Report for TRUDEVICE COST Action IC1204 STSM

Host Institution: Digital Security Group, Radboud University Nijmegen, Ass. Prof. Lejla Batina.
Visitor: Erich Wenger, Graz University of Technology, Austria.
Period: April 13th to April 26th 2014 (1.5 weeks).

Performed Research:

IT-security is an ever-growing field of research. Security concerns have to be addressed in cloud computing and even in the smallest RFID tags. To tackle most security targets, cryptographic algorithms are used on a regular basis. Especially public-key cryptography is used in a multitude of settings even tough it can have significant impacts on performance. Some of the most promising and highly regarded public-key algorithms nowadays take advantage of elliptic-curve cryptography (ECC).

For many years the target of most security engineers was to implement the fastest elliptic-curve scalar multiplications. However, nowadays it is of utmost importance that a fast implementation is also secure against practical timing-analysis, power-analysis, fault-analysis and even a combination of those attacks. Therefore, most techniques to target fast implementations are simply not feasible any more. And to make matters worse, new analysis techniques are created every year. E.g., two of the latest attack techniques are based on local electromagnetic emanation analysis and collision correlation analysis attacks.

The core goal of Erich Wenger's research visit was to evaluate the practicability of the latest implementation attacks, discuss necessary countermeasures, and discuss guidelines on how elliptic-curve cryptography should be implemented. During several discussions of guidelines, we came to the conclusion that is mandatory to further investigate horizontal collision correlation attacks before actually giving guidelines. Giving guidelines without fully understanding the latest attack techniques is "problematic".

The horizontal collision correlation attacks [1] were investigated on different levels. The core of those attacks is the fact that operands of finite-field or elliptic-curve point operations are reused during a scalar multiplication. If an attacker would be able to find a key-depended collision of operands, she would be able to recover the secret scalar. Therefore it was necessary to investigate horizontal collision correlation attacks of finite-field operations and an elliptic curve scalar multiplication algorithm.

As any scalar multiplication algorithm depends on finite-field operations [2], it was important to see which kind of operand-reuse can actually be detected. In order to visualize dependencies of operands, we performed several experiments. Figure 1 shows linear dependencies of (product-scanning) finite-field multiplications. Several sets of power traces were simulated (vcd-based toggle counts) and correlated with each other. Any linear dependence within the power-traces is shown as yellow to red. No linear dependence is displayed in blue.

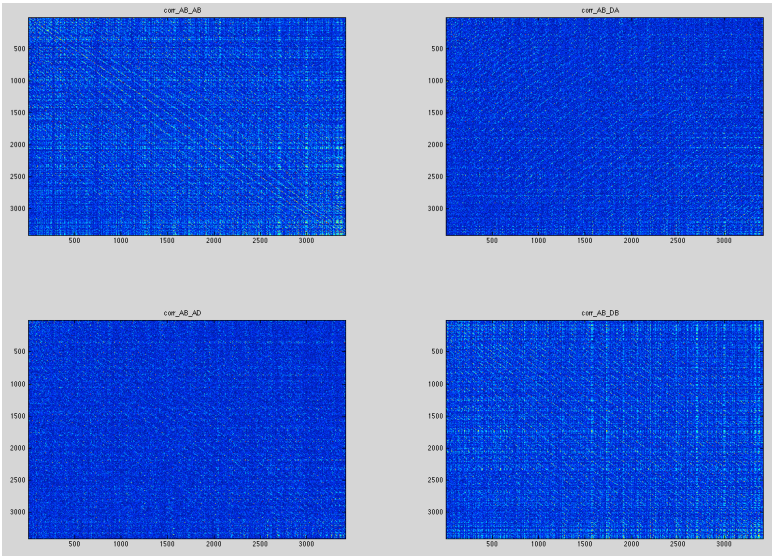

Figure 1 Correlation matrixes of different sets of power trace simulations

One can see in Figure 1 that indeed some patterns emerge. Correlating the set A×B with another set A×B (left upper) shows several linear dependences in the power traces. Such patterns even emerge in a correlation of A×B with A×D and D×B (lower row). Because of the asymmetry of the multiplier, the intensity of the patterns is different. Interestingly, also in a correlation of A×B with D×A, linear dependences could be detected.

Similar experiments have also been performed with finite-field additions and finite-field subtractions. This experiments showed that it is also possible to detect reused operands within additions and subtractions, but it is easier to detect reused operands when finite-field multiplications are tested.

Based on those promising results, we started to investigate several Montgomery ladders. As those will probably be recommended for future ECC implementations (guidelines), Montgomery ladders are of special interest.

Those experiments showed that with horizontal collision correlation attacks it was indeed possible to extract information that was hidden from standard difference-of-means tests. However, at this point further experiments are necessary before conclusions can be drawn. In future experiments we are going to conduct more experiments and only then we feel comfortable to further disclose our results.

In summary, visiting Nijmegen was an interesting, inspiring, and enlightening experience that slightly pushed the boundary on what is possible with horizontal collision correlation attacks.

[1] Erich Wenger, Thomas Korak, and Mario Kirschbaum. Analyzing Side- Channel Leakage of RFID-Suitable Lightweight ECC Hardware. Michael Hutter and Jörn-Marc Schmidt, editors, *RFIDSec*, volume 8262 of *Lecture Notes in Computer Science*, Springer, 2013.

[2] Erich Wenger, Thomas Unterluggauer, and Mario Werner. 8/16/32 Shades of Elliptic Curve Cryptography on Embedded Processors. In Goutam Paul and Serge Vaudeney, editors, *INDOCRYPT*, volume 8250 of *Lecture Notes in Computer Science*, Springer, 2013.