mgr Karol Żebrowski

Analysis of the Simple Refreshing in the Noisy Leakage Model

Summary of PhD Dissertation

June 2024

1 Introduction

The dissertation is based on the paper *Simple Refreshing in the Noisy Leakage Model* by Stefan Dziembowski, Sebastian Faust, and Karol Żebrowski [6].

Masking schemes are a prominent countermeasure against power analysis [3]. The idea behind masking schemes is to introduce a randomness into the computation by secret sharing the sensitive values. Classically, the additive n out of n scheme is used, so each sensitive value is encoded as a sum of n values, where n is the security parameter. Then, assuming the circuit computation model, to perform arbitrary computation securely, including operations of addition and multiplication, often so-called *gadgets* – subcircuits performing respective operations on encodings – are used.

A key building block to securely compose multiple masked operations is the *refreshing scheme*. It takes as input some encoding and outputs a fresh encoding of the same sensitive value. By doing so, it introduces fresh randomness into the computation and prevents accumulation of the leakage from the encondings.

Various refreshing schemes were proposed by researchers, starting with Ishai, Sahai and Wagner in [8] where it was done via "artificially" multiplicating by 1 in $O(n^2)$ complexity. Another observation that allows to construct a refreshing schemes is that it is enough to generate a uniformly random encoding of 0 and add it, wire-wise, to the encoding being refreshed. One of such schemes, which we call a *simple refreshing* was proposed by Rivain and Prouff [11]. The simple refreshing scheme is optimal in terms of complexity and randomness used, as it uses only $< 2n$ operations and $n - 1$ random gates, where n is the security parameter. Unfortunately, this scheme was shown to be insecure, when composed with some arithmetic operations,

in the classical t-threshold probing leakage model [4]. In this model, the adversary is allowed to learn the values of t chosen wires of the circuit.

2 Summary of Results

A natural question arises: "Is the simple refreshing secure in some *weaker* leakage model?" The dissertation investigates the security of a simple refreshing scheme in the *noisy* leakage model of Rivain and Prouff [10] and answers this question affirmatively. The noisy leakage model assumes that the adversary learns only a "noisy distribution" of the values carried by the wires of the circuit, and is believed to model real-world physical leakage accurately. Later this model was refined and reduced to the *p-random probing* model by Duc et al. [5], in which each wire in the circuit leaks its value independently with probability p. Hence, the analysis presented in the dissertation focuses on the random probing model.

We start our analysis by presenting the security proof informally in a simplified case of a multi-round refreshing circuit, where the encoding of a secret is just refreshed a number of times, and no actual computation on it is performed. To analyze the security of the refreshing scheme we ask a natural question: "Can we characterize the leakages which allow the adversary to compute the secret?" It turns out that there is a fairly simple distinction between the configurations of the leaking wires that compromise the secret and the ones that do not. It is made possible thanks to the introduced notion of a *leakage diagram* – a special graph representing the set of leaking wires. The distinction between compromising and non-compromising leakage is achieved by simply looking at the leakage diagram and checking if its subgraphs, namely what we call "leftmost side" and "rightmost side", are connected or not. The remaining part of the security analysis is a probability-theoretic exercise of upper-bounding the probability of the sides in the leakage diagram being connected.

The rest of the dissertation is devoted to generalizing the ideas presented in the informal part to perform masked computation when the circuit uses the simple refreshing scheme. We propose a private circuit construction composed of gadgets with simple refreshing that performs arbitrary computation. The analysis of the construction requires the following:

1. Proposing a general definition of a gadget, which can be used in our construction. The properties captured by the definition, together with the

properties of the simple refreshing, makes the gadgets composable with the refreshing scheme. The definition is similar in spirit to the existing definitions for the t-probing model, but it also takes into account *the order of the input and ouput wires* of the gadget. In the dissertation, we present also a proof that the classic ISW multiplication gadget satisfies our definition.

2. Generalizing the notion of a leakage diagram to represent leakage in a construction composed of gadgets. Our definition of a gadget allows to "project" the leaking wires in each of the gadgets onto a respective path in the leakage diagram, and thus represent the leakage in the whole private circuit.

3. Proving a theorem on the privacy of our construction in a general case. The dissertation presents all the necessary technical concepts and proofs, which were not included in the original paper. The security proof for our construction is based on, widely used in cryptography, hybrid argument. We define a series of hybrid experiments, during which an adversarial view is created. Then we argue that each two consecutive experiments produce essentially the same view, what implies that the first and the last views are the same. In consequence, we show that the adversarial view can be simulated *without knowing the secret*, which guarantees the privacy of our construction.

Our construction achieves concrete results even for small security parameters n, unlike more theoretical constructions of Ajtai [1] and Andrychowicz et al. [2]. The construction is modular and works for different implementations of the addition and multiplication gadget, as long as the gadgets satisfy our definition. In our construction, we *do not* make any strong assumptions, e.g. about leak-free components used in some other constructions [7, 9].

References

[1] Miklós Ajtai. Secure computation with information leaking to an adversary. In Lance Fortnow and Salil P. Vadhan, editors, *43rd Annual ACM Symposium on Theory of Computing*, pages 715–724. ACM Press, June 2011.

[2] Marcin Andrychowicz, Stefan Dziembowski, and Sebastian Faust. Circuit compilers with $O(1/\log(n))$ leakage rate. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 586–615. Springer, Heidelberg, May 2016.

[3] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards sound approaches to counteract power-analysis attacks. In Michael J. Wiener, editor, *Advances in Cryptology – CRYPTO'99*, volume 1666 of *Lecture Notes in Computer Science*, pages 398–412. Springer, Heidelberg, August 1999.

[4] Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain, and Thomas Roche. Higher-order side channel security and mask refreshing. In Shiho Moriai, editor, *Fast Software Encryption – FSE 2013*, volume 8424 of *Lecture Notes in Computer Science*, pages 410–424. Springer, Heidelberg, March 2014.

[5] Alexandre Duc, Stefan Dziembowski, and Sebastian Faust. Unifying leakage models: From probing attacks to noisy leakage. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 423–440. Springer, Heidelberg, May 2014.

[6] Stefan Dziembowski, Sebastian Faust, and Karol Zebrowski. Simple refreshing in the noisy leakage model. Lecture Notes in Computer Science, pages 315–344. Springer, Heidelberg, December 2019.

[7] Sebastian Faust, Tal Rabin, Leonid Reyzin, Eran Tromer, and Vinod Vaikuntanathan. Protecting circuits from leakage: the computationally-bounded and noisy cases. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 135–156. Springer, Heidelberg, May / June 2010.

[8] Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481. Springer, Heidelberg, August 2003.

[9] Eric Miles. Iterated group products and leakage resilience against NC1. In Moni Naor, editor, *ITCS 2014: 5th Conference on Innovations in Theoretical Computer Science*, pages 261–268. Association for Computing Machinery, January 2014.

[10] Emmanuel Prouff and Matthieu Rivain. Masking against side-channel attacks: A formal security proof. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 142–159. Springer, Heidelberg, May 2013.

[11] Matthieu Rivain and Emmanuel Prouff. Provably secure higher-order masking of AES. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems – CHES 2010*, volume 6225 of *Lecture Notes in Computer Science*, pages 413–427. Springer, Heidelberg, August 2010.