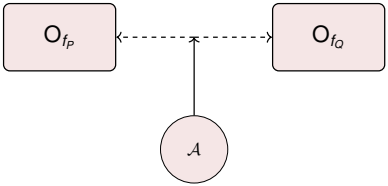

DTU

Marvin Beckmann, Christian Majenz

Quantum Oracle Distribution Switching and Applications

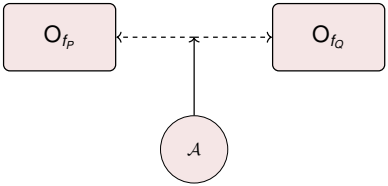
Distinguishing two Classical Distributions

Define i.i.d function $f_P : \mathcal{X} \to \mathcal{Y}$ where $f_P(x) \sim P$ for all $x \in \mathcal{X}$.



Distinguishing two Classical Distributions

Define i.i.d function $f_P : \mathcal{X} \to \mathcal{Y}$ where $f_P(x) \sim P$ for all $x \in \mathcal{X}$.



We wanted: Bounds on $\mathcal{A}$ using classical properties of P and Q

Oracle Distribution Switching using Statistical Distance

Bounds for Classical Queries

Statistical distance:

$$\Delta(P, Q) := \frac{1}{2} \sum_{x \in \Omega} |P(x) - Q(x)|$$

$\mathcal{A}$ can query the oracle q times:

$$\left| \Pr\left[1 \leftarrow \mathcal{A}^{\mathsf{O}_{f_P}}(\boldsymbol{x})\right] - \Pr\left[1 \leftarrow \mathcal{A}^{\mathsf{O}_{f_Q}}(\boldsymbol{x})\right] \right| \leq q \cdot \Delta(P, Q)$$

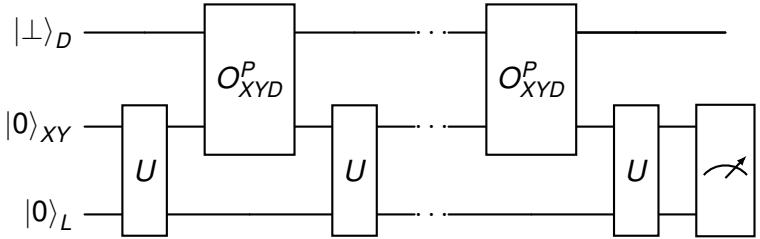
Bounds for Quantum Queries

Boneh et al. [BDF+11]	$\mathcal{O}(q^2\sqrt{\epsilon})$
Zhandry [Zha12]	$\mathcal{O}(q^{1.5}\sqrt{\epsilon})$
Our Work	$8q\sqrt{2\epsilon}$
Belovs [Bel19][1]	$\mathcal{O}(q\sqrt{\epsilon})$

▷ Grover's algorithm with q queries can produce two states with trace distance $\Theta(q\sqrt{\epsilon})$.

[1] They use a different technique; Do not derive explicit bounds; And (honestly) we were not aware of this work until we finished our derivation

Quantum Oracle Queries in Compressed Oracle View

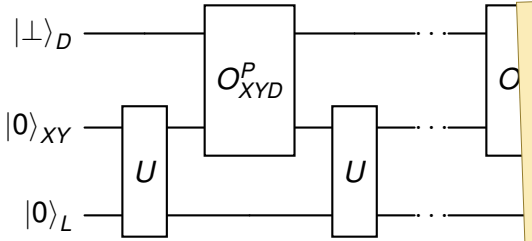


$$O^P_{XYD} = \sum_{x \in \mathcal{X}} |x\rangle\langle x|_X \otimes O^{P,x}_{YD_x}, \quad \text{with} \quad O^{P,x}_{YD_x} = F^P_{D_x}\,\mathrm{CNOT}_{YD_x}\,F^P_{D_x}$$

$$F^P = |\perp\rangle\langle\phi_P| + |\phi_P\rangle\langle\perp| + I_{\{0,1\}^n} - |\perp\rangle\langle\perp| - |\phi_P\rangle\langle\phi_P|\,.$$

$$|\phi_P\rangle := \sum_{y \in \{0,1\}^n} \sqrt{P(y)}\,|y\rangle$$

Quantum Oracle Queries in Compressed Oracle View



Adding $2q$ null terms:

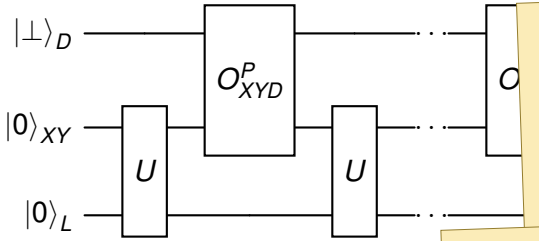
Bounds the trace distance of $\mathcal{A}$'s outputs as $4q\left\|F^P - F^Q\right\|_\infty$.

$$O^P_{XYD} = \sum_{x\in\mathcal{X}} |x\rangle\langle x|_X \otimes O^{P,x}_{YD_x}, \quad \text{with} \quad O^{P,x}_{YD_x} = F^P_{D_x}\,\mathrm{CNOT}_{YD_x}\,F^P_{D_x}$$

$$F^P = |\perp\rangle\langle\phi_P| + |\phi_P\rangle\langle\perp| + I_{\{0,1\}^n} - |\perp\rangle\langle\perp| - |\phi_P\rangle\langle\phi_P|\,.$$

$$|\phi_P\rangle := \sum_{y\in\{0,1\}^n} \sqrt{P(y)}\,|y\rangle$$

Quantum Oracle Queries in Compressed Oracle View



$$O^P_{XYD} = \sum_{x \in \mathcal{X}} |x\rangle\langle x|_X \otimes O^{P,x}_{YD_x}, \quad \text{with}$$

$$F^P = |\perp\rangle\langle\phi_P| + |\phi_P\rangle\langle\perp| + I_{\{0,1\}^n}$$

$$|\phi_P\rangle := \sum_{y \in \{0,1\}^n} \sqrt{}$$

Adding $2q$ null terms:

Bounds the trace distance of $\mathcal{A}$'s outputs as $4q\left\|F^P - F^Q\right\|_\infty$.

$\left\|F^P - F^Q\right\|_\infty$ can be bounded by a sequence of somewhat tedious computations as $\sqrt{8\Delta(P,Q)}$.

Oracle Distribution Switching using Rényi Divergence

Rényi Divergence

Rényi divergence ($\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$):

$$R_\alpha(P\|Q) = \left(\sum\nolimits_{x\in\mathrm{Supp}(P)} P(x)^\alpha \cdot Q(x)^{1-\alpha}\right)^{\frac{1}{\alpha-1}} \quad \text{for } \alpha \in (1,\infty)$$

$$R_\infty(P\|Q) = \sup\nolimits_{x\in\mathrm{Supp}(P)} P(x)/Q(x)$$

Rényi Divergence

Rényi divergence ($\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$):

$$R_\alpha(P\|Q) = \left(\sum\nolimits_{x\in\mathrm{Supp}(P)} P(x)^\alpha \cdot Q(x)^{1-\alpha}\right)^{\frac{1}{\alpha-1}} \quad \text{for } \alpha \in (1,\infty)$$

$$R_\infty(P\|Q) = \sup\nolimits_{x\in\mathrm{Supp}(P)} P(x)/Q(x)$$

Probability preservation property and the data processing inequality:

$$\Pr[P \in E]^{\frac{\alpha}{\alpha-1}} \leq R_\alpha(P\|Q) \cdot \Pr[Q \in E], \quad \text{and} \quad R_\alpha(f(P)\|f(Q)) \leq R_\alpha(P\|Q).$$

Rényi Divergence

Rényi divergence ($\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$):

$$R_\alpha(P\|Q) = \left(\sum\nolimits_{x\in\mathrm{Supp}(P)} P(x)^\alpha \cdot Q(x)^{1-\alpha}\right)^{\frac{1}{\alpha-1}} \quad \text{for } \alpha \in (1,\infty)$$

$$R_\infty(P\|Q) = \sup\nolimits_{x\in\mathrm{Supp}(P)} P(x)/Q(x)$$

Probability preservation property and the data processing inequality:

$$\Pr[P \in E]^{\frac{\alpha}{\alpha-1}} \leq R_\alpha(P\|Q) \cdot \Pr[Q \in E], \quad \text{and} \quad R_\alpha(f(P)\|f(Q)) \leq R_\alpha(P\|Q).$$

For q independent samples:

$$R_\alpha(P^q\|Q^q) = R_\alpha(P\|Q)^q.$$

Are such multiplicative bounds even possible?

