AICR · OPEN PROBLEM

Post-Quantum Minimality of One-Way Functions Under Non-Black-Box Security Reductions

The classical implication is proved without a black-box reduction between the security games

Status. Statement: AI-written from Sam Buxbaum and Mohammad Mahmoody, *A Note on the Minimality of One-Way Functions in Post-Quantum Cryptography*, IACR Communications in Cryptology, Vol. 1, No. 4, 2024 (received 2024-10-09, accepted 2024-12-03; also Cryptology ePrint Archive, Report 2024/2095, 2024), not yet checked by a human. Settled affirmatively whenever the classical implication from Q to one-way functions is witnessed by a black-box reduction between the two security games, with the implementation reduction arbitrary, for both uniform and non-uniform quantum adversaries and also for reductions that assume a deterministic adversary; open when that security implication is not witnessed by such a black-box reduction, and the paper takes no position on which way it goes.

Category. *Foundations.*

Conjecture (informal). *In classical cryptography, one-way functions are the minimal assumption: almost every basic primitive implies them. Post-quantum cryptography keeps the protocols classical but lets the attacker be quantum, and it is not obvious that the classical implications survive, because a classical proof that a primitive implies one-way functions typically works by taking an attacker on the one-way function and running it, repeatedly and from rewound states, to attack the primitive. Rewinding a quantum attacker is not generally possible. This paper shows the implications do survive whenever the classical proof is a black-box reduction between the two security games and the target primitive's security is defined by a two-message challenge-response game, which is the case for one-way functions; the argument replaces the quantum attacker by an equivalent stateful one that answers repeated questions consistently, so that rewinding it gains the reduction nothing and it becomes indistinguishable from an inefficient classical attacker the reduction was designed for. What the paper does not settle is the case where the classical implication is not proved by such a black-box reduction: the reduction may inspect the code of the attacker, and while a uniform quantum attacker is still generated by classical code, its state — and, in the non-uniform case, its quantum advice — has no classical description. The paper does not say why this case resists; it simply records it as unresolved. The question is whether the classical implication still lifts, so that one-way functions are minimal for post-quantum cryptography with no restriction on how the classical proof was carried out.*

1 The setting

One-way functions are the minimal assumption of classical cryptography: Impagliazzo and Luby showed that identification protocols, symmetric-key encryption, commitments and coin flipping all imply them [IL89], and the standard way such implications are established is a black-box reduction, which uses the primitive and the adversary as oracles and therefore relativizes [RTV04]. Non-black-box security reductions, which exploit the code of the adversary, exist but are comparatively rare [Bar01].

Quantum cryptography appears to have a different assumption hierarchy: there are oracles relative to which pseudorandom

quantum states exist while **BQP** = **QMA** [Kre21], and a classical oracle relative to which single-copy pseudorandom states exist while **P** = **NP** [KQST23], so quantum analogues of one-way functions may not sit at the base. *Post-quantum* cryptography is the intermediate regime: protocols and challengers stay classical, but adversaries are quantum. Whether the classical hierarchy survives there is not automatic, because a classical security reduction may rewind its adversary, and rewinding destroys the internal state of a quantum one. This is the difficulty that work on constructive post-quantum reductions [BBK22] and on universal reductions relative to stateful oracles [CFP22] addresses, in both cases under restrictions on the reduction (single-copy adversaries, non-adaptivity, or straight-line behaviour).

The present paper removes those restrictions on the *reduction* and instead restricts the *game*. Its main theorem: if a classical black-box game-based security reduction proves that $\mathcal{Q}$ implies a primitive $\mathcal{P}$ whose security game has only two messages, then any efficient quantum adversary breaking $\mathcal{P}$ can be turned into an efficient quantum adversary breaking $\mathcal{Q}$, so the implication lifts. The technique replaces the quantum adversary by a lazily-evaluated, memoizing version, which answers repeated queries identically and is therefore statistically indistinguishable, even under rewinding and resetting, from an inefficient classical adversary of the same advantage; a two-message game asks the adversary only one question, so this modification costs nothing in advantage. Since one-way functions have a two-message falsifiable game, every primitive that classically implies one-way functions by a black-box game-based reduction implies post-quantum one-way functions post-quantumly, for uniform and non-uniform quantum adversaries alike, and even when the reduction assumes its adversary is deterministic.

The hypothesis that the security reduction is black-box is what makes the whole argument possible: the proof works by substituting a doctored adversary into $\mathcal{R}$ as an oracle. When the classical implication from $\mathcal{Q}$ to one-way functions is proved some other way, the paper's machinery has nothing to substitute into, and the paper records this case as unresolved. Note that the paper's results are already insensitive to how the *implementation* is built from $\mathcal{Q}$: that may be arbitrarily non-black-box. Only the security direction is constrained.

