



## The NIST Crypto Reading Club

Cryptographic Technology Group, Computer Security Division



Live at <https://csrc.nist.gov/projects/crypto-reading-club>

### Once upon a time ...

... there were many **cryptography** stories to tell



The Crypto Reading Club has hosted **250+** talks!

- : Active since May 2006, for 17.5 years
- : # talks per year: 14.5 (avg) ± ≈ 6 (stdev)  
(avg = average; stdev = standard deviation)
- : ≈ 150 speakers (NIST-internal and external)
- : Virtual/hybrid (recorded) talks since ≈ 2020

### More than a word cloud!?



(Word cloud created from the titles of the crypto reading club talks)

### The benefits of public reference material

Accessibility, credibility, transparency, educational material, research ideas, training & updates, referenceability, ...

### Crypto blocks across time? (an analogy)

1. Each “reference material” item is a stone in a wall
2. Which crypto blocks will resist the test of time?



### The NIST Stone Test Wall (2018 / 1948)

2352 individual samples of stone: 2032 domestic (from 47 states) + 320 from 16 foreign countries

### The NIST C.R.Club is also:

- **Tradition:** A reference activity of the Crypto Group
- **Outreach:** A point of contact with/for external stakeholders. The mailing-list has ≈ 170 members
- **Complementary** to other outputs/activities: reports & papers, NIST workshops & external presentations, standards, SDO collaboration & public calls, ...
- **Flexible style/content:** dissemination (ongoing activities, research) classic techniques and curiosities, rehearsals, gather feedback, introduce ideas, ...

### You should join (Why, How, When)

- Come learn about recent and old cryptography topics
- Interact with crypto researchers or/and give a talk
- **How:** Subscribe to the C.R.Club mailing list for announcements
- **When:** Meetings are on interleaved Wednesdays (10–11am Eastern Time)

### Other Crypto Presentations Sets at NIST

The **CSRC** archives past NIST-hosted crypto presentations. More than **870 talks (T)** and **63 panels/discussions (P)**.

#### 37 Crypto-related Workshops (W)

<b>PQC</b>  5W-212T-4P	<b>LWC</b>  6W-156T-1P	<b>MPTS</b>  3W-91T-2P	<b>PEC</b>  1W-15T-4P	<b>STPPA</b>  6E-26T-5P
<b>RBG</b>  4W-59T-12P	<b>Hash</b>  6W-149T-16P	<b>BCM</b>  3W-34T-1P	<b>ECC/Pairs</b>  3W-54T-7P	<b>KeyMgt</b>  6W-66T-10P
				<b>PQC</b>  9 talks

#### 2 Seminars

**Legend:** BCM = Block-Cipher Modes, CSRC = Computer Security Resource Center, E = Events, ECC = Elliptic-Curve Cryptography, STPPA = Special Topics on Privacy and Public Auditability, KeyMgt = Cryptographic-Key Management, LWC = Lightweight Cryptography, MPTS = Multi-Party Threshold Schemes, Pairs = Pairings (a.k.a. bilinear maps), PEC = Privacy-Enhancing Cryptography, PQC = Post-Quantum Cryptography, RBG = Random-Bit Generation, SDO = Standards Development Organization.

Poster produced by Luís Brandão<sup>†</sup> for the NIST-ITL Science Day 2023 (November 8<sup>th</sup>).  
<sup>†</sup> Foreign Guest Researcher (non-employee) at NIST, contractor from Strativiva.  
The background and the header images were provided by the ITL Science Day Team.  
Free-use cliparts were obtained (and/or adapted) from external sources, including cldcker.com and iconpacks.net.

