Circuit Masking Schemes: New Hope for Backside Probing Countermeasures?

Ana Čović, Fatemeh Ganji, Domenic Forte
ECE Department, University of Florida, (anaswim, fganji)@ufl.edu, dforte@ece.ufl.edu

***Abstract*—Sensitive data can be extracted by mounting physical attacks, e.g., photon emission analysis, micro-probing, etc., on integrated circuits (ICs). In this paper, our ultimate goal is to examine provable security approaches that increase the number of simultaneous probes needed to perform probing in order to see how they can complement physical anti-probing countermeasures. Commonly applied mathematical models for probing attacks have employed randomized bits to mask the input, and modified computations. As the number of masks increases, the number of probes needed to extract the secret data increases linearly, assuming noise-free conditions. In another attempt, noisy leakage models have been developed to better mimic real-world scenarios, but their complexity is a major drawback. Hence, extensive research has been performed to show connections between noisy leakage models and probing models. The goal of this survey is to relate the notion of masking with physical backside attack countermeasures, which are limited in practice. To this end, our first milestone is to unify provable probing and side-channel models in order to develop and realize more practical countermeasures.**

***Index Terms*—Hardware Security, Probing, Side Channels, Masking.**

I. Introduction

Sensitive on-chip assets, such as firmware and cryptographic keys, can be extracted by mounting physical attacks on integrated circuits (ICs), e.g., photon emission analysis, micro-probing, etc. These attacks can be launched on an IC through either the front-side (i.e., passivation) or the back-side (i.e., a silicon substrate). Unlike frontside attacks, which are confronted by obstacles in the form of upper metal layers, straightforward access to transistors and logic gates can be granted through the back-side. Various physical countermeasures against back-side probing attacks have been proposed, such as physical probe detection [1], [2] and substrate shields connected to inner-logic using through-silicon-vias (TSVs) [3]. These ad-hoc countermeasures make back-side attacks significantly more complex. Nevertheless, the first one could be vulnerable against bypass attacks and circuit edit, while the latter one hinders failure analysis, a critical step for process and design engineers. To address these issue by complementing physical countermeasures, in this work, we aim to survey provable security approaches.

Commonly applied mathematical models for probing attacks have employed randomized bits to mask the input and modify computations. The masking process hides the input signal using t random numbers, splitting the signal into t shares. As the number of masks increases, the number of probes needed to extract the secret data increases linearly, assuming noise-free conditions, while the area overhead increases exponentially. Mathematical models define the strength of the adversary by deriving the bounds on the amount of probed data needed for a successful probing attack. The amount of probed data refers to a number of required probes to successfully launch an attack. Probed data is considered to be noisy, which allows the application of the side-channel attack models. These models, to prevent side-channel attacks, require leak-free gates to produce random (or fresh) masks. Unification of side-channel attack models and probing models defines an adversary, who has access to at most t simultaneous probes at each time period. Unlike the pure side-channel models, the unified model considers the physical probes. Furthermore, when implementing masking schemes, another challenge to face is the presence of glitches, [4], which inherently happen in logic circuits and reduce the effectiveness of random masks.

In addition to the security of the models, the composability of implemented masked circuits has been investigated for the higher number of random masks through the introduction of notions of non-interference, strong non-interference, and probe-isolating non-interference. These concepts have been developed for the prevention of side-channel attacks, but as they are heavily based on t-probing models, they are relevant with our goal of unifying provable probing and side-channel models to develop and realize more practical countermeasures.

Each of these security and composability frameworks carries mature research of masked circuits secured in corresponding attack models. Linear (XOR) gates have a direct and simple masking concept, while the research effort has been devoted to creating the masked version of AND gate, or multiplication operator to tackle implementation challenges. This reinforces the concept of "gadgets", i.e., the masked version of the gate that is a cluster of gates.

The rest of the paper is organized as follows. Probing and noisy leakage models are discussed in Sections II. Specific gadgets are presented in Section III. Section IV analyzes back-side probing in regard to circuit masking and side-channel analysis, and we conclude in Section V.

