National Institute of Standards and Technology
U.S. Department of Commerce

NIST Update

Eurocrypt 2018 Rump Session

Jacob Alperin-Sheriff

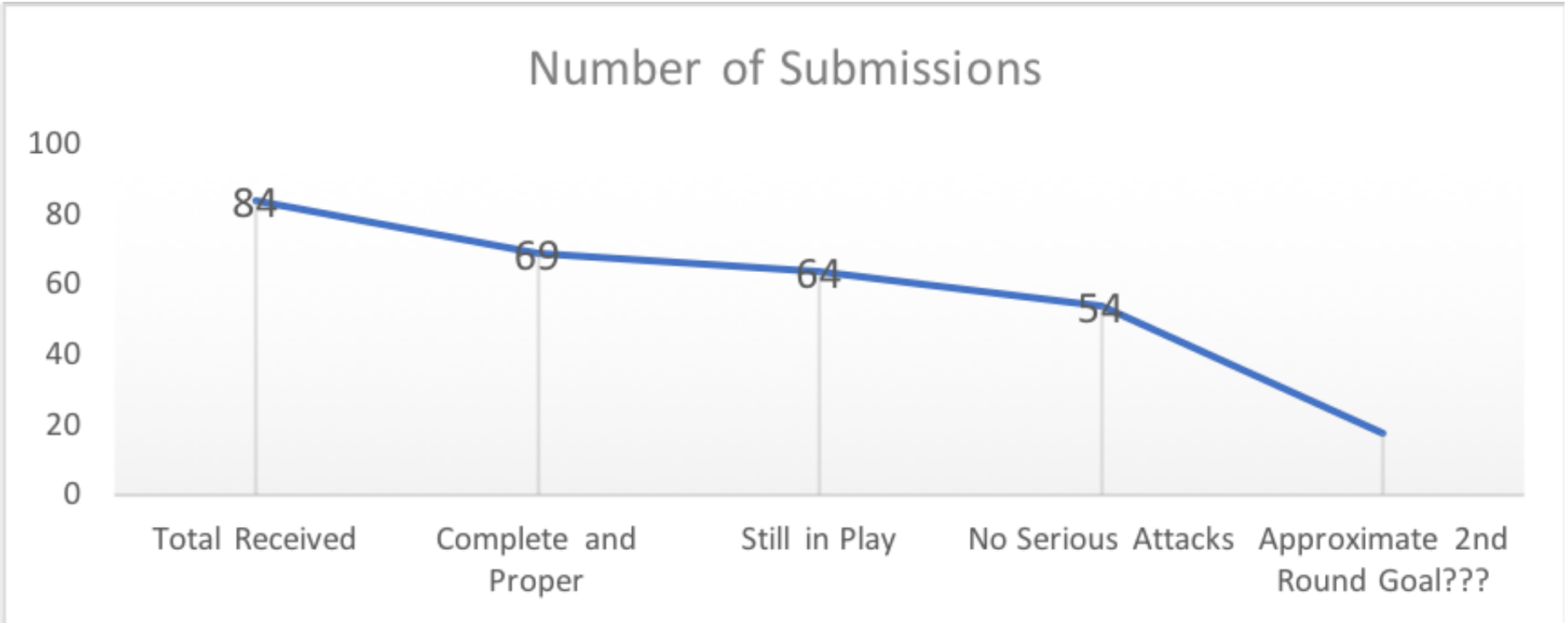
NIST

April 24, 2018

