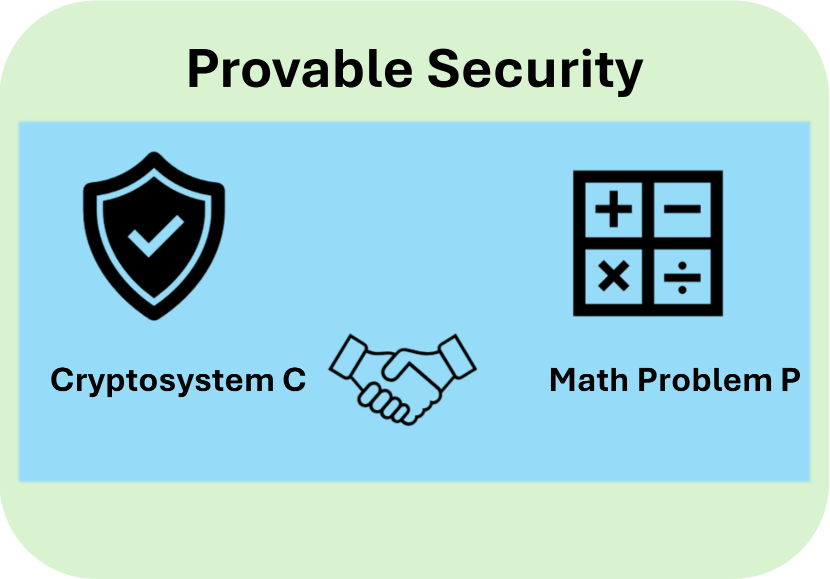
An Overview of the NIST Standardization of MPTC

Cecilia Boschini

February 21st 2026

Who am I?

- **PhD** (USI Lugano + IBM Research)
- Senior **Researcher** at ETH D-INFK
  Foundation of Cryptography group (prof. Hofheinz)



Provable Security

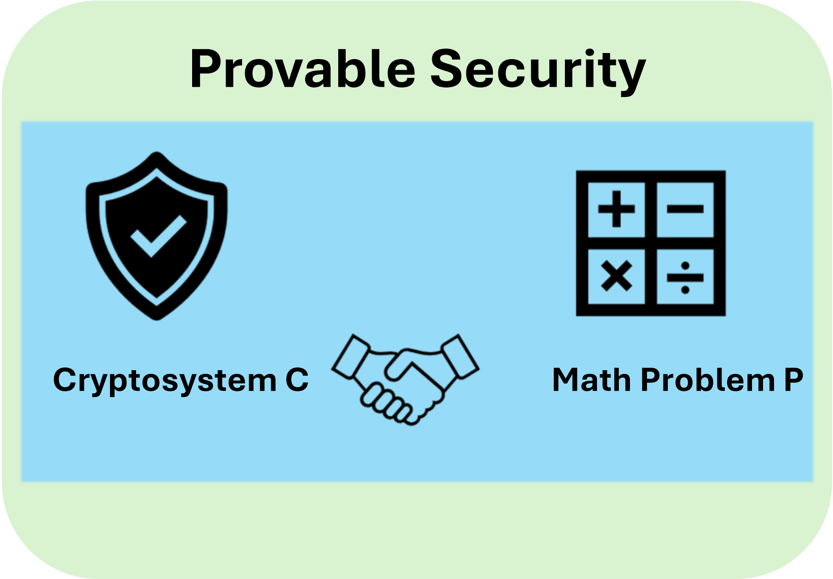
Cryptosystem C

Math Problem P

Post-Quantum Cryptography:
- schemes run on *classical* computers
- attacks could exploit *quantum* computers

Who am I?

- **PhD** (USI Lugano + IBM Research)
- Senior **Researcher** at ETH D-INFK
  Foundation of Cryptography group (prof. Hofheinz)

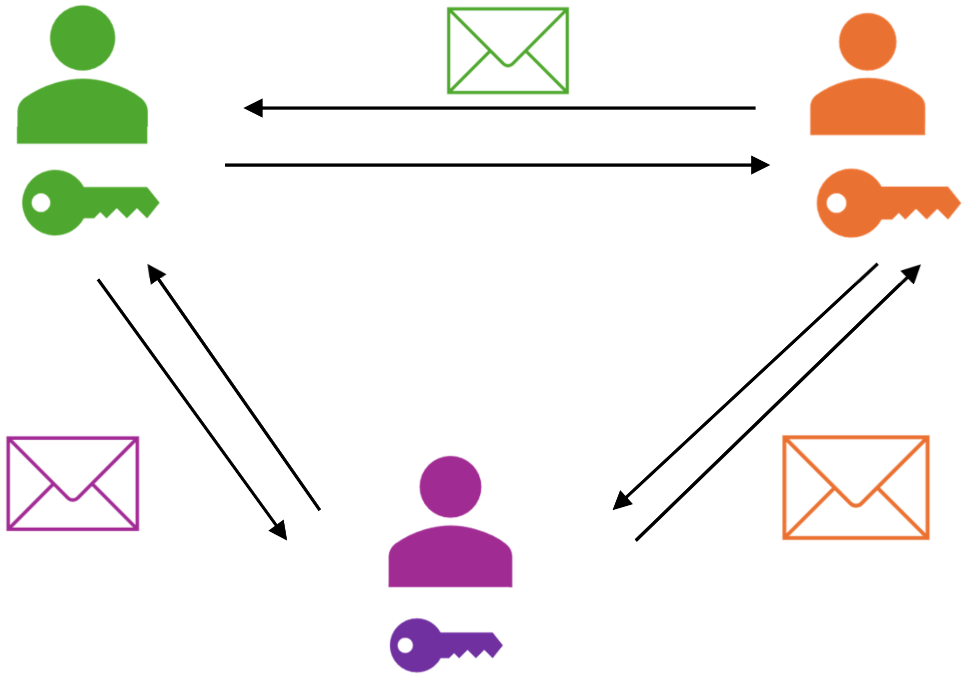


This talk: gentle intro about
- Multi-Party Computation
- Standardization processes

Goal: convince you that you might be interested in standardization too ☺

Post-Quantum Cryptography:
- schemes run on *classical* computers
- attacks could exploit *quantum* computers

Multi-Party (Threshold) Cryptography



- Multiple parties want to run some computation without revealing their secret keys.

