AICR · OPEN PROBLEM

A CPA-Secure Encryption Scheme That Only a Quantum Attacker Breaks

The source builds one for CCA-2 and for every symmetric-key primitive it tries; CPA-secure public-key encryption is the case its technique cannot reach

Status. Statement: AI-written from Alex Lombardi, Ethan Mook, Willy Quach and Daniel Wichs, *Post-Quantum Insecurity from LWE*, IACR ePrint 2022/869, TCC 2022. Not yet checked by a human. The source builds such schemes for PRFs, CPA-secure symmetric-key encryption, MACs, signatures and CCA-2-secure public-key encryption, and names the CPA public-key case as the first of the open problems its work leaves, with a stated reason why its technique stops there.

Category. *Post-quantum cryptography; counterexamples.*

Conjecture (informal). *LWE is believed to resist quantum attack, so it is tempting to think a scheme proved classically secure under LWE is automatically safe against quantum attackers. The source shows that is false, spectacularly: it builds a PRF, a symmetric-key encryption scheme, a MAC, a signature scheme and a CCA-2-secure public-key encryption scheme, each proved classically secure under LWE by a black-box reduction, each broken by a quantum attacker making two or three ordinary classical queries. The trick is that the security* game *is interactive even when the scheme is not, so a proof of quantumness can be hidden inside it. One primitive resists the trick, and it is the most basic public-key one: CPA-secure encryption. Its game has only three rounds and the last of them is publicly computable, which leaves nowhere to hide the secret state the technique needs.*

1 The setting

Post-quantum security here means what it usually means: the scheme, the honest parties and all communication stay classical, and only the adversary is quantum. The adversary keeps internal quantum state across the game but queries the cryptosystem on classical

inputs.

The phenomenon the source exploits is that a stateless, non-interactive primitive still has an *interactive* security game. A classical black-box reduction may rewind the adversary between the game's rounds; rewinding a quantum adversary that has measured is not possible. So a primitive can carry a valid classical security proof from LWE and still be quantumly broken, provided one can embed a source of interactive quantum advantage into its security game.

Two such sources are used.

- An *interactive proof of quantumness* (IPQ): a classical protocol that an efficient quantum prover passes and no efficient classical prover does. Four-message IPQs are known from LWE.
- A *quantum disclosure of secrets* (QDS): a protocol between a classical sender holding m and a receiver, where a quantum receiver learns m and a classical receiver learns nothing about it. The source constructs a three-message QDS from LWE.

Theorem 1 (What the source builds, [LMQW22, §1.1]). *Under LWE there exist: a PRF classically secure in the standard sense but broken by a quantum adversary making* 3 *classical queries (*2 *with public parameters); a CPA-secure symmetric-key encryption scheme broken by a quantum adversary making* 2 *encryption queries; a MAC broken with* 2 *authentication queries; a signature scheme broken with* 2 *signing queries; and a public-key encryption scheme that is classically CCA-2 secure but broken by a quantum adversary making* 2 *decryption queries before seeing the challenge ciphertext. All are proved classically secure under LWE via black-box reductions.*

2 Notation and parameters

- *Classically secure under LWE* means: there is a black-box reduction showing that any efficient classical attacker on the scheme yields an efficient classical algorithm for LWE.
- *Post-quantum insecure* means: some efficient quantum adversary, making only classical queries to the scheme, wins the standard security game with non-negligible advantage.
- The CPA game for public-key encryption has three rounds: the challenger sends pk; the adversary sends (m_0, m_1); the challenger sends $\mathsf{Enc}_{pk}(m_b)$. Its third round is a function of

the first two and of public randomness, and involves no secret held back by the challenger — this is the feature at issue.
- "q queries" below always means classical queries; the source does not consider superposition access.

3 The conjecture

Conjecture 1 ([LMQW22, §3]). *There exists a CPA-secure public-key encryption scheme that is classically secure under LWE via a black-box reduction, and post-quantum insecure.*

Remark 1 (How the source states it, and what is being supplied here). The source poses it as a question, first in a list headed "We mention several fascinating open problems left by our work", page 12: "Can we construct a CPA-secure public-key encryption scheme which is classically secure under LWE but post-quantum insecure?"

