Distinguishability between Multiplication and Squaring Operations: a New Marker

Alkistis Aikaterini Sigourou[1], Zoya Dyka[1,2], Peter Langendoerfer[1,2] and Ievgen Kabin[1]
[1] *IHP – Leibniz-Institut für innovative Mikroelektronik,* Frankfurt (Oder), Germany
[2] *BTU Cottbus-Senftenberg,* Cottbus, Germany
{sigourou, dyka, kabin}@ihp-microelectronics.com

***Abstract*— The most attacked operation in Elliptic Curve cryptographic protocols is the Scalar Multiplication *kP*. As a defence against simple side-channel analysis (SCA), the atomicity principle and several atomic blocks were proposed. In this paper, we demonstrate that binary *kP* algorithms based on atomic patterns are vulnerable to SCA due to clear distinctions between field squaring and multiplication operations. The primary SCA leakage source is the handling of the second operand by the multiplier, creating a visible, one-clock-cycle long marker. We demonstrated this vulnerability by experimenting with Longa's atomic patterns. This vulnerability undermines the SCA resistance of many atomic patterns, enabling key extraction. This issue is particularly critical for scaled technologies, in which scaled-down devices increase leakage currents, further amplifying susceptibility to SCA.**

Keywords— Elliptic Curve (EC), Elliptic Curve Cryptosystem (ECC), *kP*, atomic block, atomic patterns, Simple Power Analysis (SPA), Side-Channel Analysis (SCA) attacks.

I. INTRODUCTION

The Elliptic Curve Cryptosystem (ECC) is crucial in modern cryptography due to its strong security and small key sizes. Its core operation is the EC scalar multiplication, or ***kP*** operation which is often targeted by attacks with the goal to reveal the scalar (key) *k*. Side-channel analysis (SCA) methods have been used for over 25 years to uncover *k*. Binary ***kP*** algorithms, for example double-and-add left-to-right or right-to-left algorithms [1], process the scalar *k* bit-by-bit and are mostly used for a hardware implementation of EC-based cryptographic protocols. The ***kP*** algorithms are a key-dependent sequence of EC point doubling (further PD) and point addition (further PA) operations. PD and PA operations consume different amounts of energy and have different execution times, i.e. they can be distinguished from each other even by a visual inspection of a measured power or electromagnetic trace of a single ***kP*** execution. Small differences in the trace can be analysed using statistical or machine learning methods. SCA techniques analysing a single trace, exploit variations in the power consumption to separate the analysed trace into shapes corresponding to key bits '0' or '1'.

To prevent Simple Power Analysis (SPA) power shapes for processing each key bit have to be independent of the processed key bit value. Atomicity is one of the well-known countermeasure principles against SPA attacks, with various atomic-pattern ***kP*** algorithms proposed in the literature [2], [3], [4], [5]. The atomicity principle [2], introduced in 2004, aims to countermeasure simple SCA attacks and improve the computation efficiency of scalar multiplications. Each PD will be represented as a sequence of 10 atomic blocks, and each PA as a sequence of 16 atomic blocks. Atomic blocks are quite identical: each atomic block is a short (the same) set of instructions. Power profiles of atomic blocks are very similar each to other, i.e. atomic blocks are SCA-equivalent. Researchers since, have developed optimized atomic patterns for PDs and PAs to reduce the ***kP*** execution time [3], [4], [5]. An atomic block's instructions include field operations and data storing instructions, with different registers addressed for different data processing. The effectiveness of atomic blocks against SCA attacks depends on two assumptions: storing/reading of the same data into/from different registers as well as calculating the same field operations using different data are indistinguishable from the SCA point of view. Key-dependent addressing of design blocks as well as data processed during field multiplications were successfully exploited to reveal the key, see [6], [7], [8] and [9], respectively.

In this work, we demonstrate the vulnerability of atomic block patterns to simple SCA attacks, due to a new, short but good visible, marker. This marker allows us to distinguish between field multiplications and field squaring operations independently of the method implemented by the multiplier for the field product calculation.