We use Deutsch-Jozsa to show impossibility:

- Fix $y_0 := \arg\max_{y \in \mathrm{Supp}(P)} \frac{P(y)}{Q(y)}$.

Are such multiplicative bounds even possible?

We use Deutsch-Jozsa to show impossibility:

- Fix $y_0 := \arg\max_{y \in \mathrm{Supp}(P)} \frac{P(y)}{Q(y)}$.
- Map to $0/1$: Post-process outputs to 0 if they are y_0 and 1 otherwise.

Are such multiplicative bounds even possible?

We use Deutsch-Jozsa to show impossibility:

- Fix $y_0 := \arg\max_{y \in \mathrm{Supp}(P)} \frac{P(y)}{Q(y)}$.
- Map to $0/1$: Post-process outputs to 0 if they are y_0 and 1 otherwise.
- Rebalance the function in expectation for $P \Rightarrow$ for Q it is not balanced

Are such multiplicative bounds even possible?

We use Deutsch-Jozsa to show impossibility:

- Fix $y_0 := \arg\max_{y \in \mathrm{Supp}(P)} \frac{P(y)}{Q(y)}$.
- Map to $0/1$: Post-process outputs to 0 if they are y_0 and 1 otherwise.
- Rebalance the function in expectation for $P \Rightarrow$ for Q it is not balanced
- The fraction's numerator scales exponentially in n

Theorem

For all distributions $P \neq Q$ on $\mathcal{Y}$ with $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$, there exists an algorithm $\mathcal{A}$ making at most q_H quantum queries such that

$$\lim_{n\to\infty} \Pr\left[1 \leftarrow \mathcal{A}^{f_P}\right] / \Pr\left[1 \leftarrow \mathcal{A}^{f_Q}\right] = \infty.$$

▷ A bound on the ratio of probabilities is impossible.

Are such multiplicative bounds even possible?

We use Deutsch-Jozsa to show impossibility:

- Fix $y_0 := \arg\max_{y \in \mathrm{Supp}(P)} \frac{P(y)}{Q(y)}$.
- Map to $0/1$: Post-process outputs to 0 if they are y_0 and 1 otherwise.
- Rebalance the function in expectation for $P \Rightarrow$ for Q it is not balanced
- The fraction's numerator scales exponentially in n

Theorem

For all distributions $P \neq Q$ on $\mathcal{Y}$ with $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$, there exists an algorithm $\mathcal{A}$ making at most q_H quantum queries such that

$$\lim_{n\to\infty} \Pr\left[1 \leftarrow \mathcal{A}^{f_P}\right] / \Pr\left[1 \leftarrow \mathcal{A}^{f_Q}\right] = \infty.$$

▷ A bound on the ratio of probabilities is impossible. Circumvention: Use an additional additive error term.

Small-Range Distribution [Zha12]

- Sample r independent values $\{y_i\}_{i\in[r]}$ according to P.
- These simulate the oracle O_{f_P}: $\forall x \in \mathcal{X}$, $\mathrm{O}_{f_P}(x) \leftarrow \{y_i\}_{i\in[r]}$
- Indistinguishable for $\mathcal{A}$ up to an error term of $\mathcal{O}\left(q^3/r\right)$

Small-Range Distribution [Zha12]

- Sample r independent values $\{y_i\}_{i\in[r]}$ according to P.
- These simulate the oracle O_{f_P}: $\forall x \in \mathcal{X}$, $\mathsf{O}_{f_P}(x) \leftarrow \{y_i\}_{i\in[r]}$
- Indistinguishable for $\mathcal{A}$ up to an error term of $\mathcal{O}(q^3/r)$