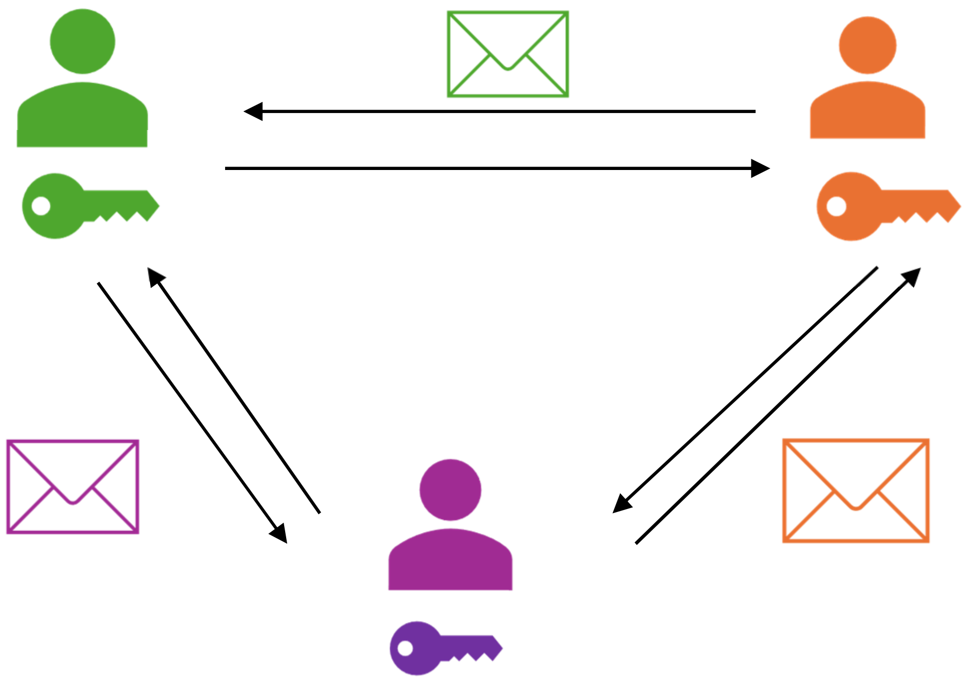
- What can you distribute? Virtually everything! Signing, encrypting, decrypting, key generation, ….

- Applications: auctions, elections, privacy-preserving ML…

- VERY OLD: first paper by Andrew Yao in 1982!!

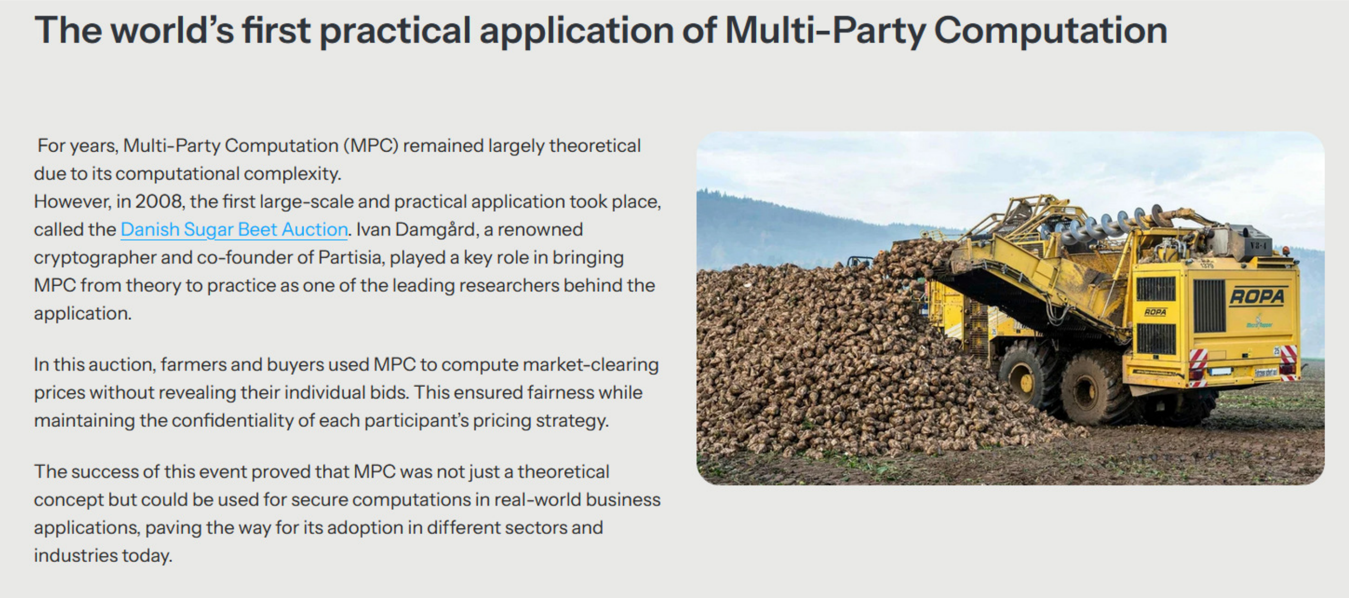
Threshold Cryptography ensures that the computation can proceed as long as a threshold of parties participates in the computation.

Security?



- IDEALLY: computation reveals nothing besides the output
- Key remains split
  ⇒ No party is a critical point of failure.
- Adversary: can corrupt some parties and misbehave
- Various degrees of compromise: from honest-but-curious, to actively malicious

Useful in practice?

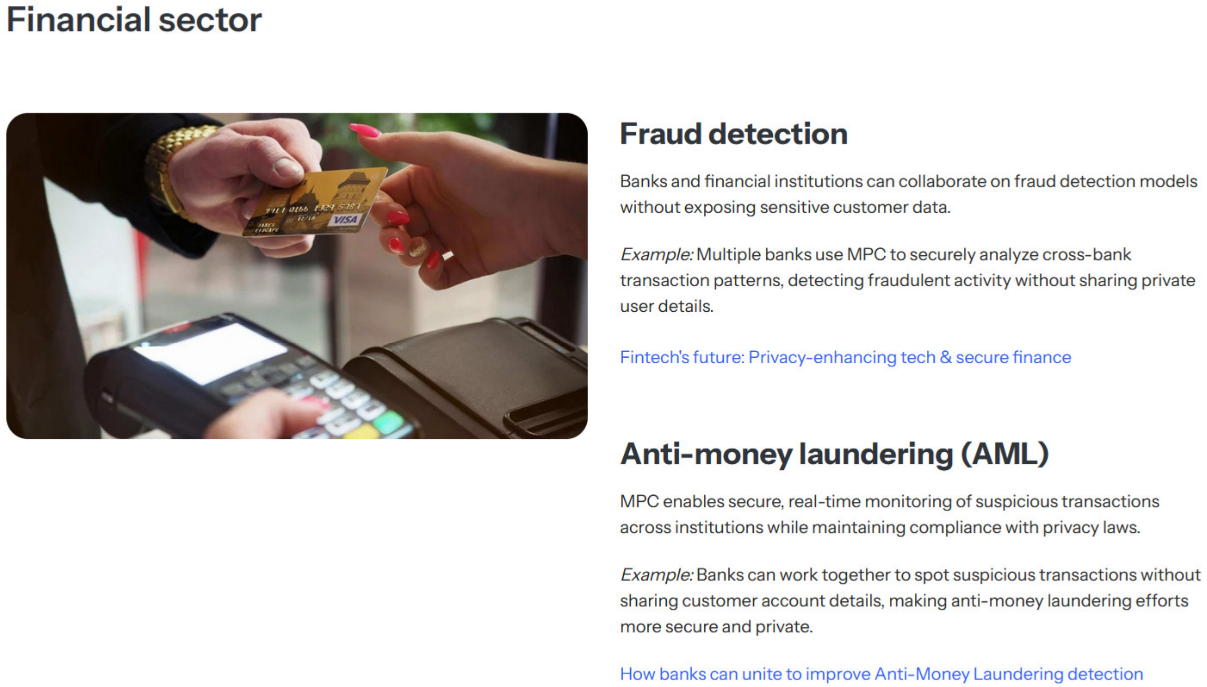


The world's first practical application of Multi-Party Computation

For years, Multi-Party Computation (MPC) remained largely theoretical due to its computational complexity.
However, in 2008, the first large-scale and practical application took place, called the Danish Sugar Beet Auction. Ivan Damgård, a renowned cryptographer and co-founder of Partisia, played a key role in bringing MPC from theory to practice as one of the leading researchers behind the application.

