On the power of non-adaptive quantum chosen-ciphertext attacks

joint work with Gorjan Alagic (UMD, NIST), Stacey Jeffery (QuSoft, CWI), and Maris Ozols (QuSoft, UvA)

Alexander Poremba

August 29, 2018

Heidelberg University; California Institute of Technology

QCrypt 2018

Cryptography + Quantum Computation

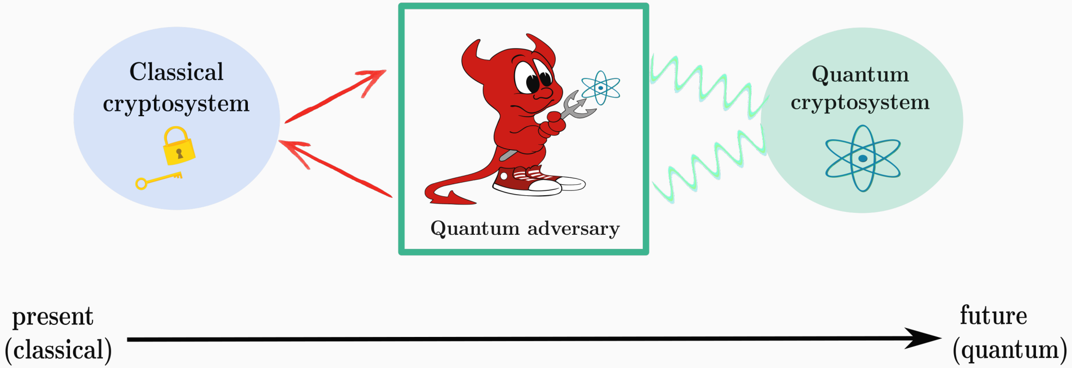
post-quantum cryptography

fully quantum cryptography

Cryptography + Quantum Computation

post-quantum cryptography

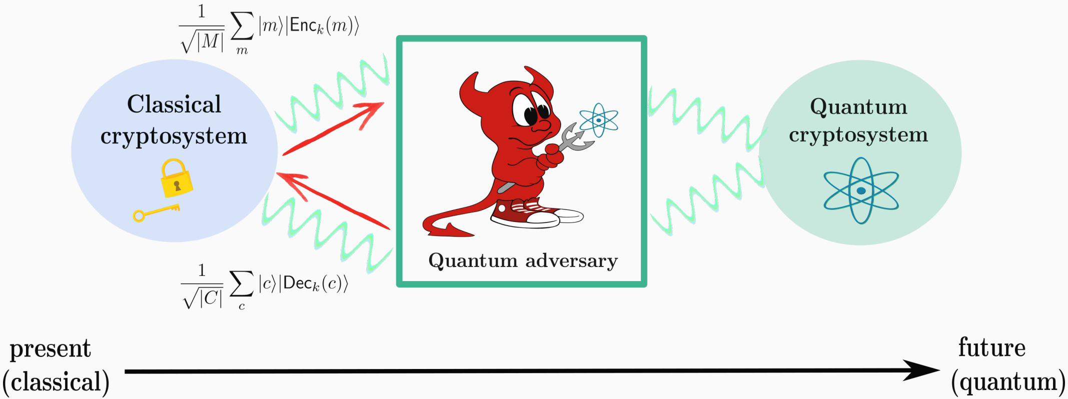
fully quantum cryptography



Cryptography + Quantum Computation

post-quantum cryptography

fully quantum cryptography

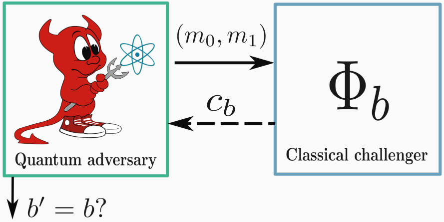


Security in a quantum world

What makes a classical scheme $\Pi = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ "quantum-secure"?

