A Novel Model for Resisting Side Channel Attack by Masking of Gates

DOI : 10.36909/jer.ICMET.17165

Jyotirmoy Pathak*, Suman Lata Tripathi

School of Electronics and Electrical Engineering, Lovely Professional University, India

*Corresponding Author: jyotirmoy.16082@lpu.co.in

ABSTRACT

The XOR gate is often used in cryptography modules. These cells' hardware implementations are subject to power analysis attacks. Correlation power attacks (CPAs) allow an attacker to estimate a highly correlated hypothetical value from the actual hidden value. By masking the input and unmaking the output, the present countermeasure technology randomises the power consumption pattern and increases the number of cells. We proposed the mask XOR gate in this study because they do not require cell unmasking and demonstrate a smaller correlation between power traces and input data.

Keyword: Power Attack, Masking, Correlation Power Attack,

Introduction

In recent decades, the integrated circuit supply chain has become increasingly globalised, owing to the semiconductor industry's ever-increasing design complexity and cost. On the other hand, globalisation comes with a cost. While globalisation of IC design, fabrication, assembly, and deployment reduces overall costs, it introduces significant risks to IP privacy and integrity. The two primary risks associated with the international IC supply chain are malicious design modification (Ujjwal.G et al., 2018, Meng.L et al., 2018) and intellectual property theft via reverse

engineering (Wenchao L, et al., 2013, Shahed E.Q. et al., 2016, Subramanyan P. et at., 2014, Sugawara T, et al., 2014, Torrance R, et al., 2009).

The design is disclosed to potentially malicious adversaries, such as unreliable foundries and end users, providing a risk of reverse engineering and intellectual property theft. On the other hand, foundries have total access to the layout and can thus easily extract information down to the transistor level (Shahed E.Q, et al., 2016, Subramanyan P, et al., 2014, Torrance R,et al., 2009). As illustrated in Figure 1, malicious end users can reproduce the circuit architecture using a packaged integrated circuit acquired from the market (Torrance R,et al., 2009). The term "physical reverse engineering" refers to the process of reconstructed layouts and net list extraction. Such reverse engineering techniques have grown rapidly during the previous decade, successfully reconstructing devices from major semiconductor companies at advanced technology nodes. As a result, to safeguard hardware intellectual property, the design must be protected against side channel attacks and reverse engineering. Indeed, the more serious threat of malicious modification necessitates some degree of successful reverse engineering in the first place.

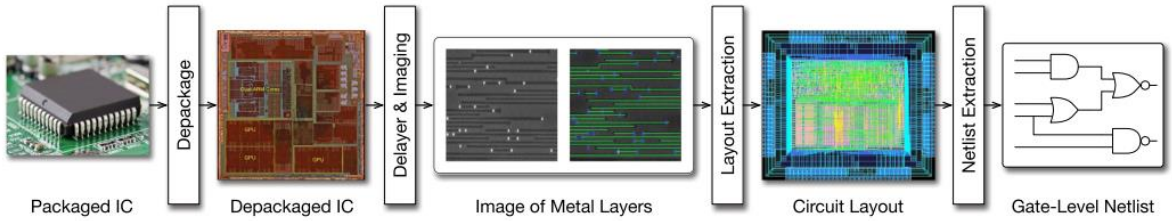

Figure 1. Flow chart fot Reverse Engineering

Nowadays, computing hardware is becoming smaller, more affordable, and faster as a result of the development of new technologies for fabrication and greater design complexity (Nandan D et al., 2018). As a result, crypto-hardware may now be easily integrated into a wide variety of devices,

ranging from smart cards to smart phones, and prepaid cards (Nandan .D 2020). Cryptography study focuses on the computational complexity of cryptographic algorithms, cyphers, and protocols. Given that cryptography's major objective is to enable secure communication while retaining confidentiality, cryptography hardware security is crucial. As a result, an attack on the hardware that executes cryptographic algorithms is gaining attention. Anti-terrorist countermeasures are being developed and analysed.

