Security notions for symmetric encryptions against quantum adversaries

Gelo Noel Tabia

YRF-QIS20 | Hsinchu, Taiwan | 27 Aug 2020

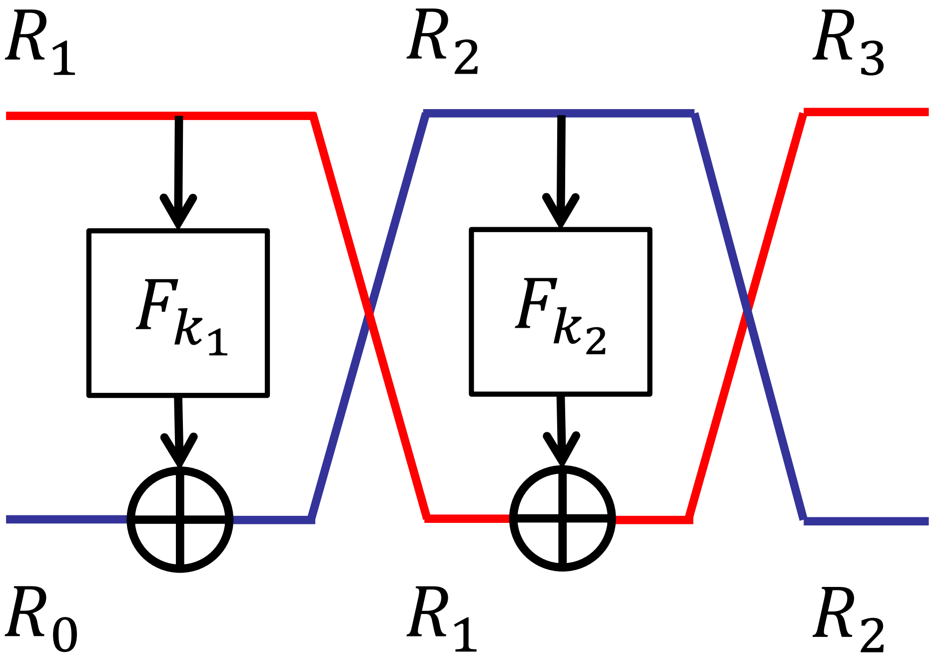
Motivation

Do symmetric ciphers remain secure if they can be accessed in superposition?

Feistel cipher

$m = (R_0, R_1)$

$c = (R_2, R_3)$



Overview

What is symmetric-key encryption

How do we define security for symmetric encryptions

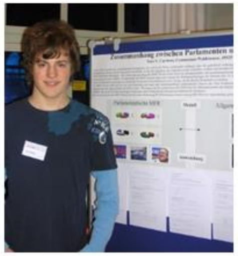
How do we extend these notions for quantum adversaries

