Post-Quantum Zero-Knowledge Proofs for Accumulators

with Applications to Ring Signatures from Symmetric-Key Primitives

David Derler[‡], **Sebastian Ramacher**[‡], Daniel Slamanig[§]

PQCRYPTO'18, April 9, 2018

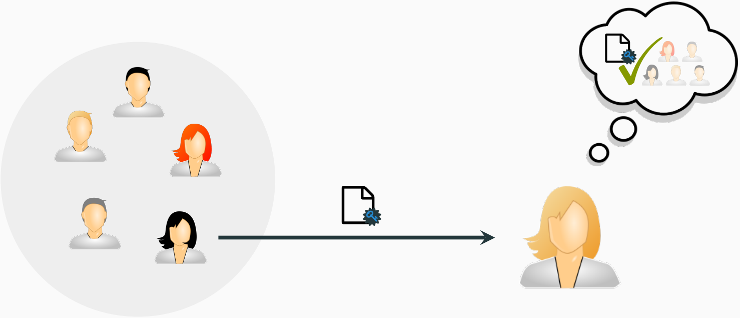
[‡] TU Graz [§] AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Ring Signatures

- Privacy enhancing primitive
- Sign a message on behalf of ad-hoc group (= ring)

» Signature attests some member of ring signed

» Signer remains anonymous within ring



PQ Ring Signatures

How to build ring signatures in a post-quantum setting?

- Code based [MCG08]
- Multivariate [MP17]

Linear size in # ring members!

Only recently first sublinear ring signatures:

- Lattice based [LLNW16]

» From generic accumulator based approach [DKNS04]

Can we build ring signatures solely from symmetric key primitives?

PQ Ring Signature Intuition

Generic approach [DKNS04]

- Compute compact representation of public keys
- Prove knowledge of a secret key
- Corresponding to one of the public keys

+ Incorporate message

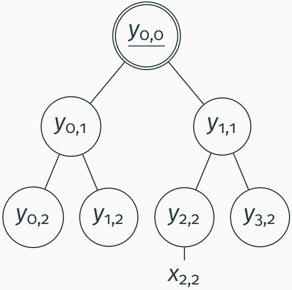
PQ Ring Signature Intuition

Generic approach [DKNS04]

- Compute compact representation of public keys
- Prove knowledge of a secret key
- Corresponding to one of the public keys

+ Incorporate message

Instantiation via Merkle trees



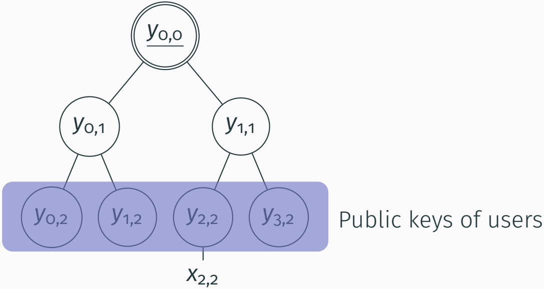
PQ Ring Signature Intuition

Generic approach [DKNS04]

- Compute compact representation of public keys
- Prove knowledge of a secret key
- Corresponding to one of the public keys

+ Incorporate message

Instantiation via Merkle trees



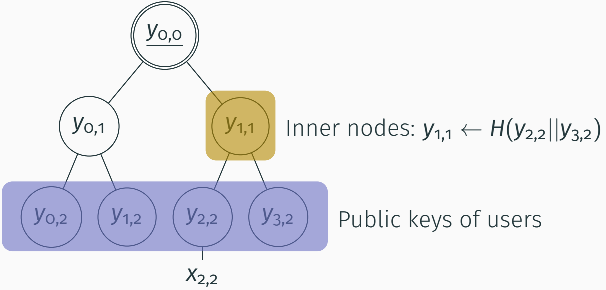
PQ Ring Signature Intuition

Generic approach [DKNS04]

- Compute compact representation of public keys
- Prove knowledge of a secret key
- Corresponding to one of the public keys

+ Incorporate message

Instantiation via Merkle trees



Inner nodes: $y_{1,1} \leftarrow H(y_{2,2}||y_{3,2})$

Public keys of users

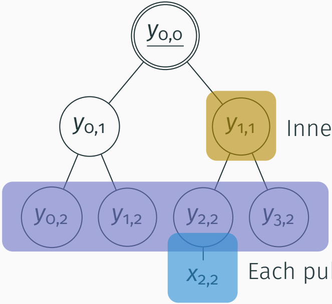
PQ Ring Signature Intuition

Generic approach [DKNS04]

- Compute compact representation of public keys
- Prove knowledge of a secret key
- Corresponding to one of the public keys

+ Incorporate message

Instantiation via Merkle trees



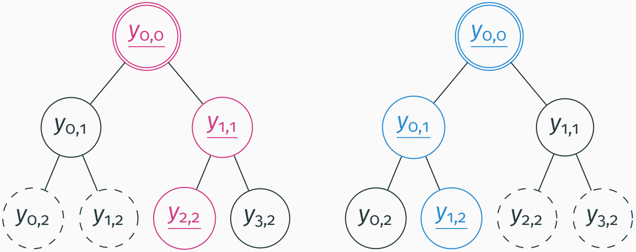
Inner nodes: $y_{1,1} \leftarrow H(y_{2,2} || y_{3,2})$

Public keys of users

Each public key associated to a secret key

Zero-Knowledge Membership Proof

Naive approach reveals path taken



Trivial approach

- Disjunctive proof of knowledge over all possible paths
- Linear size in # ring members!