- ciphertexts reveal **no information** about plaintexts (should look "indistinguishable")
- assumption that adversaries are quantum, i.e. run in quantum polynomial-time (QPT).

IndGame:



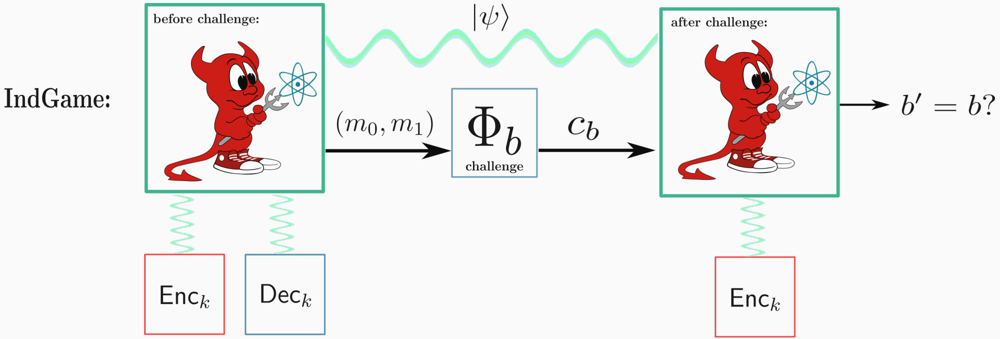
$$c_b = \begin{cases} \mathsf{Enc}_k(m_0), & b = 0 \\ \mathsf{Enc}_k(m_1), & b = 1 \end{cases}$$

Definition: (Indistinguishability - IND)

Π has **indistinguishable ciphertexts** if $\forall$QPT $\mathcal{A}$: $\quad \Pr[\mathcal{A} \text{ wins IndGame}] = 1/2 + \mathsf{negl}(n)$

Non-adaptive quantum chosen-ciphertext attacks (AJOP'18)

What if $\mathcal{A}$ gets lunch-time access to encryption & decryption?($\implies$ chosen-ciphertext attack)

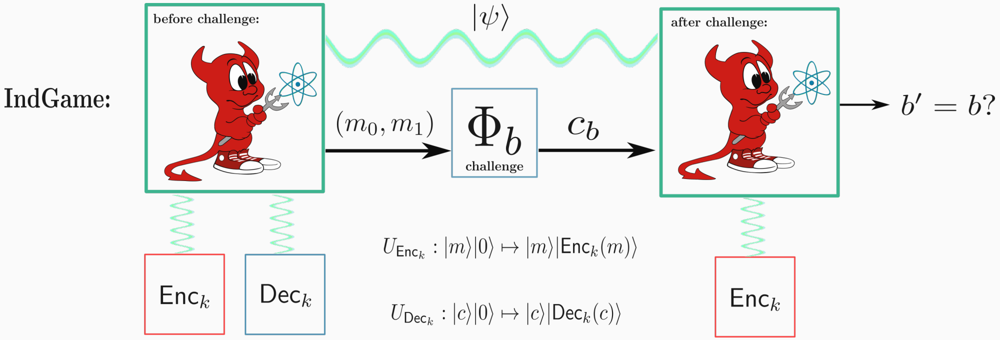


Definition: (Non-adaptive quantum chosen-ciphertext security)

Π is **IND-QCCA1** secure if $\forall$QPT $\mathcal{A}$: $\Pr[\mathcal{A} \text{ wins IndGame}] = 1/2 + \mathsf{negl}(n)$

Non-adaptive quantum chosen-ciphertext attacks (AJOP'18)

What if $\mathcal{A}$ gets lunch-time access to encryption & decryption?($\implies$ chosen-ciphertext attack)

