Quantum Uncloneability

Anne Broadbent

uOttawa

With many thanks to:
Eric Culf, Rabib Islam, Stacey Jeffery, Martti Karvonen, Monica Nevins, Sébastien Lord, Supartha Podder, Hadi Salmassian, Aarthi Sundaram

EPIT Spring School
May 26
2021

Quantum States Can't be Copied

What is uncloneability?

Aaronson (2009)
Quantum Copy-Protection and Quantum Money

Aaronson (2016)
Qcrypt 2016 after-dinner speech

Park (1970); Dieks & Wootters-Zurek (1982)

What is uncloneability?

What is security?

JOURNAL OF COMPUTER AND SYSTEM SCIENCES **28**, 270–299 (1984)

Probabilistic Encryption*

SHAFI GOLDWASSER AND SILVIO MICALI

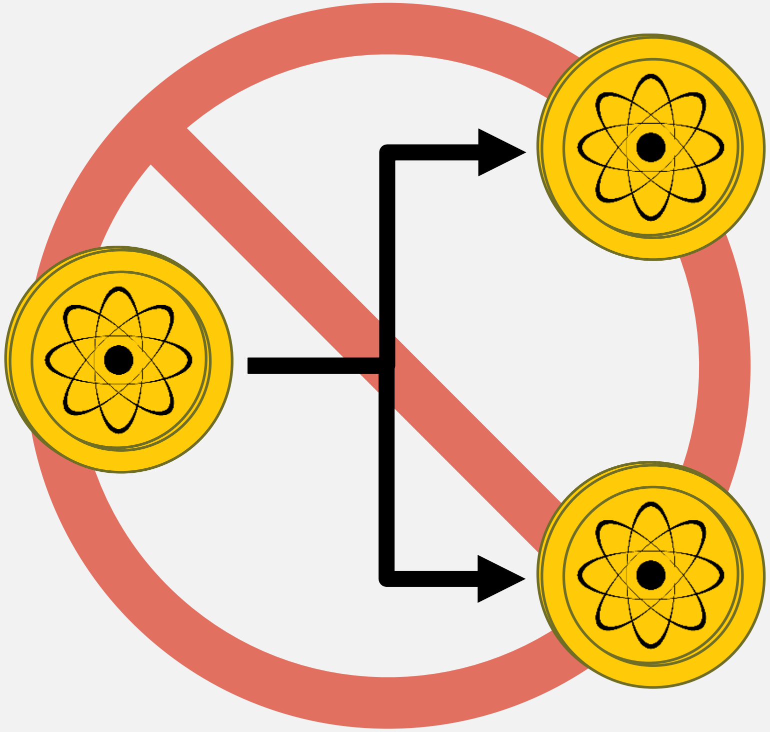
Laboratory of Computer Science, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

Received February 3, 1983; revised November 8, 1983

"Security for an encryption scheme can be defined in terms of a game"

Why should you care?

Uncloneable Authenticity



Quantum Money

Wiesner (ca. 1969)

Written in 1968
Published 1983

Submitted to IEEE, Information Theory

This paper treats a class of codes made possible by restrictions on measurement related to the uncertainty principal. Two concrete examples and some general results are given.

Conjugate Coding *

Stephen Wiesner

Columbia University, New York, N.Y.
Department of Physics

The uncertainty principle imposes restrictions on the capacity of certain types of communication channels. This paper will show that in compensation for this "quantum noise", quantum mechanics allows us novel forms of coding without analogue in communication channels adequately described by classical physics.

* Research supported in part by the National Science Foundation.

Wiesner's conjugate coding

Pick basis $\theta \in \{0,1\}$.
Pick bit $b \in \{0,1\}$.
let $|b\rangle_\theta = H^\theta|b\rangle$

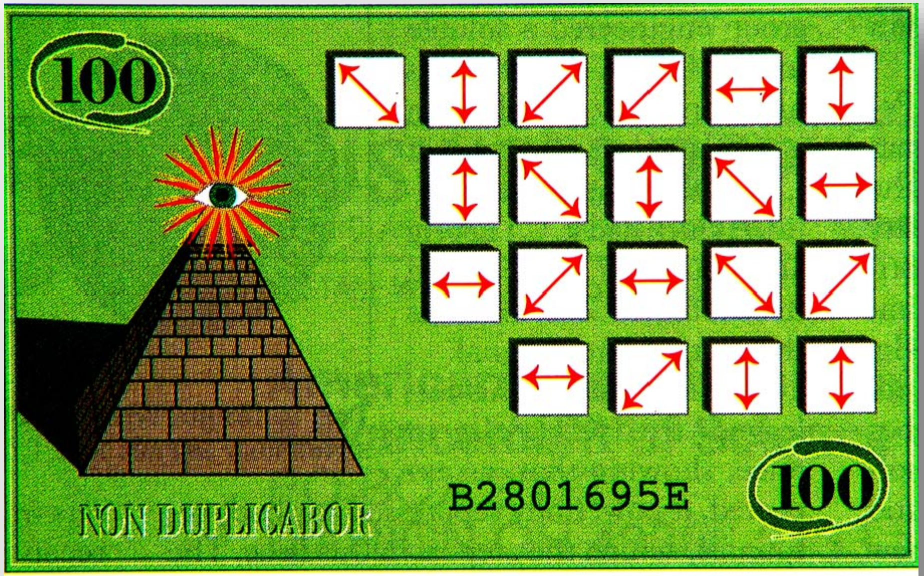
$\boldsymbol{\theta}$	$\boldsymbol{b}$	$\boldsymbol{|b\rangle_\theta}$
0	0	$|0\rangle$
0	1	$|1\rangle$
1	0	$|+\rangle$
1	1	$|-\rangle$

Given a single copy of $|b\rangle_\theta$ for random b, θ:

- Can easily verify $|b\rangle_\theta$ if b, θ are known.
- Intuitively: without knowledge of the encoding basis, no third party can create two quantum states that pass this verification with high probability.

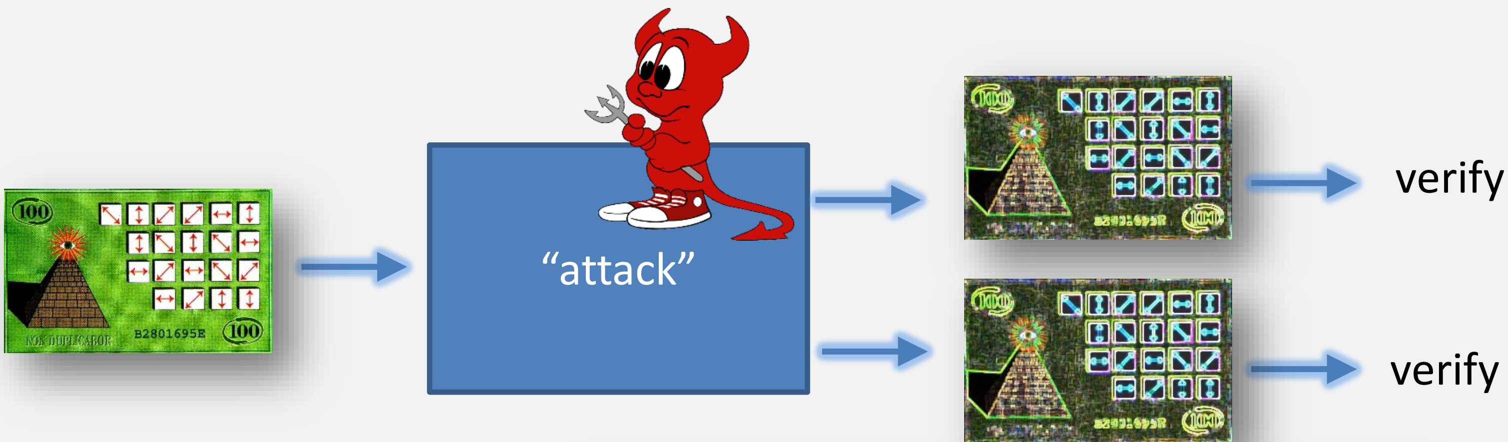
For bit-strings $\theta = \theta_1\theta_2 \ldots \theta_n$, $b = b_1 b_2 \ldots b_n$, define
$|b\rangle_\theta = |b_1\rangle_{\theta_1} \otimes |b_2\rangle_{\theta_2} \ldots \otimes |b_n\rangle_{\theta_n}$

A quantum banknote is $|b\rangle_\theta$ for random $b, \theta \in \{0,1\}^n$:



A quantum banknote, containing particles in a secret set of quantum states, cannot be copied by counterfeiters, who would disturb the particles by attempting to observe them.

