

On the impossibility of Quantum Public Key Encryption

Samuel Bouaziz--Ermann Alex Bredariol Grilo Damien
Vergnaud Quoc-Huy Vu

Sorbonne Université, LIP6, CNRS

October 16, 2023



On quantum Public-Key Encryption

- Recently, it has been shown that quantum public key encryption (qPKE) with classical ciphertext is possible [Col23, BGHD⁺23, KMNY23] from OWF.
- However, distribution of quantum public key is problematic.
- With classical public key, we do not have this problem.

On quantum Public-Key Encryption

- Recently, it has been shown that quantum public key encryption (qPKE) with classical ciphertext is possible [Col23, BGHD⁺23, KMNY23] from OWF.
- However, distribution of quantum public key is problematic.
- With classical public key, we do not have this problem.

QPKE with classical public key

We ask:

Is quantum public key encryption with classical public key possible given one-way function?

Public Key Encryption with quantum ciphertexts

We define Public Key Encryption with quantum ciphertexts.

- $(pk, sk) \leftarrow Gen(1^v)$: outputs a classical key pair (pk, sk) .
- $|qc\rangle \leftarrow Enc(pk, m)$: takes as input a classical public key pk , a plaintext m , and outputs a quantum ciphertext $|qc\rangle$.
- $m/\perp \leftarrow Dec(sk, |qc\rangle)$: takes as input a decryption key sk , a ciphertext $|qc\rangle$, and outputs a classical plaintext m or an error symbol \perp .

Public Key Encryption with quantum ciphertexts

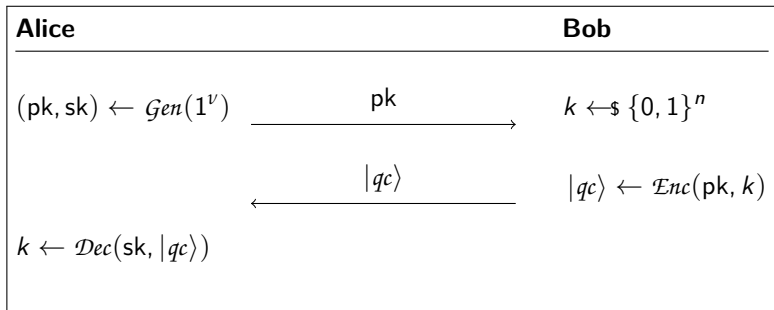
We define Public Key Encryption with quantum ciphertexts.

- $(pk, sk) \leftarrow \mathit{Gen}(1^v)$: outputs a classical key pair (pk, sk) .
- $|qc\rangle \leftarrow \mathit{Enc}(pk, m)$: takes as input a classical public key pk , a plaintext m , and outputs a quantum ciphertext $|qc\rangle$.
- $m/\perp \leftarrow \mathit{Dec}(sk, |qc\rangle)$: takes as input a decryption key sk , a ciphertext $|qc\rangle$, and outputs a classical plaintext m or an error symbol \perp .

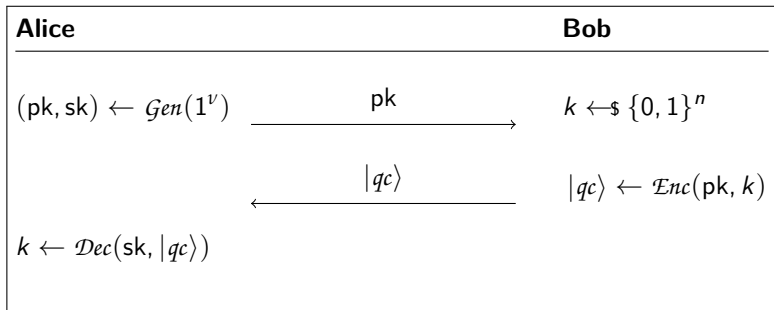
Claim

Public Key Encryption \implies *Key Distribution*

Proof that PKE implies KD

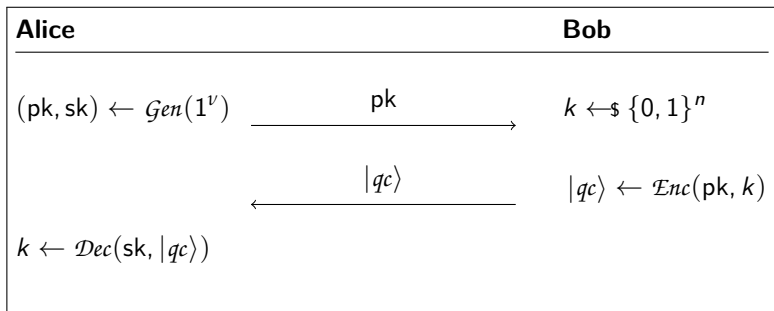


Proof that PKE implies KD



If key distribution is impossible, so is public key encryption.

