A Note on Transitional Leakage When Masking AES with Only Two Bits of Randomness

Felix Wegener and Amir Moradi

Ruhr University Bochum, Horst Görtz Institute for IT Security, Germany
{firstname.lastname}@rub.de

Abstract. Recently, Gross *et al.* demonstrated a first-order probing-secure implementation of AES using only two bits of randomness for both the initial sharing and the entire computation of AES. In this note, we recall that first-order probing security may not be sufficient for practical first-order security when randomness is re-cycled. We demonstrate that without taking the transitional leakage into account, the expected security level in a serialized design based on their concept might not be achieved in practice.

1 Masking AES with only two bits of randomness

Recently, Gross *et al.* [6] introduced a concept to mask the entire AES cipher with only two bits of randomness including the initial sharing of the plaintext. They introduce a fully-unrolled version of AES and verify the first-order probing security of individual components of their designs using the tool maskverif [2]. They further suggest to implement round-serialized and S-box-serialized versions to achieve a smaller area footprint.
In the following, we show that a serialized version of their concept does not achieve practical first-order security if not enough attention is payed with respect to transitional leakage. Indeed, we argue that a mere variation of masks in their design can never achieve first-order security in the setting of a transitional leakage model. As a take-home message, we stress that reset cycles should be considered in the design to mitigate the transitional leakage. We in fact practically demonstrate its effectiveness using side-channel measurements.

2 Problem Description

In [6] the entire state of AES is masked with only two bits of randomness. Gross *et al.* suggest to mask each of the sixteen plaintext bytes identically with mask

$$m_B := \{m_1, m_0 \oplus m_1, m_0 \oplus m_1, m_0, m_0, m_1, m_0, m_1\}$$

and maintain this mask in each round at the input of the SubBytes Layer.

Gate-Level Leakage. To realize a first-order secure AES S-box, Gross *et al.* [6] utilize the circuit introduced by Boyar and Peralta [3] and describe a first-order probing secure realization of an AND-gate in four cycles without fresh-randomness.

$$q_0 = \Big[\Big[\underbrace{[a_0 \wedge b_0]}_{t_1} \oplus [a_0 \wedge b_1 \oplus b_1]\Big]\Big] \oplus \Big[\Big[[a_1 \wedge b_0] \oplus [a_1 \wedge b_1 \oplus b_1]\Big] \oplus a_1\Big]$$

$$q_1 = \Big[\Big[[a_1]\Big]\Big]$$

We used square brackets to indicate the placement of registers.

Consider the subsequent evaluation of the AND-gate on (a^1, b^1) and (a^2, b^2)[1]: As only three masks $\{m_0, m_1, m_0 \oplus m_1\}$ are available in total, two of the four inputs necessarily share a mask. This introduces transitional leakage in the Hamming distance model, e.g., in intermediate value t_1. More precisely, the value of $t_1^1 \oplus t_1^2$ leaks information about (a^1, b^1, a^2, b^2).
Using exhaustive computation, we determined that the Hamming distance in t_1 is input-dependent for all 36 choices of masks[2]. The secret dependency is illustrated for one specific choice of masks in Table 1.

Table 1: Dependence of Hamming distance of intermediate value t_1 on secret values for mask choices $(b_1^2, a_1^2, b_1^1, a_1^1) = (m_0 \oplus m_1, m_1, m_1, m_0)$

b^2	a^2	b^1	a^1	$\#\ t_1^1 \oplus t_1^2 = x$	
				$x = 0$	$x = 1$
0	0	0	0	2	2
0	0	0	1	4	0
0	0	1	0	2	2
0	0	1	1	2	2
0	1	0	0	2	2
0	1	0	1	2	2
0	1	1	0	4	0
0	1	1	1	2	2
1	0	0	0	4	0
1	0	0	1	2	2
1	0	1	0	2	2
1	0	1	1	2	2
1	1	0	0	2	2
1	1	0	1	2	2
1	1	1	0	2	2
1	1	1	1	4	0

[1] We use superscript to distinguish between inputs to the same gate in different clock cycles

[2] The total amount of 81 masks is reduced by the 1-probing requirement that masks in one cycle are unequal.

Mitigation. Security in the presence of transitional (e.g., Hamming distance) leakage can be achieved by interleaving the computation with reset cycles [7] in which $(0, 0)$ is fed as an input to the AND-gate, thereby reducing the effective throughput by up to 50%.

3 Practical Demonstration

We implemented the secure AND-gate in hardware with a four stage pipe-line according to the specification in [6] to perform a practical side-channel evaluation. To enhance the signal-to-noise ratio of our evaluation target, we implemented 31 parallel instances of the secure AND gate, each receiving identical inputs. Our measurement setup consists of a SAKURA-G side-channel evaluation board [1] running at 6 MHz and a Picoscope 6000 series digital oscilloscope with a sampling rate of 625 MS/s. Additionally, we utilized the ZFL-1000LN+ amplifier from Mini-Circuits.
We performed a "fixed-vs-random" t-test evaluation [5, 8] over 4 input bits (a^1, b^1, a^2, b^2) which are masked with two bits of entropy with the following masks $(m_0, m_1, m_1, m_0 \oplus m_1)$.

Insecure Evaluation. If (a^1, b^1) and (a^2, b^2) are fed into the pipeline of the secure AND-gate in subsequent cycles, then transitional leakage is clearly observable (cf. Figure 1).

