AICR · OPEN PROBLEM

One Standard-Oracle Real-or-Random Challenge Query Does Not Imply One Embedding Two-Ciphertext Challenge Query

Classical learning phase, exactly one superposition challenge query on each side

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. Settled in that paper: the relation of the real-or-random standard-oracle notion $P12$ to five other panels, and that the embedding two-ciphertext notion $P7$ is not implied by the Boneh–Zhandry family or by the erasing-learning-query family (Theorem 40) while it does imply the single embedding real-or-random notion (Theorem 23); open, and conjectured below, is whether $P12 \Rightarrow P7$, one of the six non-implications the paper explicitly conjectures.

Category. *Quantum & Post-Quantum Cryptography.*

Conjecture (informal). *When a quantum adversary gets one superposition challenge query against a symmetric encryption scheme, two natural formats are available. In the first, the adversary hands over a message register and an output register, and the challenger XORs into the output register either the encryption of the submitted message or the encryption of a secretly permuted message; the adversary must decide which. In the second, the adversary hands over two message registers, the challenger itself supplies two fresh zeroed output registers, and it returns the encryptions of the two submitted registers in an order determined by the secret bit; the adversary must decide the order. Neither format is known to imply the other, and the second is already known not to imply the first. The conjecture is that the first does not imply the second: some scheme should be secure when challenged in the real-or-random format and broken when challenged in the two-ciphertext embedding format. The stated obstruction is a counting one: an adversary against the second format expects back four registers, that is two independent encryptions of two quantum inputs, whereas a single query of the first format evaluates the encryption oracle on only one quantum input, and a reduction has no way to manufacture the second evaluation.*

1 The setting

In a quantum chosen-plaintext game the challenge query can be posed in several inequivalent ways. With the *standard* oracle U_f the adversary supplies both an input and an output register; a challenge returning one or two ciphertexts this way is impossible to achieve for any scheme [BZ13b], which leaves the real-or-random format, where the challenger encrypts either the submitted message or a secretly permuted message, as in [MS16]. With the *embedding* oracle the challenger supplies the zeroed output registers itself, and then the two-ciphertext format — encrypt both submitted registers, in an order set by the secret bit — becomes achievable.

The harvested paper places these two notions in singleton equivalence classes: $P12 = \text{learn}(*, CL)\text{-chall}(1, ST, \text{ror})$ and $P7 = \text{learn}(*, CL)\text{-chall}(1, EM, 2\text{ct})$. It proves that $P12$ does not imply five other panels, that $P7$ is not implied by the Boneh–Zhandry family or by the erasing-learning-query family (Theorem 40), and that $P7$

implies the single embedding real-or-random notion (Theorem 23). Whether $P12 \Rightarrow P7$ is left open, and conjectured to fail: an adversary in the $(EM, 2\text{ct})$ game expects four registers back, holding two independent encryptions of two quantum inputs, while one (ST, ror) query evaluates the encryption oracle on a single quantum input. The paper does obtain the two-ciphertext format from the real-or-random format inside the embedding model (Theorem 20), but that reduction consumes superposition learning queries, which the classical learning phase here does not provide. A further constraint on any separating scheme comes from the same paper: no mode of operation is secure for $P12$ if, for some message length, there is an input block i and an output block j such that j does not depend on i and yet j can take any value as the input message ranges over the whole message space (Corollary 43) — a class the paper notes includes CBC, with i the second and j the first block, one of the modes whose post-quantum security was studied in [ATTU16]. Schemes secure for $P12$ exist under quantum-secure one-way functions, via quantum-secure pseudorandom permutations [Zha16]. The paper's Section 7.3 separations plant a σ-periodic structure recoverable by Simon's algorithm [Sim97] from superposition queries only, while the separations bearing on these two panels (Theorems 40 and 42, Corollary 43) instead use a single-query Hadamard interference test.

Progress to date. The paper's Theorem 23 shows that a single embedding two-ciphertext challenge query implies a single embedding real-or-random challenge query, and the embedding challenge model can be simulated by the standard one, so both notions in this conjecture imply the single embedding real-or-random notion; the question is exactly whether the real-or-random format reaches the two-ciphertext format. Its Theorem 20 does derive two-ciphertext from real-or-random in the embedding model, but that reduction spends embedding-model superposition learning queries, which are unavailable here since the learning phase is classical. Theorem 40 separates the Boneh–Zhandry family and the erasing-learning-query family from the embedding two-ciphertext notion, using the scheme that outputs the randomness together with a pseudorandom pad of the message. Any separating scheme for this conjecture must also be secure for the real-or-random standard-oracle notion, and the paper's Corollary 43 shows that no mode of operation is secure

for it if, for some message length, there is an input block i and an output block j such that j does not depend on i and yet j can take any value as the input message ranges over the whole message space — a class the paper notes includes CBC (with i the second and j the first block), which rules out the obvious candidates.