II. Attack Models

To ensure the overall security of the circuit, security designers must develop a countermeasure, resistant to (virtually all) attacks. The security must be provable, and consider the

This work was supported in part by NSF (project number 1717392), SRC (task ID 2769.001), and AFOSR MURI (project number FA9550-14-1-0351).

strongest adversary, or the worst-case privacy[1] destruction. Masking schemes were initially designed as a countermeasure against side-channel attacks. Once noise was considered in [6] for side-channel attacks, it did not take long to recognize invasive probing as the strongest side-channel attack.

A. Threshold Probing Models

The probing model in [5] was one of the first used to quantify the robustness of masking schemes against probing attacks. It considers a noise-free scenario, in which an adversary, is limited to t number of probes (a realistic assumption in practice). The number of probes t is a measure of the adversary's strength, as well as the cost of the attack. The adversary is also limited in the sense that observing different wires with the same probe within one clock cycle is impossible. To prove the security of masking schemes, two probing models are presented in [5]: threshold t probing model, and the random threshold probing model, where the input data x gets masked with random masks. Security is proven by the introduction of a simulator representing the adversary's view, who has a black-box access to the circuit. A random probing model has been also discussed, where the adversary learns about the underlying secret only with some probability. This definition is beneficial to consider average-case security instead of the worst-case scenario.

B. Model of Leaking Computation (Noisy Leakage Model)

Model of leaking computation was introduced in [7], in which the adversary is given noisy leakage function $f(x)$ with f being a noisy function, and x is a biased input. Main assumptions are (1) noise level is high, and (2) the statistical distance between distribution x and conditional distribution $x \mid f(x)$ are bounded by δ. For the δ-noisy leakage model, this distance is described through the Euclidean norm (EN) metric. This is a *natural* representation of a noisy leakage model, as it is very detailed, considers every processing step, and any type of noise can be considered as long as it satisfies statistical metrics. This provides a generalized definition of the noise, which plays the main role in depicting the bound between two distributions. Noise is the main parameter in describing this model, and it is assumed that the security designer can control noise parameter δ, which is inversely proportional to the amount of noise in computation. The value of $\delta = 0$ means that the signal contains full noise. The limitation of this model is that it considers leak-free components for producing random masks.

C. Reduction of Noisy Leakage Model to Probing Model

Since a $\delta(EN)$-noisy leakage model is very detailed, any state-of-the-art masking scheme would have to undergo tremendously extensive security analysis to be provably secure in that model [7]. Correspondingly, efforts have been made to show that the security of the noisy leakage model can be reduced to the security in the probing model introduced in [5]. The first attempt to unify these models has been made in [8], with the additional goal of combining the noisy leakage models. They use the same δ noise model as in [7], where the noise can be efficiently computed. However, instead of the Euclidean norm metric, statistical distance (SD) (i.e., in a general form) is used. The same noise characteristics are considered, where inputs are biased rather than uniform, and noise function is δ-noisy following the concept of indistinguishably of distributions. The reductions from noisy leakage model to probing model is done in two steps, as shown in Figure 1: (1) noisy leakage model to random threshold probing model, and (2) random threshold probing to threshold t-probing model. According to to [9], a reduction from EN-noisy leakage model to threshold probing model is loose in a sense that an extension from Boolean masking to larger fields (i.e., working on bytes or words) is not feasible. Nevertheless, Duc's model simplifies in security proofs with the main contribution as being a remedy for shortcomings in the EN-noisy leakage model [7].

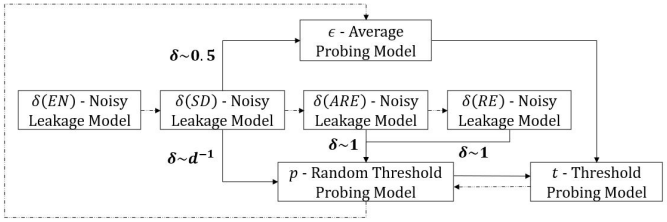

Fig. 1. Attack model development flow shown in dotted line, attack model security reduction flow shown in solid line with corresponding loss in noise parameter

