Threshold Ring Signatures: New Security Definitions and Post-Quantum Security

Abida Haque, Alessandra Scafuro

North Carolina State University

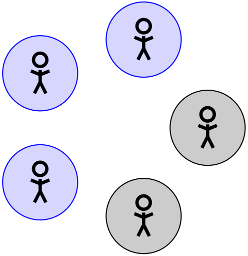
May 25, 2020

Problem Description

Threshold Ring Signature

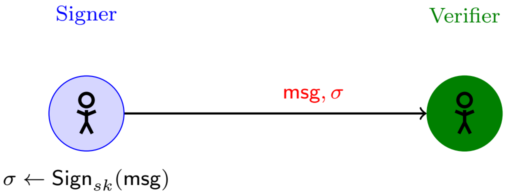
Main Definitions

Threshold ring signatures: t distinct parties anonymously sign on behalf of a ring of N public keys. The identity of the signers remains private (to any non-signers).



Threshold Ring Signature

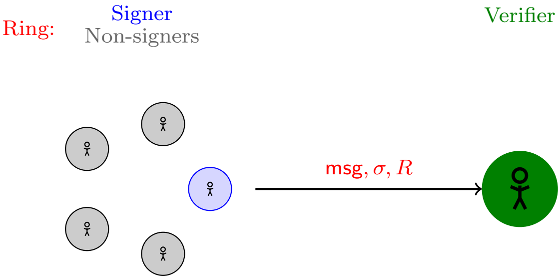
Signature



- unforgeability

Threshold Ring Signature

Ring Signature

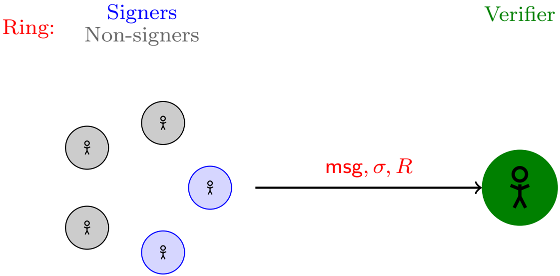


$\sigma \leftarrow \mathsf{Sign}_{sk}(\mathsf{msg}; R)$

- unforgeability
- anonymity

Threshold Ring Signature

Ring Signature

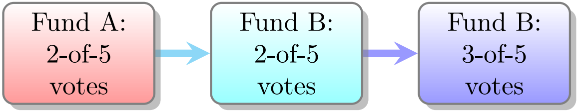


$$\sigma \leftarrow \mathsf{Sign}_{sk^i, sk^j}(\mathsf{msg}; R)$$

- unforgeability
- anonymity
- threshold

Motivation

- Increased tolerance to misbehavior of users
- Suits decentralized settings
- Settings where you need a quorum.



- an ad-hoc "voting" mechanism for community projects posted on the blockchain
- Funds: $$$

Current State of the Art

State of the Art

- Passive Security Definitions

- Post-Quantum Insecure
  1. Hardness Assumptions
  2. Techniques

Threshold Ring Signature Setting

- Ad-hoc settings where the users can generate their keys independently, and join or leave the system at any time.
- Users could join the system with dishonestly generated keys.

Passive Adversaries

- Only passive adversaries.
- Adversaries can only obtain honestly generated keys.
- Sometimes cannot even choose to add more (honest) keys (e.g., Bettaieb and Schrek (2013); Petzoldt et al. (2013)),
- Adversaries cannot corrupt parties (e.g. Okamoto et al. (2018); Petzoldt et al. (2013); Bettaieb and Schrek (2013)).
- Bender et al. (2006) observe that the above doesn't reflect the open settings of ring signatures.

State of the Art

- Passive Security Definitions
  1. passive adversaries
  2. no corruption
  3. no adding of new honest keys

- Post-Quantum Insecure
  1. Hardness Assumptions
  2. Techniques

Post-Quantum Hardness Assumptions

- Discrete log, factoring hardness assumptions are not secure against an attack from a quantum computer (Shor (1994)).
- Some constructions Melchor et al. (2011); Bettaieb and Schrek (2013); Cayrel et al. (2010); Petzoldt et al. (2013) use post-quantum secure hardness problems such as lattices or learning-with-errors.

