



Distributed Schnorr

Fireblocks-3MI

Speaker: Nikolaos Makriyannis

NIST MPTC Workshop
26/01/2026

Contents

1 Meet the team

2 Schnorr Signatures for Digital Assets

3 The “Classic” Schnorr Protocol

4 Opening the floor to discussion

Meet the team



Fireblocks - 3MI

Meet the team

1. Fireblocks:
 - a. Michael Adjedj (Cryptography Engineer - Fireblocks)
 - b. Michael Gutkin (VP Research - Fireblocks)
 - c. Nikolaos Makriyannis (Research Scientist- Fireblocks)
2. 3MI Labs:
 - a. Tomer Ashur (CEO/Chief Scientist - 3MI Labs)
 - b. Cyprien de Saint Guilhem (Head of R&D - 3MI Labs)
 - c. Amit Singh Bhati (Research Scientist - 3MI Labs)
3. External Consultant:
 - a. Geoffroy Couteau (CNRS Research Scientist)



Fireblocks - 3MI

Meet the team

1. 100+ research papers
2. Decades of combined industry experience
3. Contributions to standards (NIST, ISO)



Fireblocks

Global platform to issue, custody, move and manage any digital asset and currencies



2,400+
Institutional Customers

110
Countries Supported

1bn+
In Market Reach

830+
Employees

\$1Bn+
In funding

FUNDED BY INDUSTRY LEADERS



Ecosystem and Network, touching 1B+ Consumers

Banks & Custodians

- Custody
- Asset tokenization
- Treasury operations
- Stablecoin issuance



Asset Managers

- Fund tokenization
- Custody
- Distribution



Fintechs and Neobanks

- Crypto trading
- Yield products
- Payments
- Treasury operations



Payment Service Providers

- Stablecoin payments
- Digital accounts
- Treasury operations
- Loyalty programs



Market Makers & OTCs

- Post-trade and settlement
- Treasury operations
- Collateral management



Exchanges

- Custody
- Treasury operations
- Collateral management



Official Institutions

- CBDC trials
- Permissioned DeFi
- On Chain FX
- Programmable money



Enterprises

- Web3 experiences
- Loyalty programs
- Stablecoin payments





\$10T+

transactions secured

150

Blockchains supported

\$100b

Daily AUC

550m+

Wallets created



Wallets-as-a-Service



Treasury Management



Tokenization Engine



Payments Engine



What does it all boil down to

A look under the hood



What does it all boil down to

A look under the hood

ECDSA & Schnorr

1. Managing EC-signatures end-to-end

What does it all boil down to

A look under the hood

ECDSA & Schnorr

1. Managing EC-signatures end-to-end
2. Key management gives rise to operational/security/legal challenges
 - a. Where does the key material reside?
 - b. Is there a single point of failure?

