Romulus as NIST LWC Finalist

Chun Guo [1], Tetsu Iwata [2], Mustafa Khairallah [3], Kazuhiko Minematsu [4], Thomas Peyrin [3]

[1] Shandong University, China
chun.guo@sdu.edu.cn

[2] Nagoya University, Japan
tetsu.iwata@nagoya-u.jp

[3] Nanyang Technological University, Singapore
mustafa.khairallah@ntu.edu.sg,
thomas.peyrin@ntu.edu.sg

[4] NEC Corporation, Japan
k-minematsu@nec.com

Abstract. In this talk, we will summarize the rationale and latest results on the NIST Lightweight Cryptography competition finalist Romulus. More precisely, we will recall its three authenticated encryption with associated data (AEAD) variants (Romulus-N, Romulus-M and Romulus-T, all targeting 128-bit security for both computation and data) and its hash function Romulus-H, all based on the tweakable block cipher Skinny-128-384+.

Romulus-N is a very efficient and lightweight nonce-based beyond-birthday bound AEAD scheme. Romulus-M is a lightweight nonce-misuse resistant beyond-birthday bound AEAD scheme (the only nonce-misuse resistant candidate remaining in the competition), very similar to Romulus-N and that also offers the Release Unverified Plaintext (RUP) security feature. Nonce-misuse resistance and RUP are important for many use-cases of lightweight cryptography, but also for cryptography in general, and Romulus-M provides both for a performance profile close to that of Romulus-N. Finally, Romulus-T is a strong lightweight leakage-resilient AEAD scheme that allows a natural protection against side-channels attacks and can leverage in addition the efficient masking capability inherent to tweakable block ciphers.

We will start by reviewing the latest cryptanalysis advances on Skinny (that was recently added to the ISO standard ISO/IEC-180033-7), with a focus on Skinny-128-384+ and its very large security margin.

On the operating modes side, we will recall the security proof results covering the various Romulus schemes and also exhibit new ones for the MDPH hashing mode upon which Romulus-H is based. We will also present the outcome of the third-party analysis of our Romulus security proofs conducted by Jooyoung Lee.

Regarding the implementations, we will show latest hardware and software implementation results, as well as new masked implementations.

Furthermore, we will focus on a few typical lightweight cryptography scenarios (RFID tags, 8-bit micro-controllers, small messages, etc.) to showcase the efficiency of Romulus.