joint work with

UNIVERSITY OF TARTU
Institute of Computer Science

Dominique Unruh

Ehsan Ehbrami



Tore Vincent Carstens

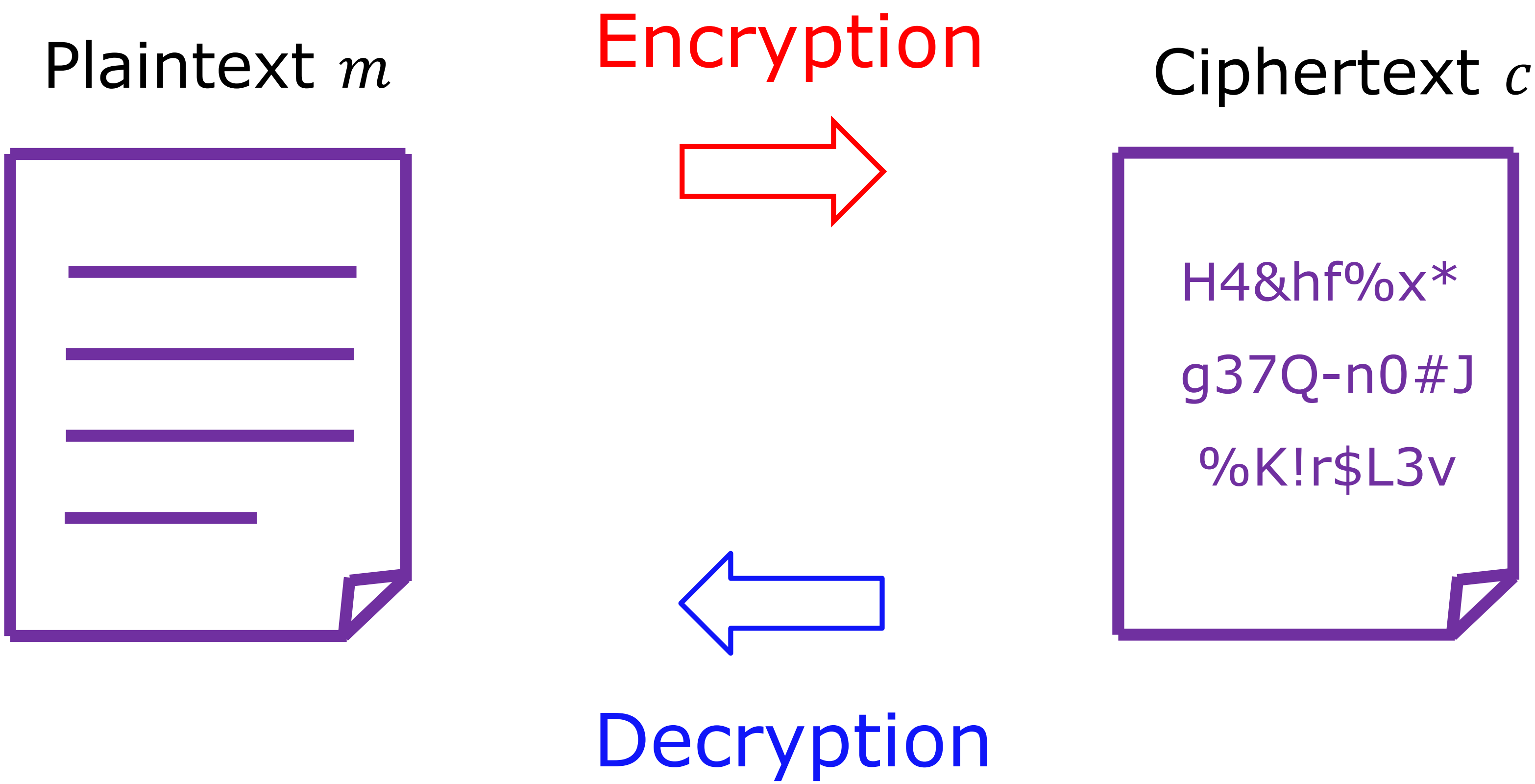
Our contributions

We describe 57 valid quantum notions grouped into 14 equivalent families.

We prove the various implications and separations among these families. (e.g., separation by set equality)