II. DEMONSTRATION OF THE DISTINGUISHABILITY

A. Implemented atomic patterns

Using Longa's atomic patterns [3] for PD and PA operations, we implemented the binary double-and-add left-to-right ***kP*** algorithm for the NIST EC P-256. Each of Longa's atomic blocks consists of the MNAMNAA field operations sequence, with field Multiplication denoted with M, Negation with N and Addition with A. Our ***kP*** architecture consists of 256-bit long registers and functional blocks for addition/subtraction and multiplication of *GF(p)* elements. The block Controller manages data loading and field operations, connecting registers and functional blocks via a multiplexer. Only one block can load output data to the bus during a clock cycle. We synthesized the design for the IHP 250 nm cell library SGB25V [10] with a clock cycle time of 30 ns using Cadence's SimVision vs. 15.20-s053. We used Synopsys PrimeTime vs. Q-2019.12-SP1 to simulate the power trace of a single ***kP*** execution.

B. Distinguishability of multiplication and squaring operations

Here, we concentrate only on the field Multiplications. The typical power profile of a Multiplication in our design could be performed either with two different or two identical operands, i.e. for a field multiplication vs. a field squaring operation. In our testing, we observed that multiplications and squaring operations are not identical from the SCA point of view, independent of the multiplication formula implemented. That is due to the fact that for squaring (opposite to multiplication), the second operand has the same value as the first multiplicand, and this value will be read from the same register. Therefore, the multiplexer is not staying active on that clock cycle and hence does not consume energy. That leads to higher power consumption of the transfer of the 2nd

operand during the multiplication in comparison with the one during the squaring operation. Thus, the reasons for this vulnerability are data-bit as well as the address-bit effects.

C. Generalization of the vulnerability

The observed distinguishability can be successfully exploited for revealing the processed scalar *k* attacking atomic pattern algorithms [2], [3], [5]. This is due to the fact that multiplication and squaring operations are no longer identical from the SCA point of view. The PD and PA patterns consist of a different number and sequence of multiplications and squaring operations, hence, the power trace can be separated into PDs and PAs. This allows to successfully reveal the key without the need for a correlation analysis, in contrast to [9]. Please note that the distinguishability described here is an inherent vulnerability of atomic patterns [2], [3] and [5]. An exception is the atomic patterns proposed in [4].

The described distinguishability can be effectively applied to attacking (at least) hardware implementations. We assume that this distinguishability can also be successfully exploited in static power analysis attacks [11], which are especially critical for scaled technologies. Furthermore, it can be exploited together with the address-bit vulnerability, which leverages key-dependent addressing of design blocks or registers. Examples of horizontal address-bit SCA attacks against Montgomery ladder, as well as Rondepierre's atomic patterns *kP* algorithm, are given in [6], [8] and [12].

D. Potential solutions

To prevent the distinguishability, designers can follow the following approaches:

- By inserting a dummy addressing between the transfer of the 1st and 2nd multiplicand. For example, the multiplier can be addressed to write (quite randomly and unknowingly to the attackers) its output value to the Bus. This approach requires an additional clock cycle for each multiplication as well as squaring operation.
- Using a dummy register to store the 1st multiplicand simultaneously with its transfer to the multiplier. In the case of a squaring operation, the 2nd multiplicand will read from the dummy register. Thus, the addresses of registers providing both multiplicands will be different. Consequently, the multiplexer consumes energy even when providing the same value as in the previous clock cycle.

More ideas to prevent address-bit vulnerability using dummy addressing and redundant (dummy) registers can be found in [13]. In our future work, we plan to investigate the effectiveness of different approaches. Additionally, we will focus on their suitability as a mechanism for the automated design of cryptographic chips with increased resistance to physical attacks.

