
DTU

Marvin Beckmann, Christian Majenz

Fully Anonymous Ring Signatures in the QROM

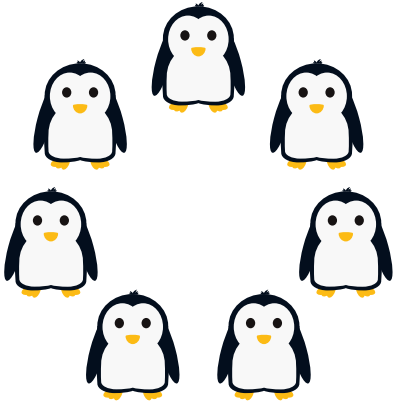
Example: Whistleblowers

Example: Whistleblowers

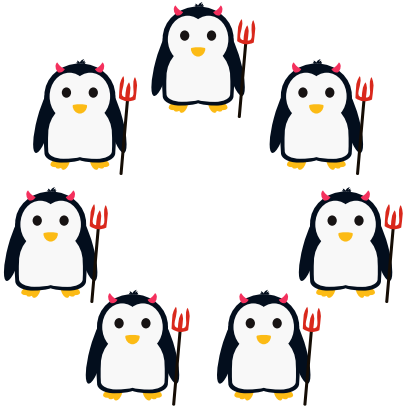
Example: Whistleblowers

Deniability and Authenticity

Ring Signatures



Ring Signatures



Ring Signatures in Messengers

- (deniable) authenticated key exchange (e.g. for Signal [8])

Ring Signatures in Messengers

- (deniable) authenticated key exchange (e.g. for Signal [8])
- only 2 parties (linear ring signatures are well-suited)

Ring Signatures in Messengers

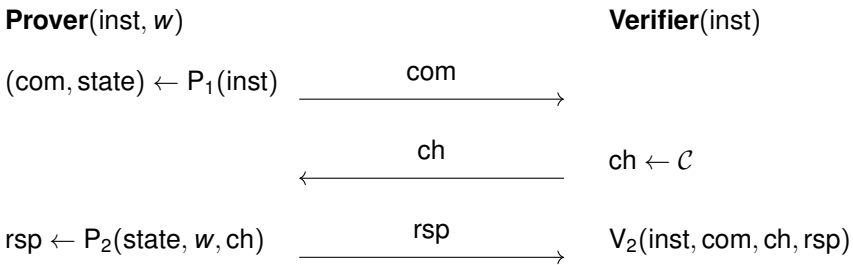
- (deniable) authenticated key exchange (e.g. for Signal [8])
- only 2 parties (linear ring signatures are well-suited)
- deniability under full key exposure

Ring Signatures in Messengers

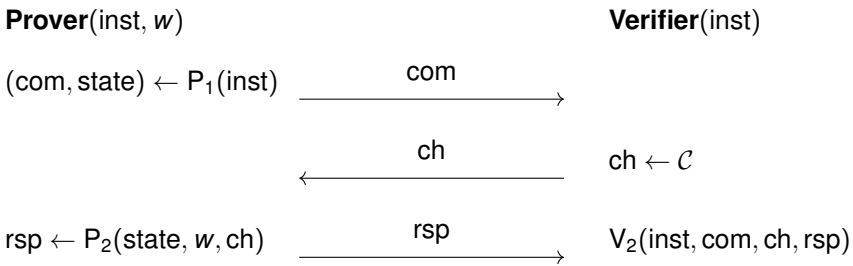
- (deniable) authenticated key exchange (e.g. for Signal [8])
- only 2 parties (linear ring signatures are well-suited)
- deniability under full key exposure

(1) AOS-transform [1] and (2) Ring Trapdoor Functions

Sigma Protocols

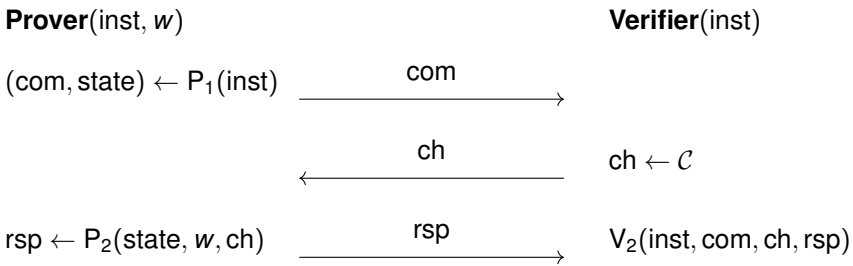


Sigma Protocols



- Impersonation, . . . , witness recovery, HVZK simulator (with min-entropy)

