Author's version accepted for CSR-2024; the final publication is available at https://ieeexplore.ieee.org/document/10679507

Static Power Consumption as a New Side-Channel Analysis Threat to Elliptic Curve Cryptography Implementations

Ievgen Kabin[1], Zoya Dyka[1,2], Alkistis-Aikaterini Sigourou[1] and Peter Langendoerfer[1,2]
[1] *IHP GmbH – Leibniz Institute for High Performance Microelectronics, 15236 Frankfurt, Germany*
[2] *Brandenburg University of Technology Cottbus-Senftenberg, 03046 Cottbus, Germany*
{kabin, dyka, sigourou, langendoerfer}@ihp-microelectronics.com

***Abstract*— Side-Channel Analysis is a category of security attacks that targets cryptographic devices or systems exploiting unintended information leakage through observable physical side-channels, e.g. power consumption. Side-Channel Analysis primarily aims at the dynamic power consumption of a target device or system during its operation, particularly when cryptographic operations or sensitive computations are being performed. As semiconductor technology nodes shrink, enabling increased transistor density and improved performance, the static current, also known as leakage current tends to increase. This increase in static power consumption can have critical implications for the security of digital systems, particularly in the context of side-channel attacks. In this paper, by examining the static phase within the clock cycle, we demonstrate how a cryptographic key can be extracted from a single power trace measurement. Our research reveals that static currents effectively expose the cryptographic key, a concern that becomes particularly critical in the context of scaled semiconductor technologies.**

Keywords*— *Side-Channel Analysis (SCA), Attack Exploiting Static Power (AESP), leakage current, horizontal attack, single-trace attack, power trace, Elliptic Curve Cryptosystem (ECC)

I. INTRODUCTION

CMOS technology is the leading choice for fabricating integrated circuits because of its low power consumption and scalability. During the operation, the power consumption of a CMOS device can be expressed by the sum of dynamic power and static power. Dynamic power is mainly caused by switching of transistors from different logic states while current leakage is the reason for static power consumption. Therefore, static power consumption refers to the power consumed by a circuit even when it is in a static, i.e. non-switching state.

It is a well-known fact that the power consumption of a device implementing cryptographic operations may be leveraged to expose confidential information processed by the device. Attacks of this type are referred to as Side-Channel Analysis (SCA) attacks. The history of SCA attacks started over two decades ago when P. Kocher introduced the concept of differential power analysis attacks [1]. Since that time SCA evolved into a dynamically developing field that significantly influences the design and evaluation of cryptographic devices.

The primary objective of power analysis attacks is directed towards retrieving the secret key of a cryptographic device based on measurements of its dynamic power consumption. Nevertheless, as technology scales, static power consumption increases at a faster rate, giving rise to new challenges in hardware security. However, static power analysis is often not taken into account as much as dynamic power analysis [2]. Only few papers were published about the success of SCA analysing static power consumption, whereby the authors [3] claim that power attacks based on dynamic power analysis typically produce better outcomes than those based on static power consumption. This probably happens for the following reasons. On the one hand dynamic power consumption is the dominant factor when comparing the contribution in the overall power consumption. On the other hand, in contrast to dynamic power analysis which sometimes can be performed even using low-cost oscilloscopes and current probes, static power analysis may require special high-precision equipment to conduct accurate measurements.

Recent studies [4], [5] have exploited static power as a target side-channel leakage to extract cryptographic keys, with a focus on symmetric block ciphers. In this paper we demonstrate that static power consumption can be successfully exploited to attack asymmetric cryptographic approaches. We performed a horizontal attack against an accelerator for the *kP* operation, which is the main operation in cryptographic protocols using elliptic curves. We measured and analysed a current leakage trace of a single *kP* execution. Although only a single current value was measured per clock cycle, about 85 % of all bits of the processed key *k* were revealed correctly. Due to the fact that the static current can be increased via overvoltage as well as increased temperature [6], [7] or laser illumination of the chip die [8]–[10] this type of SCA leakage can be the main vulnerability source in future, especially dangerous for chips manufactured in scaled technologies.