State of the Art

- Passive Security Definitions
  1. passive adversaries
  2. no corruption
  3. no adding of new honest keys

- Post-Quantum Insecure
  1. Non-PQ secure problems
  2. Techniques

Proof Techniques in Post-Quantum Setting

- Transform from Fiat and Shamir (1986) common, but security may not hold in the *quantum* setting (Boneh et al. (2011); Ambainis et al. (2014)).
- Quantum rewinding is not trivial (Watrous (2009); Ambainis et al. (2014)).
- Fiat-Shamir is post-quantum secure in certain situations (Liu and Zhandry (2019); Don et al. (2019)) but may not hold in general.

Transformation

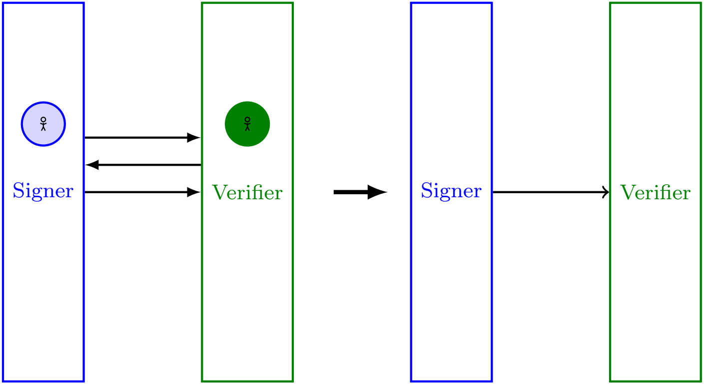


Figure: Transform an interactive protocol into a non-interactive one.

Rewinding

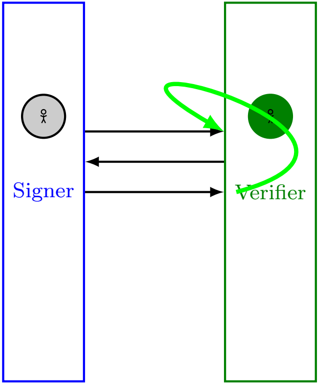
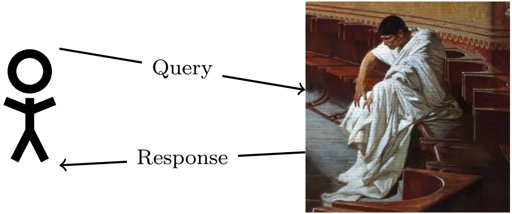


Figure: Prove scheme with rewinding. But a quantum adversary may notice!

Quantum vs Classical Access

Classical

On a single query, can only get a single response.



Quantum vs Classical Access

Quantum

Can get a *superposition* of answers.

Can define all possible outputs using only a single query. This is why we use Unruh.

State of the Art

- Passive Security Definitions
  1. passive adversaries
  2. no corruption
  3. no adding of new honest keys

- Post-Quantum Insecure
  1. Non-PQ secure problems
  2. Fiat-Shamir is not PQ-secure in general.

Our Contribution

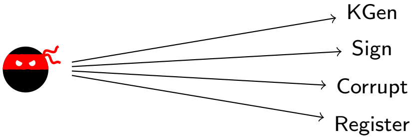
Our Contribution

1. Definitions for unforgeability and anonymity with active adversaries.
2. Post-quantum secure proof for a threshold ring signature.
   1. generalize previous approaches and provide a black-box construction from any (post-quantum) trapdoor commitment scheme.
   2. Uses Unruh Transformation to guarantee post-quantum security.

Definitions

- Make a security model by giving adversary access to oracles.
- Captures active adversaries.
- Two security notions: unforgeability and anonymity.

Anonymity and Unforgeability



Training: ask queries

Anonymity: $\mathcal{A}$ picks:

- message
- S_0, S_1 with respect to a ring R, where $|S_0| = |S_1| = t$.

$\mathcal{A}$ receives a signature from S_b ($b = 0$ or 1) and guesses b.

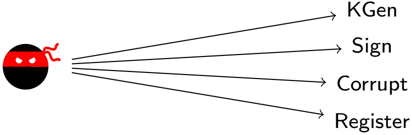
S_0, S_1 uncorrupted.

Unforgeability: $\mathcal{A}$ produces

- message
- signature
- ring

Fewer than t corrupted members in R^*.

Anonymity and Unforgeability



Training: ask queries

Anonymity: $\mathcal{A}$ picks:

- message
- S_0, S_1 with respect to a ring R, where $|S_0| = |S_1| = t$.

