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.

Quantum Public Key Encryption

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.

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

Link to Key Distribution

Public Key Encryption with quantum ciphertexts

We define Public Key Encryption with quantum ciphertexts.

- $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{Gen}(1^{\nu})$: outputs a classical key pair $(\mathsf{pk}, \mathsf{sk})$.
- $|qc\rangle \leftarrow \mathcal{Enc}(\mathsf{pk}, m)$: takes as input a classical public key pk, a plaintext m, and outputs a quantum ciphertext $|qc\rangle$.
- $m/\perp \leftarrow \mathcal{Dec}(\mathsf{sk}, |qc\rangle)$: 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*

Alice		**Bob**
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{Gen}(1^\nu)$	$\xrightarrow{\quad \mathsf{pk} \quad}$	$k \leftarrow_\$ \{0,1\}^n$
	$\xleftarrow{\quad \lvert qc\rangle \quad}$	$\lvert qc\rangle \leftarrow \mathcal{Enc}(\mathsf{pk}, k)$
$k \leftarrow \mathcal{Dec}(\mathsf{sk}, \lvert qc\rangle)$		

Proof that PKE implies KD

Alice		**Bob**
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{Gen}(1^\nu)$	$\xrightarrow{\mathsf{pk}}$	$k \leftarrow_\$ \{0,1\}^n$
	$\xleftarrow{\lvert qc\rangle}$	$\lvert qc\rangle \leftarrow \mathcal{Enc}(\mathsf{pk}, k)$
$k \leftarrow \mathcal{Dec}(\mathsf{sk}, \lvert qc\rangle)$		

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

Proof that PKE implies KD

Alice		**Bob**
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{Gen}(1^\nu)$	$\xrightarrow{\mathsf{pk}}$	$k \leftarrow_\$ \{0,1\}^n$
	$\xleftarrow{\lvert qc \rangle}$	$\lvert qc \rangle \leftarrow \mathcal{Enc}(\mathsf{pk}, k)$
$k \leftarrow \mathcal{Dec}(\mathsf{sk}, \lvert qc \rangle)$		

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

Alice		**Bob**
	$\xrightarrow{\quad m_1 \quad}$	
	$\xleftarrow{\quad m_2 \quad}$	
	$\vdots$	
	$\xrightarrow{\quad m_{i-1} \quad}$	
	$\xleftarrow{\quad m_i \quad}$	
Computes k_a		Computes k_b

Alice **Bob**

$$\xrightarrow{|\psi_1\rangle}$$

$$\xleftarrow{|\psi_2\rangle}$$

$$\vdots$$

$$\xrightarrow{|\psi_{i-1}\rangle}$$

$$\xleftarrow{|\psi_i\rangle}$$

Computes k_a Computes k_b

Claim ([IR89])

Information theoretical secure Key Distribution without assumption is impossible classically.

Key Exchange in the Plain Model

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:

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

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

KE with OWF

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 $\mathcal{O}\left(n^2\right)$ queries to the OWF.

Classical Communication Quantum Computation

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

Classical Communication Quantum Computation

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.

CCQC Impossibility result

Claim

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

CCQC Impossibility result

Claim

Conditionned 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.

Alice		**Bob**
	$\xrightarrow{m_1}$	
	$\vdots$	
	$\xrightarrow{m_{i-1}}$	
	$\xleftarrow{\vert\phi\rangle}$	
Computes k_a		Computes k_b

High level idea of the proof

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

High level idea of the proof

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

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

High level idea of the proof

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

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

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

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

High level idea of the proof

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

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

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

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

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

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

Discussion

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 $\mathcal{O}(\mathrm{poly}(n))$ classical queries to the OWF with constant probability.

Discussion

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 $\mathcal{Dec}(\cdot, \cdot)$ does not query the oracle.

Discussion

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.

Bibliography

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.

Polynomial Compatibility Conjecture

Conjecture (Polynomial Compatibility Conjecture)

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

- ***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* $\mathbb{E}_{f \leftarrow \mathbf{F}}[Inf_i(f)] \leq \delta$ *and* $\mathbb{E}_{g \leftarrow \mathbf{G}}[Inf_i(g)] \leq \delta$*, where* $\delta = \delta(d)$*.*

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