Semantic Security and Indistinguishability in the Quantum World

Tommaso Gagliardoni[1]

CASED and EC-SPRIDE and TU Darmstadt

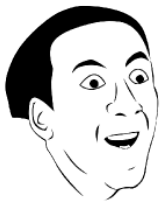
May 6th, 2015
Lugano, Switzerland

[1] from a joint work with Andreas Hülsing and Christian Schaffner

Introduction

Introduction

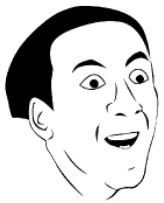
Starring



The Adversary

Introduction

Starring

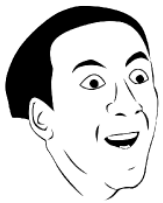


The Adversary

The Challenger

Introduction

Starring



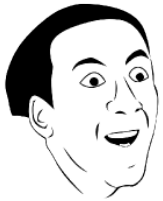
The Adversary

The Challenger

THE SIMULATOR

Introduction

Starring



The Adversary

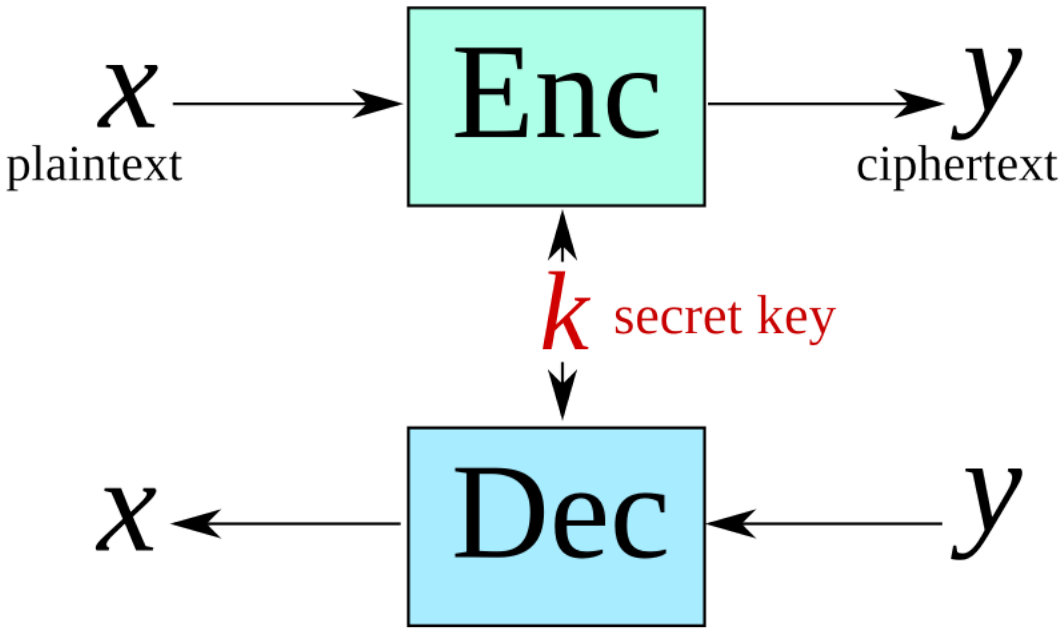
The Challenger

THE SIMULATOR

The Quantum Power

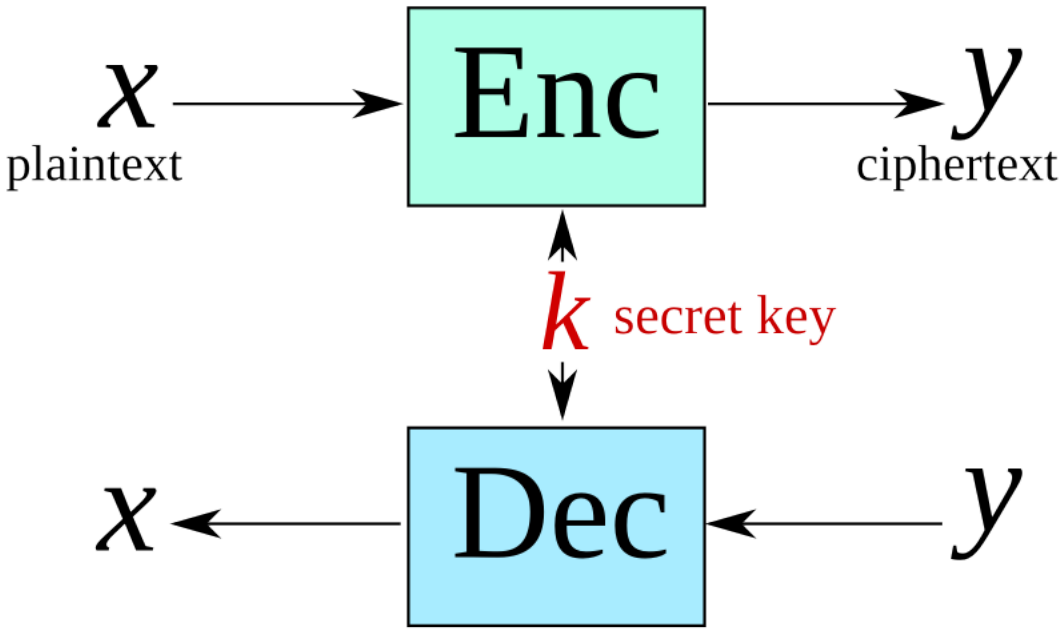
Introduction

Let's focus on symmetric-key encryption schemes



Introduction

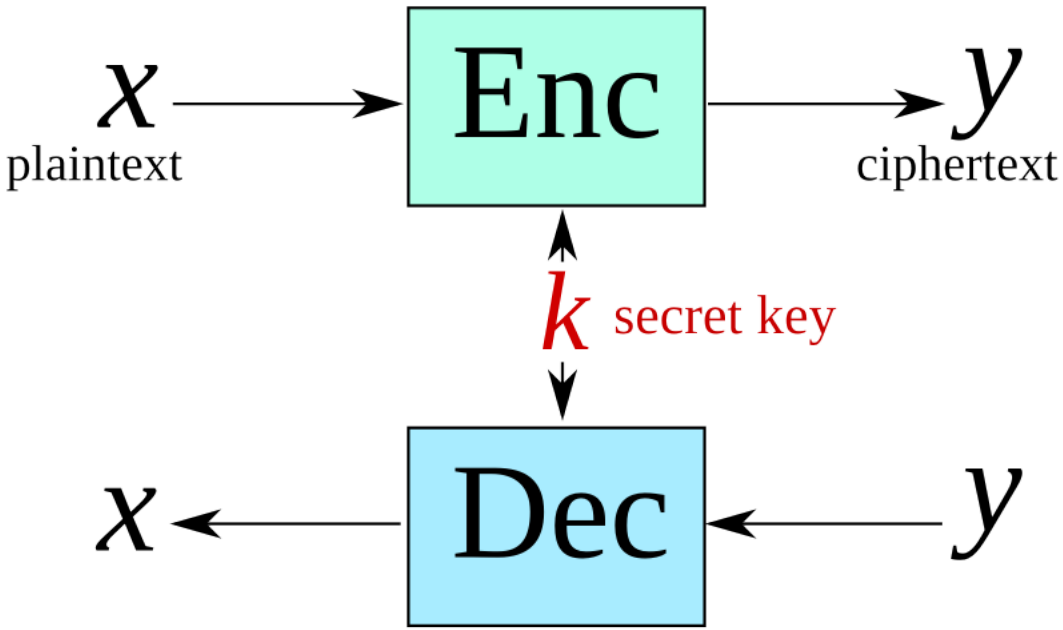
Let's focus on symmetric-key encryption schemes



We want this thing to be 'secure'.

Introduction

Let's focus on symmetric-key encryption schemes



We want this thing to be 'secure'.
But what does it mean secure?

Introduction

Definition Attempt 1

It must be hard, without k, to recover x from $\mathrm{Enc}_k(x)$.

Introduction

Definition Attempt 1

It must be hard, without k, to recover x from $\mathrm{Enc}_k(x)$.

Consider the following: $\mathrm{Enc}_k(x_1 \| x_2) = (x_1 \oplus k \| x_2)$.

Introduction

Definition Attempt 1

It must be hard, without k, to recover x from $\mathrm{Enc}_k(x)$.

Consider the following: $\mathrm{Enc}_k(x_1 \| x_2) = (x_1 \oplus k \| x_2)$.

'We will attack at dawn' $\Rightarrow$ *'5dk8k4s0lQ1ack at dawn'*

Introduction

Definition Attempt 1

It must be hard, without k, to recover x from $\mathrm{Enc}_k(x)$.

Consider the following: $\mathrm{Enc}_k(x_1 \| x_2) = (x_1 \oplus k \| x_2)$.

'We will attack at dawn' $\Rightarrow$ *'5dk8k4s0lQ1ack at dawn'*

Definition Attempt 2

It must be hard, without k, to recover any information about x from $\mathrm{Enc}_k(x)$.

Introduction

Definition Attempt 1

It must be hard, without k, to recover x from $\mathsf{Enc}_k(x)$.

Consider the following: $\mathsf{Enc}_k(x_1 \| x_2) = (x_1 \oplus k \| x_2)$.

'We will attack at dawn' $\Rightarrow$ *'5dk8k4s0lQ1ack at dawn'*

Definition Attempt 2

It must be hard, without k, to recover any information about x from $\mathsf{Enc}_k(x)$.

Consider the OTP: $\mathsf{Enc}_k(x) = (x \oplus k)$.

Introduction

Definition Attempt 1

It must be hard, without k, to recover x from $\mathsf{Enc}_k(x)$.

Consider the following: $\mathsf{Enc}_k(x_1 \| x_2) = (x_1 \oplus k \| x_2)$.

'We will attack at dawn' $\Rightarrow$ *'5dk8k4s0lQ1ack at dawn'*

Definition Attempt 2

It must be hard, without k, to recover any information about x from $\mathsf{Enc}_k(x)$.

Consider the OTP: $\mathsf{Enc}_k(x) = (x \oplus k)$.

'5dk8k4s0lQ1t6ss3hz01' $\Rightarrow$ Length$(x) = 20$ Bytes

Classical Semantic Security

Game-based security: $\mathcal{A}$ and $\mathcal{S}$ play an interactive game in two different 'worlds' against $\mathcal{C}$.

Classical Semantic Security

Game-based security: $\mathcal{A}$ and $\mathcal{S}$ play an interactive game in two different 'worlds' against $\mathcal{C}$.

SEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

Classical Semantic Security

Game-based security: $\mathcal{A}$ and $\mathcal{S}$ play an interactive game in two different 'worlds' against $\mathcal{C}$.

SEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a message distribution X on plaintext space $\mathcal{M}$,

Classical Semantic Security

Game-based security: $\mathcal{A}$ and $\mathcal{S}$ play an interactive game in two different 'worlds' against $\mathcal{C}$.

SEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a message distribution X on plaintext space $\mathcal{M}$,
- an advice function $h : \mathcal{M} \to \mathbb{N}$,

Classical Semantic Security

Game-based security: $\mathcal{A}$ and $\mathcal{S}$ play an interactive game in two different 'worlds' against $\mathcal{C}$.

SEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a message distribution X on plaintext space $\mathcal{M}$,
- an advice function $h : \mathcal{M} \to \mathbb{N}$,
- a target function $f : \mathcal{M} \to \mathbb{N}$.

Classical Semantic Security

Game-based security: $\mathcal{A}$ and $\mathcal{S}$ play an interactive game in two different 'worlds' against $\mathcal{C}$.

SEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a message distribution X on plaintext space $\mathcal{M}$,
- an advice function $h : \mathcal{M} \to \mathbb{N}$,
- a target function $f : \mathcal{M} \to \mathbb{N}$.

$\mathcal{C}$ samples $x \leftarrow X$ and sends back $(\mathrm{Enc}_k(x), h(x))$ to $\mathcal{A}$,

Classical Semantic Security

Game-based security: $\mathcal{A}$ and $\mathcal{S}$ play an interactive game in two different 'worlds' against $\mathcal{C}$.

SEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a message distribution X on plaintext space $\mathcal{M}$,
- an advice function $h : \mathcal{M} \to \mathbb{N}$,
- a target function $f : \mathcal{M} \to \mathbb{N}$.

$\mathcal{C}$ samples $x \leftarrow X$ and sends back $(\mathrm{Enc}_k(x), h(x))$ to $\mathcal{A}$, but $\mathcal{S}$ only gets $h(x)$.

Classical Semantic Security

Game-based security: $\mathcal{A}$ and $\mathcal{S}$ play an interactive game in two different 'worlds' against $\mathcal{C}$.

SEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a message distribution X on plaintext space $\mathcal{M}$,
- an advice function $h : \mathcal{M} \to \mathbb{N}$,
- a target function $f : \mathcal{M} \to \mathbb{N}$.

$\mathcal{C}$ samples $x \leftarrow X$ and sends back $(\mathrm{Enc}_k(x), h(x))$ to $\mathcal{A}$, but $\mathcal{S}$ only gets $h(x)$. The goal is to compute $f(x)$.

Classical Semantic Security

Game-based security: $\mathcal{A}$ and $\mathcal{S}$ play an interactive game in two different 'worlds' against $\mathcal{C}$.

SEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a message distribution X on plaintext space $\mathcal{M}$,
- an advice function $h : \mathcal{M} \to \mathbb{N}$,
- a target function $f : \mathcal{M} \to \mathbb{N}$.

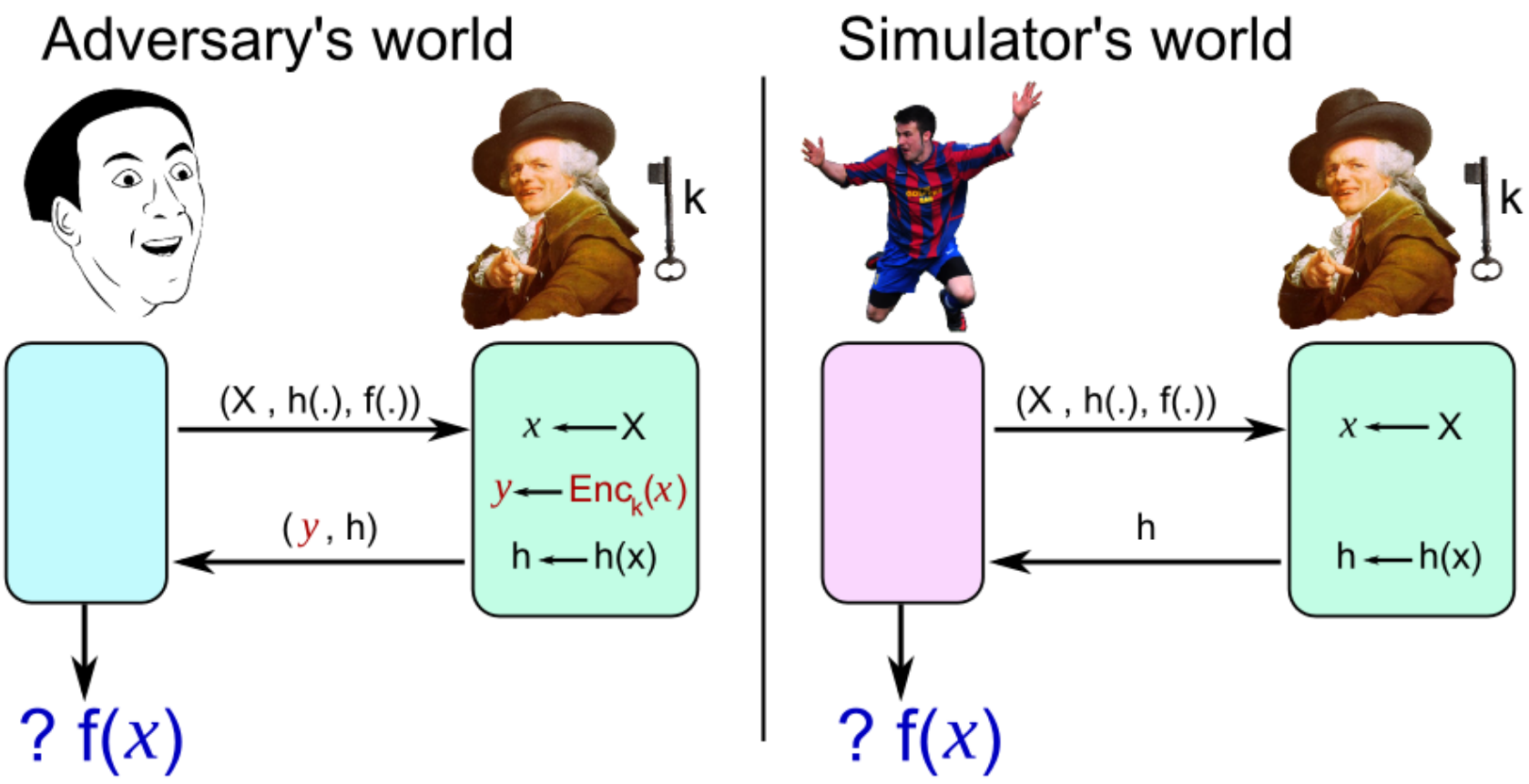
$\mathcal{C}$ samples $x \leftarrow X$ and sends back $(\mathsf{Enc}_k(x), h(x))$ to $\mathcal{A}$, but $\mathcal{S}$ only gets $h(x)$. The goal is to compute $f(x)$.

Classical Semantic Security (SEM)

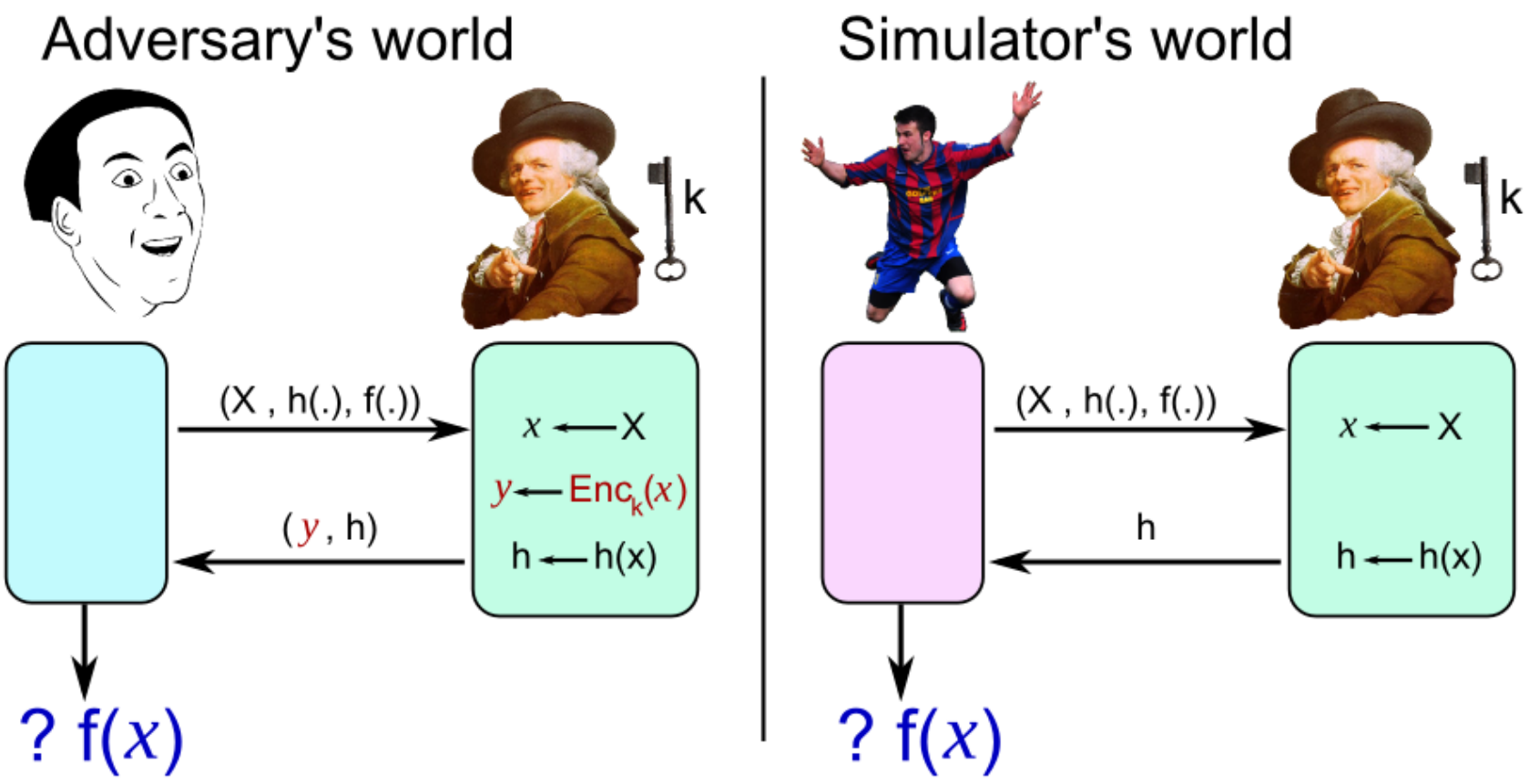
For any efficient adversary $\mathcal{A}$ there exists an efficient simulator $\mathcal{S}$ such that:

$$|\Pr[\mathcal{A}(\mathsf{Enc}_k(x), h(x)) = f(x)] - \Pr[\mathcal{S}(h(x)) = f(x)]| \leq \mathsf{negl}(n).$$

Classical Semantic Security



Classical Semantic Security



This definition is cumbersome.