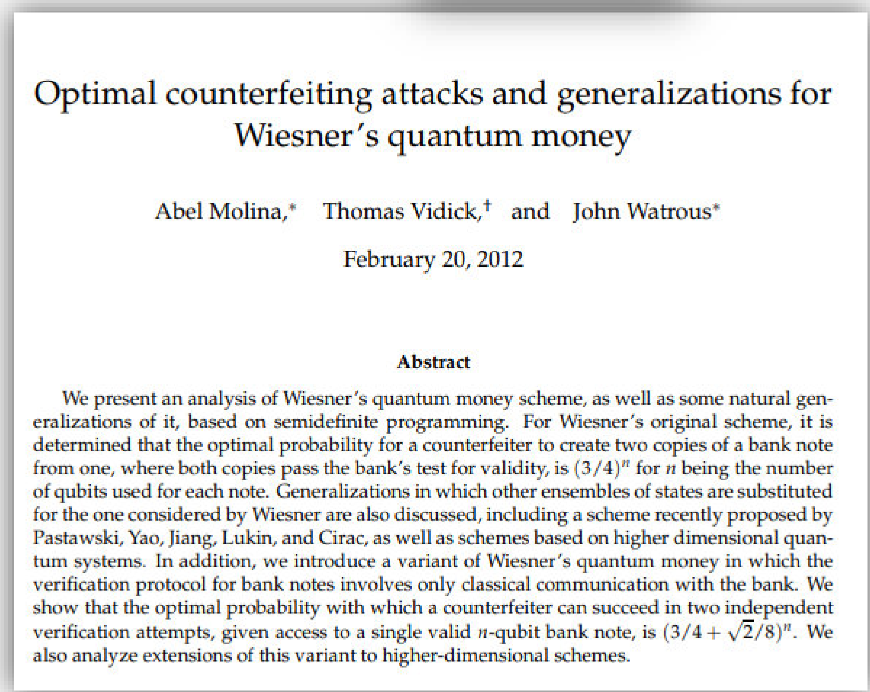
Security of Wiesner's quantum money



How does the difficulty of cloning quantum money scale with the number of qubits, n?

Answer:

$$(3/4)^n$$



Optimal counterfeiting attacks and generalizations for Wiesner's quantum money

Abel Molina,* Thomas Vidick,† and John Watrous*

February 20, 2012

Abstract

We present an analysis of Wiesner's quantum money scheme, as well as some natural generalizations of it, based on semidefinite programming. For Wiesner's original scheme, it is determined that the optimal probability for a counterfeiter to create two copies of a bank note from one, where both copies pass the bank's test for validity, is $(3/4)^n$ for n being the number of qubits used for each note. Generalizations in which other ensembles of states are substituted for the one considered by Wiesner are also discussed, including a scheme recently proposed by Pastawski, Yao, Jiang, Lukin, and Cirac, as well as schemes based on higher dimensional quantum systems. In addition, we introduce a variant of Wiesner's quantum money in which the verification protocol for bank notes involves only classical communication with the bank. We show that the optimal probability with which a counterfeiter can succeed in two independent verification attempts, given access to a single valid n-qubit bank note, is $(3/4+\sqrt{2}/8)^n$. We also analyze extensions of this variant to higher-dimensional schemes.

QUANTUM MONEY “REVIVAL”

Noise-tolerant (‘feasible with current technology’) quantum money

- Pastawski, Yao, Jiang, Lukin, Cirac (2012)

Quantum Money with classical verification

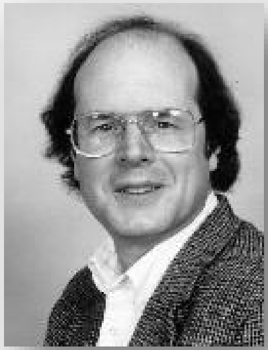
- Gavinsky (2012)

Public-key quantum money (can be verified by any user)

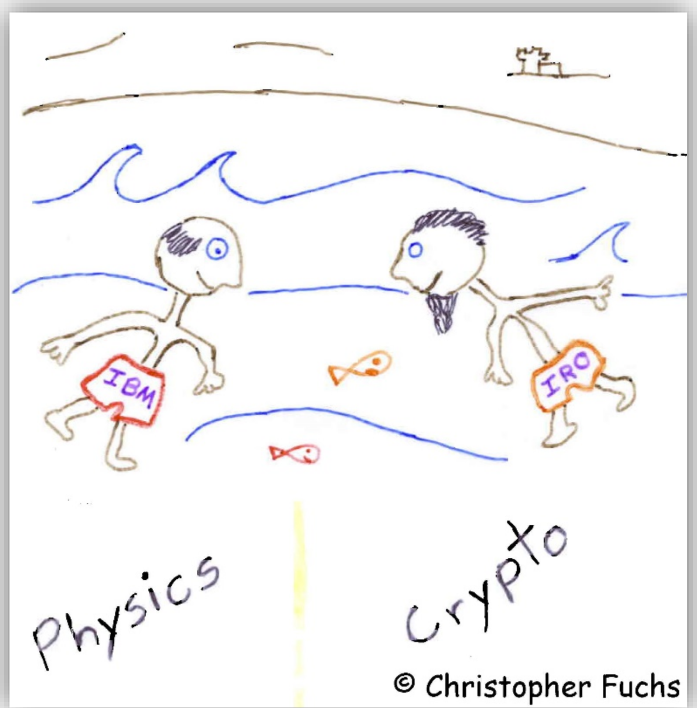
- Farhi, Gosset, Hassidim, Lutomirski, and Shor (2012)
- Aaronson and Christiano (2012)
- Zhandry (2017)

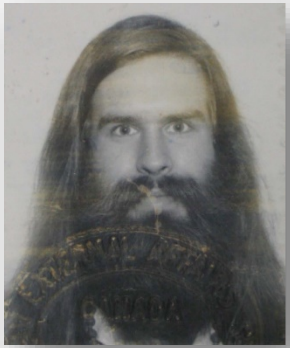
Open Question: Public-key quantum money feasible with current or short-term technology (“NISQ”-era public-key quantum money)?

1979

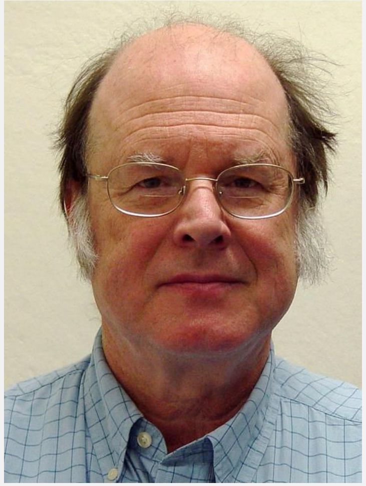


Charles
Bennett
Physicist
IBM, USA



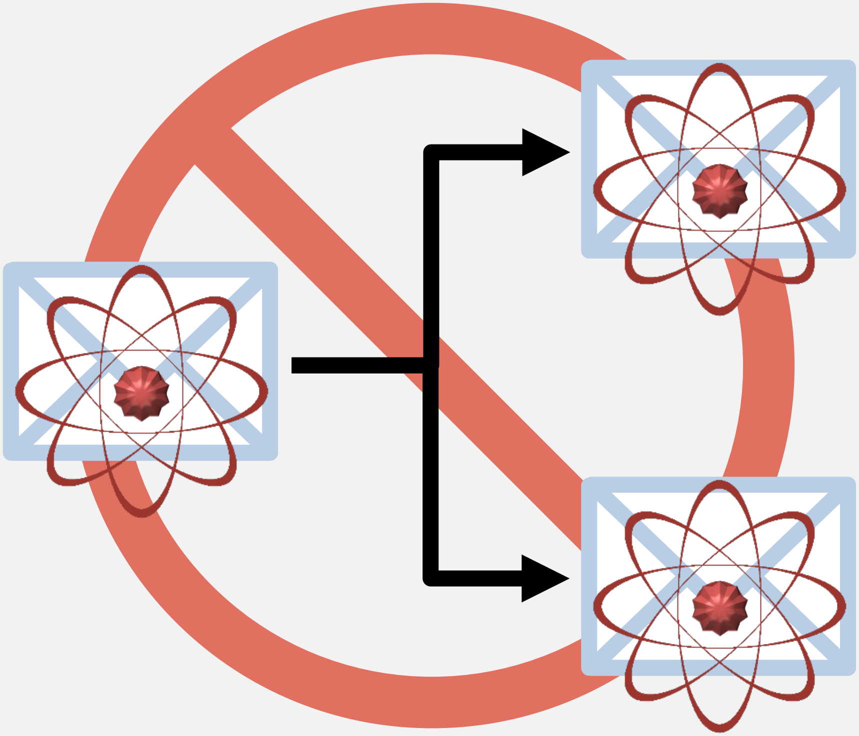


Gilles
Brassard
Computer
Scientist
Université
de Montréal,
Canada



2018

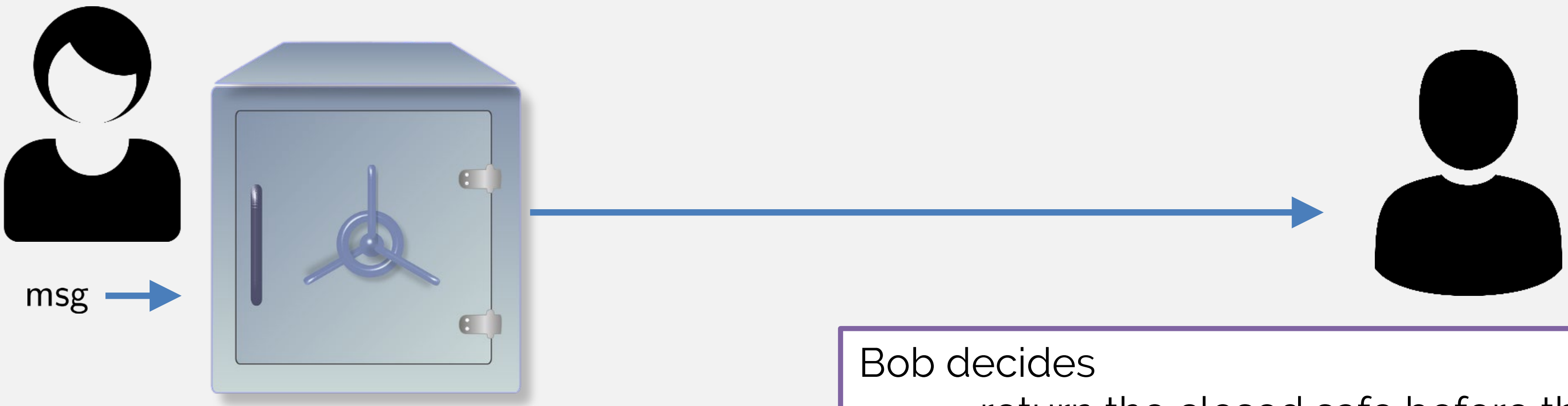
Uncloneable Information



Example 1: Certified Deletion Broadbent, Islam (2020)

Certified Deletion

A "physical" type of encryption:



Alice inserts a message into a safe, closes it and sends it to Bob.