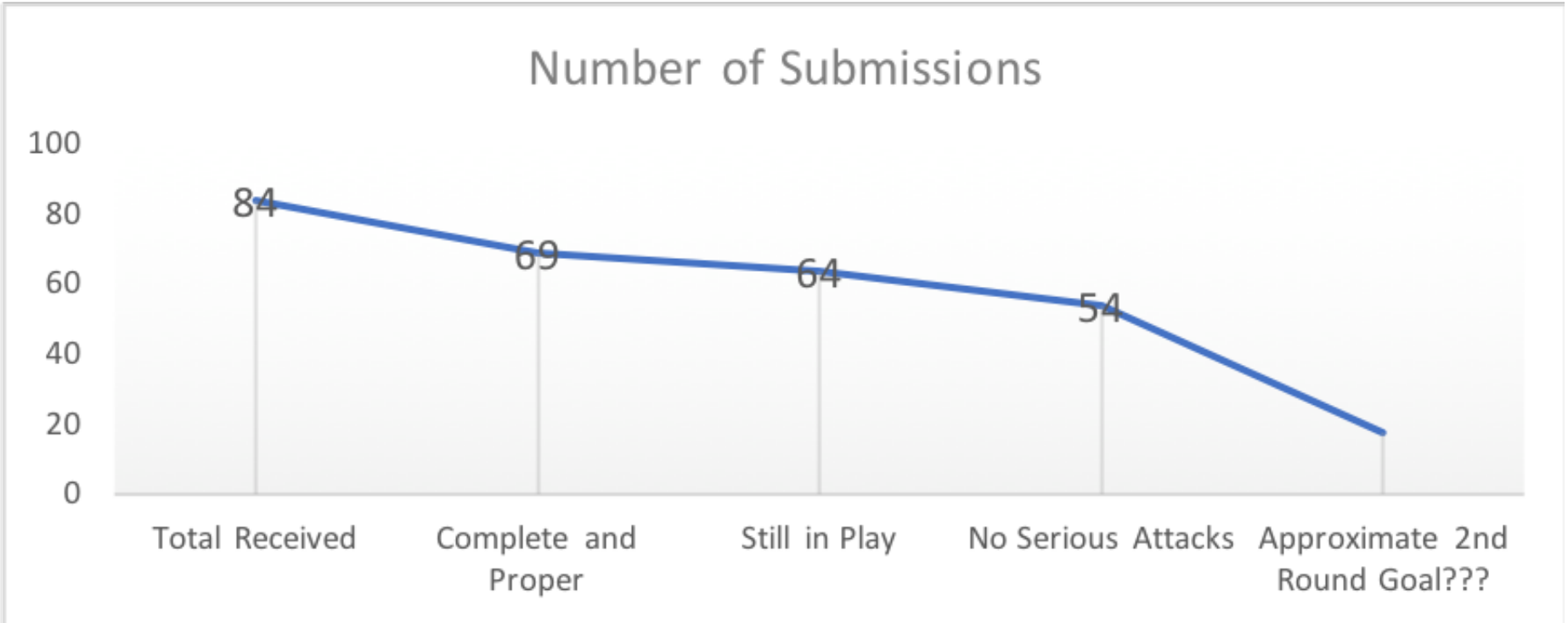
CSRC

- (Almost) every scheme was presented; 15 minutes each

- (Almost) every scheme was presented; 15 minutes each
- Thanks for making it a success!



