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


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