Bob decides

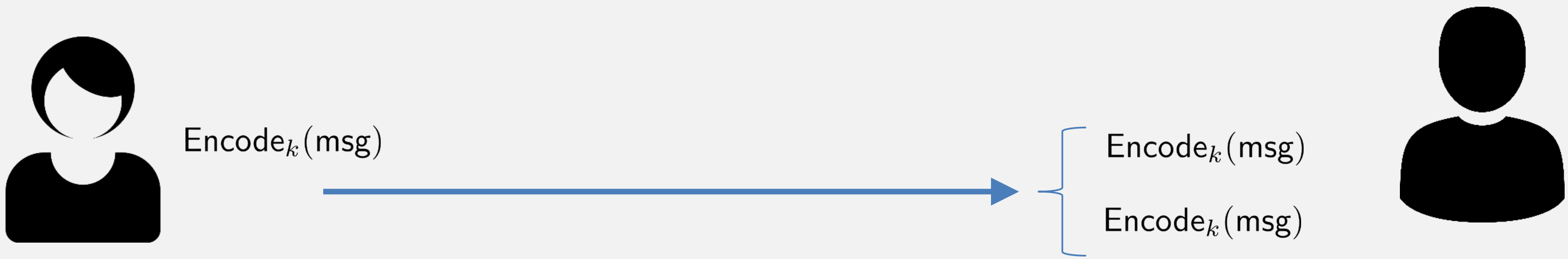
- return the closed safe before the combination is revealed as a proof that message was not read

XOR

- Keep the safe and when the combination is available, open & read the contents

Can we achieve this in a digital world?

Can we achieve this in a digital world?
<u>No</u>!
Proof by contradiction…



Bob can :

- Convince Alice that he did not read the message(use copy #1)

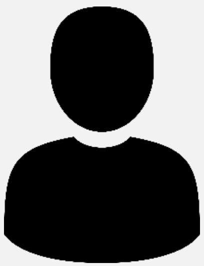
  AND

- Using combination, open & read the content (use copy #2)

Quantum Encryption with Certified Deletion

Quantum mechanics enables the best of the physical and digital worlds:

- Encoding (encrypting) a classical message into a quantum state
- Bob can prove that he deleted the message by sending Alice a classical string



Basic prepare-and-measure certified deletion scheme by example:

	θ	0	1	0	1
θ random					
r random	r	0	1	1	0
Wiesner encoding	$\lvert r\rangle_\theta$	$\lvert 0\rangle$	$\lvert -\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$
r_{comp}: substring of r where $\theta = 0$	r_{comp}	0		1	
r_{diag}: substring of r where $\theta = 1$	r_{diag}		1		0

- To encrypt $m \in \{0,1\}^2$, send $|r\rangle_\theta, m \oplus r_{comp}$

- To delete the message, measure all qubits in diagonal basis to get $y = * 1 * 0$.
- To verify the deletion, check that the $\theta = 1$ positions of d equal r_{diag}.

- To decrypt using key θ, measure qubits in position where $\theta = 0$, to get r_{comp}, then use $m \oplus r_{comp}$ to compute m.

Proof intuition

θ	0	1	0	1
r	0	1	1	0
$\|r\rangle_\theta$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$
r_{comp}	0		1	
r_{diag}		1		0

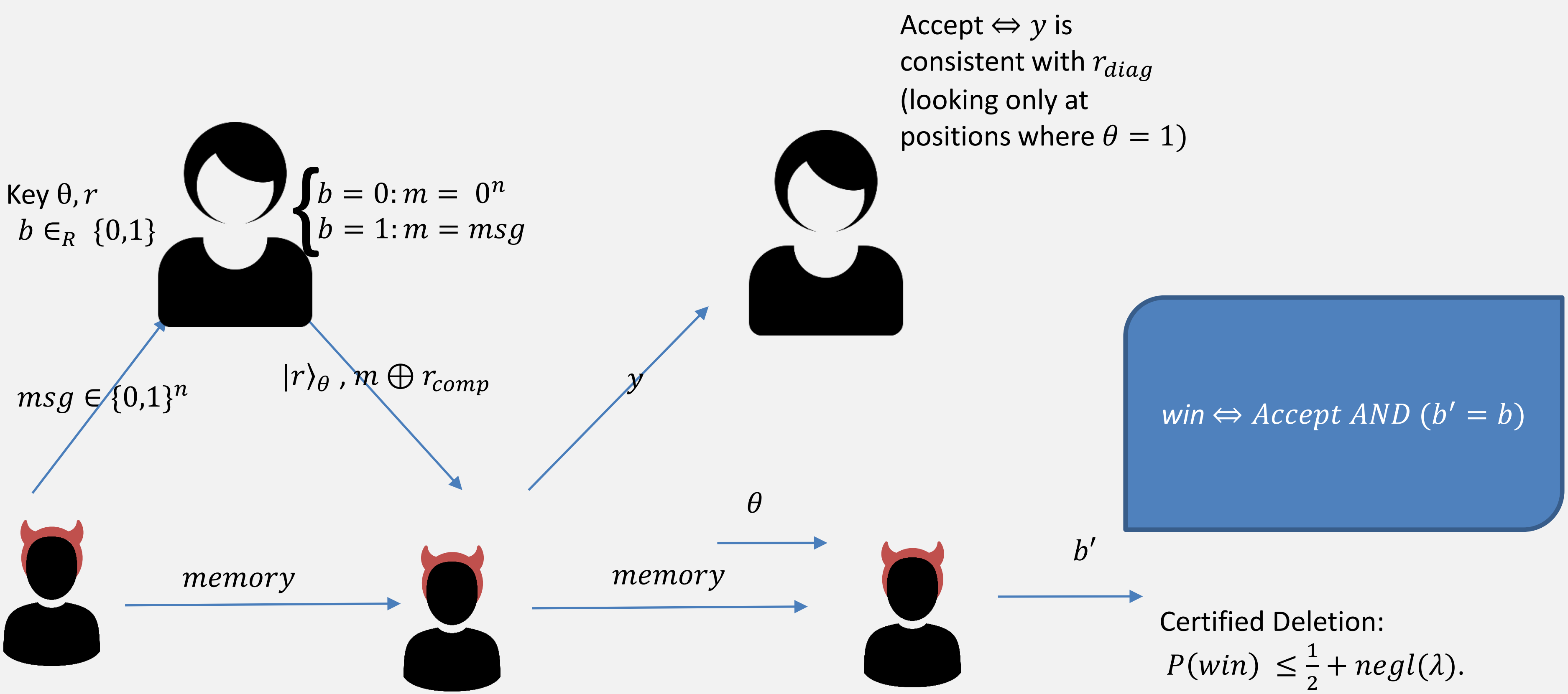
As the probability of predicting r_{diag} increases (i.e. adversary produces convincing “proof of deletion”)

$$H(X) + H(Z) \geq \log \frac{1}{c}$$

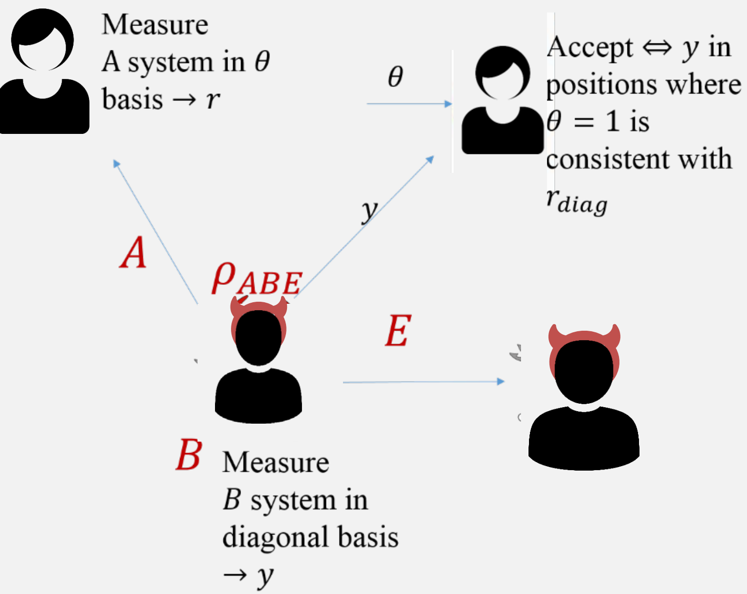
The probability of guessing r_{comp} decreases (i.e. adversary is unable to decrypt, even given the key)

Maassen & Uffink, 1988

Certified Deletion Security Game



Proof Outline



1. Consider Entanglement-based game

2. Use Entropic uncertainty relation (Tomamichel & Renner 2011):
X: outcome if Alice measures *n* qubits in computational basis
Z: outcome if Alice measures *n* qubits in diagonal basis
Z':outcome of Bob who measures *n* qubits in diagonal basis

$$H^{\epsilon}_{min}(X \mid E) + H^{\epsilon}_{max}(Z \mid Z') \geq n,$$

$H^{\epsilon}_{min}(X \mid E)$: average prob. that Eve guesses X correctly
$H^{\epsilon}_{max}(Z \mid Z')$: # of bits that are required to reconstruct Z from Z'.

