Semantic Security and Indistinguishability in the Quantum World

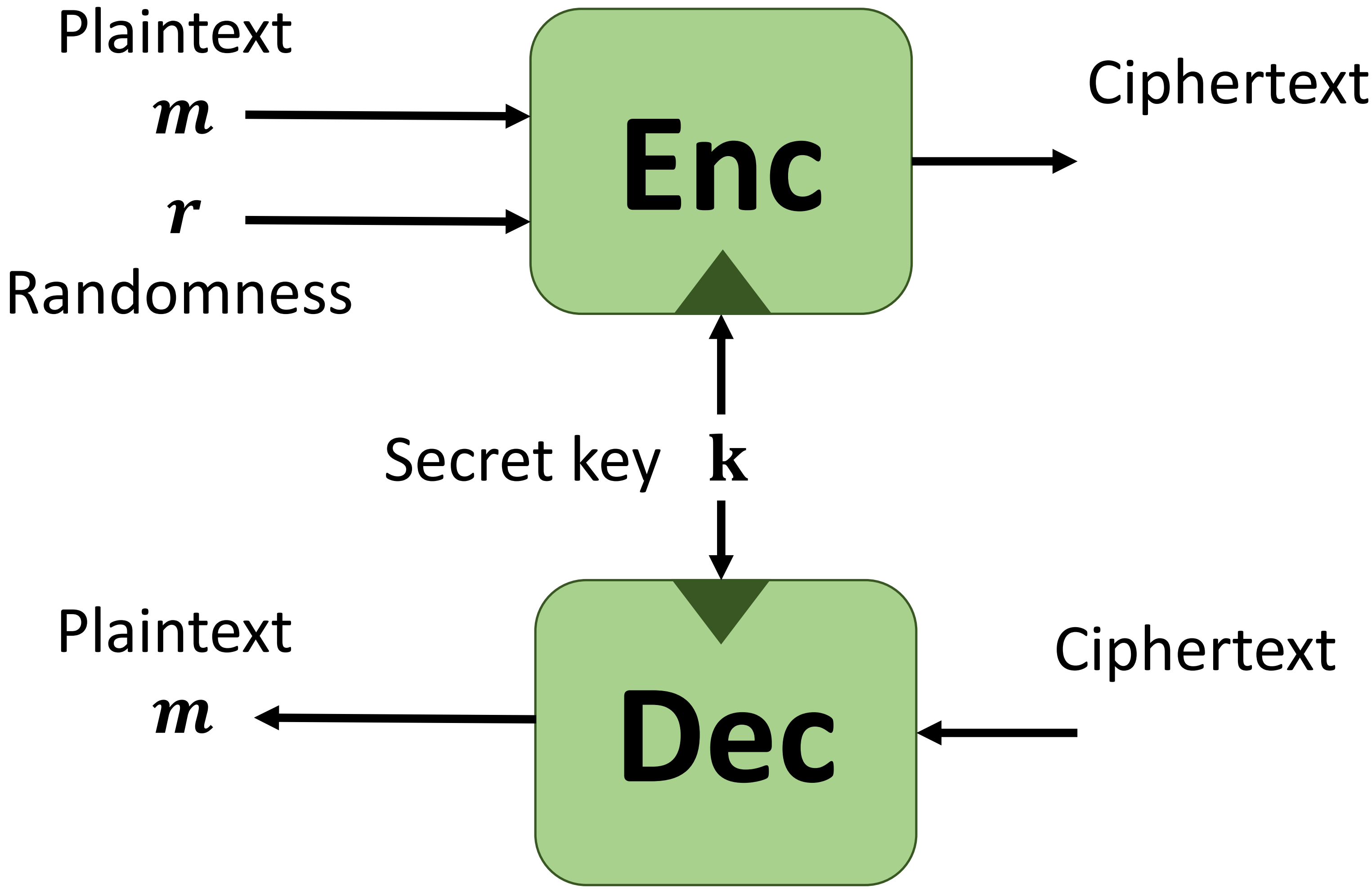
Tommaso Gagliardoni[1], Andreas Hülsing[2], Christian Schaffner[3]

[1] IBM Research, Swiss; TU Darmstadt, Germany
[2] TU Eindhoven, The Netherlands
[3]University of Amsterdam, CWI, QuSoft, The Netherlands

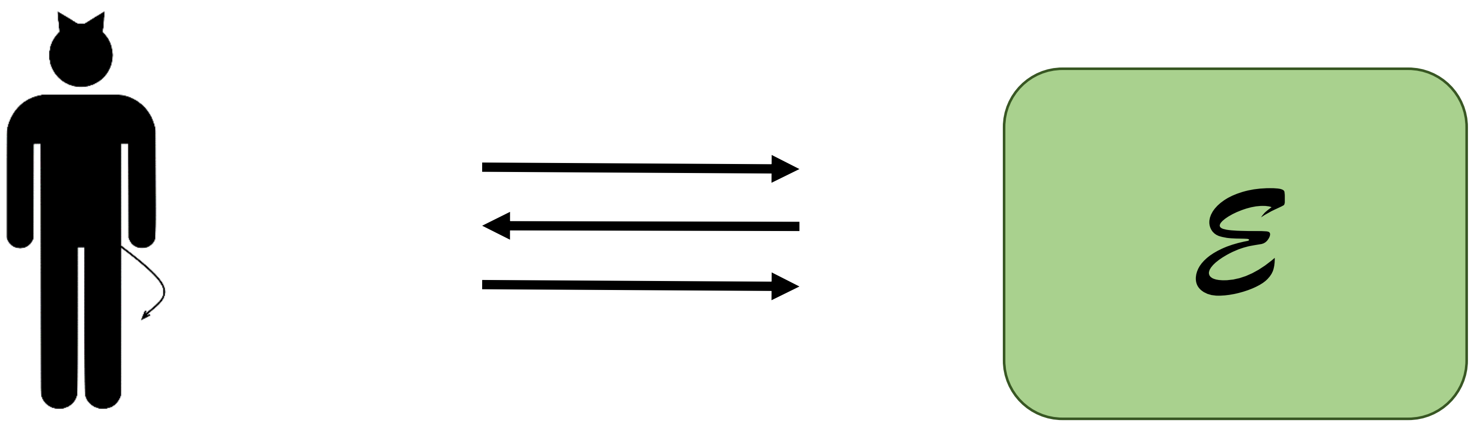
Crypto Working Group, Utrecht, NL
24/03/2017

Introduction

Symmetric encryption
$\mathcal{E}$ = (Kg, Enc, Dec)

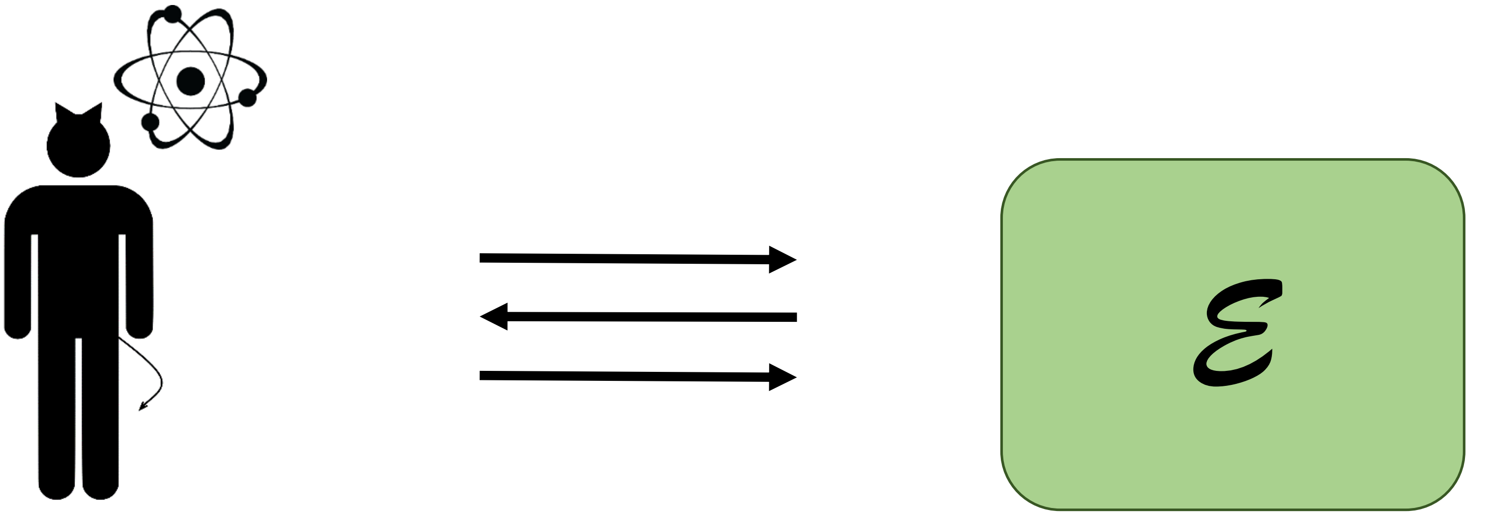


Adversaries I: Classical Security



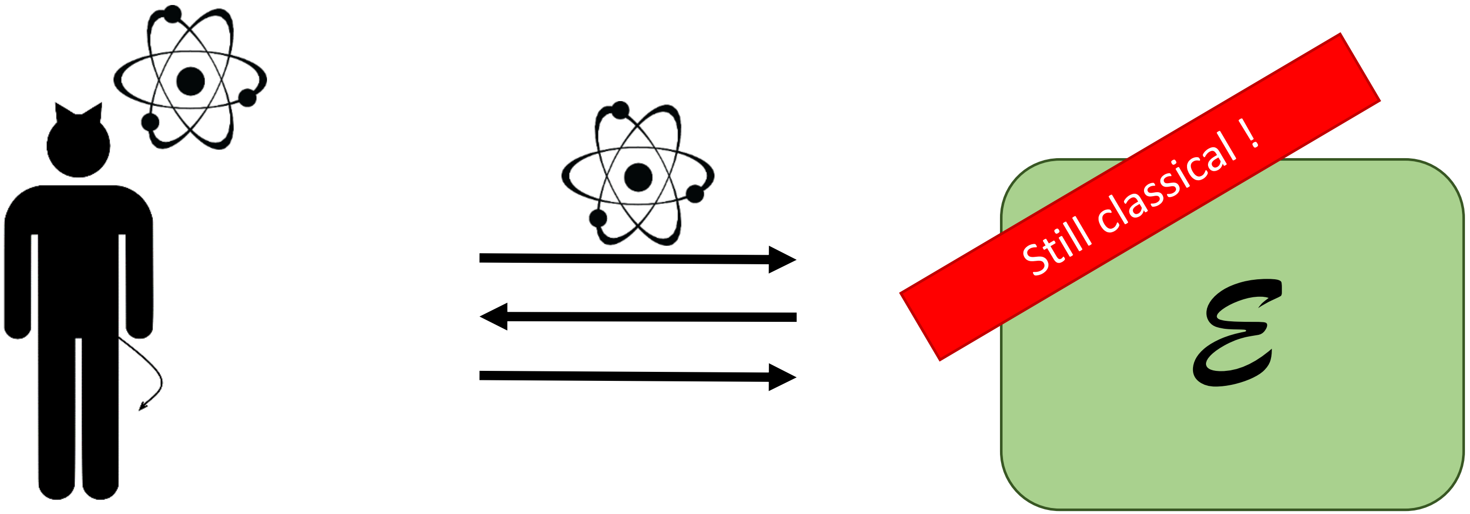
Adversary = probabilistic polynomial time (PPT) algorithm

Adversaries II: Post-Quantum Security



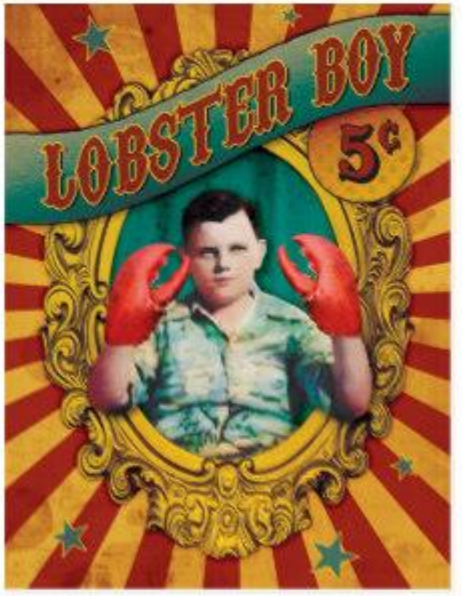
Adversary = bounded-error quantum polynomial time (BQP) algorithm

Adversaries III: Quantum Security



Adversary = bounded-error quantum polynomial time (BQP) algorithm

Why should we care?



