AICR · OPEN PROBLEM

One Erasing Challenge Query Does Not Buy Security Against Many Embedding Learning Queries

Single quantum challenge query, classical learning queries, versus polynomially many embedding-model superposition learning queries

Status. Statement: AI-written from Tore Vincent Carstens, Ehsan Ebrahimi, Gelo Tabia and Dominique Unruh, *Relationships between quantum IND-CPA notions*, IACR Cryptology ePrint Archive 2020 (preprint, 47 pages), not yet checked by a human. The paper proves that the notion with a single erasing two-ciphertext challenge query implies five other panels ($P7$, $P8$, $P9$, $P13$, $P14$), and separates it from two more ($P2$ and $P12$), but leaves its relation to six panels open, among them the family with many embedding-model superposition learning queries and classical challenge queries; that non-implication is one of the six the paper explicitly conjectures, and by the paper's own bookkeeping it is the one whose resolution would settle the largest number of the remaining open cells.

Category. *Quantum & Post-Quantum Cryptography.*

Conjecture (informal). *In quantum chosen-plaintext security definitions, superposition access to the encryption oracle can be granted in the learning phase, in the challenge phase, or both, and the number of queries allowed matters. Surprisingly, when polynomially many superposition challenge queries are available, they can be used to fake superposition learning queries, so a definition with no learning phase at all is already as strong as the corresponding definition with a full superposition learning phase. That trick consumes one challenge query per simulated learning query. This leaves open the case where the adversary gets only a single superposition challenge query: the conjecture is that a single erasing-oracle challenge query returning two ciphertexts, plus unlimited classical learning queries, does not buy security against an adversary who gets unlimited superposition learning queries in the embedding model with only classical challenges. Concretely, there should be a scheme secure in the first sense and broken in the second. Settling it would close more of the paper's open cases than any of the other separations it conjectures, because many notions sit above the second of these two.*

1 The setting

Quantum chosen-plaintext definitions for symmetric encryption differ along four axes: how many learning and challenge queries the adversary makes (0, 1, or polynomially many $*$), which query model answers superposition queries (classical CL; *standard* ST, the unitary U_f; *embedding* EM, where the challenger supplies the $|0\rangle$ output register; *erasing* ER, the isometry $\hat{U}^f$ of [KKVB02]), and what the challenge returns (one ciphertext, two ciphertexts, or real-or-random). Classically these all coincide [BDJR97]; quantumly they do not, which is why the literature contains several incompatible proposals [BZ13b, GHS16, MS16].

The harvested paper reduces the 57 achievable notions to 14 equivalence classes $P1,\ldots,P14$ and orders them. Two of its positive results are relevant here. First, its Theorem 18 shows that for erasing and embedding learning queries, and for the challenge types $(EM,2\text{ct})$, $(ER,2\text{ct})$ and $(ER,1\text{ct})$, a notion with *no* learning phase already implies the notion with polynomially many superposition learning queries; classically this is trivial by copying

the learning query into a challenge query, and the paper's contribution is to make it work without cloning. Second, its Theorem 19 does the same for real-or-random challenges. Both reductions spend one challenge query per simulated learning query. Panel $P3$ is the singleton learn$(*, CL)$-chall$(1, ER, 2\mathrm{ct})$, where only one challenge query is available, so this route is closed; panel $P11$ is the family learn$(*, EM)$-chall$(\mathfrak{c}_{\mathrm{nb}}, CL, \mathfrak{c}_{\mathrm{rt}})$ with $\mathfrak{c}_{\mathrm{nb}} \in \{1, *\}$ and $\mathfrak{c}_{\mathrm{rt}} \in \{1\mathrm{ct}, 2\mathrm{ct}, \mathrm{ror}\}$, all six members proved equivalent. The paper leaves $P3 \Rightarrow P11$ open and conjectures it fails, on the ground that one quantum challenge query cannot be made to serve as many quantum learning queries. Separating schemes of this kind are built from quantum-secure pseudorandom permutations [Zha16] with a planted period recoverable by Simon's algorithm [Sim97] from superposition queries only.

Progress to date. The simulation of Theorem 18 just described spends one challenge query per simulated superposition learning query, so it needs polynomially many challenge queries and says nothing when only one is allowed, and Theorem 19 is the same in this respect. On this record's own reading, that is why the single-challenge-query restriction looks like the crux of $P3 \Rightarrow P11$; the paper's own stated reason (p. 45) is simply that a reduction adversary is unlikely to simulate many quantum queries with only one. Established around the cell: the single erasing two-ciphertext notion implies the single erasing one-ciphertext notion, the single erasing real-or-random notion, the single embedding two-ciphertext notion, the single embedding real-or-random notion, and the fully classical notions; it does not imply either standard-query real-or-random notion: neither the family $P2$ nor the singleton learn$(*, CL)$-chall$(1, ST, \mathrm{ror})$. The paper's separations of this shape are built with Simon's algorithm [Sim97]. The paper also records (p. 44) that, since $P3$ implies $P7$, $P8$, $P9$ and $P13$, a proof that $P3 \nRightarrow P11$ would immediately give $P7, P8, P9, P13 \nRightarrow P11$ as well; by this record's bookkeeping that amounts to nine further cells of the classification.