The rest of the paper is structured as follows. In Section II we briefly describe the investigated design. Section III gives an overview of the applied measurement setup. We discuss the collection of the static power trace and results of the attack conducted against an ASIC implementation of our design in Section IV. Finally, the paper ends with conclusions and our plans for future work.

II. *KP* OPERATION IN ECC: MOSTLY ACCELERATED AND ATTACKED

Nowadays, there are two widely used asymmetric cryptographic systems that can ensure secure communication over unsecured channels: RSA (Rivest, Shamir, Adleman) and ECC (Elliptic Curve Cryptosystem). The RSA cryptographic system [11] was published in 1978. In 1985, the other asymmetric cryptographic system, ECC, was independently

developed by N. Koblitz [12] and V. Miller [13]. In comparison to symmetric cryptographic methods such as AES (Advanced Encryption Standard) [14] by NIST (National Institute of Standards and Technology, USA) [15], utilizing asymmetric methods results in significantly increased time and energy required for both data encryption and decryption processes. However, they ensure important security properties through digital signatures: identification and authentication of communicating parties, as well as non-repudiation.

For secure communication, hybrid systems are most commonly used. The RSA or ECC protocols are employed for the (mutual) authentication of communicating parties and the distribution of the symmetric session key, for example, for AES, which is then used for data encryption and decryption. Significantly shorter ECC key lengths provide several advantages over RSA, including significantly lower energy consumption and execution time for cryptographic operations and data transmission as well as reduced storage requirements. These features make ECC highly attractive for securing wireless communication in mobile devices, sensor nodes, and IoT.

Despite these advantages, ECC cryptographic operations remain computationally, time, and energy consuming, especially for battery-powered devices with limited computational resources. For such devices, implementing cryptographic operations in hardware is often the only way to ensure secure data transmission.

Assuming potential attackers may have physical access to cryptographic accelerators, cryptographic ASICs must be resistant to various Side-Channel Analysis and Fault Injection (FI) attacks. ECC is based on mathematical operations in finite fields, denoted also as Galois fields (GF). There are standardized elliptic curves (EC) over $GF(p)$ and $GF(2^n)$ [16]. The fundamental operation in all cryptographic EC protocols is called EC point multiplication, defined as the k-times addition of point P to itself, and denoted as kP. The number k is a long binary number, typically over 200 bits long and must remain secret. The attackers' intention is to obtain this number. In authentication protocols, k is the private key. In the ECDSA protocol for generating digital signatures [16], k is a randomly generated number, but knowledge of this number opens the possibility to easily calculate the private key.

Binary kP algorithms are often utilized in resource-constrained devices and ASICs. In these algorithms the scalar k is processed bitwise, i.e. bit by bit. Even small differences in the execution sequence of mathematical operations or operations involving the storage/reading of data in registers make the power profile of processing a key bit '1' distinguishable from processing a key bit '0'. These differences are then the features attackers use during analysis. Analysis can be performed by visualizing the measured trace, using statistical methods, or employing clustering algorithms belonging to machine learning methods. If the scalar k is successfully extracted based on the analysis of one single power trace of the kP execution, such an attack is called horizontal. Well-known countermeasures techniques like EC point blinding, EC point coordinates randomization, and key randomization [17], as well as various register address randomization techniques [18]–[20], are ineffective against horizontal attacks [21],[22]. Thus, horizontal attacks on kP implementations are very dangerous.

In most Power Analysis (PA) attacks, power traces (PT) captured using equipment for measuring alternating current are analysed, i.e., attackers use the dynamic power consumption of the chips for SCA. In this paper, we focus on measuring leakage current through a cryptographic ASIC, which is an accelerator for the kP operation. We demonstrate that analysing static power leakage can yield even greater success than analysing dynamic power consumption. In the rest of this paper, we describe our measurement setup and the horizontal attack, which we performed analysing the static leakage current through the attacked kP accelerator.

III. Investigated design

We have developed a hardware accelerator specifically designed to enhance the performance of the scalar multiplication operation on binary extended elliptic curves, denoted as kP. It is an implementation of the Montgomery algorithm using projective Lopez-Dahab coordinates with bitwise processing of the scalar k [23]. More detailed, the investigated design implements the modification of the kP algorithm corresponding to Algorithm A2 in [24]. The kP algorithm can be observed as a sequence of mathematical operations – multiplications, squaring operations, and additions – of elements of a finite field. The design obtains a scalar k and the two affine coordinates x and y of a point P of the EC *B-233* as inputs. X, y, and k are up to 233-bit long binary numbers that represent elements of $GF(2^{233})$, with the irreducible polynomial $f(t)=t^{233}+t^{74}+1$.