Classical Indistinguishability

IND challenge query: $\mathcal{A}$ sends $\mathcal{C}$ two plaintexts $x_0, x_1 \in \mathcal{M}$.

Classical Indistinguishability

IND challenge query: $\mathcal{A}$ sends $\mathcal{C}$ two plaintexts $x_0, x_1 \in \mathcal{M}$.

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

Classical Indistinguishability

IND challenge query: $\mathcal{A}$ sends $\mathcal{C}$ two plaintexts $x_0, x_1 \in \mathcal{M}$.

$\mathcal{C}$ flips a random bit $b \xleftarrow{\$} \{0,1\}$, computes $y \leftarrow \mathsf{Enc}_k(x_b)$,

Classical Indistinguishability

IND challenge query: $\mathcal{A}$ sends $\mathcal{C}$ two plaintexts $x_0, x_1 \in \mathcal{M}$.

$\mathcal{C}$ flips a random bit $b \xleftarrow{\$} \{0,1\}$, computes $y \leftarrow \mathsf{Enc}_k(x_b)$, and finally sends ciphertext y to $\mathcal{A}$.

Classical Indistinguishability

IND challenge query: $\mathcal{A}$ sends $\mathcal{C}$ two plaintexts $x_0, x_1 \in \mathcal{M}$.

$\mathcal{C}$ flips a random bit $b \xleftarrow{\$} \{0,1\}$, computes $y \leftarrow \mathsf{Enc}_k(x_b)$, and finally sends ciphertext y to $\mathcal{A}$.

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

Classical Indistinguishability

IND challenge query: $\mathcal{A}$ sends $\mathcal{C}$ two plaintexts $x_0, x_1 \in \mathcal{M}$.

$\mathcal{C}$ flips a random bit $b \xleftarrow{\$} \{0,1\}$, computes $y \leftarrow \mathsf{Enc}_k(x_b)$, and finally sends ciphertext y to $\mathcal{A}$.

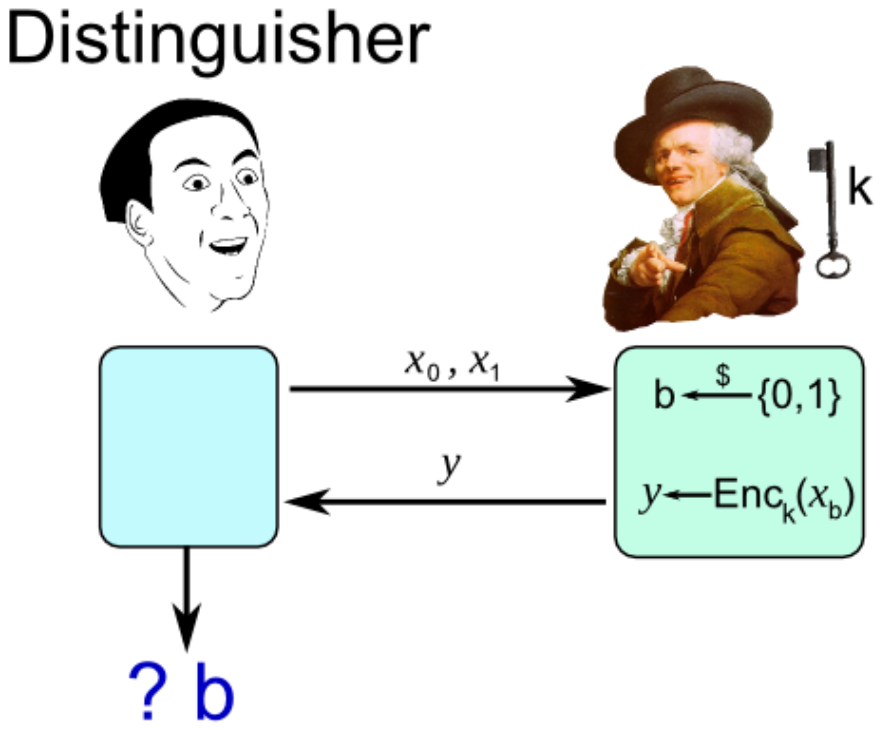
$\mathcal{A}$'s goal is to guess b.

Classical Indistinguishability (IND)

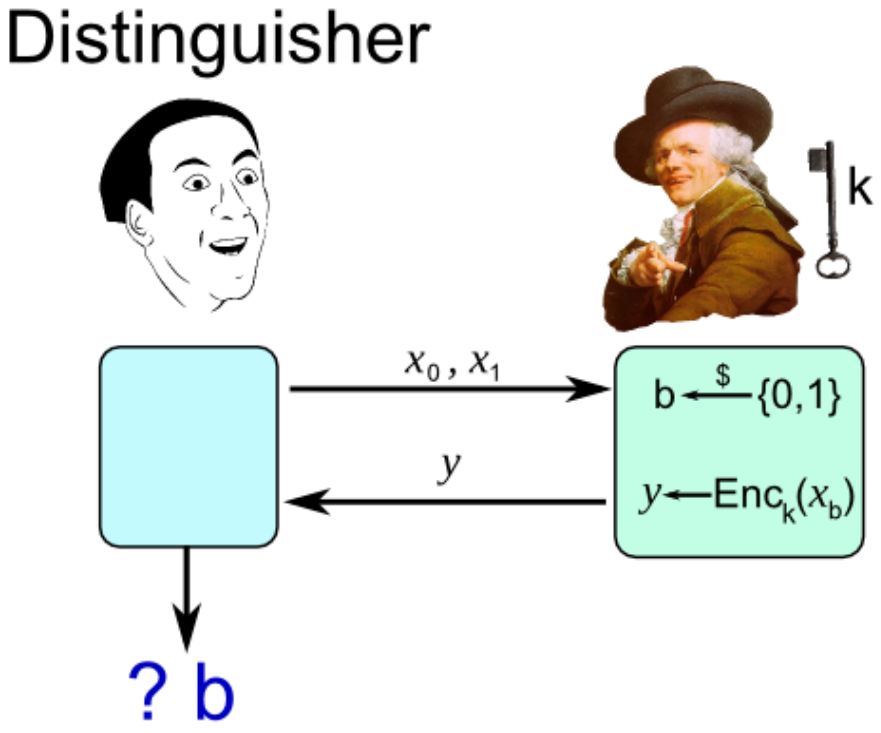
For any efficient adversary $\mathcal{A}$ and any $x_0, x_1 \in \mathcal{M}$:

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

Classical Indistinguishability



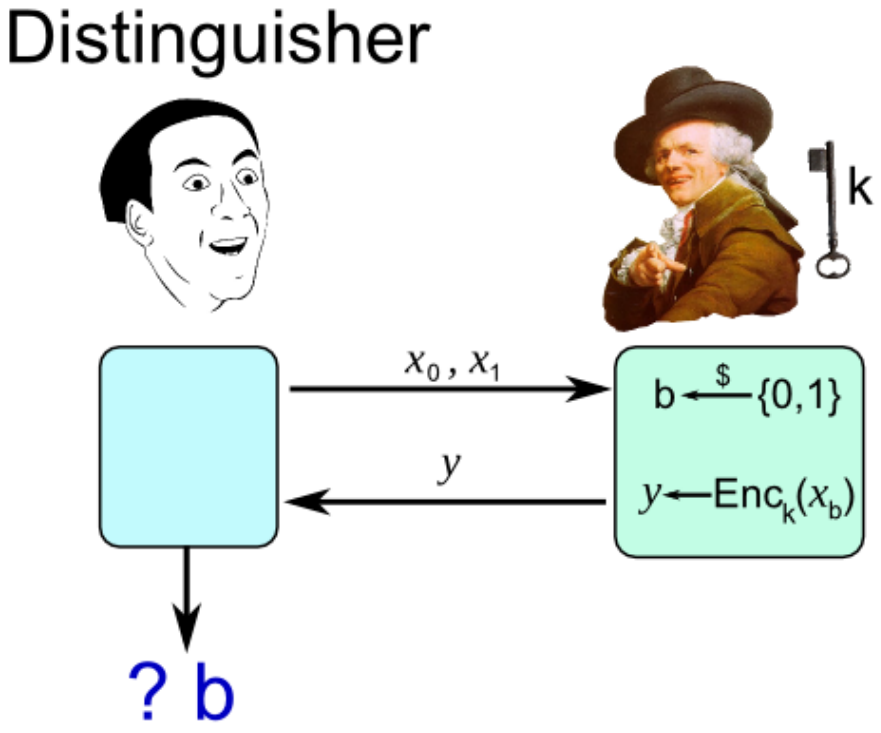
Classical Indistinguishability



Theorem

IND $\iff$ SEM.

Classical Indistinguishability



Theorem

IND $\iff$ SEM.

(many other equivalent formulations of IND and SEM)

Chosen Plaintext Attack

CPA 'learning' phase: $\mathcal{A}$ sends $\mathcal{C}$ up to $q = \text{poly}(n)$ plaintexts $x_1, \ldots, x_q \in \mathcal{M}$ (possibly adaptively).

Chosen Plaintext Attack

CPA 'learning' phase: $\mathcal{A}$ sends $\mathcal{C}$ up to $q = \text{poly}(n)$ plaintexts $x_1, \ldots, x_q \in \mathcal{M}$ (possibly adaptively).
$\mathcal{C}$ sends back $\text{Enc}_k(x_1), \ldots, \text{Enc}_k(x_q)$.

Chosen Plaintext Attack

CPA 'learning' phase: $\mathcal{A}$ sends $\mathcal{C}$ up to $q = \text{poly}(n)$ plaintexts $x_1, \ldots, x_q \in \mathcal{M}$ (possibly adaptively).
$\mathcal{C}$ sends back $\text{Enc}_k(x_1), \ldots, \text{Enc}_k(x_q)$.
Can be combined with other security notions:

Chosen Plaintext Attack

CPA 'learning' phase: $\mathcal{A}$ sends $\mathcal{C}$ up to $q = \text{poly}(n)$ plaintexts $x_1, \ldots, x_q \in \mathcal{M}$ (possibly adaptively).
$\mathcal{C}$ sends back $\text{Enc}_k(x_1), \ldots, \text{Enc}_k(x_q)$.
Can be combined with other security notions:

CPA phase + SEM phase $\Rightarrow$ SEM-CPA security.

Chosen Plaintext Attack

CPA 'learning' phase: $\mathcal{A}$ sends $\mathcal{C}$ up to $q = \text{poly}(n)$ plaintexts $x_1, \ldots, x_q \in \mathcal{M}$ (possibly adaptively).
$\mathcal{C}$ sends back $\text{Enc}_k(x_1), \ldots, \text{Enc}_k(x_q)$.
Can be combined with other security notions:

CPA phase + SEM phase $\Rightarrow$ SEM-CPA security.
CPA phase + IND phase $\Rightarrow$ IND-CPA security.

Chosen Plaintext Attack

CPA 'learning' phase: $\mathcal{A}$ sends $\mathcal{C}$ up to $q = \text{poly}(n)$ plaintexts $x_1, \ldots, x_q \in \mathcal{M}$ (possibly adaptively).
$\mathcal{C}$ sends back $\text{Enc}_k(x_1), \ldots, \text{Enc}_k(x_q)$.
Can be combined with other security notions:

CPA phase + SEM phase $\Rightarrow$ SEM-CPA security.
CPA phase + IND phase $\Rightarrow$ IND-CPA security.

Theorem

IND-CPA $\iff$ SEM-CPA.

Chosen Plaintext Attack

CPA 'learning' phase: $\mathcal{A}$ sends $\mathcal{C}$ up to $q = \text{poly}(n)$ plaintexts $x_1, \ldots, x_q \in \mathcal{M}$ (possibly adaptively).
$\mathcal{C}$ sends back $\text{Enc}_k(x_1), \ldots, \text{Enc}_k(x_q)$.
Can be combined with other security notions:

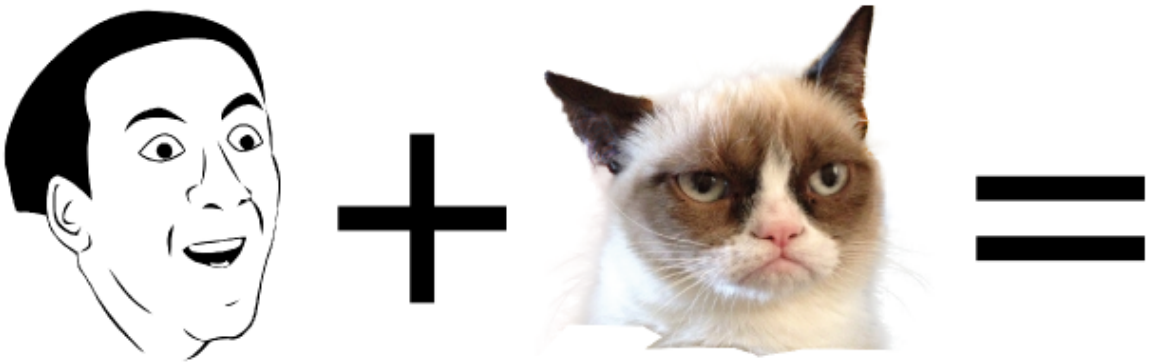
CPA phase + SEM phase $\Rightarrow$ SEM-CPA security.
CPA phase + IND phase $\Rightarrow$ IND-CPA security.

Theorem

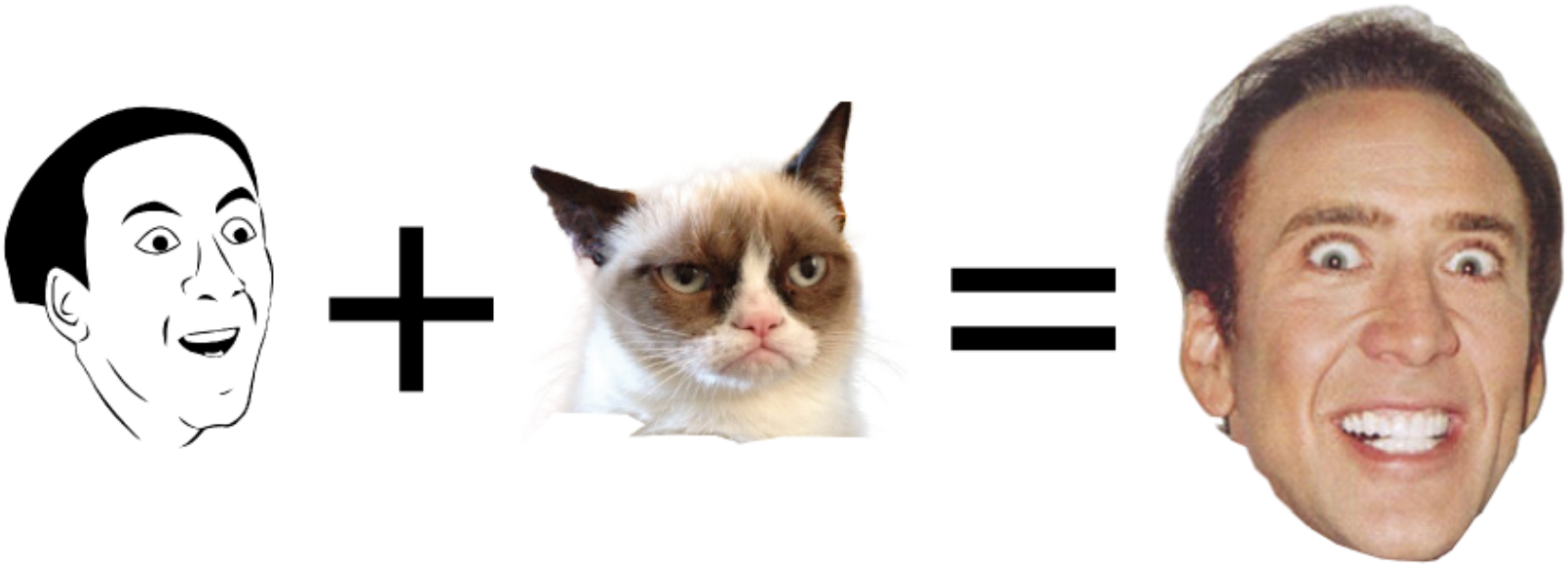
IND-CPA $\iff$ SEM-CPA.

Note: deterministic schemes are insecure $\Rightarrow$ need for randomization.

