Public-key Encryption with Quantum Keys

Quoc-Huy Vu

joint work with:

Khashayar Barooti Alex B. Grilo Loïs Huguenin-Dumittan

Giulio Malavolta Or Sattath Michael Walter

TCC 2023

November, 2023

Impagliazzo's Cryptographic Worlds

Cryptomania: public-key cryptography exists

Public-key encryption | Oblivious transfer (MPC) | Key-Agreement

Minicrypt: one-way functions exist

OWF | PRG | PRF | Signature | Private-key encryption | Zero-knowledge proofs | Commitment

Impagliazzo's Cryptographic Worlds in Quantumania

Cryptomania: public-key cryptography exists

↑ ✗ Public-key encryption

Mini Q crypt [GLSV'20, BCKM'20]

Minicrypt Q-oblivious transfer QSMPC

Q: quantum computation & quantum communication

Impagliazzo's Cryptographic Worlds in Quantumania

Cryptomania: public-key cryptography exists

Public-key encryption ✗

Mini Q crypt [GLSV'20, BCKM'20]

Minicrypt   Q-oblivious transfer   QSMPC

? Can we go even lower?

Q: quantum computation & quantum communication

Pseudorandom State Generator*

No quantum poly-time algorithm can distinguish (copies of) output of G from (copies of) an n-qubit state sampled from the Haar distribution

* ([JLS'18])

Pseudorandom State Generator*

No quantum poly-time algorithm can distinguish (copies of) output of G from (copies of) an n-qubit state sampled from the Haar distribution

Uniform distribution over quantum states over $\mathbb{C}^{2^n}$

* ([JLS'18])

Pseudorandom State Generator*

No quantum poly-time algorithm can distinguish (copies of) output of G from (copies of) an n-qubit state sampled from the Haar distribution

Fact: In 2021, Kretschmer showed OWFs cannot be constructed from PRS in black-box way.

* ([JLS'18])

Pseudorandom State Generator*

No quantum poly-time algorithm can distinguish (copies of) output of G from (copies of) an n-qubit state sampled from the Haar distribution

Fact: In 2021, Kretschmer showed OWFs cannot be constructed from PRS in black-box way.

Extension: Pseudorandom Function-like States is a keyed version of PRS [AQY'21]

* ([JLS'18])

Pseudorandom State Generator*

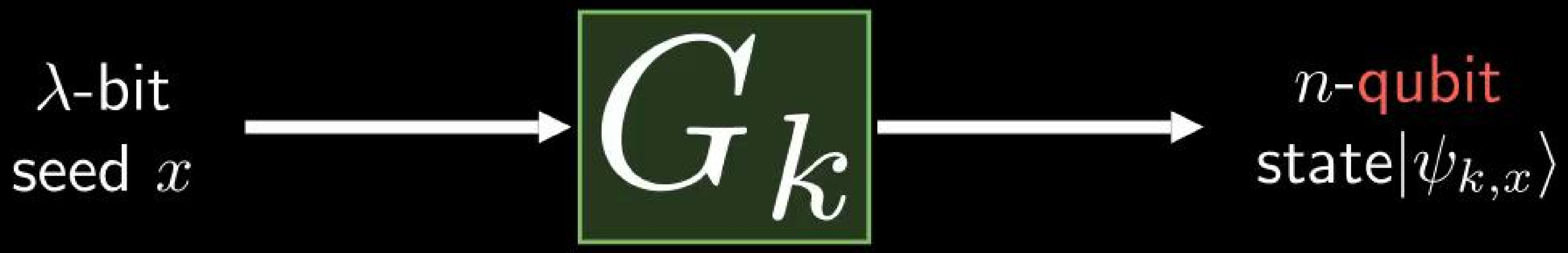
No quantum poly-time algorithm can distinguish (copies of) output of G from (copies of) an n-qubit state sampled from the Haar distribution

Fact: In 2021, Kretschmer showed OWFs cannot be constructed from PRS in black-box way.

Extension: Pseudorandom Function-like States is a keyed version of PRS [AQY'21]

* ([JLS'18])

Pseudorandom State Generator*



No quantum poly-time algorithm can distinguish (copies of) output of G from (copies of) an n-qubit state sampled from the Haar distribution

Fact: In 2021, Kretschmer showed OWFs cannot be constructed from PRS in black-box way.