In this auction, farmers and buyers used MPC to compute market-clearing prices without revealing their individual bids. This ensured fairness while maintaining the confidentiality of each participant's pricing strategy.

The success of this event proved that MPC was not just a theoretical concept but could be used for secure computations in real-world business applications, paving the way for its adoption in different sectors and industries today.



Financial sector

Fraud detection

Banks and financial institutions can collaborate on fraud detection models without exposing sensitive customer data.

Example: Multiple banks use MPC to securely analyze cross-bank transaction patterns, detecting fraudulent activity without sharing private user details.

Fintech's future: Privacy-enhancing tech & secure finance

Anti-money laundering (AML)

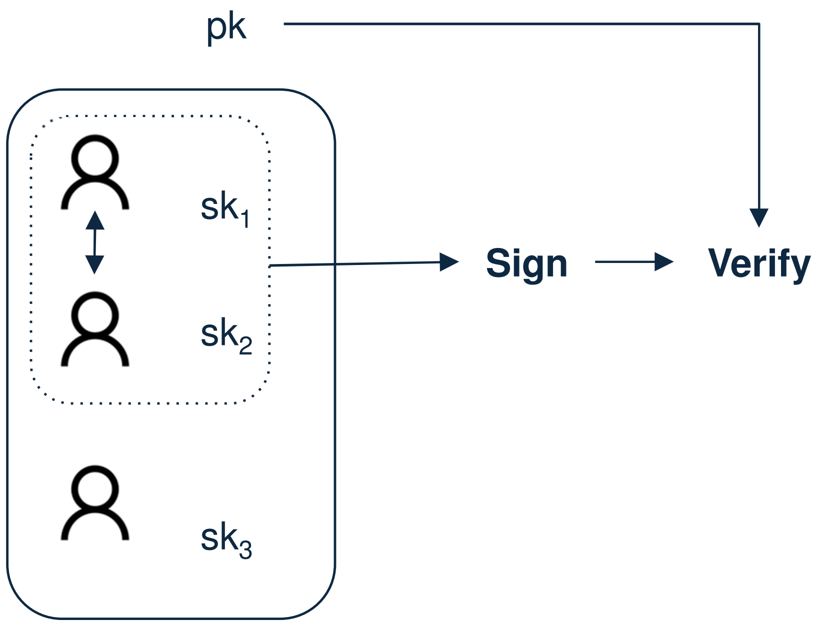
MPC enables secure, real-time monitoring of suspicious transactions across institutions while maintaining compliance with privacy laws.

Example: Banks can work together to spot suspicious transactions without sharing customer account details, making anti-money laundering efforts more secure and private.

How banks can unite to improve Anti-Money Laundering detection

https://www.partisia.com/tech/multi-party-computation

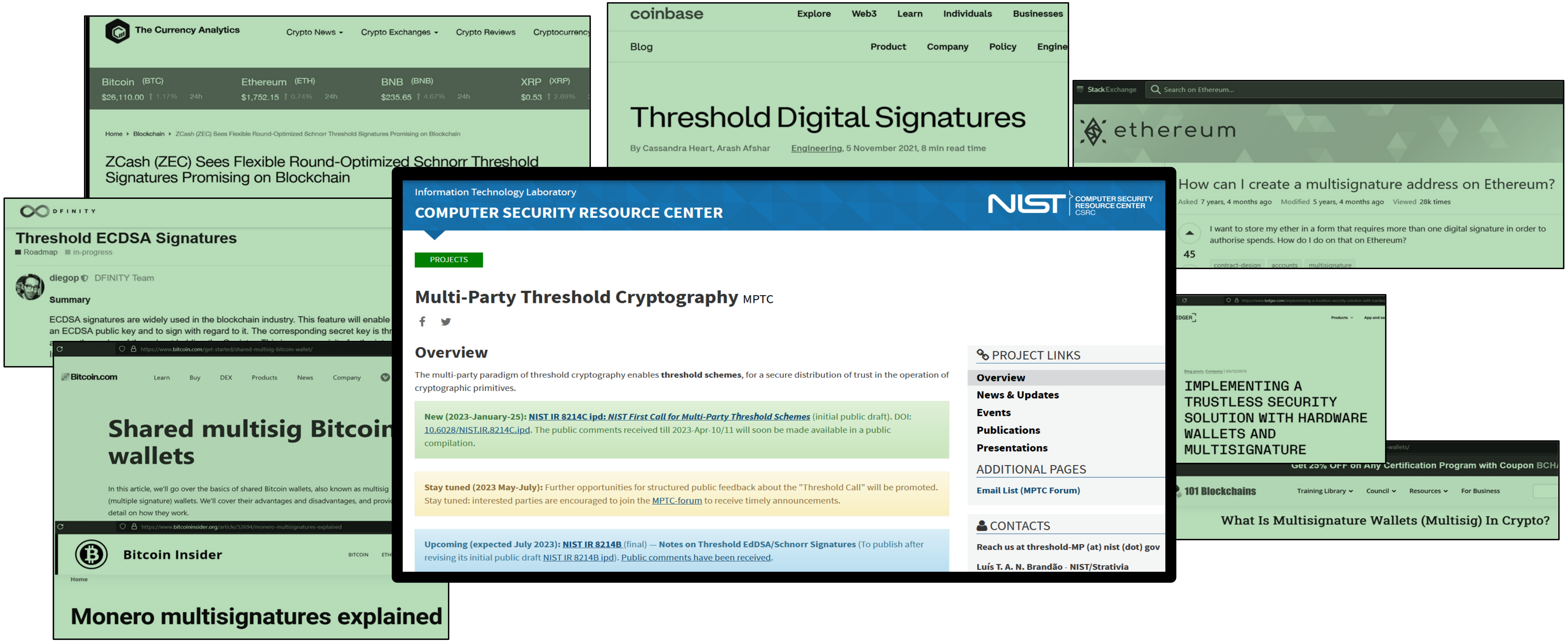
Example: Threshold Signatures



Example: 2-out-of-3 threshold sig

- Used in many blockchains (alongside multi-signature)

- The signature cannot be forged as long as **at most one** party (or more for larger sets of signers) is corrupt.



The Currency Analytics

Crypto News ▾ Crypto Exchanges ▾ Crypto Reviews Cryptocurrenc

Bitcoin (BTC) $26,110.00 ↑ 1.17% 24h

Ethereum (ETH) $1,752.15 ↑ 0.74% 24h

BNB (BNB) $235.65 ↑ 4.67% 24h

XRP (XRP) $0.53 ↑ 2.69%

Home ▸ Blockchain ▸ ZCash (ZEC) Sees Flexible Round-Optimized Schnorr Threshold Signatures Promising on Blockchain

ZCash (ZEC) Sees Flexible Round-Optimized Schnorr Threshold Signatures Promising on Blockchain

coinbase

Explore Web3 Learn Individuals Businesses

Blog

Product Company Policy Engine

Threshold Digital Signatures

By Cassandra Heart, Arash Afshar Engineering, 5 November 2021, 8 min read time

StackExchange Search on Ethereum...

ethereum

How can I create a multisignature address on Ethereum?