III. Conclusion

In this work, we demonstrate that passing the 2nd operand to the multiplier is a new marker leading to the distinguishability between multiplications and squaring operations, at least for hardware implementations of $k\boldsymbol{P}$ algorithms. This distinguishability is a strong SCA leakage source and can be exploited by attacking for example $k\boldsymbol{P}$ algorithms based on atomic patterns. Since the sequence of multiplications and squaring operations differs for PD and PA in most atomic patterns algorithms it makes atomic blocks less equivalent from an SCA point of view, allowing the key to be revealed without correlation analysis. This is critical for devices manufactured in each technology. Especially, scaled technologies exhibit heightened susceptibility due to increased static-leakage currents making them more vulnerable to static power SCA attacks.

References

[1] D. R. Hankerson, A. J. Menezes, S. A. Vanstone, D. Hankerson, A. Menezes, and S. Vanstone, Guide to elliptic curve cryptography. in Springer professional computing. New York, NY: Springer, 2004.

[2] B. Chevallier-Mames, M. Ciet, and M. Joye, "Low-cost solutions for preventing simple side-channel analysis: side-channel atomicity," IEEE Trans. Comput., vol. 53, no. 6, pp. 760–768, Jun. 2004, doi: 10.1109/TC.2004.13.

[3] P. Longa, "Accelerating the Scalar Multiplication on Elliptic Curve Cryptosystems over Prime Fields," 2008. Accessed: May 15, 2023. [Online]. Available: https://eprint.iacr.org/2008/100

[4] C. Giraud and V. Verneuil, "Atomicity Improvement for Elliptic Curve Scalar Multiplication," in Smart Card Research and Advanced Application, vol. 6035, D. Gollmann, J.-L. Lanet, and J. Iguchi-Cartigny, Eds., in Lecture Notes in Computer Science, vol. 6035. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 80–101. doi: 10.1007/978-3-642-12510-2_7.

[5] F. Rondepierre, "Revisiting Atomic Patterns for Scalar Multiplications on Elliptic Curves," in Smart Card Research and Advanced Applications, A. Francillon and P. Rohatgi, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2014, pp. 171–186. doi: 10.1007/978-3-319-08302-5_12.

[6] I. Kabin, Z. Dyka, D. Kreiser, and P. Langendoerfer, "Horizontal address-bit DPA against montgomery kP implementation," in 2017 International Conference on ReConFigurable Computing and FPGAs (ReConFig), Cancun: IEEE, Dec. 2017, pp. 1–8. doi: 10.1109/RECONFIG.2017.8279800.

[7] 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.

[8] I. Kabin, Z. Dyka, D. Kreiser, and P. Langendoerfer, "Horizontal Address-Bit DEMA against ECDSA," in 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris: IEEE, Feb. 2018, pp. 1–7. doi: 10.1109/NTMS.2018.8328695.

[9] A. Bauer, E. Jaulmes, E. Prouff, and J. Wild, "Horizontal Collision Correlation Attack on Elliptic Curves," in Selected Areas in Cryptography -- SAC 2013, vol. 8282, T. Lange, K. Lauter, and P. Lisoněk, Eds., in Lecture Notes in Computer Science, vol. 8282. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 553–570. doi: 10.1007/978-3-662-43414-7_28.

[10] "IHP : Leibniz Institute for High Performance Microelectronics." Accessed: Sep. 19, 2024. [Online]. Available: https://www.ihp-microelectronics.com/

[11] 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), London, United Kingdom: IEEE, Sep. 2024, pp. 884–889. doi: 10.1109/CSR61664.2024.10679507.

[12] I. Kabin, P. Langendoerfer, and Z. Dyka, "Vulnerability of Atomic Patterns to Simple SCA," in 2023 IEEE East-West Design & Test Symposium (EWDTS), Batumi, Georgia: IEEE, Sep. 2023, pp. 1–4. doi: 10.1109/EWDTS59469.2023.10297074.

[13] levgen KABIN, Z. Dyka, D. KLANN, and P. Langendörfer, "Cryptographic hardware accelerator with dummy block addressing for protection against side channel attacks," US20240111908A1, Apr. 04, 2024 Accessed: Mar. 05, 2025. [Online]. Available: https://patents.google.com/patent/US20240111908A1/en