Power attack (PA) is the most targeted side-channel assault danger to cryptographic circuits; it circumvents the cryptographic algorithms' theoretical strength. The purpose of power attack analysis is to extract internal information from a circuit's internal node via leaked knowledge about the cryptographic algorithm's hardware implementation (Kocher et al., 1999). The power analysis attack demonstrates the limitations of hardware implementation; MOS transistor-based VLSI design is the de facto standard for low power design using electronic design association (EDA) tool standard libraries. The CMOS cell's dynamic power maintains a linear relationship with the input data. Because the dynamic component of power leaks considerable information during computation, an attacker can determine the cryptographic device's hidden secret information by matching the device's power consumption to its input pattern.

The cryptography module's power consumption is equal to the total power utilised by the underlying cells. As a result, the power consumption of each gate must be independent of the input data to be processed. A feature that is resistant to attack must be implemented at the transistor level. The normalised energy deviation (NED) and the normalised standard deviation (NSD) are two evaluation criteria that are calculated depending on the amount of energy required to compute at the output level. NED displays the fluctuation in energy consumption each cycle. The NSD model exhibits a variance in energy usage as a function of input combinations. The NED-NSD

value should be as low as feasible, ideally zero; it should also be resistant to power attack (Mace et al., 2006, Renauls et al., 2011).

Hiding and masking are two widely used logic-level countermeasures that focus on scrambling the power consumption pattern associated with the input such that it has a weaker correlation with the processed data. The criteria for concealing countermeasures are to make the cryptographic module's power consumption dependent on both intermediate values and the operation to be performed. The concealment strategy demonstrates balance or equal power for all hypothesis keys, a correlation coefficient near zero, and is insufficient to make a proper conclusion. The adversary employs the dependency of power consumption with hamming weights or hamming distance in the power analysis attack. The cryptographic circuit's output is determined by the hamming weight of the final output terminal. The PA resistant mask circuit generates many internal nodes; instead of a single node, the power value is determined by all internal nodes. Because the adversary only has access to the output terminal, he or she will not have access to the power information for an internal node and so will be unable to guess data processing.

Side Channel Attack

Side channel attacks are typically conducted using information obtained via the non-primary interface of a cryptosystem's physical implementation, such as power, electromagnetic breaches and timing. Power Analysis Attacks: The literature discusses two distinct types of power analysis techniques: Simple Power Analysis (SPA) and Differential Power Analysis (DPA) (DPA). Both of them are capable of measuring the amount of current consumed per unit of time. For instance, RSA's modular exponentiation algorithm (m=c^d mod n, where the attacker wishes to discover the private key d), which does square operations if the key bit is zero and multiply operations if the

key bit is one, conducts square operations if the key bit is one. As illustrated in Figure 1, the square and multiply operations are readily visible from the device's current traces. Along with SPA, the attacker may conduct further attacks to recover the victim's private key. A Differential Power Analysis (DPA) (Paul Kocher et al., 1999, Popat et al., 2018) that is algorithm-specific but does not require knowledge of the algorithm's physical implementation. It is simple and inexpensive to carry out. The fundamental concept is to link the device's power consumption with the encryption data, including the key. A more sophisticated attack is DPA, which is used to reveal multiple key bits simultaneously, reducing the time required to extract the complete key. With the use of high-speed ADC (analogue to digital converters) and DSO, power samples are collected for millions of iterations of the encryption process.

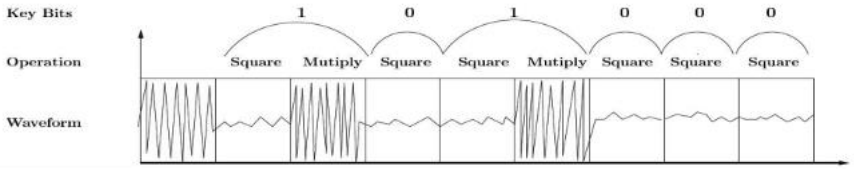

Figure 2. Simple Power Analysis trace

On the basis of acquired power samples, it is assumed that key bits exist. From pre-assumed key bits, the respective input bits are estimated. If this hypothesis is right, then the subsequent stage will assume the relevant bits. When an assumption is incorrect, it is noted that 50% of test scenarios appear to be identical to the hypothesis. After recovering a portion of the key, the attacker may conduct a brute force attack on the remaining key bits in order to recover the complete key.

