Impact of Thermal Effects on Cryptographic Resilience: A Study of an ASIC Implementation of the Montgomery Ladder

Preprint · March 2025

CITATIONS
0

READS
7

3 authors:

Ievgen Kabin
Leibniz Institute for High Performance Microelectronics
88 PUBLICATIONS **336** CITATIONS
SEE PROFILE

Peter Langendoerfer
Leibniz Institute for High Performance Microelectronics
343 PUBLICATIONS **2,061** CITATIONS
SEE PROFILE

Zoya Dyka
IHP - Innovations for High Performance Microelectronics
142 PUBLICATIONS **618** CITATIONS
SEE PROFILE

Impact of Thermal Effects on Cryptographic Resilience: A Study of an ASIC Implementation of the Montgomery Ladder

Ievgen Kabin[1], Peter Langendoerfer[1,2], and Zoya Dyka [1,2]
[1] *IHP – Leibniz Institute for High Performance Microelectronics*, Frankfurt (Oder), Germany
[2] *BTU Cottbus-Senftenberg*, Cottbus, Germany
{ kabin, langendoerfer, dyka }@ihp-microelectronics.com

***Abstract*— The side-channel attack resistance of hardware implementations of cryptographic algorithms can vary significantly with operating parameters, such as operating voltage, clock frequency, temperature, etc. This study investigates the influence of temperature on the resilience of an ASIC implementation of the Montgomery ladder against SCA. We conducted a series of experiments to evaluate how varying temperature conditions impact the resistance of our ASIC to horizontal attacks. Our results reveal that in contrast to the state-of-the-art approach of increasing the operating temperature, operating under sub-zero temperatures can result in increased vulnerability to side-channel attacks compared to high temperature experiments. We present a detailed analysis of the thermal sensitivity of our ASIC, correlating specific temperature ranges with potential security degradation.**

Keywords—side-channel analysis, SCA, static power, static current, leakage current, leakage current attacks, leakage power analysis (LPA), attacks exploiting static current, operating parameters, thermal sensitivity horizontal attacks, ECC, Montgomery Ladder, static current SCA

I. INTRODUCTION

CMOS technology is used for fabricating integrated circuits due to its low power consumption and scalability. Power consumption in CMOS devices consists of dynamic and static power. Dynamic power corresponds to transistors switching between different logic states, while static power results from current leakage in the non-switching, or static state. Taking into account the overall power consumption of a device, static power was often considered less significant in the past. However, as technology scales and transistors size continues to shrink, static power consumption has started increasing at a faster rate. This brings new challenges to the field of hardware design and security.

Dynamic power consumption has been successfully exploited as a leakage source to reveal sensitive information processed by cryptographic implementations. Attacks exploiting power consumption belong to side-channel analysis (SCA) attacks, and are known for over two decades since the first one was introduced by P. Kocher in 1999 [1].

Recent researches have also successfully exploited static power leakage to extract cryptographic keys from cryptographic implementations even though it requires more precise equipment for accurate measurements as well as more sophisticated setups. However, most of the cases published to date have focused on attacks against symmetric ciphers. There are only two papers reporting successful attacks exploiting static power consumption as a leakage source in asymmetric cryptographic approaches on the example of an elliptic curve (EC) cryptographic chip [2],[3].

In this paper, we advance the exploration of static power as a potential side-channel leakage source by targeting a hardware implementation of an elliptic curve point multiplication accelerator. In contrast to the existing papers, which suggest to increase operating temperature in order to amplify side-channel leakage related to the static power, we demonstrate that operation under sub-zero temperatures leads to the better results from the SCA vulnerability perspective.

The paper proceeds as follows: a short overview of the state-of-the-art attacks is given in Section II. Section III describes our investigated design as well as the applied measurement setup. Section IV details the collection and analysis of static power traces and presents the results of our attack on an IHP EC accelerator implemented as an ASIC. The paper ends with conclusions and our plans for future work.

II. RELATED WORKS

To date, we were able to find only 65 works related to the application of static currents for vulnerability assessment of cryptographic implementations. Some of the works present attacks against different cryptographic algorithms based on either simulated or measured data while others only discuss the application of specifically designed cells as possible countermeasures based on simulation results without providing evaluation of their effectiveness.