Zero-Knowledge Membership Proof

Use commutative hash function? [DKNS04]

- $y_i = H(a_i, b_i) = H(b_i, a_i)$
- y_i, a_i, b_i not revealed (except root of tree)
- Does not reveal whether we continue left or right
- Not directly possible in symmetric setting!

Zero-Knowledge Membership Proof

Use commutative hash function? [DKNS04]

- $y_i = H(a_i, b_i) = H(b_i, a_i)$
- y_i, a_i, b_i not revealed (except root of tree)
- Does not reveal whether we continue left or right
- Not directly possible in symmetric setting!

Our technique

- “Emulate” commutativity
- Disjunctive statement per level

  $y_i = H(a_i||b_i) \;\vee\; y_i = H(b_i||a_i)$

Our Ring Signatures

- Accumulate public keys
- Prove knowledge of secret key corresponding to public key
- Proof membership of public key

Our Ring Signatures

- Accumulate public keys
- Prove knowledge of secret key corresponding to public key
- Proof membership of public key

Unforgeability:

- From collision-free accumulator with one-way domain
- And simulation-sound extractability
- + Prove that ZKB++/FS is simulation-sound extractable

Our Ring Signatures

- Accumulate public keys
- Prove knowledge of secret key corresponding to public key
- Proof membership of public key

Unforgeability:

- From collision-free accumulator with one-way domain
- And simulation-sound extractability
+ Prove that ZKB++/FS is simulation-sound extractable

Anonymity:

- From zero-knowledge

Instantiation & Signature Size

Instantiation

- ZKB++
- One-way function: use LowMC
- Hash function: use LowMC in Sponge framework

Estimated signature sizes

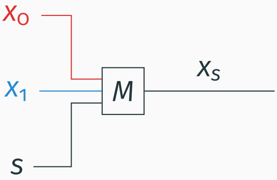
- Logarithmic in # of ring members

Ring size	$|\sigma|$ (FS/ROM)	$|\sigma|$ (Unruh/QROM)
2^5	2125 KB	3159 KB
2^{10}	4086 KB	6067 KB
2^{20}	8008 KB	11882 KB

Can we do better? - New results

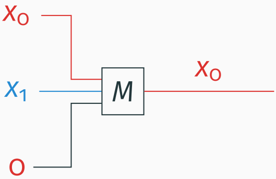
Instantiating the Circuit

Multiplexer



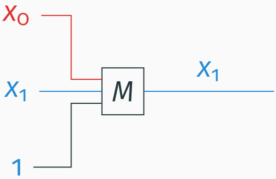
Instantiating the Circuit

Multiplexer

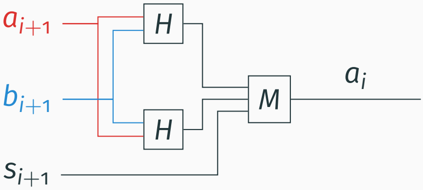


Instantiating the Circuit

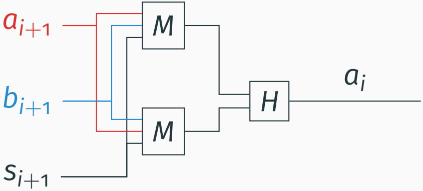
Multiplexer



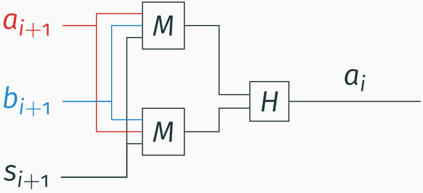
Instantiating the Circuit



Instantiating the Circuit



Instantiating the Circuit



- Requires 2 AND gates / output bit

+ Can be optimized to only require 1 AND gate / output bit

Smaller Signatures

- Only one hash function evaluation
- Two multiplexers with circuit optimizations
- Additionally AND gates in digest size

» Signature size reduction by factor ≈ 2

Ring size	$|\sigma|$ (FS/ROM)	$|\sigma|$ (Unruh/QROM)
2^5	1200 KB	2289 KB
2^{10}	2283 KB	4388 KB
2^{20}	4450 KB	8584 KB

Conclusions

Important steps towards PQ privacy enhancing primitives

- Solely from symmetric primitives
- PQ accumulators + ZK proofs
- Construction of ring signatures

Very flexible

- Similar techniques recently used by Boneh et al. [BEF18]

» In construction of PQ dynamic group signatures

Future directions

- New results $\rightarrow$ smaller signatures
- Even smaller sizes for group signatures of Boneh et al.

? Further optimizations & new constructions

Questions?

Full version: `https://ia.cr/2017/1154`

Supported by: prisma cloud

References i

[BEF18] Dan Boneh, Saba Eskandarian, and Ben Fisch. Post-quantum group signatures from symmetric primitives. *IACR Cryptology ePrint Archive*, 2018:261, 2018.

[DKNS04] Yevgeniy Dodis, Aggelos Kiayias, Antonio Nicolosi, and Victor Shoup. Anonymous identification in ad hoc groups. In *EUROCRYPT*, 2004.

[LLNW16] Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang. Zero-knowledge arguments for lattice-based accumulators: Logarithmic-size ring signatures and group signatures without trapdoors. In *EUROCRYPT*, 2016.

[MCG08] Carlos Aguilar Melchor, Pierre-Louis Cayrel, and Philippe Gaborit. A new efficient threshold ring signature scheme based on coding theory. In *PQCrypto*, 2008.

[MP17] Mohamed Saied Emam Mohamed and Albrecht Petzoldt. Ringrainbow - an efficient multivariate ring signature scheme. In *AFRICACRYPT*, 2017.