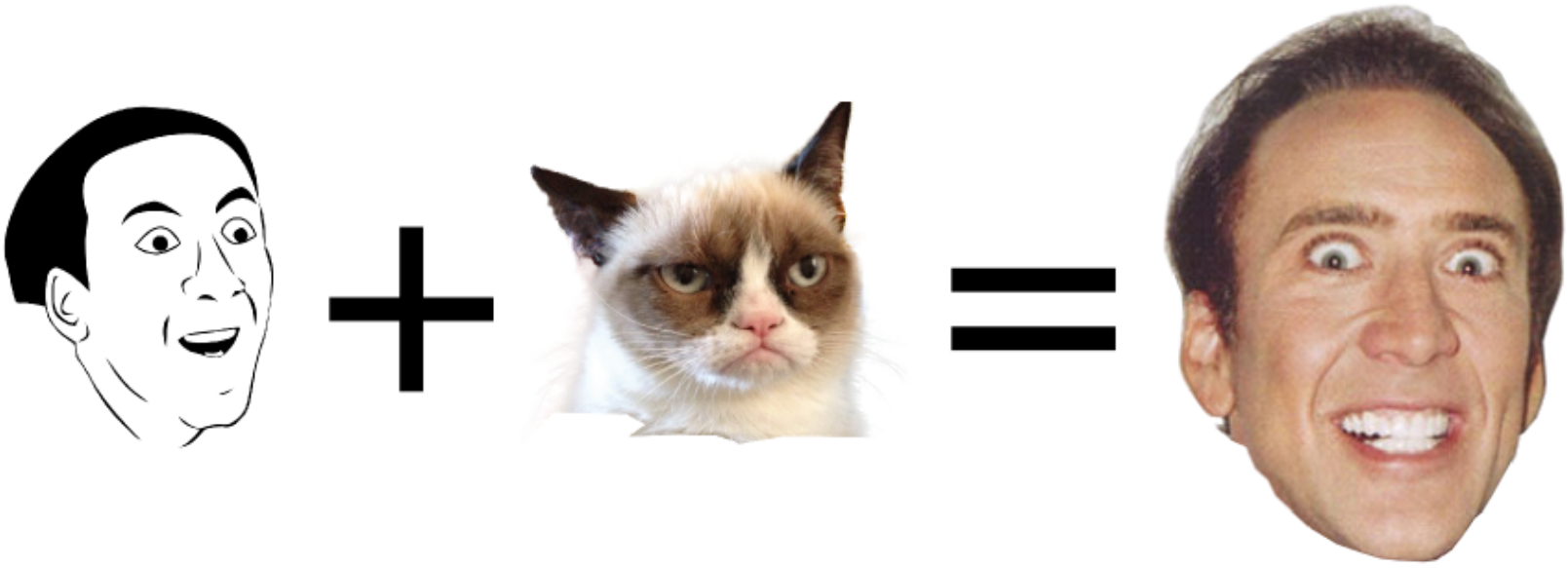
Quantum Adversaries



Quantum Adversaries

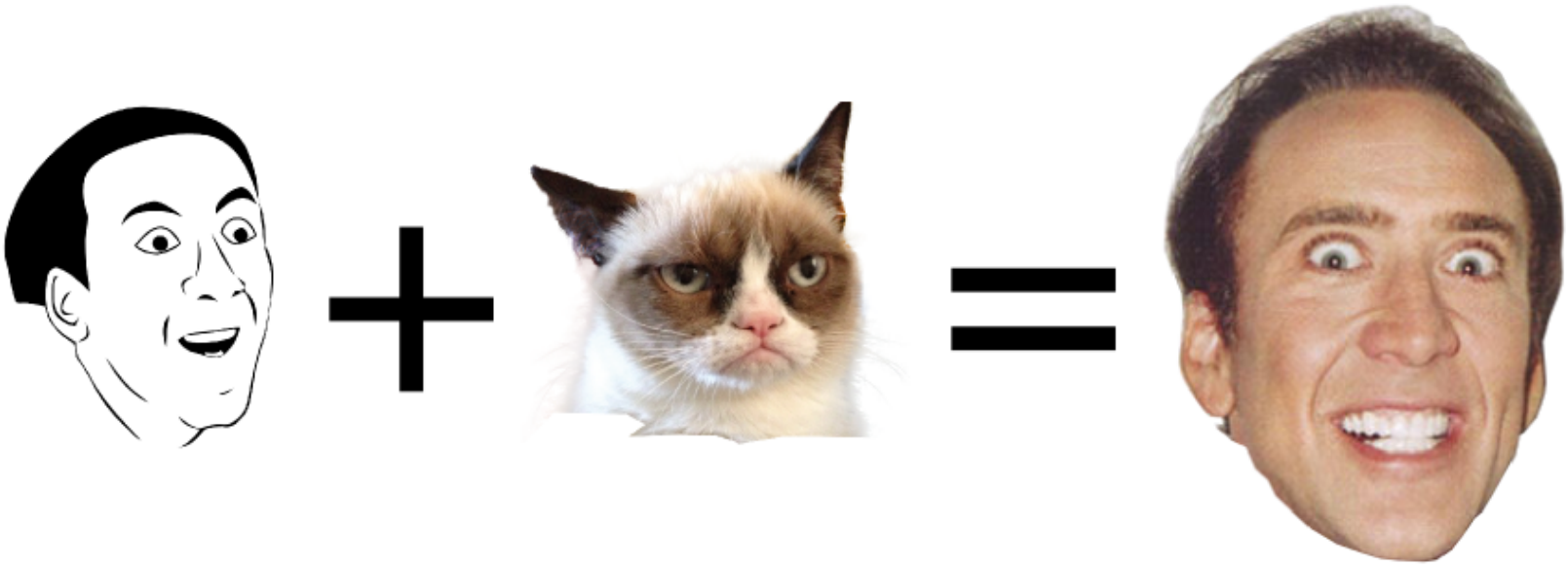


Quantum Adversaries



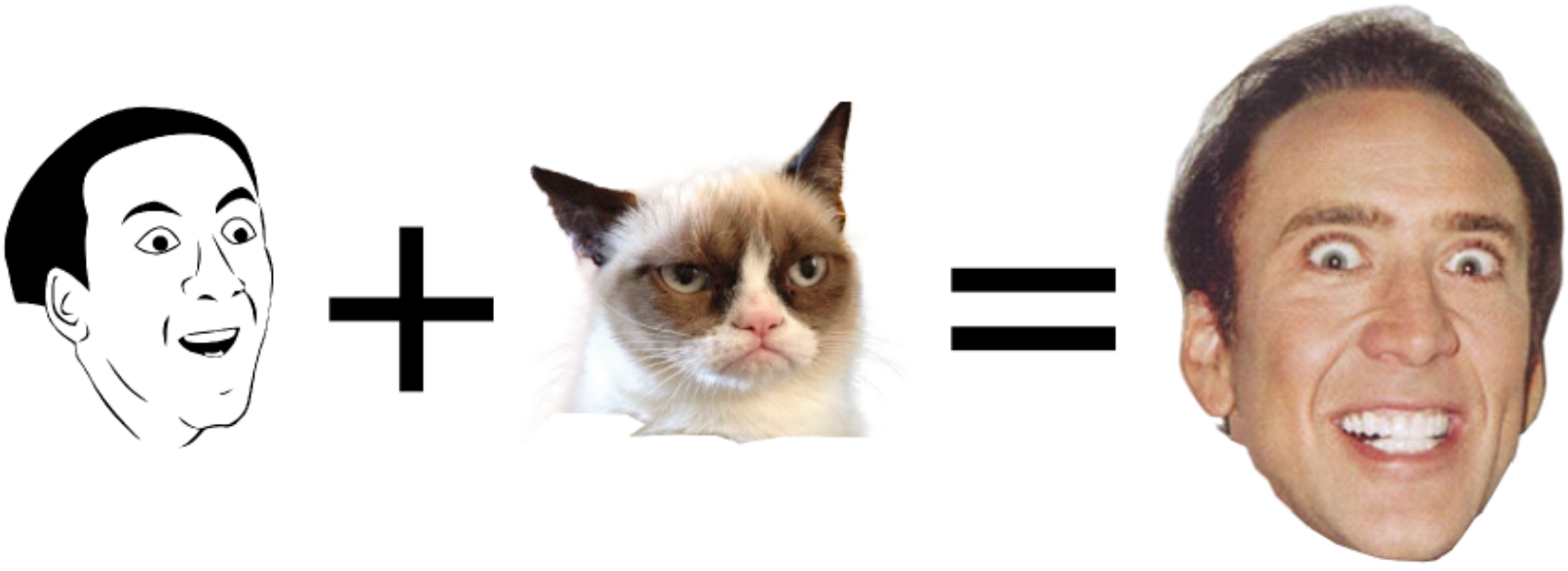
What do we know about quantum adversaries?

Quantum Adversaries



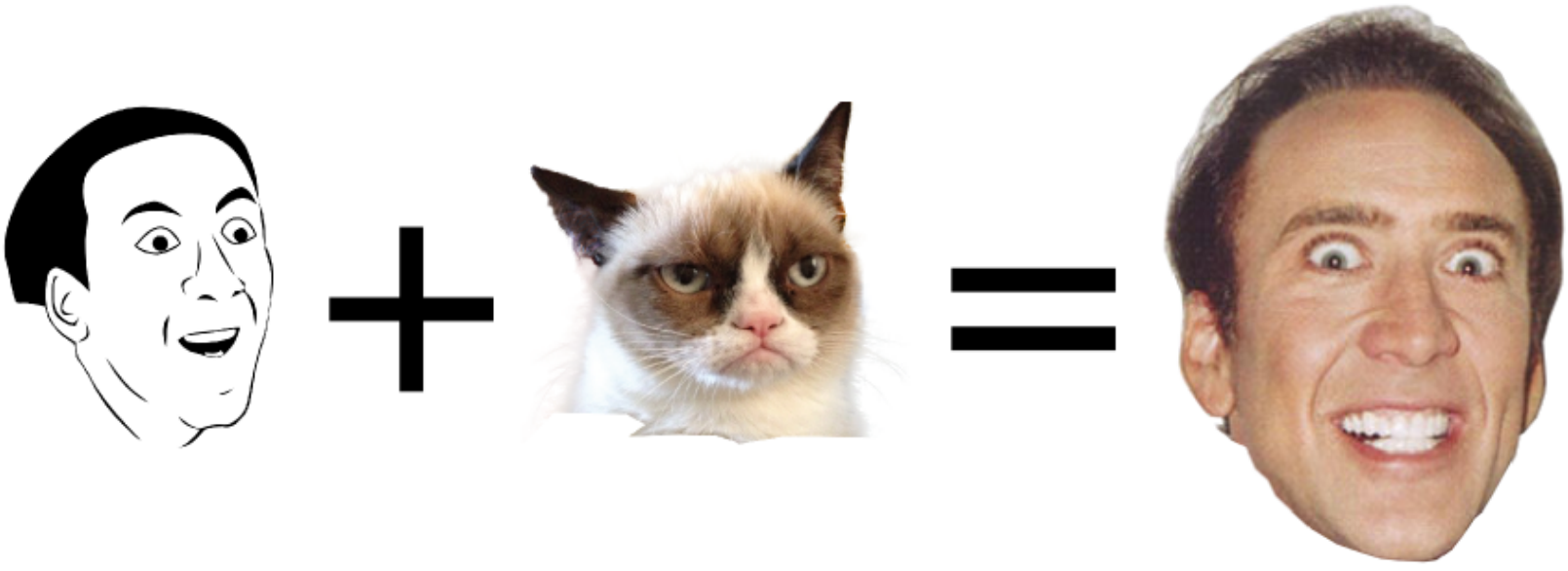
What do we know about quantum adversaries? Shor, Grover & friends: no RSA, discrete log, etc.

Quantum Adversaries



What do we know about quantum adversaries? Shor, Grover & friends: no RSA, discrete log, etc. But post-quantum crypto (lattice-based, multivariate, hash signatures etc.)

Quantum Adversaries

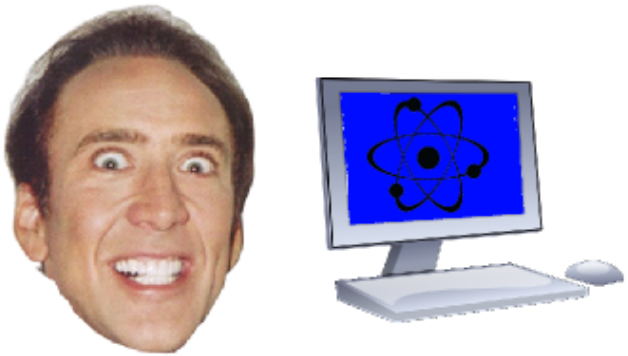


What do we know about quantum adversaries? Shor, Grover & friends: no RSA, discrete log, etc. But post-quantum crypto (lattice-based, multivariate, hash signatures etc.)

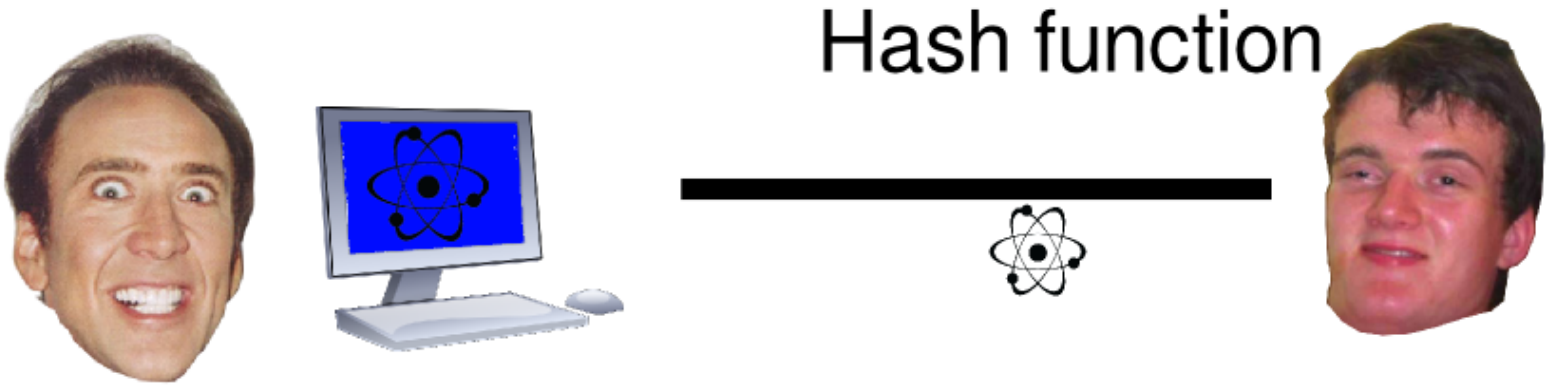
This is not enough!!!

Quantum Access

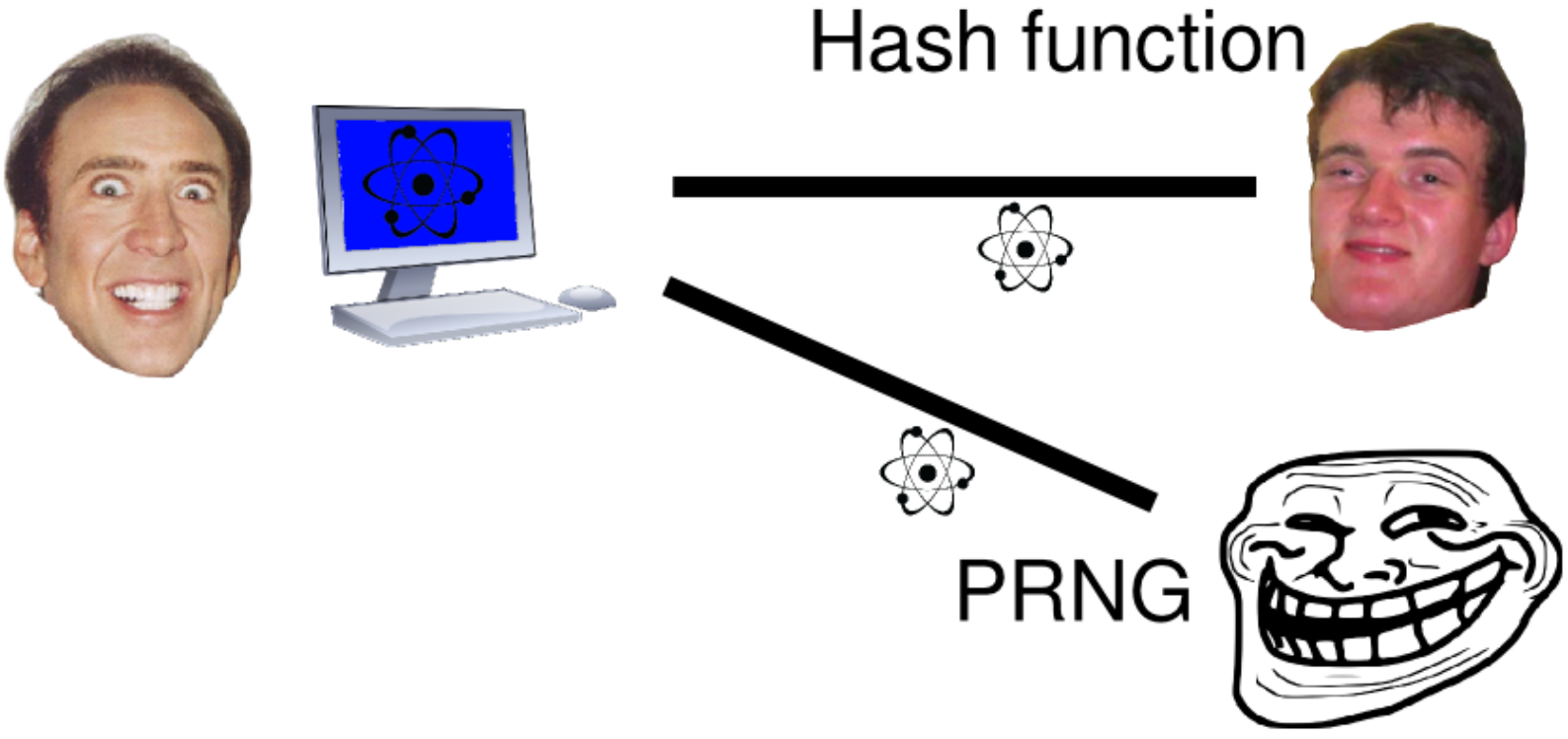
Quantum Access



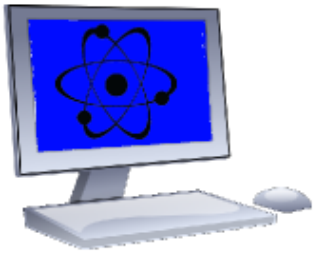
Quantum Access



Quantum Access



Quantum Access

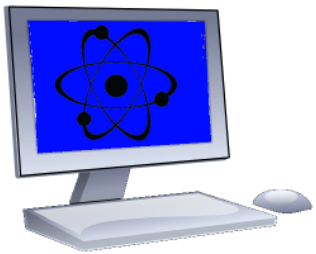


Hash function

PRNG

Encryption Oracle

Quantum Access



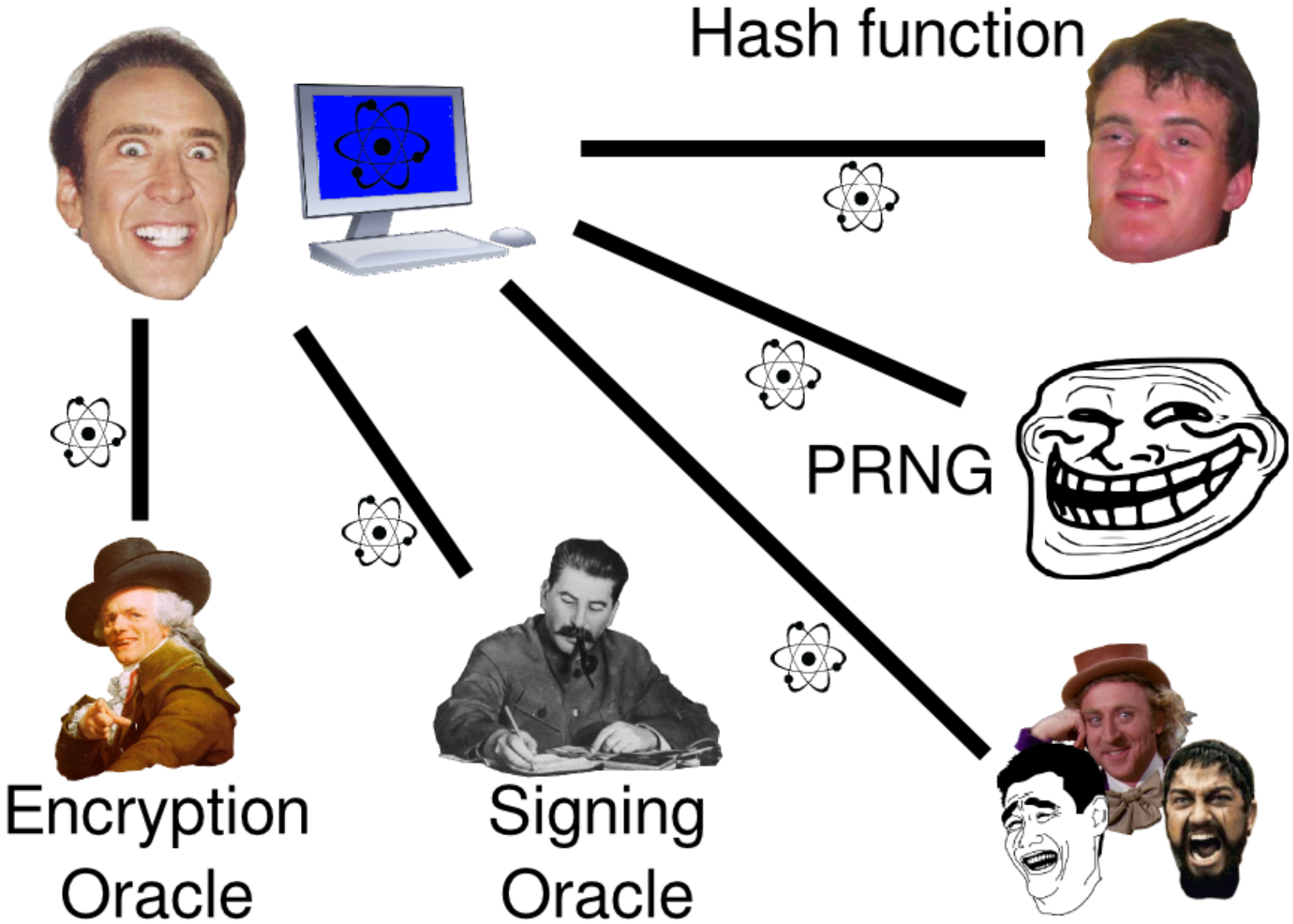
Hash function

PRNG

Encryption Oracle

Signing Oracle

Quantum Access



Example: Quantum CPA

CPA phase: $\mathcal{A}$ and $\mathcal{C}$ share a classical channel:

- $\mathcal{A}$ sends query: x_i;
- $\mathcal{C}$ replies with: $\mathrm{Enc}_k(x_i)$;
- repeat for $i = 1, \ldots, q \leq \mathrm{poly}(n)$ times.

Example: Quantum CPA

CPA phase: $\mathcal{A}$ and $\mathcal{C}$ share a classical channel:

- $\mathcal{A}$ sends query: x_i;
- $\mathcal{C}$ replies with: $\mathsf{Enc}_k(x_i)$;
- repeat for $i = 1, \ldots, q \leq \mathrm{poly}(n)$ times.

qCPA phase: $\mathcal{A}$ and $\mathcal{C}$ share a quantum channel:

- $\mathcal{A}$ sends query: $\sum_{x,i} \alpha_{x,i} |x, 0\rangle$
- $\mathcal{C}$ replies with: $\sum_{x,i} \alpha_{x,i} |x, \mathsf{Enc}_k(x)\rangle$
- repeat for $i = 1, \ldots, q \leq \mathrm{poly}(n)$ times.

Why Quantum Access?

For Hash functions, PRFs etc, quite natural.

Why Quantum Access?

For Hash functions, PRFs etc, quite natural.

But why quantum access to classical parties?

Why Quantum Access?

For Hash functions, PRFs etc, quite natural.

But why quantum access to classical parties?

- use of classical schemes as subroutines in complex quantum protocols;

Why Quantum Access?

For Hash functions, PRFs etc, quite natural.

But why quantum access to classical parties?

- use of classical schemes as subroutines in complex quantum protocols;
- quantum party communicates with classical party but adversary is able to observe state before measurement;

Why Quantum Access?

For Hash functions, PRFs etc, quite natural.

But why quantum access to classical parties?

- use of classical schemes as subroutines in complex quantum protocols;
- quantum party communicates with classical party but adversary is able to observe state before measurement;
- adversary is able to 'force' quantum behaviour in classical party (frozen smartcard).

Why Quantum Access?

For Hash functions, PRFs etc, quite natural.

But why quantum access to classical parties?

- use of classical schemes as subroutines in complex quantum protocols;
- quantum party communicates with classical party but adversary is able to observe state before measurement;
- adversary is able to 'force' quantum behaviour in classical party (frozen smartcard).

What about encryption?

Fully Quantum Indistinguishability

In [BZ13][2]: fqIND phase: $\mathcal{A}$ and $\mathcal{C}$ share three quantum registers:

[2] D. Boneh, M. Zhandry: *'Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World'*, CRYPTO 2013.

Fully Quantum Indistinguishability

In [BZ13][2]: fqIND phase: $\mathcal{A}$ and $\mathcal{C}$ share three quantum registers:

- $\mathcal{A}$ prepares state:

$$\sum_{x_0,x_1} \alpha_{x_0,x_1} |x_0, x_1, 0\rangle$$

[2] D. Boneh, M. Zhandry: *'Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World'*, CRYPTO 2013.

