
DTU

Marvin Beckmann, Christian Majenz

Quantum Oracle Distribution Switching and Applications

Distinguishing two Distributions

Given q-query quantum access to an oracle whose outputs are i.i.d. according to P or Q, how well can we distinguish?

Our Results

Statistical Distance

- new explicit bound for switching between oracles

Our Results

Statistical Distance

- new explicit bound for switching between oracles

Rényi divergence with quantum access

- Positive and negative results regarding generalising classical results
- Special cases where classical results can survive fully

Our Results

Statistical Distance

- new explicit bound for switching between oracles

Rényi divergence with quantum access

- Positive and negative results regarding generalising classical results
- Special cases where classical results can survive fully

Applications: QROM analysis

- NIST-standard FALCON [FHK+18]
- Ring Signatures for Signal key exchange
  - preimage sampleble ring trapdoor functions like GANDALF [GJK24b]
  - AOS construction [AOS02] general and assuming commit-and-open sigma protocols [DFMS22]

Our Results

Statistical Distance

- new explicit bound for switching between oracles

Rényi divergence with quantum access

- Positive and negative results regarding generalising classical results
- Special cases where classical results can survive fully

Applications: QROM analysis

- NIST-standard FALCON [FHK+18]
- Ring Signatures for Signal key exchange
  - preimage sampleble ring trapdoor functions like GANDALF [GJK24b]
  - AOS construction [AOS02] general and assuming commit-and-open sigma protocols [DFMS22]

Classical Access to the Oracle

Statistical distance:

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

Classical Access to the Oracle

Statistical distance:

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

Rényi divergence (multiplicative):

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

Classical Access to the Oracle

Statistical distance:

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

Rényi divergence (multiplicative):

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

Which of these survive quantum access?

Quantum Bounds using the Statistical Distance

Bounds for Quantum Queries

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

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	$8q\sqrt{2\epsilon}$

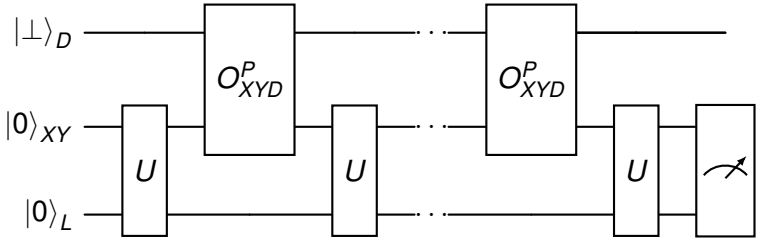
- The result is somewhat expected and lines up with quantum query complexity of the same problem formulation:
  - Constant advantage: achieved for $\Omega\left(\frac{1}{\sqrt{\epsilon}}\right)$ queries
  - [Bel19] shows that one needs $\Theta(\frac{1}{dh(P,Q)})$

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	$8q\sqrt{2\epsilon}$

- The result is somewhat expected and lines up with quantum query complexity of the same problem formulation:
  - Constant advantage: achieved for $\Omega\left(\frac{1}{\sqrt{\epsilon}}\right)$ queries
  - [Bel19] shows that one needs $\Theta(\frac{1}{dh(P,Q)})$
- [Bel19] uses the adversary method and obtains a bound at constant advantage with no explicit constants $\Rightarrow$ we can not use it to derive explicit parameters.

Quantum Oracle Queries in Compressed Oracle View

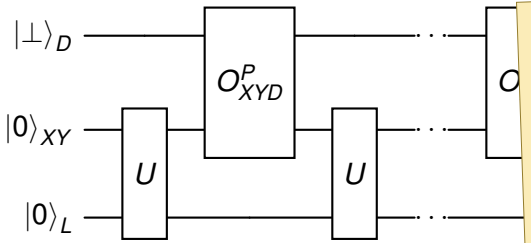


$$O^P_{XYD} = \sum_{x \in \mathcal{X}} |x\rangle\langle x|_X \otimes O^{P,x}_{YD_x}, \quad \text{with} \quad O^{P,x}_{YD_x} = F^P_{D_x}\,\mathrm{CNOT}_{YD_x}\,F^P_{D_x}$$

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

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

Quantum Oracle Queries in Compressed Oracle View



Adding $2q$ null terms:

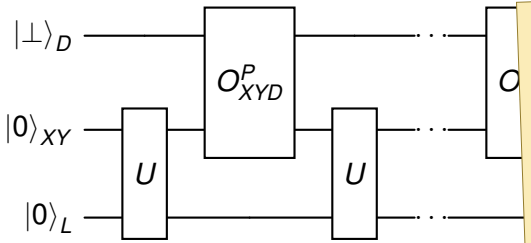
Bounds the trace distance of $\mathcal{A}$'s outputs as $4q\left\|F^P - F^Q\right\|_\infty$.