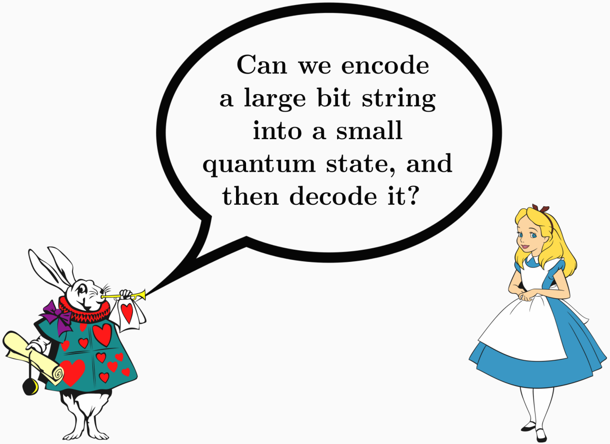


Definition: (Non-adaptive quantum chosen-ciphertext security)

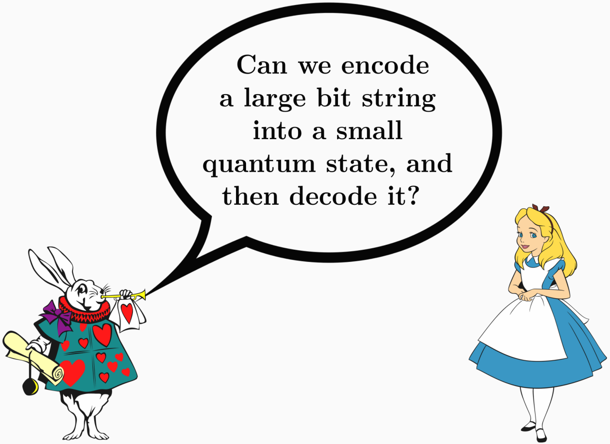
Π is **IND-QCCA1** secure if $\forall$QPT $\mathcal{A}$: $\quad \Pr[\mathcal{A} \text{ wins IndGame}] = 1/2 + \mathsf{negl}(n)$

A secure encryption scheme

Quantum random access codes (Ambainis et al.'08)



Quantum random access codes (Ambainis et al.'08)



Lemma: (AJOP'18)

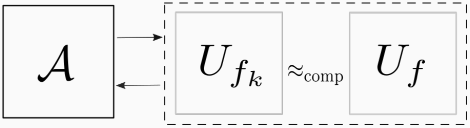
Average bias on message length $N = 2^n$ and poly(n)-sized quantum state is $O(2^{-n/2}\,\text{poly}(n))$.

A secure symmetric-key encryption scheme

Theorem: (AJOP'18)

The construction $\Pi = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ with QPRF $\{f_k : \{0,1\}^n \mapsto \{0,1\}^n\}$ is IND-QCCA1:

- KeyGen: sample a key $k \overset{\$}{\leftarrow} \{0,1\}^n$
- $\mathsf{Enc}_k(m) = (r, f_k(r) \oplus m)$, for $r \overset{\$}{\leftarrow} \{0,1\}^n$
- $\mathsf{Dec}_k(r, c) = c \oplus f_k(r)$



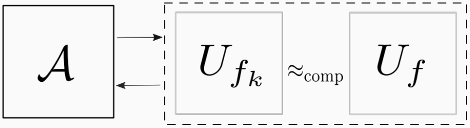
quantum-secure pseudorandom function (QPRF)

A secure symmetric-key encryption scheme

Theorem: (AJOP'18)

The construction $\Pi = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ with QPRF $\{f_k : \{0,1\}^n \mapsto \{0,1\}^n\}$ is IND-QCCA1:

- KeyGen: sample a key $k \xleftarrow{\$} \{0,1\}^n$
- $\mathsf{Enc}_k(m) = (r, f_k(r) \oplus m)$, for $r \xleftarrow{\$} \{0,1\}^n$
- $\mathsf{Dec}_k(r, c) = c \oplus f_k(r)$



quantum-secure pseudorandom function (QPRF)

Proof idea.

Fix a QPT adversary $\mathcal{A}$.