Fully Quantum Indistinguishability

In [BZ13][2]: fqIND phase: $\mathcal{A}$ and $\mathcal{C}$ share three quantum registers:

- $\mathcal{A}$ prepares state:

$$\sum_{x_0,x_1} \alpha_{x_0,x_1} |x_0, x_1, 0\rangle$$

- $\mathcal{C}$ flips $b \xleftarrow{\$} \{0,1\}$ and transforms register to:

$$\sum_{x_0,x_1} \alpha_{x_0,x_1} |x_0, x_1, \mathsf{Enc}_k(x_b)\rangle$$

[2] D. Boneh, M. Zhandry: *'Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World'*, CRYPTO 2013.

Fully Quantum Indistinguishability

In [BZ13][2]: fqIND phase: $\mathcal{A}$ and $\mathcal{C}$ share three quantum registers:

- $\mathcal{A}$ prepares state:

$$\sum_{x_0,x_1} \alpha_{x_0,x_1} |x_0, x_1, 0\rangle$$

- $\mathcal{C}$ flips $b \xleftarrow{\$} \{0,1\}$ and transforms register to:

$$\sum_{x_0,x_1} \alpha_{x_0,x_1} |x_0, x_1, \mathsf{Enc}_k(x_b)\rangle$$

- $\mathcal{A}$ must guess b.

[2] D. Boneh, M. Zhandry: *'Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World'*, CRYPTO 2013.

Fully Quantum Indistinguishability

In [BZ13][2]: fqIND phase: $\mathcal{A}$ and $\mathcal{C}$ share three quantum registers:

- $\mathcal{A}$ prepares state:

$$\sum_{x_0,x_1} \alpha_{x_0,x_1} |x_0, x_1, 0\rangle$$

- $\mathcal{C}$ flips $b \xleftarrow{\$} \{0,1\}$ and transforms register to:

$$\sum_{x_0,x_1} \alpha_{x_0,x_1} |x_0, x_1, \mathsf{Enc}_k(x_b)\rangle$$

- $\mathcal{A}$ must guess b.

Theorem

qIND is unachievable (too strong).

(attack exploits entanglement between ciphertext and plaintext)

[2] D. Boneh, M. Zhandry: *'Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World'*, CRYPTO 2013.

The Compromise

fqIND-qCPA natural but too strong, but IND-CPA too weak against quantum adversaries.

The Compromise

fqIND-qCPA natural but too strong, but IND-CPA too weak against quantum adversaries.

IND-qCPA

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

The Compromise

fqIND-qCPA natural but too strong, but IND-CPA too weak against quantum adversaries.

IND-qCPA

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

Theorem

IND-qCPA is achievable.

The Compromise

fqIND-qCPA natural but too strong, but IND-CPA too weak against quantum adversaries.

IND-qCPA

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

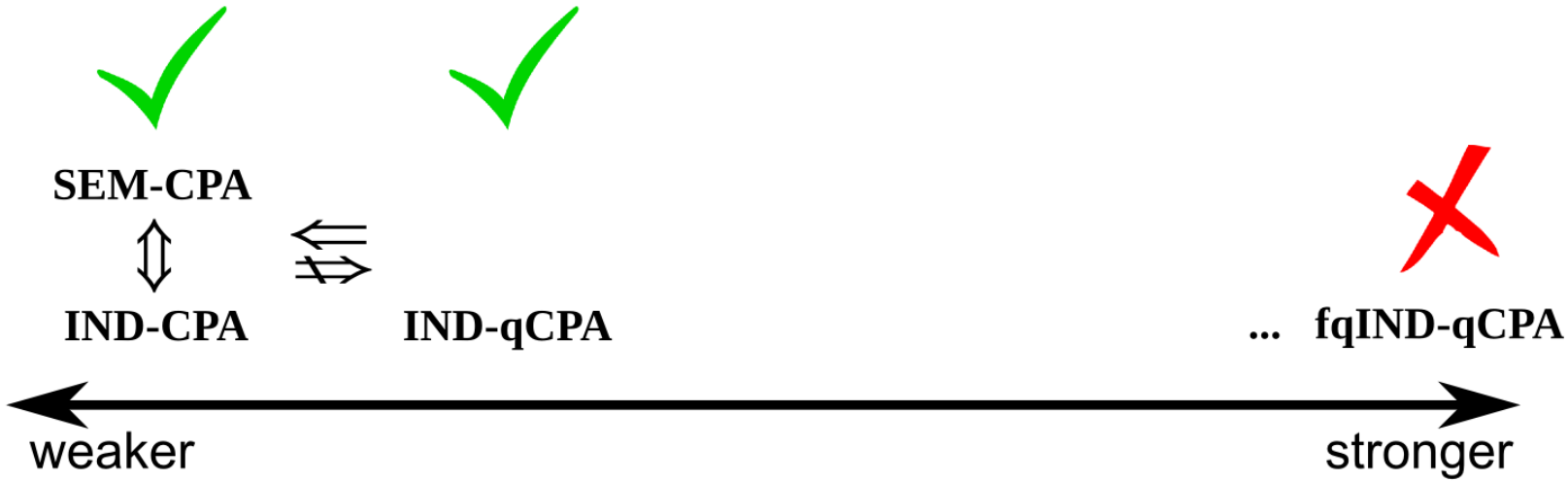
Theorem

IND-qCPA is achievable.

Theorem

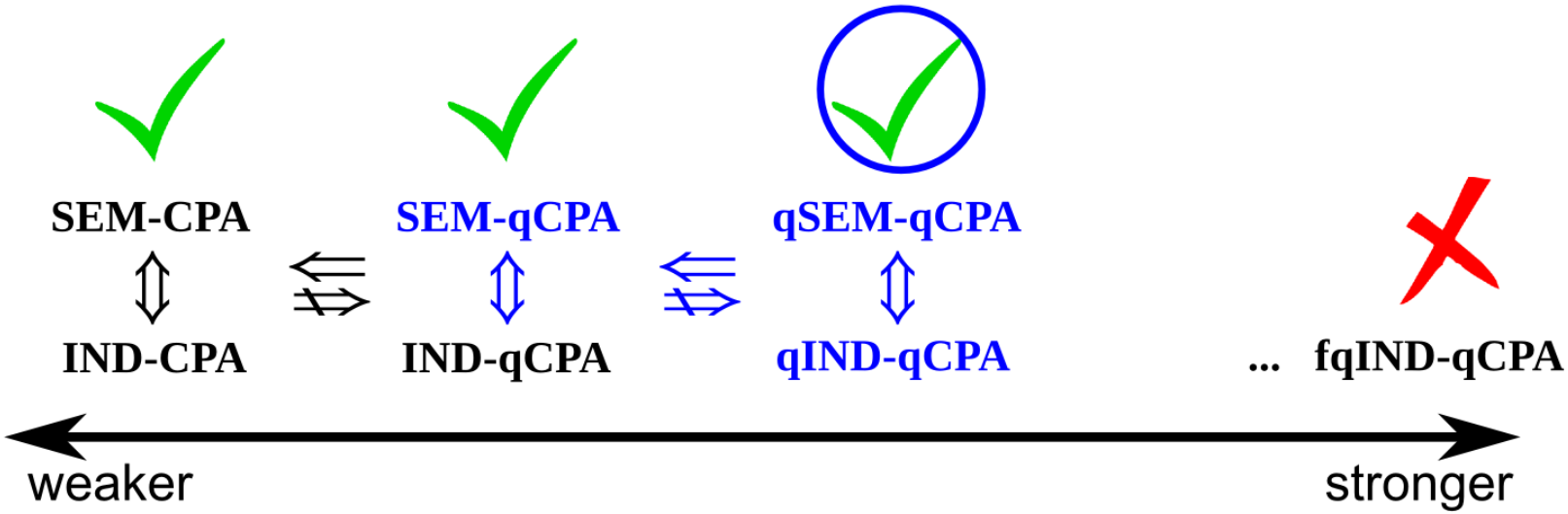
IND-qCPA is strictly stronger than classical IND-CPA.

The current situation



Unsatisfying...

The current situation



Our contribution!

The Road to qIND

(only focus on qIND- phase, but also assume a -qCPA phase)

The Road to qIND

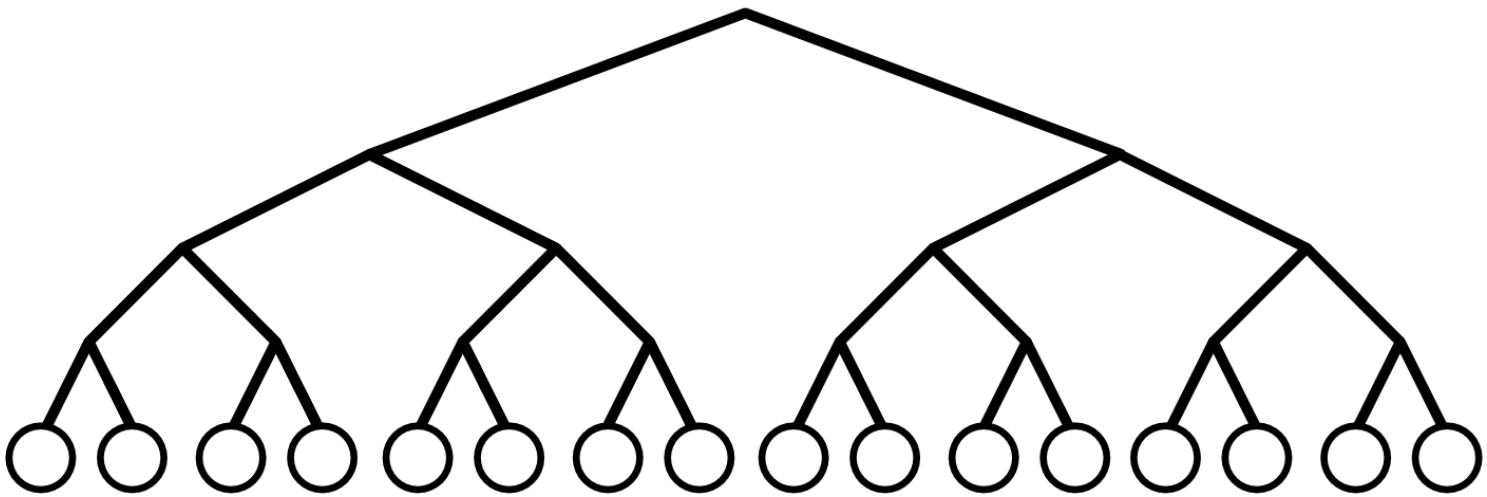
(only focus on qIND- phase, but also assume a -qCPA phase)

For fqIND-qCPA many assumptions were implicitly made.

The Road to qIND

(only focus on qIND- phase, but also assume a -qCPA phase)

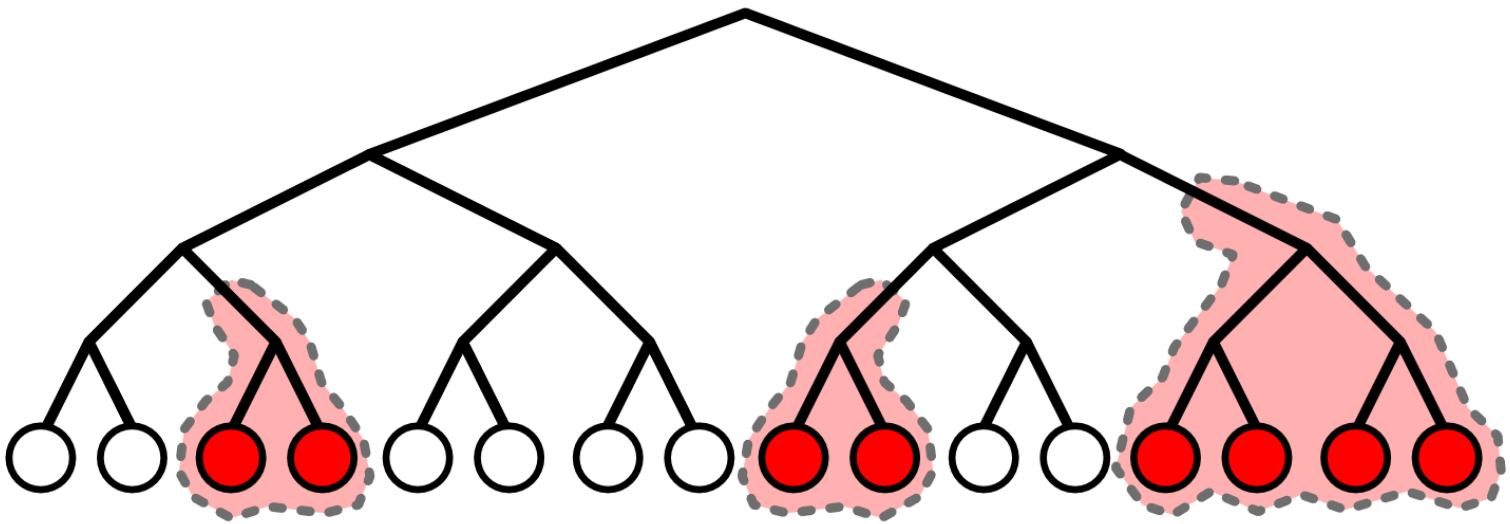
For fqIND-qCPA many assumptions were implicitly made. In our work, we explore every option: 'security tree' of definitions:



The Road to qIND

(only focus on qIND- phase, but also assume a -qCPA phase)

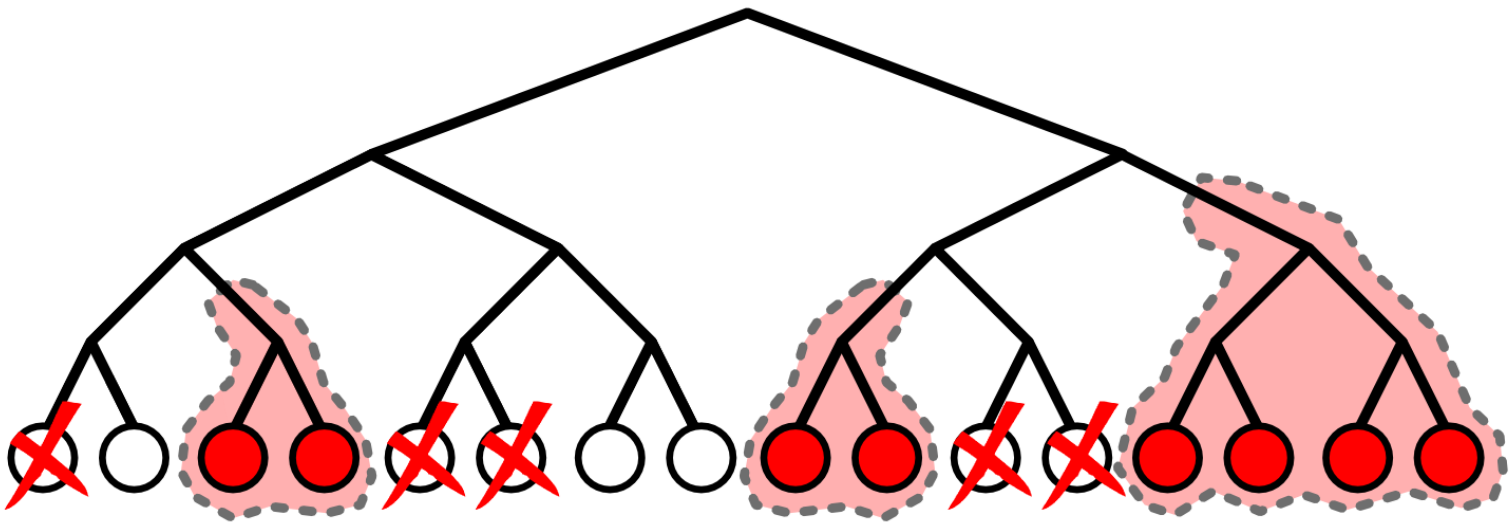
For fqIND-qCPA many assumptions were implicitly made. In our work, we explore every option: 'security tree' of definitions:



The Road to qIND

(only focus on qIND- phase, but also assume a -qCPA phase)

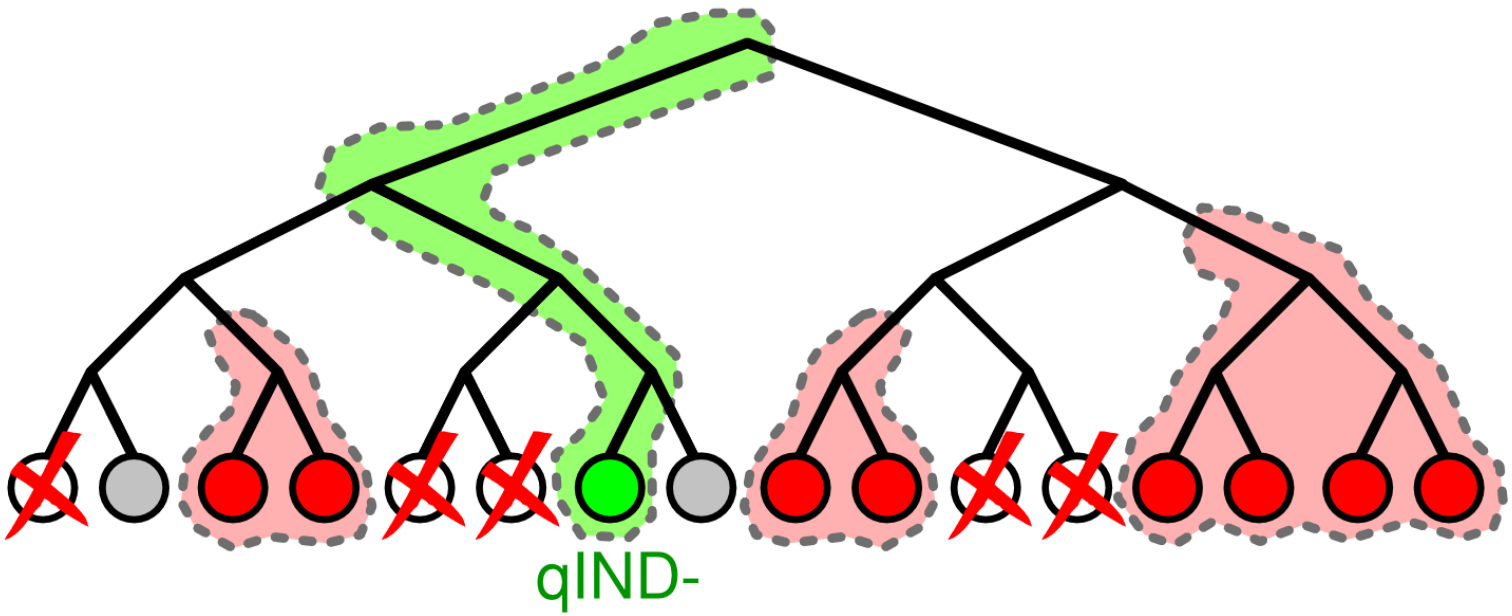
For fqIND-qCPA many assumptions were implicitly made. In our work, we explore every option: 'security tree' of definitions:



The Road to qIND

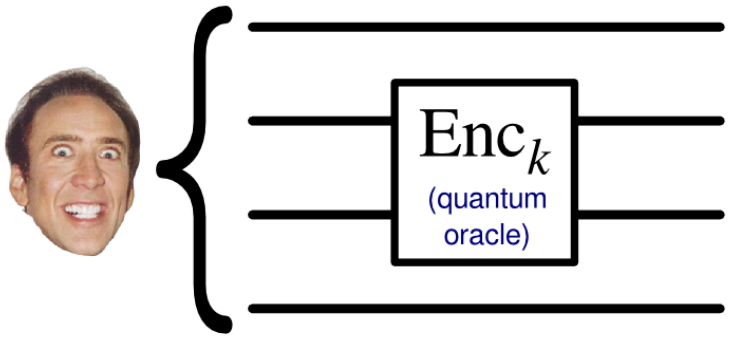
(only focus on qIND- phase, but also assume a -qCPA phase)

For fqIND-qCPA many assumptions were implicitly made. In our work, we explore every option: 'security tree' of definitions:

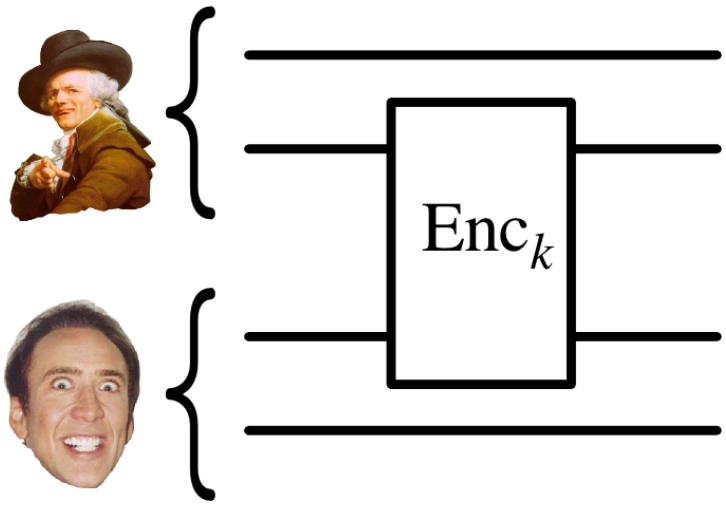


Model: $\mathcal{O}$ vs. $\mathcal{C}$

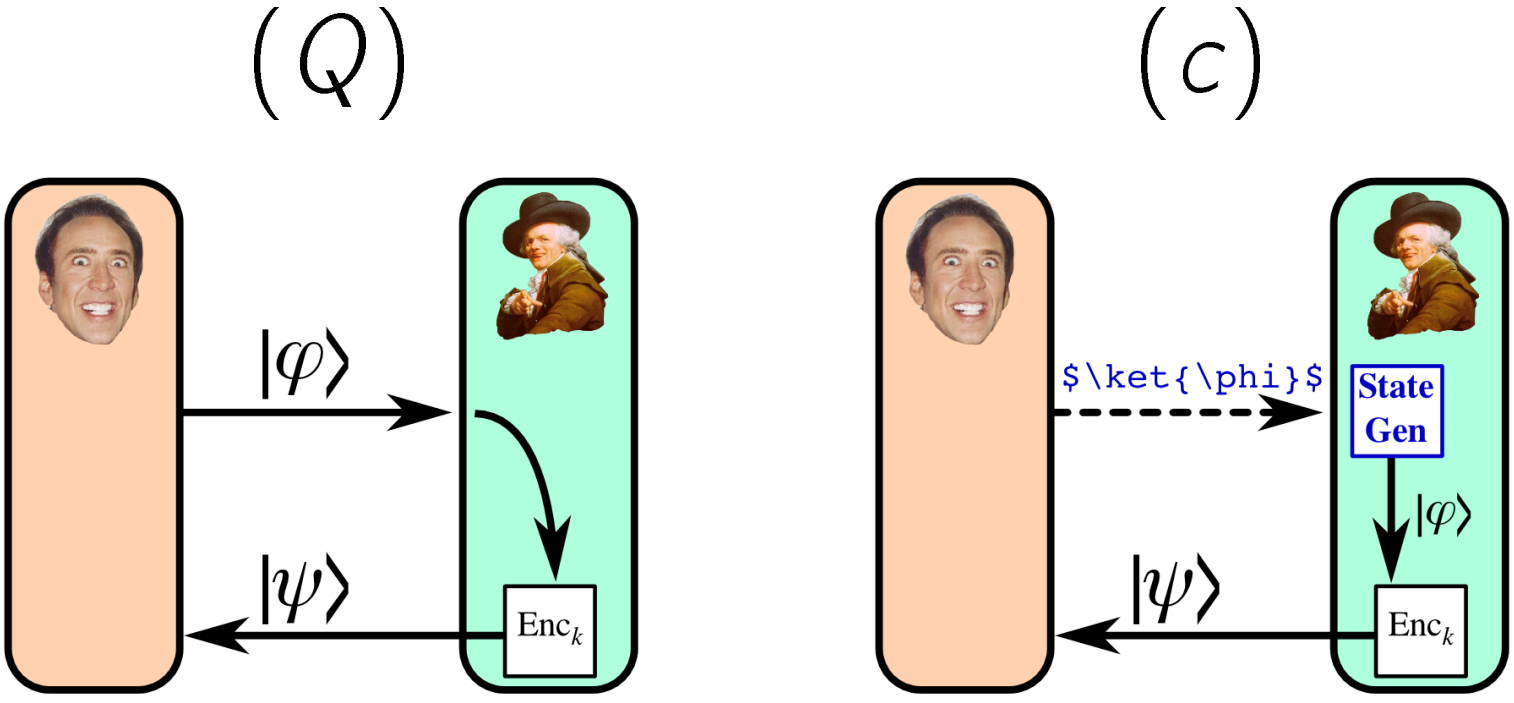
$(\mathcal{O})$



$(\mathcal{C})$

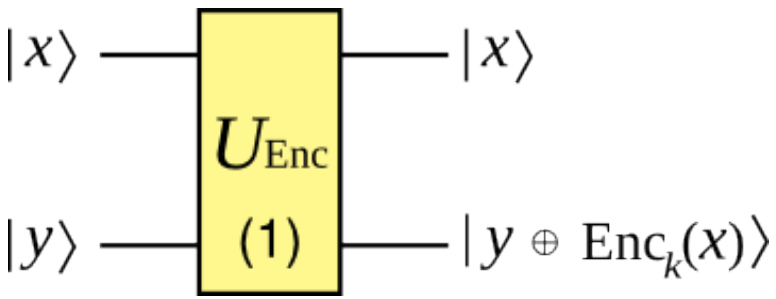


Model: Q vs. c

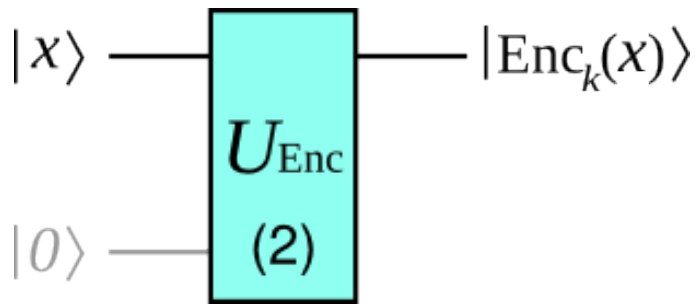

(Q)
(c)
$|\varphi\rangle$
$|\psi\rangle$
Enc_k
$\ket{\phi}$
State Gen
$|\varphi\rangle$
$|\psi\rangle$
Enc_k

Model: Type-1 vs. Type-2 Transformations

(1)



(2)



Quantum Indistinguishability

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

Quantum Indistinguishability

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

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

$$|\phi_0\rangle = \sum_{x,0} \alpha_{x,0} |x\rangle, \qquad |\phi_1\rangle = \sum_{x,1} \alpha_{x,1} |x\rangle$$

Quantum Indistinguishability

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

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

$$|\phi_0\rangle = \sum_{x,0} \alpha_{x,0} |x\rangle, \qquad |\phi_1\rangle = \sum_{x,1} \alpha_{x,1} |x\rangle$$

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

Quantum Indistinguishability

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

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

$$|\phi_0\rangle = \sum_{x,0} \alpha_{x,0} |x\rangle, \qquad |\phi_1\rangle = \sum_{x,1} \alpha_{x,1} |x\rangle$$

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

$$|\psi\rangle = U^{(2)}_{Enc} |\phi_b\rangle = \sum_{x,b} \alpha_{x,b} |\mathsf{Enc}_k(x)\rangle,$$

Quantum Indistinguishability

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

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

$$|\phi_0\rangle = \sum_{x,0} \alpha_{x,0} |x\rangle, \qquad |\phi_1\rangle = \sum_{x,1} \alpha_{x,1} |x\rangle$$

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

$$|\psi\rangle = U^{(2)}_{Enc} |\phi_b\rangle = \sum_{x,b} \alpha_{x,b} |\mathsf{Enc}_k(x)\rangle,$$

and finally sends ciphertext state $|\psi\rangle$ to $\mathcal{A}$.

Quantum Indistinguishability

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

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

$$|\phi_0\rangle = \sum_{x,0} \alpha_{x,0} |x\rangle, \qquad |\phi_1\rangle = \sum_{x,1} \alpha_{x,1} |x\rangle$$

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

$$|\psi\rangle = U_{Enc}^{(2)} |\phi_b\rangle = \sum_{x,b} \alpha_{x,b} |\mathsf{Enc}_k(x)\rangle,$$

and finally sends ciphertext state $|\psi\rangle$ to $\mathcal{A}$.

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

Quantum Indistinguishability

Quantum Indistinguishability (qIND)

For any QPPT adversary $\mathcal{A}$ and any $|\phi_0\rangle, |\phi_2\rangle$ with efficient classical representations:

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

where $|\psi\rangle = U_{Enc}^{(2)} |\phi_b\rangle$, and $b \xleftarrow{\$} \{0,1\}$.

Quantum Indistinguishability

Quantum Indistinguishability (qIND)

For any QPPT adversary $\mathcal{A}$ and any $|\phi_0\rangle, |\phi_2\rangle$ with efficient classical representations:

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

where $|\psi\rangle = U_{Enc}^{(2)} |\phi_b\rangle$, 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.

Quantum Indistinguishability

Quantum Indistinguishability (qIND)

For any QPPT adversary $\mathcal{A}$ and any $|\phi_0\rangle, |\phi_2\rangle$ with efficient classical representations:

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

where $|\psi\rangle = U_{Enc}^{(2)} |\phi_b\rangle$, 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.

what about quantum semantic security?

Quantum Semantic Security

Classical Semantic Security under qCPA (SEM-qCPA)

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

Quantum Semantic Security

Classical Semantic Security under qCPA (SEM-qCPA)

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

Theorem

IND-qCPA $\iff$ SEM-qCPA.

Quantum Semantic Security

Classical Semantic Security under qCPA (SEM-qCPA)

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

Theorem

IND-qCPA $\iff$ SEM-qCPA.

BOOOOORING...

Quantum Semantic Security

Classical Semantic Security under qCPA (SEM-qCPA)

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

Theorem

IND-qCPA $\iff$ SEM-qCPA.

Proof Idea:

'$\Rightarrow$': provide $\mathcal{S}$ with $\mathcal{A}$'s code through h, impersonate $\mathcal{C}$ and use IND to argue same prob.

'$\Leftarrow$': assume distinguisher $\mathcal{A}$, choose constant h, then no $\mathcal{S}$ can infere anything w/o ciphertext.

BOOOOORING...

Quantum Semantic Security

qSEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

Quantum Semantic Security

qSEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a distribution X of classical descriptions of quantum states,

Quantum Semantic Security

qSEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a distribution X of classical descriptions of quantum states,
- a classical advice function $h : \mathcal{M} \to \mathbb{N}$,

Quantum Semantic Security

qSEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a distribution X of classical descriptions of quantum states,
- a classical advice function $h : \mathcal{M} \to \mathbb{N}$,
- a classical target function $f : \mathcal{M} \to \mathbb{N}$.

Quantum Semantic Security

qSEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a distribution X of classical descriptions of quantum states,
- a classical advice function $h : \mathcal{M} \to \mathbb{N}$,
- a classical target function $f : \mathcal{M} \to \mathbb{N}$.

$\mathcal{C}$ samples two copies of $|\phi\rangle \leftarrow X$;

Quantum Semantic Security

qSEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a distribution X of classical descriptions of quantum states,
- a classical advice function $h : \mathcal{M} \to \mathbb{N}$,
- a classical target function $f : \mathcal{M} \to \mathbb{N}$.

$\mathcal{C}$ samples two copies of $|\phi\rangle \leftarrow X$;

- the first copy gets encrypted to $|\psi\rangle = U_{\mathsf{Enc}} |\phi\rangle$,

Quantum Semantic Security

qSEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a distribution X of classical descriptions of quantum states,
- a classical advice function $h : \mathcal{M} \to \mathbb{N}$,
- a classical target function $f : \mathcal{M} \to \mathbb{N}$.

$\mathcal{C}$ samples two copies of $|\phi\rangle \leftarrow X$;

- the first copy gets encrypted to $|\psi\rangle = U_{\mathsf{Enc}} |\phi\rangle$,
- the second copy is used to compute the Type-(1) operator $U_h^{(1)} : |x, 0\rangle \mapsto |x, h(x)\rangle$, which is then traced out on the first register obtaining advice state ρ_h.

Quantum Semantic Security

qSEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a distribution X of classical descriptions of quantum states,
- a classical advice function $h : \mathcal{M} \to \mathbb{N}$,
- a classical target function $f : \mathcal{M} \to \mathbb{N}$.

$\mathcal{C}$ samples two copies of $|\phi\rangle \leftarrow X$;

- the first copy gets encrypted to $|\psi\rangle = U_{\mathsf{Enc}} |\phi\rangle$,
- the second copy is used to compute the Type-(1) operator $U_h^{(1)} : |x, 0\rangle \mapsto |x, h(x)\rangle$, which is then traced out on the first register obtaining advice state ρ_h.

$\mathcal{C}$ sends back $(|\psi\rangle, \rho_h)$ to $\mathcal{A}$

Quantum Semantic Security

qSEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a distribution X of classical descriptions of quantum states,
- a classical advice function $h : \mathcal{M} \to \mathbb{N}$,
- a classical target function $f : \mathcal{M} \to \mathbb{N}$.

$\mathcal{C}$ samples two copies of $|\phi\rangle \leftarrow X$;

- the first copy gets encrypted to $|\psi\rangle = U_{\mathsf{Enc}} |\phi\rangle$,
- the second copy is used to compute the Type-(1) operator $U_h^{(1)} : |x, 0\rangle \mapsto |x, h(x)\rangle$, which is then traced out on the first register obtaining advice state ρ_h.

$\mathcal{C}$ sends back $(|\psi\rangle, \rho_h)$ to $\mathcal{A}$; but $\mathcal{S}$ only gets ρ_h.

Quantum Semantic Security

qSEM challenge query: $\mathcal{A}$ sends $\mathcal{C}$ challenge template:

- a distribution X of classical descriptions of quantum states,
- a classical advice function $h : \mathcal{M} \to \mathbb{N}$,
- a classical target function $f : \mathcal{M} \to \mathbb{N}$.

$\mathcal{C}$ samples two copies of $|\phi\rangle \leftarrow X$;

- the first copy gets encrypted to $|\psi\rangle = U_{\mathsf{Enc}} |\phi\rangle$,
- the second copy is used to compute the Type-(1) operator $U_h^{(1)} : |x, 0\rangle \mapsto |x, h(x)\rangle$, which is then traced out on the first register obtaining advice state ρ_h.

$\mathcal{C}$ sends back $(|\psi\rangle, \rho_h)$ to $\mathcal{A}$; but $\mathcal{S}$ only gets ρ_h.

Goal is to compute $U_f^{(1)} |\phi\rangle$ (where $U_f^{(1)} : |x, 0\rangle \mapsto |x, f(x)\rangle$) with good ϵ-approximation (in terms of *trace distance*).

Quantum Semantic Security

Quantum Semantic Security (qSEM)

For any efficient quantum adversary $\mathcal{A}$ and any small ϵ, there exists an efficient quantum simulator $\mathcal{S}$ such that:

$$|\Pr[\mathcal{A}(|\psi\rangle, \rho_h) \text{ wins qSEM }] - \Pr[\mathcal{S}(\rho_h) \text{ wins qSEM }]| \leq \text{negl}(n)$$

Quantum Semantic Security

Quantum Semantic Security (qSEM)

For any efficient quantum adversary $\mathcal{A}$ and any small ϵ, there exists an efficient quantum simulator $\mathcal{S}$ such that:

$$|\Pr[\mathcal{A}(|\psi\rangle, \rho_h) \text{ wins qSEM }] - \Pr[\mathcal{S}(\rho_h) \text{ wins qSEM }]| \leq \text{negl}(n)$$

Quantum Semantic Security under qCPA (qSEM-qCPA)

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

Quantum Semantic Security

Quantum Semantic Security (qSEM)

For any efficient quantum adversary $\mathcal{A}$ and any small ϵ, there exists an efficient quantum simulator $\mathcal{S}$ such that:

$$|\Pr[\mathcal{A}(|\psi\rangle, \rho_h) \text{ wins qSEM }] - \Pr[\mathcal{S}(\rho_h) \text{ wins qSEM }]| \leq \text{negl}(n)$$

Quantum Semantic Security under qCPA (qSEM-qCPA)

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

Theorem

qIND-qCPA $\iff$ qSEM-qCPA.

Separation Example

Theorem

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

Separation Example

Theorem

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

Consider [Gol04][3] : sample $r \xleftarrow{\$} \mathcal{R}$ and use a PRF $f : \mathcal{K} \times \mathcal{R} \to \mathcal{M}$. Then: $\mathsf{Enc}_k(x) := (x \oplus f_k(r), r)$.

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

Separation Example

Theorem

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

Consider [Gol04][3] : 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.

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

Separation Example

Theorem

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

Consider [Gol04][3] : 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]

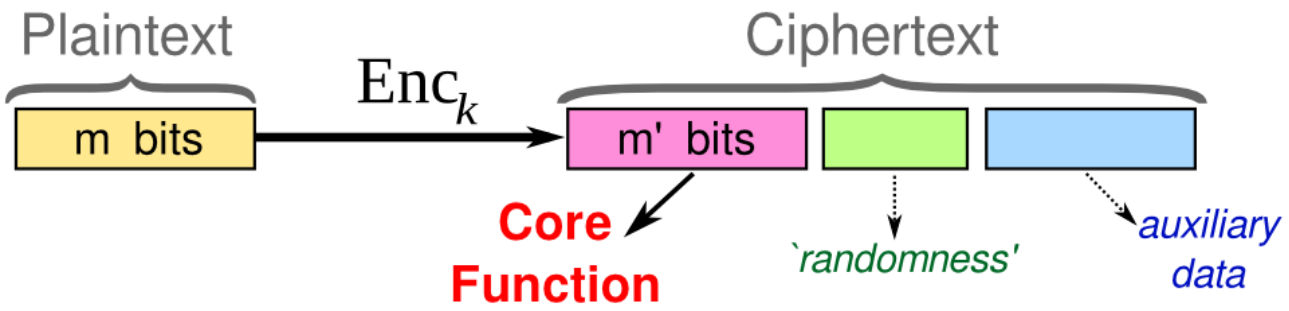
The Goldreich scheme is IND-qCPA secure, provided the PRF is quantum-secure.

Theorem

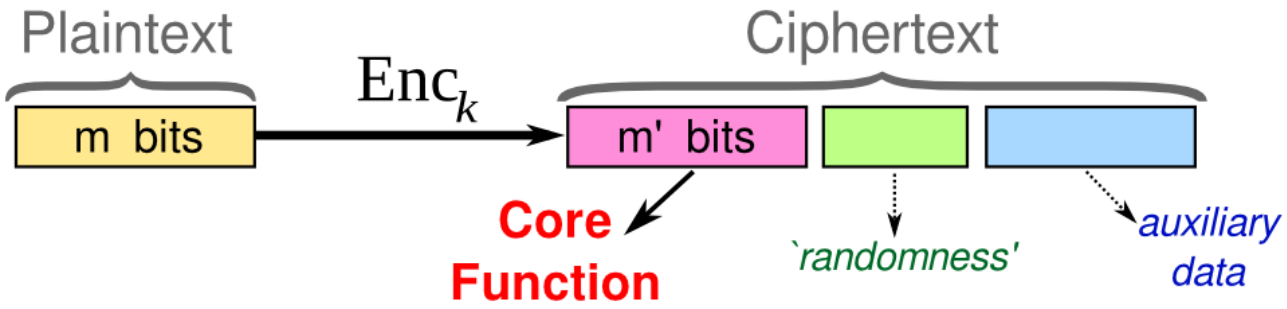
The Goldreich scheme is *not* qIND-qCPA secure.

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

Impossibility Result

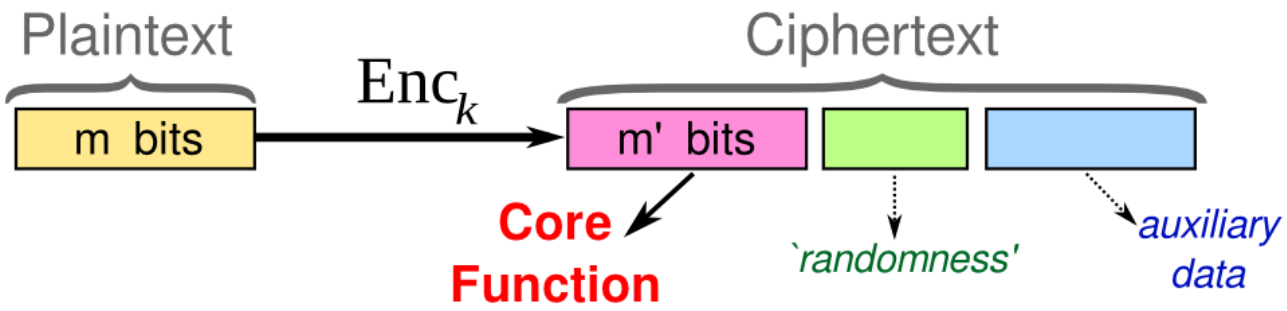


Impossibility Result



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

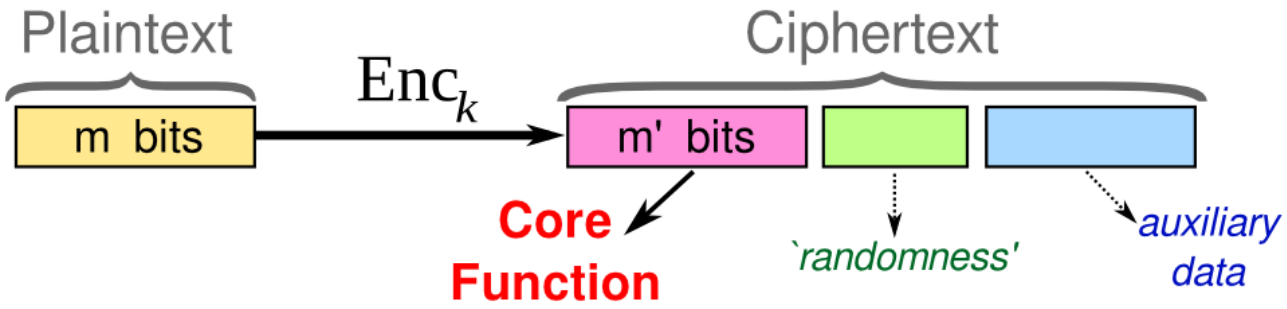
Impossibility Result



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

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

Impossibility Result



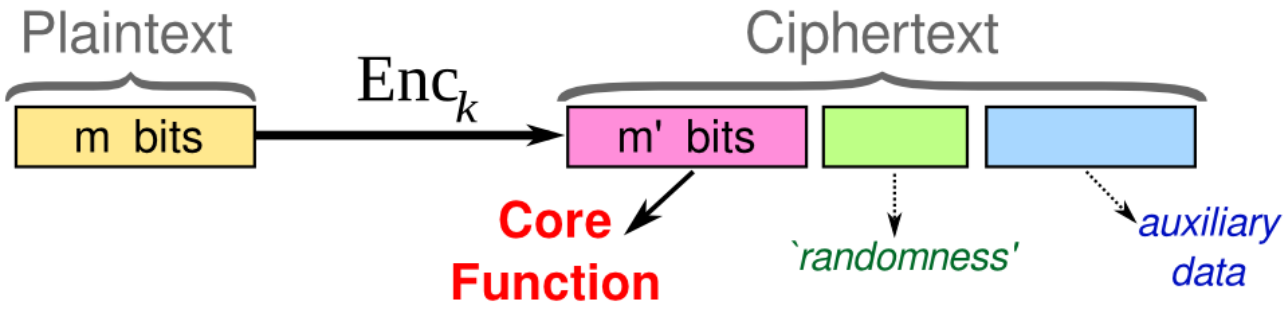
quasi–length-preserving (QLP): core function is bijective ($m = m'$).