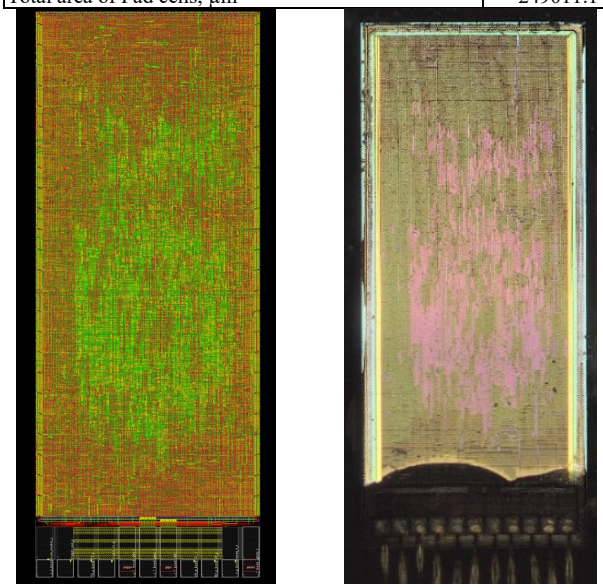
The design consists of four blocks: Controller, field Multiplier, ALU, and Registers. The block Controller manages the sequence of the field operations. It controls the data flow between the other blocks and defines which operation has to be performed in the current clock cycle. Depending on the signals of the Controller the block ALU performs addition or squaring of its operands. The block Multiplier calculates the field product of 233-bit long operands using only 9 partial products according to a fixed calculation plan. The partial multiplier for 59-bit long operands is implemented according to the classical multiplication formula, i.e. the multiplier is implemented corresponding to *Partial multiplier PM_1* in [25]. More details regarding the design can be found in [26].

We synthesized the kP design using the gate library for the IHP 250 nm technology and a *compile* optimization option (area optimization) in the Synopsys Design Compiler. The layout was done using Cadence Innovus for a maximum working frequency of 20 MHz (50ns clock cycle period). Finally, the design was manufactured as an ASIC in the IHP 250 nm technology and bonded to a printed circuit board (PCB) without any packaging. The die has a size of 2758.56 µm x 1086.12 µm. The core size is 2437.16 µm x 1029.0 µm. A photo as well as some parameters of the manufactured ASIC are provided in Fig. 1 and TABLE I. respectively.

TABLE I. Parameters of the Manufactured ASIC

Parameter	Value
Total area of Chip, μm^2	2996127.2
Chip Density (Total), %	91.661
Chip Density (Subtracting Physical Cells), %	67.650
Total area of Core, μm^2	2507837.6
Core Density (Total), %	99.579
Total area of Standard cells, μm^2	2497273.6
Core Density (Subtracting Physical Cells), %	70.892

Total area of Standard cells (Subtracting Physical Cells), μm^2	1777865.0
Total area of Pad cells, μm^2	249011.1



a) *b)*

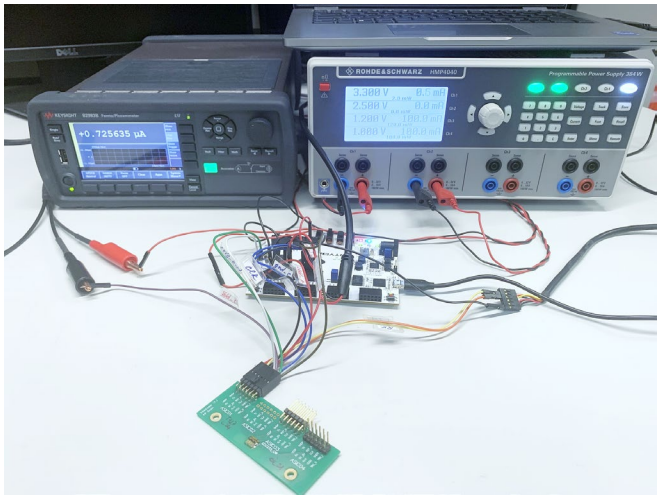
Fig. 1. The layout of the chip *(a)*, a photo of the chip surface *(b)*. The torn bottom edge on the photo is caused by a transparent epoxy resin molding compound used for the encapsulation of bonding wires to prevent their physical damage.