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

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

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

Quantum Oracle Queries in Compressed Oracle View



Adding $2q$ null terms:

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

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

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

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

$\left\|F^P - F^Q\right\|_\infty$ can be bounded as $\sqrt{8\Delta(P,Q)}$.

Quantum Bounds using the Rényi Divergence

Rényi Divergence

Definition

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

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

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

Rényi Divergence

Probability preservation and data processing:

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

Rényi Divergence

Probability preservation and data processing:

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

For q independent samples the divergence tensorizes:

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

Quantum Analog of the Classical Rényi divergence Relation

Quantum Analog of the Classical Rényi divergence Relation

Are such multiplicative bounds even possible?

Quantum Analog of the Classical Rényi divergence Relation

Are such multiplicative bounds even possible?

Theorem

For all distributions $P \neq Q$ on $\mathcal{Y}$ with $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$ and any fixed $\gamma > 0$, there exists an algorithm $\mathcal{A}$ making only 2 quantum queries with

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

Proof Sketch Multiplicative Impossibility

Run Deutsch-Jozsa without promise and from the original oracle, construct a new oracle whose underlying function is balanced in expectation for f_Q, but not for f_P and consider the output “constant”.

Proof Sketch Multiplicative Impossibility

Run Deutsch-Jozsa without promise and from the original oracle, construct a new oracle whose underlying function is balanced in expectation for f_Q, but not for f_P and consider the output "constant".

Fix $y_0 := \arg\max_y \frac{P(y)}{Q(y)}$ and define "imbalance" as $Z_u := \sum_{x \in \{0,1\}^{1+n}} (-1)^{u(x)}$.

- From $f\colon \mathcal{X} \to \mathcal{Y}$ build a Boolean $g[f]$ with $g[f](x) = 0 \iff f(x) = y_0$, then pad to $h[f]\colon \{0,1\}^{1+n} \to \{0,1\}$ such that under f_Q: $h[f]$ is *balanced in expectation*.

Proof Sketch Multiplicative Impossibility

Run Deutsch-Jozsa without promise and from the original oracle, construct a new oracle whose underlying function is balanced in expectation for f_Q, but not for f_P and consider the output "constant".

Fix $y_0 := \arg\max_y \frac{P(y)}{Q(y)}$ and define "imbalance" as $Z_u := \sum_{x \in \{0,1\}^{1+n}} (-1)^{u(x)}$.

- From $f \colon \mathcal{X} \to \mathcal{Y}$ build a Boolean $g[f]$ with $g[f](x) = 0 \iff f(x) = y_0$, then pad to $h[f] \colon \{0,1\}^{1+n} \to \{0,1\}$ such that under f_Q: $h[f]$ is *balanced in expectation*.
- Run Deutsch-Jozsa on $h[f]$ and measure if the outcome is $|+\rangle^{\otimes(1+n)}$.

Proof Sketch Multiplicative Impossibility

The acceptance probability is

$$\Pr\left[1 \leftarrow \mathcal{A}^f\right] = \mathbb{E}_f\left[\frac{Z_{h[f]}^2}{2^{2(1+n)}}\right] = \frac{\mathbb{E}_f[Z_{h[f]}]^2 + \mathrm{Var}_f(Z_{h[f]})}{2^{2(1+n)}}$$

Proof Sketch Multiplicative Impossibility

The acceptance probability is

$$\Pr\left[1 \leftarrow \mathcal{A}^f\right] = \mathbb{E}_f\left[\frac{Z_{h[f]}^2}{2^{2(1+n)}}\right] = \frac{\mathbb{E}_f[Z_{h[f]}]^2 + \mathrm{Var}_f(Z_{h[f]})}{2^{2(1+n)}}$$

and for our parameters it holds that

$$\mathbb{E}_{f_Q}[Z_{h[f_Q]}] \approx^* 0, \qquad \mathbb{E}_{f_P}[Z_{h[f_P]}] = 2^{1+n}\big(P(y_0) - Q(y_0)\big).$$