1. Use in protocols

2. Quantum cloud

3. Quantum obfuscation

4. Side-channel attacks that trigger some measurable quantum behaviour

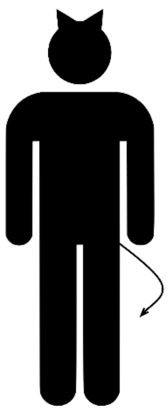
5. Oh, and because we can!

Semantic security (SEM)

- Simulation-based security notion
- Captures intuition:

  It should not be possible to learn anything about the plaintext given the ciphertext which you could not also have learned without the ciphertext.

Semantic security (SEM): Challenge phase



$(\boldsymbol{S_n, h, f})$ →

$\boldsymbol{m \leftarrow S_n}$,
$\boldsymbol{c = Enc_k(m)}$,

← $(\boldsymbol{c, h(m)})$

$(\boldsymbol{f(m)})$ →

$\mathcal{A}$

$\mathcal{C}$

$\mathcal{A}$ cannot do significantly better in the above game than a simulator $\mathcal{S}$ that does not receive c.

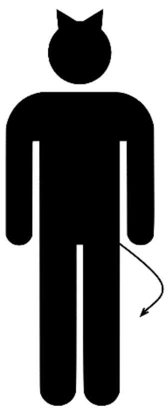
Indistinguishability (IND) (of ciphertexts)

- Pure game-based notion (no simulator)
- Easier to work with than SEM
- Intuition:

  You cannot distinguish the encryptions of two messages of your choice

- Shown to be equivalent to SEM!

Indistinguishability (IND): Challenge phase



$(m_1, m_2) \longrightarrow$

$b \leftarrow_R \{0,1\}$,
$c = Enc_k(m_b)$,

$\longleftarrow c$

$b \longrightarrow$

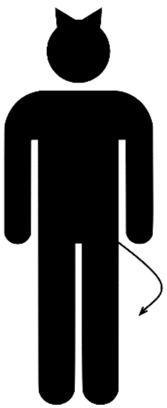
$\mathcal{A}$ $\qquad$ $\mathcal{C}$

$\mathcal{A}$ cannot output correct b with significantly bigger probability than guessing.

Chosen plaintext attacks (CPA)

- Adversary might learn encryptions of known messages
- To model worst case: Let adversary chose messages
- Can be combined with both security notions – IND & SEM
- Normally:
  Learning phases before & after challenge phase

CPA Learning phase



$\boldsymbol{m}$ →

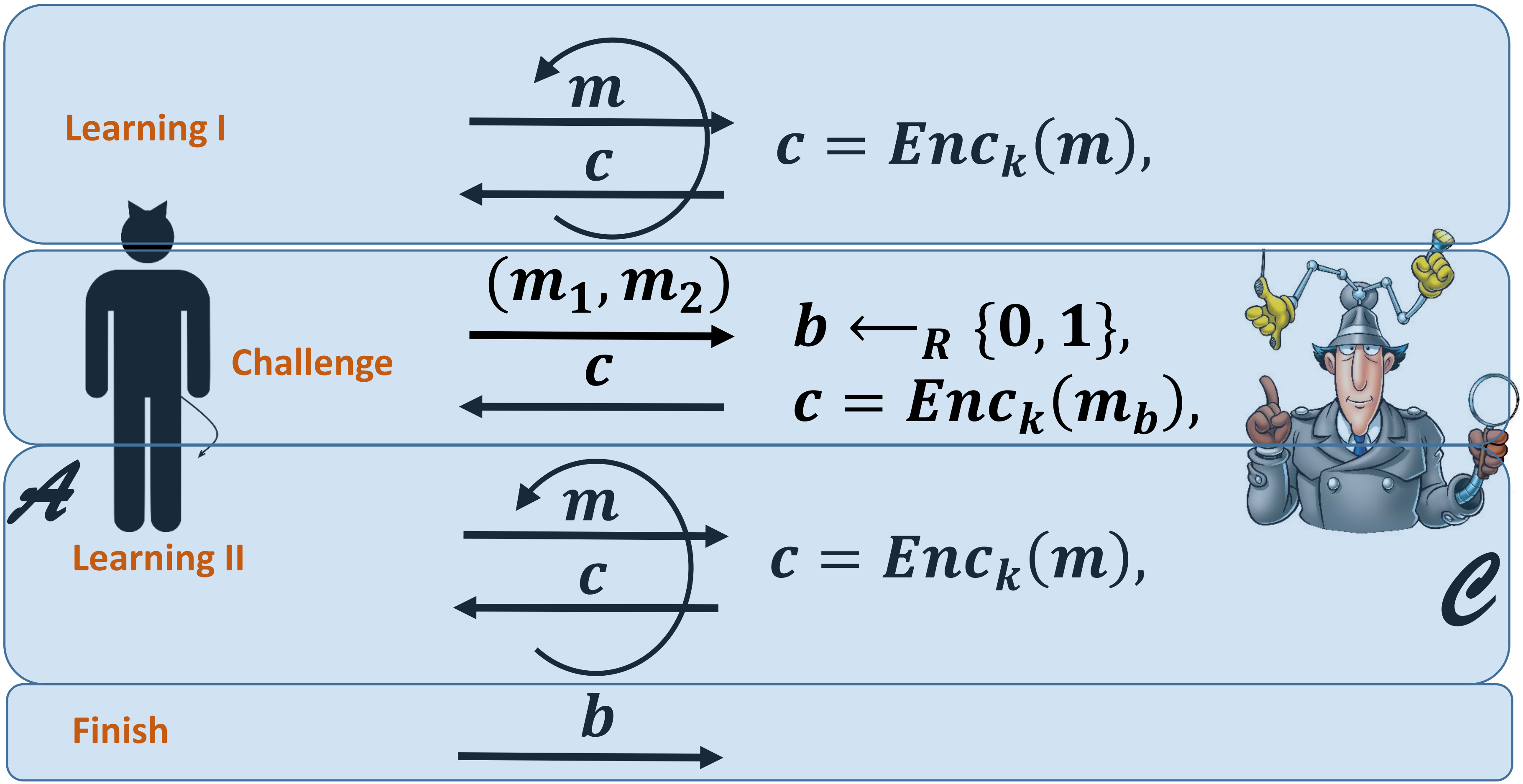
← $\boldsymbol{c}$

$\boldsymbol{c = Enc_k(m)}$

$\mathcal{A}$ $\mathcal{C}$

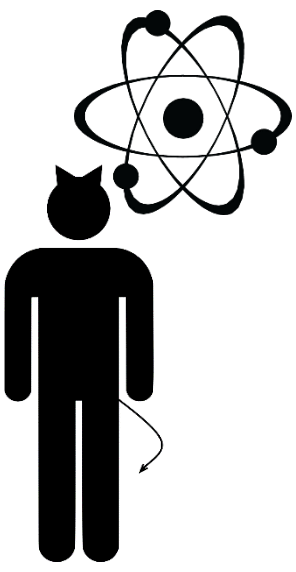
$\mathcal{A}$ can ask $q \in poly(n)$ queries in all learning phases.

IND-CPA



$\mathcal{A}$ cannot output correct b with significantly bigger probability than guessing.

Quantum security notions



Previous work

[BZ13] Boneh, Zhandry: "Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World", CRYPTO'13

Model encryption as unitary operator defined by:

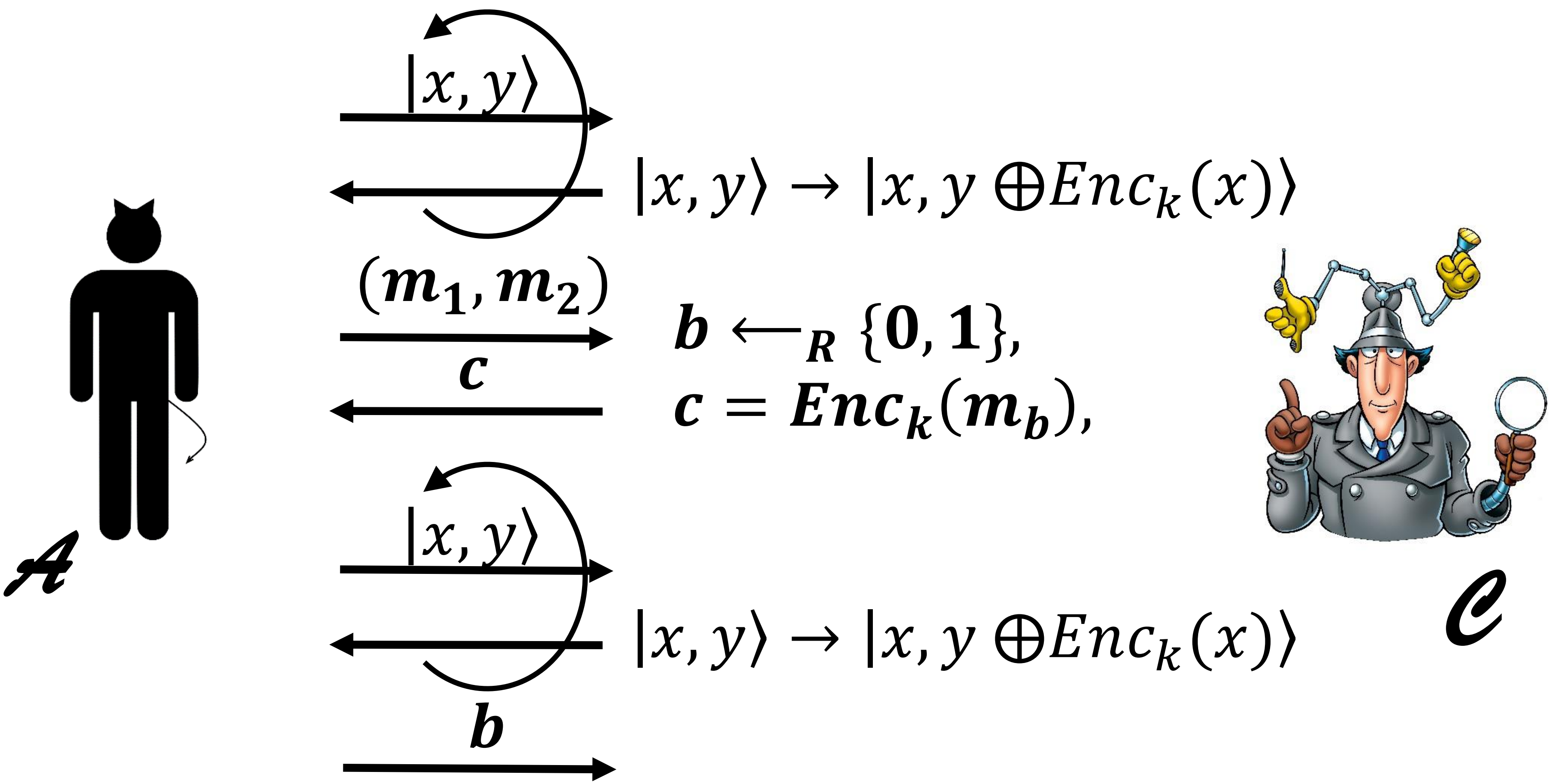
$$\sum_{x,y} |x, y\rangle \rightarrow \sum_{x,y} |x, y \oplus Enc_k(x)\rangle$$

(where $Enc_k(\cdot)$ is a classical encryption function)

Indistinguishability under quantum chosen message attacks (IND-qCPA)

- Give adversary quantum access in learning phase
- Classical challenge phase

IND-qCPA



$\mathcal{A}$ cannot output correct b with significantly bigger probability than guessing.