It's worth adding, there is no single established term for this type of attack, which complicates the search for literature. Authors use various terms such as static power attacks, leakage current attacks, leakage power analysis (LPA) attacks, attacks exploiting static power (AESP), Static Power Side-Channel Analysis (SPSCA), etc.

A. Symmetric ciphers successfully attacked

Historically, attacks based on leakage power consumption were first presented in [4] in 2007 on the example of leakage current simulations for the Serpent *S-box* synthesized for a 130 nm technology. Additionally, based on the conducted measurements authors demonstrated that leakage current can be exploited by an attacker to extract information about the secret key in a hardware implementation of AES. In 2008 an attack exploiting static current was successfully used to reveal a secret key applied in a DES simulation [5]. Attacks exploiting static power side-channel leakage against an AES implementation running on an FPGA were described in [6], whereby the authors described detailed their measurement setup and procedure. In [7] the authors attacked an AES *S-box* implementation manufactured as a custom ASIC in a 65 nm technology. They evaluated the static leakage comparing it with the dynamic leakage and assumed that masking countermeasures may be inefficient against static leakage attacks. In [8], correlation power analysis of AES-128 and Present was performed based on static currents simulations for 28 nm and 65 nm technologies.

Authors of [9] discuss the effectiveness of static power analysis in comparison to dynamic power analysis for the Present-80 block cipher using a 150 nm CMOS prototype chip as example. The authors highlighted that static power analysis attacks can significantly reduce the complexity of high-order attacks even in the presence of masking countermeasures.

[10] presents an evaluation of a PRINCE core manufactured as a custom 40 nm ASIC. The authors concluded that static current attacks can be more effective compared to dynamic power attacks due to the greater amount of useful information present in static leakage.

B. LPA attacks exploitng manipulation of the operating parameters

According to [11] the dominant components of leakage current in CMOS devices are subthreshold leakage, gate leakage and source to substrate/drain to substrate p-n junction leakage. These strongly depend not only on the physical dimensions of transistors and technology process parameters but also on the operating temperature, and supply voltage. Therefore, attackers can manipulate operating conditions to enhance leakage or reduce noise, improving the success rate of their attack.

A key to understanding the reasons for the success of such attack types, and the development of effective countermeasures against them, requires an investigation of how operating conditions affect the magnitude of SCA leakage. It is a well-known fact, that operating conditions have significant impact not only on the CMOS device performance but also on its static power consumption. Increased power supply voltage as well as device operational temperature result in exponentially increased static currents [12] which may be beneficial for potential attackers. For example, in [13], authors demonstrated the effectiveness of an attack at 65°C against PRESENT-80 implemented on a Xilinx Spartan-6. In [14], [15] increased operating temperature and power supply voltage were applied against hardware implementations of PRESENT-80 and AES. Static power analysis attacks are commonly carried out with the devices operating at elevated temperatures (90°C) and higher supply voltages, which amplify leakage currents and make them easier to exploit [16]. Finally, in [17] authors compared the leakage currents produced by protected and unprotected implementations of Present manufactured as 28nm CMOS ASIC. Static currents were measured under the normal operating conditions (20°C and 0.9V core voltage) and under a combination of the elevated temperature and core supply overvoltage (90°C and 1.35V core voltage). None of the evaluated countermeasures were able to resist the performed attack. Most of the existing countermeasures that aimed to prevent dynamic power analysis attacks were evaluated as countermeasures against static power analysis on example of symmetric ciphers only. And, as stated in [17], the countermeasures appear to only partially increase the complexity of static power attacks, i.e. the conventional countermeasures have shown to be ineffective against static leakage attacks.

To summarize, all the works mentioned in this section focus on attacks targeting symmetric cryptographic approaches. There are only two papers [2],[3]. presenting results of an LPA attack against asymmetric cryptographic approaches on the example of an EC cryptographic chip. The investigated cryptographic accelerator is the same as in this work. We describe it in the next section.

