Report for TRUDEVICE COST Action IC1204 STSM

Host Institution: Department of Computer Science, University of Bristol, Dr Elisabeth Oswald.
Visitor: Erich Wenger, Graz University of Technology, Austria.
Period: The proposed visiting period is from June 23rd to June 27th 2014 (1 week).

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 Radio-Frequency-Identification (RFID) tags. To tackle most security targets, cryptographic protocols and algorithms are used on a regular basis. For many years the target of most security engineers was to implement the fastest cryptographic primitives and protocols. 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.

A new research direction tries to avoid implementation attacks by carefully designing protocols with implementation attacks in mind. For instance [MOS13] presented a leakage resilient Message Authentication (MAC) protocol using pairing and elliptic curve cryptography. Martin, Oswald, and Stam proposed to use asymmetric pairings to derive a symmetric message encryption and authentication protocol that is provable secure against side-channel and cryptographic attacks.

The core goal of Erich Wenger's research visit was to evaluate the practicability of leakage resilient pairing-based protocols and discuss whether currently applied implementations [UW14] are sufficient to actually secure [MOS13] practically. In [UW14] Thomas Unterluggauer and Erich Wenger presented a hardware/software codesign with which it is possible to securely and efficiently compute both elliptic curve cryptography and pairings. The proposed design handles implementation attacks in hardware and in software and computes a pairing in about 250ms. Therefore the design by [UW14] is potentially ideally suitable to be used as platform to evaluate the protocol by [MOS13].

The research visit in Bristol was very fruitful. While Dan Martin and Elisabeth Oswald provided a theoretical perspective on leakage resilient MAC, Erich Wenger contributed with his background on practical hardware and software implementations of pairings and elliptic curve cryptography. Several critical issues were identified that will be further investigated within the forthcoming weeks. Some of the interesting research questions are:

- Is it possible to implement the "hashing to a group element" operation in a side-channel and fault resistant way?
- Is it possible to include fault attacks in the model used to design a leakage resilient MAC?

- How can an implementer assure that the two shares of the MAC are really calculated separately? (Combining shares preliminarily would invalidate the security proof of the leakage resilient MAC)

References

[MOS13] D. Martin, E. Oswald, and M. Stam. A Leakage Resilient MAC. Cryptology ePrint Archive, Report 2013/292, 2013. http://eprint.iacr.org/.
[UW14] T. Unterluggauer, and E. Wenger. Efficient Pairings and ECC for Embedded Systems. CHES, to appear, 2014.