Asked 7 years, 4 months ago Modified 5 years, 4 months ago Viewed 28k times

45

I want to store my ether in a form that requires more than one digital signature in order to authorise spends. How do I do that on Ethereum?

contract-design accounts multisignature

DFINITY

Threshold ECDSA Signatures

■ Roadmap ■ in-progress

diegop DFINITY Team

Summary

ECDSA signatures are widely used in the blockchain industry. This feature will enable an ECDSA public key and to sign with regard to it. The corresponding secret key is thr

https://www.bitcoin.com/get-started/shared-multisig-bitcoin-wallet/

Bitcoin.com Learn Buy DEX Products News Company

Shared multisig Bitcoin wallets

In this article, we'll go over the basics of shared Bitcoin wallets, also known as multisig (multiple signature) wallets. We'll cover their advantages and disadvantages, and provi detail on how they work.

https://www.bitcoininsider.org/article/32694/monero-multisignatures-explained

Bitcoin Insider BITCOIN ETH

Home

Monero multisignatures explained

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PROJECTS

Multi-Party Threshold Cryptography MPTC

Overview

The multi-party paradigm of threshold cryptography enables **threshold schemes**, for a secure distribution of trust in the operation of cryptographic primitives.

New (2023-January-25): NIST IR 8214C ipd: *NIST First Call for Multi-Party Threshold Schemes* (initial public draft). DOI: 10.6028/NIST.IR.8214C.ipd. The public comments received till 2023-Apr-10/11 will soon be made available in a public compilation.

Stay tuned (2023 May-July): Further opportunities for structured public feedback about the "Threshold Call" will be promoted. Stay tuned: interested parties are encouraged to join the MPTC-forum to receive timely announcements.

Upcoming (expected July 2023): NIST IR 8214B (final) — Notes on Threshold EdDSA/Schnorr Signatures (To publish after revising its initial public draft NIST IR 8214B ipd). Public comments have been received.

PROJECT LINKS

Overview

News & Updates

Events

Publications

Presentations

ADDITIONAL PAGES

Email List (MPTC Forum)

CONTACTS

Reach us at threshold-MP (at) nist (dot) gov

Luís T. A. N. Brandão - NIST/Strativia

https://www.ledger.com/implementing-a-trustless-security-solution-with-hardwa

EDGER Products App and se

Blog posts, Company | 05/12/2015

IMPLEMENTING A TRUSTLESS SECURITY SOLUTION WITH HARDWARE WALLETS AND MULTISIGNATURE

-wallets/

Get 25% OFF on Any Certification Program with Coupon BCH

101 Blockchains Training Library ▾ Council ▾ Resources ▾ For Business

What Is Multisignature Wallets (Multisig) In Crypto?

Standardization?

What is a standardization process?

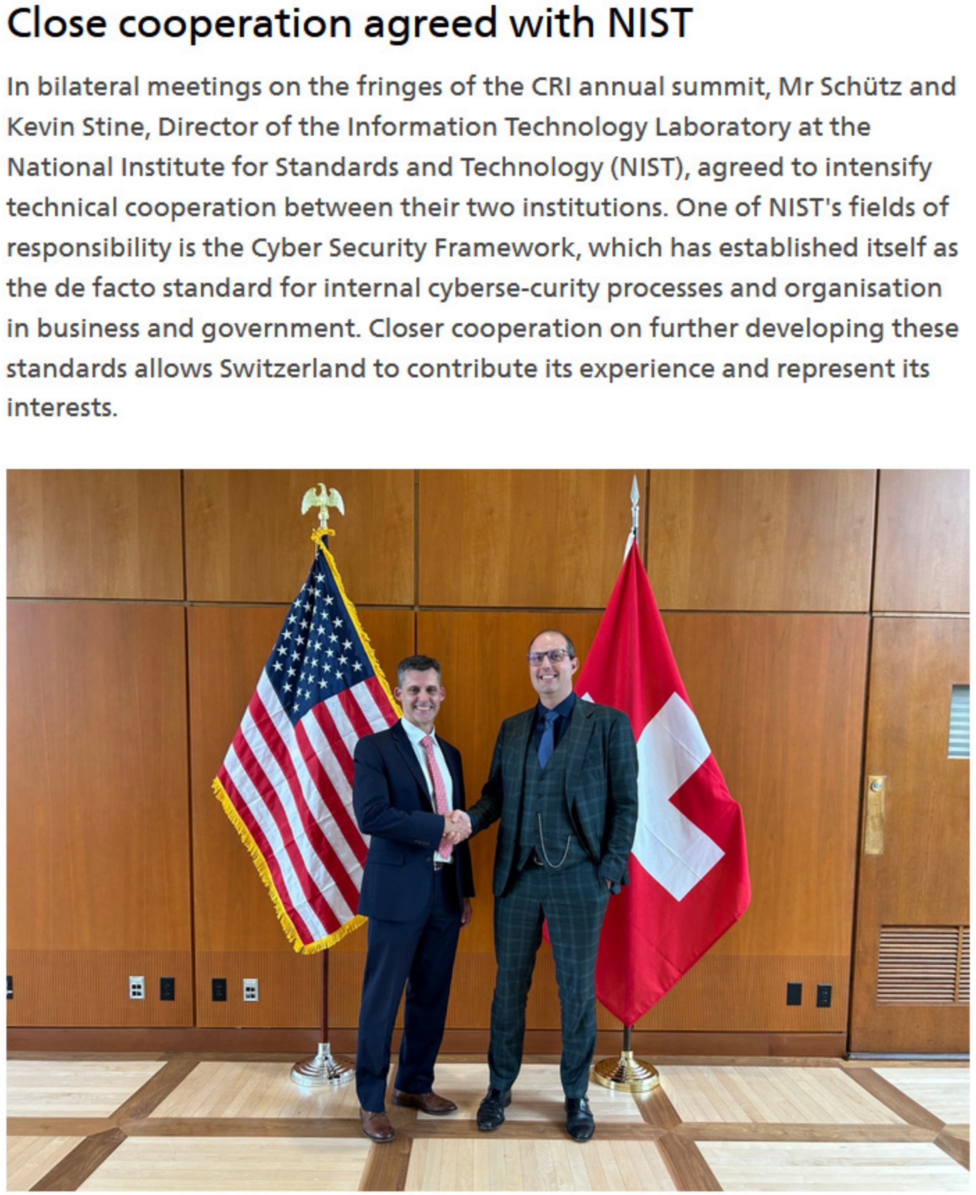
- Essentially elections for secure schemes
- Done by multiple entities (ETSI, NIST, FIPS, ISO)
- Mediate between stakeholders (who would like to use these protocols in practice) and experts
- Often public and open to everyone!