Turning that question into the existential proposition above is this statement's step, and it is the direction the source's own programme points: every other primitive it attempted, it built. A proof that no such scheme exists would be a far more surprising outcome and a much stronger result — it would say that for CPA-secure public-key encryption, classical security under LWE *does* imply post-quantum security — and it would settle the question just as well.

Remark 2 (The obstruction, in the source's own words). This is what makes the problem attackable rather than a wish: the source says exactly where its technique stops. "The CPA security game for public-key encryption consists of 3 rounds, so it may seem like we should be able to embed a QDS scheme inside it. But the 3rd round of the CPA security game must be publicly computable from the first 2 rounds, while our QDS requires secret state to compute the 3rd round."

Unpacked: the source's QDS is three-message, which fits the three rounds of the CPA game, but its sender must retain secret state between its first and third messages. In the CPA game the third round is the challenge ciphertext, which anybody holding pk and (m_0, m_1) can produce — there is no secret the challenger is holding back other than the bit b and its encryption randomness. So the

QDS sender cannot be the CPA challenger.

The CCA-2 case escapes precisely because the decryption oracle gives the challenger something secret to compute with, which is why Theorem 1 reaches CCA-2 and stops.

Remark 3 (Two routes the source names, both open). The source lists its open problems in a sequence, and two of the others are plausibly the way in to Conjecture 1 rather than independent questions.

"Can we construct a 3-message stateless/resettable QDS under LWE? This would allow us to construct cryptosystems that are classically secure in the standard sense under LWE, but fail to be even one-time post-quantum secure." A stateless three-message QDS is exactly what Remark 2 says is missing.

"Can we construct 3-message (resettably secure) IPQs from LWE?" Known IPQs from LWE take four messages, and three-message proofs of quantumness are not known under post-quantum assumptions in the plain model — the source says so when introducing its QDS, which is its workaround.

Neither is a substitute for the conjecture: they are sufficient routes, not equivalent statements.

Remark 4 (What a solution would mean). CPA-secure public-key encryption is the primitive under which most LWE-based deployments are argued. A counterexample there would say that the folklore inference — post-quantum assumption plus classical proof gives post-quantum security — fails at the most basic public-key primitive, not only at the elaborate ones. The source's framing of why such counterexamples matter applies with most force here: "Such counterexamples are extremely important and serve as a warning that can hopefully prevent us from making such mistakes in the future."

It is worth being explicit about what is *not* being suggested. The schemes in Theorem 1 are contrived, and the source says so in its abstract; none of this is evidence that LWE is quantumly easy or that any deployed scheme is at risk. The content is about what a classical proof does and does not buy.

4 Bibliography

[LMQW22] Alex Lombardi, Ethan Mook, Willy Quach and Daniel Wichs. *Post-quantum insecurity from LWE.* IACR ePrint 2022/869; TCC 2022. The source. The results are listed on pages 4 and 6 of the PDF; the open problems are Section 3, on page 12; quantum disclosure of secrets is Definition 5.14 with Theorem 5.15 and Corollary 5.16.

[BCM+18] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh V. Vazirani and Thomas Vidick. *A cryptographic test of quantumness and certifiable randomness from a single quantum device.* 59th FOCS, pages 320–331, IEEE Computer Society Press, October 2018. The four-message interactive proof of quantumness from LWE that the source starts from, and whose message count is what the three-round CPA game cannot accommodate.

[KLVY22] Yael Tauman Kalai, Alex Lombardi, Vinod Vaikuntanathan and Lisa Yang. *Quantum advantage from any non-local game.* IACR ePrint 2022/400. The compiler the source's quantum disclosure of secrets protocol relies on essentially.

[Reg05] Oded Regev. *On lattices, learning with errors, random linear codes, and cryptography.* 37th ACM STOC, pages 84–93, ACM Press, May 2005. The assumption the whole statement is relative to.

[BBK22] Nir Bitansky, Zvika Brakerski and Yael Tauman Kalai. *Constructive post-quantum reductions.* Cryptology ePrint Archive, 2022. Cited by the source in the two neighbouring open problems about one-way functions that are classically secure but post-quantum insecure given quantum auxiliary input.