Electromagnetic Analysis Attack: These assaults are based on electromagnetic signals created by current flowing through devices (Quisquater et al., 2001, Gabdolfi et al., 2001). Electromagnetic Analysis is classified into two types: Simple Electromagnetic Analysis (SEMA) and Differential

Electro-Magnetic Analysis (DEMA) (DEMA). However, there are some distinctions between a power analysis assault and an electromagnetic analysis attack. While power analysis considers solely the circuit's power usage, electromagnetic analysis is primarily concerned with antenna placement (Popat et al., 2018). In general, EM attacks can be carried out by attackers located in faraway locations. For instance, amplitude demodulators are required to conduct attacks that are fairly distant from the circuit. Electromagnetic attacks are not always perfect, as they might be damaged as a result of environmental noise and measuring problems.

Timing Information Attack: The side-channel attack demonstrates how computing time reveals critical information about secret keys (Kocher et al., 1996, Dhem et al., 1998). The assumption made here is that an adversary is aware of how a cryptographic algorithm is implemented in hardware, and that this attack is entirely dependent on that implementation. An attacker can take advantage of the variable run time cryptosystem. For example, the modular method RSA (m=c^d mod n, where the attacker wishes to discover the private key d) determines the lone square operation if the key bit is reset or the multiply-square operation if the key bit is set. This may be used to reveal information about a secret key. An adversary can begin by assuming either zero or one for the first key bit and observing which assumption produces the best match between actual and guessed computing time. This technique is repeated until all significant bits have been anticipated. As a result, the whole key search space is condensed. This attack is described as fairly simple in terms of computation.

CMOS Design: Pass Transistor Logic

The pass transistor-based circuit design technique is used to reduce the complexity of the circuit at the expense of voltage swing. (Leblebibi et al., 1996, Khan.A et al., 2014) illustrates the many

topologies of the XOR gate using a lesser number of transistors. The powerless and groundless PTL architecture achieves the functionality of XOR but with the constraint that output swing is limited. PTL XOR, as illustrated in Figure3, requires only four transistors, a reduction of 66.67 percent in transistor count over static XOR architecture. The output voltage is reduced as a result of the threshold voltage Vtp. XOR outputs Vtp for input 00, Vdd for input 01, and 10 and ground for input 11. Given that degraded output has no effect on succeeding stage threshold loss, refrain from further degrading production. It depends on whether they result in an additional drop in the subsequent stage. Table 1 compares the XOR cell characteristic with various logic. When compared to static design, PTL logic is an excellent solution for minimising the number of transistors. In static architecture, delays are minimised due to the availability of power and ground rail. PTL logic consumes less power due to the reduced gate count and the absence of a direct short path between the power and ground rails. Static current consumption is greatly reduced with PTL logic. PTL XOR saves significant amounts of power but at the expense of latency.

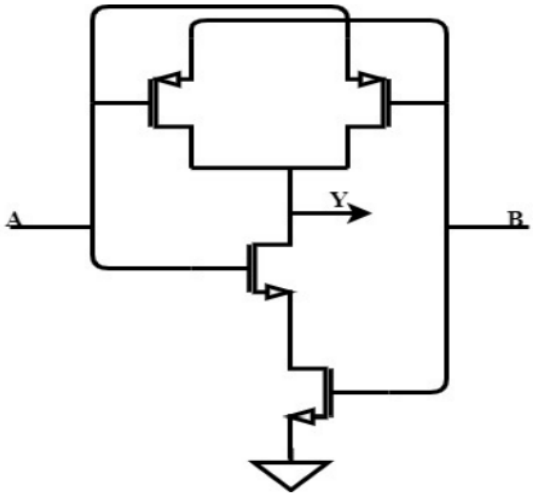

Figure 3. XOR Gate using PTL

NED is the ratio of the greatest energy consumption (Emax) to the minimum energy consumption (Emin) for all feasible input combinations (Ma J et al., 2014). NSD determine the degree to which energy consumption varies with each input.

$$NED = \frac{E_{max} - E_{min}}{E_{max}} \quad (1)$$

$$NSD = \frac{\sigma_E}{E_{avg}} \quad (2)$$

Table 1. Different Parameter comparison of Static and PTL XOR Gate

	Delay(ns)	**Power(nW)**	**No of Transistors**	**Emax(pJ)**	**Emin(pJ)**	**NED**	**NSD**
Static XOR	0.09	20.4.4	12	1.17	36.34	96.8	94.2
PTL XOR	253.4	43.25	4	2.18	8.87	76.21	62.17

NSD is a measure of how consumed energy is distributed about the mean; a big value of NSD implies that energy is widely dispersed around the mean, while a small number indicates that it is close to the mean. NED-NSD should ideally approach zero to increase resilience to power analysis attacks.

