High-Speed Implementation of the SHA-3 Candidate Shabal[⋆]

(Abstract)

Julien Francq and Céline Thuillet

EADS Defence & Security, Cyber Security Customer Solutions Center
{Julien.Francq, Celine.Thuillet}@eads.com

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 two of the SHA-3 Contest, 14 candidates 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 has stated that computational efficiency of the algorithms in hardware, over a wide range of platforms, is addressed.

This talk will detail a significant contribution in the hardware benchmarking of the SHA-3 candidates. We will show that the French SHA-3 candidate `Shabal` can achieve a high throughput on Virtex-5 FPGAs despite its restricted parallelizability. Let's recall that high-throughput hash function implementations are beneficial, for example in network server applications. Moreover, our design brings the best throughput per slice of the state-of-the-art, which means that it makes the most efficient use of FPGA area. Our interesting results are mainly due to the use of carry-save adders for computing needed multi-operand addition, and by applying the so-called "unfolding method". At the end of this talk, our results will be put back in the wider context of the SHA-3 competition.

In the case that `Shabal` would become the SHA-3 standard, it will be embedded in future FPGA devices dedicated to cryptographic applications: this is why this talk submission can be of interest for CryptArchi 2010 Workshop.

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