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

Theorem

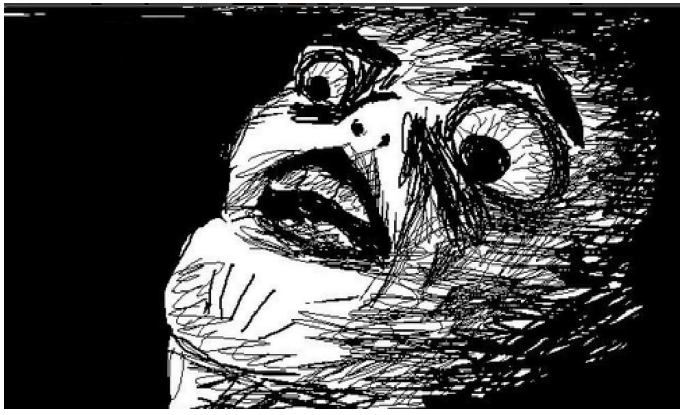
If a symmetric scheme is QLP, then it is *not* qIND-qCPA secure.

Impossibility Result



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

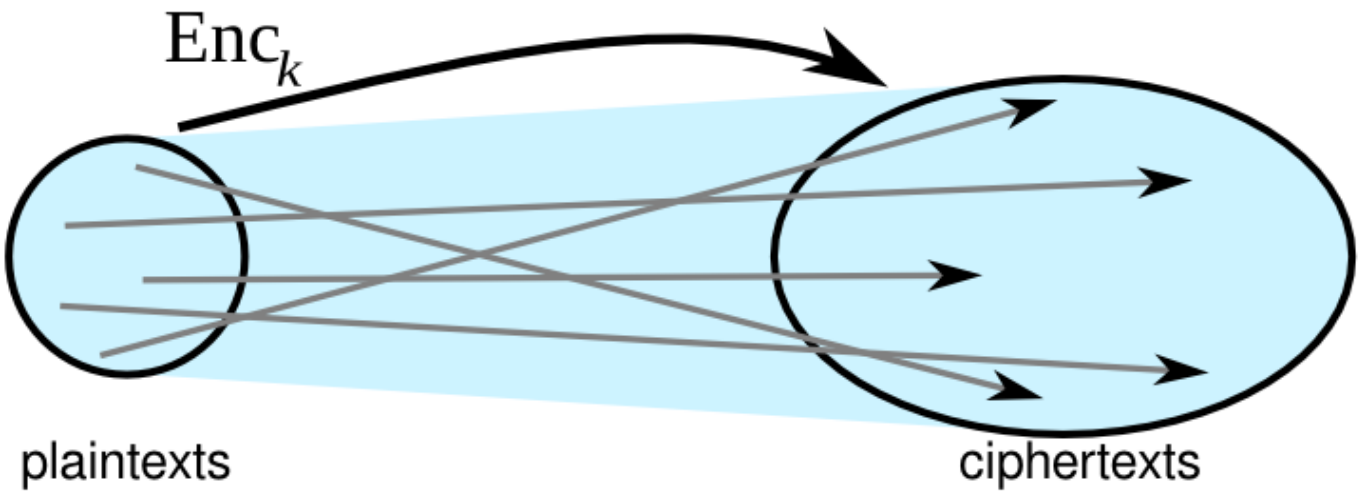
- Goldreich's scheme
- OTP
- ECB block ciphers
- stream ciphers