D. Noisy Leakage Model to Average Random Probing Model Reduction

As aforementioned, [9] claims that the security reduction in [8] is not tight, as there is a large *gap* between threshold t-probing model and SD-noisy leakage model. Therefore, the new *average probing model* was introduced in [9], which allows tighter reduction from SD-noisy leakage model to the probing model. The average probing model is similar to the random probing model in [5], where the leakage probability ϵ is uniformly drawn. The reduction from δ-noisy leakage model to ϵ-average probing model results in the δ decreasing by the factor of 0.5, which means that the number of probes required to extract meaningful information decreases. This means that loss in the noise parameter represents the loss in security of the circuit. However, this model requires leak-free components, which is the main drawback.

E. Further Noisy Leakage Model to Probing Model Reductions

Work in [10] claims that statistical distance and Euclidean norm are average-case noise metrics, which do not provide a tight reduction probing model as if they were worst-case metrics. Therefore, it presents two new metrics, namely the relative error (RE) and the average relative error (ARE). They unify definitions of all four metrics in terms of point-wise

[1]This definition of privacy should not be confused with "user privacy". We refer to extraction of the secret from the probed wires in a circuit cf. [5].

mutual information of the same distribution. These metrics are not used to simulate the leakage, but to provide the number of probes needed to perform an attack, or conversely, to design a masking scheme that would be proveably secure in a corresponding attack model. Compared to other reductions, there is no loss in noise parameter δ, and security is intact. This provides a tighter reduction, which simulates exactly the same distributions despite different metrics, because distributions depend on intermediate values, as discussed in Section II-A. In addition, this work provides a security proof of its noisy leakage models with respect to concrete noisy leakage models that follow Gaussian distributions, and is based on Renyi divergence. However, their RE noisy leakage model suffers from the requirement of leak-free gates.

III. Gadgets

Gadget is the main building block of a masking scheme. The masking scheme considers each gate of the original circuit to be transformed into the cluster of gates while preserving the functionality. Linear gates, such as NOT, XOR and XNOR, have not been of the research interest because of the commutative and associative properties of XOR, similar to addition. On the other hand, non-linear AND gate has been extensively researched. The most important construction is from [5], with its so-called *ISW AND gadget*. ISW AND gadget has been proven secure in the threshold t model, and in various noisy leakage models, as shown in Section II. Inputs to AND gadget are the so-called *shared* values of the original input, and output is the *shared* version of the output. Original inputs a and b get shared (or split) into $2t+1$ secret shares to be protected against t probes in the threshold t-probing model, where $a = a_1 \oplus a_2 \oplus \cdots \oplus a_{2t+1}$, $b = b_1 \oplus b_2 \oplus \cdots \oplus b_{2t+1}$, and a shared value is independent of its shares. Shares are randomly drawn from a uniform distribution. In practice, it is done by using a random number generator (RNG), or the so-called *refresh* gadget. Refresh gadget is usually considered as a leak-free component, and therefore, recognized as a drawback in various attack models, see Section II. Computation is performed on shared input signals, which are masked by random numbers computed from refresh gadget. ISW AND gadget expands one AND gate into t^2 gates, while signals need to be split into $2t+1$ shares to be secured against t number of probes. The reason for $2t+1$ instead of $t+1$ shares in ISW AND gate is due to the computation sequence. Therefore, the order of handling intermediate signals plays important role in the definition of security for the specific gadget, on the gate level. ISW AND gadget with shared inputs a and b, and shared output c, is constructed in the following way:

1) Random $z_{i,j}$ values are drawn from refresh gate uniformly for $1 \leq i \leq j \leq 2t+1$.
2) Intermediate values $z_{j,i}$ are computed using $z_{j,i} = (z_{i,j} \oplus a_i b_j) \oplus a_j b_i$, where parentheses signify the order of computation.
3) Finally, shared output values are computed using $c_i = a_i b_i \oplus \bigoplus_{i \neq j} z_{i,j}$.

