Support KangarooTwelve @ CFRG!

Joan Daemen Gilles Van Assche Benoît Viguier

FSE rump session
November 11, 2020

Reduce # rounds in KECCAK?

- KECCAK's round function unchanged since 2008
  - sustained cryptanalysis by multiple teams since then
    see `https://keccak.team/third_party.html`
- Nominal # rounds vs broken # rounds:
  - **24** rounds: KECCAK/SHA-3/SHAKE
  - **9** rounds: distinguishers (e.g., SymSum [Suryawanshi et al.])
  - **5** rounds: best collision attacks
    [Song et al.] [Dinur et al.] [Qiao et al.]

Can we reasonably reduce to **12** rounds?

Yes, we can!

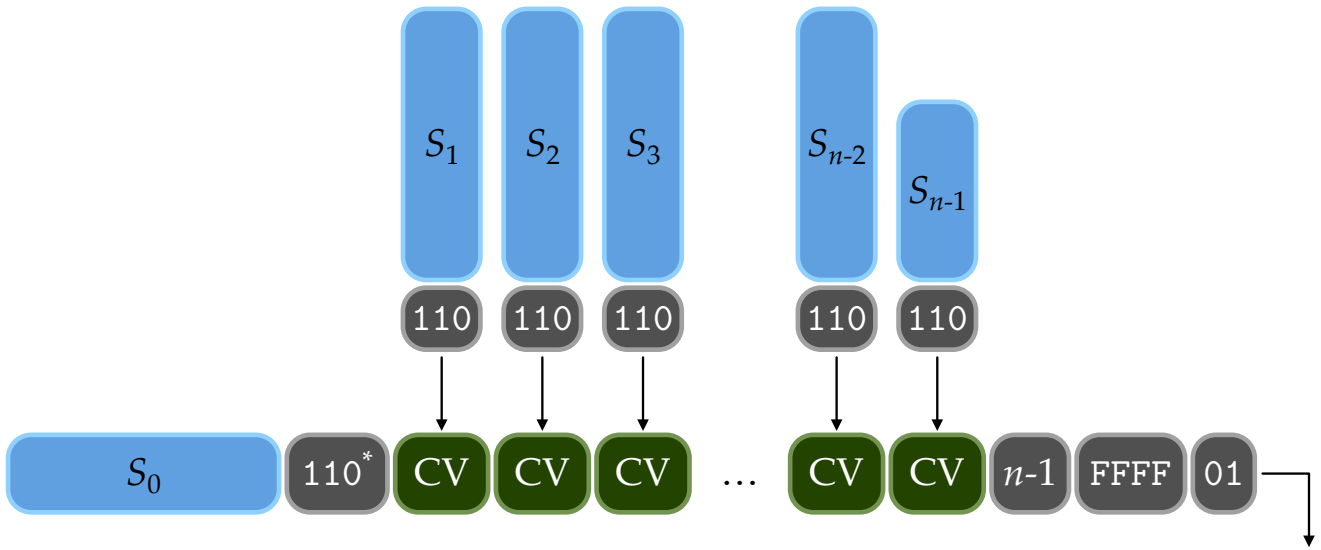
Better exploit parallelism

- SIMD with growing widths
  - 128, 256 and now even 512 bits
- Multiple cores, ...

$\Rightarrow$ let's exploit this parallelism

KangarooTwelve

Tree hash mode with Sakura encoding: [ACNS 2014, 2018]



	Short input	Long input
Skylake with AVX2	2.89 c/b	1.22 c/b
SkylakeX with AVX-512	2.07 c/b	0.51 c/b

And we proposed it as an RFC at CFRG!

Support KangarooTwelve @ CFRG!

Current status:

- WG RFC draft `draft-irtf-cfrg-kangarootwelve`
- CFRG issued a 2-week last call (ended on Monday)
  … no reactions …

What can you do? If you think:

- K12 has good safety margin in light of **your** cryptanalysis
- K12 has sound design and components
- K12 can benefit users of *Fast Software* crypto

then, **please send an email to CFRG mailing list, and say so!**

Thank you!