Indistinguishability under quantum chosen message attacks (IND-qCPA)

- Give adversary quantum access in learning phase
- Classical challenge phase

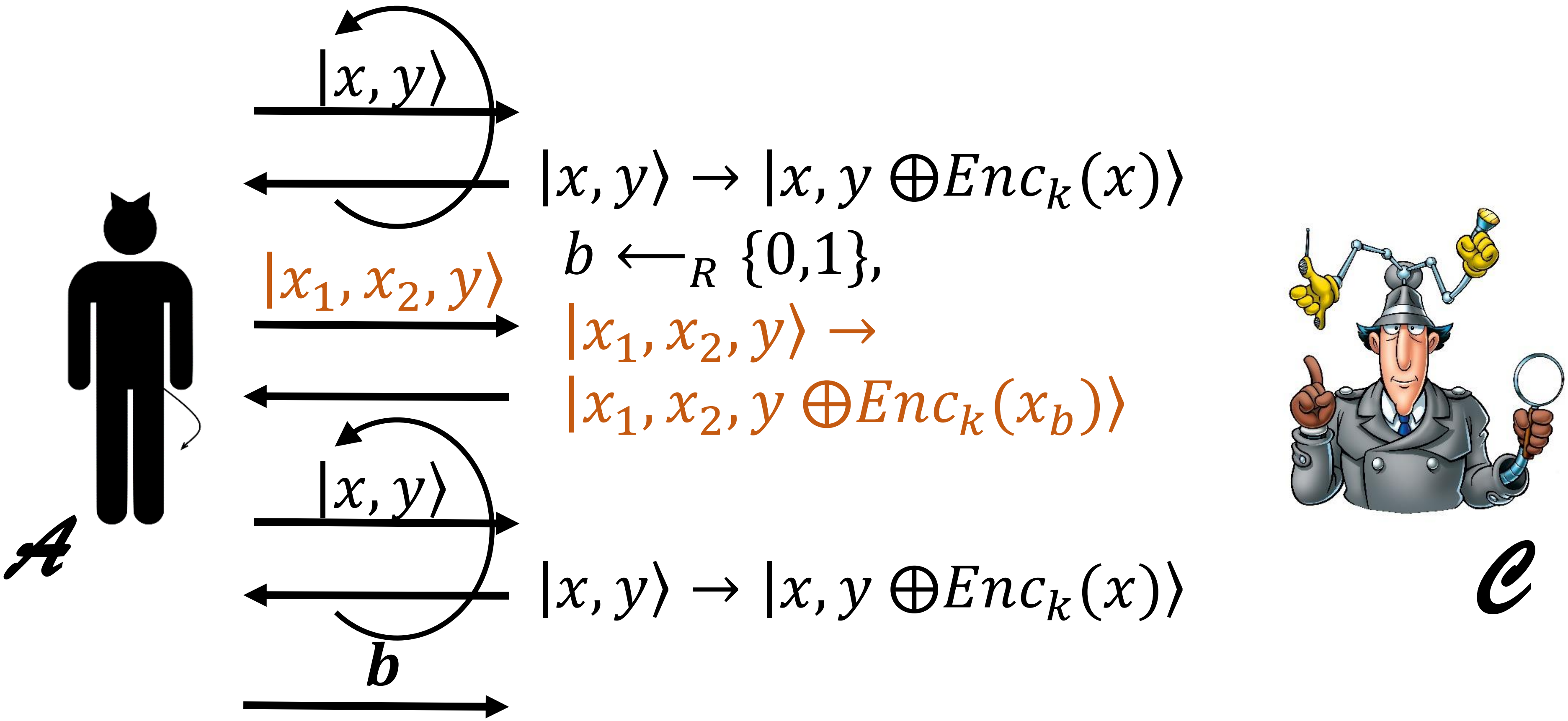
- Can be proven strictly stronger than IND-CPA

- Why would you do this?
- If we assume adversary has quantum access, why not also when it tries to learn something new?

Fully-quantum indistinguishability under quantum chosen message attacks (fqIND-qCPA)

- Give adversary quantum access in learning phase
- Quantum challenge phase

fqIND-qCPA



$\mathcal{A}$ cannot output correct b with significantly bigger probability than guessing.

fqIND is unachievable [BZ13]

(example for 1-bit messages, with normalization amplitudes omitted)

$\mathcal{A}$ initializes register to: $H|0\rangle \otimes |0\rangle \otimes |0\rangle = \sum_x |x, 0, 0\rangle$
and then calls the encryption oracle with unknown bit b. Now:

fqIND is unachievable [BZ13]

(example for 1-bit messages, with normalization amplitudes omitted)

$\mathcal{A}$ initializes register to: $H|0\rangle \otimes |0\rangle \otimes |0\rangle = \sum_x |x, 0, 0\rangle$
and then calls the encryption oracle with unknown bit b. Now:

- if $b = 0$, the state becomes: $\sum_x |x, 0, \mathsf{Enc}(x)\rangle$
  (notice the entanglement between 1st and 3rd register);
- if $b = 1$ instead, the state becomes:
  $\sum_x |x, 0, \mathsf{Enc}(0)\rangle = H|0\rangle \otimes |0\rangle \otimes |\mathsf{Enc}(0)\rangle$.

fqIND is unachievable [BZ13]

(example for 1-bit messages, with normalization amplitudes omitted)

$\mathcal{A}$ initializes register to: $H|0\rangle \otimes |0\rangle \otimes |0\rangle = \sum_x |x, 0, 0\rangle$ and then calls the encryption oracle with unknown bit b. Now:

- if $b = 0$, the state becomes: $\sum_x |x, 0, \mathsf{Enc}(x)\rangle$ (notice the entanglement between 1st and 3rd register);
- if $b = 1$ instead, the state becomes: $\sum_x |x, 0, \mathsf{Enc}(0)\rangle = H|0\rangle \otimes |0\rangle \otimes |\mathsf{Enc}(0)\rangle$.

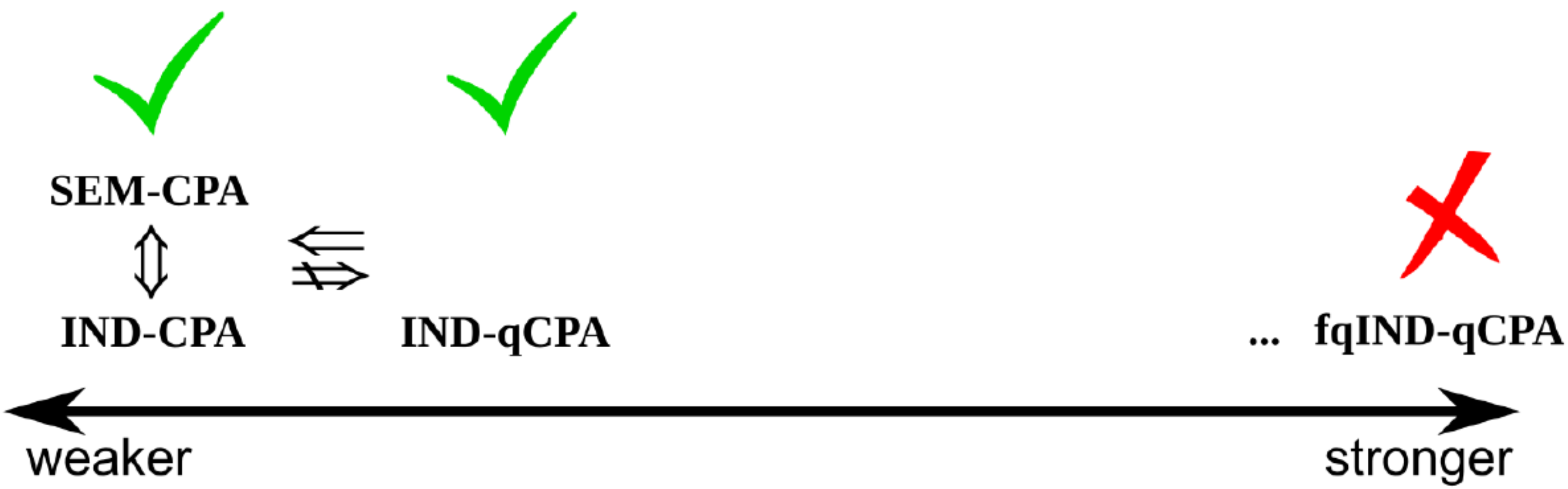
Then $\mathcal{A}$ applies a Hadamard on the 1^{st} register and measures:

- if $b = 0$, the first register is completely mixed (irrespective of the Hadamard), and the measurement outcome is random;
- if $b = 1$ instead, the first register is: $H^2|0\rangle = |0\rangle$, and the outcome is 0.

[BZ13] & our contribution

- A 'natural' notion of security (fqIND-qCPA) is unachievable
- Compromise: 'almost classical' notion of security (IND-qCPA)
- IND-qCPA is achievable and stronger than IND-CPA

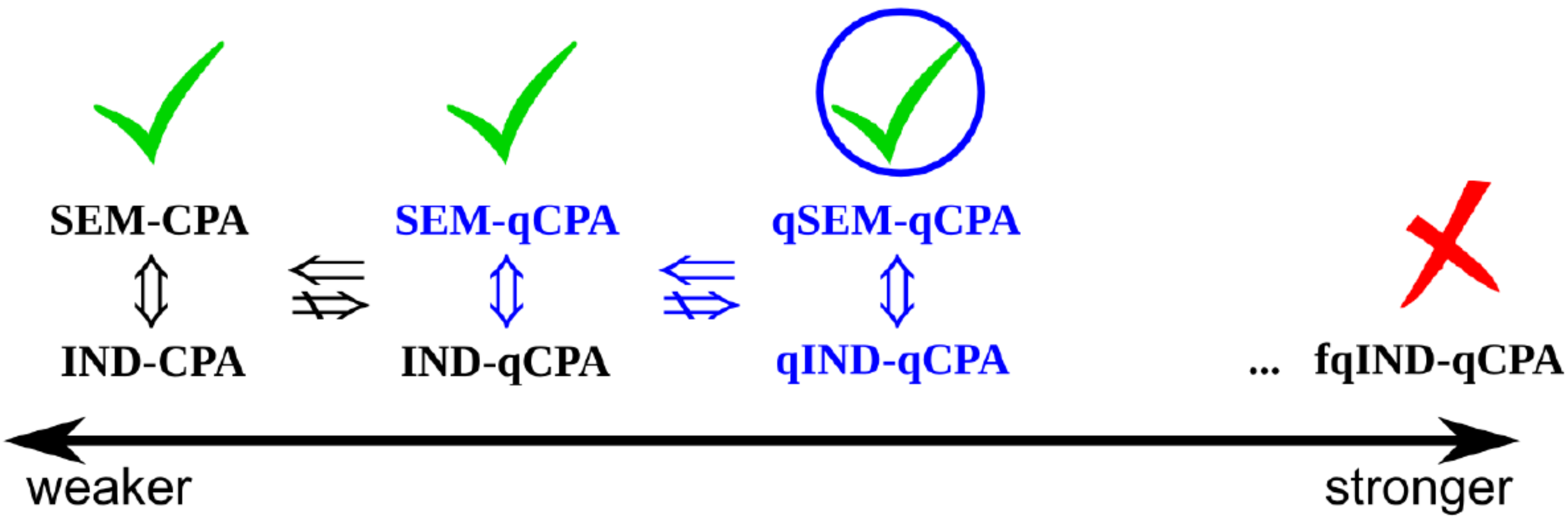
Situation:



[BZ13] & our contribution

- A 'natural' notion of security (fqIND-qCPA) is unachievable
- Compromise: 'almost classical' notion of security (IND-qCPA)
- IND-qCPA is achievable and stronger than IND-CPA

Situation:



Our contribution!

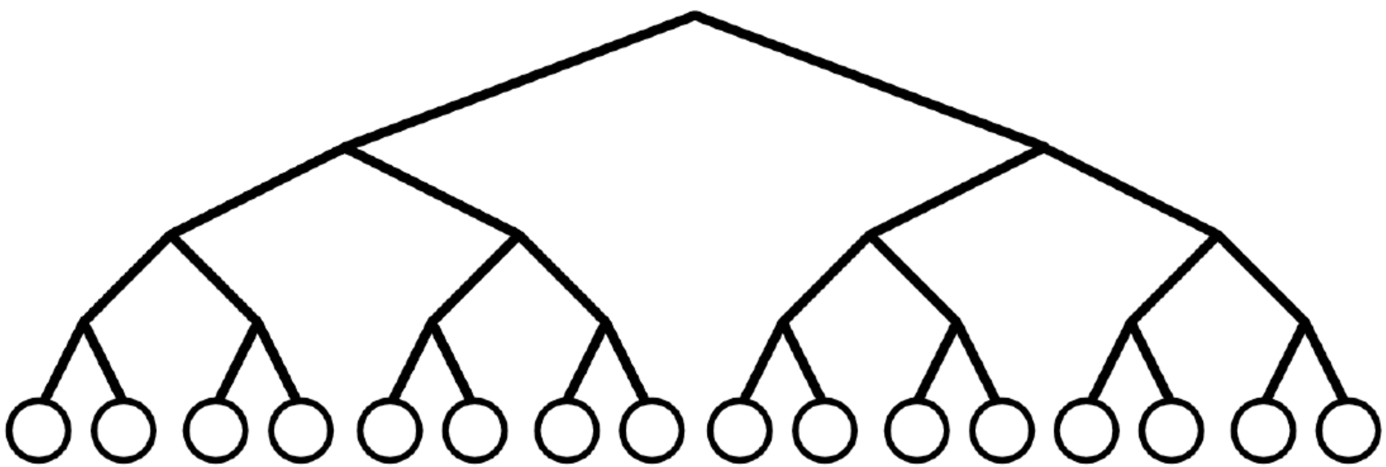
How to define qIND-qCPA?

fqIND: a seemingly natural extension of IND for quantum states

Theorem [BZ13]

fqIND is unachievable (too strong).