$\mathcal{A}$ receives a signature from S_b ($b = 0$ or 1) and guesses b.

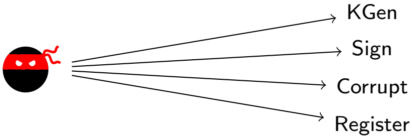
S_0, S_1 uncorrupted.

Unforgeability: $\mathcal{A}$ produces

- message
- signature
- ring

Fewer than t corrupted members in R^*.

Anonymity and Unforgeability



Training: ask queries

Anonymity: $\mathcal{A}$ picks:

- message
- S_0, S_1 with respect to a ring R, where $|S_0| = |S_1| = t$.

$\mathcal{A}$ receives a signature from S_b ($b = 0$ or 1) and guesses b.

S_0, S_1 uncorrupted.

Unforgeability: $\mathcal{A}$ produces

- message
- signature
- ring

Fewer than t corrupted members in R^*.

Oracles

- *Key Generation:* Upon query from $\mathcal{A}$, the oracle creates private-public key pair and gives the public key to $\mathcal{A}$.
- *Sign:* $\mathcal{A}$ requests a signature on message and signers w.r.t. a ring. The oracle follows the signing algorithm with the secret keys that he controls. $\mathcal{A}$ must participate in the signing procedure if there are corrupted members.
- *Corrupt:* Oracle returns requested user's secret key to $\mathcal{A}$ and updates list of corrupted users.
- *Register:* $\mathcal{A}$ provides public key to the oracle, who adds it to the ring and list of corrupted ring members.

Our Contribution

1. Definitions for unforgeability and anonymity with active adversaries.
2. Post-quantum secure proof for a threshold ring signature.
    1. generalize previous approaches and provide a black-box construction from any (post-quantum) trapdoor commitment scheme.
    2. Uses Unruh Transformation to guarantee post-quantum security.

☺

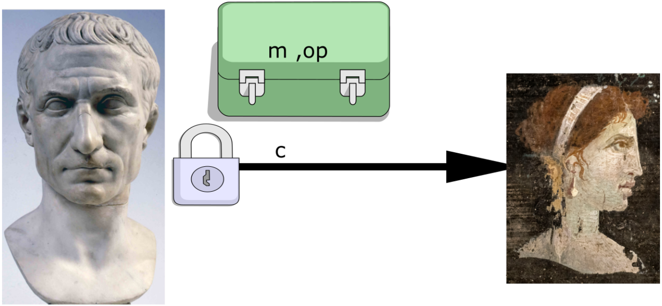
Post-Quantum Secure Problem and Technique

- Black-box use of (post-quantum) Trapdoor Commitment Scheme
- We avoid rewinding by making all outputs part of the signature (Unruh (2015)).

Our Scheme

Commitment Scheme

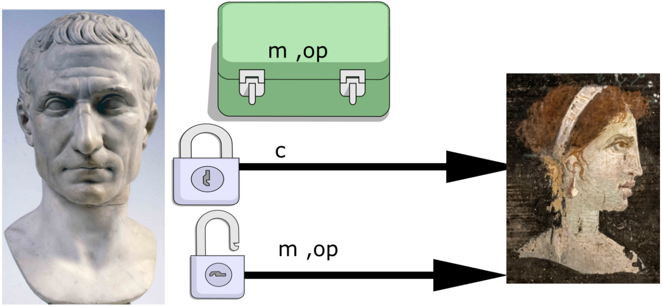
Hiding, Binding



Sender can commit to a message. Receiver cannot learn what the message is (hiding). Later sender can only open to the original message (binding).

Commitment Scheme

Hiding, Binding



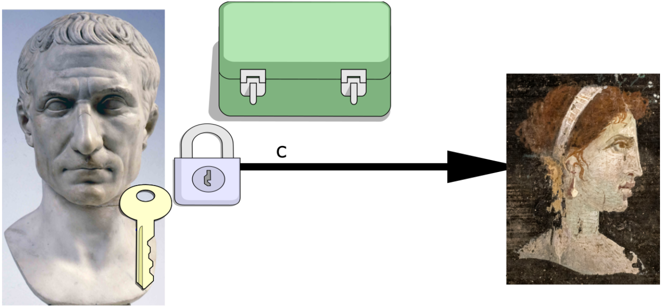
Sender can commit to a message. Receiver cannot learn what the message is (hiding). Later sender can only open to the original message (binding).