Sigma Protocols



- Impersonation, . . . , witness recovery, HVZK simulator (with min-entropy)
- To make a signature scheme: Fiat-Shamir transform

AOS Transform for Sigma Protocols

$\mathsf{Sign}(\mathsf{sk}_i = w_i, \rho = \{\mathsf{inst}_1, \ldots, \mathsf{inst}_N\}, \mu)$

1 : $(\mathsf{com}_i, \mathsf{state}_i) \leftarrow \Sigma.\mathsf{P}_1(\mathsf{inst}_i)$

2 :

3 :

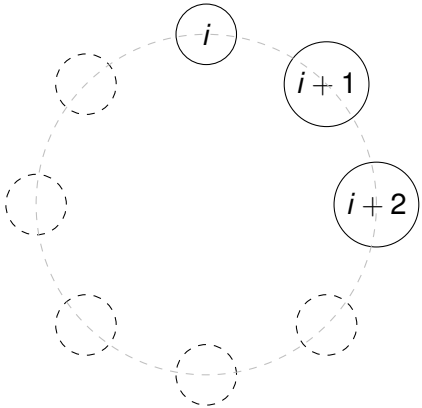
4 :

5 :

6 :

7 :

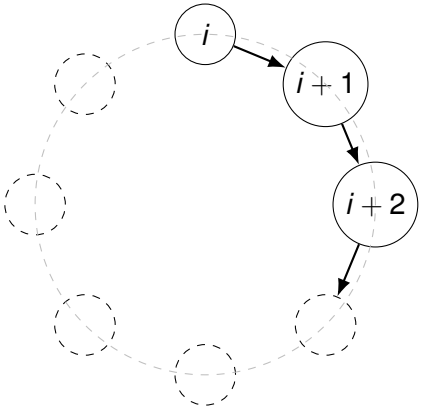
8 :



AOS Transform for Sigma Protocols

$\mathsf{Sign}(\mathsf{sk}_i = w_i, \rho = \{\mathsf{inst}_1, \ldots, \mathsf{inst}_N\}, \mu)$

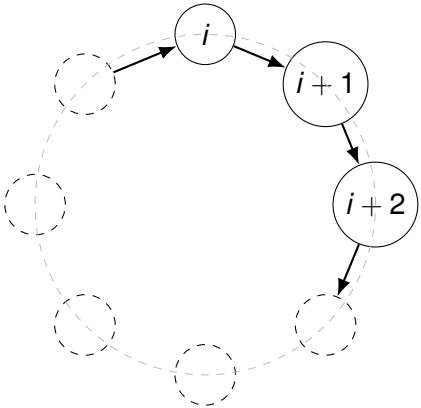
1 : $(\mathsf{com}_i, \mathsf{state}_i) \leftarrow \Sigma.\mathsf{P}_1(\mathsf{inst}_i)$
2 : **for** $j = i+1, \ldots, N, 1, \ldots, i-1$
3 : $\quad \mathsf{ch}_j \leftarrow \mathsf{H}(j, \rho, \mathsf{com}_{j-1}, \mu)$
4 : $\quad (\mathsf{com}_j, \mathsf{rsp}_j) \leftarrow \mathsf{Sim}(\mathsf{inst}_j, \mathsf{ch}_j)$
5 :
6 :
7 :
8 :



AOS Transform for Sigma Protocols

$\mathsf{Sign}(\mathsf{sk}_i = w_i, \rho = \{\mathsf{inst}_1, \ldots, \mathsf{inst}_N\}, \mu)$

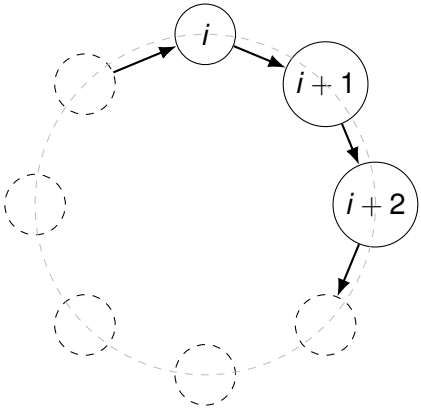
1 : $(\mathsf{com}_i, \mathsf{state}_i) \leftarrow \Sigma.\mathsf{P}_1(\mathsf{inst}_i)$
2 : **for** $j = i+1, \ldots, N, 1, \ldots, i-1$
3 : $\quad \mathsf{ch}_j \leftarrow \mathsf{H}(j, \rho, \mathsf{com}_{j-1}, \mu)$
4 : $\quad (\mathsf{com}_j, \mathsf{rsp}_j) \leftarrow \mathsf{Sim}(\mathsf{inst}_j, \mathsf{ch}_j)$
5 : $\mathsf{ch}_i \leftarrow \mathsf{H}(i, \rho, \mathsf{com}_{i-1}, \mu)$
6 :
7 :
8 :



