

Postponing the Glitches is not Enough

A Critical Analysis of the DATE 2024 E-ISW Masking Scheme

Amir Moradi

Technische Universität Darmstadt, Darmstadt, Germany
amir.moradi@tu-darmstadt.de

Abstract—The Enhanced ISW (E-ISW) masking scheme, proposed at DATE 2024, aims to reduce glitch-induced leakage by enforcing input-complete gate evaluation with artificial delays. However, our theoretical analysis shows that E-ISW still exhibits first-order leakage under its intended conditions. These flaws arise from a lack of compositional reasoning about glitches and masking, rendering the scheme insecure.

Index Terms—Side Channel Analysis, Masking, ISW, Glitches

I. INTRODUCTION AND BACKGROUND

Side-Channel Analysis (SCA) attacks have been a significant threat to cryptographic implementations since their introduction [1], prompting the development of numerous countermeasures. While many of these techniques are heuristic in nature and aim to reduce exploitable leakage below the noise level [2], their security cannot be formally guaranteed. This limitation has led to a shift towards masking schemes, which offer a stronger mathematical foundation and provable SCA security [3]. One commonly used adversary model is the probing model, where an adversary can observe up to t internal signals [4]. This model simplifies the design of secure circuits, as resistance to t probes implies security against first-order attacks like DPA and CPA [1], [5]. However, this simplification does not account for hardware-specific challenges like micro-architectural effects, which can introduce unintended interactions and security vulnerabilities [6]. In hardware, efforts have focused on mitigating leakage caused by glitches, which can still occur even in masked circuits [7]. This led to the development of schemes like Threshold Implementation (TI) [8] and Domain-Oriented Masking (DOM) [9], which are designed to provide practical security in the presence of glitches. Formal models like the robust probing model [10] have since been introduced to account for glitch propagation. These models allow for systematic design of secure circuits, though they come with performance trade-offs. Recently, Enhanced ISW (E-ISW) was introduced at DATE 2024 [11] as a solution to control delays and avoid glitches in hardware. However, in this work, we demonstrate that E-ISW does not provide adequate security guarantees, highlighting the importance of formal proof-based validation over heuristic solutions. For the full version of the paper, see [12].

II. ISW, PROBLEM, AND THE DATE 2024 SOLUTION

Throughout this paper, single-bit random variables are denoted by lowercase letters (e.g., x), vectors by uppercase letters (e.g., X), and elements of a vector by subscripts (e.g., $X : \langle x_{n-1}, \dots, x_0 \rangle$). Shares in a masking are represented with superscripts (e.g., x^0 and X^1 for the first and second shares

of masked x and X , respectively). We begin by restating the ISW masking scheme, explaining its insecurity under the robust probing model, and discussing the E-ISW technique introduced to mitigate these issues. For simplicity, we focus on the 2-input AND operation, which is the core of the E-ISW solution.

ISW masking, like other masking schemes, splits each secret random variable into Boolean shares (x^0, \dots, x^d), where their XOR sum equals the original value $x = \bigoplus_{i=0}^d x^i$. For each cipher execution, primary inputs (e.g., plaintext, key) are turned into $d+1$ shares, with one share computed as $x^0 = x \oplus \bigoplus_{i>0} x^i$. The cryptographic function operates on these masked inputs and generates a masked output, which is then unmasked to obtain the result. Here, we focus on first-order masking ($d = 1$), which uses two shares per masked value.

Boolean masking simplifies XOR operations: for $z = x \oplus y$, we compute each share as $z^i = x^i \oplus y^i$. However, for the AND operation $w = x \cdot y$, the computation is more involved: $w = x^0y^0 \oplus x^0y^1 \oplus x^1y^0 \oplus x^1y^1$. This requires splitting these terms into two groups: $w^0 = x^0y^0 \oplus x^0y^1$ and $w^1 = x^1y^1 \oplus x^1y^0$. However, a probe placed on w^0 can leak information about y , necessitating the addition of random values, denoted as r chosen from a uniform distribution. The corrected formula becomes $w^0 = x^0y^0 \oplus (x^0y^1 \oplus r)$ and $w^1 = x^1y^1 \oplus (x^1y^0 \oplus r)$.