III. Investigated Design and Measurement Setup

The investigated cryptographic design is a hardware accelerator for the operation, which is called elliptic curve scalar multiplication and denoted as *kP* operation. It is a multiplication of an elliptic curve point *P* with a scalar *k*. The multiplication is defined as *k*-times addition of the EC point *P* to itself. It is a complex operation, which can be represented as a sequence of EC point doublings and EC point additions. EC point doubling and EC point addition are also complex operations defined each as a sequence of mathematical operations with elements of the finite field for the selected EC. Our *kP* design requires values of a scalar *k* and both *x* and *y* coordinates of point *P* as inputs. These inputs are up to 233-bit long binary numbers representing elements of Galois Field $GF(2^{233})$. The processing of a scalar *k* is performed bitwise according to the modification of the Montgomery *kP* algorithm with Lopez-Dahab projective coordinates [18]. The design was manufactured as an ASIC in 250 nm technology with concurrent optimization of timing, area, and power that resulted in reduced dynamic and leakage power. Additional details regarding design implementation as well as parameters of the manufactured chip are given in [19]. The mathematic backgrounds for ECC can be found in [20]. In this paper, we concentrate only on the aspects relevant for this investigations.

We used a measurement setup similar to the one described in [3]. Specifically, it consists of a B2983B battery-powered femto/picoammeter from Keysight for current measurements, R&S HMP4040 power supply, and an Arty S7-50 FPGA board used to generate and control the clock signal as well as a trigger source for the picoammeter. Additionally, all the experiments were conducted in a climate chamber to maintain a constant operating temperature during the calculation of the *kP* operation. The investigated temperature was selected to cover the whole grade 2 range of the Automotive Electronics Council AEC-Q100 standard [21], i.e. from -40°C to +105°C.

IV. Trace Collection and Discussion of the Attack Results

In our experiments instead of using the same chip that was investigated in [19] we bonded a brand-fresh die to the PCB. This was done to exclude any impact on the static current due to aging or wear-out factors that may occur in the chip due to its prior extensive usage.

Our ASIC requires two power supply voltages – a pad voltage of 3.3V and a core voltage of 2.5V. We kept the pad voltage stable while changing the core voltage by ±20%. Thus, we investigated the influence of three core supply voltages: 2.0V, 2.5V, and 3.0V.

The temperature in the climate chamber was changed in a range from -40°C to +110°C with a step of 10°C and without humidity control. For the picoammeter settings we used a manual aperture mode with 0.01·PLC resulting in 200 µs integration time for the 50 Hz operation. As a signal amplitude range, a fixed range of 20 µA was used for all the measurements with 2.0V up to 3.0V core supply voltage, except of the case of 110°C and 3.0V core supply voltage, in which a range of 200 µA was required.

Originally, the clock source on the FPGA board was configured to generate a 4 MHz signal with a 50% duty cycle and 3.3V amplitude for the idle state. However, during the *kP* calculation, we increased the duration of the low state of the clock signal by a factor of 1999 (from 125 ns to 249875 ns) resulting in a clock cycle period of 250 µs (4 kHz clock frequency). In order to ensure that only static current measurements are conducted during each clock cycle of the *kP* operation, we triggered measurements after a sufficient delay following the falling edge of the clock. For each clock cycle this approach allows us to measure a single value of the static current, while excluding transient currents generated by switching events.

As our *kP* design requires over 12900 clock cycles for calculating the result, the execution time for a single *kP* operation takes approximately 3.22 seconds for the settings explained above. We used the maximum available picoammeter memory buffer of 100000 values for storing the captured data, i.e. a single measurement can contain seven full traces of the *kP* execution.

For each of the temperatures and each of the core supply voltages we performed one measurement by filling the picoammeter memory buffer. Thus, for each investigated case we captured seven traces of the *kP* execution. All measurements were performed with the same inputs, i.e. with the same values of the coordinates of the EC point *P* and scalar *k*. Each *kP* execution was validated by checking the correctness of calculated result. In total, 48 measurements were recorded, containing 336 static current traces of the *kP* operation. We were unable to capture valid traces for the core supply voltage of 3.0V at -40°C. This combination of operating parameters resulted in either incorrect calculation results or lost communication with the device under test. We analysed only valid traces, i.e. only the traces, for which the executed *kP* operation was correctly calculated.