Trapdoor

Knowing a trapdoor, it's possible to 'change your mind'.

Trapdoor Commitment Scheme

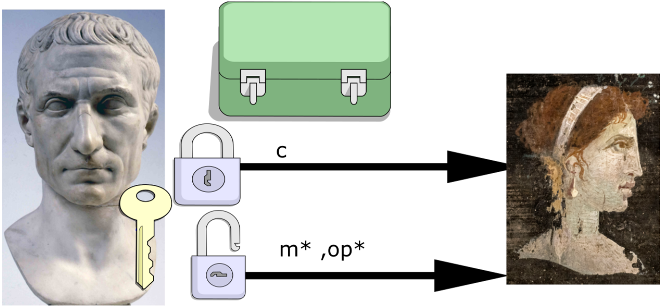
Trapdoor Indistinguishability



- With knowledge of a trapdoor t, sender can open a commitment to any message they like.
- Hiding, binding (w/o knowledge of trapdoor), and trapdoor indistinguishability.

Trapdoor Commitment Scheme

Trapdoor Indistinguishability



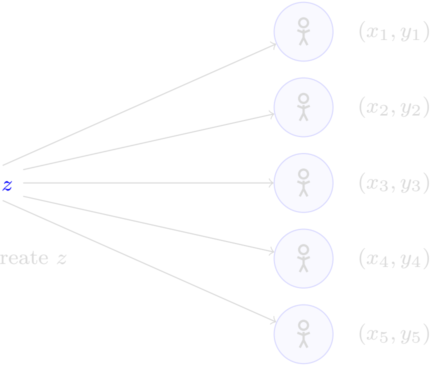
- With knowledge of a trapdoor t, sender can open a commitment to any message they like.
- Hiding, binding (w/o knowledge of trapdoor), and trapdoor indistinguishability.

Shamir Secret Sharing

Graphic

Example: Want 3-out-of-5.

Secret: z



Combine points to uniquely create z

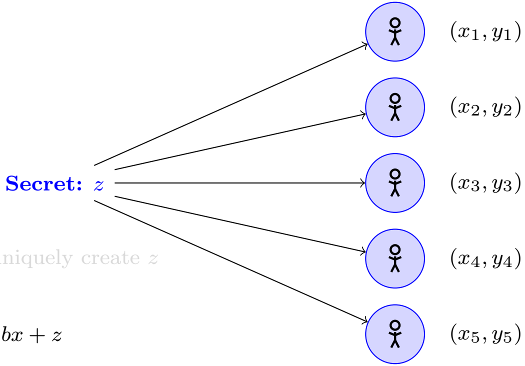
$$y = ax^2 + bx + z$$

Description

Shamir Secret Sharing

Graphic

Example: Want 3-out-of-5.



Combine points to uniquely create z

$$y = ax^2 + bx + z$$

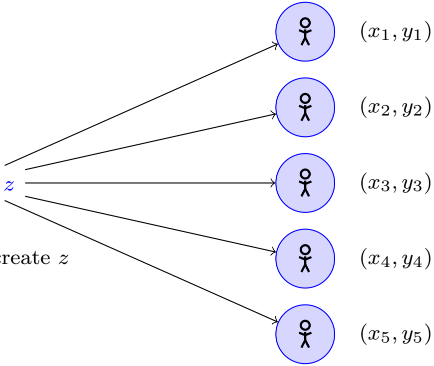
Description

Shamir Secret Sharing

Graphic

Example: Want 3-out-of-5.

