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