What does it all boil down to

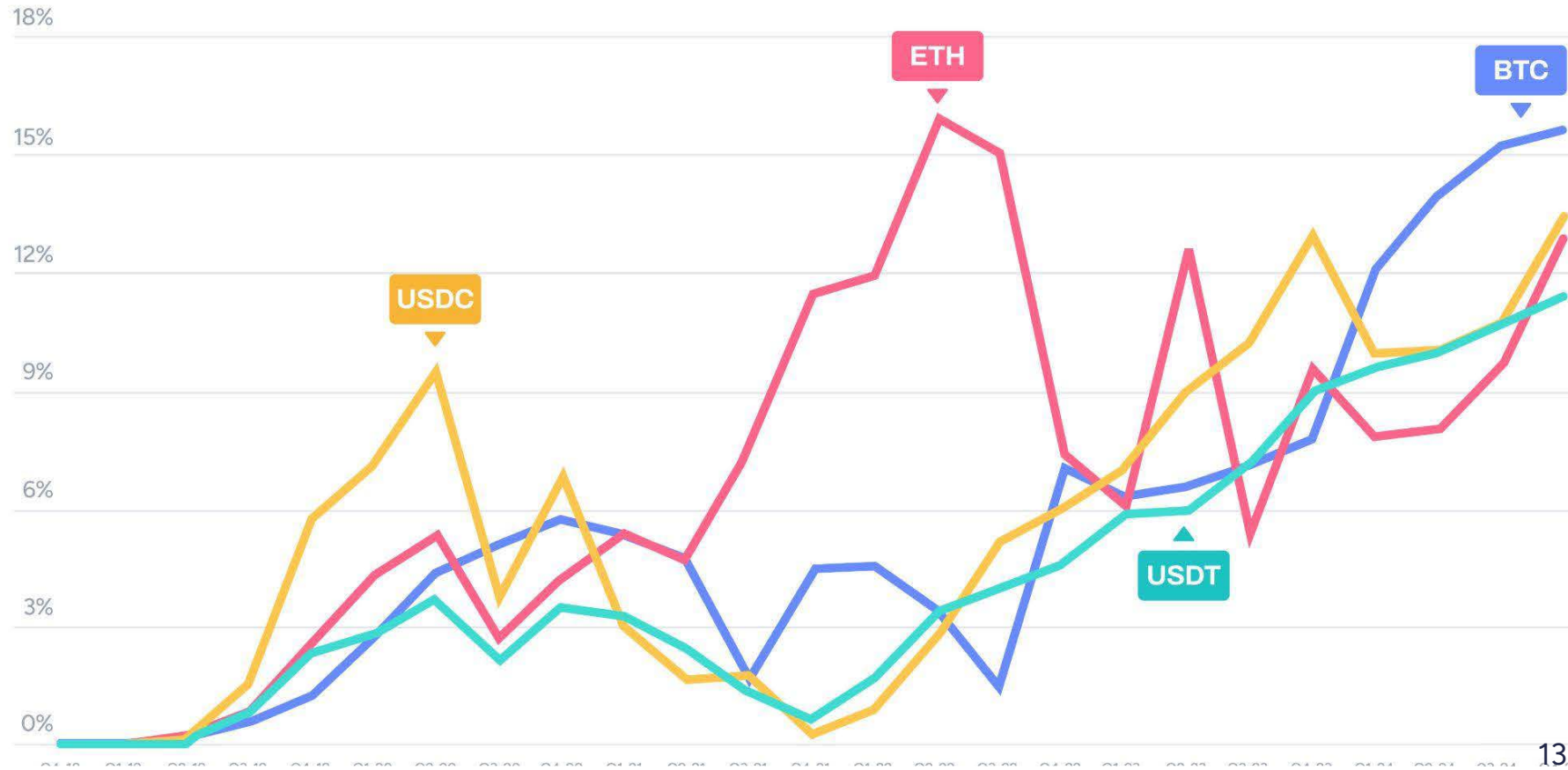
A look under the hood

ECDSA & Schnorr

1. Managing EC-signatures end-to-end
2. Key management gives rise to operational/security/legal challenges
 - a. Where does the key material reside?
 - b. Is there a single point of failure?
3. Fireblocks solves these challenges using MPC.
 - a. Key material is generated via DKG
 - b. Signatures are generated via distributed protocol



Fireblocks processes 10-15% of main blockchain transactions



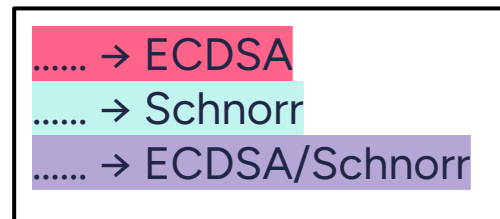
Fireblocks processes 10-15% of main blockchain transactions



Threshold signatures are a huge part of the digital assets ecosystem

Research Contributions

1. UC Non-Interactive, Proactive, Threshold ECDSA
 - *Canetti, M & Peled (eprint)*
2. UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts
 - *Canetti, Gennaro, Goldfeder, M & Peled (CCS 2021)*
3. Highly Efficient OT-Based Multiplication Protocols
 - *Haitner, M, Ranellucci, Tsfadia (Eurocrypt 2022)*
4. On the Classic Protocol for MPC Schnorr Signatures
 - *M (eprint)*
5. Efficient Asymmetric Threshold ECDSA for MPC-based Cold Storage
 - *Blokh, M, Peled (eprint)*
6. Practical Key-Extraction Attacks in Leading MPC Wallets
 - *M, Yomtov, Galansky (CCS 2024)*
7. Two-Round 2PC ECDSA at the Cost of 1 OLE
 - *Adjedj, Blokh, Couteau, Galansky, Joux, M (eprint)*
8. From OT to OLE with Subquadratic Communication
 - *Doerner, Haitner, Ishai, M (CCS 2025)*
9. Tight Bounds on Uniform-Challenge Black-Box Reductions from Sigma Protocols
 - *Haitner, M (eprint)*
10. Integer Commitments, Old and New Tools
 - *Haitner, Lindell, M (eprint)*
11. Stateless 2PC Signatures for Internet-Scale Authentication and Authorization
 - *Adjedj, Couteau, Galansky, M, Yomtov (AsiaCCS 2026)*