For fqIND-qCPA many assumptions are implicitly made. Instead, we explore every option: 'tree' of security definitions



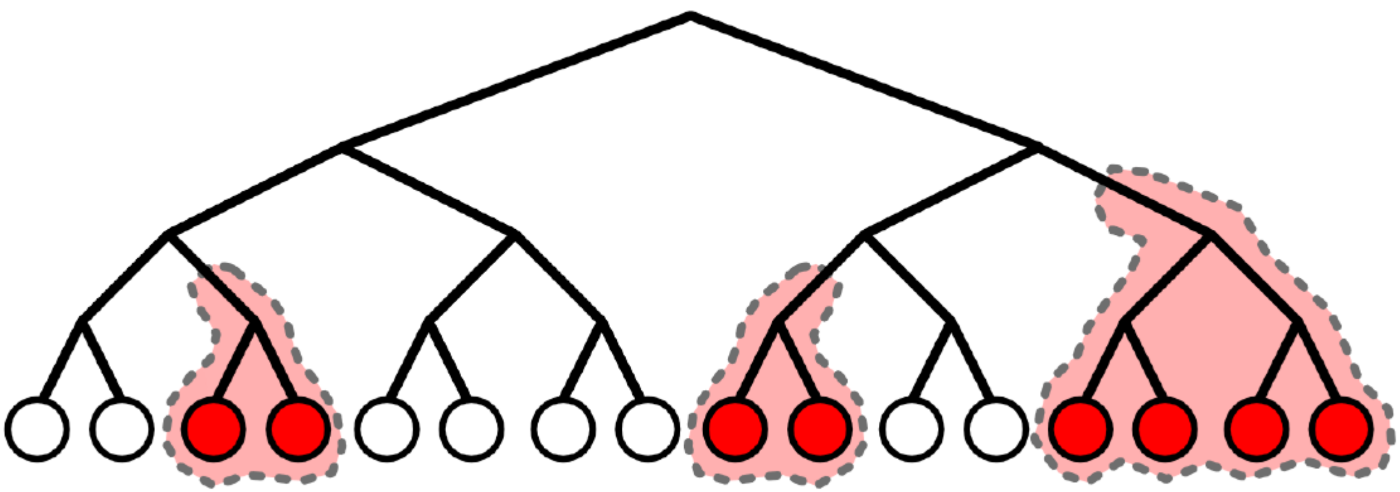
How to define qIND-qCPA?

fqIND: a seemingly natural extension of IND for quantum states

Theorem [BZ13]

fqIND is unachievable (too strong).

For fqIND-qCPA many assumptions are implicitly made. Instead, we explore every option: 'tree' of security definitions



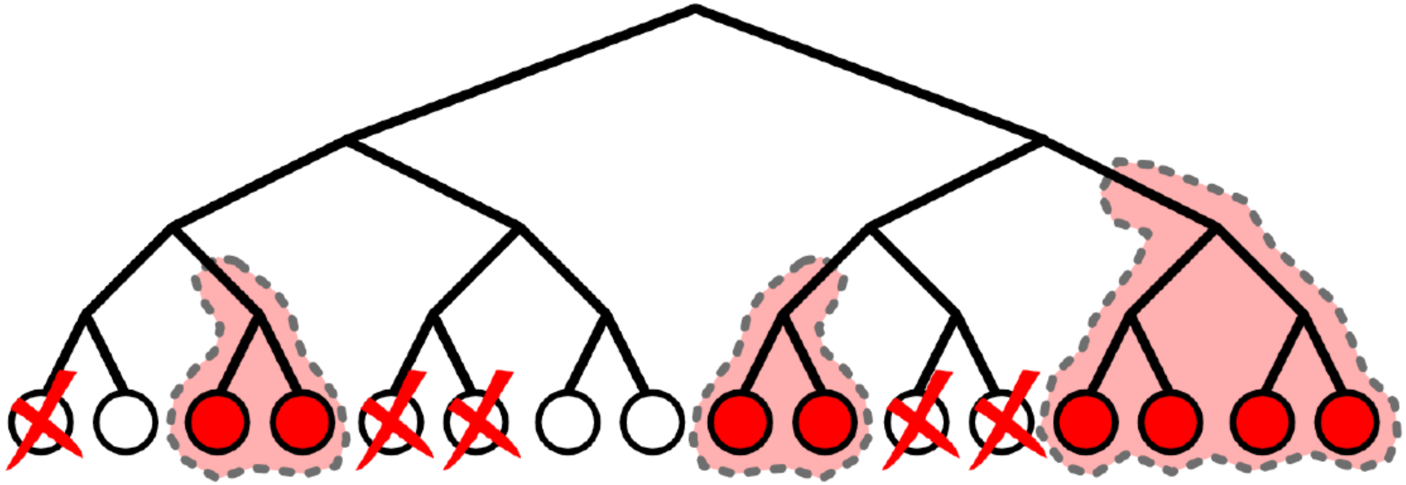
How to define qIND-qCPA?

fqIND: a seemingly natural extension of IND for quantum states

Theorem [BZ13]

fqIND is unachievable (too strong).

For fqIND-qCPA many assumptions are implicitly made. Instead, we explore every option: 'tree' of security definitions



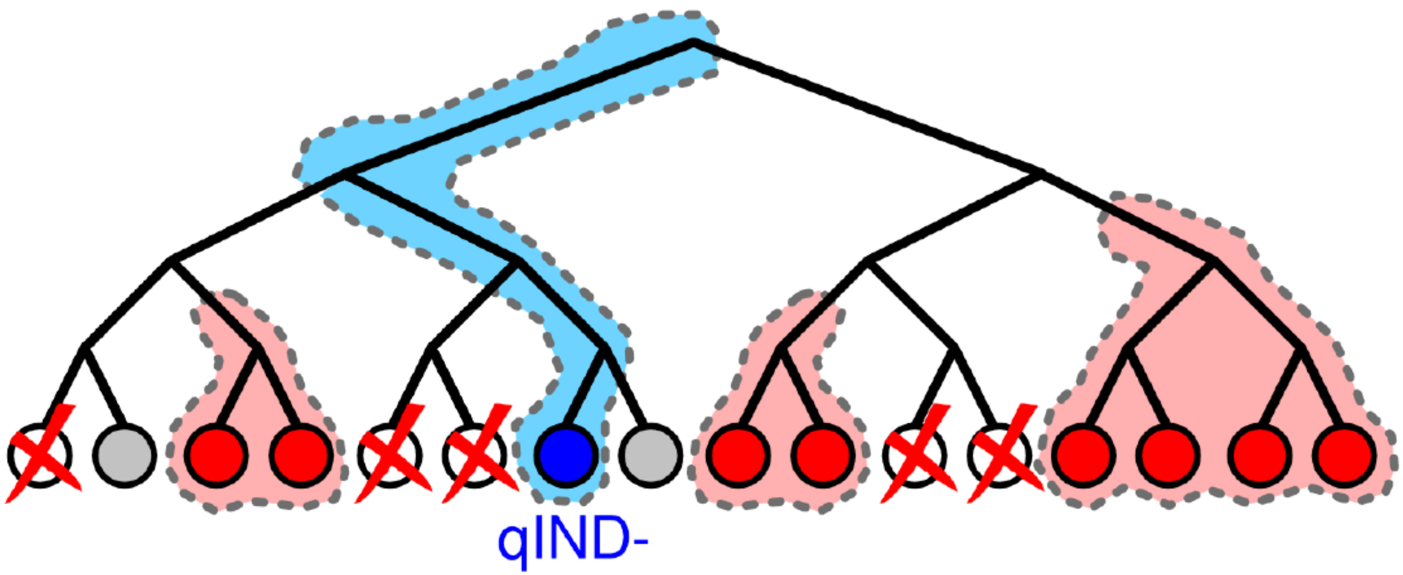
How to define qIND-qCPA?

fqIND: a seemingly natural extension of IND for quantum states

Theorem [BZ13]

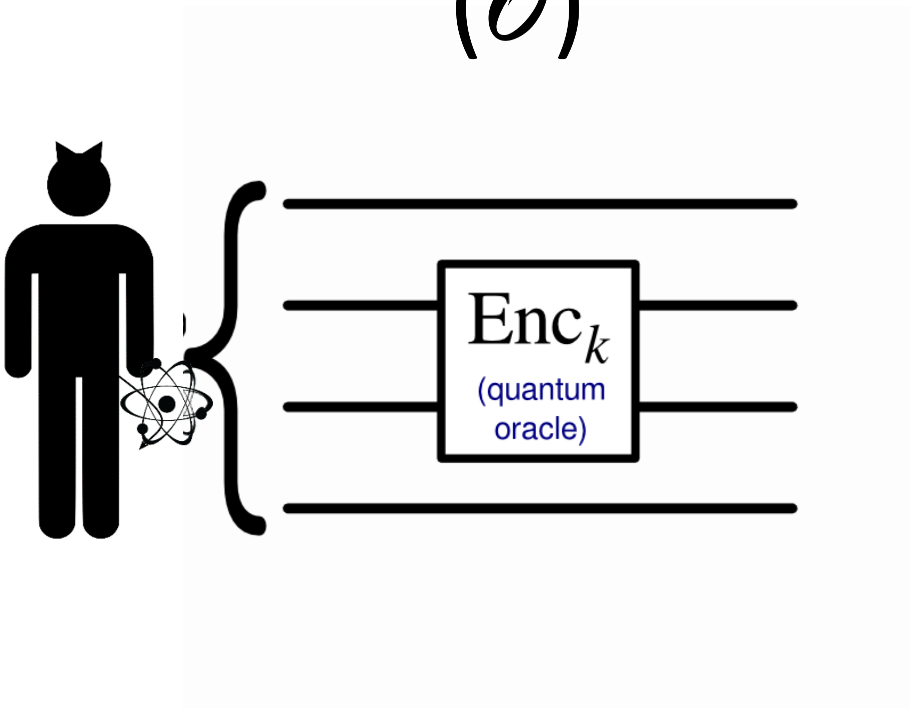
fqIND is unachievable (too strong).

For fqIND-qCPA many assumptions are implicitly made. Instead, we explore every option: 'tree' of security definitions

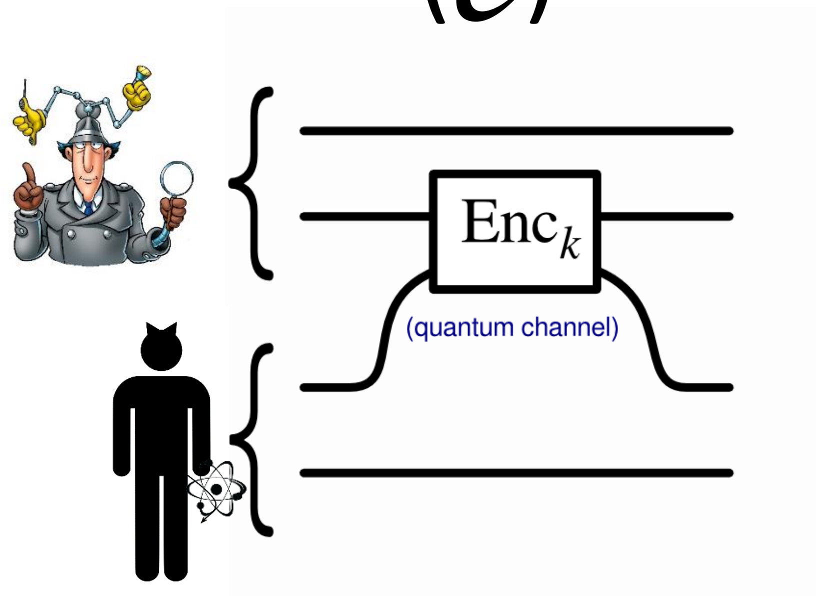


Model: ($\mathcal{O}$) vs ($\mathcal{C}$)