1. Replace f_k with a random function f (by the QPRF assumption)
2. **QRAC reduction**: Use $\mathcal{A}$ against IND-QCCA1 security to construct a code. By Lemma, the advantage is $\epsilon = O(2^{-n/2}\,\mathrm{poly}(n))$. □

Learning with Errors

Learning with Errors (Regev '05)

Learning with Errors (LWE)

- primary basis of hardness for post-quantum cryptography
- allows for PKE, FHE, QPRFs, . . .

Learning with Errors (Regev '05)

Learning with Errors (LWE)

- primary basis of hardness for post-quantum cryptography
- allows for PKE, FHE, QPRFs, ...

Search problem:

Recover a secret string $\boldsymbol{s} \in \mathbb{Z}_q^n$ from a set of noisy linear equations modulo q.

$$\boldsymbol{a}_1 \xleftarrow{\$} \mathbb{Z}_q^n; \quad c_1 = \langle \boldsymbol{a}_1, \boldsymbol{s} \rangle + e_1$$
$$\boldsymbol{a}_2 \xleftarrow{\$} \mathbb{Z}_q^n; \quad c_2 = \langle \boldsymbol{a}_2, \boldsymbol{s} \rangle + e_2$$
$$\vdots$$
$$\boldsymbol{a}_m \xleftarrow{\$} \mathbb{Z}_q^n; \quad c_m = \langle \boldsymbol{a}_m, \boldsymbol{s} \rangle + e_m,$$

Learning with Errors (Regev '05)

Learning with Errors (LWE)

- primary basis of hardness for post-quantum cryptography
- allows for PKE, FHE, QPRFs, ...

Search problem:

Recover a secret string $\boldsymbol{s} \in \mathbb{Z}_q^n$ from a set of noisy linear equations modulo q.

$$\begin{aligned} \boldsymbol{a}_1 \xleftarrow{\$} \mathbb{Z}_q^n; \quad & c_1 = \langle \boldsymbol{a}_1, \boldsymbol{s} \rangle + e_1 \\ \boldsymbol{a}_2 \xleftarrow{\$} \mathbb{Z}_q^n; \quad & c_2 = \langle \boldsymbol{a}_2, \boldsymbol{s} \rangle + e_2 \\ & \vdots \\ \boldsymbol{a}_m \xleftarrow{\$} \mathbb{Z}_q^n; \quad & c_m = \langle \boldsymbol{a}_m, \boldsymbol{s} \rangle + e_m, \end{aligned}$$

Symmetric-key encryption using LWE

- KeyGen: choose key $\boldsymbol{s} \xleftarrow{\$} \mathbb{Z}_q^n$.
- $\mathsf{Enc}_{\boldsymbol{s}}(b) = (\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e + b\lfloor q/2 \rfloor)$
- $\mathsf{Dec}_{\boldsymbol{s}}(\boldsymbol{a}, c) = 0$, if $|c - \langle \boldsymbol{a}, \boldsymbol{s} \rangle| \leq \left\lfloor \frac{q}{4} \right\rfloor$, else 1.

Learning with Errors (Regev '05)

Learning with Errors (LWE)

- primary basis of hardness for post-quantum cryptography
- allows for PKE, FHE, QPRFs, ...

Search problem:

Recover a secret string $\boldsymbol{s} \in \mathbb{Z}_q^n$ from a set of noisy linear equations modulo q.

$$\boldsymbol{a}_1 \xleftarrow{\$} \mathbb{Z}_q^n; \quad c_1 = \langle \boldsymbol{a}_1, \boldsymbol{s} \rangle + e_1$$