IV. Measurement Setup

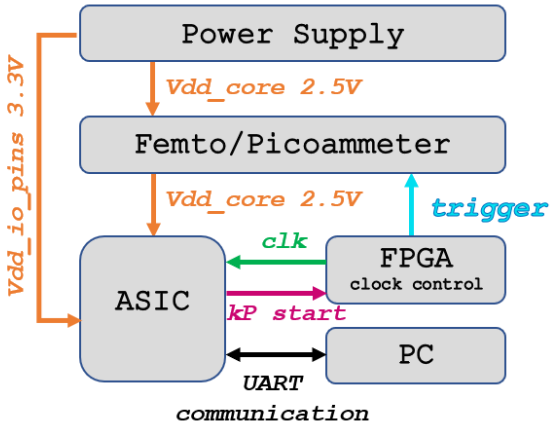
The conventional setup for the collection of power traces consists of a device under test, typically connected to the oscilloscope using a current probe. However, such a setup is not the most suitable when it comes to measuring static currents due to the fact that oscilloscopes may lack the sensitivity and resolution required for accurate measurements of low currents associated with static power consumption. Therefore, achieving an accurate measurement of static power typically requires specialized, low-noise equipment, such as picoammeters. This was demonstrated in [27] by conducting an attack on the PRESENT-80 block cipher. Additionally, to accurately measure static power, it's essential to eliminate the influence of the dynamic power part which introduces current fluctuations due to the rapid switching of transistors. This can be achieved by freezing the clock, i.e. halting the dynamic switching operations of the circuit. While the clock signal is halted, the transistors remain either active or inactive, maintaining the leakage currents at a constant level. Isolating the circuit in such a static state allows us to focus specifically on the static current/power consumption.

For collection of the static power trace we used the measurement setup depicted in Fig. 2.

The core component of the setup is a battery-powered Keysight B2983B [28] Femto/Picoammeter that allows to measure small currents with 0.01 fA resolution in a range of 0.01 fA up to 20 mA with a maximum sampling rate of 20 kS/s. The device has a memory buffer that is capable to hold 100000 measured values. The rest of the setup consists of a Rohde&Schwarz HMP4040 high-performance power supply and an Arty S7 board [29] equipped with a Xilinx Spartan-7 FPGA to control the clock signal.



(a)



(b)

Fig. 2. The photo of the measurement setup *(a)* and its schematical representation *(b)*.

The device under attack is an ASIC connected to the 3.3V and 2.5V lines of the power supply to provide the voltage for the input/output pins and core logic respectively. The Femto/Picoammeter is connected to the core power supply line (see Fig. 2-*b*).

We used an Arty S7 board as a clock source controller for the attacked ASIC as well as a source of a trigger signal for the measurement device. The clock source on the FPGA is configured to generate a 4 MHz (250 ns) clock signal with a 50% duty cycle during the idle or communication states. However, during the *kP* calculation the operating frequency will be reduced to 20 kHz and a 0.25% duty cycle. This results in a signal depicted by the green curve in Fig. 3.

The clock stays in a high state for 125 ns (half of the 4 MHz frequency period) whereas it stays for 49.875 µs in a low state. This allows us to set up a trigger signal for the picoammeter (see the cyan curve in Fig. 3) and perform current measurements during each of the clock cycles within the *kP* operation.