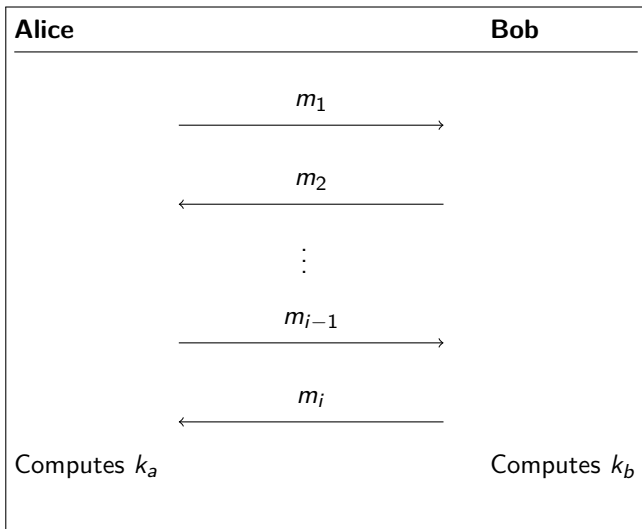
Proof that PKE implies KD



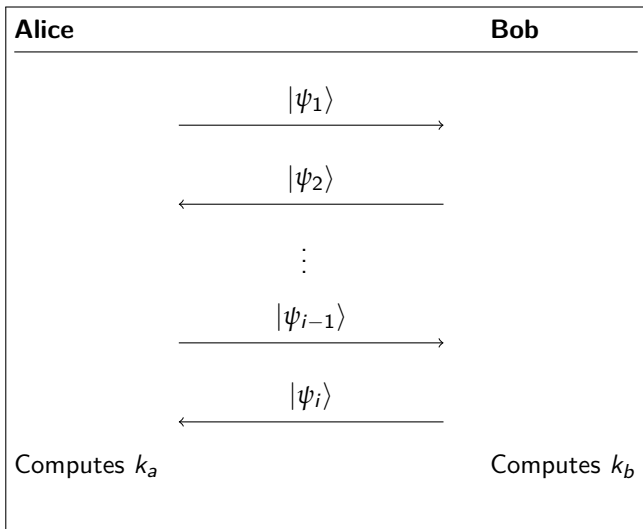
If key distribution is impossible, so is public key encryption.

But what kind of key distribution are we talking about here precisely?

Classical Key Distribution



Quantum Key Distribution



Claim ([IR89])

Information theoretical secure Key Distribution without assumption is impossible classically.

Claim ([IR89])

Information theoretical secure Key Distribution without assumption is impossible classically.

Claim ([BB84])

Information theoretical secure quantum key distribution is possible without assumptions.

One-Way Functions

- Alice and Bob know have access to a One-Way Function (OWF).
- A OWF is a function:

$$H: \mathcal{X} \rightarrow \mathcal{Y},$$

such that:

- for any $x \in \mathcal{X}$, $H(x)$ is easy to compute.
- given $H(x)$, finding x is hard.

Claim

Information theoretical secure Key Distribution with One-Way Function is impossible classically.

Claim

Information theoretical secure Key Distribution with One-Way Function is impossible classically.

Claim ([BM09], informal)

Let Π be a Key Distribution protocol, where Alice and Bob makes n queries to the OWF. Then, there exists an attacker Eve that finds the key with constant probability by making $\mathcal{O}(n^2)$ queries to the OWF.

Setting	Classical	Quantum
No assumption	✗[IR89]	✓[BB84]
With OWF	✗[IR89, BM09]	✓[BB84]

Setting	Classical	Quantum
No assumption	✗[IR89]	✓[BB84]
With OWF	✗[IR89, BM09]	✓[BB84]

Classical Communication Quantum Computation

Intermediary protocols, with quantum parties that communicates through a classical channel:

Classical Communication Quantum Computation (CCQC) Key Exchange protocols.

Claim

Conditioned on the Polynomial Compatibility Conjecture (PCC), information theoretical secure Key Distribution with One-Way Function is impossible in the CCQC setting.

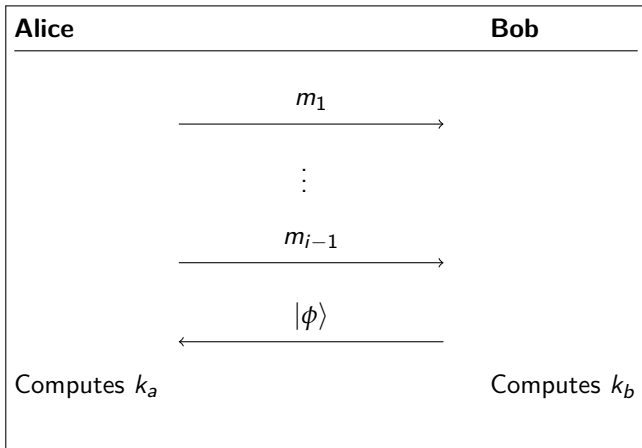
Claim

Conditioned on the Polynomial Compatibility Conjecture (PCC), information theoretical secure Key Distribution with One-Way Function is impossible in the CCQC setting.

Setting	Classical	CCQC	Quantum
No assumption	✗[IR89]	✗	✓[BB84]
With OWF	✗[IR89, BM09]	✗[ACC ⁺ 22]	✓[BB84]

Our result

We extend the previous result, to the case where the last message is quantum.