AOS Transform for Sigma Protocols

$\mathsf{Sign}(\mathsf{sk}_i = w_i, \rho = \{\mathsf{inst}_1, \ldots, \mathsf{inst}_N\}, \mu)$

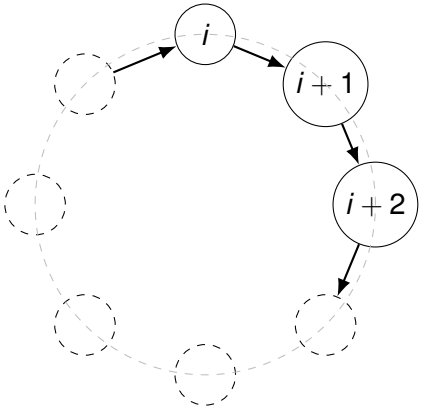
1 : $(\mathsf{com}_i, \mathsf{state}_i) \leftarrow \Sigma.\mathsf{P}_1(\mathsf{inst}_i)$
2 : **for** $j = i+1, \ldots, N, 1, \ldots, i-1$
3 : $\quad \mathsf{ch}_j \leftarrow \mathsf{H}(j, \rho, \mathsf{com}_{j-1}, \mu)$
4 : $\quad (\mathsf{com}_j, \mathsf{rsp}_j) \leftarrow \mathsf{Sim}(\mathsf{inst}_j, \mathsf{ch}_j)$
5 : $\mathsf{ch}_i \leftarrow \mathsf{H}(i, \rho, \mathsf{com}_{i-1}, \mu)$
6 : $\mathsf{rsp}_i \leftarrow \Sigma.\mathsf{P}_2(\mathsf{state}, w_i, \mathsf{ch}_i)$
7 :
8 :



AOS Transform for Sigma Protocols

$\mathsf{Sign}(\mathsf{sk}_i = w_i, \rho = \{\mathsf{inst}_1, \ldots, \mathsf{inst}_N\}, \mu)$

1 : $(\mathsf{com}_i, \mathsf{state}_i) \leftarrow \Sigma.\mathsf{P}_1(\mathsf{inst}_i)$
2 : **for** $j = i+1, \ldots, N, 1, \ldots, i-1$
3 : $\quad \mathsf{ch}_j \leftarrow \mathsf{H}(j, \rho, \mathsf{com}_{j-1}, \mu)$
4 : $\quad (\mathsf{com}_j, \mathsf{rsp}_j) \leftarrow \mathsf{Sim}(\mathsf{inst}_j, \mathsf{ch}_j)$
5 : $\mathsf{ch}_i \leftarrow \mathsf{H}(i, \rho, \mathsf{com}_{i-1}, \mu)$
6 : $\mathsf{rsp}_i \leftarrow \Sigma.\mathsf{P}_2(\mathsf{state}, w_i, \mathsf{ch}_i)$
7 : $\sigma \leftarrow ((\mathsf{com}_1, \mathsf{rsp}_1), \ldots, (\mathsf{com}_N, \mathsf{rsp}_N))$
8 : **return** σ



A QROM-Proof for AOS

Goal: Reduce ring signature unforgeability to impersonation security

[1] multiplicative loss exponential in ring size
[2] Additive error term

A QROM-Proof for AOS

Goal: Reduce ring signature unforgeability to impersonation security

1. removing all signing queries:

[1] multiplicative loss exponential in ring size

[2] Additive error term

A QROM-Proof for AOS

Goal: Reduce ring signature unforgeability to impersonation security

1. removing all signing queries:
   - Adaptive reprogramming in the QROM [7] and HVZK simulator

[1] multiplicative loss exponential in ring size
[2] Additive error term

A QROM-Proof for AOS

Goal: Reduce ring signature unforgeability to impersonation security

1. removing all signing queries:
   - Adaptive reprogramming in the QROM [7] and HVZK simulator
   - To ensure the correctness of the final forgery: QROM collision resistance [3], witness-recovery and CUR

[1] multiplicative loss exponential in ring size

[2] Additive error term

A QROM-Proof for AOS

Goal: Reduce ring signature unforgeability to impersonation security

1. removing all signing queries:
   - Adaptive reprogramming in the QROM [7] and HVZK simulator
   - To ensure the correctness of the final forgery: QROM collision resistance [3], witness-recovery and CUR
2. reduce to impersonation adversary

[1] multiplicative loss exponential in ring size

[2] Additive error term

A QROM-Proof for AOS

Goal: Reduce ring signature unforgeability to impersonation security

1. removing all signing queries:
   - Adaptive reprogramming in the QROM [7] and HVZK simulator
   - To ensure the correctness of the final forgery: QROM collision resistance [3], witness-recovery and CUR
2. reduce to impersonation adversary
   - problem: the order of commitment and challenge for party i is not fixed...