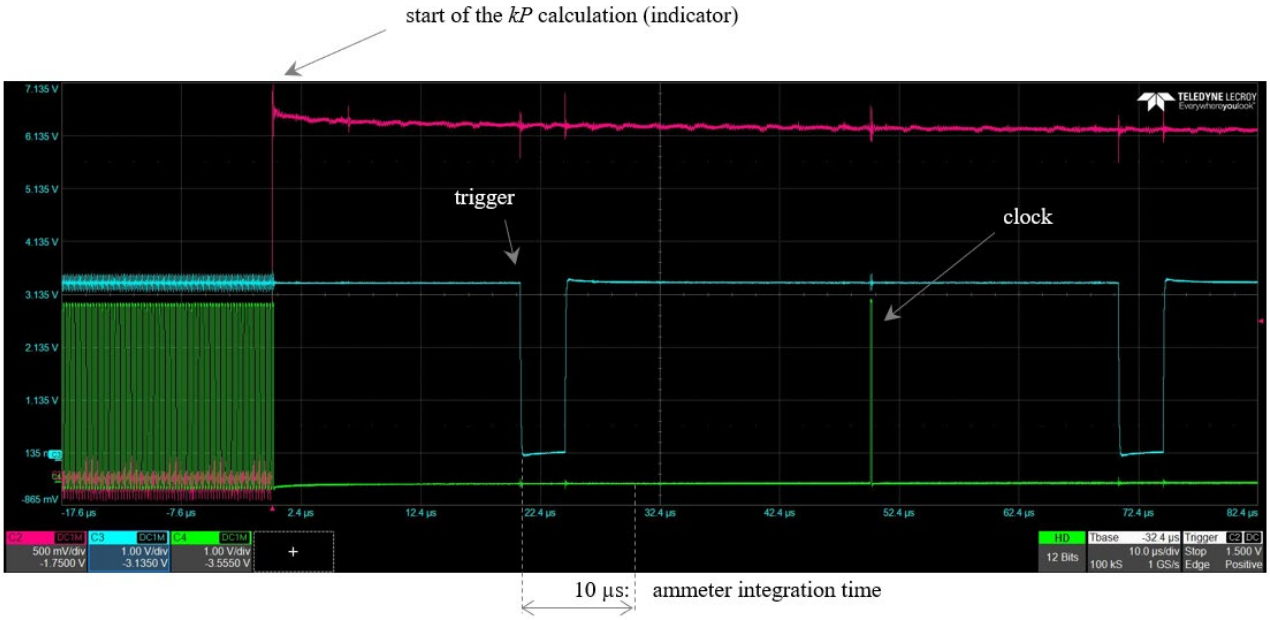


Fig. 3. Oscilloscope diagrams explaining the measurement process. The red curve indicates the start of the *kP* operation; the green curve shows the clock signal before the *kP* operation (left side) and during the *kP* operation (right). Cyan curve: trigger signal for the Keysight B2983B Femto/Picoammeter during the *kP* operation.

V. Trace Collection and Results of the Attack

We captured the static current values during the execution of the *kP* operation using the measurement setup described in the previous section. The measurement of the static leakage current, referred to as the static power trace, was conducted at room temperature. The picoammeter was configured with a 200 µA range for current detection, 0.001 power line cycles (PLC), and an integration time of 10 µs. In total a single trace consists of 12907 measured values, i.e. only a single sample per clock cycle was measured. A part of the trace is depicted in Fig. 4.

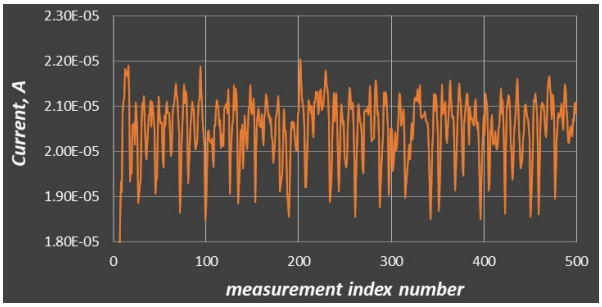


Fig. 4. A part of a static power trace representing the start of the *kP* operation. The average value of the measured static current is about 20.53µA

We performed the *comparison to the mean* attack [30] against the measured trace. As the trace contains only one measured sample per clock cycle the trace compression was not applied. For our design the attack is expected to generate 54 potential key candidates.