Secret: z



Combine points to uniquely create z

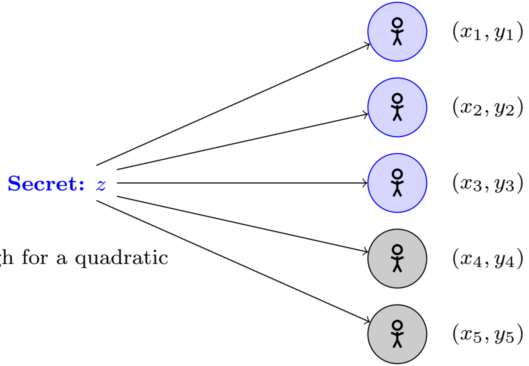
$$y = ax^2 + bx + z$$

▸ Description

Shamir Secret Sharing

Graphic

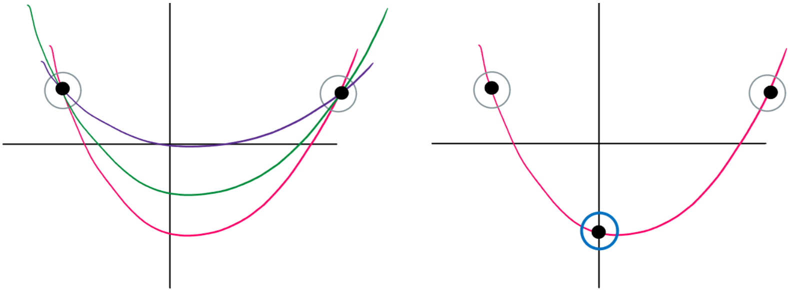
Example: Want 3-out-of-5.



2 points is not enough for a quadratic

▸ Description

Shamir Secret Sharing

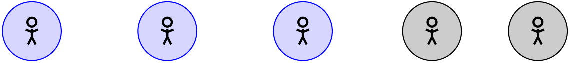


- With 2 points there are lots of solutions to the quadratic polynomial.
- By adding the third point we uniquely define the polynomial.

Protocol

Ring Members

For a 3-out-of-5 threshold ring signature:



$(vk^1, sk^1), (vk^2, sk^2), (vk^3, sk^3)$ vk^4 vk^5

Where $vk^s = (pk^s, x^s)$.

Template

Signer

$c^s \leftarrow \mathsf{TCom}(sk^s)$

$com = \boxed{c^1}\boxed{c^2}\boxed{c^3}\boxed{c^4}\boxed{c^5}$

$\mathsf{msg}, com \longrightarrow \boxed{\mathcal{H}} \longrightarrow z$

Verifier

$com, \boxed{\{(y^i, op^i)\}_{i=1}^5} \longrightarrow$

Non-signer

$(pk^q, ?)$

$c^q, op^q \leftarrow \mathsf{Com}_{pk^q}(y^q)$

Unruh

Template

Signer

msg, $com \longrightarrow \boxed{\mathcal{H}} \longrightarrow z$

$c^s \leftarrow \mathsf{TCom}(sk^s)$

Verifier

$com = \boxed{c^1}\boxed{c^2}\boxed{c^3}\boxed{c^4}\boxed{c^5}$ $\xrightarrow{com,\ \{(y^i, op^i)\}_{i=1}^5}$

