CONJURA · OPEN PROBLEM

Erasing Real-or-Random Quantum IND-CPA Does Not Imply Boneh–Zhandry Security

Symmetric encryption under superposition chosen-plaintext queries, polynomially many queries on both sides

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: $P1 \Rightarrow P6$ and $P1 \Rightarrow P4$, that $P4 \nRightarrow P1$, and — in the quantum random oracle model only — that $P6 \nRightarrow P4$; open, and conjectured below, is whether $P4 \Rightarrow P6$, one of the 41 cells the paper's implication table leaves open and one of the six non-implications the paper explicitly conjectures.

Category. *Quantum & Post-Quantum Cryptography.*

Conjecture (informal). *Classically, all the usual ways of writing down chosen-plaintext indistinguishability for symmetric encryption are equivalent to each other. As soon as the attacker may query the encryption oracle on a superposition of messages this stops being true, because it now matters how the oracle hands its answer back and how the challenge is phrased. Two of the definitions that appear in the literature are: (a) an attacker whose superposition queries are answered by an erasing oracle, which consumes the message register and returns only a ciphertext register, and whose challenge is real-or-random, meaning the challenger either encrypts the submitted message or encrypts a secretly permuted version of it; and (b) the Boneh–Zhandry definition, in which superposition learning queries are answered by the usual oracle that XORs the ciphertext into an adversary-supplied output register, while the challenge consists of two classical messages of which one is encrypted. Neither definition is known to imply the other, and it is already proved, in the quantum random oracle model, that (b) does not imply (a). The conjecture is that (a) does not imply (b) either: there should be a scheme that is provably secure in sense (a) and yet completely broken in sense (b), so that the two definitions are incomparable. The reason this is hard is that the obvious reduction — take an attacker against (b) and run it inside the game (a) — has to answer that attacker's standard-model learning queries using only erasing queries, and an erasing query does not give the message register back, while no-cloning prevents the reduction from keeping a copy of it.*

1 The setting

Classically, the one-ciphertext, two-ciphertext and real-or-random forms of IND-CPA for symmetric encryption are all equivalent up to polynomial loss [BDJR97]. In the quantum setting one must also decide how a superposition query to the encryption oracle is answered. Three query models are used: the *standard* model ST, where the unitary U_f XORs the answer into an adversary-supplied output register; the *embedding* model EM, where the challenger supplies the output register in state $|0\rangle$; and the *erasing* model ER, where the isometry $\hat{U}^f$ consumes the input register and returns only $|f(x)\rangle$ [KKVB02]. Boneh and Zhandry [BZ13b] showed that a superposition challenge query returning one or two ciphertexts in the standard model is

unachievable, and therefore proposed the definition with superposition learning queries in the standard model and classical challenge queries. Gagliardoni, Hülsing and Schaffner [GHS16] moved to erasing challenge queries, and Mossayebi and Schack [MS16] to real-or-random challenges with standard queries.

The source paper systematizes this: of 120 combinations of (number of learning queries, number of challenge queries, query model, challenge return type) it discards the exotic and impossible ones, leaving 57 achievable notions, which it groups into 14 equivalence classes called panels $P1,\dots,P14$ and orders by implication. Panel $P6$ is the Boneh–Zhandry family learn$(*,ST)$-chall$(\cdot,CL,\cdot)$; panel $P4$ is the erasing real-or-random family, which contains learn$(*,ER)$-chall$(*,ER,\mathrm{ror})$; panel $P1$ is the erasing one- and two-ciphertext family, which contains the notion of [GHS16]. The paper proves $P1 \Rightarrow P6$ (its Theorem 24, via [GHS16]) and $P1 \Rightarrow P4$, and separates $P4$ from $P1$ and $P6$ from $P4$. It does not resolve whether $P4 \Rightarrow P6$, and conjectures that it does not, on the ground that a reduction would have to answer the Boneh–Zhandry adversary's ST learning queries using ER queries, which do not return the input register and cannot be undone by copying it. Separations of this kind in the paper are all conditional on quantum-secure one-way functions, from which quantum-secure pseudorandom permutations are available [Zha16], and the separating schemes are built by planting a structure that only a superposition adversary can exploit, using Simon's algorithm [Sim97]. All non-implications in the paper assume quantum-secure one-way functions, and all hold in the standard model except Theorem 39, which holds in the quantum random oracle model and is what yields $P6 \not\Rightarrow P4$.

Progress to date. Established around this cell: the erasing one-ciphertext family implies the Boneh–Zhandry family (the paper's Theorem 24, quoting a chain of implications from Gagliardoni–Hülsing–Schaffner); the erasing one-ciphertext family implies the erasing real-or-random family (the paper's Theorem 22); the erasing real-or-random family does not imply the erasing one-ciphertext family — Corollary 29 (p. 37) states $P2,P4 \not\Rightarrow P8$, where $P8$ is learn$(*,CL)$-chall$(1,ER,1\mathrm{ct})$, and the paper then deduces $P4 \not\Rightarrow P1,P3$ on p. 36 because $P1,P3 \Rightarrow P8$; the bare claim that Panel 1 is strictly stronger than Panel 4 is also stated outright on p. 6. The mechanism is quasi-length-preserving schemes: any quasi-length-

preserving scheme is insecure for a single erasing one-ciphertext challenge query, while a quasi-length-preserving scheme secure for erasing real-or-random exists under quantum-secure one-way functions. Finally, the paper establishes the reverse direction of the conjecture below ($P6$ does not imply $P4$) in the quantum random oracle model: Theorem 39 shows $P2 \nRightarrow P10$ in the QROM, and $P6 \nRightarrow P4$ follows since $P2 \Rightarrow P6$ and $P4 \Rightarrow P10$. This is the paper's only separation that is not in the standard model (p. 6). Settling the conjectured direction would also give, by transitivity, that six further panels fail to imply the Boneh–Zhandry family. The paper's separation toolkit for problems of this shape consists of Simon's algorithm [Sim97], Shi's SetEquality problem, quasi-length-preserving schemes, and the paper's own decoherence lemmas.