To evaluate the success of the attack for each key candidate its relative correctness δ was calculated. This is the number of the correctly revealed bits in the key candidate divided by all revealed bits represented in %. The relative correctness δ is a value between 0% and 100%. If a key candidate has the correctness δ=100% it means that the key candidate is equal to the real key k. If a key candidate has the correctness δ=0% it means that the key candidate is equal to the real key k after performing the inversion of all key bits. Considering this fact, when evaluating the success of the attack, correctness can be expressed within a range of 50% to 100%. In this range, 50% represents the worst-case scenario from the attacker's perspective and the best-case scenario from the designer's standpoint.

The results of the attack are represented by an orange line in Fig. 5. In total, there are 6 key candidates revealed with a correctness of more than 70% (see key candidates with indexes 8, 14, 39 to 41, and 44), whereas the best key candidate has a correctness of 84.3%.

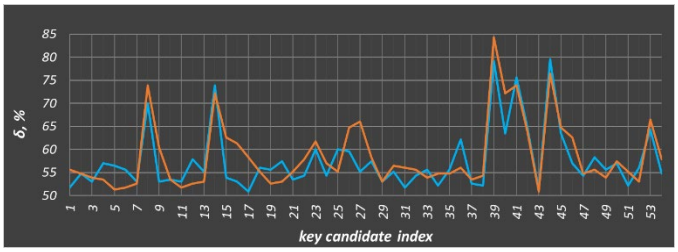


Fig. 5. Results of the *comparison to the mean* attack analysing the measured static leakage current trace (orange line) and analysing a conventional power trace (blue line).

Fig. 5 also demonstrates the results of the *comparison to the mean* attack conducted against the same ASIC analysing its power trace measured with the conventional setup (see the blue line), i.e. dynamic power trace obtained using the Riscure current probe connected to the Lecroy WavePro 254HD oscilloscope. In this case the design was running at a stable 4 MHz clock frequency. The power trace was captured using 2.5 GS/s sampling rate, resulting in 625 measured values per clock

cycle. After the trace compression the conducted attack resulted in five key candidates revealed with a correctness of 70% or more. The maximum correctness was 79.56% for the 44th key candidate. Please note that in both setups the *kP* calculations were done using the same inputs, i.e. the same values of the scalar *k* and the coordinates of the point P.

It can be clearly seen, that the results of the attack conducted against the static power trace are comparable to those, obtained by attacking the dynamic power trace. However, in the case of a static power analysis there are several key candidates extracted with even higher correctness, see key candidates with indexes 8, 39 and 40 in Fig. 5.

VI. Conclusions and Future Work

Over the last 25 years, power analysis of cryptographic implementations has evolved thanks to:

- numerous investigations of the impact of various trace analysis methods on attack success, ranging from simple, that are based solely on visualizing different markers and distinguishers using the naked eye, to the application of different machine learning methods.
- significant improvements in measurement techniques and measuring equipment.

The latter has revealed many interesting facts, such as the distinguishability of addressing different registers. Therefore, the assumption about the indistinguishability of register addressing operations needs to be revised, at least for the hardware implementation of cryptographic algorithms. This is especially relevant for binary *kP* algorithms, where key-dependent addressing of registers is their inherent part. Enhancements in the resolution, sensitivity, and acquisition memory length of measurement instruments provide the opportunity to significantly improve traditional measurement setups. For power and electromagnetic analysis, these setups traditionally rely on the assumption that the dynamic power consumption of the investigated circuit predominates over the static and serves as the main source of SCA leakage. Consequently, the conventional measurement setup is focused on measuring the dynamic power consumption caused by alternating currents caused by the switching of CMOS logic.

Nowadays, improvements in measurement equipment allow the exploitation of static power consumption as a side-channel leakage. To the best of our knowledge, this work is the first reporting practical results of the static power analysis attack against *kP* implementations. We showed that small variations of data-dependent leakage currents can be successfully exploited in SCA attacks. In this study, we demonstrated the effectiveness of such measurements for the side-channel analysis on the example of our *kP* design manufactured as an ASIC in a 250 nm technology. As static power consumption is considered to increase with technologies scaling, the main focus of power analysis measurements can be shifted from dynamic to static power. Please note that static power consumption depends on temperature, overvoltage, laser illumination, and aging. The combination of these effects can enhance the success of SCA attacks and therefore has to be investigated in the future.