[1] multiplicative loss exponential in ring size

[2] Additive error term

A QROM-Proof for AOS

Goal: Reduce ring signature unforgeability to impersonation security

1. removing all signing queries:
   - Adaptive reprogramming in the QROM [7] and HVZK simulator
   - To ensure the correctness of the final forgery: QROM collision resistance [3], witness-recovery and CUR
2. reduce to impersonation adversary
   - problem: the order of commitment and challenge for party i is not fixed...
   - general approach: using measure-and-reprogram [4], get an order of all queries from a forgery[1]

[1] multiplicative loss exponential in ring size

[2] Additive error term

A QROM-Proof for AOS

Goal: Reduce ring signature unforgeability to impersonation security

1. removing all signing queries:
   - Adaptive reprogramming in the QROM [7] and HVZK simulator
   - To ensure the correctness of the final forgery: QROM collision resistance [3], witness-recovery and CUR
2. reduce to impersonation adversary
   - problem: the order of commitment and challenge for party i is not fixed...
   - general approach: using measure-and-reprogram [4], get an order of all queries from a forgery[1]
   - alternative approach: assume commit-and-open sigma protocols: use framework [3] based on Zhandrys compressed oracle slightly adjusted in [5] [2]

[1] multiplicative loss exponential in ring size

[2] Additive error term

Commit-and-Open Protocols for AOS

Reduce to witness-recovery instead:

- Commit-and-open protocols
  - commitments contain responses
  - challenge determines which commitments to open with responses

Commit-and-Open Protocols for AOS

Reduce to witness-recovery instead:

- Commit-and-open protocols
  - commitments contain responses
  - challenge determines which commitments to open with responses
- interested in a search problem: generate a valid transcript without possible extractions

Commit-and-Open Protocols for AOS

Reduce to witness-recovery instead:

- Commit-and-open protocols
  - commitments contain responses
  - challenge determines which commitments to open with responses
- interested in a search problem: generate a valid transcript without possible extractions
- compressed-oracle formalism (classical analogue: query lists)
  - analyse probability of database satisfying search problem

Commit-and-Open Protocols for AOS

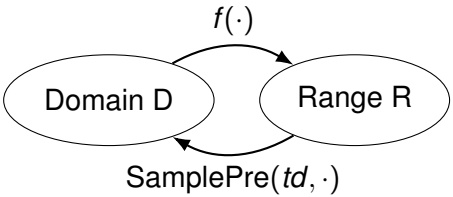
Reduce to witness-recovery instead:

- Commit-and-open protocols
  - commitments contain responses
  - challenge determines which commitments to open with responses
- interested in a search problem: generate a valid transcript without possible extractions
- compressed-oracle formalism (classical analogue: query lists)
  - analyse probability of database satisfying search problem
  - depends on maximal fraction of challenges that can be answered for a fixed commitment without extraction being possible

Yay, QROM Proofs for AOS Ring Signatures!

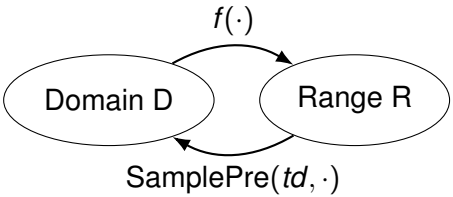
Trapdoor Functions and PSFs [6]

- f is one-way
- SampePre returns preimages under f



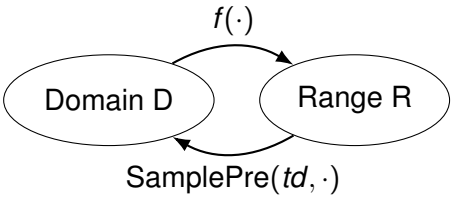
Trapdoor Functions and PSFs [6]

- f is one-way
- SampePre returns preimages under f
- PSFs: $\exists$ a distribution D on D s.t.
  - $f(d) \approx \mathcal{U}(\mathrm{R})$ where $d \leftarrow D$
  - SamplePre(td, r) is indistinguishable from $d \leftarrow D$ conditioned on $f(d) = r$



