From: Markku-Juhani O. Saarinen <mjos.crypto@gmail.com>
Sent: Wednesday, May 29, 2019 6:02 AM
To: lwc-forum
Subject: [lwc-forum] OFFICIAL COMMENT: SNEIK

Hi,

I realized that the change in SNEIK 1.1 has not been submitted as an "official comment".

So again; In response to the differential flaw discovered Léo Perrin [1] and used by Mustafa Khairallah in a forgery attack [2], the specifications and implementations of SNEIK have been updated to include the 1-bit rotation fix suggested in by Léo in [1]. I've been in touch with Léo, Mustafa, and Samuel Neves regarding this. I can't talk on their behalf but they also seem to consider the 1-bit rotation to be a sound fix to this issue. The change has a very limited impact on implementation characteristics of software and hardware implementations.

Updated specifications and implementations are available at https://github.com/pqshield/sneik

Cheers,
- markku

[1] Léo Perrin, "Probability 1 Iterated Differential in the SNEIK Permutation", https://eprint.iacr.org/2019/374
[2] Mustafa Khairallah, "Forgery Attack on SNEIKEN", https://eprint.iacr.org/2019/408

Cheers,
- markku

Dr. Markku-Juhani O. Saarinen <mjos@iki.fi>
--
To unsubscribe from this group, send email to lwc-forum+unsubscribe@list.nist.gov
Visit this group at https://groups.google.com/a/list.nist.gov/d/forum/lwc-forum

From: Markku-Juhani O. Saarinen <mjos@pqshield.com>
Sent: Monday, August 19, 2019 5:47 AM
To: lwc-forum@list.nist.gov; lightweight-crypto
Subject: OFFICIAL COMMENT: SNEIK

Hello,

There's a new technical report related to the performance of SNEIK on lightweight CPUs, and also hardware-software codesign:

Markku-Juhani O. Saarinen,
"SNEIK on Microcontrollers: AVR, ARMv7-M, and RISC-V with Custom Instructions", IACR ePrint 2019/936
https://eprint.iacr.org/2019/936

- Implementation on 32-bit RISC-V (RV32I), measurements. Describes a hardware-software codesign based on an ISA extension (about 5x speed improvement with few hundred LUTs on Artix-7).

- In addition to timing just the permutation, presents benchmarks of the SNEIKEN AEAD and SNEIKHA hash on messages of 50, 100, 500, and 1000 bytes on AVR, ARMv7-M, and RV32I. This is relevant especially when comparing SNEIK to smaller permutations (e.g. Gimli, Xoodoo).

- The new ARMv7-m implementations have about 10% speed improvement and smaller size.

The official SNEIK distribution at https://github.com/pqshield/sneik has been updated with improved ARMv7 assembler. Also added the base RV32I assembler version, which is a new target for SNEIKEN and SNEIKHA. The v1.1 specification document is unchanged.

ps. The ARMv7 assembler code indeed runs on all ARMv7 (such as ARMv7-a of 32-bit Android devices) in addition to ARMv7-m of Cortex M3/M4 MCUs and SecurCore SC300 secure elements.

Cheers,
- markku

Dr. Markku-Juhani O. Saarinen <mjos@pqshield.com> PQShield, Oxford UK.