TRUDEVICE Short Term Scientific Missions Application

ICT COST Action IC1204: Trustworthy Manufacturing and Utilization of Secure Devices

November 5, 2014

Involved Institutions

Home Institution: IST, University of Lisbon, Portugal, Ricardo Chaves
Host Institution: Radboud University Nijmegen, The Netherlands, Lejla Batina

Visit Details

Visiting researcher: Ricardo Chaves
Visiting period: from **16/03/2015** to **15/05/2015**

Cost Estimation

Travel: 300 Euros
Accommodation: 2x690 = 1380 Euros
Meals: 60x10€/day = 600 Euros
Total: **2280 Euros**

Mission Statement

Physical and Side-Channel Attacks (SCA) refer to attacks that exploit the system's implementation characteristics. The research in this area has shown that (unintended) physical leakage caused by a straightforward implementation of a secure system can be crucial in terms of security. These leakages can be used to extract the secret values from cryptographic implementations, representing a serious threat to the system. Several techniques have been proposed to mitigate these attacks, namely by masking techniques, data independent execution, and computation balancing. However, all these solutions impose significant costs and still present leakages. Towards, more SCA resistant, reliable, and efficient designs alternative design methods need to be considered. One possible solution is the use of Residual Numbering Systems (RNS). RNS are carry-free arithmetic systems with modular characteristic that offer the potential for high-speed and applications on low power computational arithmetic's [Garner1959]. In RNS the operations can be carried out independently and concurrently on several residue channels, being more efficiently computed than in the conventional two's complement systems. Moreover, when large numbers need to be considered, the ability to obtain RNS moduli sets with a large amount of channels result in circuits with better performance, since each channel uses a lower number of bits, reducing the delay of the overall system [Hiasat2005]. RNS have also gained additional interest in preventing SCA [Schinianakis2006] while achieving overall gains. Bajard et. al. [Bajard2010] optimized the Montgomery algorithm using RNS multiplication, claiming that their design is secure against side channel attacks. However, no reliable attacks are still performed to fully justify this claim [Pettenghi2014].

The main goal of this mission is to adequately evaluate the resistance of asymmetric encryption implementations supported on RNS and design more SCA resistant cryptographic systems based on RNS. As the base system, supporting the RSA and ECC implementations to be SCA evaluated, the generic RNS architecture being developed at the Home Institution will be used. The expertise of the Host Institution in SCA evaluation and in the design of cryptographic primitives makes it an excellent destination to promote this research and collaboration towards this goal.

References

[Garner1959] Garner, Harvey L. "The residue number system." *Electronic Computers, IRE Transactions on* 2 (1959): 140-147.

[Hiasat2005] Hiasat, Ahmad A. "VLSI implementation of new arithmetic residue to binary decoders." *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on* 13, no. 1 (2005): 153-158.

[Schinianakis2006] Schinianakis, D. M., A. P. Kakarountas, and T. Stouraitis. "A new approach to elliptic curve cryptography: an RNS architecture." In Electrotechnical Conference, 2006. MELECON 2006. IEEE Mediterranean, pp. 1241-1245. IEEE, 2006.

[Bajard2010] Bajard, Jean-Claude, Sylvain Duquesne, and Milos D. Ercegovac. "Combining leak-resistant arithmetic for elliptic curves defined over Fp and RNS representation." IACR Cryptology ePrint Archive 2010 (2010): 311.

[Pettenghi2014] Hector Pettenghi, Ricardo Chaves, Leonel Sousa, and Jude Angelo Ambrose. “Method for designing Multi-Channel RNS Architectures to prevent Power Analysis SCAs." *In International Symposium on Circuits and Systems (ISCAS)*, 2014.