Proof Sketch Multiplicative Impossibility

The acceptance probability is

$$\Pr\left[1 \leftarrow \mathcal{A}^f\right] = \mathbb{E}_f\left[\frac{Z_{h[f]}^2}{2^{2(1+n)}}\right] = \frac{\mathbb{E}_f[Z_{h[f]}]^2 + \mathrm{Var}_f(Z_{h[f]})}{2^{2(1+n)}}$$

and for our parameters it holds that

$$\mathbb{E}_{f_Q}[Z_{h[f_Q]}] \approx^* 0, \qquad \mathbb{E}_{f_P}[Z_{h[f_P]}] = 2^{1+n}\big(P(y_0) - Q(y_0)\big).$$

and the variance is

$$\mathrm{Var}_f(Z_{h[f]}) = 2^{2+n} \cdot \begin{cases} P(y_0)(1 - P(y_0)) & \text{if } f = f_P \\ Q(y_0)(1 - Q(y_0)) & \text{if } f = f_Q \end{cases}$$

Proof Sketch Multiplicative Impossibility

The acceptance probability is

$$\Pr\left[1 \leftarrow \mathcal{A}^f\right] = \mathbb{E}_f\left[\frac{Z_{h[f]}^2}{2^{2(1+n)}}\right] = \frac{\mathbb{E}_f[Z_{h[f]}]^2 + \mathrm{Var}_f(Z_{h[f]})}{2^{2(1+n)}}$$

and for our parameters it holds that

$$\mathbb{E}_{f_Q}[Z_{h[f_Q]}] \approx^* 0, \qquad \mathbb{E}_{f_P}[Z_{h[f_P]}] = 2^{1+n}\big(P(y_0) - Q(y_0)\big).$$

and the variance is

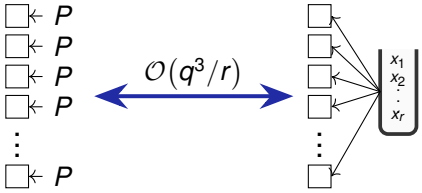
$$\mathrm{Var}_f(Z_{h[f]}) = 2^{2+n} \cdot \begin{cases} P(y_0)(1-P(y_0)) & \text{if } f = f_P \\ Q(y_0)(1-Q(y_0)) & \text{if } f = f_Q \end{cases}$$

$$\frac{\Pr\left[1 \leftarrow \mathcal{A}^{f_P}\right]}{\Pr\left[1 \leftarrow \mathcal{A}^{f_Q}\right]^\gamma} = \Theta(2^{n\gamma}).$$

Can we get “almost purely” Multiplicative Bounds?

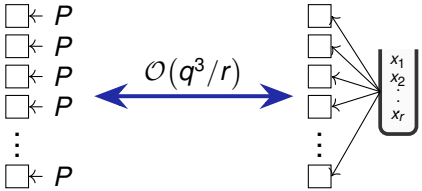
By assuming a small additional additive error, we can use the small-range distribution results from [Zha12].

Small-Range Distribution [Zha12]

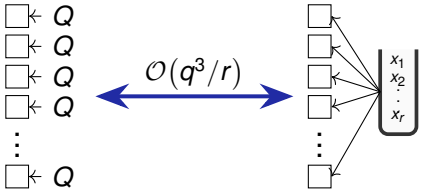


$x_1, \ldots, x_r \sim P$

Small-Range Distribution [Zha12]

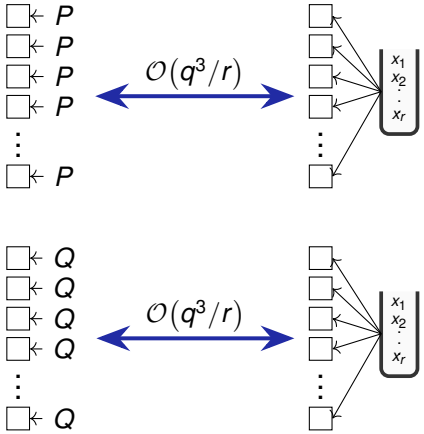


$x_1, \ldots, x_r \sim P$



$x_1, \ldots, x_r \sim Q$

Small-Range Distribution [Zha12]



$x_1, \ldots, x_r \sim P$

mult. loss:
$R_\alpha(P\|Q)^r$

$x_1, \ldots, x_r \sim Q$

Replacing the Entire Oracle with Rényi Divergence

Lemma

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

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

Replacing the Entire Oracle with Rényi Divergence

Lemma

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

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

▷ Circumvents the impossibility, but the additive $\mathcal{O}(q^3/r)$ forces r large and explicit parameter comparison is needed.

