Protecting Elliptic Curve Cryptography Against Fault Injection Attacks

Location. SEN group of the COMELEC department at Telecom ParisTech (37 rue Dareau, 75014, Paris). This internship can lead to a PhD thesis.

Advisors. Pablo Rauzy and Sylvain Guilley ({*firstname.lastname*}@telecom-paristech.fr).

Context. A fault injection attack consists in modifying an intermediate value of a computation (using an electromagnetic pulse or by acting on the power supply of the circuit) and exploiting the faulted final result to gather information about the computation that would not be accessible in a correct final result. For instance, did you know that due to the simplicity of the arithmetic behind RSA, injecting a single fault in an RSA computation makes it possible to easily extract the secret key? [2] The state of the art of countermeasures consists in defining attack conditions [1] (states of the computation which lead to a faulted result exploitable by an attacker) and proving that implementations do not verify these conditions, even when faulted. Currently, there exists a bunch of different ad-hoc countermeasures of which few have been formalized (or proved). However, no systematic approaches have been developed.

In the particular case of CRT-RSA, we have recently shown that existing countermeasures are effective against not only one but an arbitrary number of fault injections (up to a trivial adaptation) [4]. Some of these countermeasures were also able to thwart fault attacks that have been discovered after their publication. The particularity of these countermeasures is that they attempt to verify the integrity of the computation, in order to return the final result if and only if it is correct, thus avoiding any information leakage. The global idea behind these countermeasures is to achieve a verification in two different structures, one of which being *entangled* with the functional computation [3]. Therefore, an inconsistency in the redundant structure hints at a perturbation. Moreover, the mathematics employed by these protection techniques are not specific to the algorithm they protect, thus these countermeasures strategies can be applied to other cryptographic algorithms which also rely on arithmetic.

Problems.

- — Studying whether the *entanglement* technique can be used to develop a generic countermeasure that could be automatically applied to implementations of cryptographic algorithms.
- — Proving the efficiency of the countermeasure and the correctness of the resulting implementation.

Organization. During this internship the candidate should:

1. Familiarize herself/himself with:
   - – the literature on fault injection attacks;
   - – the finja[1] tool;
   - – existing countermeasures.
2. Prove that the *entanglement* strategy can apply to elliptic curve cryptography.
3. Implement an ECC algorithm (most likely a pairing computation) protected using this method, and then evaluate it:
   - – study the cost of the countermeasure in time and space;
   - – verifying it in practice on the fault injection bench of the lab.
4. Write a paper and submit it to a peer-reviewed conference ☺.

[1] `http://pablo.rauzy.name/sensi/finja.html`

References

[1] Gilles Barthe, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, and Jean-Christophe Zapalowicz. Synthesis of fault attacks on cryptographic implementations. *IACR Cryptology ePrint Archive*, 2014:436, 2014.

[2] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the Importance of Checking Cryptographic Protocols for Faults. In *Proceedings of Eurocrypt'97*, volume 1233 of *LNCS*, pages 37–51. Springer, May 11-15 1997. Konstanz, Germany. DOI: 10.1007/3-540-69053-0_4.

[3] Pablo Rauzy and Sylvain Guilley. Towards Generic Countermeasures Against Fault Injection Attacks, March 2015. TRUDEVICE workshop, at DATE (Grenoble, France).

[4] Pablo Rauzy and Sylvain Guilley. Countermeasures Against High-Order Fault-Injection Attacks on CRT-RSA. Cryptology ePrint Archive, Report 2014/559, 2014. `http://eprint.iacr.org/`.