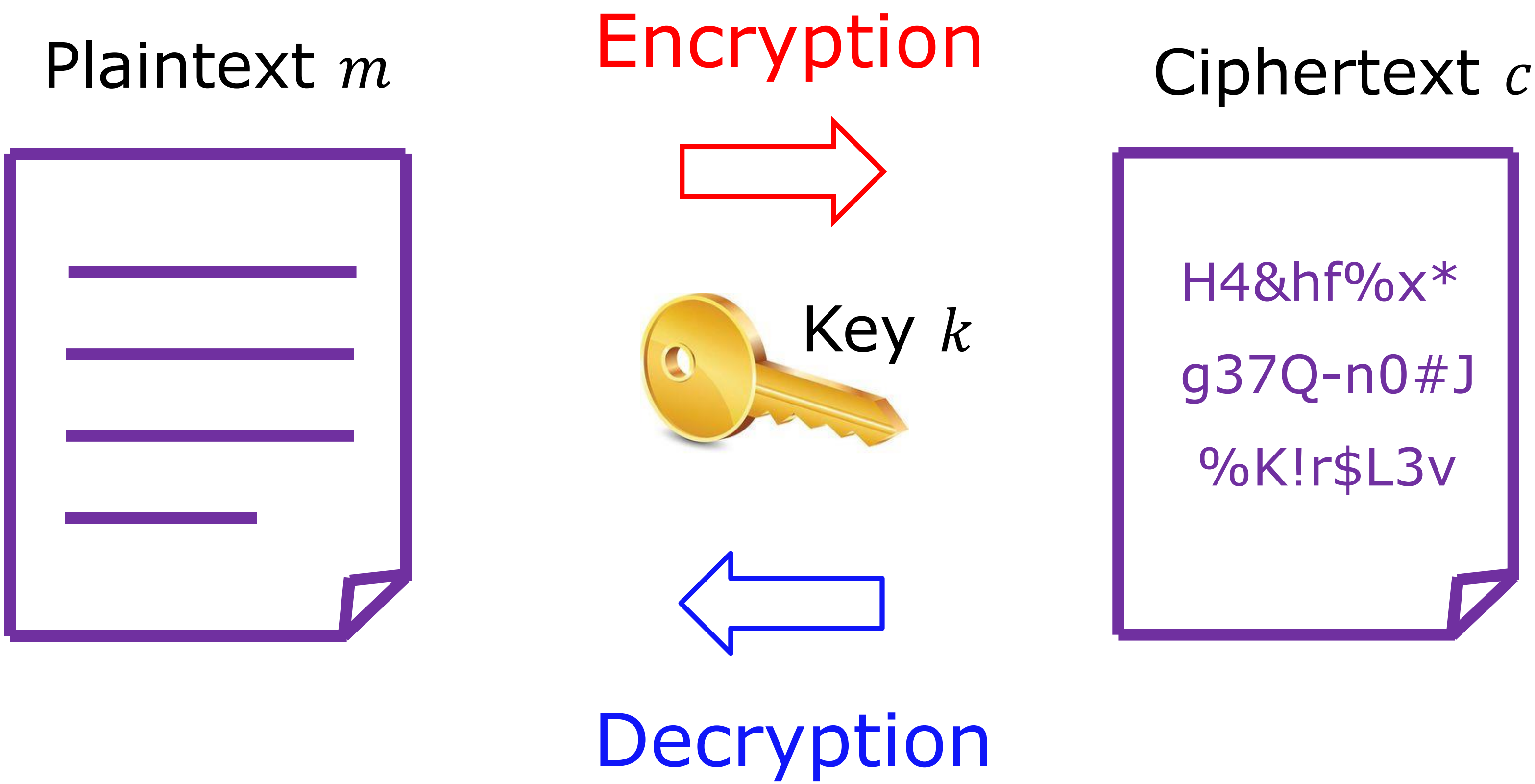
We give an encryption function that is secure in all notions.

Symmetric encryption



Symmetric encryption

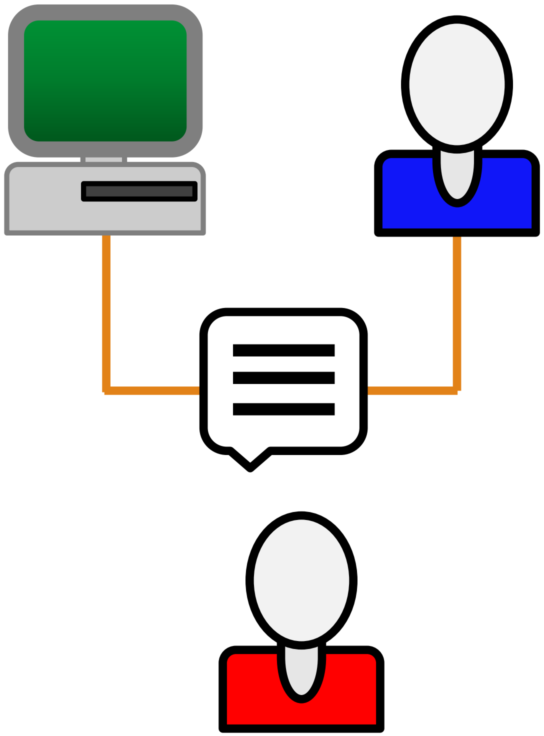
$m \mapsto c = \mathrm{Enc}_k(m)$



$c \mapsto m = \mathrm{Dec}_k(c)$

Indistinguishability

A real protocol $\mathcal{R}$ is secure in terms of indistinguishability if no algorithm can tell it apart from its ideal functionality $\mathcal{I}$.