Masking of Gate

It is not possible to completely eliminate the data dependency. Correlations between actual and expected power can be reduced by adding noise or lowering the power value at an internal terminal. Masking applied algorithmically without affecting the cryptographic circuit's power consumption features.

$$A_m = A \wedge m_a$$

$$B_m = B \wedge m_b \quad (3)$$

$$Q = Q_m \wedge m_q$$

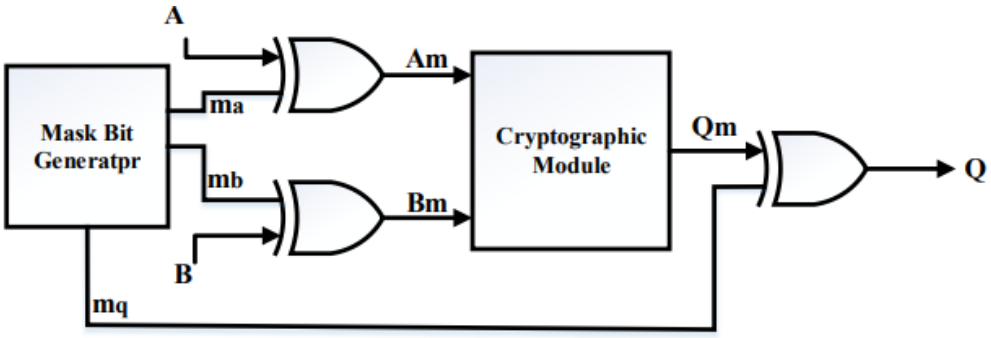

Figure 4. Masked XOR Gate

Masking is a technique for randomising internal results that can be used at either the algorithmic or gate level. In Figure 4, the input is XORed with random bits, and the output is then XORed with their random bits. Figure 4 illustrates the architectural description of the normal and masks gates. A random mask bit generated by a mask generator circuit is applied to each gate of the regular gate. The mask generator generates a bit that is XORed with the input signal. Similarly, the mask gate's output is unmasked using a mask bit generated externally or internally by the circuit (Masoumi.M, 2019).

Proposed Design

The proposed mask XOR architecture depicted in Figure 5 is implemented using a 6-XOR and a 1-NOT gate. The binary expression for mask XOR is given in Equation (4). The m0, m1 mask bit obscures the current inputs A and B. The unmasked output is computed directly; no additional XOR or mask bit is necessary. The circuit's binary expression checks the XOR gate's functionality. Increased cell count results in an increase in delay and power consumption when compared to static architecture. Masked XOR consumes 515.5 nW of power, while static XOR consumes 202.8 nW.

Boolean function for Masked XOR gate

$$Y= (((A \wedge m0) \wedge (m0 \wedge m1)) \wedge ((B \wedge m0) \wedge (m0 \wedge m1)))' \qquad (4)$$

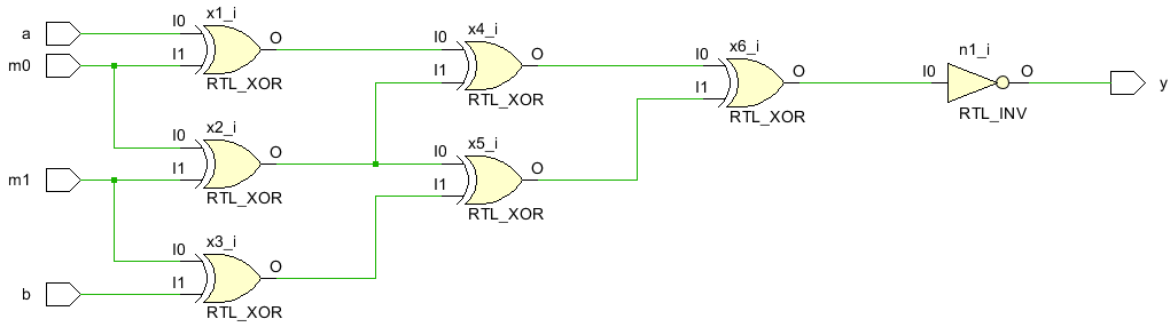

Figure 5. Masked XOR gate

Mask XOR implements the XOR operation on the mask bits '01' and '10' as shown in Figure6. The mask gate's truth table at the internal terminal demonstrates that the hamming weight is uniformly distributed "2". Because the equal value of the hamming weight present on the internal terminal does not store value, the energy required to set the output node is distributed on an internal terminal and is statically independent; in order to breach the mask gate's security, the attacker must know the value of each intermediate terminal.

