POLITECNICO
MILANO 1863

SCUOLA DI INGEGNERIA INDUSTRIALE
E DELL'INFORMAZIONE

Executive Summary of the Thesis

An Analysis of Random Probing Security Properties in Masked Cryptographic Circuits

Laurea Magistrale in Computer Science and Engineering - Ingegneria Informatica

Author: Giuseppe Manzoni

Advisor: Prof. Vittorio Zaccaria

Academic year: 2021-2022

1. Introduction

This thesis explores the security of a circuit implementation of a cryptographic system, in particular how it holds up to an adversary able to see the value of each wire with a given probability. Among the possible properties, we focus on the Random Probing Security (RPS) of a circuit and the Random Probing Composability (RPC) of a gadget.

For the Random Probing Security (RPS), we rewrite two definitions and an approximation present in the literature using the correlation matrix, and we use it to compare their accuracy and structure. Of particular relevance is that [2] introduced their definition without comparing it to [1]'s definition, and so we compare the two and prove that the former can be seen as an approximation of the latter. We also provide other four approximations at different levels of the accuracy and execution time trade-off, compare their accuracy and structure, as explained in Section 2.

For RPC, we note that its definition in [1] is more specific than it's required to prove the relevant theorems, and so we propose a class of RPC-like definitions, all with the three necessary properties to ensure they're equivalent to the existing definition of RPC. This class will allow to search for tighter properties. To this end we provide two new definitions and three approximations, and write them using the correlation matrix to compare them in accuracy and structure, as explained in Section 3.

Lastly, we have written a software tool that implements those functions using the correlation matrix, and provide the graphs of the comparison among a few of the functions described. We also report an example that indicates how the IronMask tool of [2] doesn't provide correct results, and we compare our tool with the only other tool (VRAPS of [1]) that provides numerical results as explained in Section 4.

Both from the results of the tool and from the theoretical analysis of the accuracy and asymptotic execution time, we highlighted the presence of a trade-off between those two characteristics, both for RPS and for RPC-like properties. We have also shown how the correlation matrix is a useful tool to compare those definitions and approximations, even when they were originally created using a different abstraction, like probabilistic experiments.

2. Remodelling RPS

As done in [3] and [1], given a circuit it's possible to create a masked version by substituting (or

encoding) each wire with d wires called shares so that the sum of the shares has the same value as the original wire. Each gate is substituted with a sub-circuit or gadget and both the inputs and the outputs are encoded too. This transformation is used to create a circuit that computes the same function, but that respects the security properties of a given model.
In this thesis, we initially provide a definition of RPS that is equivalent to the RPS of [1]: given a masked circuit with I underlying inputs, W internal wires and with a probabilistic function g that from the masked inputs returns the value of the internal wires, given p that is the probability that a single wire leaks, given $\varepsilon \in [0, 1]$ that is the probability that the secret leaks, given enc the probabilistic function that encodes the underlying input and using $|w|$ as the number of 1s in w, we say that the circuit is (p,ε)-RPS (Random Probing Secure) if there exists a probabilistic simulator Sim such that $\forall x \in \mathbb{F}_2^I$, ε is greater or equal than:

$$\sum_{w \in \mathbb{F}_2^W} p^{|w|}(1-p)^{W-|w|}\mathrm{SD}\left[Sim(w); g(enc(x)) \cap w\right]$$

We then analyze which components of the correlation matrix of g are used by this definition and provide an upper bound of

$$1 - 2^{-I} \tag{1}$$

on the SD (statistical distance) of the definition that can be obtained by choosing the Sim carefully.
The six approximations we analyze can be seen in Figure 1 ordered by accuracy. Of those, four originate from our thesis (those colored in green in Figure 1), while for the other two we provide a new, and equivalent, definition in terms of the correlation matrix.
Regarding the existing ones, RPS_VRAPS is equivalent to the approximation [1] gives immediately after the definition of RPS. Similarly, RPS_IRONMASK is equivalent to [2]'s definition of RPS. As [2] doesn't compare its definition with [1]'s, we do it in our thesis, and we report that RPS_IRONMASK implies RPS_VRAPS but not vice versa, which makes the former less tight and a valid approximation of the latter. This can also be seen in the components of the correlation matrix used by RPS_IRONMASK: that expression depends upon additional components that we have shown to be ignored by [1]'s definition.
Yet while RPS_VRAPS is tighter than RPS_IRONMASK, there is no indication about its own tightness. This happens because [1] introduces it immediately after the definition of RPS, and then proceeds to always use the approximation. To partially correct this, we provide RPS_COR1, which is more accurate than RPS_VRAPS. This new approximation is equivalent to the definition of RPS when we use the same simulator of Expression (1). Due to RPS_COR1's elevated asymptotic execution time, we provide further approximations called RPS_COR2 and RPS_COR3, which are progressively less accurate and faster.
This last approximation (RPS_COR3) happens to be RPS_VRAPS multiplied by Expression (1). This means that with negligible additional execution time, it's possible to halve the leakage of the secret (the ε) in all copy gadgets, while the 2-inputs gadgets receive a 25% reduction.