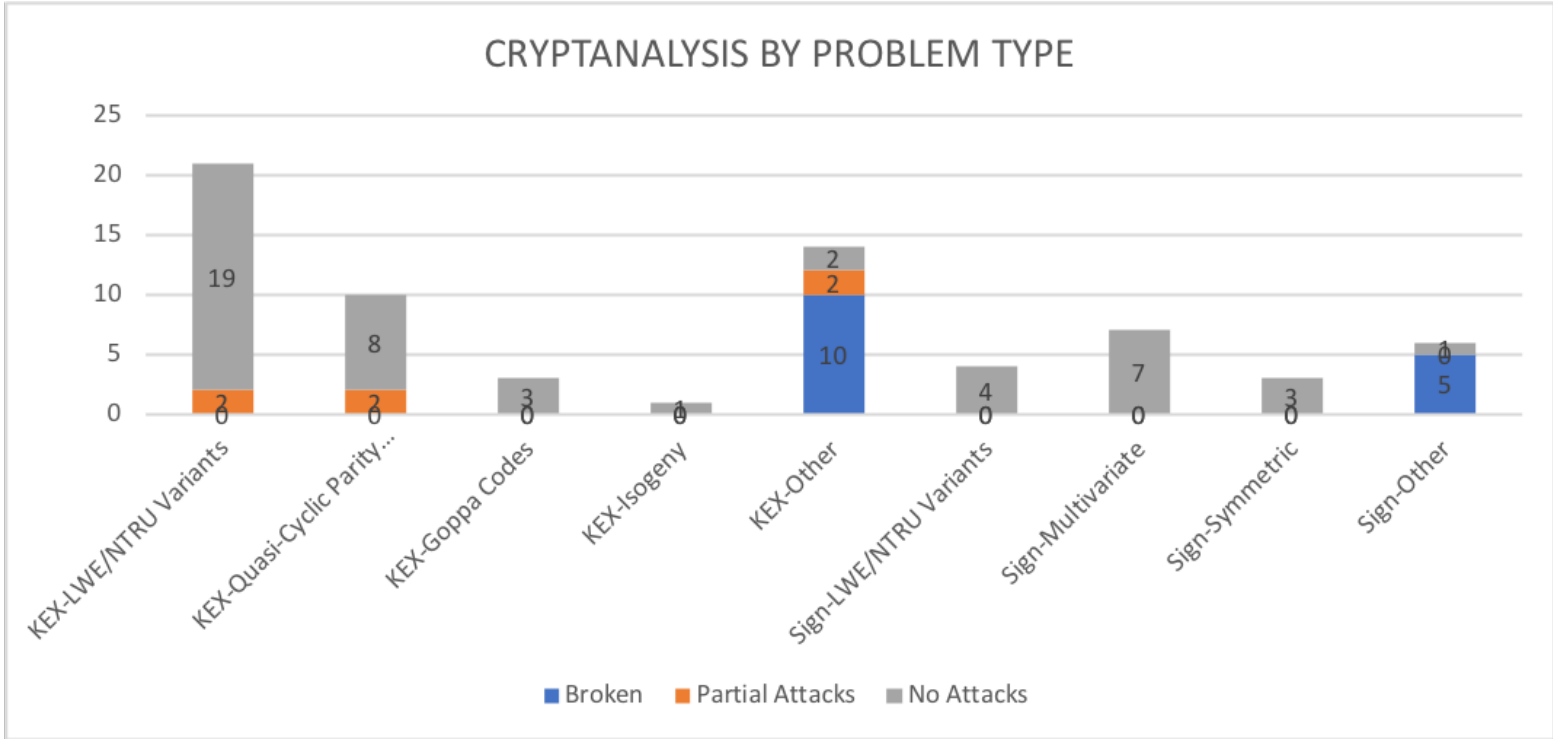
NO CONCRETE GOAL YET FOR 2nd ROUND



NO CONCRETE GOAL YET FOR 2nd ROUND

- 2nd Round decisions expected late 2018-early 2019

PQC–Breaks by Problem Category



PQC–We Need Comments

- ✔ Cryptanalysis Success = Publication

PQC–We Need Comments

- ✔ Cryptanalysis Success = Publication
- ✗ Cryptanalysis Failure = Dead Silence

✔ Cryptanalysis Success = Publication

✗ Cryptanalysis Failure = Dead Silence

PLEASE TELL US BOTH!