Implications for the Rényi Divergence

Purely multiplicative bounds are impossible.

Small-range distributions rescue a bound, but at the expense of an additive error, introducing a tradeoff.

Implications for the Rényi Divergence

Purely multiplicative bounds are impossible.

Small-range distributions rescue a bound, but at the expense of an additive error, introducing a tradeoff.

Alternative: if we can avoid having to replace the entire oracle, and only do the replacement for queries where the input has high min-entropy, then we can reprogram on the fly instead.

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 Reprogramming 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*

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

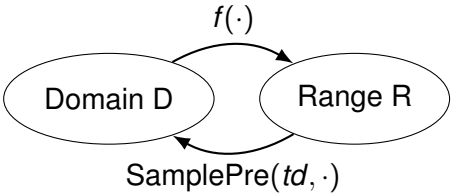
$$\Pr\left[1 \leftarrow \mathsf{Dist}^{f_{\mathcal{U}(\mathcal{Y})}}\right] \leq \left(R_\alpha(\mathcal{U}(\mathcal{Y})\|Q)^R \Pr\left[1 \leftarrow \mathsf{Dist}^{f_Q}\right]\right)^{\frac{\alpha-1}{\alpha}} + \delta_{repr}$$

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

Applications

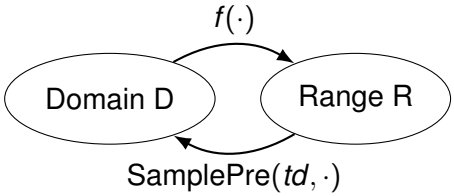
Trapdoor Functions and Preimage Sampleable Functions (PSFs)

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



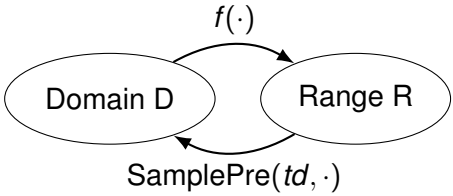
Trapdoor Functions and Preimage Sampleable Functions (PSFs)

- f is one-way
- SamplePre returns preimages under f
- PSFs [GPV08]: $\exists$ a distribution D on D
  - $f(d) \approx \mathcal{U}(\mathrm{R})$ where $d \leftarrow D$
  - SamplePre(td, r) is indistinguishable from $d \leftarrow D$ conditioned on $f(d) = r$



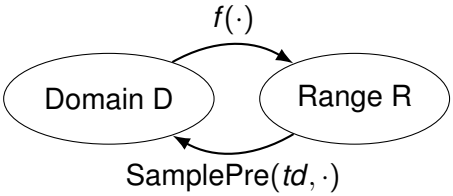
Trapdoor Functions and Preimage Sampleable Functions (PSFs)

- f is one-way
- SamplePre returns preimages under f
- PSFs [GPV08]: $\exists$ a distribution D on D
  - $f(d) \approx \mathcal{U}(\mathrm{R})$ where $d \leftarrow D$
  - SamplePre(td, r) is indistinguishable from $d \leftarrow D$ conditioned on $f(d) = r$



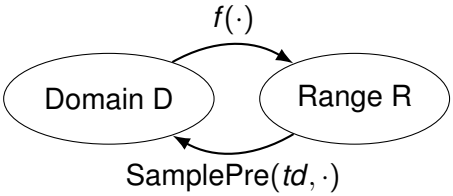
Trapdoor Functions and Preimage Sampleable Functions (PSFs)

- f is one-way
- SamplePre returns preimages under f
- PSFs [GPV08]: $\exists$ a distribution D on D
  - $f(d) \approx \mathcal{U}(\mathrm{R})$ where $d \leftarrow D$
  - SamplePre(td, r) is indistinguishable from $d \leftarrow D$ conditioned on $f(d) = r$
- The NIST standard FALCON argues $f(d) \approx \mathcal{U}(\mathrm{R})$ via the Rényi divergence for tighter parameters [FHK+18, GJK24a].