Why do we care about what NIST says?

- NIST is the standardization body of the US
- It “certifies” algorithms that are ready/safe to adopt IRL
- Its actions are often copied by other standardization bodies (e.g., ETSI, the European standardization body)
- The process is open to external comments (from both security people and stakeholders)

- We can influence it ☺

Side Quest: standardization in CH?



Close cooperation agreed with NIST

In bilateral meetings on the fringes of the CRI annual summit, Mr Schütz and Kevin Stine, Director of the Information Technology Laboratory at the National Institute for Standards and Technology (NIST), agreed to intensify technical cooperation between their two institutions. One of NIST's fields of responsibility is the Cyber Security Framework, which has established itself as the de facto standard for internal cyberse-curity processes and organisation in business and government. Closer cooperation on further developing these standards allows Switzerland to contribute its experience and represent its interests.

SNV

Die Welt braucht Normen.

Swiss Association for Standardization
SNV - Schweizerische Normen-Vereinigung

- Established in 1919 as non-profit organization under private law.
- Founding member of ISO and CEN.
- < 650 members from industry and services, associations and institutions, public companies and administrative authorities.

https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2024/cri-summit-24.html

How can anyone participate

- Google group is open for everyone to join!

  https://csrc.nist.gov/Projects/threshold-cryptography/email-list

- Workshops are free to attend online (at least for now)

- Why do you care:
  If *cryptanalyst/hacker*: try to break our stuff!
  If *cryptographer*: time to submit your candidate MPC protocol!
  Else: now you know more about standardization!

How does standardization happen?

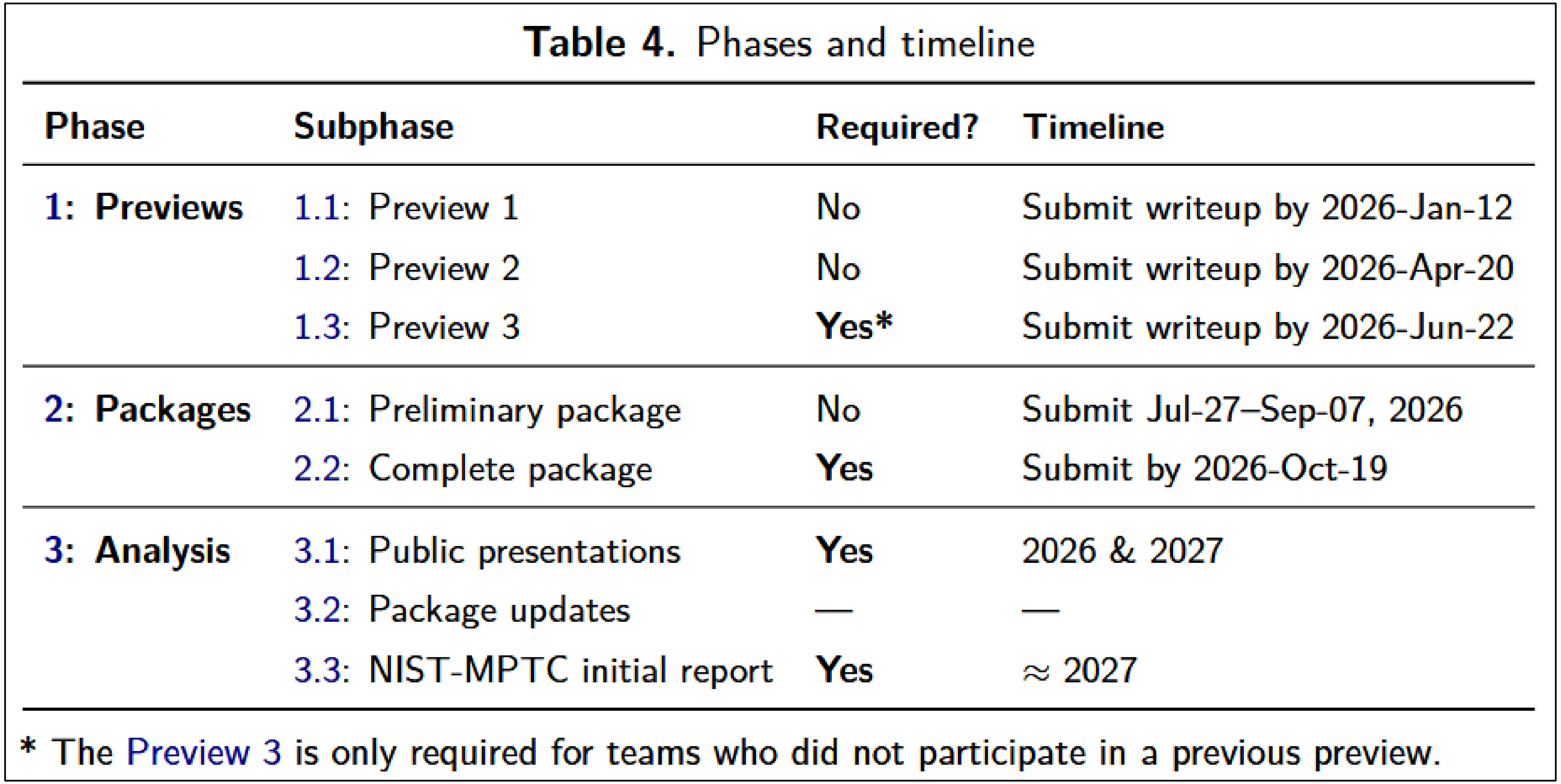


Table 4. Phases and timeline

Phase	Subphase	Required?	Timeline
1: Previews	1.1: Preview 1	No	Submit writeup by 2026-Jan-12
	1.2: Preview 2	No	Submit writeup by 2026-Apr-20
	1.3: Preview 3	**Yes***	Submit writeup by 2026-Jun-22
2: Packages	2.1: Preliminary package	No	Submit Jul-27–Sep-07, 2026
	2.2: Complete package	**Yes**	Submit by 2026-Oct-19
3: Analysis	3.1: Public presentations	**Yes**	2026 & 2027
	3.2: Package updates	—	—
	3.3: NIST-MPTC initial report	**Yes**	≈ 2027

* The Preview 3 is only required for teams who did not participate in a previous preview.

https://nvlpubs.nist.gov/nistpubs/ir/2026/NIST.IR.8214C.pdf

Overview of the first previews (1)

Type	Scheme
Sign	**5 group-based ThSig:** Gargos (Threshold Schnorr), Classic Schnorr (Threshold Schnorr), FROST (Threshold Schnorr), RedETA signatures (Threshold ECDLP-based Signatures), tBLS (Threshold BLS)
	4 threshold ECDSA: TECLA (2-party Threshold ECDSA), THE-CLASH (n-party Threshold ECDSA), BAM (2-party ECDSA), CCGMP (n-party ECDSA) and gadgets
	8(+2) PQ thSig: Haystack (Threshold HBS), Hermine (Threshold Sign) [Lattice-based], LEAST (Threshold Sign) [from code-based group-actions], Macaw (Threshold Signature) (from Isogeny-based Group Actions), Mithril (Threshold ML-DSA), Quorus (Threshold ML-DSA), Tanuki (Threshold Lattice-based Signature), Threshold UOV+MAYO Signatures (Multivariate-based)

https://csrc.nist.gov/Projects/threshold-cryptography/tcall-1

Overview of the first previews (2)