Trapdoor Functions and PSFs [6]

- f is one-way
- SampePre returns preimages under f
- PSFs: $\exists$ a distribution D on D s.t.
  - $f(d) \approx \mathcal{U}(\mathrm{R})$ where $d \leftarrow D$
  - SamplePre(td, r) is indistinguishable from $d \leftarrow D$ conditioned on $f(d) = r$



Ring Trapdoor Functions

- Each subset of parties ρ defines a function $f_\rho : D_\rho \to R_\rho$
- Each party in ρ has a trapdoor for f_ρ

[3] With additional care for key-exposure and malicious public keys

Ring Trapdoor Functions

- Each subset of parties ρ defines a function $f_\rho : D_\rho \to R_\rho$
- Each party in ρ has a trapdoor for f_ρ
- We again define PSF-like properties[3]

[3] With additional care for key-exposure and malicious public keys

Ring Trapdoor Functions for Ring Signatures

Sign(sk, ρ, m)

1 : $s \leftarrow \{0,1\}^{\lambda}$
2 : $h \leftarrow \mathsf{H}(\rho, s, m)$
3 : $\sigma \leftarrow \mathsf{SamplePre}(\mathsf{sk}, \rho, h)$
4 : **return** (s, σ)

[a] requires statistical distance ϵ and yields additive term of $\approx q^2\sqrt{\epsilon}$

Ring Trapdoor Functions for Ring Signatures

1. query simulation strategy
   - sample in domain D_ρ and apply f_ρ
   - do a history-free proof [2]; use randomness (deterministically derived from ρ, s, m) for domain sampling [a]

[a] requires statistical distance ϵ and yields additive term of $\approx q^2\sqrt{\epsilon}$

$\mathsf{Sign}(\mathsf{sk}, \rho, m)$

1 : $s \leftarrow \{0,1\}^\lambda$
2 : $h \leftarrow \mathsf{H}(\rho, s, m)$
3 : $\sigma \leftarrow \mathsf{SamplePre}(\mathsf{sk}, \rho, h)$
4 : **return** (s, σ)

Ring Trapdoor Functions for Ring Signatures

Sign(sk, ρ, m)

1 : $s \leftarrow \{0,1\}^{\lambda}$
2 : $h \leftarrow \mathsf{H}(\rho, s, m)$
3 : $\sigma \leftarrow \mathsf{SamplePre}(\mathsf{sk}, \rho, h)$
4 : **return** (s, σ)

[a] requires statistical distance ϵ and yields additive term of $\approx q^2\sqrt{\epsilon}$

Summary

QROM proof for

- AOS-transform
  - General bound with multiplicative term of q^{2N}
  - Commit-and-open additive term
- Preimage sampleable ring trapdoor function
  - only work with statistical distance [a]

[a] We are working on changing this

References I

[1] Masayuki Abe, Miyako Ohkubo, and Koutarou Suzuki. “1-out-of-n Signatures from a Variety of Keys”. In: 2002, pp. 415–432. DOI: 10.1007/3-540-36178-2_26.

[2] Dan Boneh et al. “Random Oracles in a Quantum World”. In: 2011, pp. 41–69. DOI: 10.1007/978-3-642-25385-0_3.

[3] Kai-Min Chung et al. “On the Compressed-Oracle Technique, and Post-Quantum Security of Proofs of Sequential Work”. In: 2021, pp. 598–629. DOI: 10.1007/978-3-030-77886-6_21.

[4] Jelle Don, Serge Fehr, and Christian Majenz. “The Measure-and-Reprogram Technique 2.0: Multi-round Fiat-Shamir and More”. In: 2020, pp. 602–631. DOI: 10.1007/978-3-030-56877-1_21.

References II

[5] Jelle Don et al. “Efficient NIZKs and Signatures from Commit-and-Open Protocols in the QROM”. In: 2022, pp. 729–757. DOI: 10.1007/978-3-031-15979-4_25.

[6] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. “Trapdoors for hard lattices and new cryptographic constructions”. In: 2008, pp. 197–206. DOI: 10.1145/1374376.1374407.

[7] Alex B. Grilo et al. “Tight Adaptive Reprogramming in the QROM”. In: 2021, pp. 637–667. DOI: 10.1007/978-3-030-92062-3_22.

[8] Keitaro Hashimoto et al. “An Efficient and Generic Construction for Signal’s Handshake (X3DH): Post-Quantum, State Leakage Secure, and Deniable”. In: 2021, pp. 410–440. DOI: 10.1007/978-3-030-75248-4_15.