2 Notation and parameters

- η is the security parameter. All of h, n, n', t, t' are polynomially bounded functions of η; *QPT* means quantum polynomial time in η; a function ε is *negligible* if $\varepsilon(\eta) < 1/p(\eta)$ for every

polynomial p and all sufficiently large η. A *quantum-secure one-way function* is an efficiently computable family of functions that no QPT algorithm inverts with non-negligible probability.

- An (h, n, n', t, t')*-encryption scheme* is a triple $\Pi = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ of efficient classical algorithms with

$$\begin{aligned} \mathsf{KGen}&: \{0,1\}^{t'} \to \{0,1\}^{h}, \\ \mathsf{Enc}&: \{0,1\}^{h} \times \{0,1\}^{n} \times \{0,1\}^{t} \to \{0,1\}^{n'}, \\ \mathsf{Dec}&: \{0,1\}^{h} \times \{0,1\}^{n'} \to \{0,1\}^{n} \cup \{\bot\} \end{aligned}$$

  such that $\mathsf{Dec}_k(\mathsf{Enc}_k(m;r)) = m$ for all k, m, r. We write $\mathsf{Enc}_k(m;r) := \mathsf{Enc}(k,m,r)$ and $\mathsf{Enc}_k(\cdot\,;r)$ for the map $m \mapsto \mathsf{Enc}_k(m;r)$, injective for each fixed k, r by correctness. $\mathsf{KGen}()$ means running KGen on uniform randomness.

- For $f : \{0,1\}^a \to \{0,1\}^c$, U_f is the unitary $|x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$ on $a + c$ qubits.

- For injective $g : \{0,1\}^a \to \{0,1\}^c$, $\hat{U}^g$ is the isometry $|x\rangle \mapsto |g(x)\rangle$ from a to c qubits; it is realizable by an efficient quantum circuit whenever g and a left inverse of g are efficiently computable.

- $\bar{b} := 1 - b$ for $b \in \{0,1\}$.

- Q_{in}, Q_{in0}, Q_{in1} denote n-qubit input registers and Q_{out} an n'-qubit output register.

The parameters, at a glance:

- η — security parameter; all other parameters are polynomially bounded functions of it.
- n — plaintext length in bits.
- n' — ciphertext length in bits.
- h — key length in bits.
- t — length of the per-encryption randomness.
- t' — length of the key-generation randomness.

- b — challenge bit, fixed once for the whole game.
- $\mathfrak{c}_{\mathrm{nb}}$ — number of challenge queries permitted: exactly one, or polynomially many.

3 The conjecture

Definition 1 (Query types). Fix an (h, n, n', t, t')-encryption scheme Π, a key $k \in \{0,1\}^h$ and a bit $b \in \{0,1\}$. In each query below the randomness values r, r_0, r_1 are sampled freshly and uniformly from $\{0,1\}^t$; a single superposition query uses one value of r for all messages in the superposition.

- A *CL-learning query*: the adversary sends a classical $m \in \{0,1\}^n$ and receives $\mathsf{Enc}_k(m; r)$.
- An *EM-learning query*: the adversary hands over Q_{in} (n qubits); the challenger prepares Q_{out} in state $|0\rangle^{\otimes n'}$, applies $U_{\mathsf{Enc}_k(\cdot;r)}$ to (Q_{in}, Q_{out}), and returns both registers.
- A $(CL, 1\mathrm{ct})$-*challenge query*: the adversary sends classical $m_0, m_1 \in \{0,1\}^n$ and receives the classical ciphertext $\mathsf{Enc}_k(m_b; r)$.
- An $(ER, 2\mathrm{ct})$-*challenge query*: the adversary hands over registers Q_{in0}, Q_{in1} (each n qubits); the challenger applies the isometry

$$|m_0\rangle|m_1\rangle \mapsto |\mathsf{Enc}_k(m_b; r_0)\rangle\,|\mathsf{Enc}_k(m_{\bar{b}}; r_1)\rangle$$

and returns the two resulting n'-qubit registers.

