DTU Compute
Department of Applied Mathematics and Computer Science

Quantum Oracle Distribution Switching and Applications to Falcon and Ring Signatures

Marvin Beckmann[1], Christian Majenz[1]

[1] {mabeck, chmaj}@dtu.dk, Technical University of Denmark, DTU Compute, Kgs. Lyngby, Denmark

Given q-query access to two classical distributions P and Q via i.i.d. functions, how do

$$\Pr\left[1 \leftarrow \mathcal{A}^{f_P}\right] \quad \text{and} \quad \Pr\left[1 \leftarrow \mathcal{A}^{f_Q}\right]$$

compare when given classical or quantum access to the oracle. Classically, the statistical distance yields

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

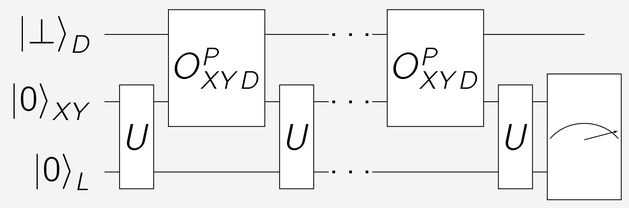
and the Rényi divergence yields

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

1 Statistical Distance

Boneh et al. [2]	$\mathcal{O}(q^2\sqrt{\Delta(P,Q)})$
Zhandry [5]	$\mathcal{O}(q^{1.5}\sqrt{\Delta(P,Q)})$
Our Work	$8q\sqrt{2\Delta(P,Q)}$

Aligns with quantum query complexity results: for constant advantage $\Theta(1/\mathrm{dh}(P,Q))$ queries are needed [1]. Our result implies constant advantage with $\Omega(1/\sqrt{\Delta(P,Q)})$ queries.
First, view the entire algorithm $\mathcal{A}$ with oracle access via the compressed oracle formalism.



The operator O^P_{XYD} performs the oracle query for each x independently, where F^P puts the state into the correct superposition according to P.

$$F^P = |\perp\rangle(\langle\phi_P| - \langle\perp|) + |\phi_P\rangle(\langle\perp| - \langle\phi_P|) + \mathbb{1},$$

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

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

Then, add $2q$ null-terms, bound the trace distance of $\mathcal{A}$'s outputs as $4q\left\|F^P - F^Q\right\|_\infty$, and $\left\|F^P - F^Q\right\|_\infty$ can be bounded as $\sqrt{8\Delta(P,Q)}$.

2 Rényi Divergence

Using the Deutsch-Jozsa (DJ) algorithm we obtain an algorithm such that the following holds.

Theorem 1. *For all distributions $P \neq Q$ with $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$ and any fixed $\gamma \in (0,1]$, there exists an algorithm $\mathcal{A}$ such that*

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

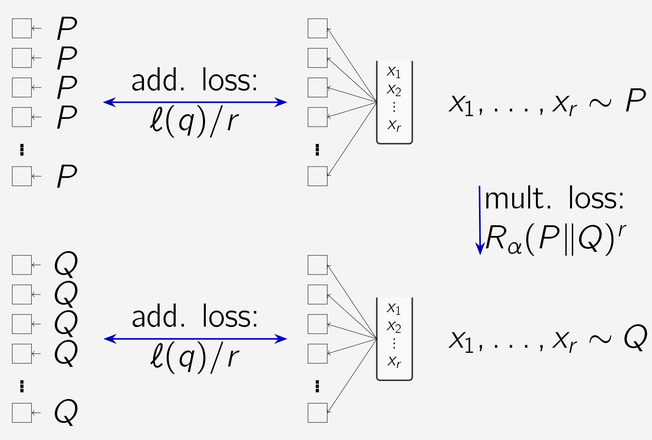
Use DJ without the promise, and construct from f_P or f_Q a function that is balanced in expectation when based on f_Q, and unbalanced for f_P; only using 2 queries to f_P or f_Q. $\Pr\left[1 \leftarrow \mathcal{A}^f\right]$ converges to a constant for f_P (output of DJ is "constant" with constant probability), and for f_Q it behaves as $\Theta(2^{-n})$. The ratio with γ as the exponent in the denominator behaves as $\Theta(2^{\gamma n})$. Therefore, when given quantum access to the oracle, no *purely multiplicative* bound is possible.