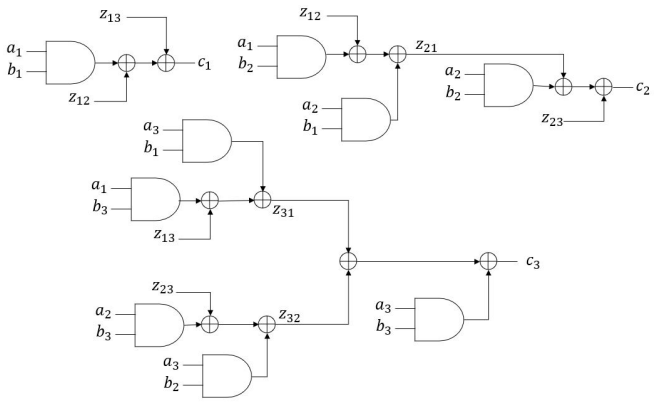

Fig. 2. ISW AND gadget secured against $t = 1$ probe.

An ISW AND gadget secured against 1 probe (i.e., $t = 1$), with three shares per input ($2t + 1 = 3$), three shares per output c and uniform and random masks z_{12}, z_{13}, z_{23} is shown in Figure 2.

IV. Discussion

Back-side probing is a serious, physical attack because of non-existing countermeasures, which would increase the complexity of the attack, or potentially stop the attack from happening. Existing countermeasures protect against front-side attacks, and in particular, side-channel analysis with masking schemes ensuring provable security. On the contrary, physical countermeasures against the back-side attacks, such as back-side metal shield, are ad-hoc, which would protect against the attack with certain adversary capabilities. While in theory this would hold, it halts failure analysis techniques, which are essential for the design and testing of the device.

Circuit masking, as an elegant, provable solution, could potentially give insight into how to formalize and deal with the problem of back-side probing. For this purpose, attack models developed for side-channel analysis offer potential since they consider the most powerful attacker, which can access any points within the circuit. As a back-side attack could be more powerful than front-side probing attacks, it can be thought that the attack models used for circuit masking countermeasure, can be extended to take back-side probing attacks into account. Nevertheless, there are challenges to face in this regard, e.g., efficient implementation of masked circuits, which would mimic the theory the closest.

For this, various gadgets have been proposed in various attack models, but ISW AND gadget from Figure 2, secured in threshold t-probing model, has always been the basic and main building block. One of the issues with this is the existence of physical glitches, which have been problematic to design engineers as well; hence, methods for minimizing the effect of glitches have been studied well. Physical glitches interrupt, destroy or limit the functionality of refresh gadgets that create random values used for generating the shares and masking. However, this issue was recognized early, so it has been

considered in implementations by developing variations of ISW AND gadget [5].

Other issues have been recognized once the circuit masking schemes were implemented. Implementations such as threshold implementation (TI), domain-oriented masking (DOM), consolidated masking scheme (CMS), Generic Low Latency Masking (GLM), and Unified Masking Approach (UMA) suffer from local flaws, as well as the issue of composability, as shown in [11]. The paper argues that those issues arise because of the trade-off between combinatorial circuits, sequential circuits, and refresh gadgets. Composability is the issue with the arrangement of the implemented gadgets that can result in a security challenge because certain gadget configurations leak more information than others. Work has been devoted in the development of different security notions that consider composability in the gadgets secured in probing models. Among them are t-non interference and t-strong non interference models developed in [12], and further analyzed and supplemented in, e.g., [13] and [14].

In line with this, bridging the gap between the theory and practice should be set as an ultimate goal. To this end, the following issues must be considered: (1) integrating the back-side attacks in probing models, (2) considering physical glitches and composability in that model, (3) making the obtained model realistic by including the noisy leakage models, and (4) employing security notions for higher-order attacks.

The main question that arises from recognizing the need for perfectly secure masking scheme is if the creation of this theoretically provable countermeasure, once it is implemented, would raise unknown implementation aspects that could make the countermeasure weak. The masking implementation which considers all known issues may still be vulnerable against side-channel attacks because of the aspects which are not considered yet and may see daylight once current issues are overcome, in the same way as certain physical countermeasure protect against one type of the probing or side-channel attack, but not the others.