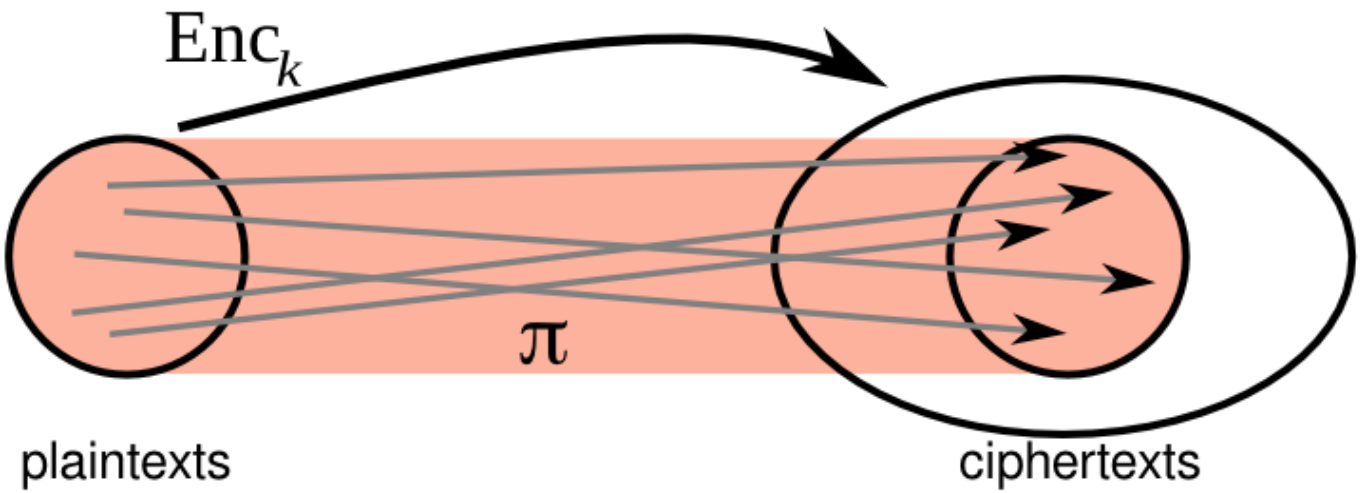
Theorem

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

The Attack



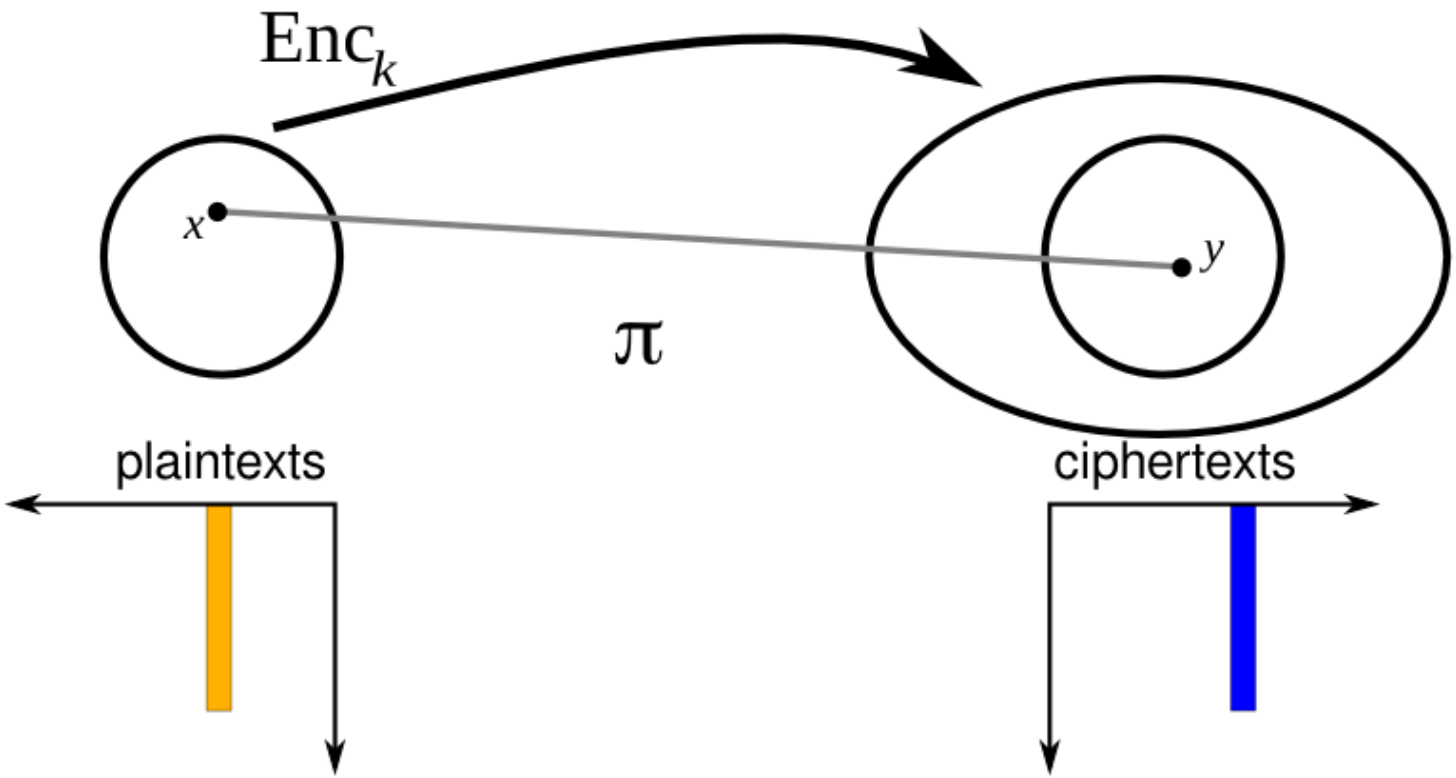
The Attack



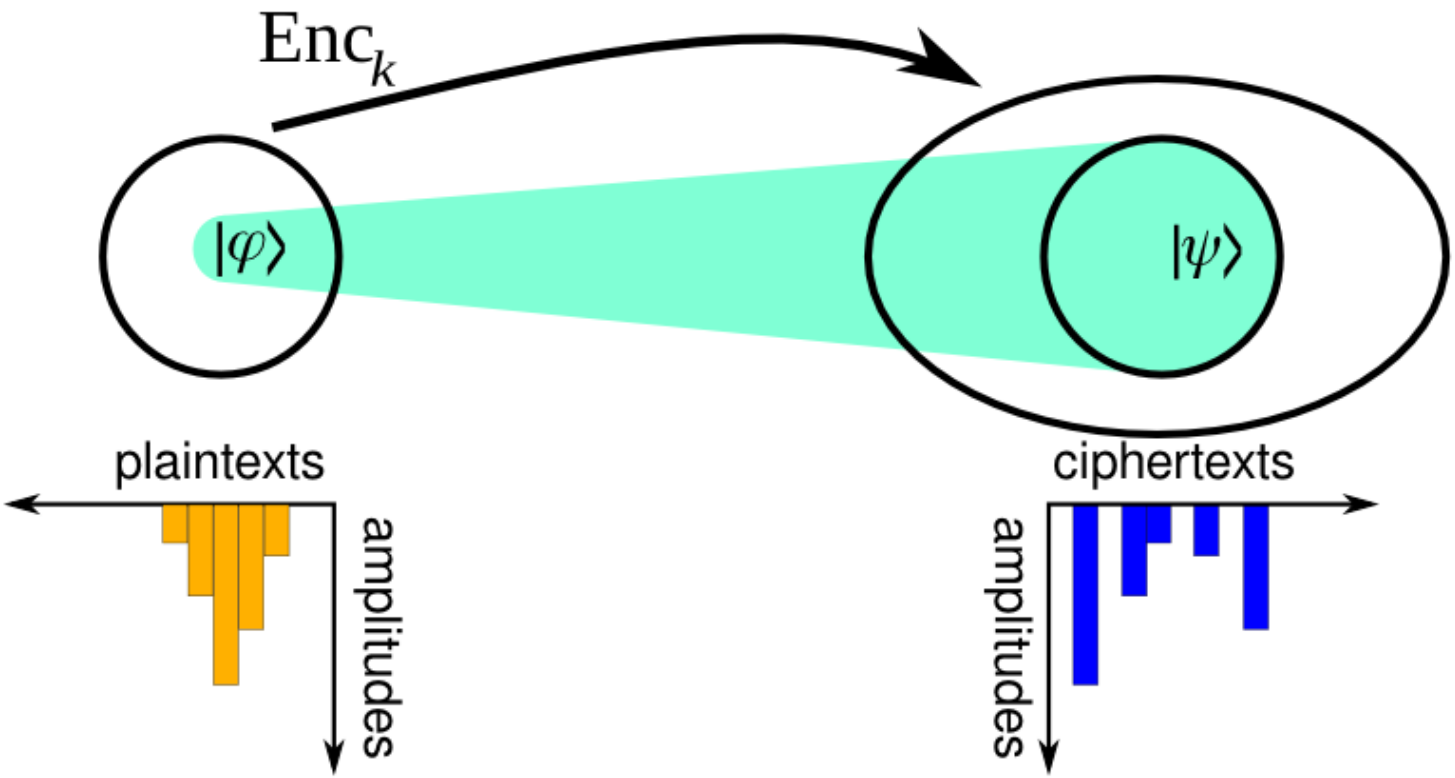
QLP cipher

Core Function = permutation π

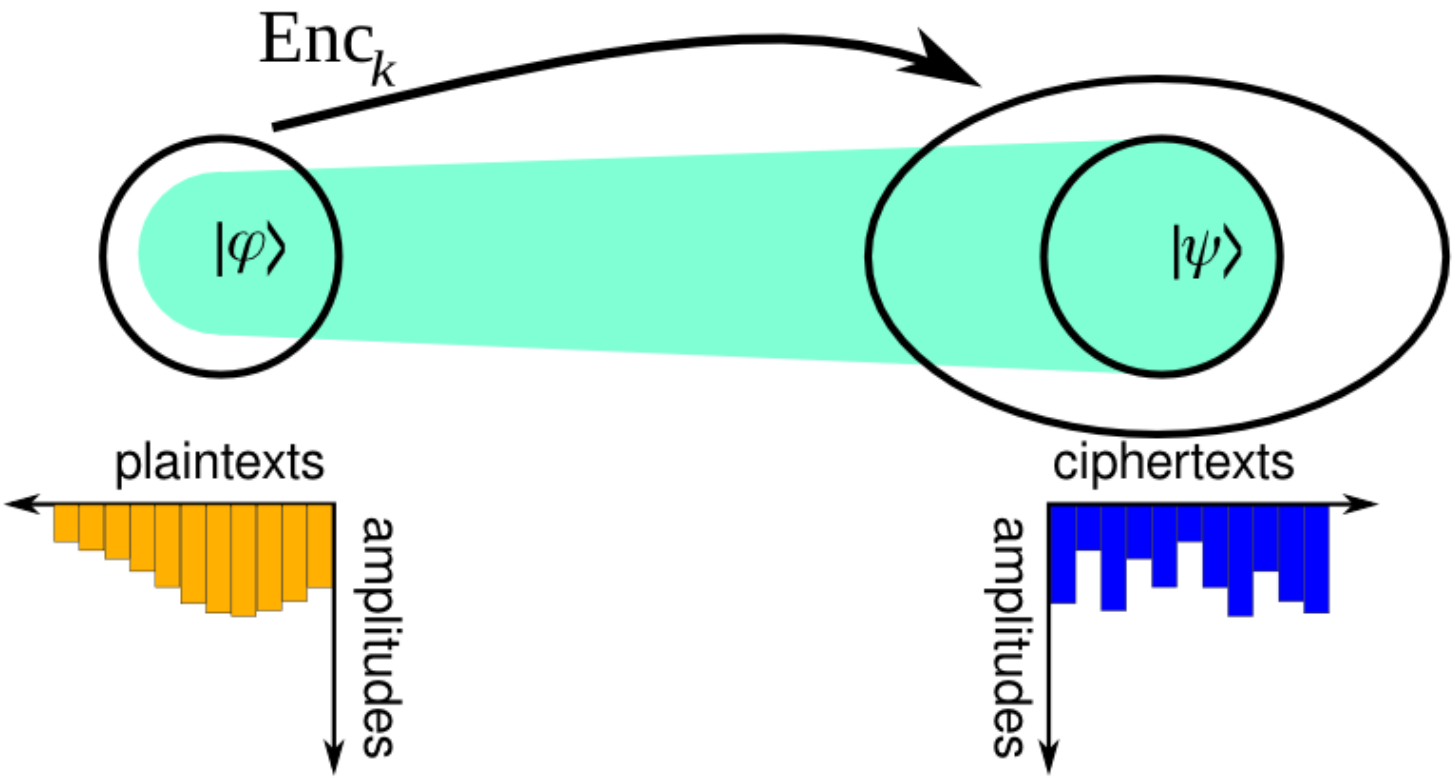
The Attack



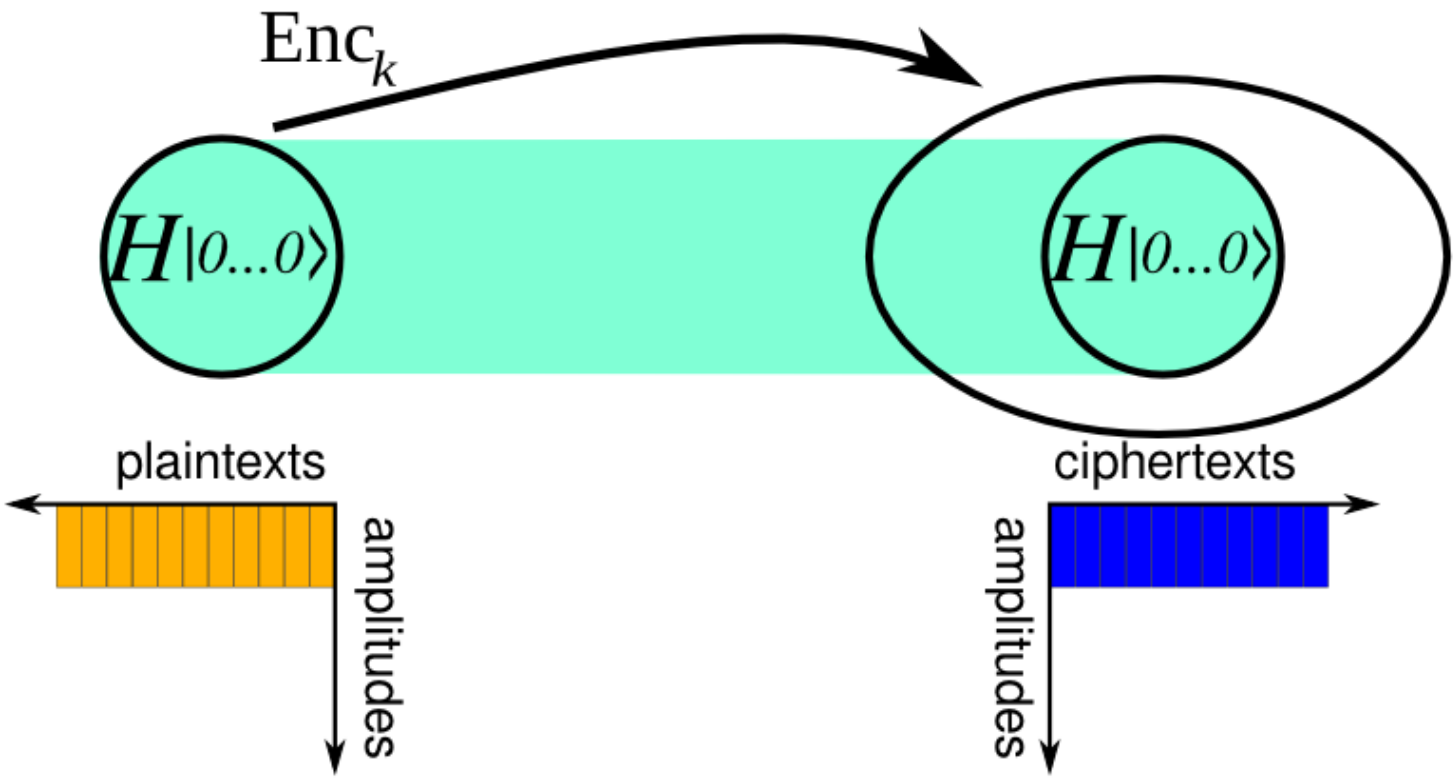
The Attack


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

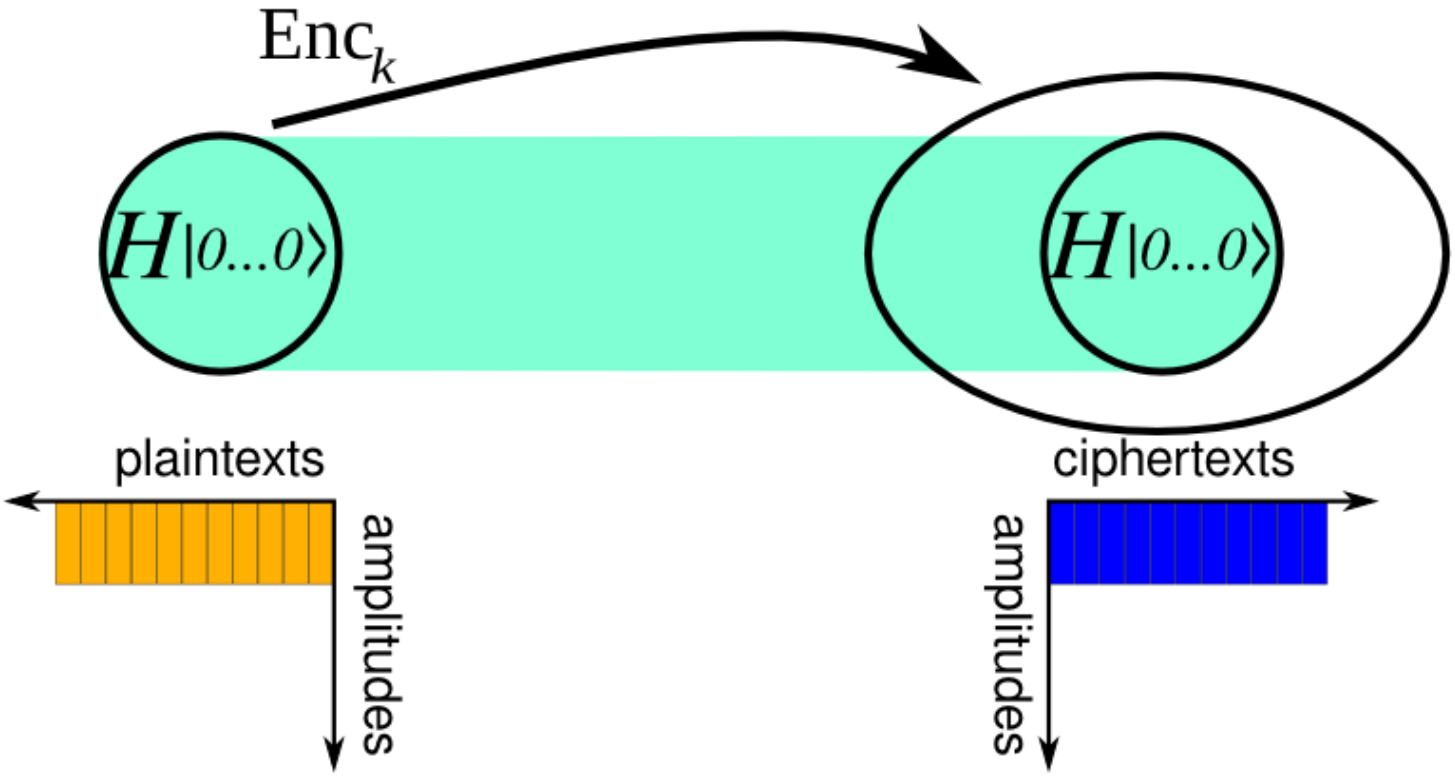
The Attack


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

The Attack


Enc_k
$H|0\ldots0\rangle$
$H|0\ldots0\rangle$
plaintexts
amplitudes
ciphertexts
amplitudes

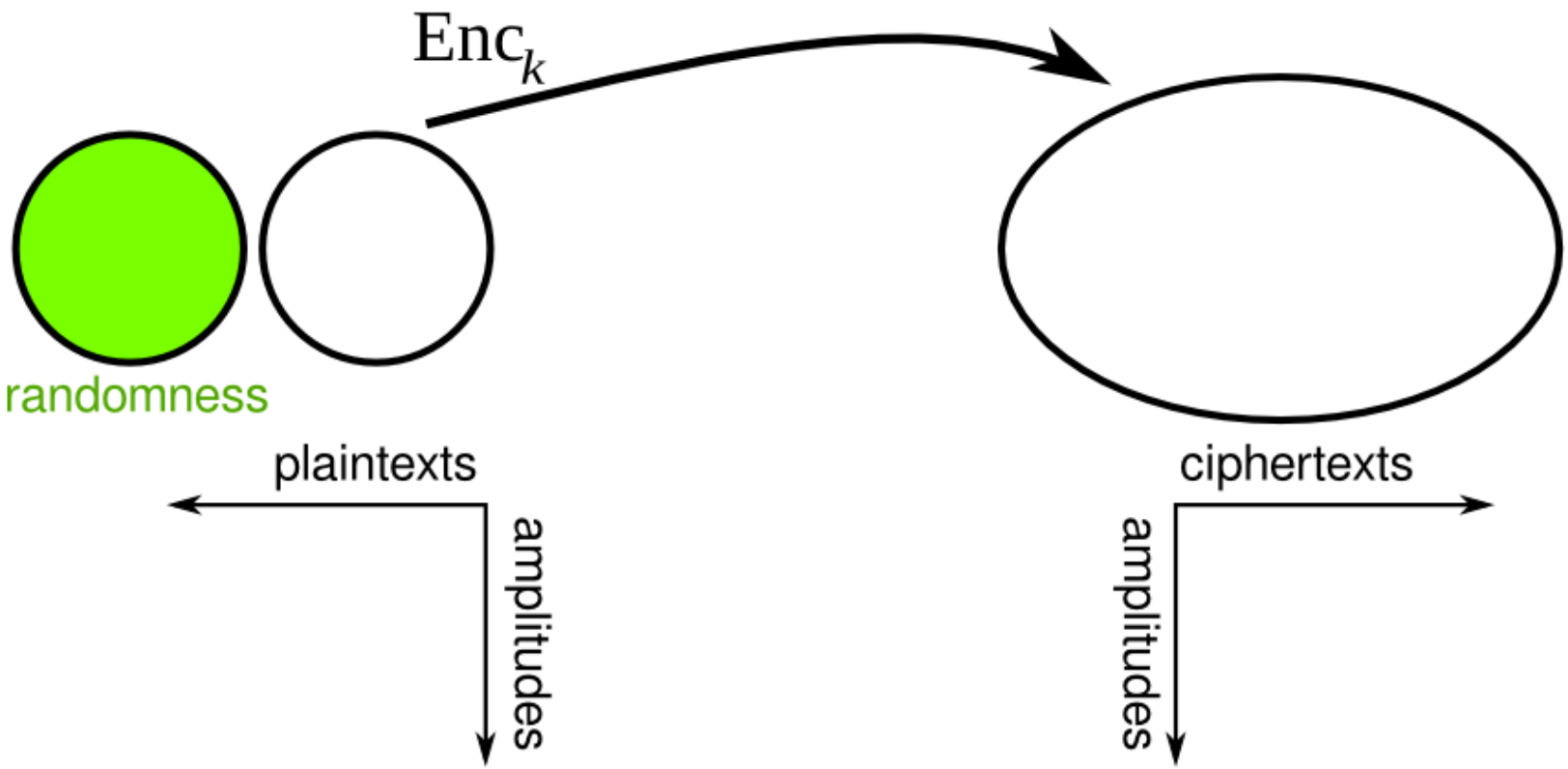
The Attack



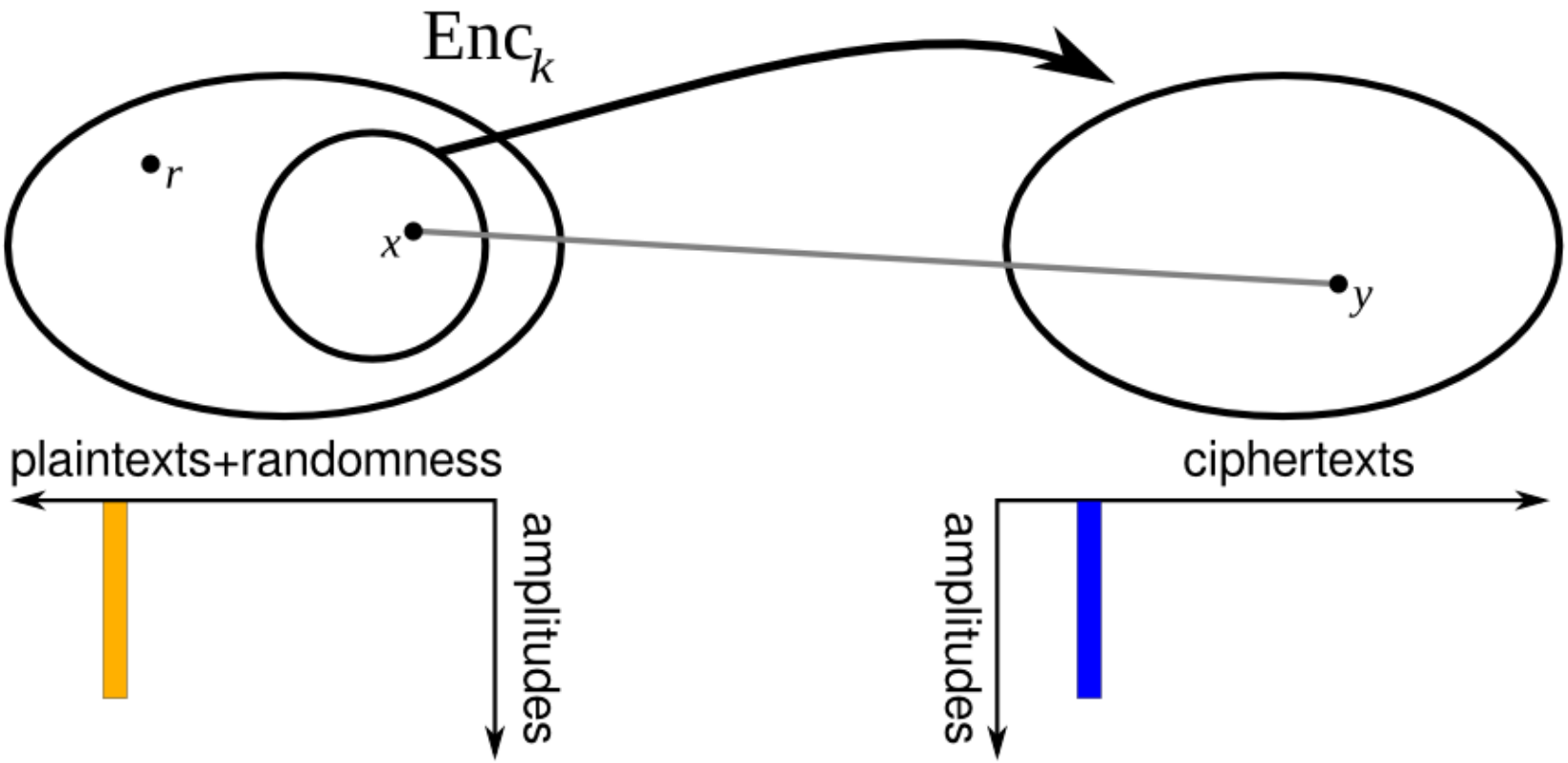
$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{\mathsf{Enc}_k} \frac{1}{\sqrt{2}}|\pi(0)\rangle + \frac{1}{\sqrt{2}}|\pi(1)\rangle = |+\rangle$$

Easy to distinguish!

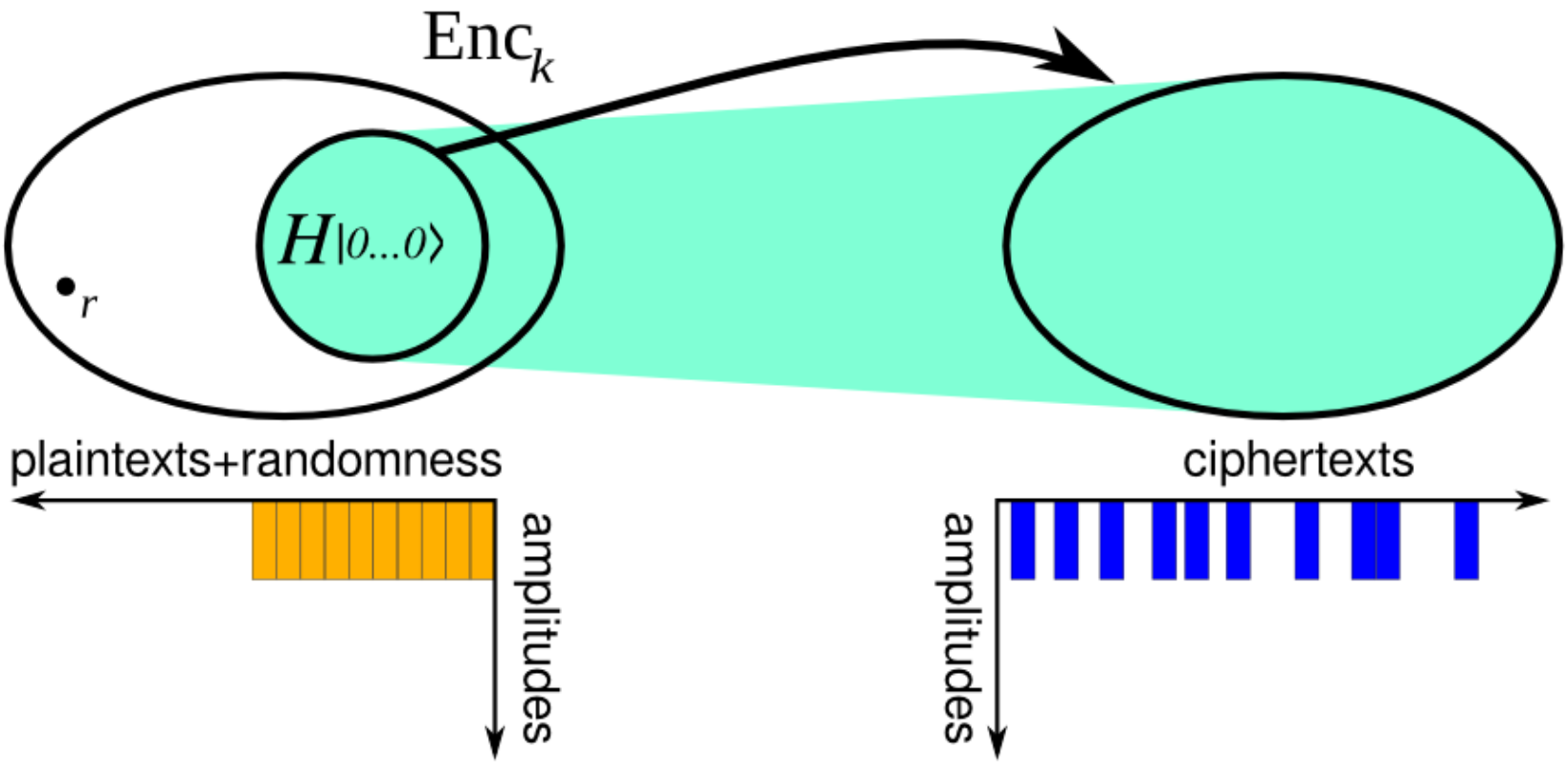
The Solution



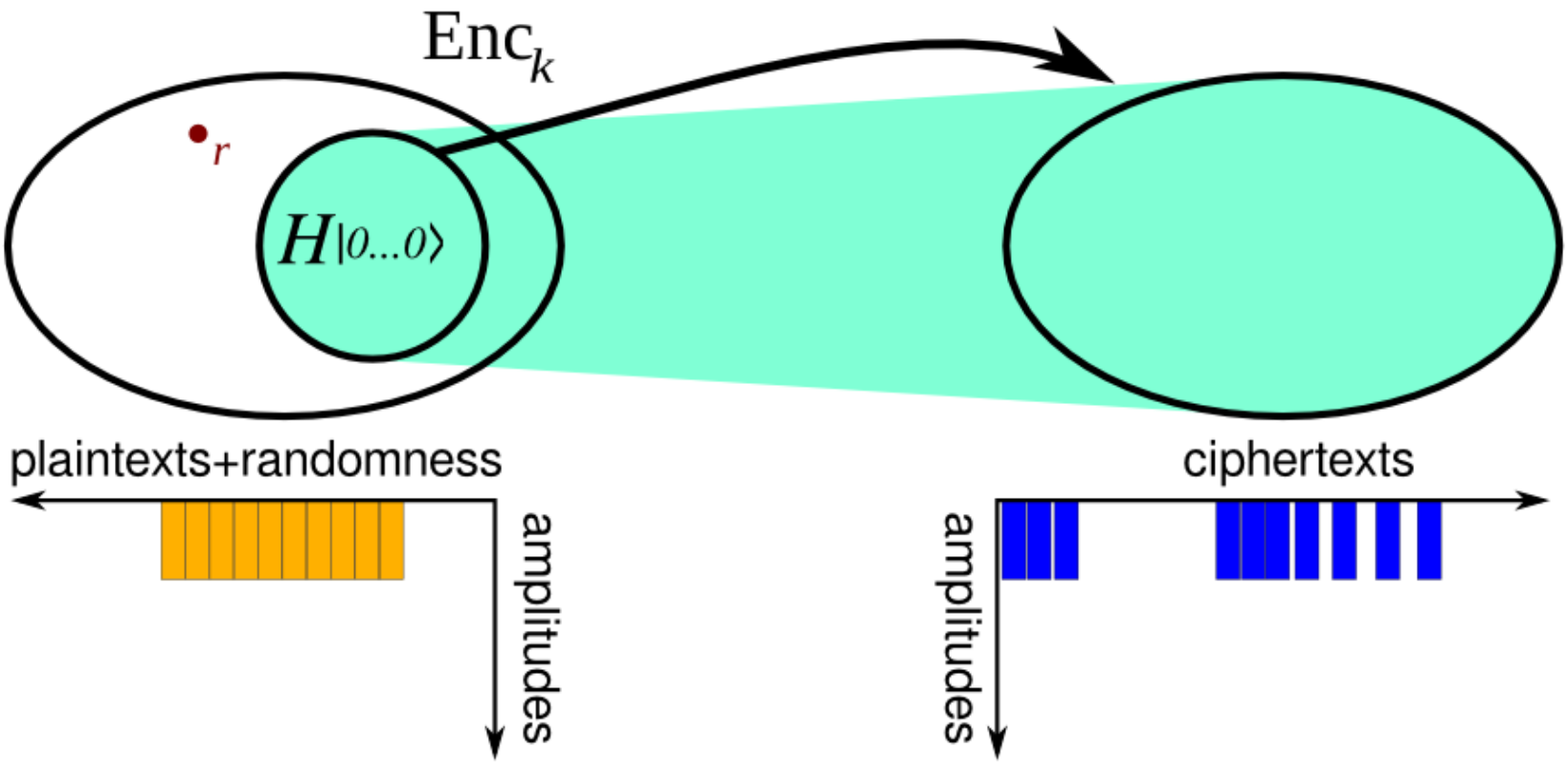
The Solution



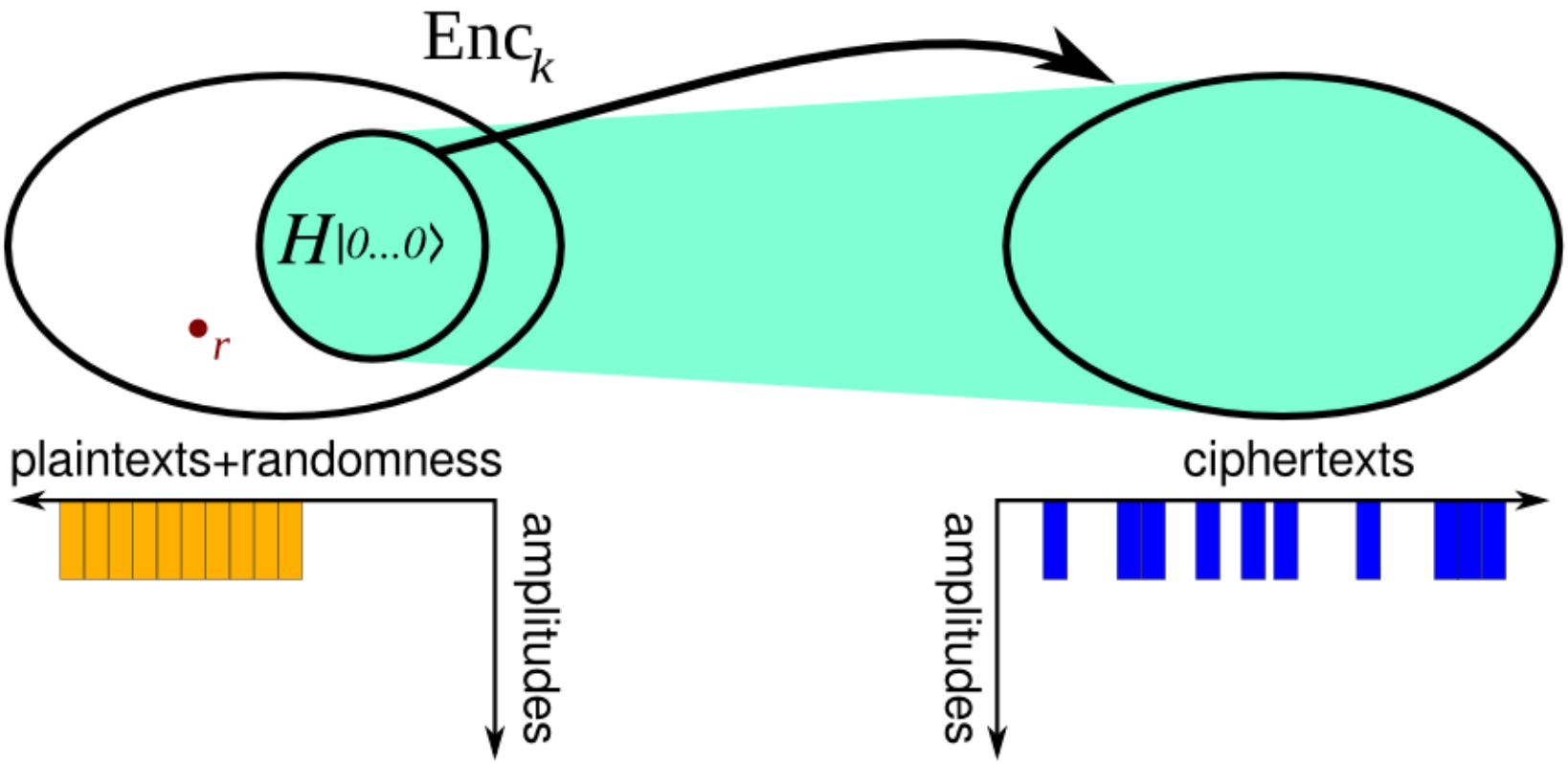
The Solution



The Solution



The Solution



Secure Construction

Π family of quantum-secure pseudorandom permutations (QPRP).