Turing test

IND-CPA game

Learning phase:

Adversary collects information about Enc.

m →

← $c = \mathrm{Enc}_k(m)$

Adversary

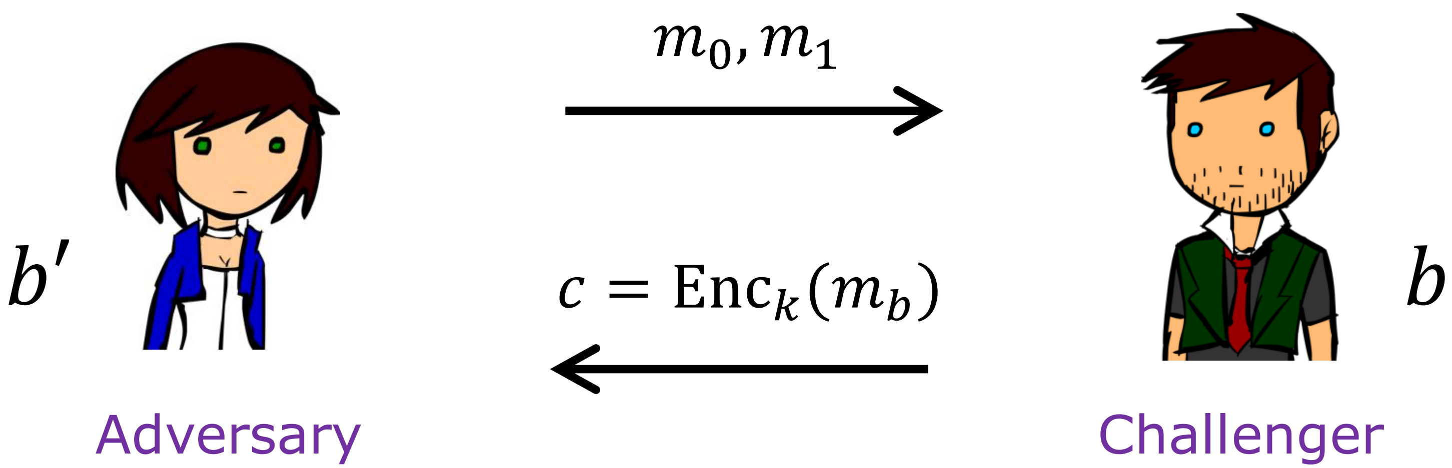
Challenger

IND-CPA = Indistinguishability under chosen plaintext attack

IND-CPA game

Challenge phase:

Adversary picks two messages. She obtains $\mathrm{Enc}_k(m_b)$ and must guess b.