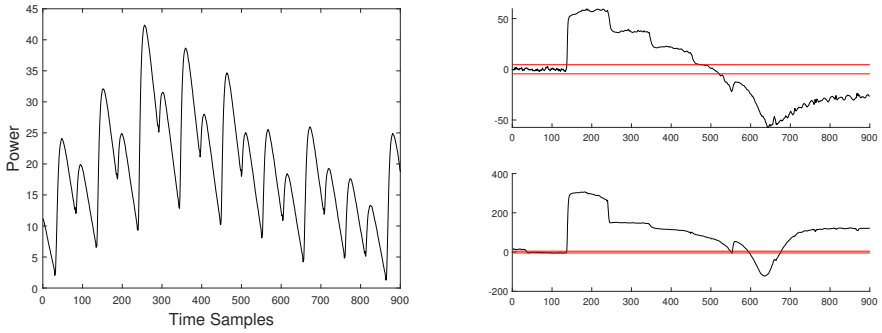
Secure Evaluation. If the evaluation of (a^1, b^1) and (a^2, b^2) is interleaved with the input $(0, 0)$ (to which we refer as a reset cycle), no first-order leakage is observable (cf. Figure 2).
As expected in a two-share design, both evaluations show severe second-order leakage.

4 Discussion

In this note, we demonstrated how a naive evaluation of the 1-probing model may lead to leakage in practice. Commonly, if a design is masked with a high entropy, transitional leakage is not present in serialized designs, because subsequent inputs to components of the circuit have mutual information zero (e.g. in an S-box serialization design if all state bytes are masked independently). Hence, most of the time high entropy masking only necessitates to check a given circuit for security in the 1-probing model, while transitional security is obtained "for free" through independent masks. However, if entropy is shared between the serialized units of a circuit, a formal verification of $(1, 0, 0)$-robust 1-probing security[3] is insufficient for practical side-channel security. Hence, a formal verification of $(1, 1, 0)$-robust 1-probing security is necessary in serialized designs with shared masks.

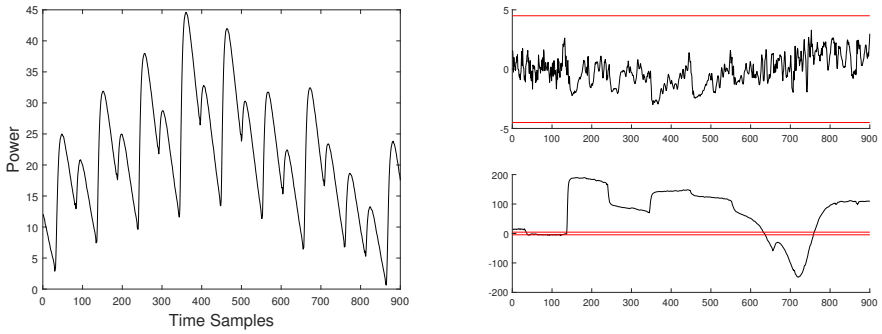
[3] using the notation from [4]

We would like to highlight the necessity of adopting the verification tools to cover such transitional leakages. As we showed here, a design whose security is verified by means of such a tool may fail in practice when facing transitional leakages.



(a) Average trace over 100 measurements **(b)** First and second order t-test evaluation

Figure 1: Insecure: Evaluation of secure AND-gate, masked with two bits of entropy, without reset cycle, 500 000 traces.



(a) Average trace over 100 measurements **(b)** First and second order t-test evaluation

Figure 2: Secure: Evaluation of secure AND-gate, masked with two bits of entropy, interleaved with reset cycle, 500 000 traces.

References

1. Side-channel AttacK User Reference Architecture. http://satoh.cs.uec.ac.jp/SAKURA/index.html.
2. Gilles Barthe, Sonia Belaïd, Pierre-Alain Fouque, and Benjamin Grégoire. maskverif: a formal tool for analyzing software and hardware masked implementations. *IACR Cryptology ePrint Archive*, 2018:562, 2018.
3. Joan Boyar and René Peralta. A small depth-16 circuit for the AES s-box. In Dimitris Gritzalis, Steven Furnell, and Marianthi Theoharidou, editors, *Information Security and Privacy Research - 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012. Proceedings*, volume 376 of *IFIP Advances in Information and Communication Technology*, pages 287–298. Springer, 2012.
4. Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, and François-Xavier Standaert. Composable masking schemes in the presence of physical defaults & the robust probing model. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(3):89–120, 2018.
5. Gilbert Goodwill, Benjamin Jun, Josh Jaffe, and Pankaj Rohatgi. A testing methodology for Side channel resistance validation. In *NIST Non-invasive Attack Testing Workshop*, 2011.
6. Hannes Gross, Lauren De Meyer, Martin Krenn, and Stefan Mangard. Masking the aes with only two random bits. Cryptology ePrint Archive, Report 2018/1007, 2018. https://eprint.iacr.org/2018/1007.
7. Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power analysis attacks - revealing the secrets of smart cards*. Springer, 2007.
8. Tobias Schneider and Amir Moradi. Leakage assessment methodology - A clear roadmap for side-channel evaluations. In Tim Güneysu and Helena Handschuh, editors, *Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings*, volume 9293 of *Lecture Notes in Computer Science*, pages 495–513. Springer, 2015.