NIST Update (CHES version)

John Kelsey, NIST / KU Leuven

Lightweight Crypto Standardization

- **Plan:** Standardize lightweight crypto algorithms for constrained environments.

- **Aug 27, 2018:** Call for submissions for a lightweight AEAD scheme with optional hashing functionality.

Subscribe to mailing list: lwc-forum+subscribe@list.nist.gov

Project webpage: https://csrc.nist.gov/projects/lightweight-cryptography

Threshold Cryptography Standardization

- **Plan:** Standardize threshold schemes for crypto primitives
- Draft NISTIR 8214: "Threshold Schemes for Cryptographic Primitives."
  - Public comments are due by **October 22, 2018**.

- **NIST Threshold Cryptography Workshop 2019**
  - **March 11-12, 2019** at NIST (Gaithersburg, MD).
  - Call for submissions: https://csrc.nist.gov/events/2019/NTCW19

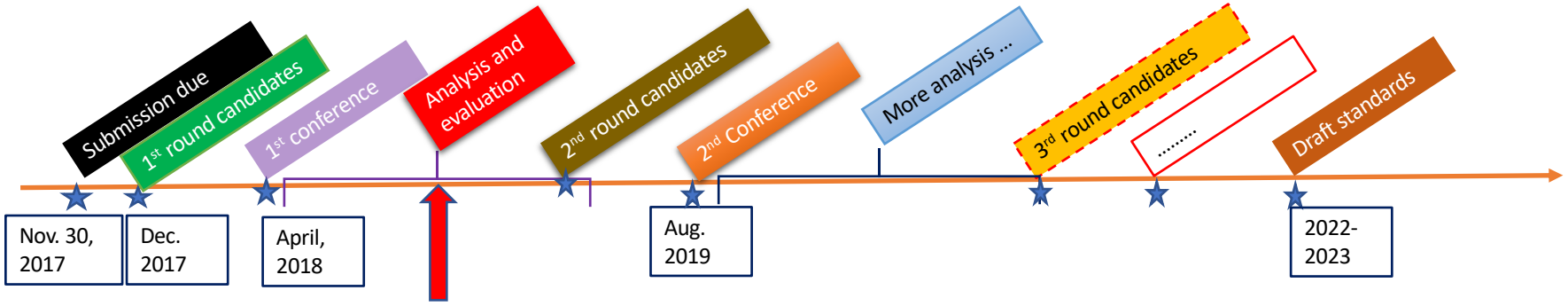
Mailing list: https://groups.google.com/a/list.nist.gov/forum/#!forum/tc-forum

Project webpage: https://csrc.nist.gov/projects/threshold-cryptography

Contact us: threshold-crypto@nist.gov

Post-quantum Standardization Update

- 63 submissions currently in consideration
  - 69 “complete and proper” first round candidates; 5 withdrawn; 1 proposed merger
- NIST will announce 2nd round candidates early in 2019
  - To be considered for 2nd round selection, mergers should be announced by November 30.
- 2nd NIST Post-quantum Standardization Conference Aug. (2019) to be collocated with CRYPTO2019!



Update to SP800-131A Rev. 2 (DRAFT)

How NIST updates key lengths and algorithm recommendations

- NOTE: Strategy for retiring TDEA (aka 3DES)
  - Depecated through 2023
  - Disallowed after 2023

- **Comment period ended on 09/07/2018**
- **…but we will read comments sent a few days late.**

https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/draft

Email comments to: *sp800-131a_comments@nist.gov*

SP 800-90B: Entropy Sources for RNGs

- Published January 2018
- Received lots of feedback
- Soon: Errata list and corrected version
- Eventually: Revision (after we get experience using it)

- We want to hear from you!

  Send comments to rbg-comments@nist.gov

Talk on 90B: Thursday at FTDC, followed by panel discussion on RNGs

NIST Beacon

- Source of signed, timestamped, **public** random numbers
- New format (version 2.0)
  - Lots of new security features
  - Support for combining pulses from multiple beacons
  - Support for incorporating external sources
- Other beacons planning to follow protocol
  - Universidad de Chile
  - INMETRO (Brazilian standards organization)
- NIST-IR (basically a whitepaper) describing new format
  - Coming soon

- https://beacon.nist.gov/home

FIPS 186-5 Digital Signature Standard

- Under revision, out for public comment soon

Important points:

- EdDSA and deterministic version of ECDSA to be added
- Larger modulus sizes for RSA signatures allowed ($n > 3072$ bits)
- Recommended elliptic curves will be put into a new document
  - SP 800-186

Email comments to: **fips186-comments@nist.gov**