Non-signer

$(pk^q, ?)$

$c^q, op^q \leftarrow \mathsf{Com}_{pk^q}(y^q)$

Unruh

Template

Signer

$\mathsf{msg}, com \longrightarrow \boxed{\mathcal{H}} \longrightarrow z$

$c^s \leftarrow \mathsf{TCom}(sk^s)$

Verifier

$com = \boxed{c^1}\,\boxed{c^2}\,\boxed{c^3}\,\boxed{c^4}\,\boxed{c^5}$

$\xrightarrow{com,\ \{(y^i, op^i)\}_{i=1}^{5}}$

Non-signer

$(pk^q, ?)$

$c^q, op^q \leftarrow \mathsf{Com}_{pk^q}(y^q)$

Unruh

Template

Signer

$c^s \leftarrow \mathsf{TCom}(sk^s)$

$com = \boxed{c^1}\boxed{c^2}\boxed{c^3}\boxed{c^4}\boxed{c^5}$

msg, $com \longrightarrow \boxed{\mathcal{H}} \longrightarrow z$

Verifier

com, $\{(y^i, op^i)\}_{i=1}^{5}$

Non-signer

$(pk^q, ?)$

$c^q, op^q \leftarrow \mathsf{Com}_{pk^q}(y^q)$

Unruh

Template

Signer

$c^s \leftarrow \mathsf{TCom}(sk^s)$

$com = \boxed{c^1}\boxed{c^2}\boxed{c^3}\boxed{c^4}\boxed{c^5}$

Non-signer

$(pk^q, ?)$

$c^q, op^q \leftarrow \mathsf{Com}_{pk^q}(y^q)$

$\mathsf{msg}, com \longrightarrow \boxed{\mathcal{H}} \longrightarrow z$

Verifier

$com, \boxed{\{(y^i, op^i)\}_{i=1}^5} \longrightarrow$

Unruh

Template

Signer

$c^s \leftarrow \mathsf{TCom}(sk^s)$

$com = \boxed{c^1}\boxed{c^2}\boxed{c^3}\boxed{c^4}\boxed{c^5}$

$\mathsf{msg}, com \longrightarrow \boxed{\mathcal{H}} \longrightarrow z$

Verifier

$com, \boxed{\{(y^i, op^i)\}_{i=1}^5} \longrightarrow$

Non-signer

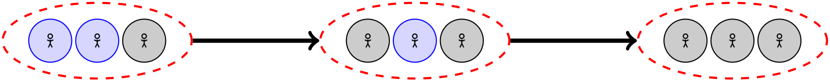
$(pk^q, ?)$

$c^q, op^q \leftarrow \mathsf{Com}_{pk^q}(y^q)$

Unruh

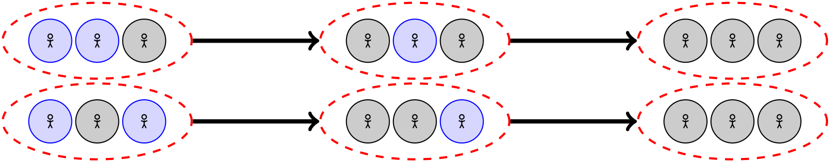
Core Technique

- Swap every trapdoor commitment out with an honest commitment step-by-step.
- At the end signers and non-signers look perfectly alike!



Anonymity

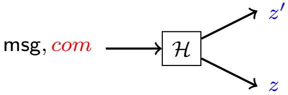
With all honest trapdoors two signatures look exactly alike.

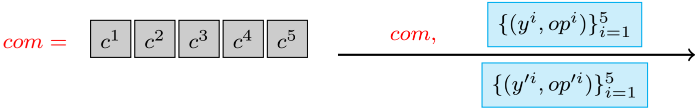


Replacing a trapdoor commitment with an honest commitment is indistinguishable.

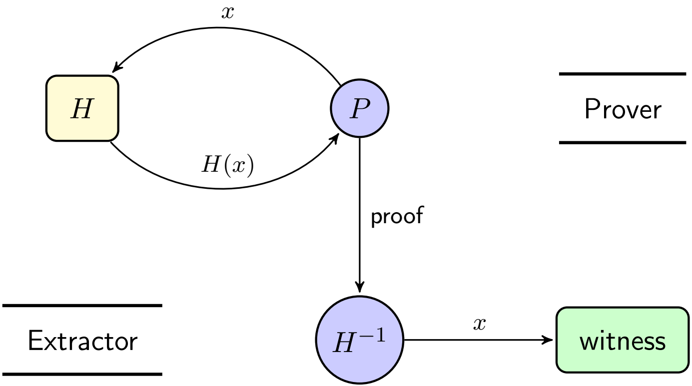
Unforgeability

With all honest commitments use a forgery to break binding.



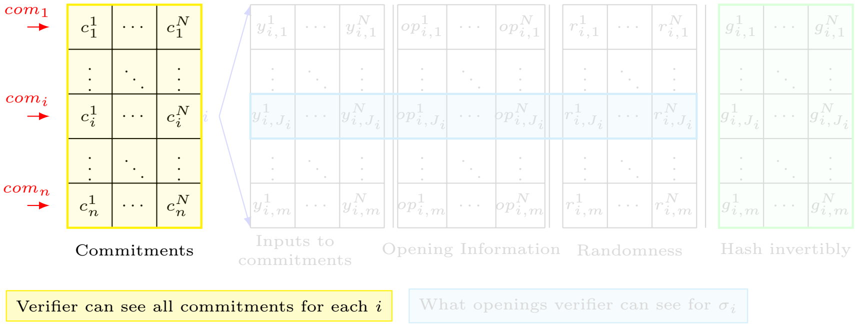


Unruh Transformation



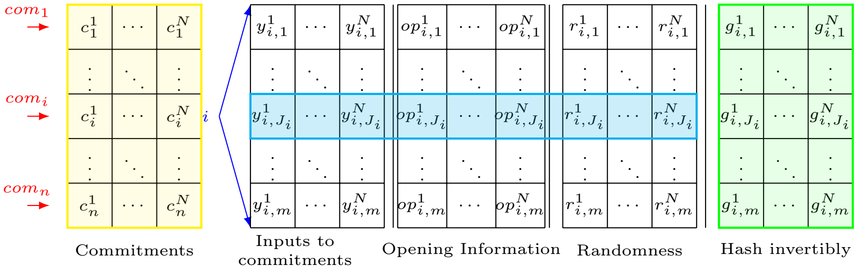
- make the RO invertible
- include all outputs in the proof

Unruh Transformation



Instead of making a single commitment, make n commitments and answer m challenges.