By giving an upper bound on the max-entropy, we obtain a lower bound on the min-entropy.

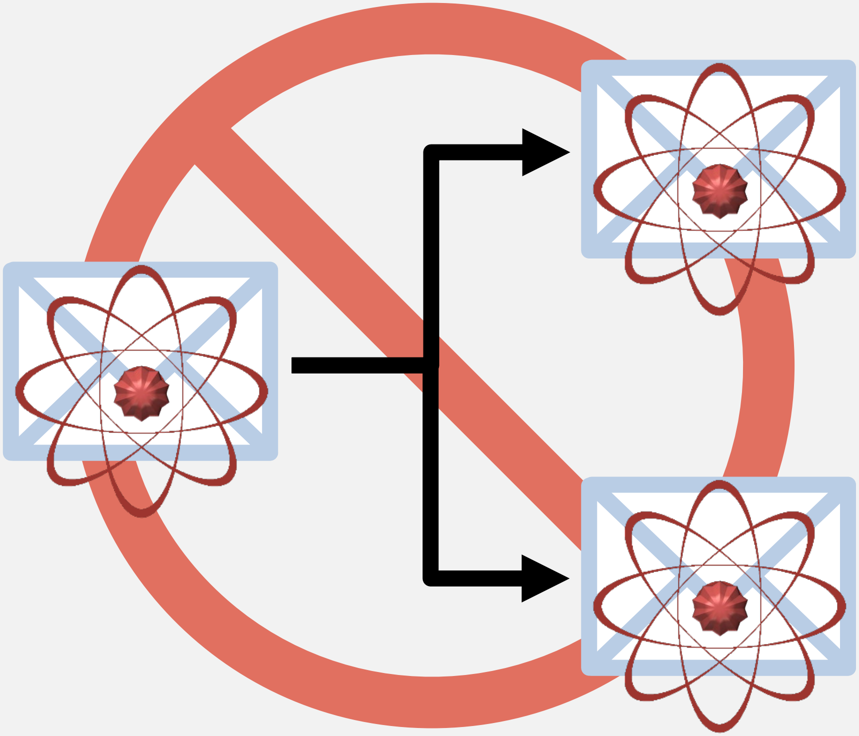
Refinements of the basic protocol:
-reduce and make uniform E's advantage: Use **privacy amplification** (2-universal hash function) to make r_{comp} exponentially close to uniform from E's point of view:

$$P(win) \leq \frac{1}{2} + negl(\lambda).$$

-noise tolerance: Accept y if less than $k\delta$ bits are wrong; use **error correction**.

Kundu, Tan (2020) : Composably secure device-independent encryption with certified deletion

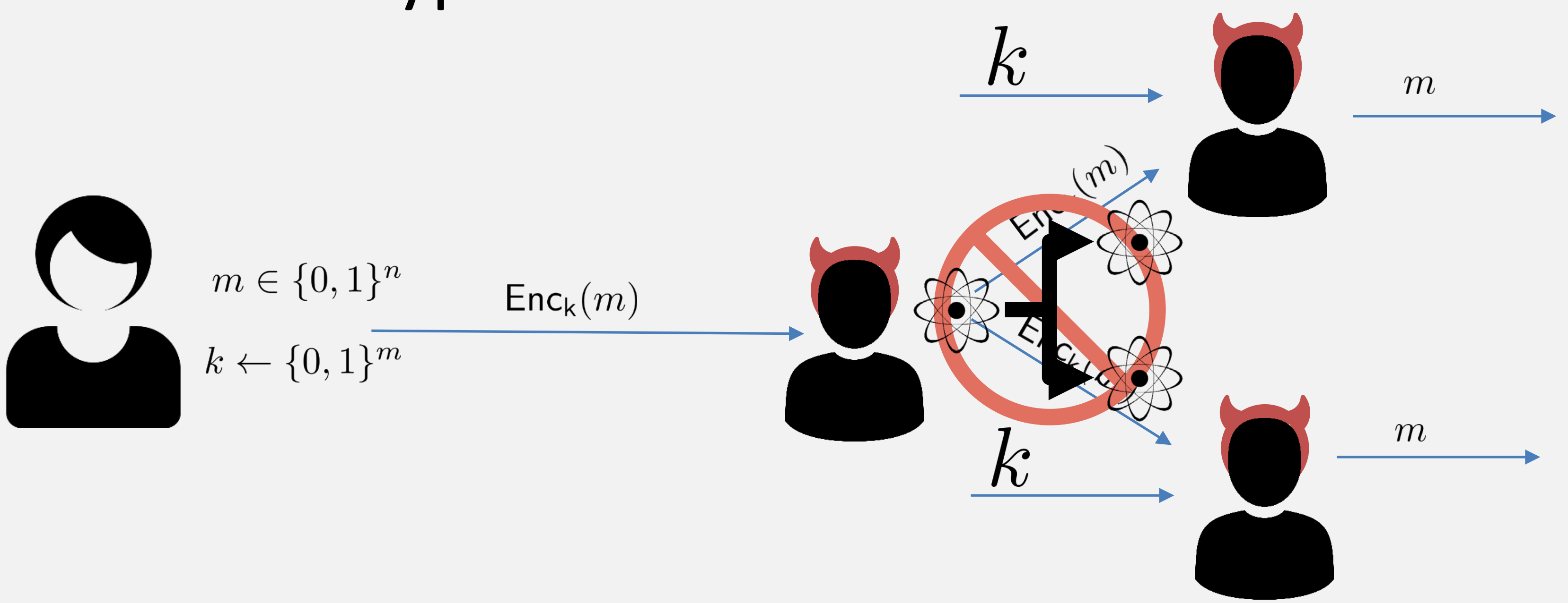
Uncloneable Information



Example 2: Uncloneable Encryption

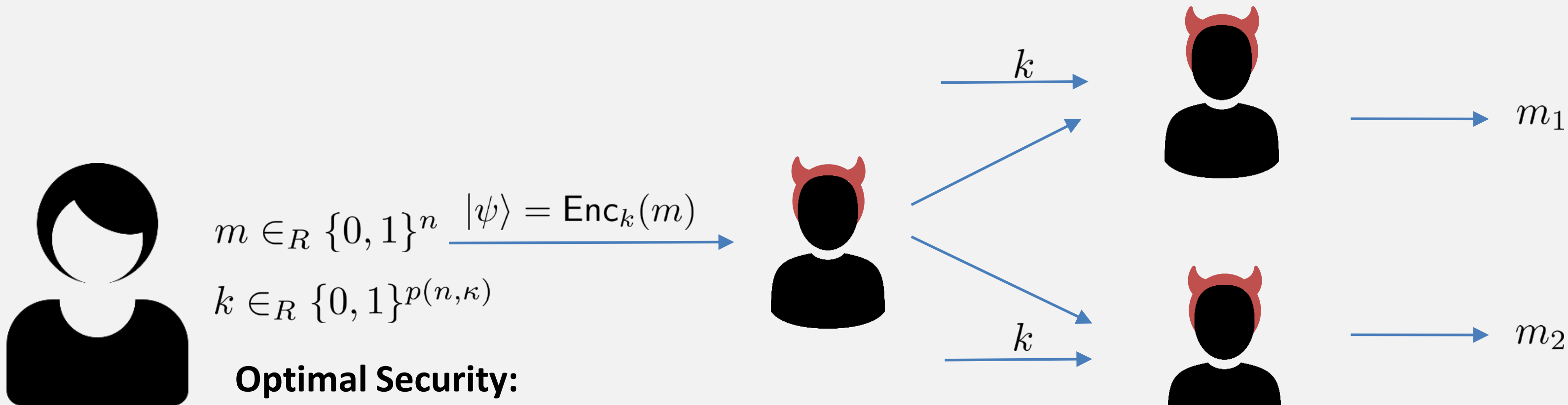
Gottesman (2002)

When encryption is classical:



Classical ciphertexts can be copied, hence it is always possible for the adversary and the honest party to perfectly decrypt, given k.