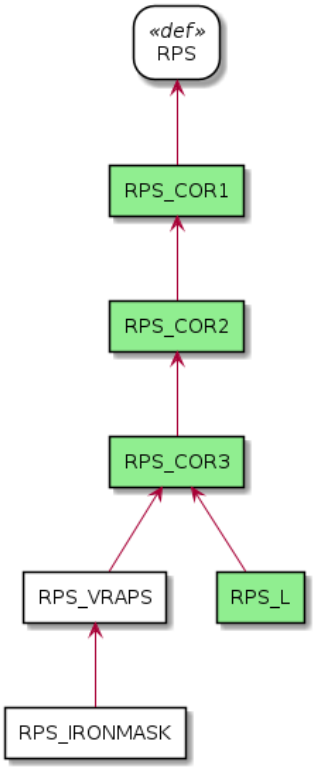

Figure 1: Accuracy, arrows toward the higher accuracy. Light green for the newly introduced approximations.

Lastly, from RPS_COR3 we provide an

even faster (and less accurate) approximation RPS_L. This one is the only one not directly expressed in terms of the correlation matrix, but instead it uses a matrix derived from it, and this allows RPS_L to have a significantly lower the asymptotic execution time in case one calculates all the coefficients of the expression.
Overall, this highlights the presence of a trade-off between accuracy and execution time, with the accuracy shown in Figure 1. All the relationships presented there have been proven during our research. Formally, we say that an approximation A is more accurate than an approximation B if both that in all gadgets

$$\forall p \in [0,1], \varepsilon_A(p) \leq \varepsilon_B(p)$$

and if there is a gadget for which:

$$\forall p \in (0,1), \varepsilon_A(p) < \varepsilon_B(p)$$

3. Remodelling RPC

As per the RPC, we report how an RPC-like definition K such that a gadget can be said to be (p, ε, S)-K need only to satisfy the following properties:

- for any gadget (p, ε, S)-K implies (p, ε)-RPS
- given two gadgets respectively (p, ε_1, S)-K and (p, ε_2, S)-K, their parallel is (p, $\varepsilon_1 + \varepsilon_2$, S)-K
- given two gadgets respectively (p, ε_1, S)-K and (p, ε_2, S)-K, their series (when meaningful) is (p, $\varepsilon_1 + \varepsilon_2$, S)-K

From those properties it's easy to see how any RPC-like definition guarantees that the composition of arbitrary gadgets is RPS with that p the sums of the ε. We can then define the accuracy of an RPC-like definition by the accuracy of the implied RPS, and we can see the comparison of the RPC-like properties in Figure 2.

We report three definitions. The first uses simulations with failure and is the original one of [1] which we call RPC_VRAPS from the name of their tool. Yet those simulations with failure are akin to those of RPS_VRAPS, and so we introduce a definition called RPC_SD that uses the Statistical Distance like the RPS definition, with the aim to improve the accuracy. Lastly, we go in the opposite direction and improve the asymptotic execution speed. As the tool is based on the correlation matrix, we provide a definition RPC_C defined directly in terms of the correlation matrix. This definition also happens to be hard to translate in terms of probability distributions and simulations, which reveals that there are many more avenues of research than those usually considered in the literature.
In addition to those definitions, we provide three approximations, which all have a corresponding approximation in the RPS. The first is RPC_C_L, which is an approximation of RPC_C using the same matrix as RPS_L, and it has the same asymptotic execution time. The other two are both approximations of RPC_SD using the real circuit as simulator and randoms for the missing input bits. This leads us to RPC_SD_COR1 which is similar to RPS_COR1, and to RPC_SD_COR2 which mimics RPS_COR3. Similar to what happens in the RPS, RPC_SD_COR2 is the same as RPC_VRAPS multiplied by a constant, which is the upper bound on RPC_SD.

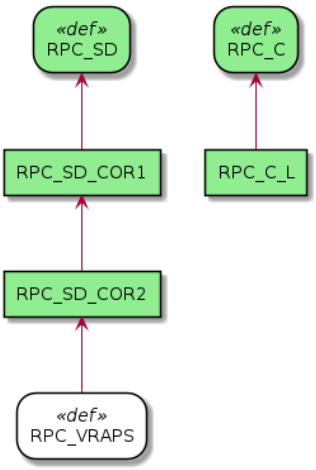

Figure 2: Accuracy, arrows toward the higher accuracy. Light green for the newly introduced definitions/approximations.

In Figure 2 we can see the accuracy relationships between those definitions and approximations as proven in our research.