Lemma

Let P, Q be classical distributions over $\mathcal{Y}$ with $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$ and $\delta = R_\alpha(P\|Q)$, for $\alpha \in (1,\infty]$. For any $\mathcal{A}$ making at most q quantum queries

$$\Pr\left[1 \leftarrow \mathcal{A}^{f_P}\right] \leq \left(\delta^r\left(\Pr\left[1 \leftarrow \mathcal{A}^{f_Q}\right] + \mathcal{O}\left(\frac{q^3}{r}\right)\right)\right)^{\frac{\alpha-1}{\alpha}} + \mathcal{O}\left(\frac{q^3}{r}\right).$$

Small-Range Distribution [Zha12]

- Sample r independent values $\{y_i\}_{i\in[r]}$ according to P.
- These simulate the oracle O_{f_P}: $\forall x \in \mathcal{X}$, $\mathsf{O}_{f_P}(x) \leftarrow \{y_i\}_{i\in[r]}$
- Indistinguishable for $\mathcal{A}$ up to an error term of $\mathcal{O}(q^3/r)$

Lemma

Let P, Q be classical distributions over $\mathcal{Y}$ with $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$ and $\delta = R_\alpha(P\|Q)$, for $\alpha \in (1,\infty]$. For any $\mathcal{A}$ making at most q quantum queries

$$\Pr\left[1 \leftarrow \mathcal{A}^{f_P}\right] \leq \left(\delta^r\left(\Pr\left[1 \leftarrow \mathcal{A}^{f_Q}\right] + \mathcal{O}\left(\frac{q^3}{r}\right)\right)\right)^{\frac{\alpha-1}{\alpha}} + \mathcal{O}\left(\frac{q^3}{r}\right).$$

▷ Can circumvent problems, but explicit parameter comparison is needed

Adaptive Reprogramming [GHHM21]

In essence: “If the input to the oracle has enough min-entropy, then you can reprogram on-the-fly”.

Adaptive Reprogramming [GHHM21]

In essence: “If the input to the oracle has enough min-entropy, then you can reprogram on-the-fly”.

Lemma (Adaptive Reporgramming with Distribution Switching)

A distinguisher Dist *that queries an oracle R times with underlying distribution Q over $\mathcal{Y}$ or the uniform distribution $\mathcal{U}(\mathcal{Y})$, behaves similarly based on the statistical distance and Rényi divergence*

$$\left| \Pr\left[1 \leftarrow \mathsf{Dist}^{f_Q}\right] - \Pr\left[1 \leftarrow \mathsf{Dist}^{f_{\mathcal{U}(\mathcal{Y})}}\right] \right| \leq R \cdot \Delta(Q, \mathcal{U}(\mathcal{Y})) + \delta_{repr}$$

$$\Pr\left[1 \leftarrow \mathsf{Dist}^{f_{\mathcal{U}(\mathcal{Y})}}\right] \leq \left(R_\alpha(\mathcal{U}(\mathcal{Y}) \| Q)^R \Pr\left[1 \leftarrow \mathsf{Dist}^{f_{\mathcal{U}(\mathcal{Y})}}\right] \right)^{\frac{\alpha-1}{\alpha}} + \delta_{repr}$$

where δ_{repr} a term determined by the min-entropy of the input to the queries and the number of queries.

Applications

Our Motiviation

- Provable PQ secure Signal
- Essentially two viable solutions for deniable authentication:
  split-KEMs [CHN+24] and ring signatures [HKKP21, BFG+22, HKW25]
- Most efficient PQ ring signature proposals are only proven in the ROM
- Primary interest: linear-sized ring signatures

  (1) Ring Trapdoor Functions and (2) AOS-transform [AOS02]

