Side-Channel Analysis of the SHA-3 Finalists on SASEBO* (Abstract)

Julien Francq[1], Jean-Baptiste Rigaud[2] and Antoine Wurcker[1,3]

[1]CASSIDIAN, Cassidian CyberSecurity,
[2]École Nationale Supérieure des Mines de Saint-Étienne,
[3]Université de Limoges
[1]Julien.Francq@cassidian.com, [2]rigaud@emse.fr,
[3]antoine.wurcker@etu.unilim.fr

Cryptographic hash functions are involved in widely-used protocols such as signature schemes, Message Authentication Codes (MAC) or encryption schemes. Recently, some of them have been successfully attacked, and serious attacks have been published against the NIST approved cryptographic hash functions SHA-1, and the SHA-2 family. Consequently, NIST has decided to develop one or more additional hash functions through a public competition in order to specify its future hash standard SHA-3. The goal is to publish the augmented and revised Hash Function Standard by 2012. The SHA-3 competition is similar to the development process of the Advanced Encryption Standard (AES) that took place in 1997, and chose the new symmetric primitive in 2001.

In round three of the SHA-3 Contest, 5 finalists remain for consideration. These hash algorithms are available for public comment and scrutiny, and such research is vital to the selection process. In particular, NIST needs evaluation of the computational efficiency of the protected finalists against side-channel attacks.

Previous papers deal with attacks on finalists implementation in software and don't estimate the cost of protection against first order differential side-channel attacks. In our presentation, we will show physical attacks on hardware implementations and give the overhead brought by our side-channel protections.

In the first part of the talk, we will detail our hardware SHA-3 implementations on Virtex-5 FPGAs. We have implemented many variants which will be described. A deep design-space exploration have been done which gives good implementation results compared to the state-of-the-art.

Then, we will give the cost of using SHA-3 implementations in keyed-HMAC mode. We will see that some finalists are best adapted to HMAC in hardware than others.

In the third part of the talk, we will detail our first order masking schemes that we have implemented for each finalist and give the corresponding overheads in terms of area and throughput.

Finally, we will show that our side-channel protections are efficient thanks to deep analysis with Side-channel Attack Standard Evaluation BOard (SASEBO).

* This work is partially supported by the French Agence Nationale de la Recherche through the SAPHIR2 project under Contract ANR-08-VERS-014.

At the end of this talk, our results will be put back in the wider context of the SHA-3 competition.

The SHA-3 standard will be embedded in future FPGA devices dedicated to cryptographic applications: this is why this talk submission can be of interest for CryptArchi 2012 Workshop.