Extension: Pseudorandom Function-like States is a keyed version of PRS [AQY'21]

* ([JLS'18])

Impagliazzo's Cryptographic Worlds in Quantumania

Cryptomania: public-key cryptography exists

↑ ✗ Public-key encryption

Mini Q crypt [GLSV'20, BCKM'20]

Minicrypt Q-oblivious transfer QSMPC

? Can we go even lower?

Q: quantum computation & quantum communication

Impagliazzo's Cryptographic Worlds in Quantumania

Cryptomania: public-key cryptography exists

Public-key encryption ✗

Mini Q crypt [GLSV'20, BCKM'20]

Minicrypt

Micro Q crypt: pseudorandom quantum states exist [JLS'18, Kre'21, MY'21, AQY'21]

One-time Q-signature | Q-pseudo OTP | QZKP | Q-commitment | QSMPC

Q: quantum computation & quantum communication

Impagliazzo's Cryptographic Worlds in Quantumania

Cryptomania: public-key cryptography exists

↑ ✗ Public-key encryption

Mini Q crypt [GLSV'20, BCKM'20]

↑ ✗ Minicrypt

Micro Q crypt: pseudorandom quantum states exist [JLS'18, Kre'21, MY'21, AQY'21]

One-time Q-signature — Q-pseudo OTP — QZKP — Q-commitment — QSMPC

Q: quantum computation & quantum communication

Impagliazzo's Cryptographic Worlds in Quantumania

Impagliazzo's Cryptographic Worlds in Quantumania

Cryptomania: public-key cryptography exists

Public-key encryption ✗

Where to put (quantum) public-key encryption?

Mini Q crypt [GLSV'20, BCKM'20]

Minicrypt ✗

Micro Q crypt: pseudorandom quantum states exist [JLS'18, Kre'21, MY'21, AQY'21]

One-time Q-signature | Q-pseudo OTP | QZKP | Q-commitment | QSMPC

Q: quantum computation & quantum communication

Our Work: Quantum Public-Key Encryption (qPKE)

Definitions — syntax and security definitions for qPKE

- classical/quantum public-keys
- classical/quantum ciphertexts

Our Work: Quantum Public-Key Encryption (qPKE)

Definitions

syntax and security definitions for qPKE

- classical/quantum public-keys
- classical/quantum ciphertexts

Constructions

qPKE with quantum public-keys

- classical ciphertexts from OWFs
- quantum ciphertexts from PRFS

Our Work: Quantum Public-Key Encryption (qPKE)

Definitions

syntax and security definitions for qPKE

- classical/quantum public-keys
- classical/quantum ciphertexts

Constructions

qPKE with quantum public-keys

- classical ciphertexts from OWFs
- quantum ciphertexts from PRFS

Impossibility

unconditional security of qPKE

- uses quantum shadow tomography to learn the secret-key from public-keys

*another proof using quantum Shanon's bound [MY22]

qPKE: Definitions

Key generation

$\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$

*sk is classical

$|\mathsf{pk}\rangle^{\otimes t} \leftarrow \mathsf{QPKGen}^{\otimes t}(\mathsf{sk})$

* $|\mathsf{pk}\rangle$ is a pure state

qPKE: Definitions

Key generation

$\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$

*sk is classical

$|\mathsf{pk}\rangle^{\otimes t} \leftarrow \mathsf{QPKGen}^{\otimes t}(\mathsf{sk})$

* $|\mathsf{pk}\rangle$ is a pure state

Encryption

$\rho \leftarrow \mathsf{Encrypt}(|\mathsf{pk}\rangle, m)$

* ρ can be either classical or quantum

qPKE: Definitions

Key generation

$\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$

*sk is classical

$|\mathsf{pk}\rangle^{\otimes t} \leftarrow \mathsf{QPKGen}^{\otimes t}(\mathsf{sk})$

* $|\mathsf{pk}\rangle$ is a pure state

Encryption

$\rho \leftarrow \mathsf{Encrypt}(|\mathsf{pk}\rangle, m)$

* ρ can be either classical or quantum

Decryption

$m \leftarrow \mathsf{Decrypt}(\mathsf{sk}, \rho)$

qPKE: Definitions

Key generation

$\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$

*sk is classical

$|\mathsf{pk}\rangle^{\otimes t} \leftarrow \mathsf{QPKGen}^{\otimes t}(\mathsf{sk})$