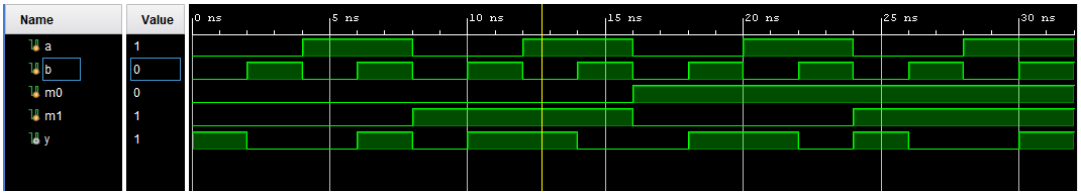

Figure 6. Output waveform of Masked XOR gate

Security Measures

Mask gates provide an additional layer of security at the expense of increased gate count and power consumption. The criteria for an attack-resistant gate are that the intermediate output must be independent of the primary input and distributed uniformly. Due to the uniform distribution of the hamming weight, the output is independent of the primary input; a reverse engineer would be unable to predict the sensitive information presented in (Lin et al., 2007, Sasdrich et al., 2020) of the circuit. The term "hamming weight" refers to the amount of energy required to move from the logic level to the physical level. In a normal gate, the transition from low to high consumes more energy than the transfer from high to low. The difference between the average energy $E_{(y=1)}$ and $E_{(y=0)}$ at the masked gate should be as little as possible. The difference in mean energy between masked and unmasked XOR is 1.5625fJ. As a result, it concludes that the proposed masked XOR gates are excellent candidates for attack mitigation. Table 2 shows the comparison of energy parameters of masked XOR gate.

Table 2. Energy parameter of Masked Gate

Masked Cell	**E_{Min}(pJ)**	**E_{Max}(pJ)**	**NED**	**NSD**	**Pearson Coefficient**
XOR with '01'	0.08	15.36	8.9	1.53	0.0358
XOR with '10'	0.09	16.86	9.7	1.368	0.0418

Conclusion

This paper discusses the encryption and decryption processes used in crypto-chips. Although it is one of the most widely used DFT techniques, scanning cryptographic equipment creates a backdoor for security threats. The secret key can be acquired via side-channel attacks, device injection failures, or by utilising existing test infrastructure. This work proposes an efficient and power attack-resistant XOR cell with equally distributed power values to the internal terminal. The

proposed masked XOR gate reduces the number of cells by 11.11 percent. In comparison to the unmask cell, the lower value of NED and NSD suggests a complicated arrangement that needs the attacker to successfully estimate the hidden value. Additionally, the correlation coefficient for the proposed cell is improved by 42.13 percent.

References

Dhem, J. -F. , Koeune, F. , Leroux, P. -A. , Mestr, P. , Quisquater, J. J. & Willems, J. -J. (1998). A practical implementation of the timing attack. In J. Quisquater & B. Schneier (Eds.). CARDIS, Lecture Notes in Computer Science (Vol. 1820, pp. 167-182). Berlin: Springer

Gandolfi, K. , Mourtel, C. , Olivier, F. (2001). Electromagnetic analysis: concrete results. In . K. Ko et al. [cKKNP01], (pp. 251261).

Kocher, P., Jaffe, J., & Jun, B. (1999, August). Differential power analysis. In Annual International Cryptology Conference (pp. 388-397). Springer, Berlin, Heidelberg.

Kocher, P. C. (1996). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In N. Koblitz (Ed.), CRYPTO, Lecture Notes in Computer Science (Vol. 1109, pp. 104113). Berlin:Springer.