2 Notation and parameters

- $n \in \mathbb{N}$ is the security parameter. A function is *negligible* if it is eventually smaller than $1/p(n)$ for every polynomial p; a probability is *non-negligible* otherwise.
- PPT denotes a classical probabilistic polynomial-time algorithm.
- QPT denotes a uniform efficient quantum algorithm with classical inputs and outputs: a family $\{Q_n\}_{n\in\mathbb{N}}$ of quantum circuits of size $\mathrm{poly}(n)$ whose descriptions are produced by a PPT machine on input 1^n, with work registers initialized to $|0\rangle$ and the output register measured in the computational basis.
- QPT/poly denotes the non-uniform variant: the same, except the work registers of Q_n are initialized with a quantum advice state $|\phi_n\rangle$ on $\mathrm{poly}(n)$ qubits, depending only on n.
- E ranges over $\{\mathrm{QPT}, \mathrm{QPT/poly}\}$ and denotes the class of efficient quantum adversaries fixed in the statement.
- $\mathcal{P} = (F_{\mathcal{P}}, R_{\mathcal{P}})$ denotes a classical primitive, with $F_{\mathcal{P}}$ its set of correct implementations and $R_{\mathcal{P}}$ its breaking relation; $C_{\mathcal{P},f}$ is its challenger on implementation f and $t_{\mathcal{P}}$ its success threshold. $\mathcal{P}'$ denotes the post-quantum variant of $\mathcal{P}$.
- $\mathcal{Q}$ and $\mathcal{Q}'$ denote the primitive in the hypothesis and its post-quantum variant; $\mathcal{F}$ and $\mathcal{F}'$ denote the one-way function primitive and its post-quantum variant.
- f denotes an implementation of $\mathcal{Q}$ and g_f the implementation of $\mathcal{F}$ obtained from it; A, $A_{\mathcal{P}}$, $A_{\mathcal{Q}}$, $A_{\mathcal{F}}$ denote adversaries, and $\mathcal{R}$ a black-box reduction.

The parameters are:

- n, the security parameter; all efficiency and negligibility are asymptotic in it.

- E, the fixed class of efficient quantum adversaries, either uniform (QPT) or non-uniform with polynomial-size quantum advice (QPT/poly). The conjecture is asserted for each choice separately.
- Q, an arbitrary classical primitive with a game-based security definition, quantified universally.
- t_Q, the success threshold of Q's security game; unrestricted (it may be 0, 1/2, or anything else).
- f, g_f: a PPT implementation of Q, and the PPT implementation of one-way functions built from it by the implementation clause of the reduction.

3 The conjecture

Definition 1 (Game-based classical primitive). A *classical primitive* is a pair $\mathcal{P} = (F_\mathcal{P}, R_\mathcal{P})$, where $F_\mathcal{P}$ is a set of (possibly inefficient) randomized algorithms, called the correct implementations of $\mathcal{P}$, and $R_\mathcal{P}$ is a relation on pairs (f, A) of algorithms; $(f, A) \in R_\mathcal{P}$ is read "A $\mathcal{P}$-breaks f".
The primitive is *game-based* if $R_\mathcal{P}$ is given by a security game: an interactive protocol, over classical communication, between a challenger $C_{\mathcal{P},f}$ (which may depend on the implementation f) and an adversary A, on common input the security parameter 1^n, at the end of which $C_{\mathcal{P},f}$ outputs 1 ("A wins") or 0; together with a *success threshold* $t_\mathcal{P} : \mathbb{N} \to [0,1]$. Then $(f, A) \in R_\mathcal{P}$ iff there is a polynomial p such that

$$\Pr\left[\, C_{\mathcal{P},f}(1^n) \text{ outputs 1 against } A \,\right] \geq t_\mathcal{P}(n) + \frac{1}{p(n)}$$

for infinitely many $n \in \mathbb{N}$.

Definition 2 (Classical and post-quantum existence). Let $\mathcal{P} = (F_\mathcal{P}, R_\mathcal{P})$ be a game-based classical primitive.
$\mathcal{P}$ *exists classically* if there is a PPT implementation $f \in F_\mathcal{P}$

such that no PPT algorithm A satisfies $(f, A) \in R_{\mathcal{P}}$.
The *post-quantum variant* $\mathcal{P}'$ of $\mathcal{P}$ against a class E of efficient quantum adversaries is the same primitive with the same implementations and the same challenger $C_{\mathcal{P},f}$, with the adversary now ranging over E; the communication with the challenger remains classical. Thus $\mathcal{P}'$ *exists* if there is a PPT implementation $f \in F_{\mathcal{P}}$ such that no $A \in \mathsf{E}$ wins $C_{\mathcal{P},f}(1^n)$ with probability at least $t_{\mathcal{P}}(n) + 1/p(n)$ for any polynomial p and infinitely many n.