* $|\mathsf{pk}\rangle$ is a pure state

Encryption

$\rho \leftarrow \mathsf{Encrypt}(|\mathsf{pk}\rangle, m)$

* ρ can be either classical or quantum

Decryption

$m \leftarrow \mathsf{Decrypt}(\mathsf{sk}, \rho)$

Semantic Security

$\forall$ QPT $\mathcal{A}$:

$$\{ |\mathsf{pk}\rangle^{\otimes t}, \mathsf{Encrypt}(0) \} \approx \{ |\mathsf{pk}\rangle^{\otimes t}, \mathsf{Encrypt}(1) \}$$

qPKE: Definitions

Key generation

$\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$

*sk is classical

$|\mathsf{pk}\rangle^{\otimes t} \leftarrow \mathsf{QPKGen}^{\otimes t}(\mathsf{sk})$

* $|\mathsf{pk}\rangle$ is a pure state

Encryption

$\rho \leftarrow \mathsf{Encrypt}(|\mathsf{pk}\rangle, m)$

*ρ can be either classical or quantum

Decryption

$m \leftarrow \mathsf{Decrypt}(\mathsf{sk}, \rho)$

Semantic Security

$\forall$ QPT $\mathcal{A}$:

$$\{ |\mathsf{pk}\rangle^{\otimes t}, \mathsf{Encrypt}(0) \} \approx \{ |\mathsf{pk}\rangle^{\otimes t}, \mathsf{Encrypt}(1) \}$$

- $|\mathsf{pk}\rangle$ is generically unclonable, thus poly-many copies are given to the adversaries

qPKE: Definitions

Key generation

$\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$

*sk is classical

$|\mathsf{pk}\rangle^{\otimes t} \leftarrow \mathsf{QPKGen}^{\otimes t}(\mathsf{sk})$

* $|\mathsf{pk}\rangle$ is a pure state

Encryption

$\rho \leftarrow \mathsf{Encrypt}(|\mathsf{pk}\rangle, m)$

*ρ can be either classical or quantum

Decryption

$m \leftarrow \mathsf{Decrypt}(\mathsf{sk}, \rho)$

Semantic Security

$\forall$ QPT $\mathcal{A}$:

$$\{\, |\mathsf{pk}\rangle^{\otimes t}, \mathsf{Encrypt}(0) \} \approx \{\, |\mathsf{pk}\rangle^{\otimes t}, \mathsf{Encrypt}(1) \}$$

- $|\mathsf{pk}\rangle$ is generically unclonable, thus poly-many copies are given to the adversaries
- $|\mathsf{pk}\rangle$ is pure implying a non-trivial way to distribute quantum public keys

qPKE: Definitions

Key generation

$\mathsf{sk} \leftarrow \mathsf{Gen}(1^\lambda)$

*sk is classical

$|\mathsf{pk}\rangle^{\otimes t} \leftarrow \mathsf{QPKGen}^{\otimes t}(\mathsf{sk})$

* $|\mathsf{pk}\rangle$ is a pure state

Encryption

$\rho \leftarrow \mathsf{Encrypt}(|\mathsf{pk}\rangle, m)$

*ρ can be either classical or quantum

Decryption

$m \leftarrow \mathsf{Decrypt}(\mathsf{sk}, \rho)$

Semantic Security

$\forall$ QPT $\mathcal{A}$:

$$\{ |\mathsf{pk}\rangle^{\otimes t}, \mathsf{Encrypt}(0) \} \approx \{ |\mathsf{pk}\rangle^{\otimes t}, \mathsf{Encrypt}(1) \}$$

- $|\mathsf{pk}\rangle$ is generically unclonable, thus poly-many copies are given to the adversaries
- $|\mathsf{pk}\rangle$ is pure implying a non-trivial way to distribute quantum public keys
    - $|\mathsf{pk}\rangle$ is sent to different CAs and use SWAP-test for validation [Gottesman'05]
    - Only achieve inverse-poly soundness error

qPKE: A Simple Construction from OWFs

Key generation

1. $\mathsf{sk} \leftarrow \{0,1\}^\lambda$
2. $|\mathsf{pk}\rangle \leftarrow \sum_x |x, \mathsf{PRF}(\mathsf{sk}, x)\rangle$

qPKE: A Simple Construction from OWFs

Key generation

1. $\mathsf{sk} \leftarrow \{0,1\}^\lambda$
2. $|\mathsf{pk}\rangle \leftarrow \sum_x |x, \mathsf{PRF}(\mathsf{sk}, x)\rangle$

