CONJURA · OPEN PROBLEM

A Constant Number of Luby–Rackoff Rounds Is Indistinguishable from a Random Invertible Permutation

Random round functions, superposition queries in both directions

Status. Statement: AI-written from Dominique Unruh, *Towards Compressed Permutation Oracles*, IACR Cryptology ePrint Archive (preprint, University of Tartu) 2023, not yet checked by a human. Open for $r \geq 5$. Three rounds fail already classically (p. 14, fn. 22) and four rounds are ruled out in the quantum setting by a chosen-ciphertext attack on Feistel ciphers (p. 3, fn. 3); the paper names five rounds as a round count nothing excludes. The paper reports that the one published proof of the weaker forward-only statement for four rounds contains a flaw, with a fix work in progress. The paper proves nothing about Luby–Rackoff itself; Theorem 1 only shows that a proof via its compressed permutation oracle would additionally establish the oracle's soundness for free.

Category. *Symmetric-Key Primitives.*

Conjecture (informal). *The classical Luby–Rackoff theorem says that four rounds of the Feistel construction, built from independent random round functions on n-bit strings, give a permutation on $2n$-bit strings that no efficient adversary can distinguish from a uniformly random permutation, even when it may query in both directions. Against quantum adversaries with superposition access this is known to fail at four rounds: there is an attack. Nothing rules out that a few more rounds suffice, and this is the natural quantum analogue of the classical theorem, but no number of rounds has ever been proved to work. The obstruction is a missing proof technique rather than a missing idea: the target is indistinguishability from an invertible random permutation, and the quantum lazy-sampling method that would make such an argument routine has never been extended from random functions to permutations that can be inverted. The one published claim in this direction proves a weaker statement — forward queries only — and its proof has a flaw. The conjecture is that some constant number of rounds does work, with five being the first candidate not ruled out.*

1 The setting

The Luby–Rackoff theorem [LR88] is the textbook route from a pseudorandom function to a strong pseudorandom permutation: four Feistel rounds with independent random round functions are indistinguishable from a uniformly random invertible permutation, given classical access in both directions. Against quantum adversaries with superposition access the picture is different. Four rounds are broken: there is a quantum chosen-ciphertext attack on Feistel ciphers [IHMSI19]. A published claim that four-round Luby–Rackoff is a qPRP [HI19] concerns the weaker forward-only notion, and the paper reports that its proof contains a flaw with a fix in progress [HI21]. So even the non-strong case is not on firm ground, and for the strong case nothing at all is known.

The paper identifies why. To establish the strong version it suffices to show that Luby–Rackoff with uniformly random round functions is indistinguishable from a random permutation given queries in both directions — an information-theoretic statement about superposition query complexity, and the form in which the

conjecture below is stated. The natural tool would be the quantum analogue of lazy sampling: Zhandry's compressed oracle [Zha19] makes exactly this kind of argument routine when the ideal object is a random *function*, by giving the proof an explicit record of all queries made so far and letting one argue by an invariant on that record. But the technique has resisted every attempt at being ported to invertible permutations, because a random permutation does not have independently distributed outputs; and the escape route available in the forward-only setting — replacing the permutation by a random function [Zha15] — is exactly what breaks when the adversary can invert. This is the paper's motivation for defining a compressed permutation oracle, and its main theorem yields a two-for-one: proving that Luby–Rackoff is indistinguishable from that oracle would give both the conjecture below and, for free, the soundness of the oracle methodology itself. Note also that random invertible permutations are known to be efficiently simulatable from quantum one-way functions [Zha16]; the paper's point is that this gives no technique for analysing schemes that use a qPRP (p. 4).

Progress to date. The paper contributes a route rather than a partial result: by its Theorem 1, showing that Luby–Rackoff (as a permutation-construction from random round functions) is indistinguishable from the compressed permutation oracle would yield both this statement and the soundness of the compressed permutation oracle methodology. It also records the negative data points: four rounds do not suffice in the quantum setting, three rounds fail already classically, and the claimed four-round forward-only proof is flawed with a fix reported as work in progress.

Why it matters. This is the missing quantum half of one of the foundational theorems of symmetric cryptography, and the paper treats it as the motivating application for the whole compressed-permutation-oracle programme. A proof for any constant number of rounds would give the first information-theoretic strong-qPRP result for a natural construction and would validate a proof technique for invertible random permutations, which is precisely what is absent today. It also has direct consequences for how one may argue about block ciphers in post-quantum proofs, where the standard step of replacing a strong PRP by a random invertible permutation currently has no accompanying toolbox. A refutation for small r would extend the existing quantum Feistel attacks and sharpen where the classical

intuition breaks.

Why it is clean. The construction is a two-line recursion over independent uniformly random round functions, the target is indistinguishability from a uniformly random permutation, and the statement is information-theoretic with no assumption and no idealized-model apparatus. Both experiments are standard XOR query unitaries. The classical answer is textbook, and the quantum status is pinned down at $r = 4$ by a published attack, so an attacker of the problem knows exactly where the boundary currently lies.