Trapdoor Functions and Preimage Sampleable Functions (PSFs)

- f is one-way
- SamplePre returns preimages under f
- PSFs [GPV08]: $\exists$ a distribution D on D
  - $f(d) \approx \mathcal{U}(\mathrm{R})$ where $d \leftarrow D$
  - SamplePre(td, r) is indistinguishable from $d \leftarrow D$ conditioned on $f(d) = r$
- The NIST standard FALCON argues $f(d) \approx \mathcal{U}(\mathrm{R})$ via the Rényi divergence for tighter parameters [FHK+18, GJK24a].
- Previous QROM proofs assumed statistical-distance closeness, which is insufficient for FALCON.



Theorem 5 (SUF-CMA of CoreFalcon+). *For any adversary $\mathcal{A}$ against the* SUF-CMA *security of* CoreFalcon+*, making at most q_s signing queries and q_H to the QROM, there exists an adversary $\mathcal{B}$ against C_F-$\mathcal{R}$-NTRU-SPISIS, an adversary $\mathcal{C}$ against $\mathcal{R}$-NTRU-ISIS and an adversary $\mathcal{D}$ against t-$\mathcal{R}$-NTRU-ISIS, s.t. for all $C_s, t \in \mathbb{N}^{\geq 1}, \alpha_\mathrm{u}, \alpha_\mathrm{p} \in \mathbb{R}^{>1}$:*

$$\mathsf{Adv}^{\text{SUF-CMA}}_{\mathcal{A},\text{CoreFalcon}^+,d_s}(\lambda) \leq \left(r^{C_r}_{\alpha_\mathrm{u}}\left(r^{C_s}_{\alpha_\mathrm{p}}(\epsilon + \epsilon')\right)^{\frac{\alpha_\mathrm{p}-1}{\alpha_\mathrm{p}}}\right)^{\frac{\alpha_\mathrm{u}-1}{\alpha_\mathrm{u}}} + \delta$$

where ϵ and the runtimes of $\mathcal{B}$ and $\mathcal{D}$ are bounded in Table 1 and the other parameters are defined in Table 2.

Assumption	Reduction Runtime	Bound on ϵ
single-target	$\mathsf{poly}(\lambda, C_s, q_\mathrm{H})$	$(2q_\mathrm{H}+2C_s+3)^2\mathsf{Adv}^{\mathcal{R}\text{-NTRU-ISIS}}_{\mathrm{C}_\mathrm{F},1,q,\alpha,\beta}(\lambda)$
multi-target	$\mathsf{poly}(\lambda, C_s, t)$	$\mathsf{Adv}^{\text{t-}\mathcal{R}\text{-NTRU-ISIS}}_{\mathcal{D},1,q,\alpha,\beta}(\lambda) + \frac{14(q_\mathrm{H}+1)^3}{t}$

Summary

- Rényi divergence: purely multiplicative bounds are impossible, an error term is required
- Statistical distance: explicit switching bound via the compressed oracle
- application: first QROM treatment of FALCON's Rényi-based sampler [FHK+18]

Summary

- Rényi divergence: purely multiplicative bounds are impossible, an error term is required
- Statistical distance: explicit switching bound via the compressed oracle
- application: first QROM treatment of FALCON's Rényi-based sampler [FHK+18]

Also complementary QROM proofs for ring signatures via the AOS-transform, and preimage sampleable ring trapdoor functions

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

- Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner.
  Online-extractability in the quantum random-oracle model.
  pages 677–706, 2022.
- 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.

References III

- Phillip Gajland, Jonas Janneck, and Eike Kiltz.
  A closer look at falcon.
  Cryptology ePrint Archive, Report 2024/1769, 2024.
- Phillip Gajland, Jonas Janneck, and Eike Kiltz.
  Ring signatures for deniable AKEM: Gandalf's fellowship.
  pages 305–338, 2024.
- Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan.
  Trapdoors for hard lattices and new cryptographic constructions.
  pages 197–206, 2008.
- Mark Zhandry.
  How to construct quantum random functions.
  pages 679–687, 2012.