In this work we focus on single-trace attacks against ECC which are the most critical, as multi-trace attacks can be successfully mitigated by applying state-of-the-art countermeasures described in [22]. We have not applied any trace pre-processing or trace averaging, i.e. we used a single measured trace for the analysis. For each of the measured 329 traces we applied the *comparison to the mean* attack as described in [23], i.e. we performed 329 times the single-trace attack. Each attack results in 54 key candidates for the attacked implementation. We evaluated the success of attacks using the relative correctness of the key candidates. The relative correctness of a key candidate shows in percent the number of the revealed bits. For example, if the correctness of a 230-bit long key candidate is 100% this means that all its 230 bits are identical to the scalar *k* processed during the *kP* operation. A correctness of 80% means that only 80%·230=184 bits of the key candidate are the same as in the scalar *k*. For each of the traces, out of 54 key candidates we selected a key candidate with a maximum correctness. From each group of seven traces we also selected the maximum value of correctness. The attack results are presented graphically in Fig. 1.

As it can be seen, the best correctness for the key of 79.13% is achieved attacking the trace captured at 0°C and the nominal core voltage. In general, the traces captured for the temperatures below 0°C and reduced core voltage result in a higher correctness of the key revealed compared to most combinations of nominal core voltage and temperatures above zero.

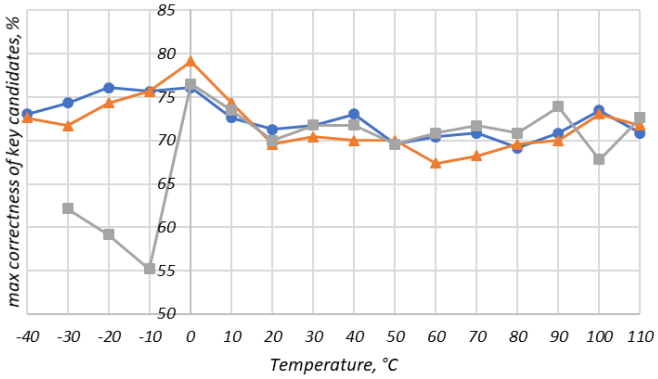

Fig. 1. Results of the performed side-channel analysis attack exploiting the measured static current, demonstrating the maximum correctness of key candidates depending on the core supply voltage (2.0 V - blue line, 2.5 V - orange line, 3.0 V - grey line) and the ambient temperature.

It appears that the noise present in static current measurements at low temperatures, as well as the current drift is increasing with the core power supply voltage. These factors are not visible for the naked eye when observing the traces for core voltages of 2.0 to 3.0V but are sufficient to impact the results of the attack. In our opinion, this is the reason for the low correctness of key candidates obtained attacking the traces captured below zero degrees using 3.0V as a core voltage. To increase the attack's success rate it might be necessary to further reduce the core voltage, as well as operating frequency while increasing the ammeter integration time.

Surprisingly, the results of our attack conducted against static current traces are not only comparable to but also outperform the results of the attack analysing dynamic power

published in [19], even for such an old technology as 250 nm, with very small static leakage currents. The maximum correctness of the key revealed is increased from 76% when attacking a measured dynamic power trace to 79% when attacking a measured static current trace.

V. Conclusions

In this work, we analysed the effectiveness of single-trace side-channel attacks against elliptic curve cryptography using static current measurements conducted under different operating conditions such as variation of the core voltage and ambient temperature. To the best of our knowledge, this work is the first analysing the resistance of asymmetric cryptographic approaches against static current side-channel analysis attacks under the variation of operating parameters. We performed enhanced measurements allowing to compare the resistance of an elliptic curve cryptographic accelerator to a horizontal SCA attack analysing the measured static current traces for a broad range of temperatures and for different core voltages. In contrast to the existing investigations of symmetric ciphers such as AES, we demonstrated that an EC accelerator operating under sub-zero temperatures and undervoltage leads to better results from the SCA vulnerability perspective. In our experiments we used a chip manufactured in a 250 nm technology. We expect that the vulnerability of chips manufactured in more advanced technologies will be higher, as in those the static current is much higher compared to the dynamic than in less scaled technologies.

In future work we plan to investigate the resistance of cryptographic chips manufactured in a 22 nm technology as well as the impact of aging on horizontal static current SCA attacks.

References

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

[2] I. Kabin, P. Langendoerfer, and Z. Dyka, "Exploiting Static Power Consumption in Side-Channel Analysis," in *2024 IEEE 25th Latin American Test Symposium (LATS)*, Apr. 2024, pp. 1–4. doi: 10.1109/LATS62223.2024.10534604.