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 $k \in \{0,1\}^h$, $m \in \{0,1\}^n$, $r \in \{0,1\}^t$. Here $\mathsf{Enc}_k(m;r) := \mathsf{Enc}(k,m,r)$, and $\mathsf{Enc}_k(\cdot\,;r)$ denotes the function $m \mapsto \mathsf{Enc}_k(m;r)$, which is 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 (*standard* oracle, query model ST).

- For injective $g : \{0,1\}^a \to \{0,1\}^c$, $\hat{U}^g$ is the isometry $|x\rangle \mapsto |g(x)\rangle$ from a qubits to c qubits (*erasing* oracle, query model ER); it is realizable by an efficient quantum circuit whenever g and a left inverse of g are efficiently computable.
- 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 $\pi^1 = \pi$.
- Q_{in}, Q_{out} denote quantum registers supplied by the adversary or by the challenger, of n and n' qubits respectively.

The parameters, at a glance:

- η — security parameter; all other parameters are polynomially bounded functions of it.
- n — plaintext length in bits (message space $\{0,1\}^n$).
- 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, resampled per 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 $b \in \{0,1\}$. In each query below, r is sampled freshly and uniformly from $\{0,1\}^t$ and π freshly and uniformly from Σ_n; a single superposition query uses one value of r for all messages in the superposition.

- An *ST-learning query*: the adversary hands over registers Q_{in} (n qubits) and Q_{out} (n' qubits); the oracle applies $U_{\mathsf{Enc}_k(\cdot;r)}$ to (Q_{in}, Q_{out}) and returns both registers.

- An *ER-learning query*: the adversary hands over Q_{in} (n qubits); the oracle applies $\hat{U}^{\mathsf{Enc}_k(\cdot;r)}$ to it and returns the resulting n'-qubit register.
- A $(CL,1\mathrm{ct})$-*challenge query*: the adversary sends classical $m_0, m_1 \in \{0,1\}^n$; the oracle returns the classical ciphertext $\mathsf{Enc}_k(m_b;r)$.
- An (ER,ror)-*challenge query*: the adversary hands over Q_{in} (n qubits); the oracle applies the isometry $|m\rangle \mapsto |\mathsf{Enc}_k(\pi^b(m);r)\rangle$ to it and returns the resulting n'-qubit register.

Definition 2 (𝔩-𝔠-IND-CPA). Let $\mathfrak{l}$ name a learning-query type and $\mathfrak{c}$ a challenge-query type. In the $\mathfrak{l}$-$\mathfrak{c}$-IND-CPA game the challenger samples $k \leftarrow \mathsf{KGen}()$ and a uniform $b \in \{0,1\}$; a QPT adversary $\mathcal{A}$ may then make polynomially many learning queries of type $\mathfrak{l}$ and polynomially many challenge queries of type $\mathfrak{c}$, in any interleaved order, all answered with this same k and this same b; finally $\mathcal{A}$ outputs a bit b' and wins iff $b' = b$. We write $\mathrm{learn}(*,X)$-$\mathrm{chall}(*,Y,\mathrm{rt})$ for this game with X-learning queries and (Y,rt)-challenge queries, 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 ($P4$ does not imply $P6$). *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 $\mathrm{learn}(*,ER)$-$\mathrm{chall}(*,ER,\mathrm{ror})$-IND-CPA-secure, i.e. every QPT adversary that makes polynomially many ER-learning queries and polynomially many (ER,ror)-challenge queries wins the $\mathfrak{l}$-$\mathfrak{c}$-IND-CPA game with probability at most $\frac{1}{2}+\varepsilon(\eta)$ for some negligible ε.*
2. *Π is not $\mathrm{learn}(*,ST)$-$\mathrm{chall}(*,CL,1\mathrm{ct})$-IND-CPA-secure: there exist a QPT adversary $\mathcal{A}$ making polynomially many ST-*

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 (on the one-way-function hypothesis). The hypothesis "assuming quantum-secure one-way functions exist" is supplied here rather than quoted. The source paper states this hypothesis for all of its proved separations (p. 6) but does not restate it for the six conjectured ones. Some assumption is in fact necessary: if no quantum-secure one-way function exists then no scheme is secure in either notion and the implication $P4 \Rightarrow P6$ holds vacuously. A reviewer should check that this is the intended reading and not a change of strength.

Remark 2 (representatives and panel bookkeeping). Conjecture 1 fixes one representative notion from each panel: learn$(*, ER)$-chall$(*, ER, \mathrm{ror})$ for $P4$ and learn$(*, ST)$-chall$(*, CL, 1\mathrm{ct})$ for $P6$. This is faithful only because the paper proves all notions inside a panel equivalent, so a reviewer should confirm the two memberships. Panel membership must be read off the paper's Figure 1 and Section 6, not off the boxed lists on pp. 4–5: the Panel 11 box on p. 5 duplicates the contents of the Panel 10 box, which is plainly a typo. That typo does not affect the two notions used here, but it affects panel bookkeeping generally.

Remark 3 (currency of the source). The source is a 2020 ePrint. A later revision, the peer-reviewed version, or follow-up work may have closed some of these cells; no resolution is known to the writer of this record, but this should be 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.