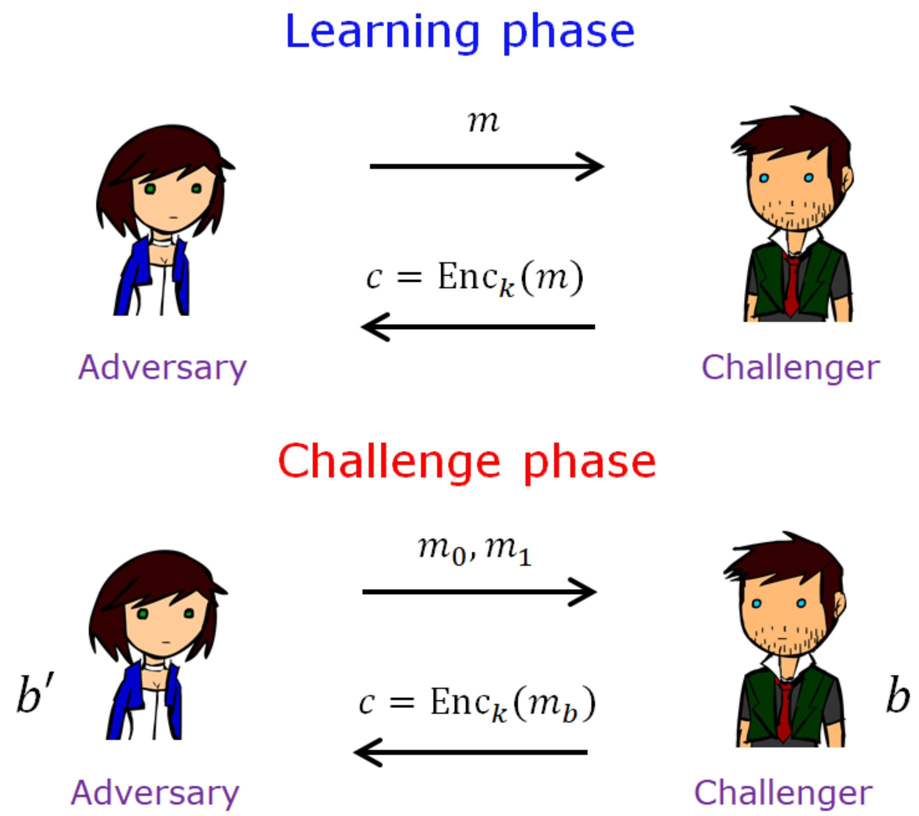


IND-CPA = Indistinguishability under chosen plaintext attack

IND-CPA security

Enc is IND-CPA ϵ-secure if

$$\Pr[b' = b] = \frac{1}{2} + \epsilon$$



Post-quantum crypto

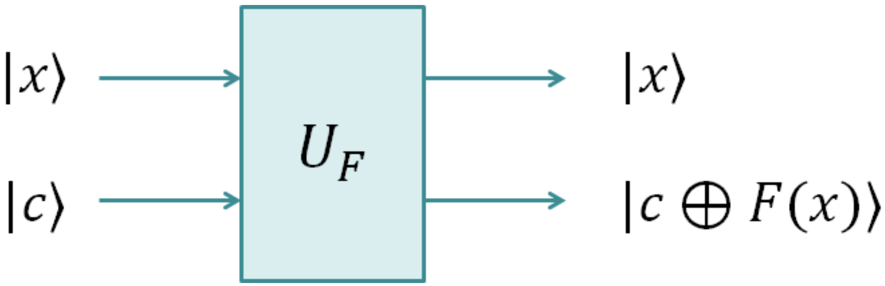
Also known as quantum-safe or quantum-resistant crypto

Goal is to build classical cryptosystems that are secure against quantum adversaries.

Based on problems that are believed to be hard for quantum computers (e.g. lattice problems, linear code decoding, etc.)

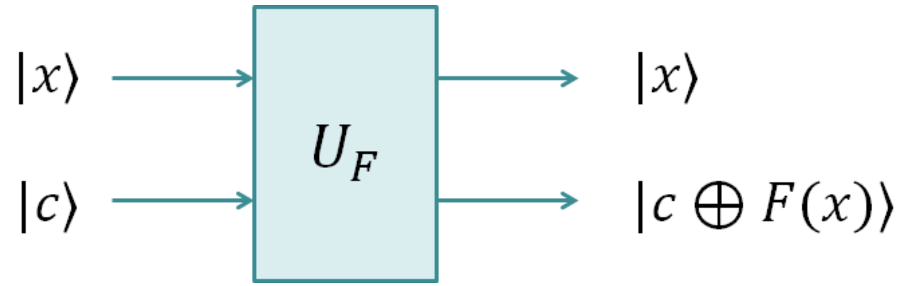
Quantum query types

Standard (ST)

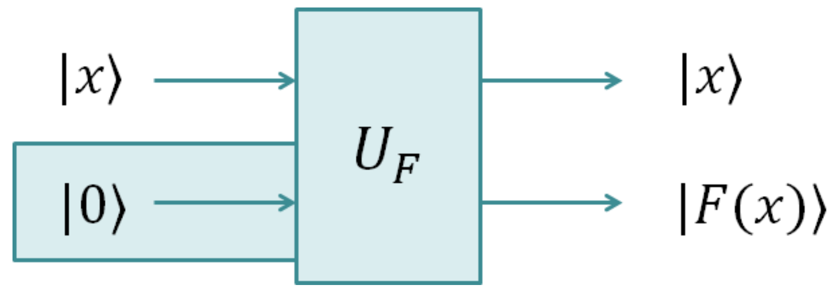


Quantum query types

Standard (ST)

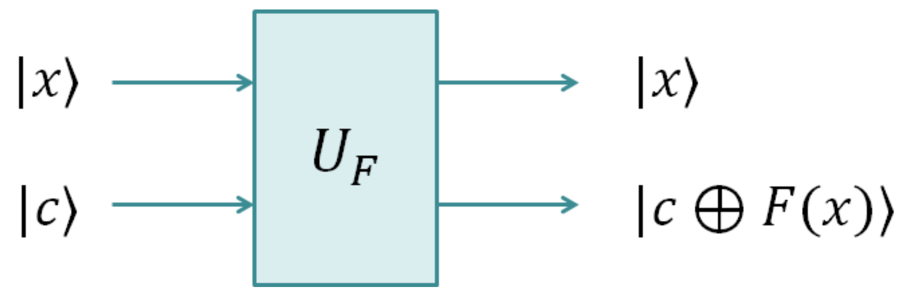


Embedding (EM)