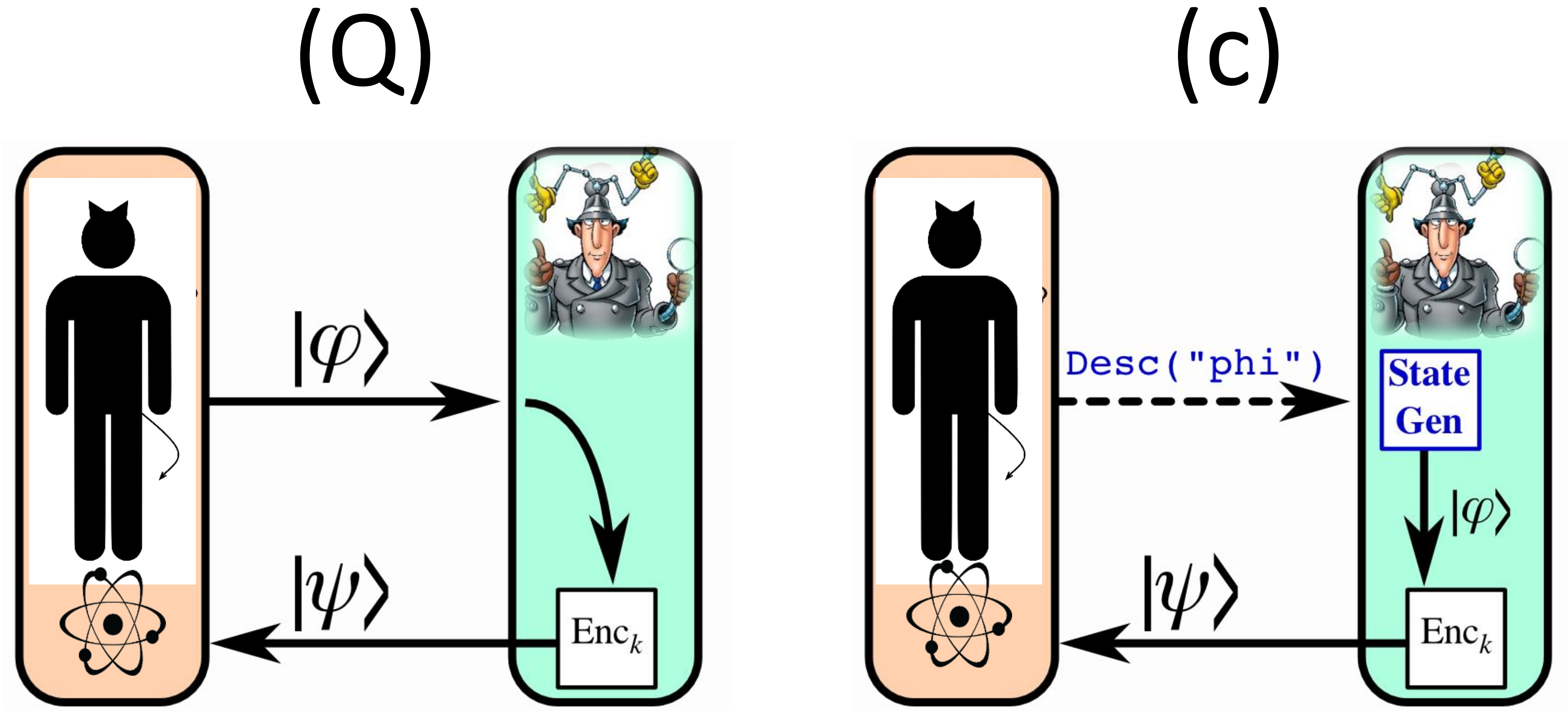
($\mathcal{O}$)



($\mathcal{C}$)



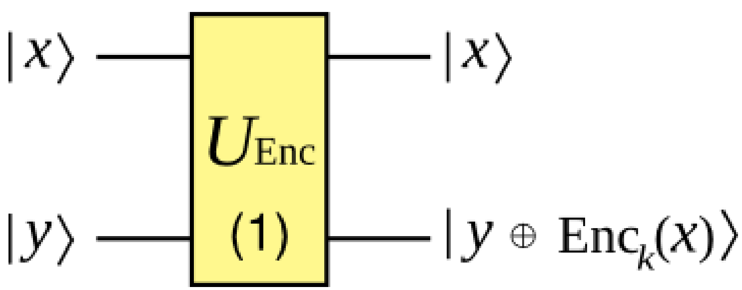
Model: (Q) vs (c)



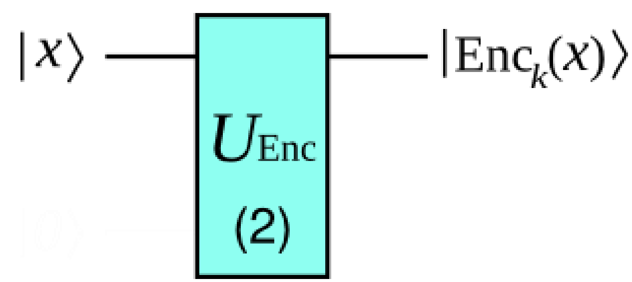
Classical description of a quantum state ρ: a classical bitstring describing the quantum circuit outputting ρ from $|0\ldots0\rangle$.

Model: Type (1) vs type (2)

Type (1)



Type (2)



Type-(2) oracles are also called *minimal* oracles[1].

Notice: in our specific case, and limited to the qIND phase, the two types are both meaningful.

[1]Kashefi et al., 'A Comparison of Quantum Oracles', Phys. Rev. A 65

Quantum indistinguishability (qIND)

qIND challenge query: $\mathcal{A}$ and $\mathcal{C}$ are two BQP machines sharing a classical channel and a quantum channel.

$\mathcal{A}$ sends $\mathcal{C}$ two classical, poly-sized descriptions of plaintext states ρ_0, ρ_1.

$\mathcal{C}$ flips a random bit $b \xleftarrow{\$} \{0,1\}$, and computes:

$$\psi = U_{\mathsf{Enc}} \rho_b U_{\mathsf{Enc}}^{\dagger}$$

and finally sends ciphertext state ψ to $\mathcal{A}$.

$\mathcal{A}$'s goal is to guess b.

Quantum indistinguishability (qIND)

Quantum Indistinguishability (qIND)

For any BQP adversary $\mathcal{A}$ and any ρ_0, ρ_1 with efficient classical representations:

$$\left| \Pr[\mathcal{A}(\psi) = b] - \frac{1}{2} \right| \leq \mathsf{negl}\,(n)\,,$$

where $\psi = U_{\mathsf{Enc}} \rho_b U_{\mathsf{Enc}}^{\dagger}$, and $b \xleftarrow{\$} \{0,1\}$.

Quantum Indistinguishability under qCPA (qIND-qCPA)

An encryption scheme is IND-qCPA secure if it is secure according to the qIND notion, augmented by a qCPA learning phase.

Separation example

Theorem

IND-qCPA $\not\Rightarrow$ qIND-qCPA

Separation example

Theorem

IND-qCPA $\not\Rightarrow$ qIND-qCPA

Consider [Gol04][2] : sample $r \xleftarrow{\$} \mathcal{R}$ and use a PRF $f : \mathcal{K} \times \mathcal{R} \to \mathcal{M}$. Then: $\mathrm{Enc}_k(x) := (x \oplus f_k(r), r)$

Theorem [BZ13]

The Goldreich scheme is IND-qCPA secure, provided the PRF is quantum-secure.

Separation example

Theorem

IND-qCPA $\not\Rightarrow$ qIND-qCPA

Consider [Gol04][2] : sample $r \xleftarrow{\$} \mathcal{R}$ and use a PRF $f : \mathcal{K} \times \mathcal{R} \to \mathcal{M}$. Then: $\mathsf{Enc}_k(x) := (x \oplus f_k(r), r)$

Theorem [BZ13]

The Goldreich scheme is IND-qCPA secure, provided the PRF is quantum-secure.

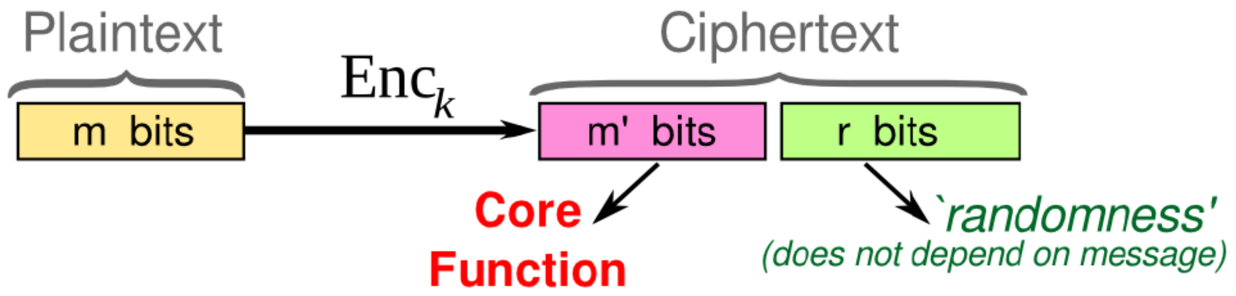
Theorem

The Goldreich scheme is *not* qIND-qCPA secure.

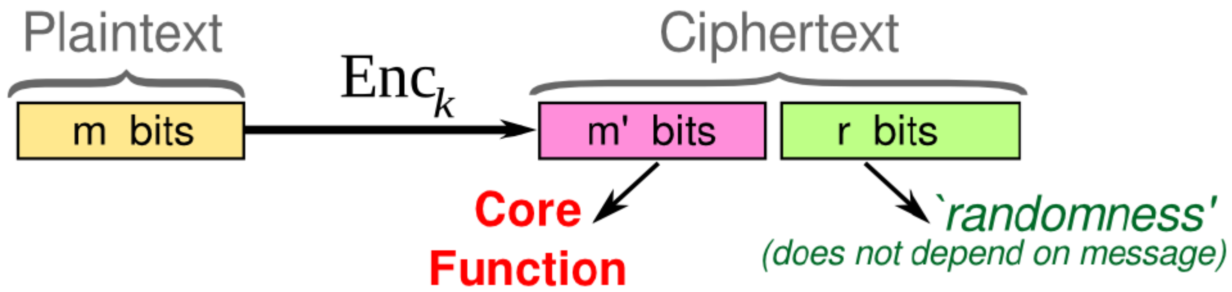
---

[2] O. Goldreich: *'Foundations of Cryptography: Volume 2'*

Impossibility result



Impossibility result



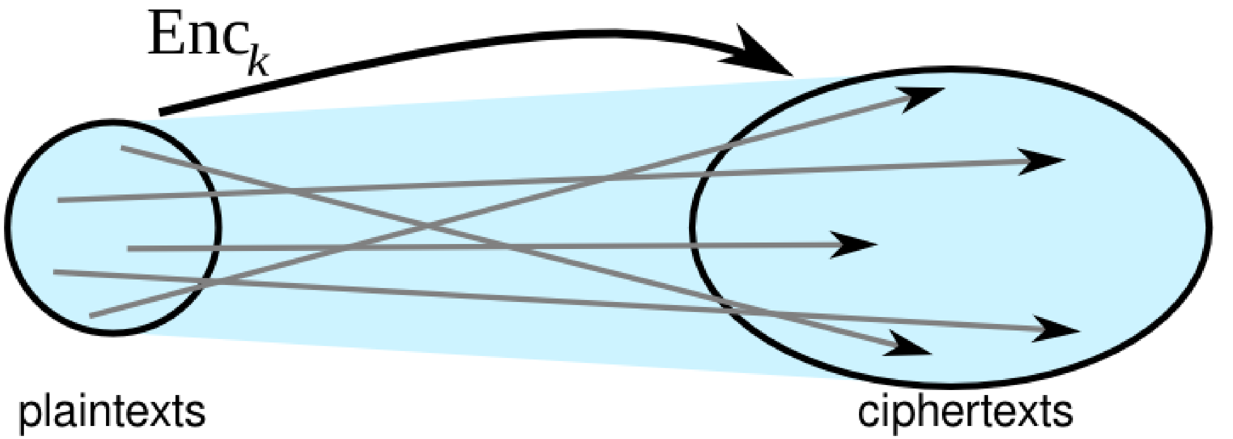
quasi–length-preserving (QLP): core function is bijective ($m = m'$)

- Goldreich's scheme
- OTP
- ECB block ciphers
- stream ciphers

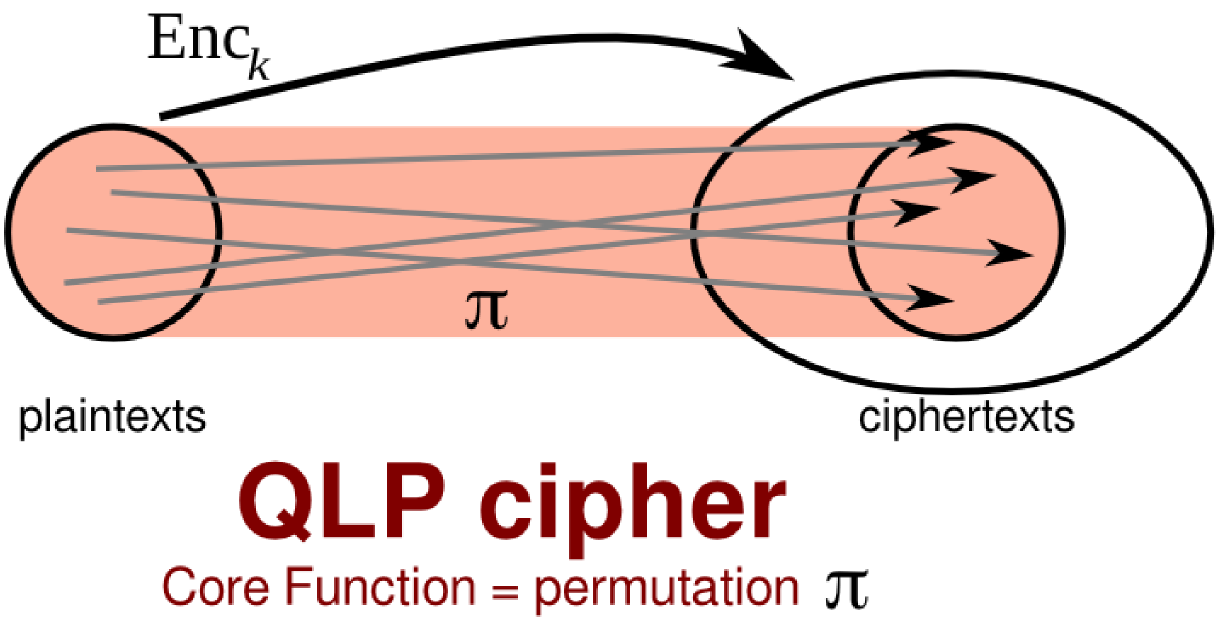
Theorem

If a symmetric scheme is QLP, then it is *not* qIND-qCPA secure.