Research Contributions

1. UC Non-Interactive, Proactive, Threshold ECDSA
 - *Canetti, M & Peled (eprint)*
2. UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts
 - *Canetti, Gennaro, Goldfeder, M & Peled (CCS 2021)*
3. Highly Efficient OT-Based Multiplication Protocols
 - *Haitner, M, Ranellucci, Tsfadia (Eurocrypt 2022)*
4. On the Classic Protocol for MPC Schnorr Signatures
 - *M (eprint)*
5. Efficient Asymmetric Threshold ECDSA for MPC-based Cold Storage
 - *Blokh, M, Peled (eprint)*
6. Practical Key-Extraction Attacks in Leading MPC Wallets
 - *M, Yomtov, Galansky (CCS 2024)*
7. Two-Round 2PC ECDSA at the Cost of 1 OLE
 - *Adjedj, Blokh, Couteau, Galansky, Joux, M (eprint)*
8. From OT to OLE with Subquadratic Communication
 - *Doerner, Haitner, Ishai, M (CCS 2025)*
9. Tight Bounds on Uniform-Challenge Black-Box Reductions from Sigma Protocols
 - *Haitner, M (eprint)*
10. Integer Commitments, Old and New Tools
 - *Haitner, Lindell, M (eprint)*
11. Stateless 2PC Signatures for Internet-Scale Authentication and Authorization
 - *Adjedj, Couteau, Galansky, M, Yomtov (AsiaCCS 2026)*

Submission Packages
for NIST-MPTC



Schnorr Signatures for Digital Assets



Schnorr Signatures for Digital Assets

Background

1. EC-based signatures schemes dominate the ecosystem



Schnorr Signatures for Digital Assets

Background

1. EC-based signatures schemes dominate the ecosystem
2. Schnorr signatures seen as the gold standard by “technologists”
 - a. Efficiency and Simplicity
 - b. Solid theoretical foundation
 - c. Aggregation and threshold-friendliness
 - d. ZK-friendliness



Schnorr Signatures for Digital Assets

Background

1. EC-based signatures schemes dominate the ecosystem
2. Schnorr signatures seen as the gold standard by “technologists”
 - a. Efficiency and Simplicity
 - b. Solid theoretical foundation
 - c. Aggregation and threshold-friendliness
 - d. ZK-friendliness
3. Widespread adoption especially among “high-throughput” blockchains (Solana, Sui, ...)
 - a. Also supported by Bitcoin via “Taproot” upgrade



Schnorr Signatures

Definition

1. The public key is a random element X in the EC subgroup
 - a. The secret key is x such that $x \cdot G = X$
2. Signatures have the form (R, s)
 - a. $R = k \cdot G$ is a random point in the EC subgroup
 - b. $s = k + e \cdot x$

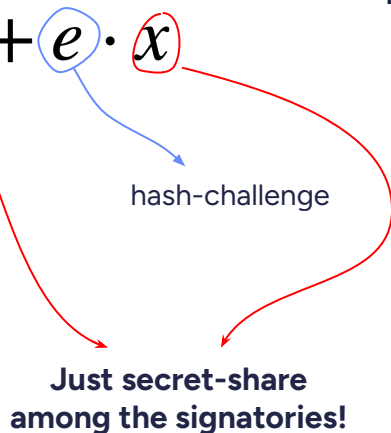
hash-challenge



Schnorr Signatures

Definition

1. The public key is a random element X in the EC subgroup
 - a. The secret key is x such that $x \cdot G = X$
2. Signatures have the form (R, s)
 - a. $R = k \cdot G$ is a random point in the EC subgroup
 - b. $s = k + e \cdot x$