If the chip is not completely accessible, and perfectly secure masking implementation is not achievable, the security of the circuit can be relaxed to the notion of being *good enough* against all current probing attacks, and those predicted in foreseeable future. For such relaxed privacy, it is not necessary to use the most powerful attack *contact-to-silicide*, but less devastating probing attack *contact-to-metal*. In such probing attack model, adversary would be limited to possession of certain type of probe, in addition to number of probes.

Finally, we believe that physical countermeasures, which protects against contact-to-metal back-side probing attack could be used to compensate for the lost security through the relaxation of the privacy in the probing attack. Our future study aims to design physical countermeasures that protect lowest metal layers of the circuit through the introduction of the inner active shield, which turns circuit off once the probing is detected. In this regard, we explore methods to decrease the area overhead. Our countermeasure can be used to protect the security-critical, specific nets, which leak the information in the corresponding probing attack model.

V. Conclusion

Masking has been the main side-channel analysis countermeasure. In this mature field, a probing attack is considered as the worst possible *side-channel attack*. Consequently, it was considered that if the circuit was secured against a probing attack, it must be secured against side-channel attacks. This has been augmented with more realistic representation considering the noise in an attack model. However, there have been various limitations and difficulties in implementing masking countermeasures and achieving the security theory promises. Many implementations have been proposed, but each suffers from specific weaknesses. There is a great need for the development of masking countermeasure and attack model, which would be universal and not susceptible to the *worst*-worst-case side-channel attack – back-side probing attack.

References

[1] S. Manich, M. S. Wamser, and G. Sigl, "Detection of probing attempts in secure ics," in *2012 IEEE International Symposium on Hardware-Oriented Security and Trust*. San Francisco, CA, USA: IEEE, 2012, pp. 134–139.

[2] E. Amini, A. Beyreuther, N. Herfurth, A. Steigert, B. Szyszka, and C. Boit, "Assessment of a chip backside protection," *Journal of Hardware and Systems Security*, vol. 2, no. 4, pp. 345–352, 2018.

[3] A. Covic, Q. Shi, H. Shen, and D. Forte, "Contact-to-silicide probing attacks on integrated circuits and countermeasures," in *2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*. Xi'an, P.R. China: IEEE, 2019, pp. 1–6.

[4] S. Nikova, V. Rijmen, and M. Schläffer, "Secure hardware implementation of nonlinear functions in the presence of glitches," *Journal of Cryptology*, vol. 24, no. 2, pp. 292–321, 2011.

[5] Y. Ishai, A. Sahai, and D. Wagner, "Private circuits: Securing hardware against probing attacks," in *Annual International Cryptology Conference*. Springer, 2003, pp. 463–481.

[6] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," in *Annual International Cryptology Conference*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 398–412.

[7] E. Prouff and M. Rivain, "Masking against side-channel attacks: A formal security proof," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2013, pp. 142–159.

[8] A. Duc, S. Dziembowski, and S. Faust, "Unifying leakage models: From probing attacks to noisy leakage." in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2014, pp. 423–440.

[9] S. Dziembowski, S. Faust, and M. Skorski, "Noisy leakage revisited," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2015, pp. 159–188.

[10] T. Prest, D. Goudarzi, A. Martinelli, and A. Passelègue, "Unifying leakage models on a rényi day," in *Annual International Cryptology Conference*. Springer, 2019, pp. 683–712.

[11] T. Moos, A. Moradi, T. Schneider, and F.-X. Standaert, "Glitch-resistant masking revisited," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 256–292, 2019.

[12] G. Barthe, S. Belaïd, F. Dupressoir, P.-A. Fouque, B. Grégoire, P.-Y. Strub, and R. Zucchini, "Strong non-interference and type-directed higher-order masking," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 116–129.

[13] G. Cassiers and F.-X. Standaert, "Trivially and efficiently composing masked gadgets with probe isolating non-interference," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2542–2555, 2020.

[14] S. Faust, V. Grosso, S. Pozo, C. Paglialonga, and F.-X. Standaert, "Composable masking schemes in the presence of physical defaults & the robust probing model," *IACR Cryptology ePrint Archive*, 2018.