Uncloneable Encryption Security Game



Optimal Security:

$$\Pr(m_1 = m_2 = m) \leq \frac{1}{2^n} + \mathsf{negl}(\kappa)$$

Wiesner-encoding based scheme (in the Quantum Random Oracle Model (QROM):
[Broadbent, Lord 2020]

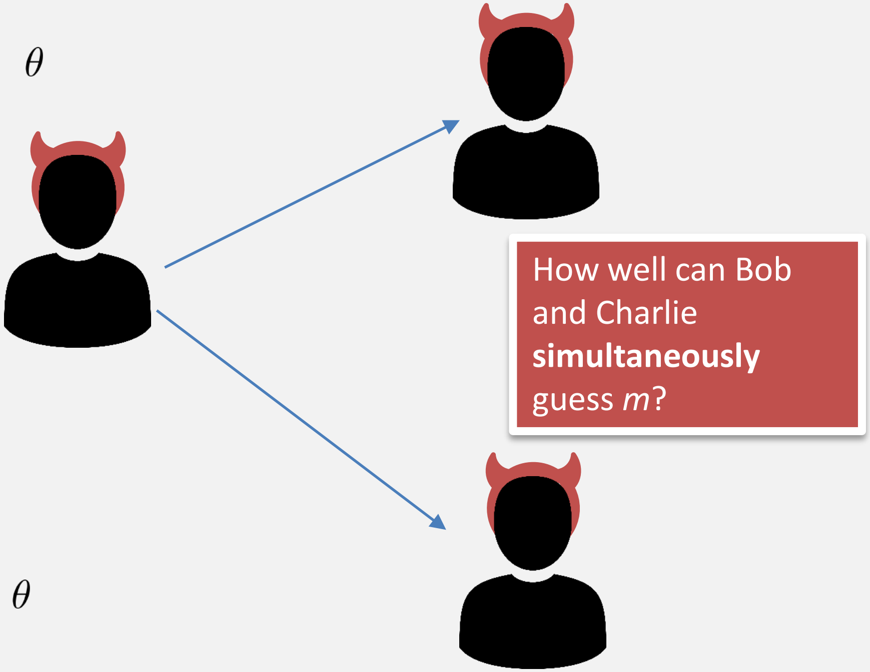
$$\Pr(m_1 = m_2 = m) \leq 9\frac{1}{2^n} + \mathsf{negl}(\kappa)$$

Uncloneable Encryption Scheme + Security

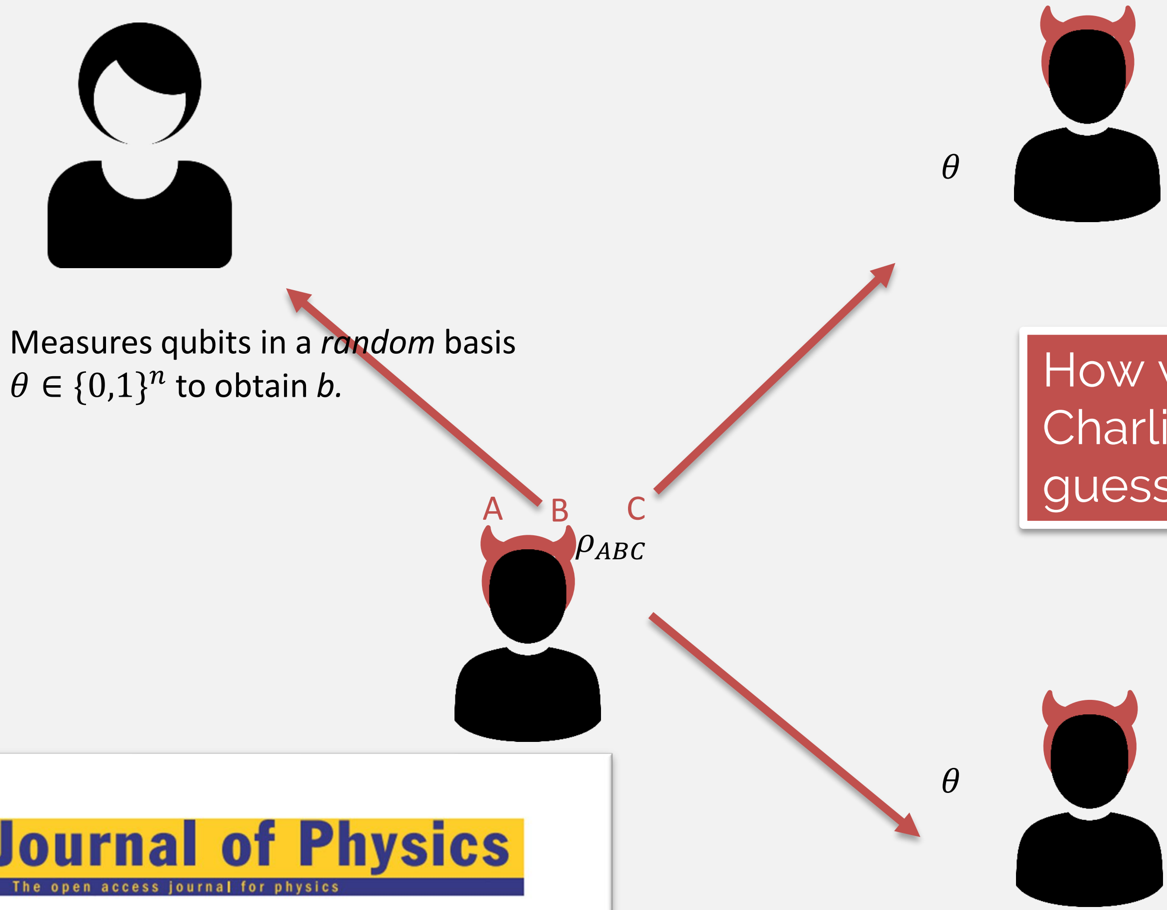
To encrypt $m \in \{0,1\}^n$,
Prepare $|b\rangle_\theta$ for random
$b, \theta \in \{0,1\}^n$

$|b\rangle_\theta$, $m \oplus b$

θ



θ



How well can Bob and Charlie **simultaneously** guess *b*?

Optimal winning probability: $\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n$

$> (1.2)^n \cdot \frac{1}{2^n}$

Idea: amplify this using a QROM.

New Journal of Physics
The open access journal for physics

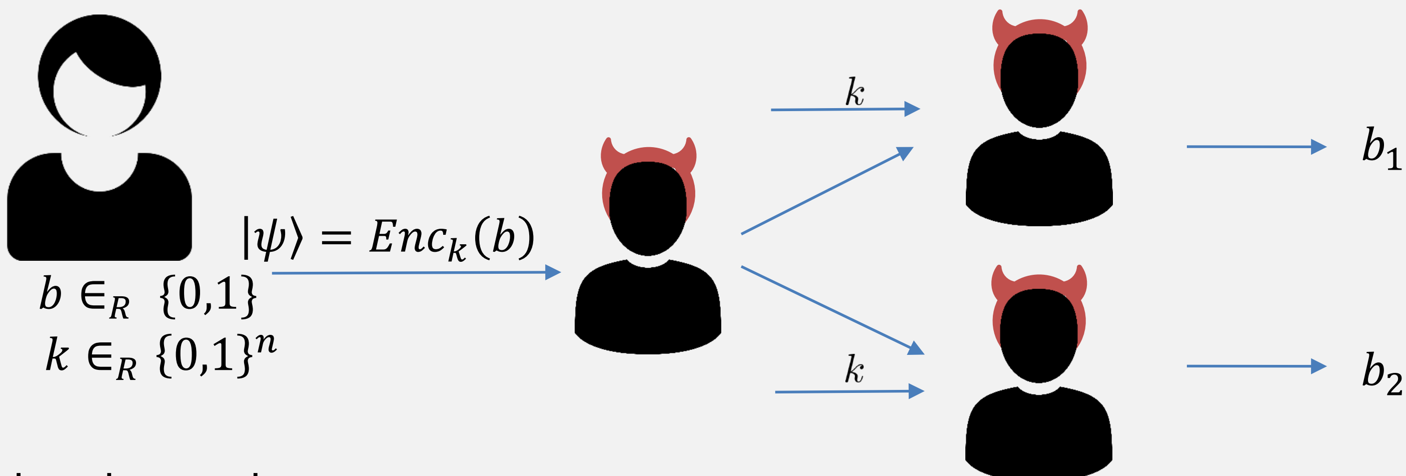
A monogamy-of-entanglement game with applications to device-independent quantum cryptography

Marco Tomamichel[1,3], Serge Fehr[2,3], Jędrzej Kaniewski[1] and Stephanie Wehner[1]
[1] Centre for Quantum Technologies (CQT), National University of Singapore, Singapore
[2] Centrum Wiskunde and Informatica (CWI), Amsterdam, The Netherlands
E-mail: cqtmarco@nus.edu.sg and serge.fehr@cwi.nl

New Journal of Physics **15** (2013) 103002 (24pp)

Open Questions:

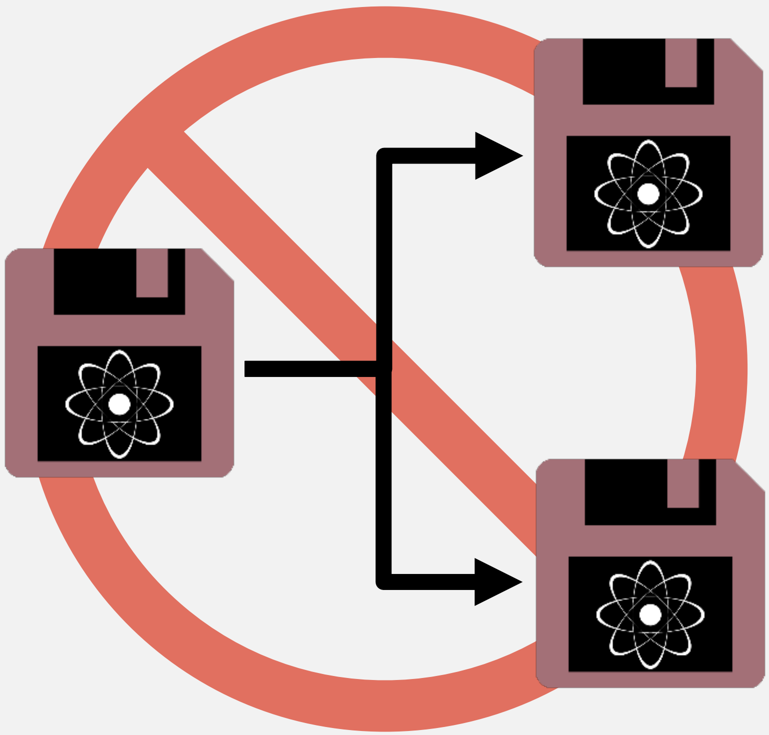
- Security for uncloneable encryption without the QROM.
- Show security for a indistinguishability-based definition
    - Instead of asking that Bob and Charlie simultaneously guess *m* (given the key) ask that they not be able to *both* distinguish an encryption of *m* from an encryption of a fixed message.
- Solve the "Uncloneable bit" problem:



Find a scheme where

$$\Pr(b_1 = b_2 = b) \to \frac{1}{2} \quad as\ n \to \infty$$

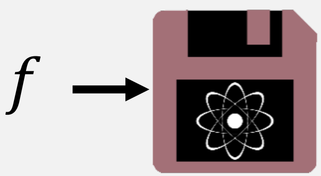
Uncloneable Functionality

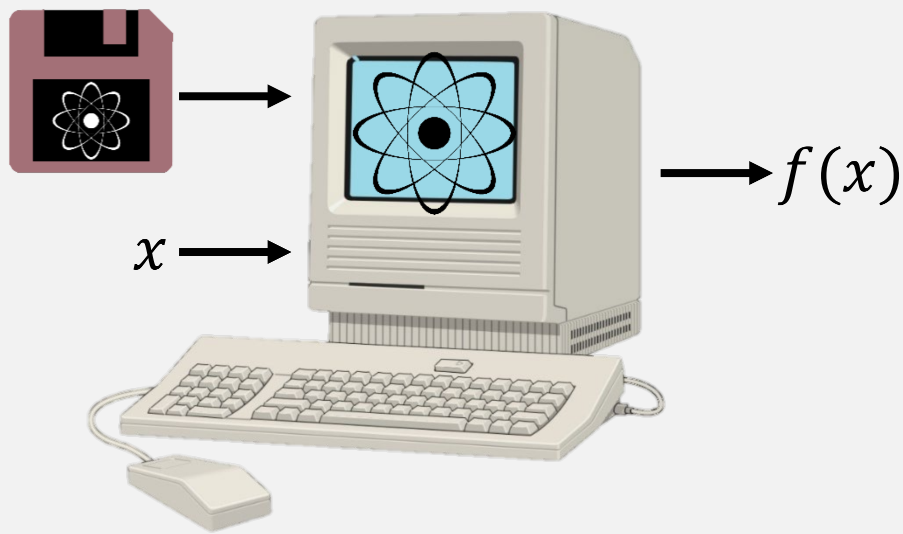


Copy-protected Software

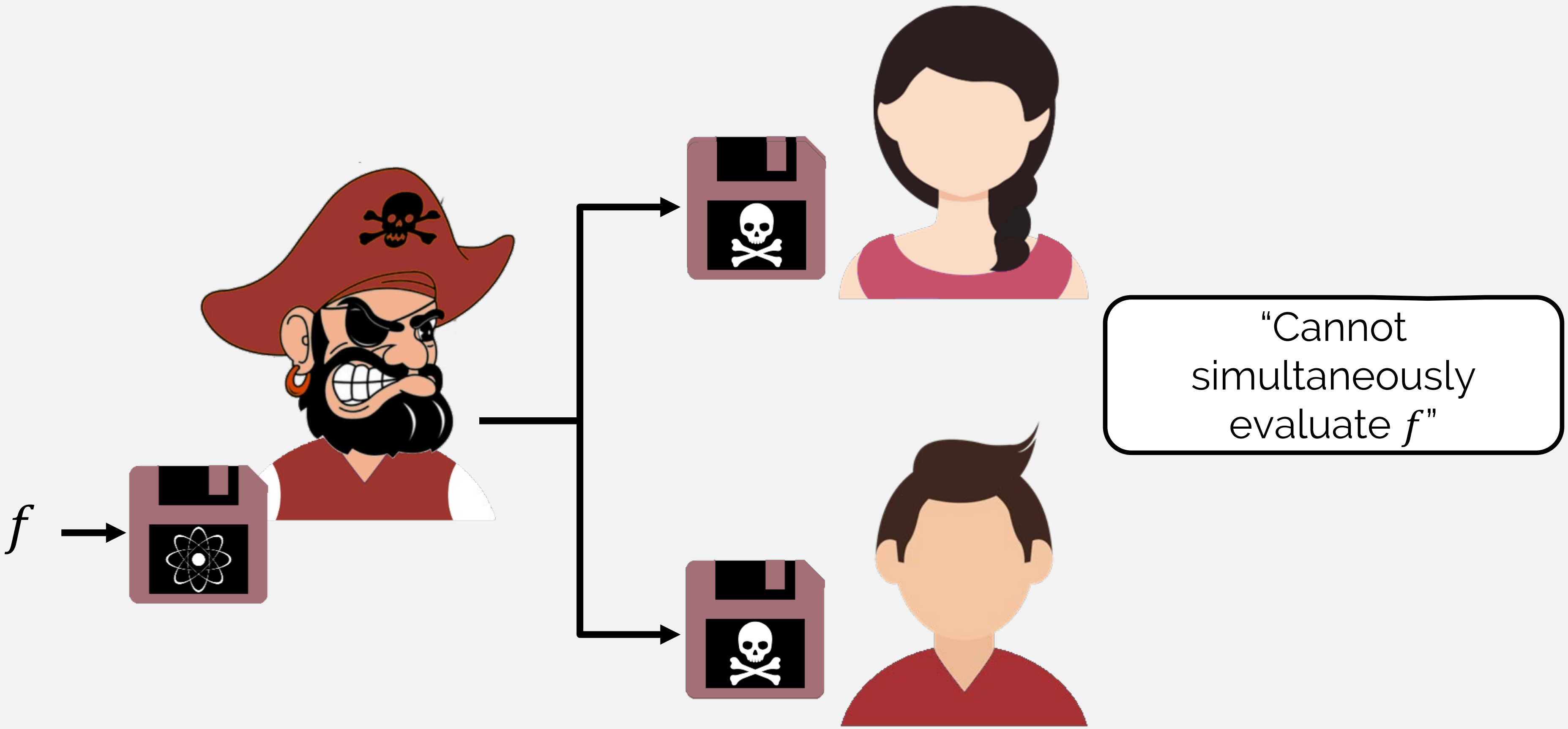
Aaronson (2009)

What is quantum copy protection?

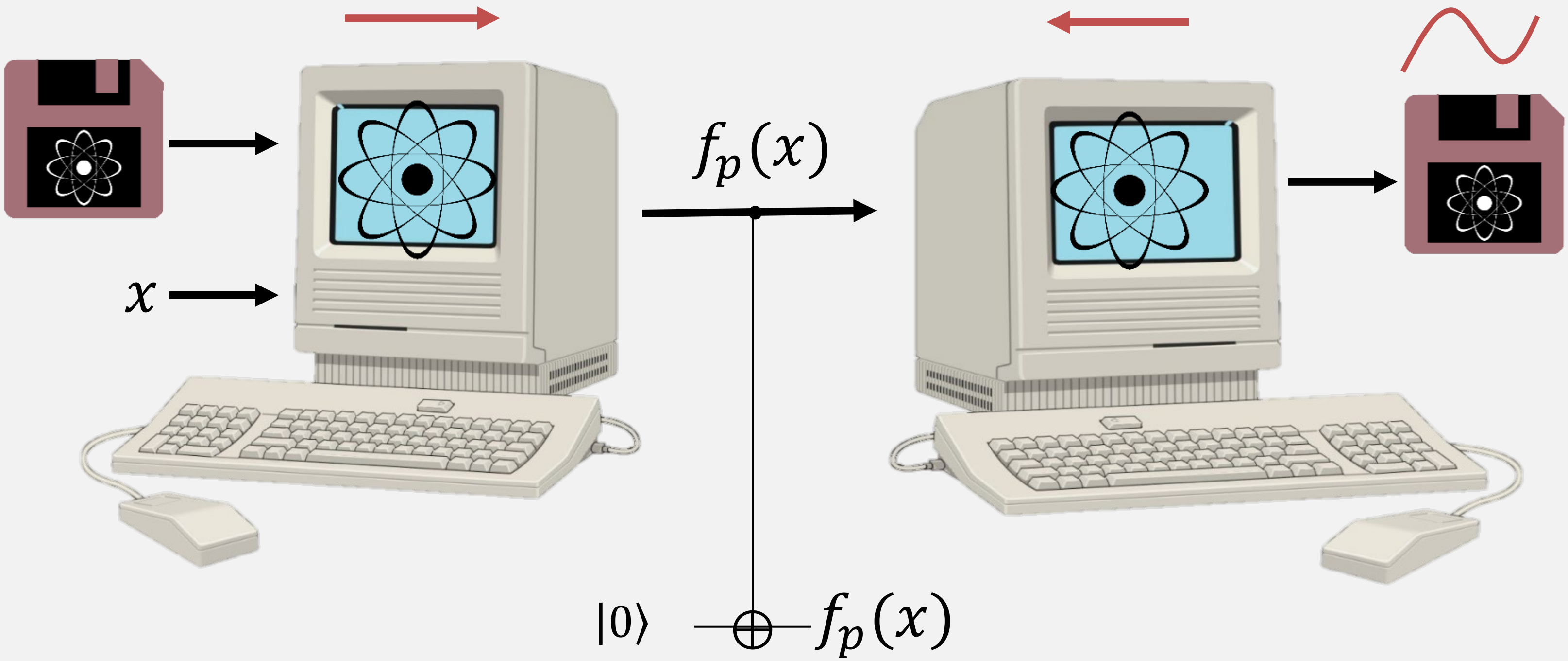




What is quantum copy protection?