The "Classic" Schnorr Protocol



Threshold Signature Schemes

Assessment criteria



Threshold Signature Schemes

Assessment criteria

1. Performance
 - a. Communication, computation, rounds



Threshold Signature Schemes

Assessment criteria

1. Performance
 - a. Communication, computation, rounds
2. Theoretical considerations
 - a. Security assumptions and models
 - b. Quality of the reductions



Threshold Signature Schemes

Assessment criteria

1. Performance
 - a. Communication, computation, rounds
2. Theoretical considerations
 - a. Security assumptions and models
 - b. Quality of the reductions
3. Conservative design
 - a. Algorithmic design simplicity
 - b. Security analysis simplicity



"Classic" Schnorr

Protocol Description

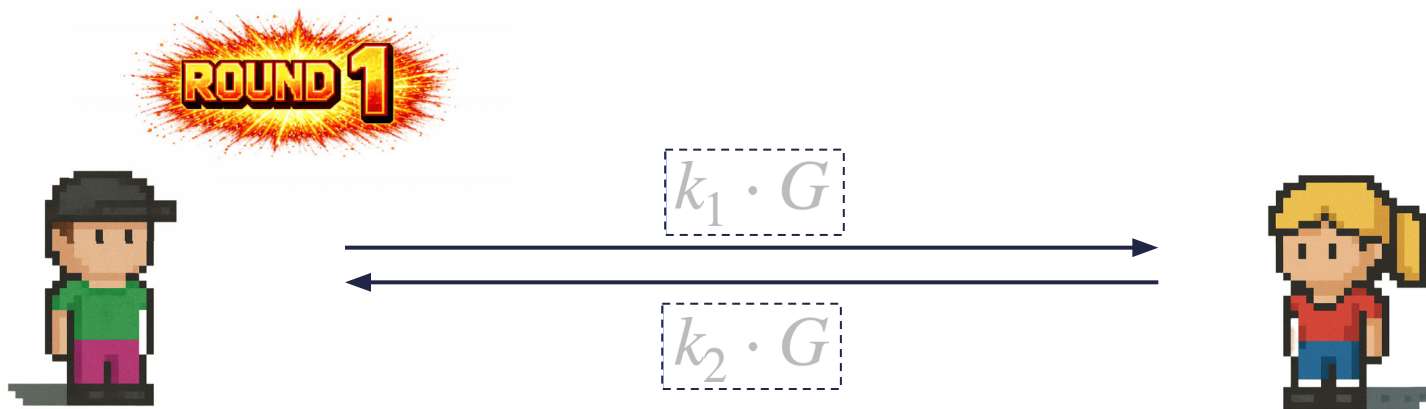
1. Sample a random group element via coin-toss (2 rounds)
2. Compute and release the signature share (1 round)



"Classic" Schnorr

Protocol Description

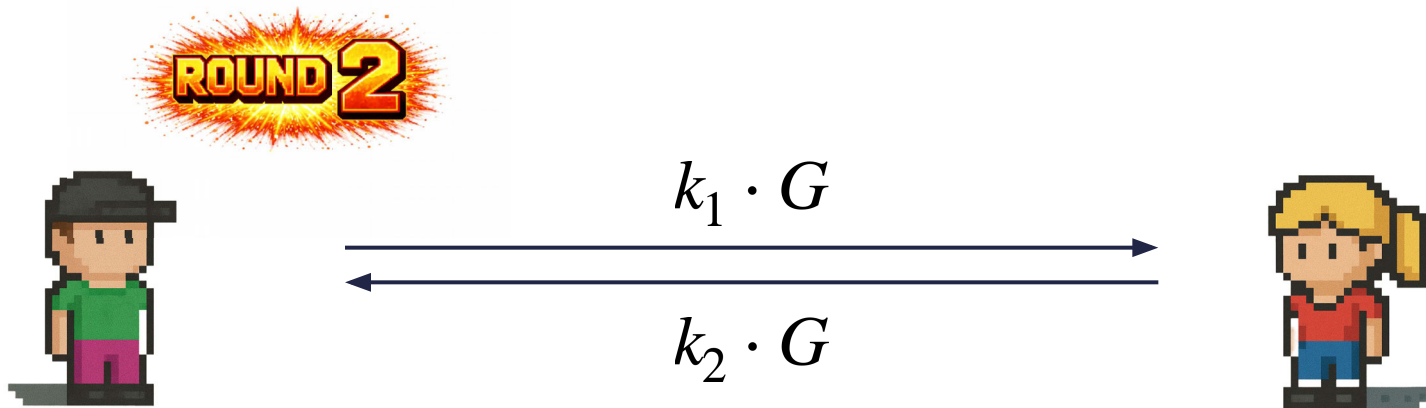
1. Sample a random group element via coin-toss (2 rounds)
2. Compute and release the signature share (1 round)