Definition 3 (One-way functions as a game-based primitive). The primitive $\mathcal{F} = (F_{\mathcal{F}}, R_{\mathcal{F}})$ of one-way functions has $F_{\mathcal{F}}$ equal to the set of all functions $f : \{0,1\}^* \to \{0,1\}^*$, viewed as deterministic algorithms; a PPT implementation is one computable in deterministic polynomial time.
Its security game is the 2-message game with threshold $t_{\mathcal{F}} = 0$: on security parameter 1^n the challenger samples $x \leftarrow \{0,1\}^n$ and sends $f(x)$; the adversary replies with a single message x'; the challenger outputs 1 iff $f(x') = f(x)$.
Hence $\mathcal{F}$ exists classically iff classical one-way functions exist, and $\mathcal{F}'$ exists against E iff there is a deterministic polynomial-time computable f with

$$\Pr_{\substack{x \leftarrow \{0,1\}^n, \\ x' \leftarrow A(f(x), 1^n)}} \left[f(x') = f(x) \right]$$

negligible in n for every $A \in \mathsf{E}$.

Definition 4 (Potentially non-constructive reduction). A *potentially non-constructive reduction* from a classical primitive $\mathcal{P} = (F_{\mathcal{P}}, R_{\mathcal{P}})$ to a classical primitive $\mathcal{Q} = (F_{\mathcal{Q}}, R_{\mathcal{Q}})$ exists if both of the following hold.

1. *Implementation.* For every PPT implementation $f \in F_{\mathcal{Q}}$ there is a PPT implementation $g_f \in F_{\mathcal{P}}$.

2. *Security.* For every PPT implementation $f \in F_{\mathcal{Q}}$: if there is a PPT adversary $A_{\mathcal{P}}$ that $\mathcal{P}$-breaks g_f, then there is a

PPT adversary A_Q that Q-breaks f.

Neither clause carries any black-box requirement; clause 2 is a bare existential statement, and clauses 1 and 2 together entail that the classical existence of Q implies the classical existence of $\mathcal{P}$.

A reduction is additionally *game-based black-box* if $\mathcal{P}$ and Q are game-based and the existence of A_Q in clause 2 is established by a black-box reduction: a PPT oracle algorithm $\mathcal{R}$ that is additionally given $1^{1/\varepsilon}$ as an input parameter, such that for every (possibly inefficient) adversary A winning in $C_{\mathcal{P},g_f}$ with advantage $\varepsilon(n_1) \geq 1/\mathrm{poly}(n_1)$ at every security parameter n_1, the algorithm $\mathcal{R}^A$ wins in $C_{Q,f}$ with advantage $\delta_\varepsilon \geq 1/\mathrm{poly}(n_2)$ above t_Q, where $\mathcal{R}$ may query A on inputs of its choice, on several security parameters, and may rewind A or reset its randomness.

Conjecture 1 (post-quantum minimality of one-way functions without a black-box security reduction). *Fix a class of efficient quantum adversaries* $\mathsf{E} \in \{\mathrm{QPT}, \mathrm{QPT/poly}\}$*, and keep it fixed throughout.*

Let $Q = (F_Q, R_Q)$ *be any classical primitive with a game-based security definition (Definition 1), with challenger* $C_{Q,f}$ *and success threshold* t_Q*, and let* $\mathcal{F}$ *be the one-way function primitive (Definition 3).*

Suppose that a potentially non-constructive reduction from $\mathcal{F}$ *to* Q *exists in the sense of Definition 4; this is the paper's formalization of the classical existence of* Q *implying the classical existence of one-way functions, and in particular it entails that implication. No assumption is made about how the security clause of Definition 4 is established: in particular, the passage from a* PPT *adversary* $A_{\mathcal{F}}$ *breaking* g_f *to a* PPT *adversary* A_Q *breaking* f *need* not *be witnessed by a black-box reduction from winning in* $C_{Q,f}$ *to winning in* $C_{\mathcal{F},g_f}$*, and may depend arbitrarily on the code of* $A_{\mathcal{F}}$*.*

Then: if the post-quantum variant Q' *of* Q *against* E *exists (Definition 2), one-way functions secure against* E *exist, i.e. the post-quantum variant* $\mathcal{F}'$ *of* $\mathcal{F}$ *against* E *exists.*

Remark 1 (openness). The paper poses the question and records

the non-black-box case as unresolved: "Our work leaves open answering our main question when Q implies OWFs through a non-black-box security reduction, or when P uses a more complicated security game than a two-message one" (p. 1). The question itself is stated there as "If a classically secure cryptographic primitive Q implies one-way functions, does the post-quantum-secure variant of P imply (post-quantum) one-way functions as well?" (p. 3). The paper conjectures no direction, so the affirmative phrasing of Conjecture 1 is a site convention rather than the authors' claim, and a solver should treat both directions as live.