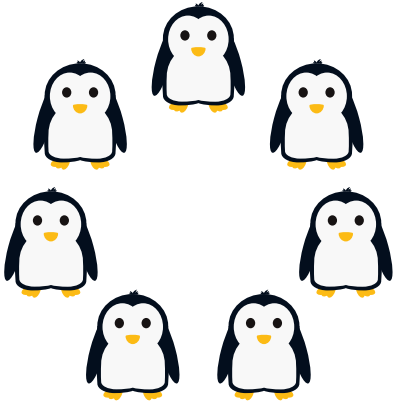
Example: Whistleblowers

Example: Whistleblowers

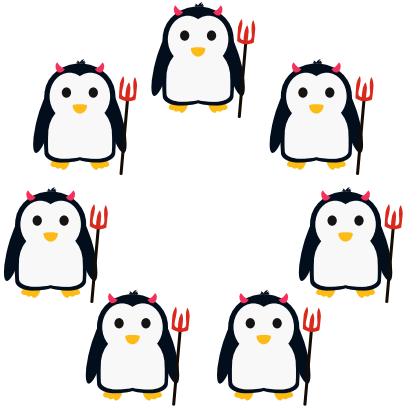
Example: Whistleblowers

Deniability and Authenticity

Ring Signatures



Ring Signatures



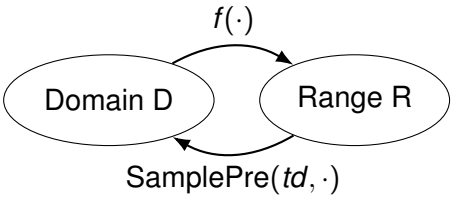
Ring Signature Algorithms

- $\mathsf{Stp}(1^n) \to \mathsf{p}$: define maximal ring size κ and public params p
- $\mathsf{KGen}(\mathsf{p}) \to (\mathsf{pk}, \mathsf{sk})$: generate a pair of public and secret key
- $\mathsf{Sign}(\rho, \mathsf{sk}, \mu) \to \sigma$ where $\rho = \{\mathsf{pk}_i\}_{i \in [N]}$: sign on behalf of the ring
- $\mathsf{Vf}(\rho, \mu, \sigma) \to \{0, 1\}$: verify a signature for a fixed ring

Ring Signatures from Ring Trapdoor Functions

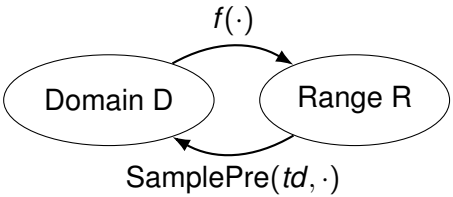
Trapdoor Functions and PSFs [GPV08]

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



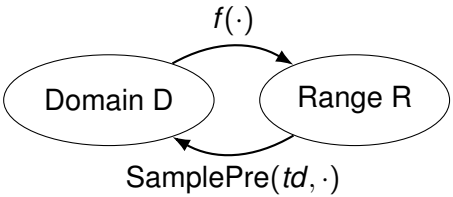
Trapdoor Functions and PSFs [GPV08]

- 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 [GPV08]

- 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

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[2]

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

Ring Trapdoor Functions for Ring Signatures

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

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

History-free proof using [BDF+11]:

- all hash queries: sample in D_ρ and apply f_ρ
- use randomness (deterministically derived from ρ, s, m) for domain sampling
- *only* works with statistical distance argument and does not need salt

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

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

History-free proof using [BDF+11]:

- all hash queries: sample in D_ρ and apply f_ρ
- use randomness (deterministically derived from ρ, s, m) for domain sampling
- *only* works with statistical distance argument and does not need salt

Adaptive reprogramming proof:

- *only* signature queries: sample in D_ρ and apply f_ρ
- works with statistical distance *and* Rényi divergence arguments

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

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)

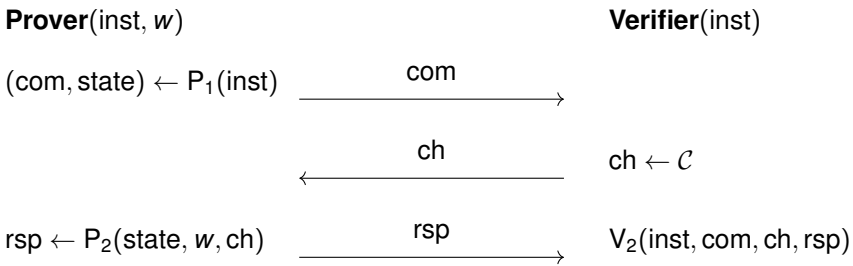
Explicit Construction

We looked at GANDALF [GJK24]