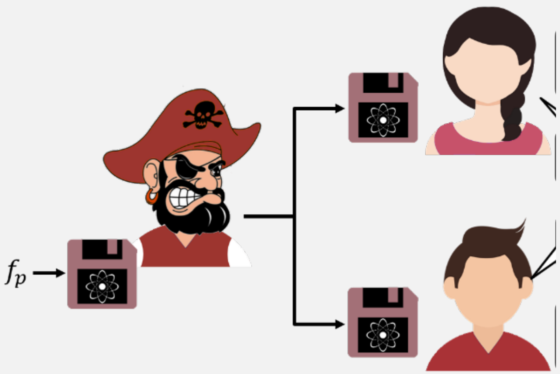


Quantum software is reusable to a certain extent



η-correctness implies output program is $O(\eta)$-close to original program

Limitations of Quantum Copy-Protection



Learnable Functions

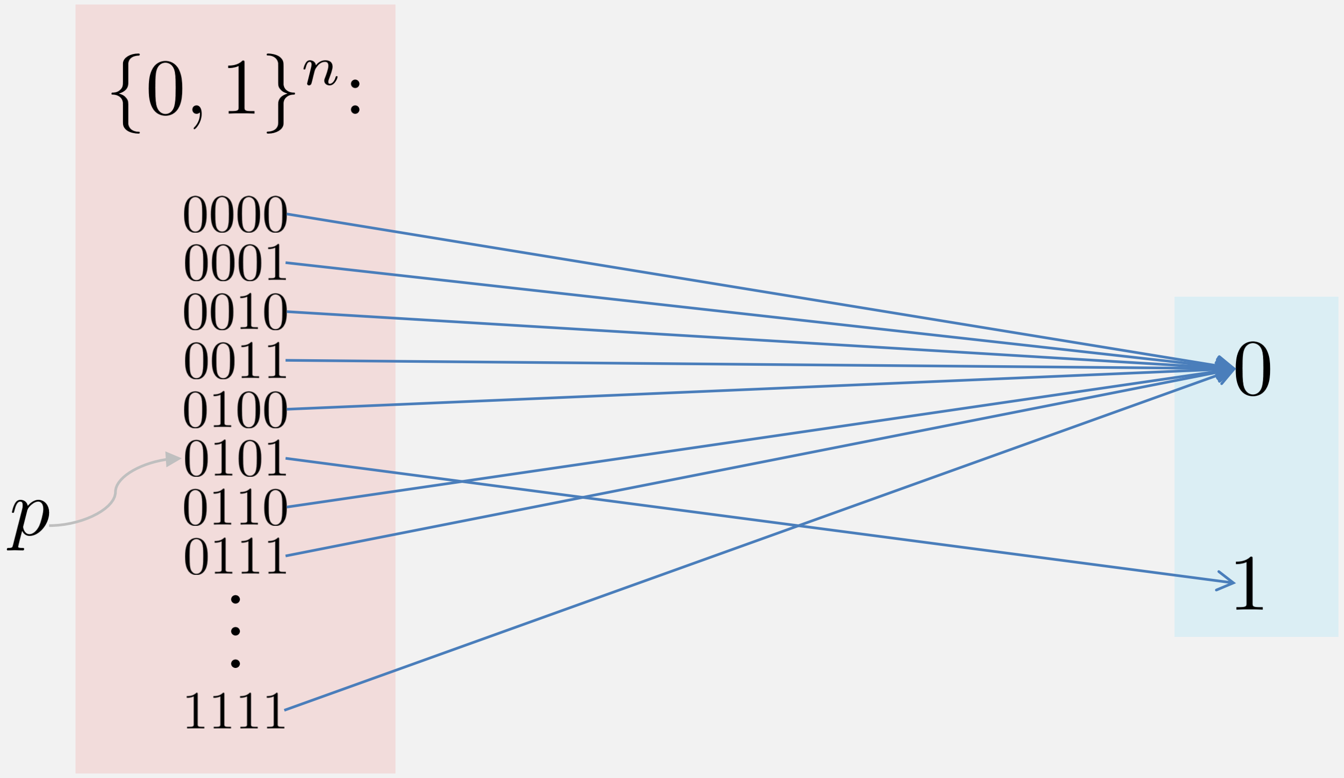
- Cannot be copy-protected

Perfectly correct ($\eta = 0$)

- Cannot be secure against unbounded adversaries

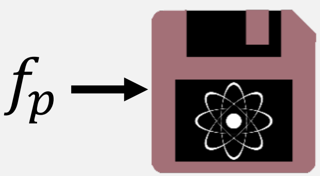
Point Functions

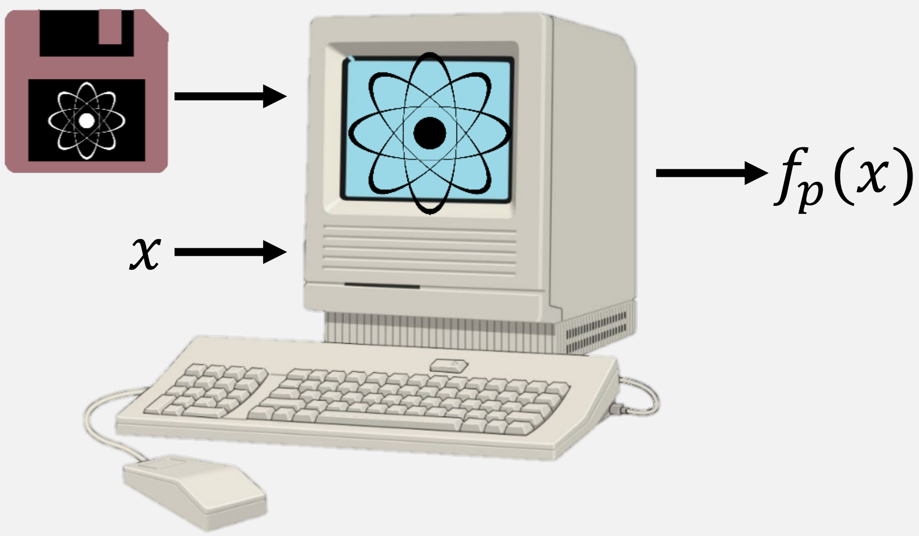
$$f_p : \{0,1\}^n \to \{0,1\}$$



*results hold for a more general class of functions called compute-and-compare (Colandangelo, Majenz, Poremba 2020)

What is quantum copy protection?