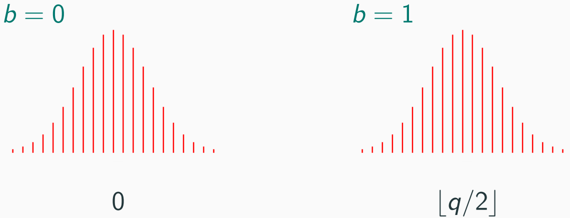
$$\boldsymbol{a}_2 \xleftarrow{\$} \mathbb{Z}_q^n; \quad c_2 = \langle \boldsymbol{a}_2, \boldsymbol{s} \rangle + e_2$$

$$\vdots$$

$$\boldsymbol{a}_m \xleftarrow{\$} \mathbb{Z}_q^n; \quad c_m = \langle \boldsymbol{a}_m, \boldsymbol{s} \rangle + e_m,$$

Symmetric-key encryption using LWE

- KeyGen: choose key $\boldsymbol{s} \xleftarrow{\$} \mathbb{Z}_q^n$.
- $\mathrm{Enc}_{\boldsymbol{s}}(b) = (\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e + b\lfloor q/2 \rfloor)$
- $\mathrm{Dec}_{\boldsymbol{s}}(\boldsymbol{a}, c) = 0$, if $|c - \langle \boldsymbol{a}, \boldsymbol{s} \rangle| \leq \left\lfloor \frac{q}{4} \right\rfloor$, else 1.



Learning with Errors (Regev '05)

Learning with Errors (LWE)

- primary basis of hardness for post-quantum cryptography
- allows for PKE, FHE, QPRFs, ...

Search problem:

Recover a secret string $\mathbf{s} \in \mathbb{Z}_q^n$ from a set of noisy linear equations modulo q.

$$\begin{aligned} \mathbf{a}_1 &\xleftarrow{\$} \mathbb{Z}_q^n; \quad c_1 = \langle \mathbf{a}_1, \mathbf{s} \rangle + e_1 \\ \mathbf{a}_2 &\xleftarrow{\$} \mathbb{Z}_q^n; \quad c_2 = \langle \mathbf{a}_2, \mathbf{s} \rangle + e_2 \\ &\vdots \\ \mathbf{a}_m &\xleftarrow{\$} \mathbb{Z}_q^n; \quad c_m = \langle \mathbf{a}_m, \mathbf{s} \rangle + e_m, \end{aligned}$$

Symmetric-key encryption using LWE

- KeyGen: choose key $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$.
- $\mathsf{Enc}_{\mathbf{s}}(b) = (\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e + b\lfloor q/2 \rfloor)$
- $\mathsf{Dec}_{\mathbf{s}}(\mathbf{a}, c) = 0$, if $|c - \langle \mathbf{a}, \mathbf{s} \rangle| \leq \lfloor \frac{q}{4} \rfloor$, else 1.

This talk:

- new quantum attack on plain LWE encryption
- attack uses a **single** quantum decryption
- classical attack: $\Omega(n \log q)$
- quantum attack: $O(1)$.

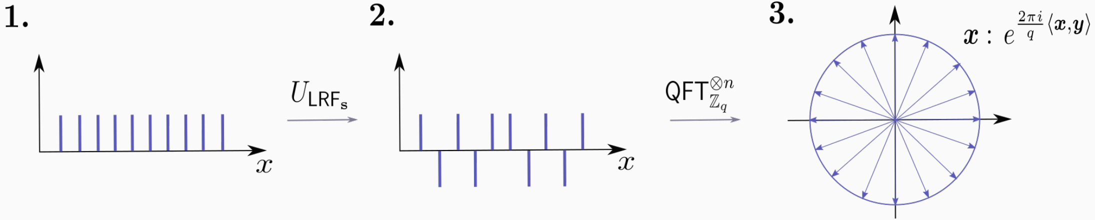
Quantum attack

Linear rounding function with key $\boldsymbol{s} \in \mathbb{Z}_q^n$,

Oracle: $U_{\mathsf{LRF_s}} : |\mathbf{x}\rangle|b\rangle \mapsto |\mathbf{x}\rangle|b \oplus \mathsf{LRF_s}(\boldsymbol{x})\rangle$

$$\mathsf{LRF_s}(\boldsymbol{x}) := \begin{cases} 0 & \text{if } |\langle \boldsymbol{x}, \boldsymbol{s}\rangle| \leq \lfloor \frac{q}{4} \rfloor \\ 1 & \text{otherwise} \end{cases}$$

