Tutorial on Keccak and SHA-3

by Guido Bertoni

Abstract:

Keccak has been selected as SHA-3 in 2012. It is a very flexible algorithm allowing to perform all the primitives of symmetric key cryptography: stream cipher, hash, tree hashing, pseudo random number generation, authenticated encryption, MGF, KDF…

In this tutorial there will be a survey of the sponge construction, the general structure proposed for building permutation based primitives and how to use it.

A **second part** will explain the Keccak algorithm, the steps composing the algorithm, the parameters that can be tuned for different trade-off in term of security and speed.

The **third part** is about implementations: hardware, software, and protection against side channel attacks.

Finally an overview of the SHA-3 standard status and latest evolutions (Keyak and Ketje) submitted to the Caesar competition.

Intended audience: The presentation can be interesting for students and professionals that will have to implement SHA-3 in their upcoming products and/or want to study the implementation aspects of the algorithm

Agenda:

1. Introduction to symmetric primitives: encryption, hashing, authenticated encryption, key derivation function, mask generation…
2. The sponge construction: Security claims of the Sponge construction and use of sponge for developing symmetric primitives.
3. Keccak: description and motivation of the round function, security analysis.
4. Keccak implementation: software and hardware implementation
5. Side Channel: Attacks and protections of HW and SW implementation.
6. Status on SHA-3 standardization process and future trends