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 $m \mapsto \mathsf{Enc}_k(m; r)$. $\mathsf{KGen}()$ 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.

- Σ_n is the set of all permutations of $\{0,1\}^n$; for $\pi \in \Sigma_n$ and $b \in \{0,1\}$ we write $\pi^0 = \mathrm{id}$ and $\pi^1 = \pi$. Also $\bar{b} := 1 - b$.

- Q_{in}, Q_{in0}, Q_{in1} denote n-qubit input registers and $Q_{out}, Q_{out0}, Q_{out1}$ denote n'-qubit output registers.

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.
- π — permutation of the message space, sampled for the real-or-random challenge query.

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 $b \in \{0,1\}$. The randomness values r, r_0, r_1 are sampled freshly and uniformly from $\{0,1\}^t$ per query, and π freshly and uniformly from Σ_n; 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 (ST, ror)*-challenge query*: the adversary hands over registers Q_{in} (n qubits) and Q_{out} (n' qubits); the challenger applies the unitary $U_{\mathsf{Enc}_k(\pi^b(\cdot);r)}$, that is

$$|m\rangle|c\rangle \mapsto |m\rangle|c \oplus \mathsf{Enc}_k(\pi^b(m); r)\rangle,$$

  and returns both registers.
- An $(EM, 2\mathrm{ct})$*-challenge query*: the adversary hands over registers Q_{in0}, Q_{in1} (each n qubits); the challenger prepares Q_{out0}, Q_{out1} each in state $|0\rangle^{\otimes n'}$, applies the unitary

$$|m_0\rangle|m_1\rangle|0\rangle|0\rangle \mapsto |m_0\rangle|m_1\rangle|\mathsf{Enc}_k(m_b; r_0)\rangle|\mathsf{Enc}_k(m_{\bar{b}}; r_1)\rangle,$$

  and returns all four registers.

Definition 2 (ł-ć-IND-CPA with one challenge query). In the learn$(*, CL)$-chall$(1, Y, \mathrm{rt})$-IND-CPA game the challenger samples $k \leftarrow \mathsf{KGen}()$ and a uniform $b \in \{0,1\}$; a QPT adversary $\mathcal{A}$ makes polynomially many CL-learning queries followed by exactly one challenge query of type (Y, rt), all answered with this same k and this same b; finally $\mathcal{A}$ outputs a bit b' and wins iff $b' = b$. Π is secure for the notion iff every QPT adversary wins with probability at most $\frac{1}{2} + \varepsilon(\eta)$ for some negligible ε.

Conjecture 1 ($P12$ does not imply $P7$). *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$(1, ST, \mathrm{ror})$*-IND-CPA-secure, i.e. every QPT adversary that makes polynomially many classical learning queries and* exactly one *(ST, ror)-challenge query wins the game with probability at most $\frac{1}{2} + \varepsilon(\eta)$ for some negligible ε.*

2. *Π is* not learn$(*, CL)$-chall$(1, EM, 2\mathrm{ct})$*-IND-CPA-secure: there exist a QPT adversary $\mathcal{A}$ making polynomially many classical learning queries and exactly one $(EM, 2\mathrm{ct})$-challenge query, 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 (on the one-way-function hypothesis). The hypothesis "assuming quantum-secure one-way functions exist" is supplied here rather than quoted, following the paper's convention for its proved separations (p. 6). Some assumption of this kind is unavoidable: if no quantum-secure one-way function exists then no scheme is secure in either notion and the implication $P12 \Rightarrow P7$ holds vacuously. A reviewer should check that this is the intended reading and not a change of strength.

Remark 2 (on the reading of Theorem 20). The claim in Section 1 that Theorem 20's derivation of the two-ciphertext format from the real-or-random format fails here specifically because it consumes

embedding-model learning queries is a reading of that proof, not a sentence the paper states about this cell. The paper's own stated obstruction is the register-counting one quoted above.

Remark 3 (panel bookkeeping). The paper's per-panel bookkeeping should be checked independently: the boxed panel lists on pp. 4–5 contain at least one error, the Panel 11 box repeating the contents of the Panel 10 box. The two singleton panels used here are stated consistently in those boxes, in Figure 1 and in Corollary 43, but panel bookkeeping generally should be read off Figure 1 and Section 6.

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 newest version has not been checked.

4 Bibliography

[ATTU16] M. V. Anand, E. E. Targhi, G. N. Tabia, D. Unruh. *Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation.* Post-Quantum Cryptography — 7th International Workshop, PQCrypto 2016, volume 9606 of Lecture Notes in Computer Science, pages 44–63, Springer, 2016.

[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.

[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.