Algorithm:



$$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} |\boldsymbol{x}\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} (-1)^{\mathsf{LRF_s}(\mathbf{x})} |\boldsymbol{x}\rangle$$

$$\frac{1}{q^n} \sum_{\mathbf{y}, \mathbf{x} \in \mathbb{Z}_q^n} (-1)^{\mathsf{LRF_s}(\mathbf{x})} e^{\frac{2\pi i}{q}\langle \mathbf{x}, \mathbf{y}\rangle} |\boldsymbol{y}\rangle$$

Bernstein-Vazirani for linear rounding (AJOP'18)

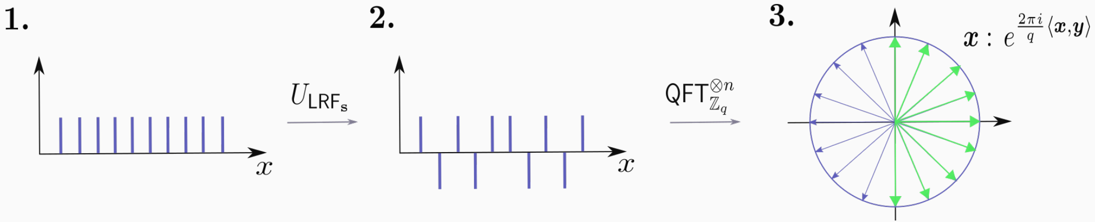
Linear rounding function with key $\boldsymbol{s} \in \mathbb{Z}_q^n$,

$$\mathsf{LRF}_{\mathbf{s}}(\boldsymbol{x}) := \begin{cases} 0 & \text{if } |\langle \boldsymbol{x}, \boldsymbol{s} \rangle| \leq \lfloor \frac{q}{4} \rfloor \\ 1 & \text{otherwise} \end{cases}$$

Oracle: $U_{\mathsf{LRF}_{\mathbf{s}}} : |\mathbf{x}\rangle|b\rangle \mapsto |\boldsymbol{x}\rangle|b \oplus \mathsf{LRF}_{\mathbf{s}}(\boldsymbol{x})\rangle$

Success probability: $\Pr[\boldsymbol{y} = \boldsymbol{s}] \approx 4/\pi^2$.

Algorithm:

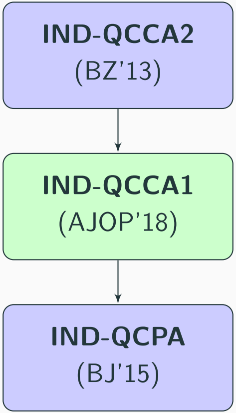


$$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} |\boldsymbol{x}\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} (-1)^{\mathsf{LRF}_{\mathbf{s}}(\mathbf{x})} |\boldsymbol{x}\rangle$$

$$\frac{1}{q^n} \sum_{\mathbf{y}, \mathbf{x} \in \mathbb{Z}_q^n} (-1)^{\mathsf{LRF}_{\mathbf{s}}(\mathbf{x})} e^{\frac{2\pi i}{q}\langle \mathbf{x}, \mathbf{y} \rangle} |\boldsymbol{y}\rangle$$

Our results (AJOP'18)



Non-adative quantum chosen-ciphertext attacks:

1. **Formal security definition (IND-QCCA1)**
    - ”half-way” between existing security notions
2. **A secure symmetric-key encryption scheme:**
   → QPRF construction
    - uses quantum-secure pseudorandom functions
    - proof technique: quantum random access codes
3. **Quantum attack on Learning with Errors encryption**
    - Bernstein-Vazirani algorithm for linear rounding

Questions?