Type	Scheme
PKE	**PQ Threshold PKE:** Amber (Threshold Lattice-based KEM), Kea (Threhold PKE) (from Isogeny-based Group Actions),
	(threshold) FHE: FHE (RLWE-based) and Threshold FHE, TFHE (Torus), Nexus (Threshold FHE)
Other	**Generic MPC:** Maestro (T-AES), SHArp (T-SHA), MACnifico (T-MAC) and gadgets (inc one-hot vectors), MiniMPC (Threshold AES+SHA+MAC) and gadgets (inc. OT and garbling), SplitKey (Server-assisted threshold signatures and PKE)
	2 DKG: PiVer (Verifiable Secret Sharing), Kakapo (SKG) (from Isogeny-based Group Actions)
	3 Distributed ZK: VOLEith-based ZKPoK, SmallWood (hash-based ZKPoK), ZHEnith (ZKP)

https://csrc.nist.gov/Projects/threshold-cryptography/tcall-1

Our submission: Tanuki

Cecilia Boschini, Thomas Espitau, Aaron Kaiser, Shuichi Katsumata, Darya Kaviani, Russell W.F. Lai, Giulio Malavolta, Thomas Prest, Peter Schwabe, Akira Takahashi, Kaoru Takemure, Mehdi Tibouchi

ETH zürich · PQ SHIELD · MAX-PLANCK-INSTITUT FÜR POLYMERFORSCHUNG · AIST · Berkeley UNIVERSITY OF CALIFORNIA · Aalto University · Bocconi Università Commerciale Luigi Bocconi · Radboud University · J.P.Morgan · NTT

- PQ threshold signature,
- 2 rounds(first one preprocesseable)
- based on standard module-lattice assumptions (and the ROM)
- Assumes trusted key generation (with Shamir’s secret sharing)
- Based on Threshold Raccoon (3-rounds TS from lattices)

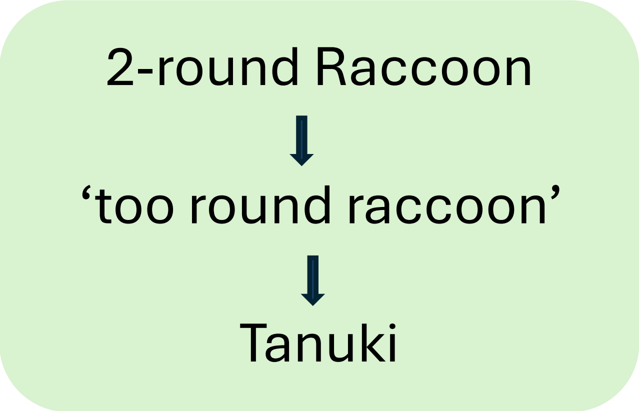
Structure of the slides by Akira Takahashi

Our submission: Tanuki

Cecilia Boschini, Thomas Espitau, Aaron Kaiser, Shuichi Katsumata, Darya Kaviani, Russell W.F. Lai, Giulio Malavolta, Thomas Prest, Peter Schwabe, Akira Takahashi, Kaoru Takemure, Mehdi Tibouchi

ETH zürich, PQ SHIELD, MAX-PLANCK-INSTITUT FÜR POLYMERFORSCHUNG, AIST, Berkeley UNIVERSITY OF CALIFORNIA, Aalto University, Bocconi Università Commerciale Luigi Bocconi, Radboud University, J.P.Morgan, NTT

- PQ threshold signature,
- 2 rounds(first one preprocesseable)
- based on standard module-lattice assumptions (and the ROM)
- Assumes trusted key generation (with Shamir's secret sharing)
- Based on Threshold Raccoon (3-rounds TS from lattices)



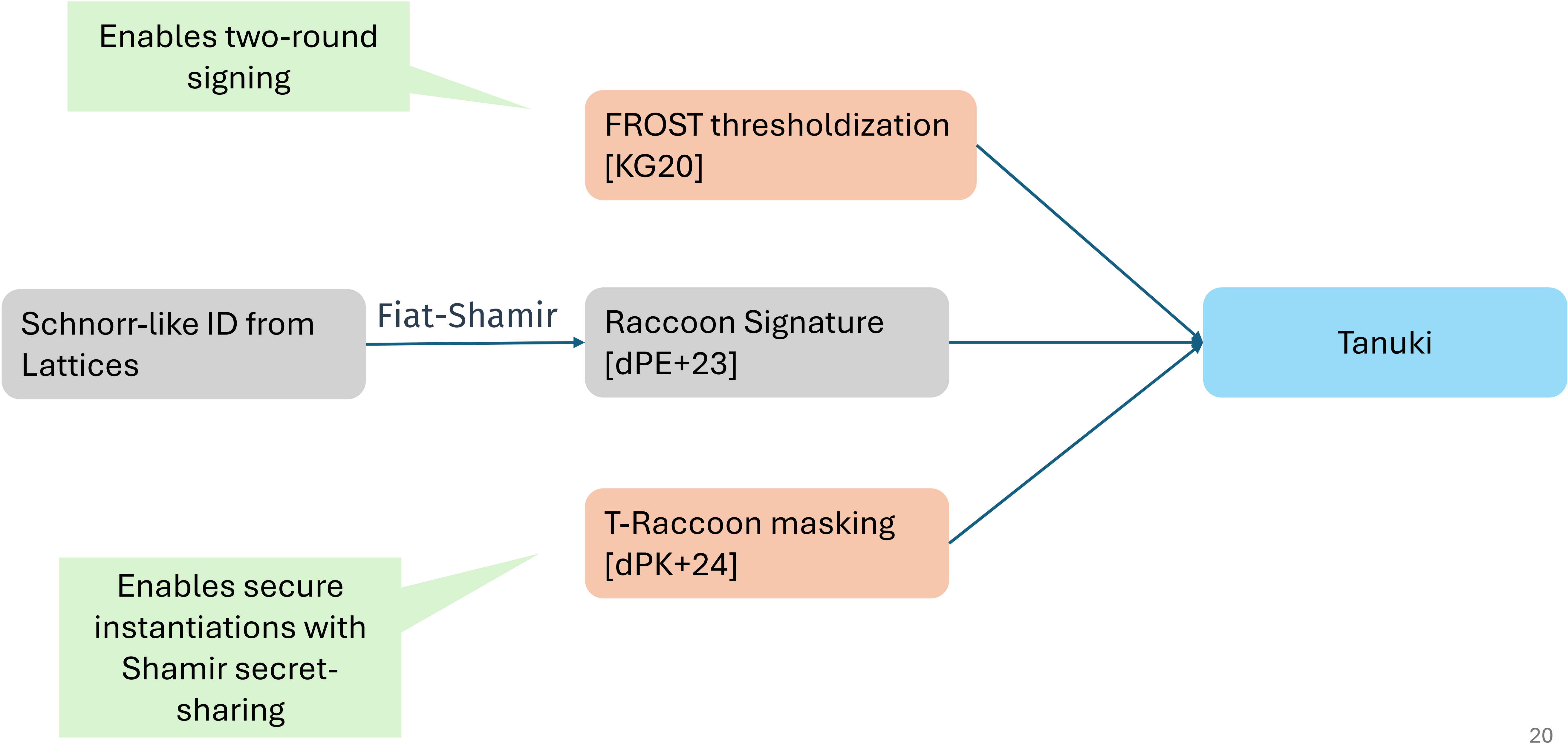
2-round Raccoon

'too round raccoon'