However, implementing this in hardware can lead to glitches due to timing issues between XOR and AND gates. To address this, DOM [9] introduces registers after the blinding operation to prevent leakage dependencies between terms like x^0y^0 and $(x^0y^1 \oplus r)$. This solution ensures that masked values are secure under glitch-extended robust probing models. However, it comes at the cost of additional latency in the hardware, as each operation must wait for the previous step to complete.

To avoid the latency introduced by DOM, the authors of E-ISW [11] proposed a solution where delay elements are added to ensure the proper order of operations (see Fig. 1). By delaying the second input of the final XOR operation, $x^0y^0 \oplus \text{delayed}(x^0y^1 \oplus r)$, they hoped to prevent harmful glitches from revealing information about y . While this approach aims to address the timing issues, we demonstrate that E-ISW still fails to guarantee sufficient security in practice

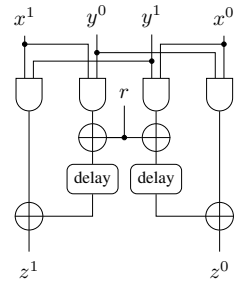


Fig. 1. E-ISW AND.

TABLE I
GLITCH PATTERNS OF ISW AND E-ISW AND GADGETS, ASSUMING r ARRIVES AFTER ALL OTHER PRIMARY INPUTS.

y	y^0	y^1	x^0	r	$x^0 y^0$	$x^0 y^1$	$x^0 y^1 \oplus r$	ISW z^0	delayed ($x^0 y^1 \oplus r$)	E-ISW z^0
0	0	0	0	0	—	—	—	—	—	—
			0	1	—	—	—	—	—	—
			1	0	—	—	—	—	—	—
	1	1	0	0	—	—	—	—	—	—
			0	1	—	—	—	—	—	—
			1	0	—	—	—	—	—	—
1	0	1	0	0	—	—	—	—	—	—
			0	1	—	—	—	—	—	—
			1	0	—	—	—	—	—	—
	1	0	0	0	—	—	—	—	—	—
			0	1	—	—	—	—	—	—
			1	0	—	—	—	—	—	—

III. ANALYSIS

Before analyzing E-ISW, we discuss the impact of glitches in SCA and their treatment in the robust probing model. Glitches arise from asynchronous input changes in a gate, propagating through the circuit and affecting power consumption, which is measured via a shunt resistor in the Vdd or GND path [2]. This causes variations in the power consumption curve, which is influenced by all input changes. The glitch extension of the robust probing model requires observing all inputs when probing an output. Though conservative, this approach is widely used in analyses due to its simplicity [13].

We now analyze ISW and E-ISW with respect to glitches to see if E-ISW prevents data-dependent transient behaviors compared to ISW and alternatives like DOM. Our analysis simplifies the model to expose weaknesses in the masking logic, isolating the effects of signal arrival times and glitch propagation.

We make the following assumptions: 1) Each gate has a unique, constant propagation delay. 2) All primary inputs are initialized to zero for clarity. 3) We trace input-to-output transitions and categorize glitch patterns.

We begin by revisiting the ISW gadget, assuming (as in the E-ISW paper) that the refresh input r arrives after the primary inputs x^0 , x^1 , y^0 , and y^1 . This causes the partial product terms $x^0 y^0$ and $x^0 y^1$ to be evaluated before r , delaying the blinding effect of r . As a result, a probe on the intermediate value $x^0 y^0 \oplus x^0 y^1$ may leak sensitive information before $x^0 y^1$ is blinded.

To examine this, we present Table I, which shows signal behavior for different input combinations. The upper half corresponds to $y = 0$, and the lower half to $y = 1$. For security, the signal patterns for $y = 0$ should match those for $y = 1$ (up to permutation). We highlight the behavior of $x^0 y^1$, where glitch patterns remain unchanged regardless of y . However, this does not hold for the output z^0 in the ISW design. The glitch patterns for $y = 0$ and $y = 1$ differ, revealing a leakage path. This confirms that ISW fails to maintain masking security in the presence of glitches, consistent with previous studies.

Next, we examine the E-ISW design under the same conditions. The second-to-last column of Table I shows the behavior of the delayed signal $x^0 y^1 \oplus r$. With sufficient delay, this signal exhibits consistent glitch patterns across both values of y , indicating effective masking. However, for the final output signal z^0 in E-ISW (rightmost column), the glitch patterns still depend on y , revealing a leak. Thus, E-ISW does not resolve the issue of data-dependent glitches, despite attempts to synchronize signal arrival.