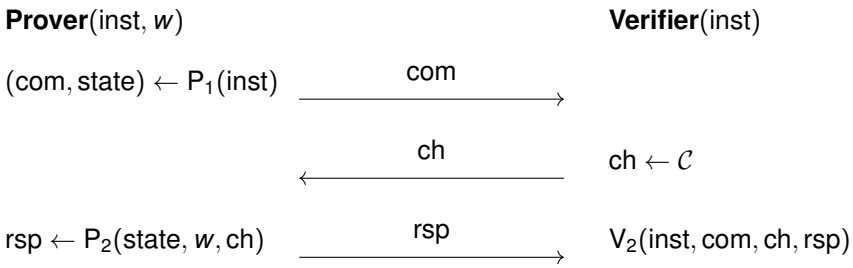
- lattice-based NTRU signature
- requires usage of Rényi divergence arguments
- we show that, as an example, GANDALF can be used to instantiate a ring trapdoor function yielding a QROM proof

Ring Signatures in the AOS Framework

Sigma Protocols

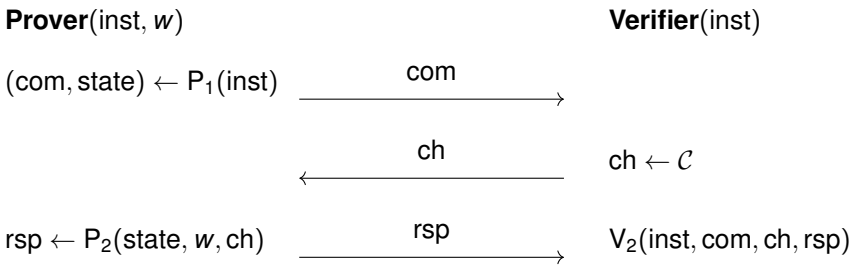


Sigma Protocols



- 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 :

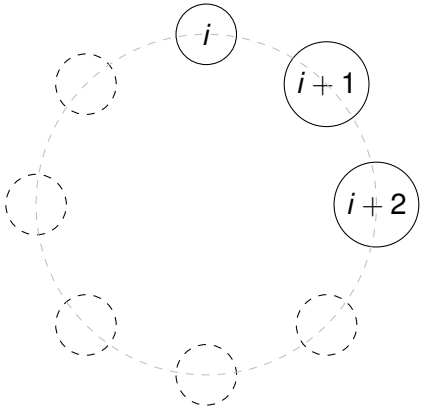
4 :

5 :

6 :

7 :

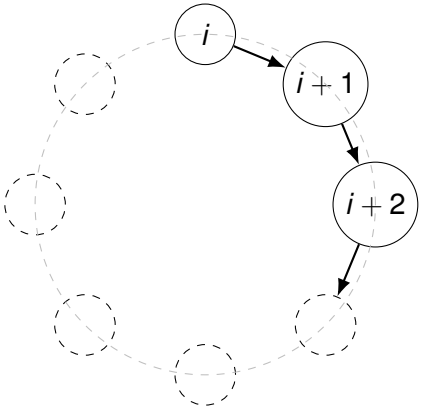
8 :



AOS Transform for Sigma Protocols

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

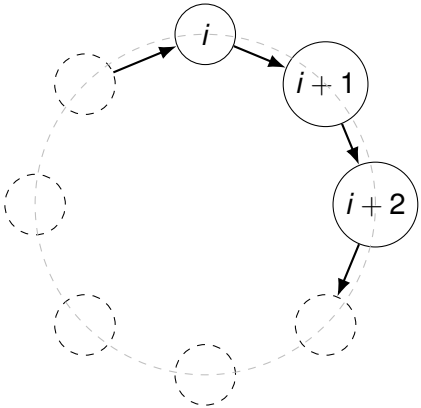
1 : $(\mathsf{com}_i, \mathsf{state}_i) \leftarrow \Sigma.\mathsf{P}_1(\mathsf{inst}_i)$
2 : **for** $j = i+1, \ldots, N, 1, \ldots, i-1$
3 : $\quad \mathsf{ch}_j \leftarrow \mathsf{H}(j, \rho, \mathsf{com}_{j-1}, \mu)$
4 : $\quad (\mathsf{com}_j, \mathsf{rsp}_j) \leftarrow \mathsf{Sim}(\mathsf{inst}_j,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