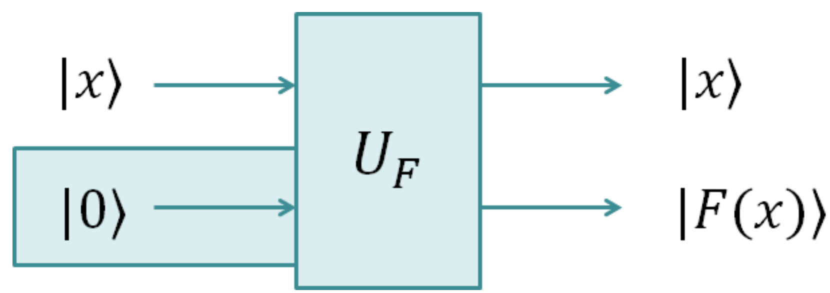


Quantum query types

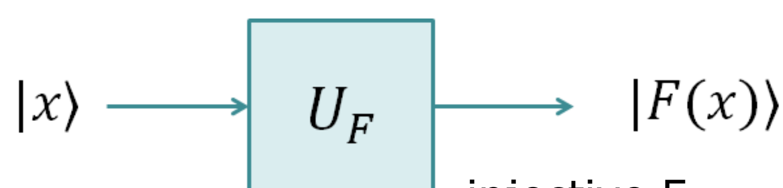
Standard (ST)



Embedding (EM)



Erasing (ER)



injective F

Example

Suppose Enc is a secure encryption function

Learning phase:

$$|m, c\rangle \mapsto |m, c \oplus \mathrm{Enc}_k(m)\rangle$$

Challenge phase:

$$|m_0, m_1, c\rangle \mapsto |m_0, m_1, c \oplus \mathrm{Enc}_k(m_b)\rangle$$

Can adversary guess b?

Example

Suppose Enc is a secure encryption function

Learning phase:

$$|m, c\rangle \mapsto |m, c \oplus \mathrm{Enc}_k(m)\rangle$$

Challenge phase:

$$|m_0, m_1, c\rangle \mapsto |m_0, m_1, c \oplus \mathrm{Enc}_k(m_b)\rangle$$

Can adversary guess b? YES

Choose $m_0 = |0\rangle, m_1 = |\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$

An insecure notion

If $b = 0$ or $b = 1$, respectively:

$$|0\rangle|\psi\rangle|c \oplus \mathrm{Enc}_k(0)\rangle, \quad \frac{1}{\sqrt{2^n}} \sum_x |0\rangle|x\rangle|c \oplus \mathrm{Enc}_k(x)\rangle$$

Measure 3rd register in computational basis.

An insecure notion

If $b = 0$ or $b = 1$, respectively:

$$|0\rangle|\psi\rangle|c \oplus \mathrm{Enc}_k(0)\rangle, \quad \frac{1}{\sqrt{2^n}}\sum_x |0\rangle|x\rangle|c \oplus \mathrm{Enc}_k(x)\rangle$$

Measure 3rd register in computational basis.