Remark 2 (what is proved). Theorem 1 lifts any classical black-box reduction from a game $\mathcal{Q}$ to a 2-message game $\mathcal{P}$ to the post-quantum setting, uniformly and non-uniformly. Theorem 3 turns this into a statement about primitives, and Corollary 1 specialises it to $\mathcal{P} =$ one-way functions, with no restriction on how the reduction calls its adversary, because the one-way function game is falsifiable: "To derive Corollary 1 from Theorem 3 we merely observe that one-way functions have a 2-message security game and that their security game is falsifiable" (p. 22). Theorem 2 extends the lifting to reductions that assume their oracle adversary is deterministic, under any one of three side conditions ($\mathcal{Q}$ threshold-zero with single-security-parameter calls; $\mathcal{P}$ falsifiable; $\mathcal{Q}$ falsifiable with single-security-parameter calls). In the other direction, the paper observes that the 2-message restriction on $\mathcal{P}$ cannot simply be dropped: a contrived primitive built from the 4-message qubit certification test of Brakerski et al. is implied by LWE classically through a black-box reduction but, the paper argues, not post-quantumly unless LWE is quantumly broken.

Remark 3 (the scope of the black-box hypothesis). Only the security direction is constrained in the settled case: "This means that our results do not depend on how the implementation reduction is performed, as formalized in [RTV04], meaning that we can handle non-black-box constructions, so long as the security reduction is a black-box reduction between games" (p. 11). The post-quantum variant is the same primitive with a quantum adversary: "Then, we define the post-quantum variant of P to be the same primitive, but now the security definition allows efficient quantum adversaries to participate in the same security game (using classical communica-

tion)" (p. 11).

Remark 4 (caveats for a reviewer). Four things a reviewer should press on. First, whether this is a problem or a programme: the paper gives no account of what makes the non-black-box case hard and offers no partial result towards it. "Non-black-box security reduction" is not a structured class the way black-box reductions are; the hypothesis of Conjecture 1, as Definition 4 makes explicit, is little more than the bare implication "Q classically exists $\Rightarrow$ one-way functions classically exist", so a positive proof would have to be a general lifting theorem with no reduction structure to grip. The honest reading may be that the affirmative direction is not attackable, and that only the refuting direction — a contrived primitive, in the style of the paper's own 4-message counterexample — has a visible line of attack. Second, the paper leaves the question open without conjecturing a direction (Remark 1). Third, the literature after December 2024 has not been checked for a resolution, and the paper is short and recent enough that a follow-up could exist. Fourth, the third "Furthermore" clause of Corollary 1 (deterministic-adversary reductions) is asserted for one-way functions on the strength of the falsifiability of the one-way function game; the conjecture above is deliberately kept free of any deterministic-adversary hypothesis, matching the black-box statement the paper proves.

4 Bibliography

[Bar01] Boaz Barak. *How to go beyond the black-box simulation barrier.* 42nd IEEE Symposium on Foundations of Computer Science, pages 106–115, 2001.

[BBK22] Nir Bitansky, Zvika Brakerski, and Yael Tauman Kalai. *Constructive post-quantum reductions.* Advances in Cryptology — CRYPTO 2022, pages 654–683, Springer, 2022.

[CFP22] Benjamin Chan, Cody Freitag, and Rafael Pass. *Universal reductions: Reductions relative to stateful oracles.* Theory of Cryptography (TCC), pages 151–180, Springer, 2022.

[IL89] Russell Impagliazzo and Michael Luby. *One-way functions are essential for complexity based cryptography.* 30th Annual Symposium on Foundations of Computer Science, pages 230–235, 1989.

[KQST23] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. *Quantum cryptography in algorithmica.* 55th Annual ACM Symposium on Theory of Computing (STOC), pages 1589–1602, 2023.

[Kre21] William Kretschmer. *Quantum Pseudorandomness and Classical Complexity.* 16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021), LIPIcs vol. 197, pages 2:1–2:20, 2021.

[RTV04] Omer Reingold, Luca Trevisan, and Salil Vadhan. *Notions of reducibility between cryptographic primitives.* Theory of Cryptography (TCC), pages 1–20, Springer, 2004.