AOS Transform for Sigma Protocols

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

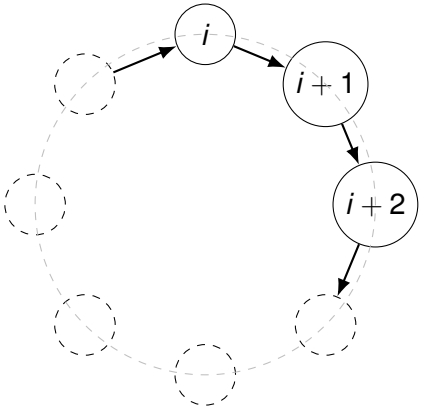
1 : $(\mathsf{com}_i, \mathsf{state}_i) \leftarrow \Sigma.\mathsf{P}_1(\mathsf{inst}_i)$
2 : **for** $j = i+1, \ldots, N, 1, \ldots, i-1$
3 : $\quad \mathsf{ch}_j \leftarrow \mathsf{H}(j, \rho, \mathsf{com}_{j-1}, \mu)$
4 : $\quad (\mathsf{com}_j, \mathsf{rsp}_j) \leftarrow \mathsf{Sim}(\mathsf{inst}_j,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



AOS Transform for Sigma Protocols

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

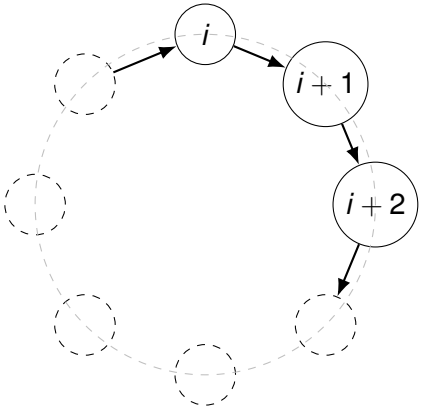
1 : $(\mathsf{com}_i, \mathsf{state}_i) \leftarrow \Sigma.\mathsf{P}_1(\mathsf{inst}_i)$
2 : **for** $j = i+1, \ldots, N, 1, \ldots, i-1$
3 : $\quad \mathsf{ch}_j \leftarrow \mathsf{H}(j, \rho, \mathsf{com}_{j-1}, \mu)$
4 : $\quad (\mathsf{com}_j, \mathsf{rsp}_j) \leftarrow \mathsf{Sim}(\mathsf{inst}_j,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

[3] multiplicative loss exponential in ring size

[4] Additive error term

A QROM-Proof for AOS

Goal: Reduce ring signature unforgeability to impersonation security

1. removing all signing queries:

[3] multiplicative loss exponential in ring size

[4] 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 [GHHM21] and HVZK simulator

[3] multiplicative loss exponential in ring size

[4] 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 [GHHM21] and HVZK simulator
   - To ensure the correctness of the final forgery: QROM collision resistance [CFHL21], witness-recovery and CUR

[3] multiplicative loss exponential in ring size

[4] 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 [GHHM21] and HVZK simulator
   - To ensure the correctness of the final forgery: QROM collision resistance [CFHL21], witness-recovery and CUR
2. reduce to impersonation adversary

[3] multiplicative loss exponential in ring size

[4] 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 [GHHM21] and HVZK simulator
   - To ensure the correctness of the final forgery: QROM collision resistance [CFHL21], witness-recovery and CUR
2. reduce to impersonation adversary
   - problem: the order of commitment and challenge for party i is not fixed...