Encryption

1. Measure $|\mathsf{pk}\rangle$ to get $x, y = \mathsf{PRF}(\mathsf{sk}, x)$
2. Sample a uniformly random r
3. Encrypt $m \in \{0,1\}$ as $c = (r, x, \mathsf{PRF}(y, r\|m))$

qPKE: A Simple Construction from OWFs

Key generation

1. $\mathsf{sk} \leftarrow \{0,1\}^\lambda$
2. $|\mathsf{pk}\rangle \leftarrow \sum_x |x, \mathsf{PRF}(\mathsf{sk}, x)\rangle$

Encryption

1. Measure $|\mathsf{pk}\rangle$ to get $x, y = \mathsf{PRF}(\mathsf{sk}, x)$
2. Sample a uniformly random r
3. Encrypt $m \in \{0,1\}$ as $c = (r, x, \mathsf{PRF}(y, r\|m))$

Decryption

1. Compute $y \leftarrow \mathsf{PRF}(\mathsf{sk}, x)$
2. Return 0 if $c = \mathsf{PRF}(y, r\|0)$, 1 otherwise.

qPKE: A Construction from PRFS

Key generation

1. $\mathsf{sk} \leftarrow \{0,1\}^\lambda$
2. $|\mathsf{pk}\rangle \leftarrow \sum_x |x, \psi_{\mathsf{sk},x}\rangle$

qPKE: A Construction from PRFS

Key generation

1. $\mathsf{sk} \leftarrow \{0,1\}^\lambda$
2. $|\mathsf{pk}\rangle \leftarrow \sum_x |x, \psi_{\mathsf{sk},x}\rangle$

Encryption

1. Measure $|\mathsf{pk}\rangle$ to get $(x, |\psi_{\mathsf{sk},x}\rangle)$ // only measure the first register
2. If $m = 0$, return $(x, |\psi_{\mathsf{sk},x}\rangle)$
3. Else, return $(x, \frac{\mathcal{I}}{2^n})$ // i.e., a maximally mixed state

qPKE: A Construction from PRFS

Key generation

1. $\mathsf{sk} \leftarrow \{0,1\}^\lambda$
2. $|\mathsf{pk}\rangle \leftarrow \sum_x |x, \psi_{\mathsf{sk},x}\rangle$

Encryption

1. Measure $|\mathsf{pk}\rangle$ to get $(x, |\psi_{\mathsf{sk},x}\rangle)$ // only measure the first register
2. If $m = 0$, return $(x, |\psi_{\mathsf{sk},x}\rangle)$
3. Else, return $(x, \frac{\mathcal{I}}{2^n})$ // i.e., a maximally mixed state

Decryption

1. Interpret c as $(x, |\phi\rangle)$
1. Return 0 if $|\phi\rangle = |\psi_{\mathsf{sk},x}\rangle$, 1 otherwise

Impossibility

Step 1. Let $|\mathsf{pk}^*\rangle$ be the honestly generated public key.
Our first observation is that, for any other $|\mathsf{pk}'\rangle$, if $|\mathsf{pk}^*\rangle$ and $|\mathsf{pk}'\rangle$ are close, then we can use the corresponding secret key of $|\mathsf{pk}'\rangle$ to decrypt the ciphertext encrypted with $|\mathsf{pk}^*\rangle$

Impossibility

Step 1. Let $|\mathsf{pk}^*\rangle$ be the honestly generated public key.
Our first observation is that, for any other $|\mathsf{pk}'\rangle$, if $|\mathsf{pk}^*\rangle$ and $|\mathsf{pk}'\rangle$ are close, then we can use the corresponding secret key of $|\mathsf{pk}'\rangle$ to decrypt the ciphertext encrypted with $|\mathsf{pk}^*\rangle$

$$\Pr\left[\mathsf{Decrypt}(\mathsf{sk}, \rho) = m \;\middle|\; \begin{array}{r} |\mathsf{pk}'\rangle \leftarrow \mathsf{QPKGen}(\mathsf{sk}) \\ m \xleftarrow{\$} \{0,1\} \\ (\rho, \cdot) \leftarrow \mathsf{Encrypt}(|\mathsf{pk}^*\rangle, m) \end{array}\right] \geq 1 - 3\varepsilon \text{ if } \|\langle \mathsf{pk}' | \mathsf{pk}^* \rangle\| \geq 1 - \varepsilon$$