Measure 2nd register with $\{P_\psi = |\psi\rangle\langle\psi|, I - P_\psi\}$

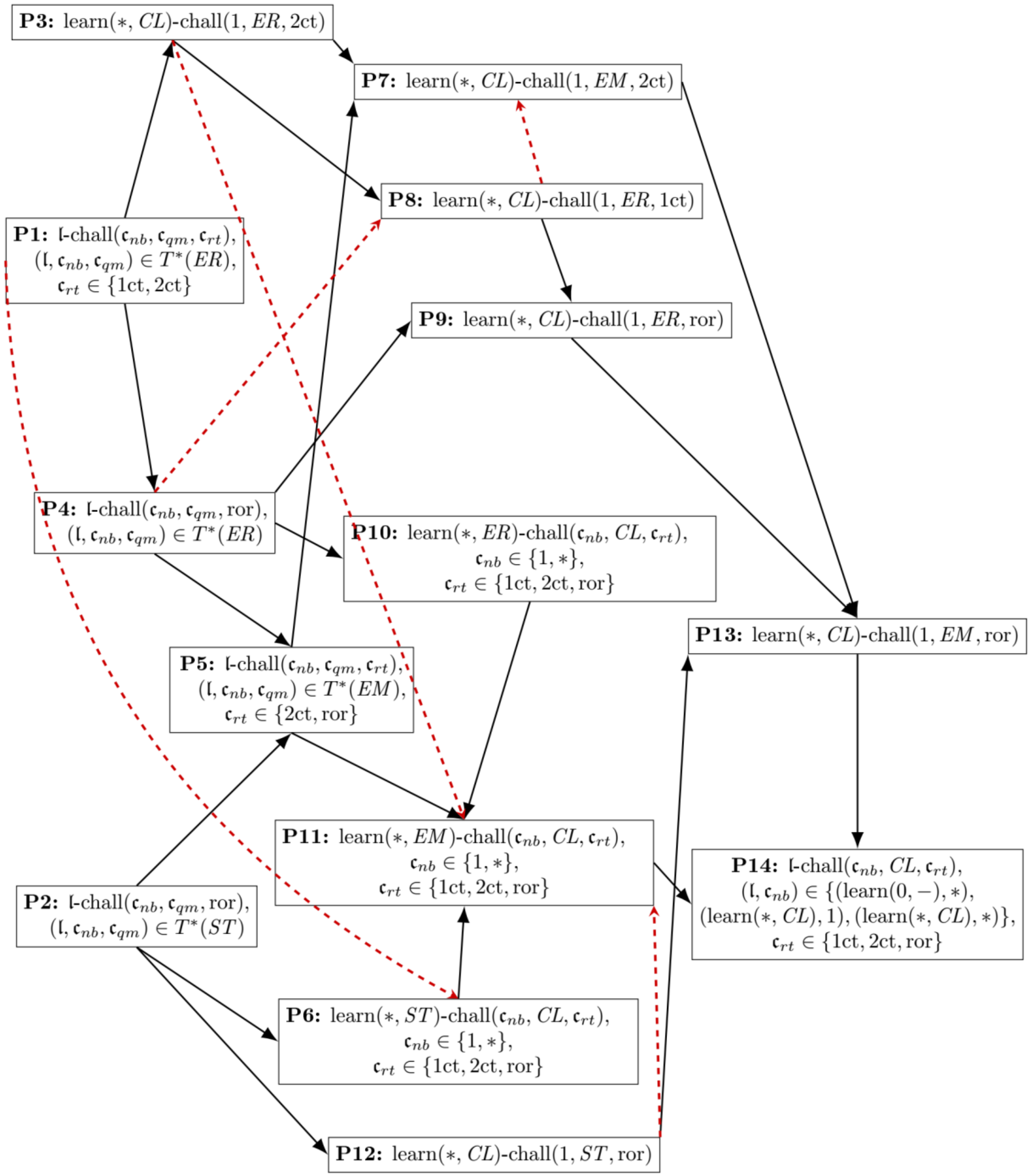
$$\Pr[P_\psi | b = 0] = 1, \qquad \Pr[P_\psi | b = 1] = \frac{1}{2^n}$$

qIND-CPA notions

Variants of qIND-CPA according to:

1. Number of learning $(0, \text{many})$ and challenge $(1, \text{many})$ queries
2. Query model (CL, ST, EM, ER)
3. Challenge query type $(1\text{ct}, 2\text{ct}, \text{ror})$

Learning and challenge queries are same quantum type or classical-quantum.


P3: learn(∗, CL)-chall(1, ER, 2ct)
P7: learn(∗, CL)-chall(1, EM, 2ct)
P8: learn(∗, CL)-chall(1, ER, 1ct)
P1: l-chall(c_nb, c_qm, c_rt), (l, c_nb, c_qm) ∈ T*(ER), c_rt ∈ {1ct, 2ct}
P9: learn(∗, CL)-chall(1, ER, ror)
P4: l-chall(c_nb, c_qm, ror), (l, c_nb, c_qm) ∈ T*(ER)
P10: learn(∗, ER)-chall(c_nb, CL, c_rt), c_nb ∈ {1, ∗}, c_rt ∈ {1ct, 2ct, ror}
P13: learn(∗, CL)-chall(1, EM, ror)
P5: l-chall(c_nb, c_qm, c_rt), (l, c_nb, c_qm) ∈ T*(EM), c_rt ∈ {2ct, ror}
P11: learn(∗, EM)-chall(c_nb, CL, c_rt), c_nb ∈ {1, ∗}, c_rt ∈ {1ct, 2ct, ror}
P14: l-chall(c_nb, CL, c_rt), (l, c_nb) ∈ {(learn(0, −), ∗), (learn(∗, CL), 1), (learn(∗, CL), ∗)}, c_rt ∈ {1ct, 2ct, ror}
P2: l-chall(c_nb, c_qm, ror), (l, c_nb, c_qm) ∈ T*(ST)
P6: learn(∗, ST)-chall(c_nb, CL, c_rt), c_nb ∈ {1, ∗}, c_rt ∈ {1ct, 2ct, ror}
P12: learn(∗, CL)-chall(1, ST, ror)