Tanuki

Structure of the slides by Akira Takahashi

Our submission: Tanuki



Enables two-round signing

FROST thresholdization [KG20]

Schnorr-like ID from Lattices

Fiat-Shamir

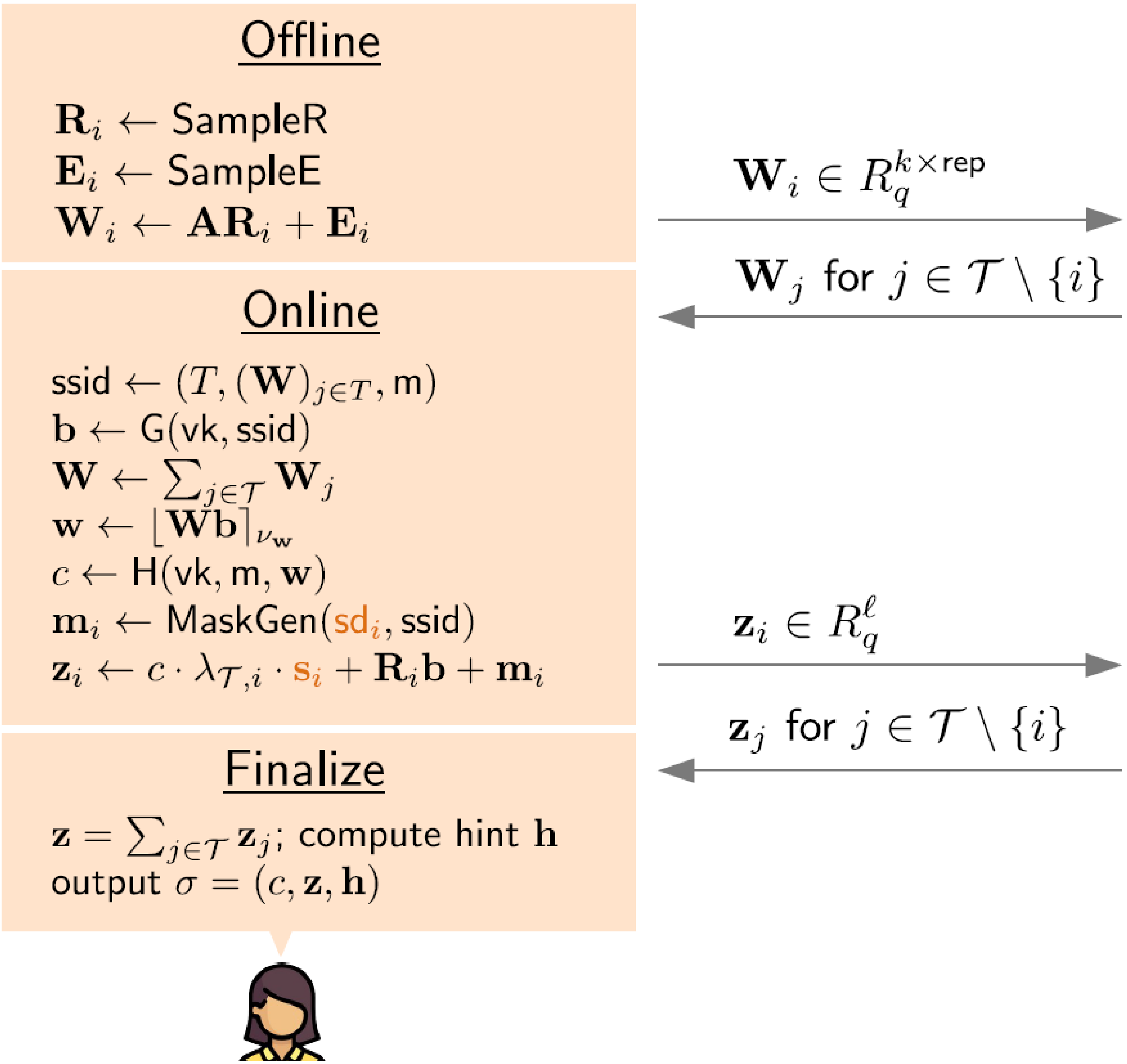
Raccoon Signature [dPE+23]

Tanuki

T-Raccoon masking [dPK+24]

Enables secure instantiations with Shamir secret-sharing

Our submission: Tanuki



Offline

$\mathbf{R}_i \leftarrow \mathsf{SampleR}$
$\mathbf{E}_i \leftarrow \mathsf{SampleE}$
$\mathbf{W}_i \leftarrow \mathbf{A}\mathbf{R}_i + \mathbf{E}_i$

$\mathbf{W}_i \in R_q^{k \times \mathsf{rep}}$ →

$\mathbf{W}_j$ for $j \in \mathcal{T} \setminus \{i\}$ ←

Online

$\mathsf{ssid} \leftarrow (\mathcal{T}, (\mathbf{W})_{j \in \mathcal{T}}, \mathsf{m})$
$\mathbf{b} \leftarrow \mathsf{G}(\mathsf{vk}, \mathsf{ssid})$
$\mathbf{W} \leftarrow \sum_{j \in \mathcal{T}} \mathbf{W}_j$
$\mathbf{w} \leftarrow \lfloor \mathbf{W}\mathbf{b} \rceil_{\nu_{\mathsf{w}}}$
$c \leftarrow \mathsf{H}(\mathsf{vk}, \mathsf{m}, \mathbf{w})$
$\mathbf{m}_i \leftarrow \mathsf{MaskGen}(\mathsf{sd}_i, \mathsf{ssid})$
$\mathbf{z}_i \leftarrow c \cdot \lambda_{\mathcal{T},i} \cdot \mathbf{s}_i + \mathbf{R}_i \mathbf{b} + \mathbf{m}_i$

$\mathbf{z}_i \in R_q^{\ell}$ →

$\mathbf{z}_j$ for $j \in \mathcal{T} \setminus \{i\}$ ←

Finalize

$\mathbf{z} = \sum_{j \in \mathcal{T}} \mathbf{z}_j$; compute hint $\mathbf{h}$
output $\sigma = (c, \mathbf{z}, \mathbf{h})$

KeyGen

$(\mathbf{s}, \mathbf{e}) \leftarrow \mathsf{SampleKey}$
$(\mathbf{s}_1, \ldots, \mathbf{s}_n) \leftarrow \mathsf{ShamirShare}(\mathbf{s})$
$\mathbf{t} \leftarrow \lfloor \mathbf{A}\mathbf{s} + \mathbf{e} \rceil_{\nu_{\mathbf{t}}}$
$(\mathsf{sd}_1, \ldots, \mathsf{sd}_n) \leftarrow \mathsf{SeedGen}$