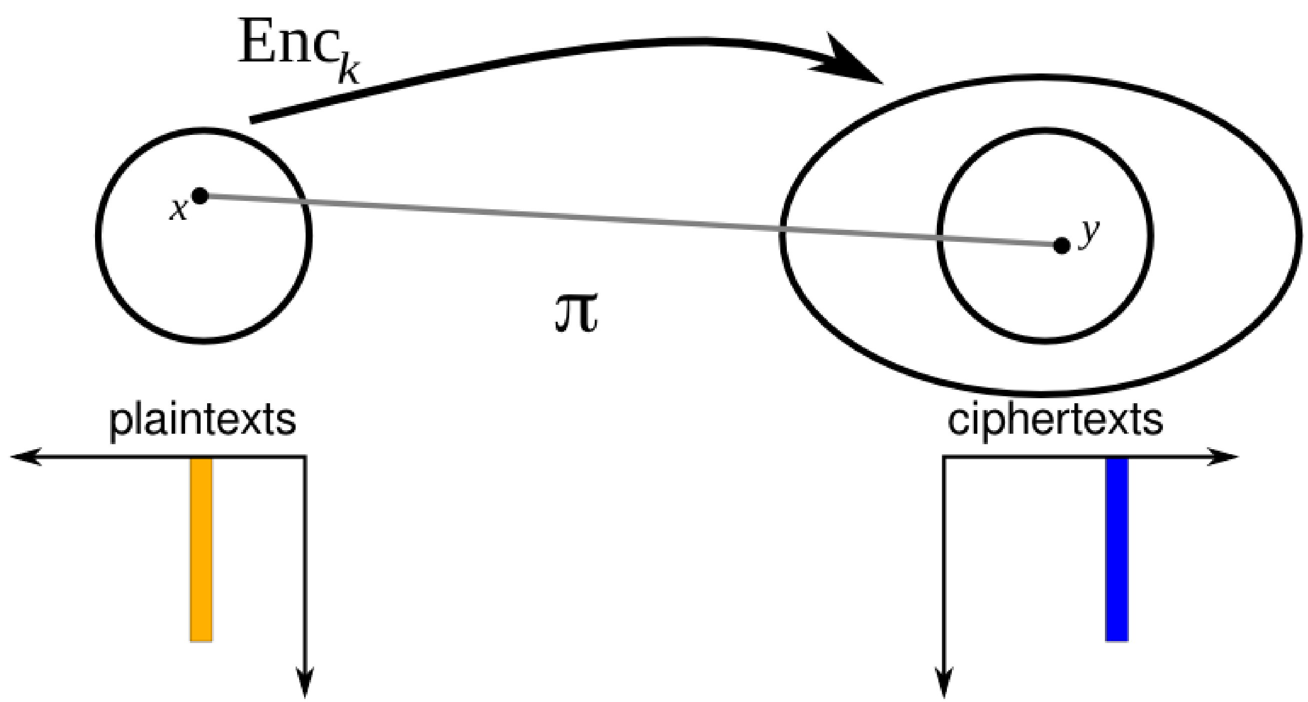
The attack



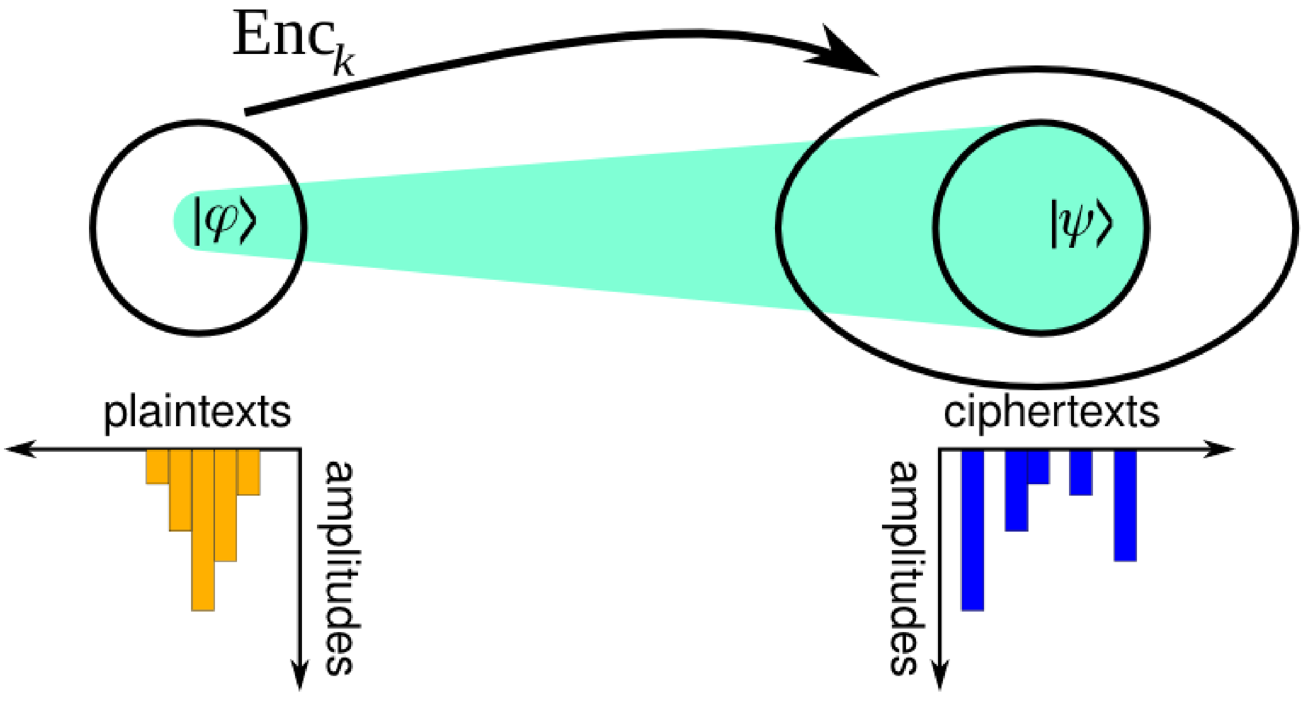
The attack


Enc$_k$
π
plaintexts
ciphertexts
QLP cipher
Core Function = permutation π

The attack

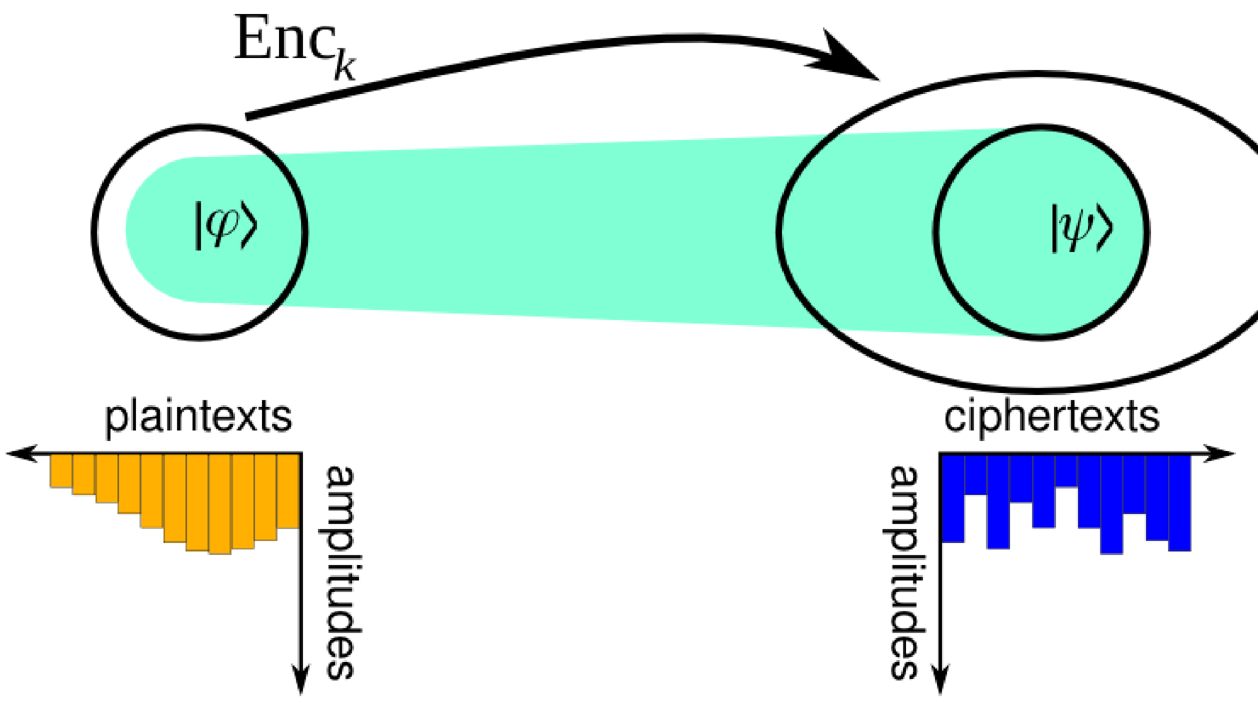


The attack



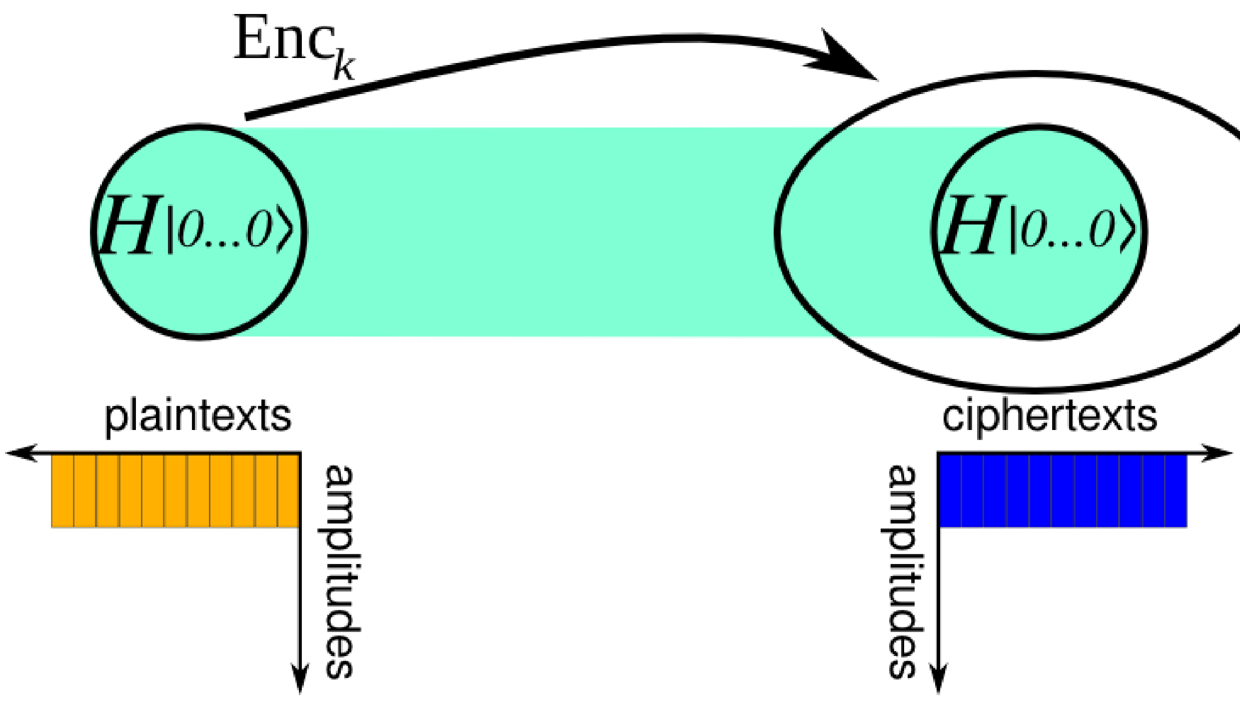
Enc_k
$|\varphi\rangle$
$|\psi\rangle$
plaintexts
amplitudes
ciphertexts
amplitudes