Conclusions

There are several ways to extend classical security notions to quantum

A classical encryption function may become insecure when accessible in superposition

Challenge query types

One-ciphertext (1ct):

$$m_0, m_1 \mapsto \mathrm{Enc}_k(m_b)$$

Two-ciphertext (2ct):

$$m_0, m_1 \mapsto \left(\mathrm{Enc}_k(m_b), \mathrm{Enc}_\mathrm{k}(m_{\overline{b}})\right)$$

Real-or-random (ror):

$$m \mapsto \mathrm{Enc}_k(m) \text{ or } r \leftarrow \$, \mathrm{Enc}_k(r)$$

Classically, all three types are equivalent.

Separation by SetEq

Set equality problem (SetEq): given oracle access to injective $f, g: X \to Y$

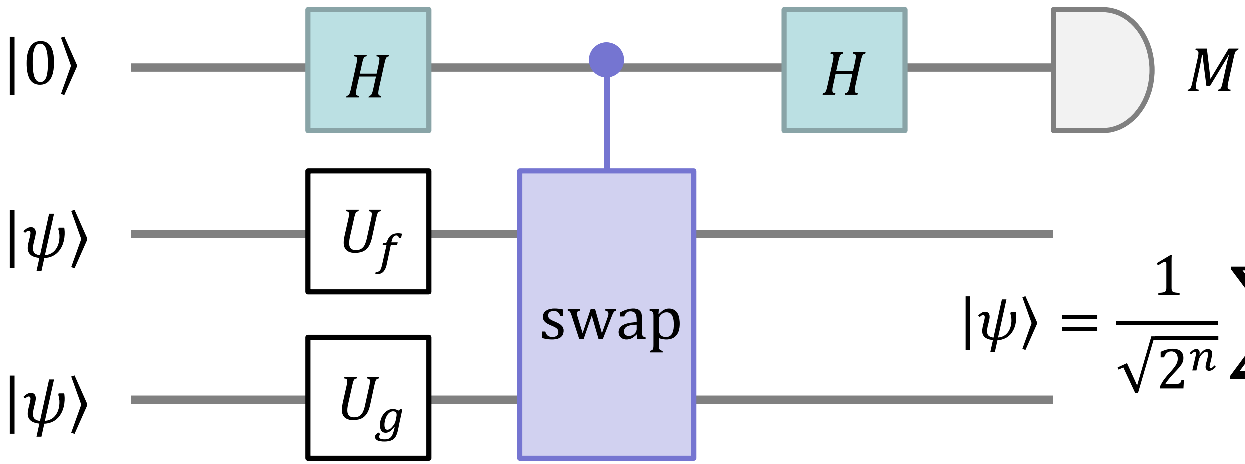
Image of f, g is (1) same or (2) disjoint

Decide if (1) or (2) holds.

Zhandry (2015): $\sim 2^{m/3}$ ST-type queries needed to distinguish the 2 cases.

Separation by SetEq

But a few ER-type queries suffice:



$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$$

If (1), $\Pr[M = 0] = 1$.

If (2), $\Pr[M = 0] = \Pr[M = 1] = \frac{1}{2}$.

Secure in all notions

Enc is secure in all notions if it is secure in the setting with

a) No learning queries

b) Challenge: $(*, ER, 1\mathrm{ct})$ or $(*, ST, \mathrm{ror})$

A possible construction is

$$\mathrm{Enc}_k(m; r, r') = \mathrm{qPRP}_r(r' || m) \,||\, \mathrm{sPRP}_k(r)$$