Unruh Transformation



Verifier can see all commitments for each i

What openings verifier can see for σ_i

Instead of making a single commitment, make n commitments and answer m challenges. 1

Unforgeability

$g_{i,1}^{1}$	$\cdots$	$g_{i,1}^{N}$
$\vdots$	$\ddots$	$\vdots$
g_{i,J_i}^{1}	$\cdots$	g_{i,J_i}^{N}
$\vdots$	$\ddots$	$\vdots$
$g_{i,m}^{1}$	$\cdots$	$g_{i,m}^{N}$

W.h.p. 2 commitments have 2 valid responses.

Summary

Summary

1. First formal definitions for a t-out-of-N threshold ring signature scheme in the presence of active adversaries that leverage malicious keys in their attacks. Generalized the definitions of Bender et al. (2006) from 1-out-of-N ring signatures to threshold t-out-of-N ring signatures.
2. Created a scheme which uses black-box trapdoor commitments, meaning that the parties can use any (post-quantum) trapdoor commitment scheme.
3. First construction that is provably secure against quantum adversaries that have quantum access to the random oracle.

Questions for Future Research

- Can we use Fiat-Shamir for thring signatures in a way that's provably post-quantum secure?
- Can we make a post-quantum secure thring signature which has anonymity amongst signers?

The End

https://eprint.iacr.org/2020/135

Bibliography I

Ambainis, A., Rosmanis, A., and Unruh, D. (2014). Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *Foundations of Computer Science (FOCS), 2014 IEEE 55th Annual Symposium on*, pages 474–483. IEEE.

Bender, A., Katz, J., and Morselli, R. (2006). Ring signatures: Stronger definitions, and constructions without random oracles. In *Theory of Cryptography Conference*, pages 60–79. Springer.

Bettaieb, S. and Schrek, J. (2013). Improved lattice-based threshold ring signature scheme. In *International Workshop on Post-Quantum Cryptography*, pages 34–51. Springer.

Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., and Zhandry, M. (2011). Random oracles in a quantum world. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 41–69. Springer.

Cayrel, P.-L., Lindner, R., Rückert, M., and Silva, R. (2010). A lattice-based threshold ring signature scheme. In *International Conference on Cryptology and Information Security in Latin America*, pages 255–272. Springer.

Bibliography II

Don, J., Fehr, S., Majenz, C., and Schaffner, C. (2019). Security of the fiat-shamir transformation in the quantum random-oracle model. Cryptology ePrint Archive, Report 2019/190. `https://eprint.iacr.org/2019/190`.

Fiat, A. and Shamir, A. (1986). How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptology, CRYPTO 86*, pages 186–194. Springer.

Liu, Q. and Zhandry, M. (2019). Revisiting post-quantum fiat-shamir. Cryptology ePrint Archive, Report 2019/262. `https://eprint.iacr.org/2019/262`.

Melchor, C. A., Cayrel, P.-L., Gaborit, P., and Laguillaumie, F. (2011). A new efficient threshold ring signature scheme based on coding theory. *IEEE Transactions on Information Theory*, 57(7):4833–4842.

Okamoto, T., Tso, R., Yamaguchi, M., and Okamoto, E. (2018). A k-out-of-n ring signature with flexible participation for signers. *IACR Cryptology ePrint Archive*, 2018:728.

Petzoldt, A., Bulygin, S., and Buchmann, J. (2013). A multivariate based threshold ring signature scheme. *Applicable Algebra in Engineering, Communication and Computing*, 24(3-4):255–275.

Bibliography III

Shor, P. W. (1994). Polynomial time algorithms for discrete logarithms and factoring on a quantum computer. In *International Algorithmic Number Theory Symposium*, pages 289–289. Springer.

Unruh, D. (2015). Non-interactive zero-knowledge proofs in the quantum random oracle model. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 755–784. Springer.

Watrous, J. (2009). Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58.