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 $\pi^{-1}(y)$.

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.

Secure Construction

Π family of quantum-secure pseudorandom permutations (QPRP).

Construction

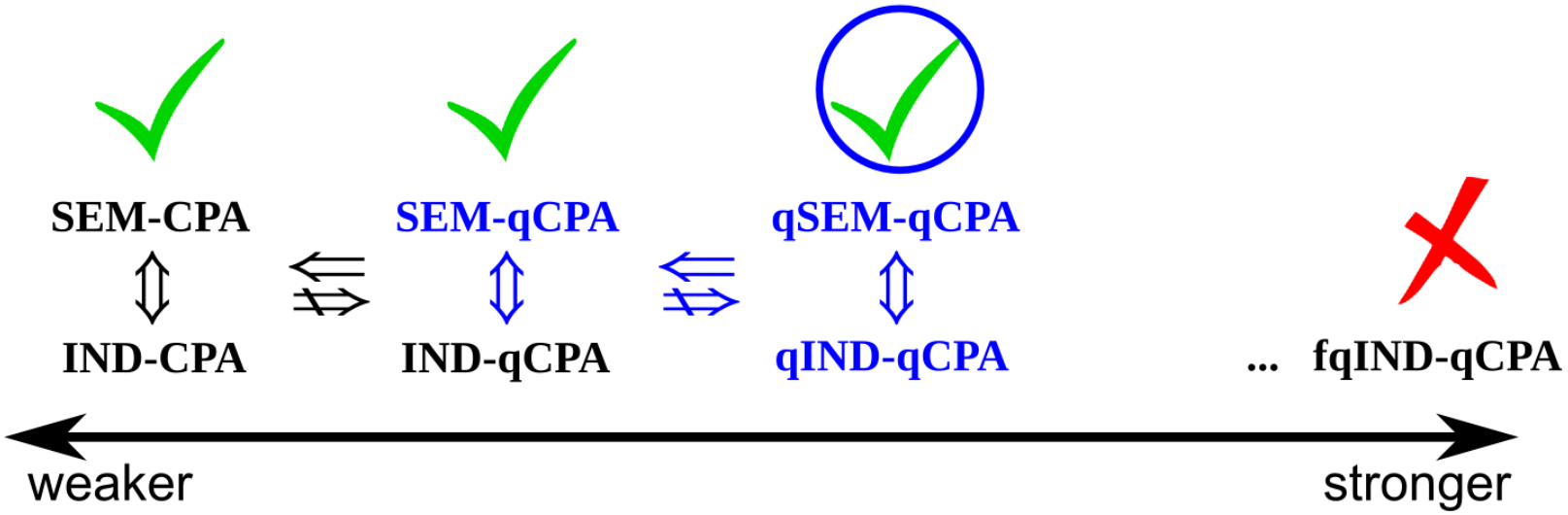
- Generate key: sample $(\pi, \pi^{-1}) \leftarrow \Pi$;
- Encrypt message x: pad with n bits of randomness r and set $y = \pi(r \| x)$;
- Decrypt y: truncate the first n bits of $\pi^{-1}(y)$.

Theorem

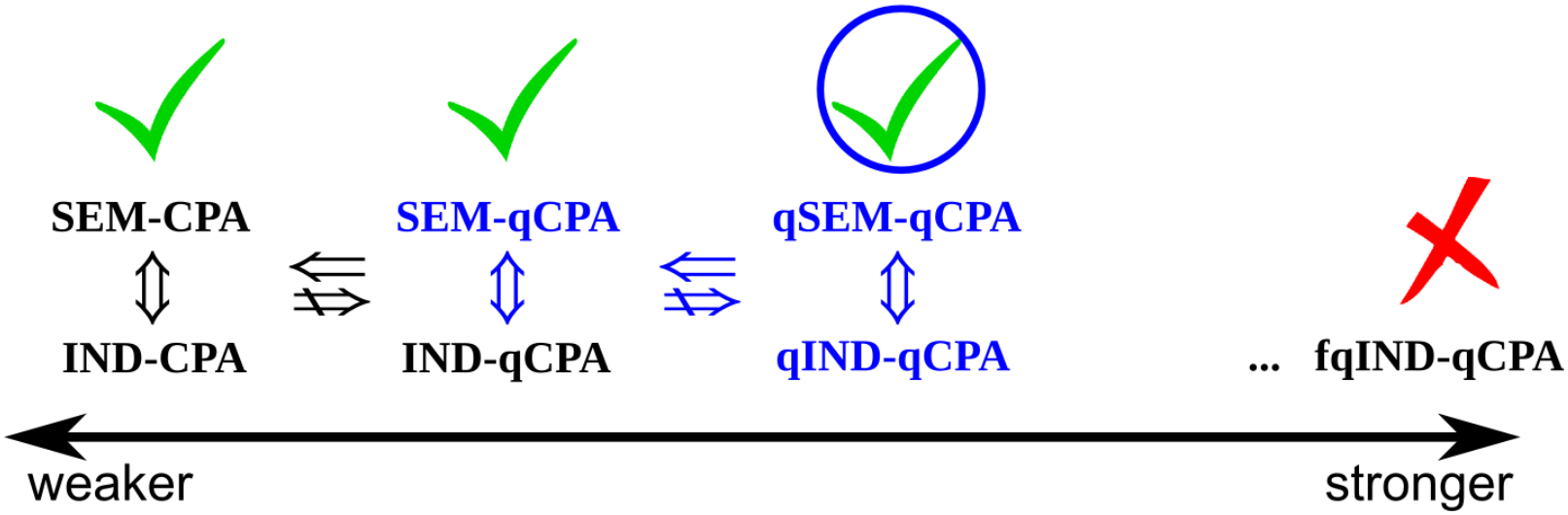
The above scheme is qIND-qCPA secure.

(Idea of proof: show that for every two plaintext states $|\phi_0\rangle, |\phi_1\rangle$, the trace distance of the states ρ_0, ρ_1 obtained by considering their encryption under a mixture of every possible key is negligible)

Conclusions



Conclusions



Future directions:

- public-key encryption;
- CCA security;
- slightly different models of qIND or qSEM;
- superposition of keys/randomness;
- patch IND-qCPA $\Rightarrow$ qIND-qCPA;
- 'fully' quantum scenario (ongoing work).

End of this talk

Thanks for your attention!

tommaso@gagliardoni.net

TECHNISCHE
UNIVERSITÄT
DARMSTADT

CASED

EC SPRIDE
EUROPEAN CENTER FOR
SECURITY AND PRIVACY BY DESIGN

Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

BZ Attack

(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:

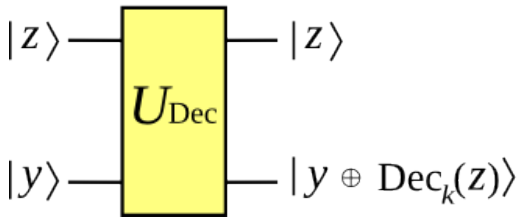
- if $b = 0$, the state becomes: $\sum_x |x, 0, \mathrm{Enc}(x)\rangle$ (notice entanglement between 1^{st} and 3^{rd} registers);
- if $b = 1$ instead, the state becomes: $\sum_x |x, 0, \mathrm{Enc}(0)\rangle = H|0\rangle \otimes |0\rangle \otimes |\mathrm{Enc}(0)\rangle$.

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

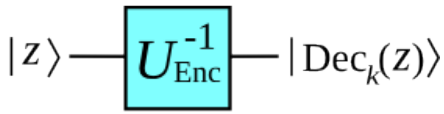
- if $b = 0$, the Hadamard maps the state to a complete mixture, and the measurement outcome is random;
- if $b = 1$ instead, the first register is: $H^2|0\rangle = |0\rangle$, and the outcome is 0.

Equivalence between Type-1 and Type-2

Type-1
Decryption Oracle

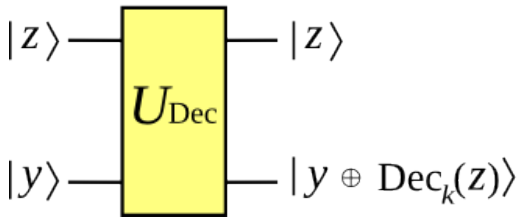


Type-2
Decryption Oracle

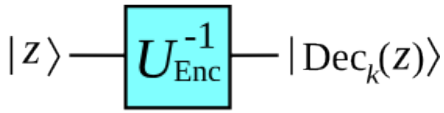


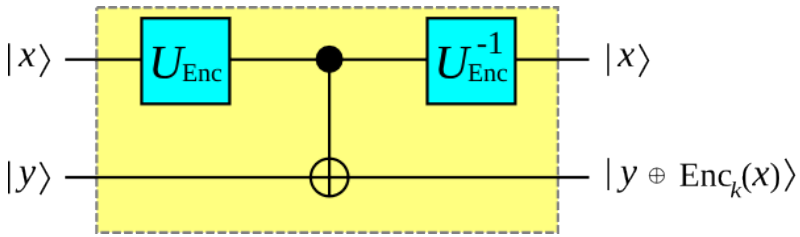
Equivalence between Type-1 and Type-2

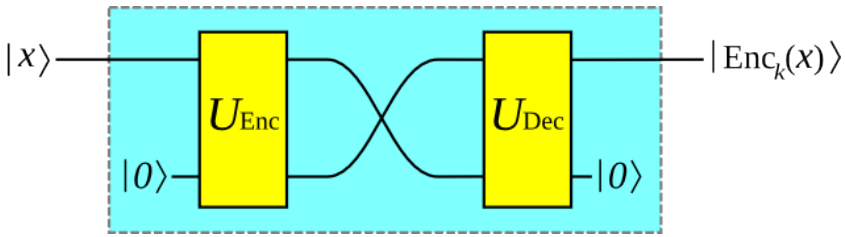
Type-1
Decryption Oracle



Type-2
Decryption Oracle







qSEM $\Rightarrow$ qIND

By contradiction: let $\mathcal{A}$ be an efficient qIND distinguisher. We show that there exists an efficient $\mathcal{A}'$ for qSEM which does not admit simulator.
$\mathcal{A}'$ invokes $\mathcal{A}$, which starts a qIND challenge query consisting of two classical descriptions s_0, s_1 of states $|\phi_0\rangle, |\phi_1\rangle$.
$\mathcal{A}'$ records this template, then prepare his own qSEM challenge template consisting of:

- as distribution X, the uniform distribution over $\{s_0, s_1\}$;
- as advice function h, a constant function (not depending on s_0, s_1);
- as target function f, the *identity function* $f(x) = x$.

$\mathcal{A}'$ receives $\mathcal{C}$'s response, forwards the ciphertext to $\mathcal{A}$, and observes output.
Since $\mathcal{A}$ recovers b with non-negligible probability, $\mathcal{A}'$ can then reconstruct the correct $|\phi_b\rangle$ (having recorded its description) and compute the output reduced state ρ_f.
Any simulator $\mathcal{S}$, on the other hand, only receives a constant function h, and then cannot do better than guessing.

qSEM $\Leftarrow$ qIND

Let $\mathcal{A}$ be any QPT adversary against qSEM. Then its circuit has a short classical representation ξ.

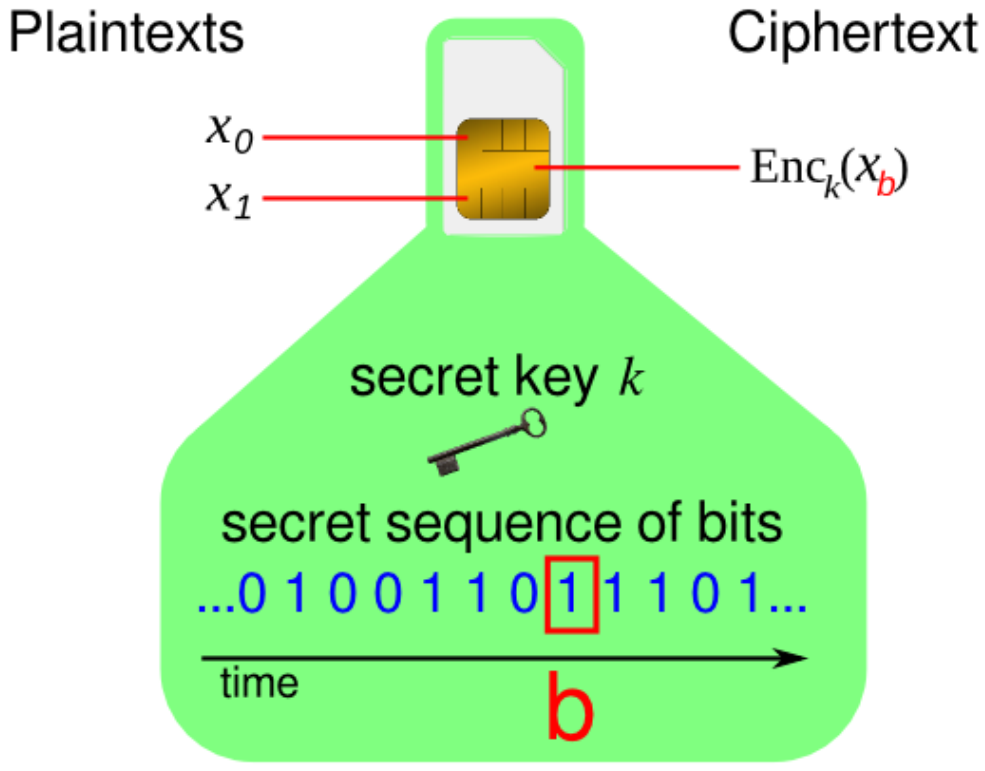
Then here is a simulator $\mathcal{S}$ with the same success probability:

1. $\mathcal{S}$ receives ξ as nonuniform advice (this is allowed);
2. then $\mathcal{S}$ implements and run $\mathcal{A}$ through ξ;
3. when $\mathcal{A}$ produces a qSEM challenge template (X, h, f), $\mathcal{S}$ forwards it to $\mathcal{C}$;
4. when $\mathcal{C}$ replies with its advice function, $\mathcal{S}$ forwards it to $\mathcal{A}$, together with the encryption of a bogus state;
5. finally, $\mathcal{S}$ outputs whatever $\mathcal{A}$ does.

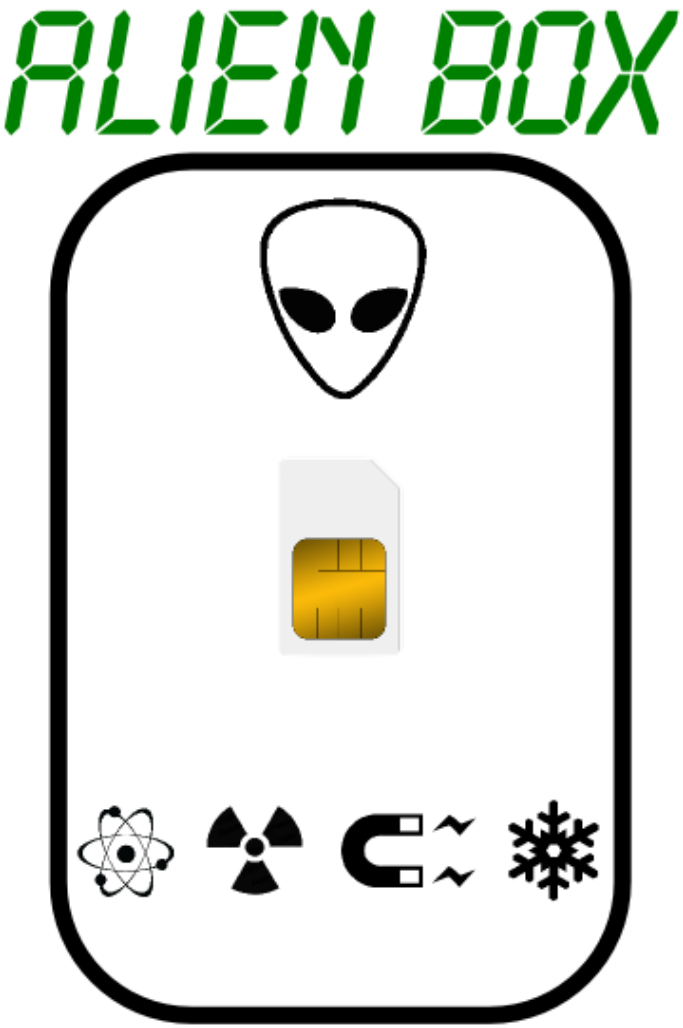
The presence of the bogus encryption state instead of the right one does not affect $\mathcal{A}$'s success probability. In fact, if this were the case, we could turn $\mathcal{S}$ into an efficient distinguisher against qIND.

The ‘Frozen Smartcard’ Example

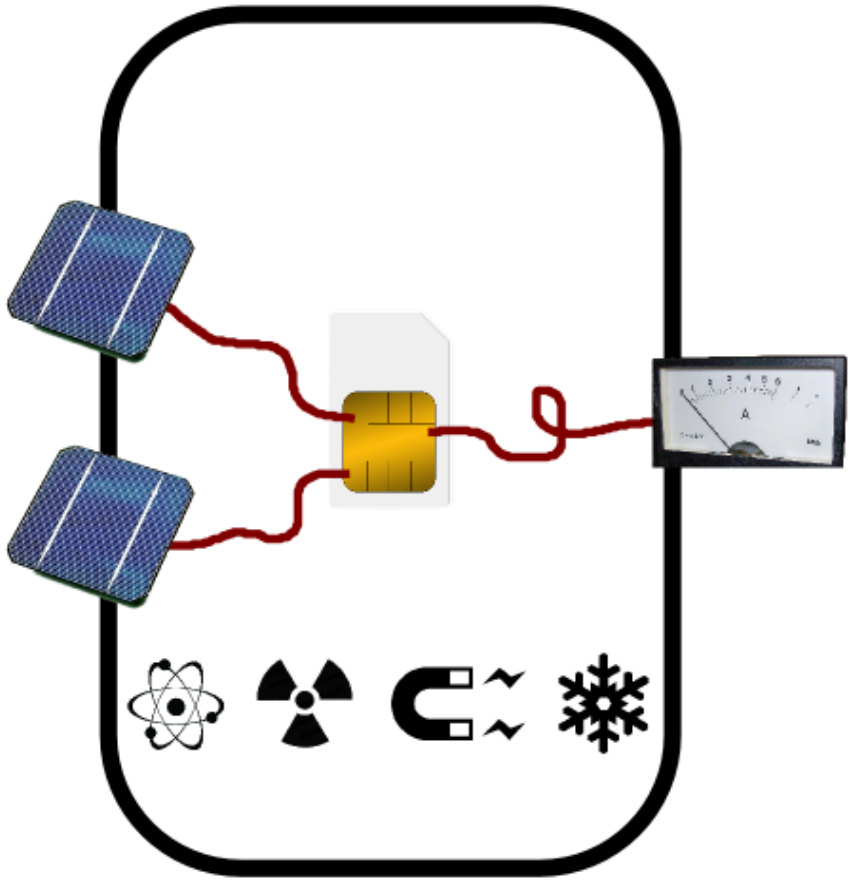
The 'Frozen Smartcard' Example



The ‘Frozen Smartcard’ Example



The ‘Frozen Smartcard’ Example



The ‘Frozen Smartcard’ Example