F. Kreupl, and R. Brederlow, "A CMOS temperature stabilized 2-d mechanical stress sensor with 11-bit resolution," *IEEE Jour. Solid-State Circuits*, vol. 55, no. 4, pp. 846–855, 2020.

[28] V. Immler, J. Obermaier, M. König, M. Hiller, and G. Sig, "B-TREPID: Batteryless tamper-resistant envelope with a puf and integrity detection," in *HOST*, 2018, pp. 49–56.

[29] V. Immler and K. Uppund, "New insights to key derivation for tamper-evident physical unclonable functions," *CHES*, vol. 2019, no. 3, pp. 30–65, May 2019.

[30] C. Qiu *et al.*, "Scaling CNT complementary FETs to a 5-nm gate lengths," *Science*, pp. 271–276, 2017.

[31] G. Rosendale *et al.*, "A 4 megabit carbon nanotube-based nonvolatile memory (NRAM)," in *ESSCIRC*, 2007, pp. 478–481.

[32] M. Hartmann *et al.*, "Gate spacer investigation for improving the speed of high-frequency carbon nanotube-based field-effect transistors," *ACS Appl.Mater.Interfaces*, pp. 27 461–27 466, 2020.

[33] G. S. Rose, M. Uddin, and M. B. Majumder, "A designer's rationale for nanoelectronic hardware security primitives," in *ISVLSI*, 2016, pp. 194–199.

[34] J. Burchard, M. Gay, A. S. M. Ekossono, J. Horácek, B. Becker, T. Schubert, M. Kreuzer, and I. Polian, "Autofault: Towards automatic construction of algebraic fault attacks," in *FDTC*, 2017, pp. 65–72.

[35] D. Šišejković, F. Merchant, L. M. Reimann, R. Leupers, M. Giacometti, and S. Kegreiß, "A secure hardware-software solution based on RISC-V, logic locking and microkernel," in *Int'l W Software & Compilers for Embedded Systems*, 2020, p. 62–65.

[36] D. Šišejković, F. Merchant, R. Leupers, G. Ascheid, and S. Kegreiss, "Inter-Lock: logic encryption for processor cores beyond module boundaries," in *2019 IEEE European Test Symposium (ETS)*, 2019, pp. 1–6.

[37] P. Estrela, V. Pachauri, and S. Ingebrandt, "Biologically sensitive field-effect transistors: from ISFETs to NanoFETs," *Essays in Biochemistry*, vol. 60, no. 1, pp. 81–90, 06 2016.

[38] D. Šišejković, F. Merchant, R. Leupers, G. Ascheid, and S. Kegreiss, "Control-lock: Securing processor cores against software-controlled hardware trojans," in *GLSVLSI*, New York, NY, USA, 2019, p. 27–32.

[39] P. Kocher *et al.*, "Spectre attacks: Exploiting speculative execution," in *IEEE Symp. on Security and Privacy*, 2019.

[40] M. Lipp *et al.*, "Meltdown: Reading kernel memory from user space," in *USENIX Security*, 2018.

[41] M. Schwarz, M. Lipp, D. Moghimi, J. Van Bulck, J. Stecklina, T. Prescher, and D. Gruss, "ZombieLoad: Cross-privilege-boundary data sampling," in *ACM SIGSAC CCS*, 2019, pp. 753–768.

[42] O. Mutlu and J. S. Kim, "Rowhammer: A retrospective," *IEEE Trans. Computer-Aided Design*, 2019.

[43] F. Dall, G. D. Micheli, T. Eisenbarth, D. Genkin, N. Heninger, A. Moghimi, and Y. Yarom, "CacheQuote: efficiently recovering long-term secrets of SGX EPID via cache attacks," *IACR Trans. CHES*, vol. 2018, no. 2, pp. 171–191, 2018.

[44] J. Van Bulck *et al.*, "Foreshadow: Extracting the keys to the Intel {SGX} kingdom with transient out-of-order execution," in *USENIX Security*, 2018, pp. 991–1008.

[45] M. R. Fadiheh, D. Stoffel, C. Barrett, S. Mitra, and W. Kunz, "Processor hardware security vulnerabilities and their detection by unique program execution checking," in *DATE*, 2019.