Submissions: `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`

Comments: `pqc-comments@nist.gov`

- NIST has initiated a process to standardize lightweight cryptographic algorithms suitable for constrained environments.
- In April 2018, NIST published a **draft** call for submissions that asks for a lightweight AEAD scheme with optional hashing functionality.
  - Send your comments on the draft to `lightweight-crypto@nist.gov`

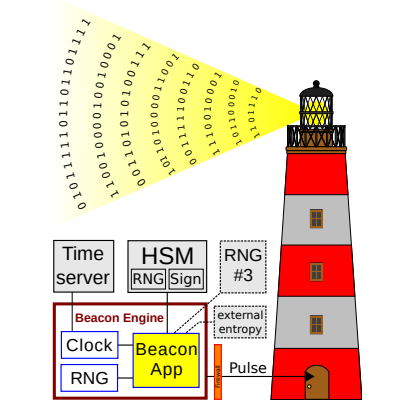
- NIST has initiated a process to standardize lightweight cryptographic algorithms suitable for constrained environments.
- In April 2018, NIST published a **draft** call for submissions that asks for a lightweight AEAD scheme with optional hashing functionality.
  - Send your comments on the draft to `lightweight-crypto@nist.gov`
- Next step: Finalize the call based on public comments.

- NIST has initiated a process to standardize lightweight cryptographic algorithms suitable for constrained environments.
- In April 2018, NIST published a **draft** call for submissions that asks for a lightweight AEAD scheme with optional hashing functionality.
  - Send your comments on the draft to `lightweight-crypto@nist.gov`
- Next step: Finalize the call based on public comments.

Mailing List: `mailto:lwc-forum+subscribe@list.nist.gov`

Webpage: `https://csrc.nist.gov/projects/lightweight-cryptography`

The NIST Randomness Beacon

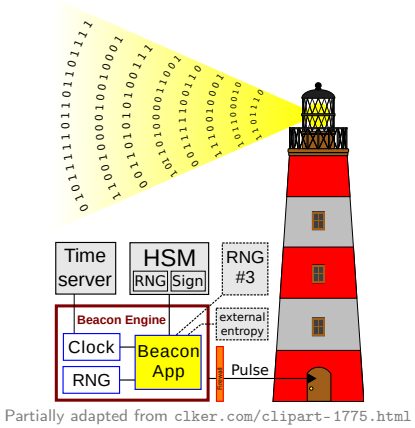


Partially adapted from clker.com/clipart-1775.html

Version 1 online since 2013: https://beacon.nist.gov

- 512 random bits per minute
- Timestamped, signed, hash-chained, preserved forever
- $>$2 million pulses by April 2018

The NIST Randomness Beacon



Partially adapted from clker.com/clipart-1775.html

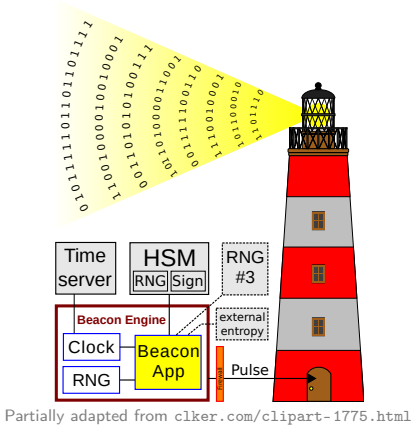
Version 1 online since 2013: https://beacon.nist.gov

- 512 random bits per minute
- Timestamped, signed, hash-chained, preserved forever
- >2 million pulses by April 2018

NIST Beacon v2 ... coming soon:

- New randomness field, pre-committed, for combining beacons
- Several countries will have inter-operable Beacons: Brazil, Chile, ...

The NIST Randomness Beacon



Partially adapted from clker.com/clipart-1775.html

Version 1 online since 2013: https://beacon.nist.gov

- 512 random bits per minute
- Timestamped, signed, hash-chained, preserved forever
- >2 million pulses by April 2018

NIST Beacon v2 ... coming soon:

- New randomness field, pre-committed, for combining beacons
- Several countries will have inter-operable Beacons: Brazil, Chile, ...

Envisioned applications:

- Randomization for statistical trials, quality control, clinical experiments, ...
- Assign court cases to judges; select politicians for audit; ...
- ... we'd appreciate hearing your suggestions