Khan A.A, Pandey S, Pathak J, (2014), A review paper on 3-T Xor Cells and 8-T Adder design in Cadence 180nm, International Conference on Convergence of Technology, Pune.

Leblebici, Y., & Kang, S. M. (1996). CMOS digital integrated circuits: analysis and design. McGraw-Hill.

Lin, J. F., Hwang, Y. T., Sheu, M. H., & Ho, C. C. (2007). A novel high-speed and energy efficient 10-transistor full adder design. IEEE Transactions on Circuits and Systems I: Regular Papers, 54(5), 1050-1059.

Macé, F., Standaert, F. X., Hassoune, I., Legat, J. D., & Quisquater, J. J. (2004, November). A dynamic current mode logic to counteract power analysis attacks. In Proc. 19th International Conference on Design of Circuits and Integrated Systems (DCIS) (pp. 186-191).

Ma, J., Li, X., & Wang, M. (2014). Power-aware hiding method for S-box protection. Electronics Letters, 50(22), 1604-1606.

Masoumi, M. (2019). A highly efficient and secure hardware implementation of the advanced encryption standard. Journal of Information Security and Applications, 48, 102371

Meng Li, Bei Yu, Yibo Lin, Xiaoqing Xu, Wuxi Li, and David Z. Pan. (2018) A practical split manufacturing framework for Trojan prevention via simultaneous wire lifting and cell insertion. In Proceedings of the Asia and South Pacific Design Automation Conference. 265–270.

Nandan D, Kanungo J, Mahajan A, (2018), An efficient architecture of iterative logarithm multiplier, International Journal of Engineering and Technology, 7, (2.16), 24-28.

Namdan D, An efficient antilogrithmic converter by using correction scheme for DSP processor, Traitement du Signal, 37(1), 77-80.

Popat.J, Mehta.U, (2018), Hardware Security in case of scan based attack on Crypto Hardware, Internationl Journal of VLSI design& Communication System, vol. 9, no. 2.

P. Subramanyan, N. Tsiskaridze, Wenchao Li, A. Gascon, Wei Yang Tan, A. Tiwari, N. Shankar, S. A. Seshia, and S. Malik. (2014). Reverse engineering digital circuits using structural and functional analyses. IEEE Trans. Emerg. Top. Comput. 2,(1), 63–80.

Quisquater, J. -J., Samyde, D. (2001). ElectroMagnetic analysis (EMA): Measures and countermeasures for smart cards. In I. Attali & T. P. Jensen (Eds.), E-smart, Lecture Notes in Computer Science (Vol. 2140, pp. 200210). Berlin: Springer.

Renauld, M., Kamel, D., Standaert, F. X., & Flandre, D. (2011, September). Information theoretic and security analysis of a 65-nanometer DDSLL AES S-box. In International Workshop on Cryptographic Hardware and Embedded Systems(pp. 223-239). Springer, Berlin, Heidelberg

Randy Torrance and Dick James. (2009). The state-of-the-art in IC reverse engineering. In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems. Springer, 363–381

Sasdrich, P., Bilgin, B., Hutter, M., & Marson, M. E. (2020). Low-Latency Hardware Masking with Application to AES. IACR Transactions on Cryptographic Hardware and Embedded Systems, 300-326.

Shahed E. Quadir, Junlin Chen, Domenic Forte, Navid Asadizanjani, Sina Shahbazmohamadi, Lei Wang, John Chandy, and Mark Tehranipoor, (2016). A survey on chip to system reverse engineering. ACM J. Emerg. Technol. Comput. Syst. 13,(1), 6:1–6:34

Takeshi Sugawara, Daisuke Suzuki, Ryoichi Fujii, Shigeaki Tawa, Ryohei Hori, Mitsuru Shiozaki, and Takeshi Fujino. (2014). Reversing stealthy dopant-level circuits. In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems. Springer, 112–126.

Ujjwal Guin, Ziqi Zhou, and Adit Singh. (2018), Robust design-for-security architecture for enabling trust in ic manufacturing and test. IEEE Trans. VLSI Syst. 26 (5), 818–830.

Wenchao Li, A. Gascon, P. Subramanyan, Wei Yang Tan, A. Tiwari, S. Malik, N. Shankar, and S. A. Seshia, (2013). WordRev: Finding word-level structures in a sea of bit-level gates. In Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust. 67–74