In summary, our analysis identifies a fundamental flaw in E-ISW, showing that it cannot prevent data-dependent glitch propagation. These vulnerabilities are likely to be more pronounced in realistic or adversarial settings. Further analyses, including cases where r arrives earlier or a comparison with glitch-immune alternative DOM, are available in the full paper [12], along with FPGA-based experiments confirming our findings.

IV. CONCLUSIONS

The E-ISW scheme, proposed as a hardware enhancement to the ISW masking scheme, aims to reduce glitch-induced leakage by controlling signal arrival with artificial delays. However, our theoretical analysis reveals that E-ISW fails to eliminate data-dependent glitches in its output signals. Despite the added delays, the final output remains distinguishable based on unmasked inputs, violating the core requirement of indistinguishability in masked implementations. While the delay-based strategy of E-ISW seems intuitively sound, the leakage detection results in [11] may provide a false sense of security, as they do not account for complex real-world signal interactions.

This work emphasizes that heuristic solutions cannot replace formal security guarantees. For effective hardware countermeasures, masking schemes must be validated not just by leakage detection, but also through compositional, circuit-aware proofs.

ACKNOWLEDGMENTS

This work has been supported in part by the German Research Foundation (DFG) through the project 549340884 (MatSec).

REFERENCES

- [1] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *CRYPTO '99*, ser. Lecture Notes in Computer Science, vol. 1666. Springer, 1999, pp. 388–397.
- [2] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks - revealing the secrets of smart cards*. Springer, 2007.
- [3] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," in *CRYPTO '99*, ser. Lecture Notes in Computer Science, vol. 1666. Springer, 1999, pp. 398–412.
- [4] Y. Ishai, A. Sahai, and D. A. Wagner, "Private Circuits: Securing Hardware against Probing Attacks," in *CRYPTO 2003*, ser. Lecture Notes in Computer Science, vol. 2729. Springer, 2003, pp. 463–481.
- [5] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," in *CHES 2004*, ser. Lecture Notes in Computer Science, vol. 3156. Springer, 2004, pp. 16–29. [Online]. Available: https://doi.org/10.1007/978-3-540-28632-5_2
- [6] A. Beckers, L. Wouters, B. Gierlichs, B. Preneel, and I. Verbauwhede, "Provable Secure Software Masking in the Real-World," in *COSADE 2022*, ser. Lecture Notes in Computer Science, vol. 13211. Springer, 2022, pp. 215–235. [Online]. Available: https://doi.org/10.1007/978-3-030-99766-3_10
- [7] S. Mangard, N. Pramstaller, and E. Oswald, "Successfully Attacking Masked AES Hardware Implementations," in *CHES 2005*, ser. Lecture Notes in Computer Science, vol. 3659. Springer, 2005, pp. 157–171.
- [8] S. Nikova, V. Rijmen, and M. Schl affer, "Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches," *J. Cryptol.*, vol. 24, no. 2, pp. 292–321, 2011.
- [9] H. Gro , S. Mangard, and T. Korak, "Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order," in *TIS@CCS 2016*. ACM, 2016, p. 3.
- [10] S. Faust, V. Grosso, S. M. D. Pozo, C. Paglialonga, and F. Standaert, "Composable Masking Schemes in the Presence of Physical Defaults & the Robust Probing Model," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2018, no. 3, pp. 89–120, 2018. [Online]. Available: <https://doi.org/10.13154/tches.v2018.i3.89-120>
- [11] S. Takarabt, J. Bahrani, M. Ebrahimabadi, S. Guilley, and N. Karimi, "Securing ISW Masking Scheme Against Glitches," in *DATE 2024*. IEEE, 2024, pp. 1–2. [Online]. Available: <https://doi.org/10.23919/DATE58400.2024.10546525>
- [12] A. Moradi, "Postponing the Glitches is Not Enough - A Critical Analysis of the DATE 2024 E-ISW Masking Scheme," Cryptology ePrint Archive, Paper 2025/2084, 2025. [Online]. Available: <https://eprint.iacr.org/2025/2084>
- [13] N. M uller and A. Moradi, "Robust but Relaxed Probing Model," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2024, no. 4, pp. 451–482, 2024. [Online]. Available: <https://doi.org/10.46586/tches.v2024.i4.451-482>