[3] I. Kabin, Z. Dyka, A.-A. Sigourou, and P. Langendoerfer, "Static Power Consumption as a New Side-Channel Analysis Threat to Elliptic Curve Cryptography Implementations," in *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, Sep. 2024, pp. 884–889. doi: 10.1109/CSR61664.2024.10679507.

[4] J. Giorgetti, G. Scotti, A. Simonetti, and A. Trifiletti, "Analysis of data dependence of leakage current in CMOS cryptographic hardware," in *Proceedings of the 17th ACM Great Lakes symposium on VLSI*, in GLSVLSI '07. New York, NY, USA: Association for Computing Machinery, Mar. 2007, pp. 78–83. doi: 10.1145/1228784.1228808.

[5] L. Lin and W. Burleson, "Leakage-based differential power analysis (LDPA) on sub-90nm CMOS cryptosystems," in *2008 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2008, pp. 252–255. doi: 10.1109/ISCAS.2008.4541402.

[6] A. Moradi, "Side-Channel Leakage through Static Power," in *Cryptographic Hardware and Embedded Systems – CHES 2014*, L. Batina and M. Robshaw, Eds., Berlin, Heidelberg: Springer, 2014, pp. 562–579. doi: 10.1007/978-3-662-44709-3_31.

[7] S. M. Del Pozo, F.-X. Standaert, D. Kamel, and A. Moradi, "Side-channel attacks from static power: When should we care?," in *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Mar. 2015, pp. 145–150. Accessed: Nov. 28, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/7092373

[8] J. Bhandari, L. Mankali, M. Nabeel, O. Sinanoglu, R. Karri, and J. Knechtel, "Beware Your Standard Cells! On Their Role in Static Power Side-Channel Attacks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 43, no. 12, pp. 4439–4452, Dec. 2024, doi: 10.1109/TCAD.2024.3394736.

[9] T. Moos, A. Moradi, and B. Richter, "Static power side-channel analysis of a threshold implementation prototype chip," in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*, Mar. 2017, pp. 1324–1329. doi: 10.23919/DATE.2017.7927198.

[10] T. Moos, "Unrolled Cryptography on Silicon: A Physical Security Analysis," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 416–442, Aug. 2020, doi: 10.13154/tches.v2020.i4.416-442.

[11] K. Roy, A. Agarwal, and C. H. Kim, 'Circuit techniques for leakage reduction', in *Low-Power Electronics Design*, CRC Press, 2004, pp. 13–1--13--17.

[12] W. Shockley, "The theory of p-n junctions in semiconductors and p-n junction transistors," *The Bell System Technical Journal*, vol. 28, no. 3, pp. 435–489, Jul. 1949, doi: 10.1002/j.1538-7305.1949.tb03645.x.

[13] 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.

[14] 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.

[15] 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.

[16] N. Karimi, T. Moos, and A. Moradi, "Exploring the Effect of Device Aging on Static Power Analysis Attacks," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 233–256, May 2019, doi: 10.13154/tches.v2019.i3.233-256.

[17] T. Moos and A. Moradi, "Countermeasures against Static Power Attacks: – Comparing Exhaustive Logic Balancing and Other Protection Schemes in 28 nm CMOS –," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 780–805, Jul. 2021, doi: 10.46586/tches.v2021.i3.780-805.

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

[19] I. Kabin, Z. Dyka, D. Klann, and P. Langendoerfer, "Horizontal Attacks Against ECC: From Simulations to ASIC," in *Computer Security*, A. P. Fournaris, M. Athanatos, K. Lampropoulos, S. Ioannidis, G. Hatzivasilis, E. Damiani, H. Abie, S. Ranise, L. Verderame, A. Siena, and J. Garcia-Alfaro, Eds., Cham: Springer International Publishing, 2020, pp. 64–76. doi: 10.1007/978-3-030-42051-2_5.

[20] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Berlin, Heidelberg: Springer-Verlag, 2003.

[21] "AEC Documents." Accessed: Nov. 28, 2024. [Online]. Available: http://www.aecouncil.com/AECDocuments.html

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

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