The conventional SCA countermeasures are aimed at reducing the success of dynamic power analysis. The question of whether such countermeasures can also reduce the success of static power analysis has to be investigated in the future. Due to the fact that static power leakage, aging processes, reaction on overvoltage or laser illumination can be modeled, the models of the logic cells reaction on these parameters can be helpful to estimate the resistance of cryptographic designs in the early design phase.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in Advances in Cryptology — CRYPTO' 99, vol. 1666, Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397. doi: 10.1007/3-540-48405-1_25.

[2] N. D. P. Avirneni and A. K. Somani, "Countering Power Analysis Attacks UsingReliable and Aggressive Designs," IEEE Transactions on Computers, vol. 63, no. 6, pp. 1408–1420, Jun. 2014, doi: 10.1109/TC.2013.9.

[3] K. Palma and F. Moll, "Analysis of Random Body Bias Application in FDSOI Cryptosystems as a Countermeasure to Leakage-Based Power Analysis Attacks," IEEE Access, vol. 9, pp. 114977–114988, 2021, doi: 10.1109/ACCESS.2021.3105635.

[4] D. Bellizia, G. Scotti, and A. Trifiletti, "Implementation of the PRESENT-80 block cipher and analysis of its vulnerability to Side Channel Attacks Exploiting Static Power," in 2016 MIXDES - 23rd International Conference Mixed Design of Integrated Circuits and Systems, Jun. 2016, pp. 211–216. doi: 10.1109/MIXDES.2016.7529734.

[5] T. Moos, A. Moradi, and B. Richter, "Static Power Side-Channel Analysis—An Investigation of Measurement Factors," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, no. 2, pp. 376–389, Feb. 2020, doi: 10.1109/TVLSI.2019.2948141.

[6] J. A. Butts and G. S. Sohi, "A static power model for architects," in Proceedings 33rd Annual IEEE/ACM International Symposium on Microarchitecture. MICRO-33 2000, Dec. 2000, pp. 191–201. doi: 10.1109/MICRO.2000.898070.

[7] T. Moos, "Static Power SCA of Sub-100 nm CMOS ASICs and the Insecurity of Masking Schemes in Low-Noise Environments," IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 202–232, May 2019, doi: 10.13154/tches.v2019.i3.202-232.

[8] S. Skorobogatov, "Optically Enhanced Position-Locked Power Analysis," in Cryptographic Hardware and Embedded Systems - CHES 2006, L. Goubin and M. Matsui, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2006, pp. 61–75. doi: 10.1007/11894063_6.

[9] J. Di-Battista, J.-C. Courrege, B. Rouzeyre, L. Torres, and P. Perdu, "When Failure Analysis Meets Side-Channel Attacks," in Cryptographic Hardware and Embedded Systems, CHES 2010, S. Mangard and F.-X. Standaert, Eds., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2010, pp. 188–202. doi: 10.1007/978-3-642-15031-9_13.

[10] D. Petryk, Z. Dyka, M. Krstic, J. Bělohoubek, P. Fišer, F. Steiner, T. Blecha, P. Langendörfer, I. Kabin, "On the Influence of the Laser Illumination on the Logic Cells Current Consumption," In proc, of 2023 30th IEEE International Conference on Electronics, Circuits and Systems (ICECS).

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.

[12] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comp.*, vol. 48, no. 177, pp. 203–209, 1987, doi: 10.1090/S0025-5718-1987-0866109-5.

[13] V. S. Miller, "Use of Elliptic Curves in Cryptography," in *Advances in Cryptology — CRYPTO '85 Proceedings*, H. C. Williams, Ed., in Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1986, pp. 417–426. doi: 10.1007/3-540-39799-X_31.

[14] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," U.S. Department of Commerce, Federal Information Processing Standard (FIPS) 197, Nov. 2001. doi: 10.6028/NIST.FIPS.197.

[15] National Institute of Standards and Technology (NIST) - http://csrc.nist.gov/ [Accessed: July 20, 2024].

[16] National Institute of Standards and Technology (NIST), "Digital Signature Standard (DSS)," U.S. Department of Commerce, Federal Information Processing Standard (FIPS) 186-5, Feb. 2023. doi: 10.6028/NIST.FIPS.186-5.