Small-Range Distributions [5]

Proposition 1. *Let P, Q be classical distributions 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 $\Pr\left[1 \leftarrow \mathcal{A}^{f_P}\right]$ is bounded as*

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

where $\ell(q) = \pi^2(2q)^3/6 < 14q^3$.



Adaptive Reprogramming If we only have to switch from a uniform distribution to Q at positions with high input entropy, then we can use adaptive reprogramming tools [4, Proposition 2].

Lemma 1. *(simplified) Let $\mathcal{D}$ be any distinguisher, issuing q (quantum) queries to the oracle and R reprogramming instructions. Then*

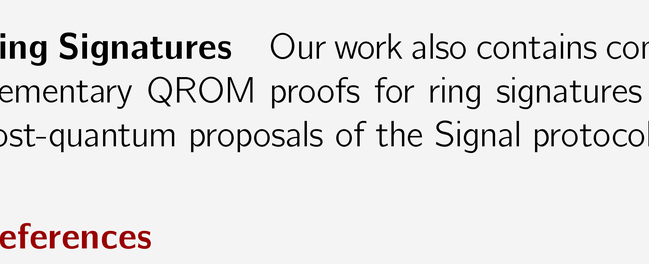
$$\left|\Pr\left[1 \leftarrow \mathcal{D}^{\mathsf{O}}\right] - \Pr\left[1 \leftarrow \mathcal{D}^{\mathsf{O}_{Q,R}}\right]\right| \leq R\epsilon + \delta_{repr}$$

$$\Pr\left[1 \leftarrow \mathcal{D}^{\mathsf{O}}\right] \leq \left(r_\alpha^R \cdot \Pr\left[1 \leftarrow \mathcal{D}^{\mathsf{O}_{Q,R}}\right]\right)^{\frac{\alpha-1}{\alpha}} + \delta_{repr}$$

where $\alpha \in (1,\infty], \epsilon = \Delta(Q, \mathcal{U}(\mathcal{Y})), r_\alpha = R_\alpha(\mathcal{U}(\mathcal{Y})\|Q), \delta_{repr} = \frac{3R}{2}\sqrt{q \cdot p_{\max}}$ with $p_{\max}$ being the max input probability.

3 Applications

NIST Standard Falcon (FN-DSA) [3]



$$\mathrm{Sign}(td, m) := \mathrm{SamplePre}(\mathrm{td}, H(m))$$

$$\mathrm{Vfy}(f, m, \sigma) := [[f(\sigma) = H(m)]]$$

Simulating signatures: $f(d) \sim \mathcal{U}(R)$ where $d \leftarrow D$. In Falcon, currently the NIST PQ standard with the smallest signatures, this switch uses the Rényi divergence, and not the statistical distance. Previous QROM proofs with the statistical distance yield insufficient security levels.

Ring Signatures Our work also contains complementary QROM proofs for ring signatures in post-quantum proposals of the Signal protocol.

References

[1] Belovs, A.: Quantum algorithms for classical probability distributions
[2] Boneh, D., et al.: Random oracles in a quantum world
[3] Fouque, P.A., et al.: Falcon: Fast-fourier lattice-based compact signatures over ntru
[4] Grilo, A.B., et al.: Tight adaptive reprogramming in the QROM
[5] Zhandry, M.: How to construct quantum random functions

ePrint 2026/293
arXiv 2602.16268

DTU Compute
Department of Applied Mathematics and Computer Science
DTU Compute
Department of Applied Mathematics and Computer Science
DTU Compute
Department of Applied Mathematics and Computer Science
DTU Compute
Department of Applied Mathematics and Computer Science