The attack



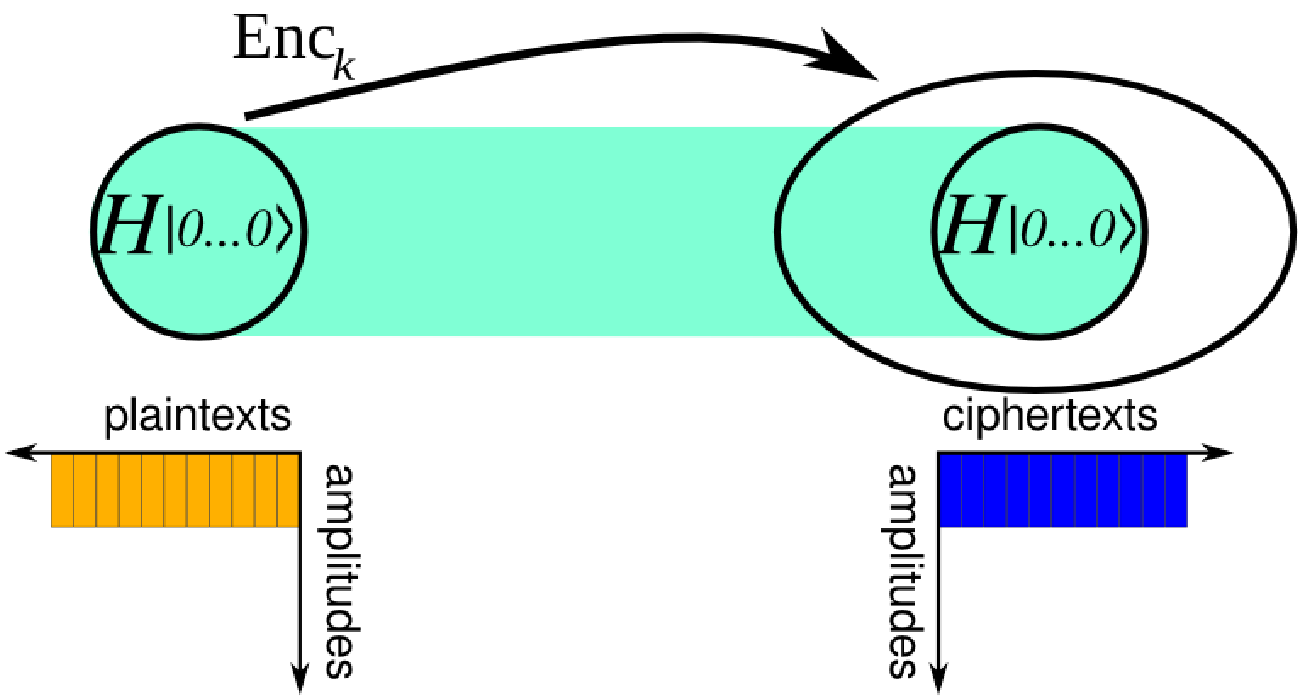
Enc_k
$|\varphi\rangle$
$|\psi\rangle$
plaintexts
amplitudes
ciphertexts
amplitudes

The attack



Enc$_k$
$H|0...0\rangle$
$H|0...0\rangle$
plaintexts
amplitudes
ciphertexts
amplitudes

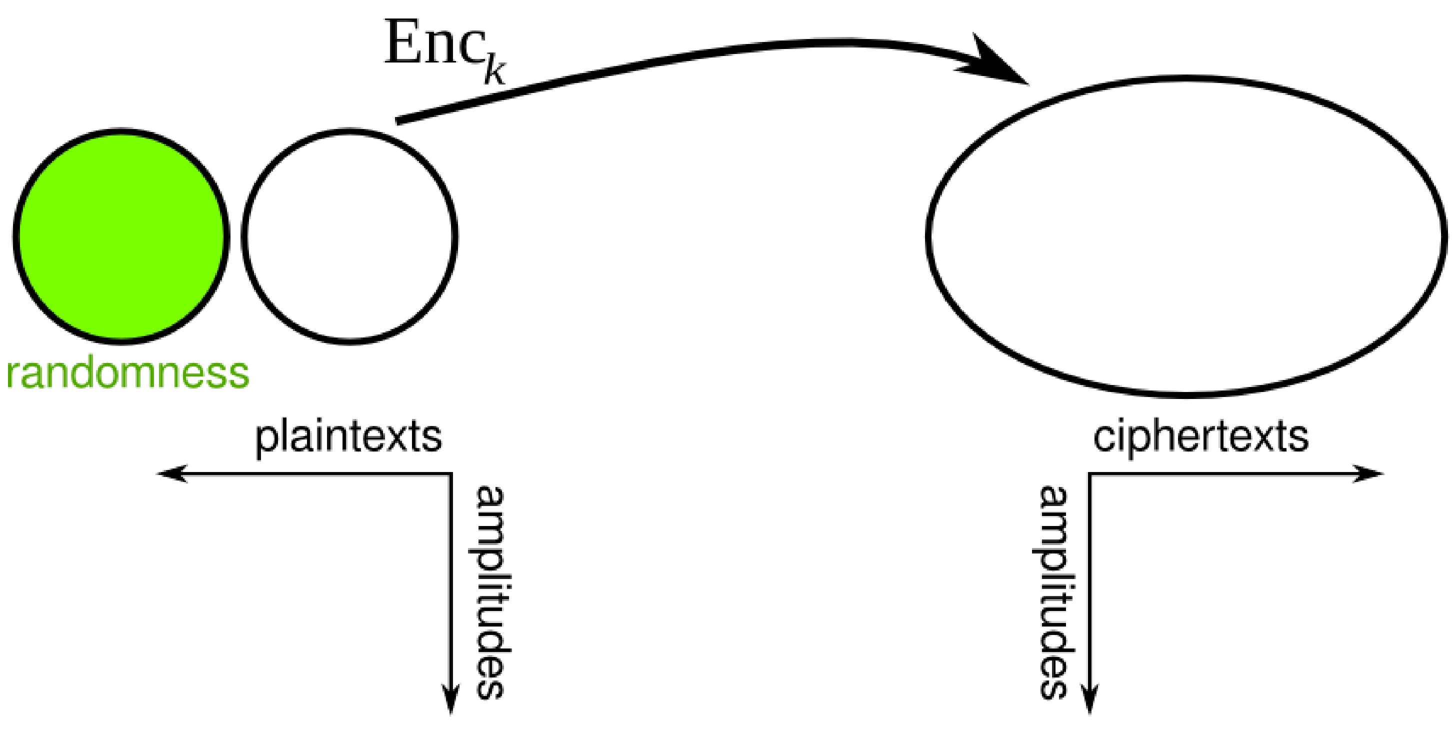
The attack



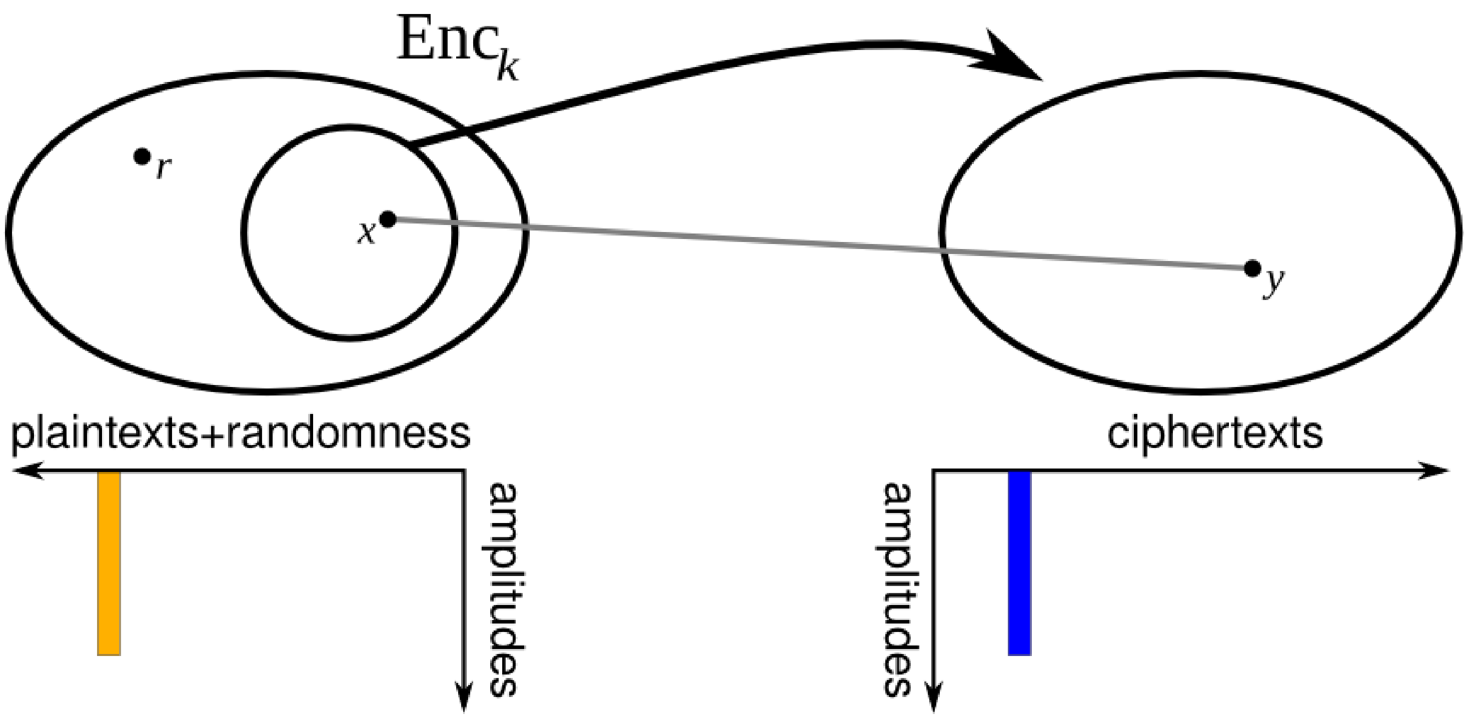
$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{\mathsf{Enc}_k} \frac{1}{\sqrt{2}}|\pi(0)\rangle + \frac{1}{\sqrt{2}}|\pi(1)\rangle = |+\rangle$$

$\mathsf{Enc}_k |+\rangle$ is easy to distinguish from $\mathsf{Enc}_k |-\rangle$, e.g. by applying a Hadamard and measuring.

