KangarooTwelve

draft-irtf-cfrg-kangarootwelve

Benoît Viguier[1] David Wong[2] Gilles Van Assche[3]
Quynh Dang[4] Joan Daemen[1]

[1] Radboud University, The Netherlands
[2] Facebook, USA
[3] STMicroelectronics, Belgium
[4] NIST, USA

CFRG meeting
IETF 110, March 12, 2021

Refresh: what is KANGAROOTWELVE?

Start with SHAKE128 [FIPS 202], then

- reduce to 12 rounds;
- add parallelism.

For instance: 0.51 cycles/byte on CascadeLake and SkylakeX.

Recent history of draft-irtf-cfrg-kangarootwelve

2019-08-06	version -00, becomes a WG item
2020-01-04	version -01 (typos)
2020-02-15	comments from Jean-Philippe Aumasson
2020-03-12	version -02 (JP's and Stephen Farrell's comments)
2020-07-17	comments from Thomas Pornin
2020-09-01	version -03 (Thomas' comments)
2020-09-21	version -04 (comments from Pascal Junod)
2020-10-27	**last call from the CFRG chairs**
2020-11-25	positive feedback from Christoph Dobraunig
2021-02-16	**last call reminder**
2021-02-19	version -05 (Benoît's email changed)
2021-02-21	comments from Mark 'pendame' Rogers

Why is KangarooTwelve useful?

Distinct implementation properties

- Short critical path in circuits
  (also examplified by some new CPU instructions)
- Efficient countermeasures against DPA, when needed

Synergy with SHA-3-related investments

- Same cryptanalysis effort as for Keccak/SHA-3
- Re-use of implementations (see also Apple A14 and M1)

Thanks for your attention!