Definition 2 ($\mathfrak{l}$-$\mathfrak{c}$-IND-CPA). Let $\mathfrak{l}$ name a learning-query type and $\mathfrak{c}$ a challenge-query type together with a permitted number of challenge queries, 1 or $*$ (polynomially many). In the game the challenger samples $k \leftarrow \mathsf{KGen}()$ and a uniform $b \in \{0,1\}$; a QPT adversary $\mathcal{A}$ makes polynomially many learning queries of type $\mathfrak{l}$ and the permitted number of challenge queries, in any interleaved order (learning queries may be made before

and after a challenge query), all answered with this same k and this same b; finally $\mathcal{A}$ outputs a bit b' and wins iff $b' = b$. We write learn$(*, X)$-chall$(\mathfrak{c}_{\mathrm{nb}}, Y, \mathrm{rt})$ for this game with X-learning queries and $\mathfrak{c}_{\mathrm{nb}} \in \{1, *\}$ challenge queries of type (Y, rt), and call Π secure for it iff every QPT adversary wins with probability at most $\frac{1}{2} + \varepsilon(\eta)$ for some negligible ε.

Conjecture 1 ($P3$ does not imply $P11$). *Assume that quantum-secure one-way functions exist. Then there exist polynomially bounded parameters h, n, n', t, t' (functions of η) and an (h, n, n', t, t')-encryption scheme $\Pi = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ such that both of the following hold.*

1. *Π is* learn$(*, CL)$-chall$(1, ER, 2\mathrm{ct})$*-IND-CPA-secure, i.e. every QPT adversary that makes polynomially many classical learning queries and* exactly one $(ER, 2\mathrm{ct})$*-challenge query wins the game with probability at most $\frac{1}{2} + \varepsilon(\eta)$ for some negligible ε.*
2. *Π is* not learn$(*, EM)$-chall$(*, CL, 1\mathrm{ct})$*-IND-CPA-secure: there exist a QPT adversary $\mathcal{A}$ making polynomially many EM-learning queries and polynomially many $(CL, 1\mathrm{ct})$-challenge queries, and a polynomial p, such that $\mathcal{A}$ wins that game with probability at least $\frac{1}{2} + 1/p(\eta)$ for infinitely many η.*

Remark 1 (panel identification). Conjecture 1 names one representative of each panel: learn$(*, CL)$-chall$(1, ER, 2\mathrm{ct})$ for $P3$, which is a singleton, and learn$(*, EM)$-chall$(*, CL, 1\mathrm{ct})$ for $P11$, whose six members the paper proves equivalent. Panel membership must not be read off the boxed lists on p. 5: the box for Panel 11 there erroneously repeats the contents of Panel 10 (erasing learning queries) instead of the embedding learning queries. Figure 1 on p. 22 and the Panel 11 equivalence derivations on p. 24 make clear that Panel 11 is the family with EM learning queries and classical challenge queries, and this record follows those. A reviewer should confirm that reading, since the conjecture is stated with a representative member of that panel.

Remark 2 (on the one-way-function hypothesis). The hypothesis

"assuming quantum-secure one-way functions exist" is supplied here rather than quoted. The paper states this hypothesis for its proved separations but not explicitly for the conjectured ones. Without some such assumption no scheme is secure in either notion and the implication holds vacuously.

Remark 3 (strength of the recorded obstruction). The paper's account of why the implication is hard is one sentence (p. 45), about simulating many quantum queries with a single quantum query, so a reviewer may judge the recorded obstruction thinner than for the paper's other conjectured separations. The substantive evidence is that the paper's own simulation theorem, Theorem 18, provably needs many challenge queries.

Remark 4 (currency of the source). The source is a 2020 ePrint. A later version of this work, or follow-up work, may have closed this cell; the record has not been checked against the newest version.

4 Bibliography

[BDJR97] M. Bellare, A. Desai, E. Jokipii, P. Rogaway. *A concrete security treatment of symmetric encryption.* 38th Annual Symposium on Foundations of Computer Science, FOCS '97, pages 394–403, IEEE Computer Society, 1997.

[BZ13b] D. Boneh, M. Zhandry. *Secure signatures and chosen ciphertext security in a quantum computing world.* Advances in Cryptology — CRYPTO 2013, Part II, volume 8043 of Lecture Notes in Computer Science, pages 361–379, Springer, 2013.

[GHS16] T. Gagliardoni, A. Hülsing, C. Schaffner. *Semantic security and indistinguishability in the quantum world.* Advances in Cryptology — CRYPTO 2016, volume 9816 of Lecture Notes in Computer Science, pages 60–89, Springer, 2016.

[KKVB02] E. Kashefi, A. Kent, V. Vedral, K. Banaszek. *Comparison of quantum oracles.* Phys. Rev. A, 65:050304, 2002.

[MS16] S. Mossayebi, R. Schack. *Concrete security against adversaries with quantum superposition access to encryption and decryption oracles.* CoRR, abs/1609.03780, 2016.

[Sim97] D. R. Simon. *On the power of quantum computation.* SIAM J. Comput., 26(5):1474–1483, 1997.

[Zha16] M. Zhandry. *A note on quantum-secure PRPs.* IACR Cryptology ePrint Archive, 2016:1076, 2016.