"Classic" Schnorr

Protocol Description

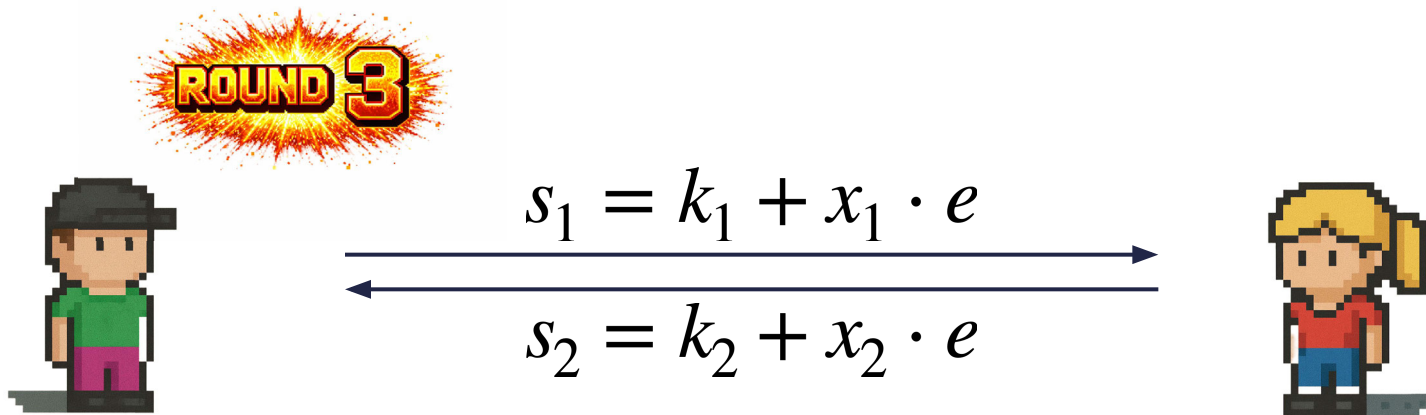
1. Sample a random group element via coin-toss (2 rounds)
2. Compute and release the signature share (1 round)



"Classic" Schnorr

Protocol Description

1. Sample a random group element via coin-toss (2 rounds)
2. Compute and release the signature share (1 round)



"Classic" Schnorr

Performance

1. Sample a random group element via coin-toss (2 rounds)
2. Compute and release the signature share (1 round)



Computation	1 EC multiplication (exponentiation)
Communication	64B + commitment
Rounds	3



"Classic" Schnorr

Features

1. Essentially the simplest design for a *secure* protocol
2. No ZK(PoK) → zero overhead
3. Natively supports identifiable abort
4. Tight security reduction vanilla Schnorr Signatures
5. Adaptive security comes for free*