Design Choices

1. FROST-style aggregation [KG20]
2. One-time mask for secure aggregation [dPK+24]
   - $\sum_{j \in \mathcal{T}} \mathbf{m}_j = \mathbf{0}$
   - MaskGen can be instantiated with PRF
   - Why? – $\mathbf{R}_i \mathbf{b}$ doesn't mask large $c \cdot \lambda_{\mathcal{T},i} \cdot \mathbf{s}_i$!
   - Allows standard Shamir-sharing of $\mathbf{s}$ with large Lagrange coefficients and shares

Tanuki Implementation

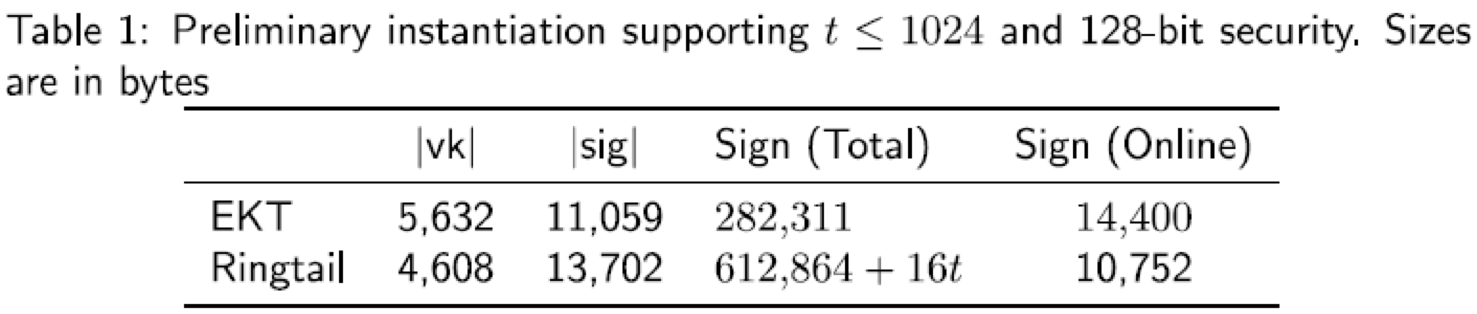


Table 1: Preliminary instantiation supporting $t \leq 1024$ and 128-bit security. Sizes are in bytes

	|vk|	|sig|	Sign (Total)	Sign (Online)
EKT	5,632	11,059	282,311	14,400
Ringtail	4,608	13,702	$612{,}864 + 16t$	10,752

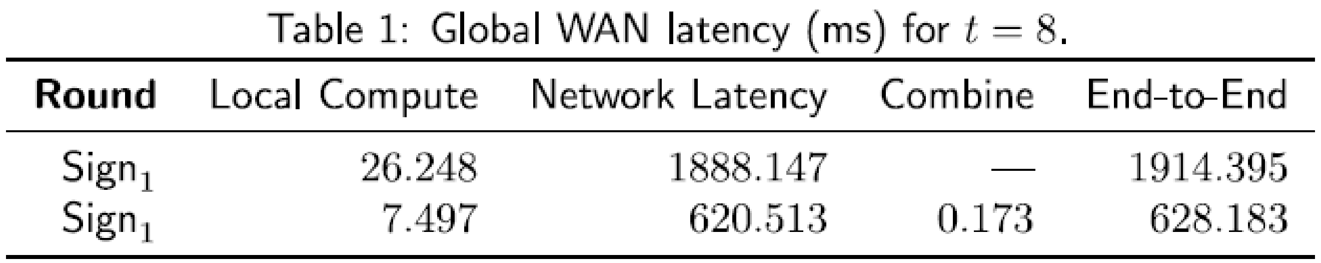
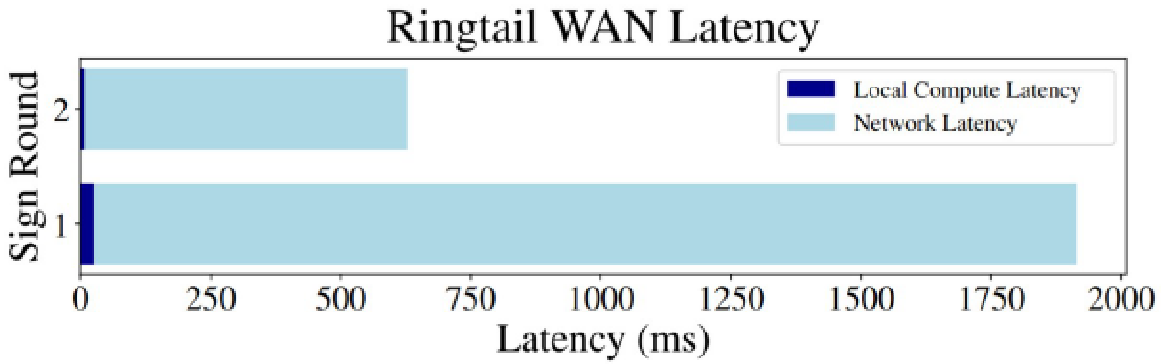


Table 1: Global WAN latency (ms) for $t = 8$.

Round	Local Compute	Network Latency	Combine	End-to-End
Sign_1	26.248	1888.147	—	1914.395
Sign_1	7.497	620.513	0.173	628.183



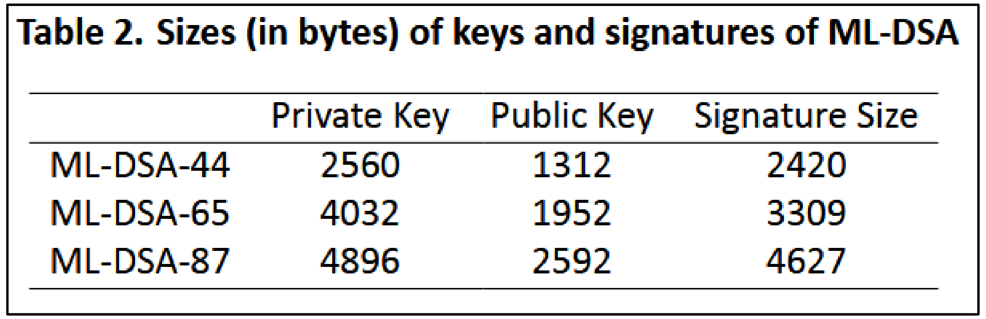


Table 2. Sizes (in bytes) of keys and signatures of ML-DSA

	Private Key	Public Key	Signature Size
ML-DSA-44	2560	1312	2420
ML-DSA-65	4032	1952	3309
ML-DSA-87	4896	2592	4627

Preliminary Experiment:

- Implemented in go with latigo library
- WAN experiments with AWS c5.4xlarge
- 8 regions across 5 continents
- Average RTT: 170.11 ms
- Average network throughput: 183.23 Mbps

Future Directions:

- Reimplement core module in Rust
- Update parameters
- More network experiments

https://github.com/daryakaviani/ringtail

Thank you!

https://csrc.nist.gov/projects/threshold-cryptography
https://eprint.iacr.org/2024/496.pdf
https://eprint.iacr.org/2024/1113.pdf