2 Notation and parameters

Fix $n \in \mathbb{N}$. Write $\oplus$ for bitwise XOR and $u\|v$ for concatenation; every element of $\{0,1\}^{2n}$ is written uniquely as $x_L\|x_R$ with $x_L, x_R \in \{0,1\}^n$. Let Func_n be the set of all functions $\{0,1\}^n \to \{0,1\}^n$ and $\mathrm{Perm}(\{0,1\}^{2n})$ the set of bijections $\{0,1\}^{2n} \to \{0,1\}^{2n}$.

For a permutation G on $\{0,1\}^{2n}$, U_G is the unitary with $U_G|u\rangle|v\rangle = |u\rangle|v \oplus G(u)\rangle$ for $u, v \in \{0,1\}^{2n}$; superposition access to G means black-box access to U_G.

An oracle algorithm A with two oracles alternates unitaries on its own registers with invocations of either oracle; its *query count* is the total number of invocations, and $\Pr[A^{O_1,O_2} \Rightarrow 1]$ is the probability that measuring its output register yields 1.

A function $\mu : \mathbb{N} \to \mathbb{R}_{\geq 0}$ is *negligible* if for every $c > 0$ there is n_0 with $\mu(n) < n^{-c}$ for all $n \geq n_0$.

Parameters.

- r — the number of Feistel rounds. $r \leq 3$ fails already classically (p. 14, fn. 22) and $r = 4$ is ruled out by a known quantum chosen-ciphertext attack (p. 3, fn. 3); the paper offers five rounds as an example of a count nothing excludes.
- n — bit length of each half; the round functions map $\{0,1\}^n$ to $\{0,1\}^n$ and the permutation acts on $\{0,1\}^{2n}$.
- p — polynomial bounding the adversary's total number of forward and inverse superposition queries.

3 The conjecture

Definition 1 (Luby–Rackoff construction). For $f \in \mathrm{Func}_n$ let $\Psi_f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ be the Feistel round

$$\Psi_f(x_L \| x_R) \;:=\; x_R \,\|\, (x_L \oplus f(x_R)),$$

which is a permutation with $\Psi_f^{-1}(u\|v) = (v \oplus f(u))\|u$. For $r \geq 1$ and $f_1, \ldots, f_r \in \mathrm{Func}_n$, the *r-round Luby–Rackoff construction* is

$$\mathrm{LR}_{f_1,\ldots,f_r} \;:=\; \Psi_{f_r} \circ \cdots \circ \Psi_{f_1} \;\in\; \mathrm{Perm}(\{0,1\}^{2n}).$$

Conjecture 1 (constant-round Luby–Rackoff). *There exists $r \in \mathbb{N}$ such that for every polynomial p there is a negligible function μ with the following property. For all $n \in \mathbb{N}$ and every oracle algorithm A with query count at most $p(n)$,*

$$\Big|\Pr\big[A^{U_\Psi, U_{\Psi^{-1}}} \Rightarrow 1 \;:\; f_1, \ldots, f_r \xleftarrow{\$} \mathrm{Func}_n,\ \Psi := \mathrm{LR}_{f_1,\ldots,f_r}\big] - \Pr\big[A^{U_\pi, U_{\pi^{-1}}} \Rightarrow 1 \;:\; \pi \xleftarrow{\$} \mathrm{Perm}(\{0,1\}^{2n})\big]\Big| \;\leq\; \mu(n),$$

where the f_i are drawn independently and uniformly, and $\mathrm{LR}_{f_1,\ldots,f_r}$ is as in Definition 1.

4 Bibliography

[HI19] A. Hosoyamada, T. Iwata. *4-Round Luby-Rackoff Construction is a qPRP.* Lecture Notes in Computer Science, pages 145–174, Springer, 2019.

[HI21] A. Hosoyamada, T. Iwata. *Personal communication*, 2021.

[IHMSI19] G. Ito, A. Hosoyamada, R. Matsumoto, Y. Sasaki, T. Iwata. *Quantum Chosen-Ciphertext Attacks Against Feistel Ciphers.* Topics in Cryptology — CT-RSA 2019, pages 391–411, Springer, 2019.

[LR88] M. Luby, C. Rackoff. *How to Construct Pseudorandom Permutations from Pseudorandom Functions.* SIAM Journal on Computing 17.2, pages 373–386, 1988.

[Zha15] M. Zhandry. *A note on the quantum collision and set equality problems.* Quantum Inf. Comput. 15.7&8, pages 557–567, 2015.

[Zha16] M. Zhandry. *A Note on Quantum-Secure PRPs.* Cryptology ePrint Archive, Report 2016/1076, 2016.

[Zha19] M. Zhandry. *How to Record Quantum Queries, and Applications to Quantum Indifferentiability.* Crypto 2019, volume 11693 of LNCS, pages 239–268, Springer, 2019.