"Classic" Schnorr

Security Analysis

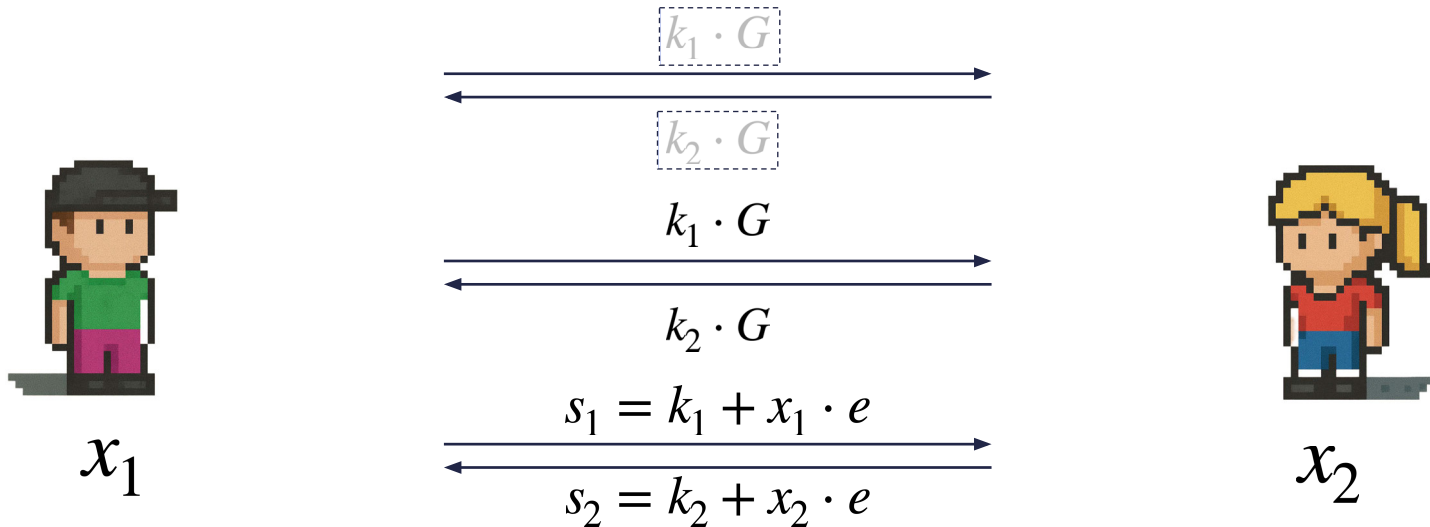
1. Within the provable security framework, each property (unforgeability, id-abort, adaptive security) can be proved to be satisfied via its own game-based security definition.
2. Security guarantees can be "lifted" into UC theorem showing that the protocol realizes a threshold signatures functionality.



"Classic" Schnorr

How does the simulation work?

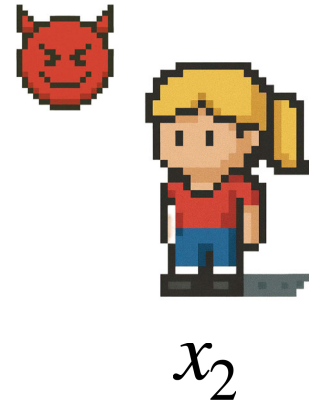
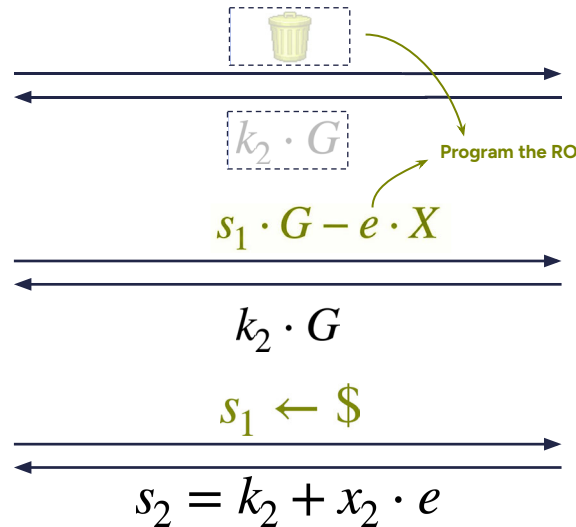
1. Typically the simulator extract's the attacker's secrets to simulate the honest parties' messages
2. There are no ZK(PoK)s in the protocol to do that!?



"Classic" Schnorr

How does the simulation work?

1. Typically the simulator extract's the attacker's secrets to simulate the honest parties' messages
2. There are no ZK(PoK)s in the protocol to do that!?



Opening the floor to discussion



Key takeaways and next steps

1. “Classic Schnorr”
 - a. Highly efficient
 - b. Secure
 - c. Simple
2. Let’s make NIST’s life easier
 - a. Avoid overlapping submissions (we’re open to collab).
 - b. Prioritize simple and widely used protocols.