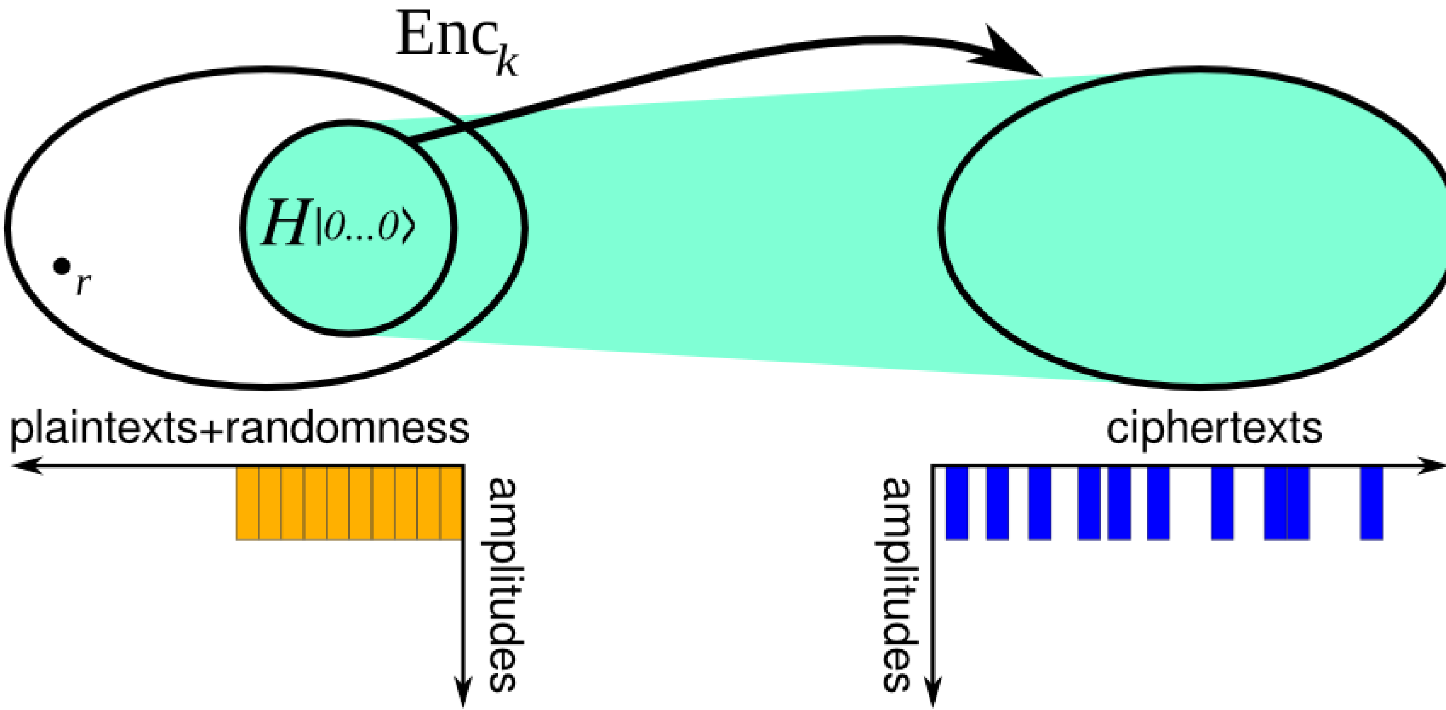
The solution



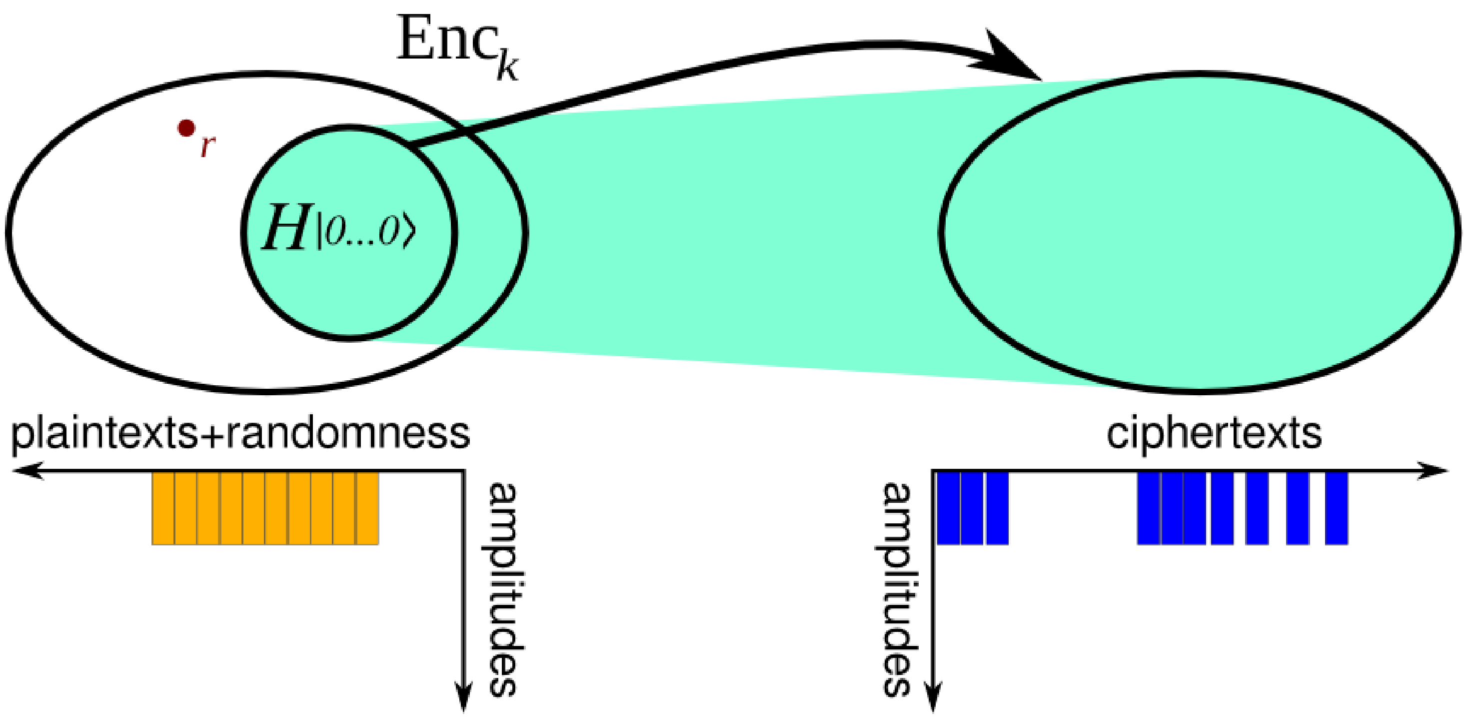
The solution



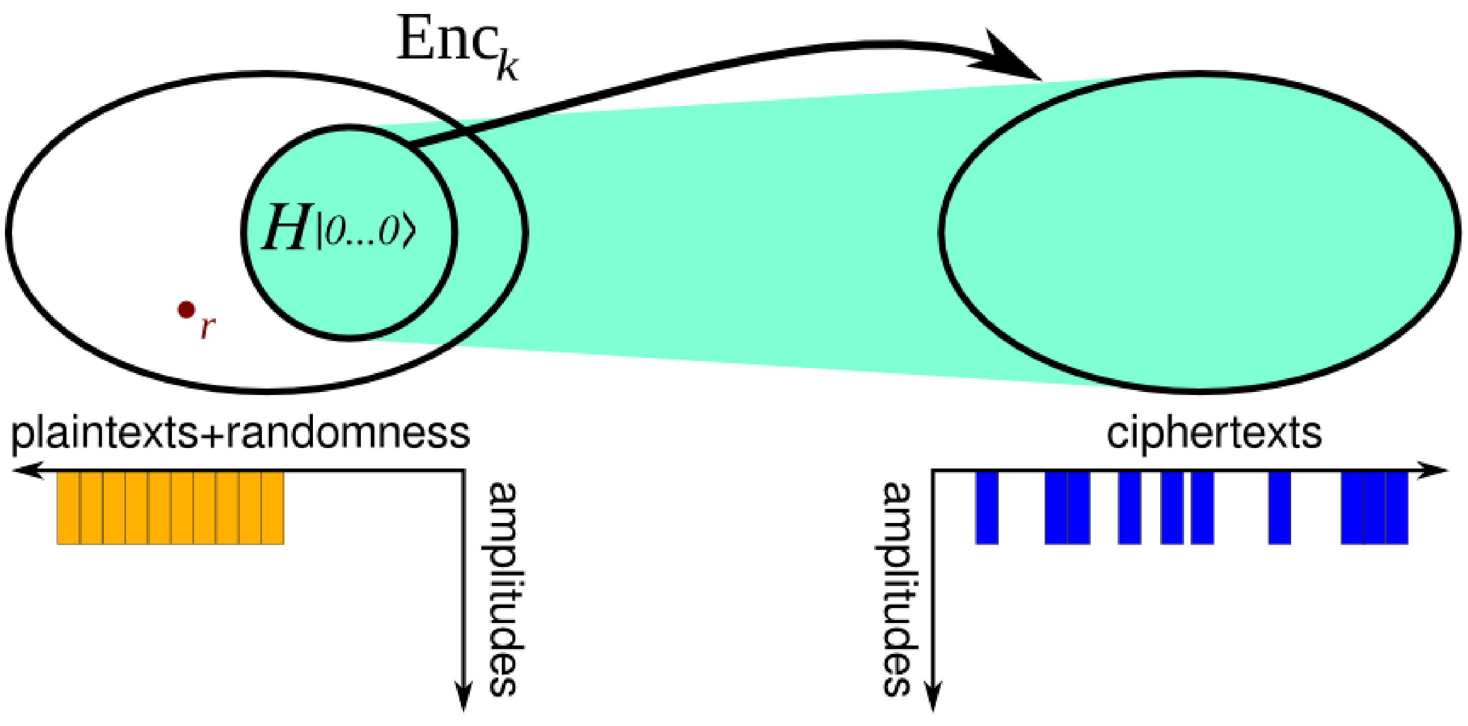
The solution



The solution



The solution



Secure Construction

Π family of quantum-secure pseudorandom permutations (QPRP)

Construction

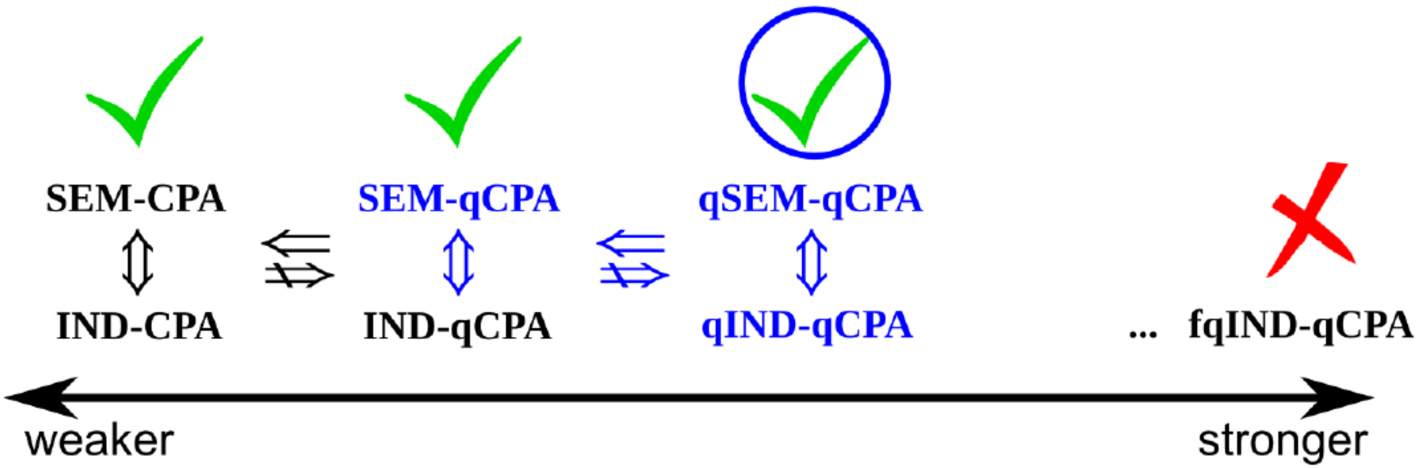
- Generate key: sample $(\pi, \pi^{-1}) \leftarrow \Pi$
- Encrypt message x: pad with n bits of randomness r and set $y = \pi(r \| x)$
- Decrypt y: truncate the first n bits of $\pi^{-1}(y)$

Theorem

The above scheme is qIND-qCPA secure.

(Idea of proof: show that for every two plaintext states φ_0, φ_1, the trace distance of the states ρ_0, ρ_1 obtained by considering their encryption under a mixture of every possible key is negligible)

Conclusion



Additional results:

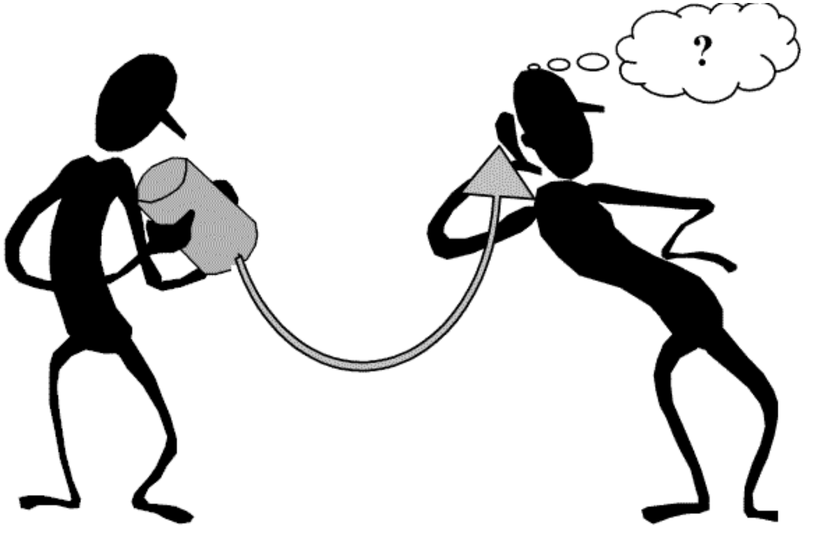
- can get rid of the 'classical description' restriction
- arbitrary length messages: 'randomized' ECB mode

Future directions:

- public-key encryption
- CCA security
- patch IND-qCPA $\Rightarrow$ qIND-qCPA

Thank you!

Questions?



https://eprint.iacr.org/2015/355