4. Tool and Graphs

After describing the tools we found in the literature (VRAPS, STRAPS and IronMask) that calculate the RPS and RPC we explain why we only used VRAPS: STRAPS tool only outputs graphs, making it impossible to use it to com-

pare the accuracy without altering it.
As per IronMask, we then report a simple example of a wider phenomenon we found while using it: it regularly returns coefficients that are lower to what our tool calculates as minimum, and we couldn't find any error in the tool or in the proof of the expression used by our tool. To search for a solution to this contradiction, we calculated the RPC_VRAPS of a few simple gadgets compared it with the result of IronMask, and we saw a discrepancy. For example, the wires $W_1 = I_1 + R, W_2 = I_2 + R$ can be simulated perfectly without any input if taken by themselves (due to the random), but if taken together the input is needed, as xoring the two wires gives $W_1 + W_2 = I_1 + I_2$ which depends on both. In the example we report, IronMask ignores 9 combinations with this kind of dependency, which unduly lowers the f it calculates.
For the RPS we report in Figure 3 a limited example of the results for the ISW multiplication introduced in [3]. It's an accuracy and execution time graph with two logarithmic scales, and it contains the results of VRAPS with our tool's RPS_COR1, RPS_COR2 and RPS_COR3. The accuracy is measured as the maximum p for which the gadget provides a leakage of the secret that is lower than that of the wires.

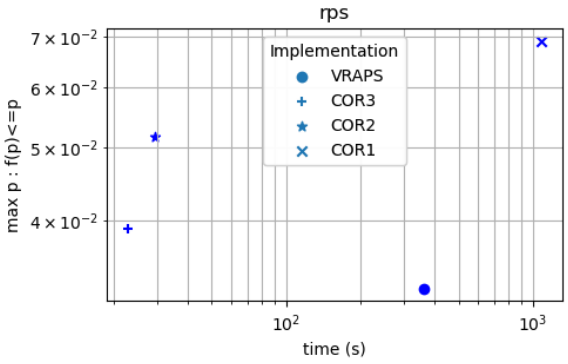

Figure 3: Plot of the RPS in logarithmic scales of execution time and accuracy of [3]'s multiplication with 3 shares and coefficients up to c_8.

For RPC we instead show Figure 4, with a similar graph (always for the ISW multiplication) that covers the result of VRAPS, RPC_SD_COR1 and RPC_SD_COR2.

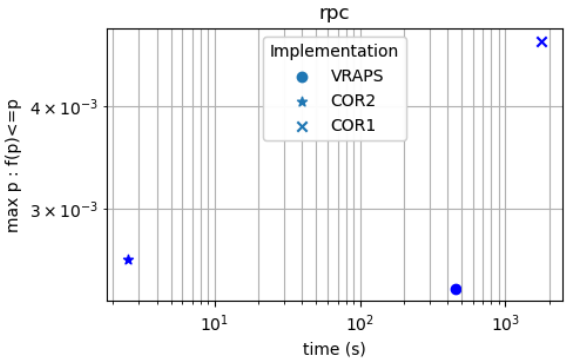

Figure 4: Plot of the RPC in logarithmic scales of execution time and accuracy of [3]'s multiplication with 3 shares and coefficients up to c_5.

5. Conclusions

This thesis shows how RPC is not a settled concept as various alternative definitions are indeed possible, many with execution time or accuracy advantages, and some even defined in ways that aren't easily re-written with the usual tools of simulatabilty, standard deviation and random experiment, opening the field to many more possibilities.
Both in RPS and RPC, the best of the explored alternatives seem to create an accuracy and execution time trade-off, and the exponential nature of the problem means that this trade-off can span entire order of magnitudes. At the same time, a slower execution that rises the accuracy could also be rewarding, as a lower accuracy may cause an increased production cost due to the need to artificially increase the noise in the microchip to at least reach the required $\max_p : f(p) \leq p$, or the gadget will only make the secret leak faster.
This thesis has also shown that the correlation matrix is effective at expressing in compact ways a multitude of definitions and approximations. This effectiveness is present both in how our tool compares to the existing tools, and in how each part of the expression refers to a specific characteristic of the definition/approximation, with similar parts appearing even across RPS and RPC. It's also effective in showing what kind of information is used by a given approximation, for example the effects of going from an SD-based definition to an all-or-nothing simulation with failure.

6. Acknowledgements

References

[1] Sonia Belaïd, Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain, and Abdul Rahman Taleb. Random probing security: Verification, composition, expansion and new constructions. Cryptology ePrint Archive, Paper 2020/786, 2020. https://eprint.iacr.org/2020/786.

[2] Sonia Belaïd, Darius Mercadier, Matthieu Rivain, and Abdul Rahman Taleb. Ironmask: Versatile verification of masking security. Cryptology ePrint Archive, Paper 2021/1671, 2021. https://eprint.iacr.org/2021/1671.

[3] Yuval Ishai, Amit Sahai, and David A. Wagner. Private circuits: Securing hardware against probing attacks. In *CRYPTO*, 2003.