High level idea of the proof

- Using previous result, we can generate a state $|\psi_A^E\rangle$ that simulate Alice's internal state.

High level idea of the proof

- Using previous result, we can generate a state $|\psi_A^E\rangle$ that simulate Alice's internal state.
- We show that using this state and the message from Bob, Eve finds the key:

$$\left\| \Pi_{k_A} A_{fin} |\psi_A^E\rangle \otimes |\phi\rangle \right\| \geq 1 - \lambda.$$

High level idea of the proof

- Using previous result, we can generate a state $|\psi_A^E\rangle$ that simulate Alice's internal state.
- We show that using this state and the message from Bob, Eve finds the key:

$$\left\| \Pi_{k_A} A_{fin} |\psi_A^E\rangle \otimes |\phi\rangle \right\| \geq 1 - \lambda.$$

- Then, Eve outputs a message $|\phi^E\rangle$ that is close to the real message

$$\langle \phi^E | \phi \rangle \geq 1 - \lambda.$$

High level idea of the proof

- Using previous result, we can generate a state $|\psi_A^E\rangle$ that simulate Alice's internal state.
- We show that using this state and the message from Bob, Eve finds the key:

$$\left\| \Pi_{k_A} A_{fin} |\psi_A^E\rangle \otimes |\phi\rangle \right\| \geq 1 - \lambda.$$

- Then, Eve outputs a message $|\phi^E\rangle$ that is close to the real message

$$\langle \phi^E | \phi \rangle \geq 1 - \lambda.$$

- Finally, we show that given this message, Alice computes the right key

$$\left\| \Pi_{k_A} A_{fin} |\psi_A\rangle \otimes |\phi\rangle \right\| \geq 1 - \lambda.$$

Theorem (Informal)

Let Π be a key agreement protocol between Alice and Bob in our setting. Let n be the number of queries that Alice and Bob make to the OWF. Then, Eve can find the key with $\mathcal{O}(\text{poly}(n))$ classical queries to the OWF with constant probability.

Theorem (Informal)

Let Π be a key agreement protocol between Alice and Bob in our setting. Let n be the number of queries that Alice and Bob make to the OWF. Then, Eve can find the key with $\mathcal{O}(\text{poly}(n))$ classical queries to the OWF with constant probability.

Limitations and implications of our result

- In our setting, Alice cannot query the OWF after receiving the last message.
- This means a separation result for qPKE with classical public key, where $\text{Dec}(\cdot, \cdot)$ does not query the oracle.

Contributions

- Impossibility result for quantum PKE from OWF.
- Better understanding of Quantum Key Distribution.

Open questions

- Better understanding of quantum PKE.
- Proving the Polynomial Compatibility Conjecture.
- Extend result to the case where the decryption algorithm can query the oracle.



Per Austrin, Hao Chung, Kai-Min Chung, Shiuan Fu, Yao-Ting Lin, and Mohammad Mahmoody.

On the impossibility of key agreements from quantum random oracles.
In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part II*, volume 13508 of *LNCS*, pages 165–194. Springer, Heidelberg, August 2022.



Charles H. Bennett and Gilles Brassard.

Quantum cryptography: Public key distribution and coin tossing.
In *EEE International Conference on Computers, Systems and Signal Processing*, volume 175, page 8, 1984.



Khashayar Barooti, Alex B. Grilo, Loïs Huguenin-Dumittan, Giulio Malavolta, Or Sattath, Quoc-Huy Vu, and Michael Walter.

Public-key encryption with quantum keys.
Cryptology ePrint Archive, Paper 2023/877, 2023.
<https://eprint.iacr.org/2023/877>.



Boaz Barak and Mohammad Mahmoody-Ghidary.

Merkle puzzles are optimal - an $O(n^2)$ -query attack on any key exchange from a random oracle.

In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 374–390. Springer, Heidelberg, August 2009.

Conjecture (Polynomial Compatibility Conjecture)

There exists a finite abelian group and a function $\delta(d) = \frac{1}{\text{poly}(d)}$ such that the following holds for all d . Let \mathbf{F} and \mathbf{G} be two distributions of functions from \mathbb{N} to \mathbb{R} such that the following holds for all $f \in \text{supp}(\mathbf{F})$ and $g \in \text{supp}(\mathbf{G})$.

- **Unit ℓ_2 norm:** f and g have ℓ_2 -norm 1.
- **d -degrees:** $\deg(f) \leq d$ and $\deg(g) \leq d$.
- **δ -influences on average:** For all $i \in \mathbb{N}$, we have $\mathbb{E}_{f \leftarrow \mathbf{F}}[\text{Inf}_i(f)] \leq \delta$ and $\mathbb{E}_{g \leftarrow \mathbf{G}}[\text{Inf}_i(g)] \leq \delta$, where $\delta = \delta(d)$.

Then, there is an $f \in \text{supp}(\mathbf{F})$, $g \in \text{supp}(\mathbf{G})$ and $x \in \mathbb{N}$ such that $f(x) \cdot g(x) \neq 0$.