[17] J.-S. Coron, "Resistance Against Differential Power Analysis For Elliptic Curve Cryptosystems," in *Cryptographic Hardware and Embedded Systems*, vol. 1717, Ç. K. Koç and C. Paar, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 292–302. doi: 10.1007/3-540-48059-5_25.

[18] K. Itoh, T. Izu, and M. Takenaka, "Address-Bit Differential Power Analysis of Cryptographic Schemes OK-ECDH and OK-ECDSA," in *Cryptographic Hardware and Embedded Systems - CHES 2002*, Springer, Berlin, Heidelberg, Aug. 2002, pp. 129–143. doi: 10.1007/3-540-36400-5_11.

[19] K. Itoh, T. Izu, and M. Takenaka, "A Practical Countermeasure against Address-Bit Differential Power Analysis," in *Cryptographic Hardware and Embedded Systems - CHES 2003*, in Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, Sep. 2003, pp. 382–396. doi: 10.1007/978-3-540-45238-6_30.

[20] M. Izumi, J. Ikegami, K. Sakiyama, and K. Ohta, "Improved countermeasure against Address-bit DPA for ECC scalar multiplication," in *2010 Design, Automation Test in Europe Conference Exhibition (DATE 2010)*, Mar. 2010, pp. 981–984. doi: 10.1109/DATE.2010.5456907.

[21] I. Kabin, Z. Dyka, D. Kreiser, and P. Langendoerfer, "Evaluation of resistance of ECC designs protected by different randomization countermeasures against horizontal DPA attacks," in *2017 IEEE East-West Design Test Symposium (EWDTS)*, Sep. 2017, pp. 1–7. doi: 10.1109/EWDTS.2017.8110037.

[22] I. Kabin, Z. Dyka, and P. Langendoerfer, "Randomized Addressing Countermeasures are Inefficient Against Address-Bit SCA," in *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, Jul. 2023, pp. 580–585. doi: 10.1109/CSR57506.2023.10224968.

[23] J. López and R. Dahab, "Fast Multiplication on Elliptic Curves Over GF(2m) without precomputation," in *Cryptographic Hardware and Embedded Systems*, vol. 1717, Ç. K. Koç and C. Paar, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 316–327. doi: 10.1007/3-540-48059-5_27.

[24] I. Kabin, Z. Dyka, and P. Langendoerfer, "Atomicity and Regularity Principles Do Not Ensure Full Resistance of ECC Designs against Single-Trace Attacks," *Sensors*, vol. 22, no. 8, Art. no. 8, Jan. 2022, doi: 10.3390/s22083083.

[25] I. Kabin, Z. Dyka, D. Klann, and P. Langendoerfer, "Horizontal DPA Attacks against ECC: Impact of Implemented Field Multiplication Formula," in *2019 14th International Conference on Design Technology of Integrated Systems In Nanoscale Era (DTIS)*, Apr. 2019, pp. 1–6. doi: 10.1109/DTIS.2019.8735011.

[26] I. Kabin, "Horizontal address-bit SCA attacks against ECC and appropriate countermeasures," BTU Cottbus - Senftenberg, 2023. doi: 10.26127/BTUOpen-6397.

[27] D. Bellizia, D. Cellucci, V. Di Stefano, G. Scotti, and A. Trifiletti, "Novel measurements setup for attacks exploiting static power using DC pico-ammeter," in *2017 European Conference on Circuit Theory and Design (ECCTD)*, Sep. 2017, pp. 1–4. doi: 10.1109/ECCTD.2017.8093333.

[28] Keysight B2983B Femto / Picoammeter, https://www.keysight.com/us/en/product/B2983B/b2983b.html [Accessed: July 20, 2024].

[29] Digilent Arty S7 board, https://digilent.com/reference/programmable-logic/arty-s7/start [Accessed: July 20, 2024].

[30] I. Kabin, D. Kreiser, Z. Dyka and P. Langendoerfer, "FPGA Implementation of ECC: Low-Cost Countermeasure against Horizontal Bus and Address-Bit SCA," *2018 International Conference on ReConFigurable Computing and FPGAs (ReConFig)*, Cancun, Mexico, 2018, pp. 1-7, doi: 10.1109/RECONFIG.2018.8641732