A Simulator for Evaluating the Leakage in Arithmetic Circuits.

Audrey LUCAS
CNRS, IRISA UMR 6074, INRIA - Univ Rennes

Side channel attacks (SCA) [1] (or observation attacks) are considered as important threats for embedded crypto-processors. They use external measurements of the circuit execution to guess secrets (*e.g.* timings, power consumption, electromagnetic radiation). Some of them, like differential power analysis (DPA), employ statistical tools. More particularly, observation attacks, with power consumption, are feasible since external measurements depend on the data manipulated in the circuit. Indeed, for one bit, the power behavior is different depending on the type of transition (0->1 or 1->0).

Scalar multiplication (SM) is the main operation on *elliptic curve cryptography* (ECC). It consist in performing $k \times P$ where k is a scalar (the secret key in some primitives) and P a public curve point. In order to perform SM, *point addition* and *point doubling* operations are used. If these operations have different cost or behavior and if a weak algorithm is employed for SM, then SCA is achievable [2].

In order to protect against SCAs, the dependencies between secret values and observable variations of the physical parameter(s) must be avoided. Uniformization and randomization are two ways to achieve this purpose. The SM can be uniformized with regular algorithms, uniform formulas or dummy operations. Thus, the operation sequences are indistinguishable whatever the actual secret bits manipulated in the circuit. The randomization consists in generating a random activity in order to scramble the measurements. Thus, this random activity is considered as data by statistical tools. The random activity can be created by different methods as random masks or addition of dummy operations.

In this work, we focus on the uniformization case. More particularly, we study the impact of different inputs of operators (*e.g.* adder and multiplier) during SM over 32-bit architecture. In other words, for a same operator (*e.g.* adder), we study if some inputs (*e.g.* x and x or x and $2x$) have a distinguished behavior. For this purpose, a theoretical arithmetic simulator of 32-bit architecture material is developed. During SM execution, the hamming weight (HW) variations of field elements are measured in the simulator.

It enables to verify that some inputs induce a measurable HW variation at one moment of SM.

Calculated HW variation is a theoretical model of dynamic consumption of the circuit during execution. In the real circuit, in addition to arithmetic units, the control of circuit has a part on real consumption trace. As we only consider operators, arithmetic traces are obtained without control of circuit consumption. Thus, potential arithmetic leaks could be easily identified. Once leaks are detected, SCA (*e.g* template attack) could be simplified since the attacker knows where to research in real traces.

Another simulator usage can be SCA prevention. More precisely, in order to protect simultaneously SM against SCA and fault attack (FA), the simulator can be useful for testing countermeasures. Indeed, if arithmetical leaks are detected in algorithm or FA countermeasure then, the initial code can be corrected.

Our simulator is developed in Python and Sage mathematical software and could allow to identify physical leaks more easily than with VHDL simulator. Indeed, arithmetic tools are not implemented in VDHL. Moreover, in ECC, numbers manipulated have size larger than 100-bit, so VHDL simulator is very slow.

Finally, with our simulator, on the one hand, SCA could be facilitated since leaks are spotted. On the other hand, if leaks are detected, the protection could be also facilitated.

.

Acknowledgments

This work is partly funded by DGA-PEC.

References

[1] S. Mangard, E. Oswald, and T. Popp. *Power analysis attacks - revealing the secrets of smart cards.* Springer, 2007.

[2] Eric Brier and Marc Joye. Weierstraß Elliptic Curves and Side-Channel Attacks. In *Proc. Public Key Cryptography - PKC*, pages 335–345, Paris, France, 2002.