Impossibility

Step 1. Let $|\mathsf{pk}^*\rangle$ be the honestly generated public key.
Our first observation is that, for any other $|\mathsf{pk}'\rangle$, if $|\mathsf{pk}^*\rangle$ and $|\mathsf{pk}'\rangle$ are close, then we can use the corresponding secret key of $|\mathsf{pk}'\rangle$ to decrypt the ciphertext encrypted with $|\mathsf{pk}^*\rangle$

$$\Pr\left[\mathsf{Decrypt}(\mathsf{sk}, \rho) = m \;\middle|\; \begin{array}{r} |\mathsf{pk}'\rangle \leftarrow \mathsf{QPKGen}(\mathsf{sk}) \\ m \xleftarrow{\$} \{0,1\} \\ (\rho, \cdot) \leftarrow \mathsf{Encrypt}(|\mathsf{pk}^*\rangle, m) \end{array}\right] \geq 1 - 3\varepsilon \text{ if } \|\langle \mathsf{pk}' | \mathsf{pk}^* \rangle\| \geq 1 - \varepsilon$$

Step 2. Estimate all the values $\|\langle \mathsf{pk}' | \mathsf{pk}^* \rangle\|$ for all sk from random Clifford measurements on polynomially many copies of $|\mathsf{pk}^*\rangle$

Impossibility

Step 1. Let $|\mathsf{pk}^*\rangle$ be the honestly generated public key.
Our first observation is that, for any other $|\mathsf{pk}'\rangle$, if $|\mathsf{pk}^*\rangle$ and $|\mathsf{pk}'\rangle$ are close, then we can use the corresponding secret key of $|\mathsf{pk}'\rangle$ to decrypt the ciphertext encrypted with $|\mathsf{pk}^*\rangle$

$$\Pr\left[\mathsf{Decrypt}(\mathsf{sk},\rho) = m \;\middle|\; \begin{array}{r} |\mathsf{pk}'\rangle \leftarrow \mathsf{QPKGen}(\mathsf{sk}) \\ m \xleftarrow{\$} \{0,1\} \\ (\rho,\cdot) \leftarrow \mathsf{Encrypt}(|\mathsf{pk}^*\rangle, m) \end{array}\right] \geq 1 - 3\varepsilon \text{ if } \|\langle \mathsf{pk}'|\mathsf{pk}^*\rangle\| \geq 1-\varepsilon$$

Step 2. Estimate all the values $\|\langle \mathsf{pk}'|\mathsf{pk}^*\rangle\|$ for all sk from random Clifford measurements on polynomially many copies of $|\mathsf{pk}^*\rangle$

This is done using the shadow tomography technique [HKP'20]

Conclusion

This talk:

- definitions of quantum public-key encryption
- (im)possibility of constructing qPKE

Caveats:

- broken if quantum public keys are tampered
- a single public key can be used to by only one encryptor

Conclusion

This talk:

- definitions of quantum public-key encryption
- (im)possibility of constructing qPKE

Caveats:

- broken if quantum public keys are tampered
- a single public key can be used to by only one encryptor

Open questions:

- distribution of quantum public-keys (follow-up works [KMNY23], [MW23])
- (im)possibility of reusable qPKE

Conclusion

This talk:

- definitions of quantum public-key encryption
- (im)possibility of constructing qPKE

Caveats:

- broken if quantum public keys are tampered
- a single public key can be used to by only one encryptor

Open questions:

- distribution of quantum public-keys (follow-up works [KMNY23], [MW23])
- (im)possibility of reusable qPKE

Thank you!

Conclusion

This talk:

- definitions of quantum public-key encryption
- (im)possibility of constructing qPKE

Caveats:

- broken if quantum public keys are tampered
- a single public key can be used to by only one encryptor

Open questions:

- distribution of quantum public-keys (follow-up works [KMNY23], [MW23])
- (im)possibility of reusable qPKE

Thank you!