[3] multiplicative loss exponential in ring size

[4] 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 [GHHM21] and HVZK simulator
   - To ensure the correctness of the final forgery: QROM collision resistance [CFHL21], 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 [DFM20], get an order of all queries from a forgery[3]

[3] multiplicative loss exponential in ring size

[4] 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 [GHHM21] and HVZK simulator
   - To ensure the correctness of the final forgery: QROM collision resistance [CFHL21], 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 [DFM20], get an order of all queries from a forgery[3]
   - alternative approach: assume commit-and-open sigma protocols: use framework [CFHL21] based on Zhandrys compressed oracle slightly adjusted in [DFMS22] [4]

[3] multiplicative loss exponential in ring size

[4] 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 ratio of challenges that can be answered for a fixed commitment without extraction being possible

Further Applications

Trapdoor-Based Signatures

- The NIST-candidate FALCON falls into this category of signatures.
- Currently its QROM argument relies on the GPV framework [GPV08], which uses the statistical distance in its argument
- The actual parameters of the construction are computed using the Rényi divergence
- In short: There is/was effectively no QROM security proof of FALCON.

In this work we did not fully analyze FALCON, but our tools should be sufficient.

Summary

Quantum oracles with Rényi divergence

- error term is required: purely multiplicative bounds impossible
- further applications to FALCON [FHK+18]

QROM proof for

- AOS-transform
  - General bound with multiplicative term of q^{2N}
  - Commit-and-open additive term
- Preimage sampleable ring trapdoor function

Summary

Quantum oracles with Rényi divergence

- error term is required: purely multiplicative bounds impossible
- further applications to FALCON [FHK+18]

QROM proof for

- AOS-transform
  - General bound with multiplicative term of q^{2N}
  - Commit-and-open additive term
- Preimage sampleable ring trapdoor function

eprint: 2026/293

arXiv: 2602.16268

References I

Masayuki Abe, Miyako Ohkubo, and Koutarou Suzuki.
1-out-of-n signatures from a variety of keys.
pages 415–432, 2002.

Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry.
Random oracles in a quantum world.
pages 41–69, 2011.

Aleksandrs Belovs.
Quantum algorithms for classical probability distributions.
arXiv preprint arXiv:1904.02192, 2019.

References II

- Jacqueline Brendel, Rune Fiedler, Felix Günther, Christian Janson, and Douglas Stebila.
  Post-quantum asynchronous deniable key exchange and the Signal handshake.
  pages 3–34, 2022.
- Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, and Tai-Ning Liao.
  On the compressed-oracle technique, and post-quantum security of proofs of sequential work.
  pages 598–629, 2021.
- Daniel Collins, Loïs Huguenin-Dumittan, Ngoc Khanh Nguyen, Nicolas Rolin, and Serge Vaudenay.
  K-waay: Fast and deniable post-quantum X3DH without ring signatures.
  2024.

References III

Jelle Don, Serge Fehr, and Christian Majenz.
The measure-and-reprogram technique 2.0: Multi-round fiat-shamir and more.
pages 602–631, 2020.

Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner.
Efficient NIZKs and signatures from commit-and-open protocols in the QROM.
pages 729–757, 2022.

References IV

- Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, Zhenfei Zhang, et al.
  Falcon: Fast-fourier lattice-based compact signatures over ntru.
  Submission to the NIST's post-quantum cryptography standardization process, 36(5):1–75, 2018.
- Alex B. Grilo, Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz.
  Tight adaptive reprogramming in the QROM.
  pages 637–667, 2021.
- Phillip Gajland, Jonas Janneck, and Eike Kiltz.
  Ring signatures for deniable AKEM: Gandalf's fellowship.
  pages 305–338, 2024.

References V

- Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan.
  Trapdoors for hard lattices and new cryptographic constructions.
  pages 197–206, 2008.
- Keitaro Hashimoto, Shuichi Katsumata, Kris Kwiatkowski, and Thomas Prest.
  An efficient and generic construction for Signal's handshake (X3DH): Post-quantum, state leakage secure, and deniable.
  pages 410–440, 2021.
- Keitaro Hashimoto, Shuichi Katsumata, and Thom Wiggers.
  Bundled authenticated key exchange: A concrete treatment of (post-quantum) signal's handshake protocol.
  Cryptology ePrint Archive, Paper 2025/040, 2025.

References VI

Mark Zhandry.
How to construct quantum random functions.
pages 679–687, 2012.