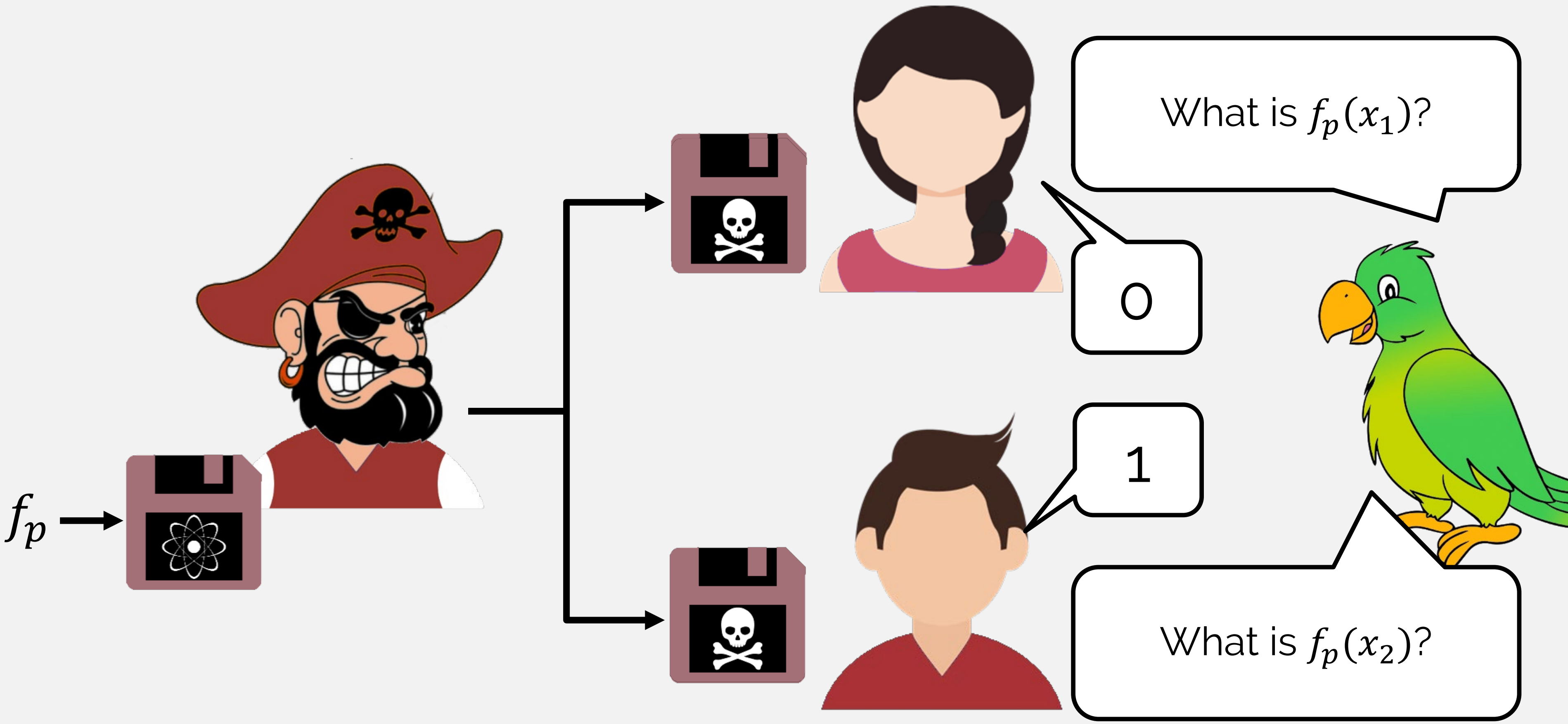


$$\Pr[x = p] = \frac{1}{2}$$

$$\Pr[x = p'] = \frac{1}{2(2^n - 1)}$$

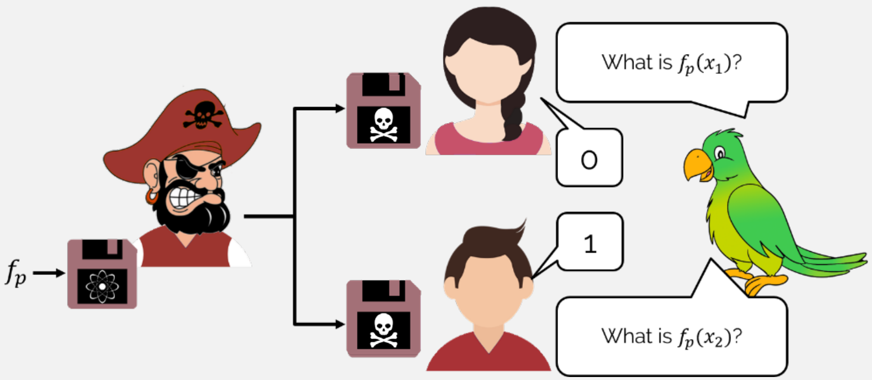
Average Correctness:
Up to some error term η, outcome is correct in expectation over choice of x.

What is quantum copy protection?



Coladangelo, Majenz and Poremba (2020)

What is copy protection?



Challenge Distribution

$$\Pr[x_i = p] = \frac{1}{2}$$

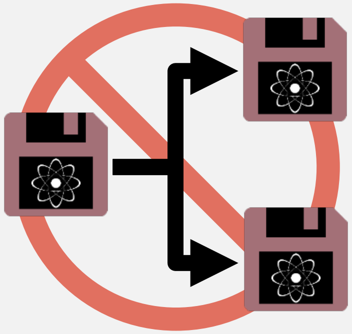
$$\Pr[x_i = p'] = \frac{1}{2(2^n - 1)}$$

$win \Leftrightarrow$ Alice outputs $f_p(x_1)$ AND Bob outputs $f_p(x_2)$

$$\epsilon - \text{security: } \Pr(win) \leq \frac{1}{2} + \epsilon$$

*can be generalized to other functions and challenge distributions

Results on Quantum Copy Protection

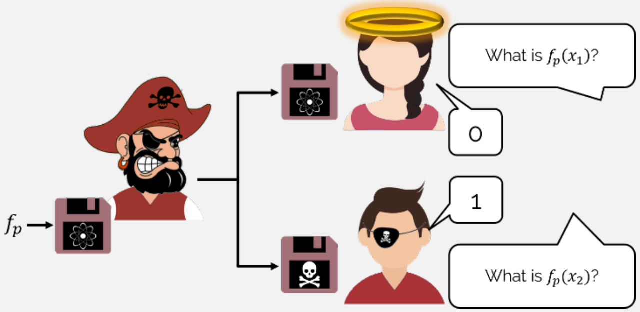


Aaronson 2009:
- All functions (not learnable)
- Assumes a quantum oracle

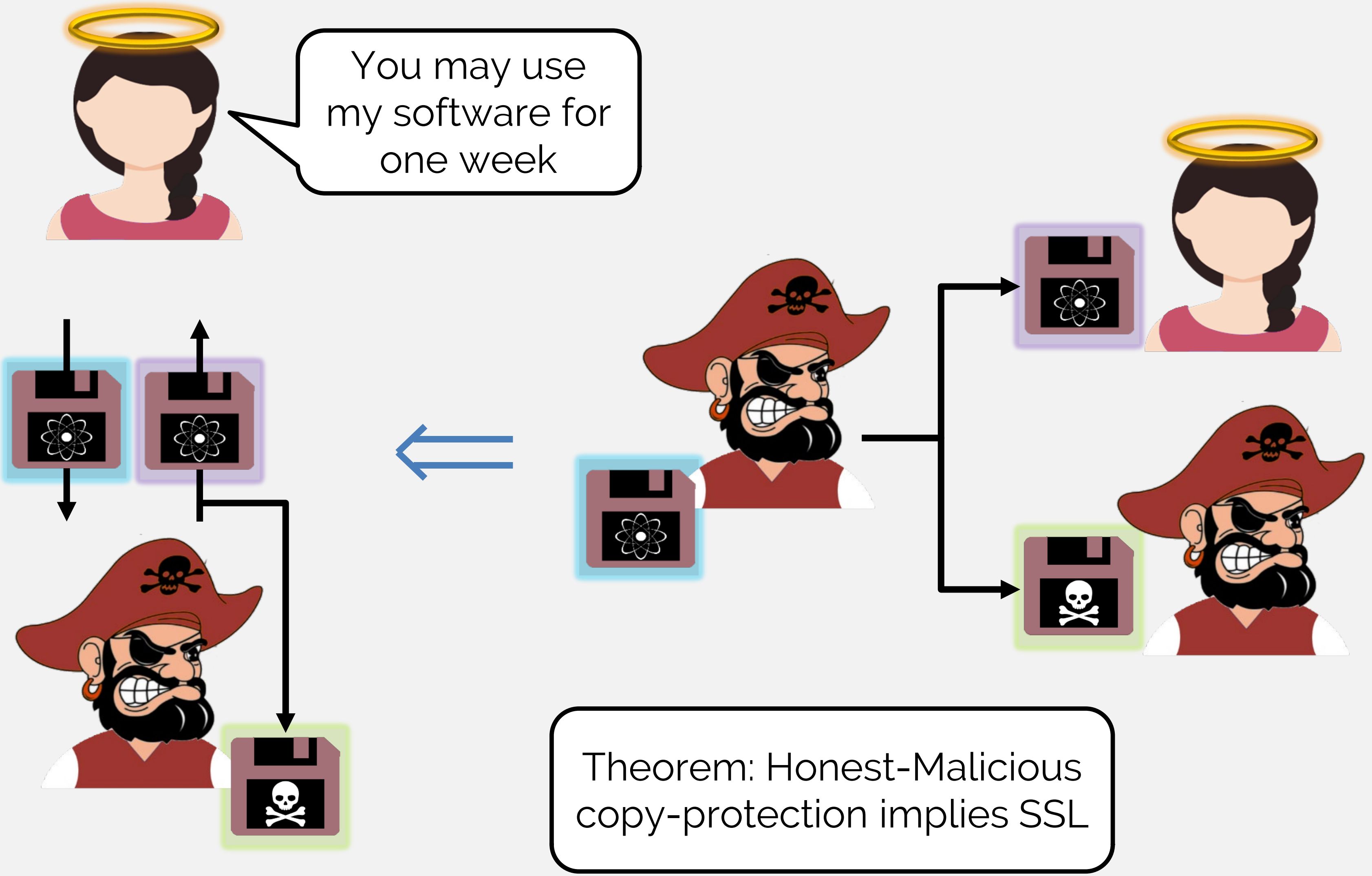
Aaronson, Liu, Liu, Zhandry, Zhang 2020:
- All functions (not learnable)
- Assumes a classical oracle

Coladangelo, Majenz, Poremba 2020:
- Point functions
- Assumes a quantum random oracle

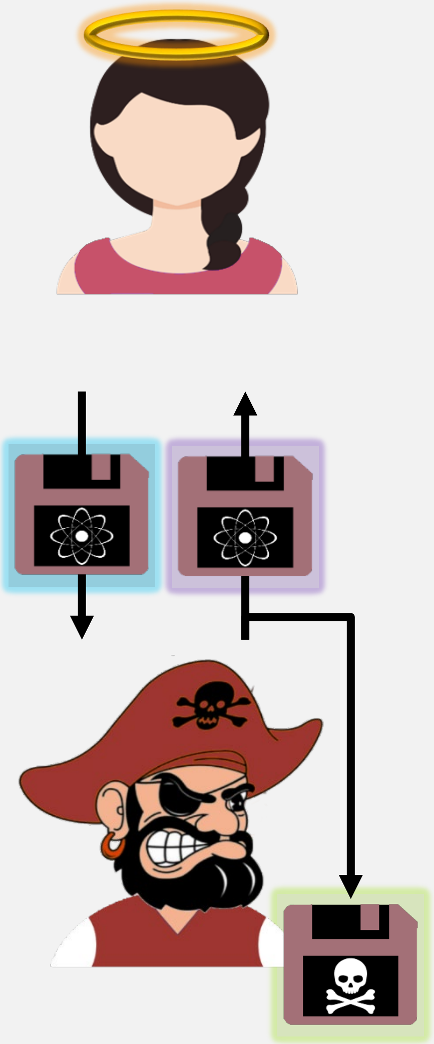
Broadbent, Jeffery, Lord, Podder, Sundaram 2021:
- Point Functions
- Restricted Class of Adversaries
  - "Honest-Malicious"
- No other assumptions



Secure Software Leasing



Secure Software Leasing



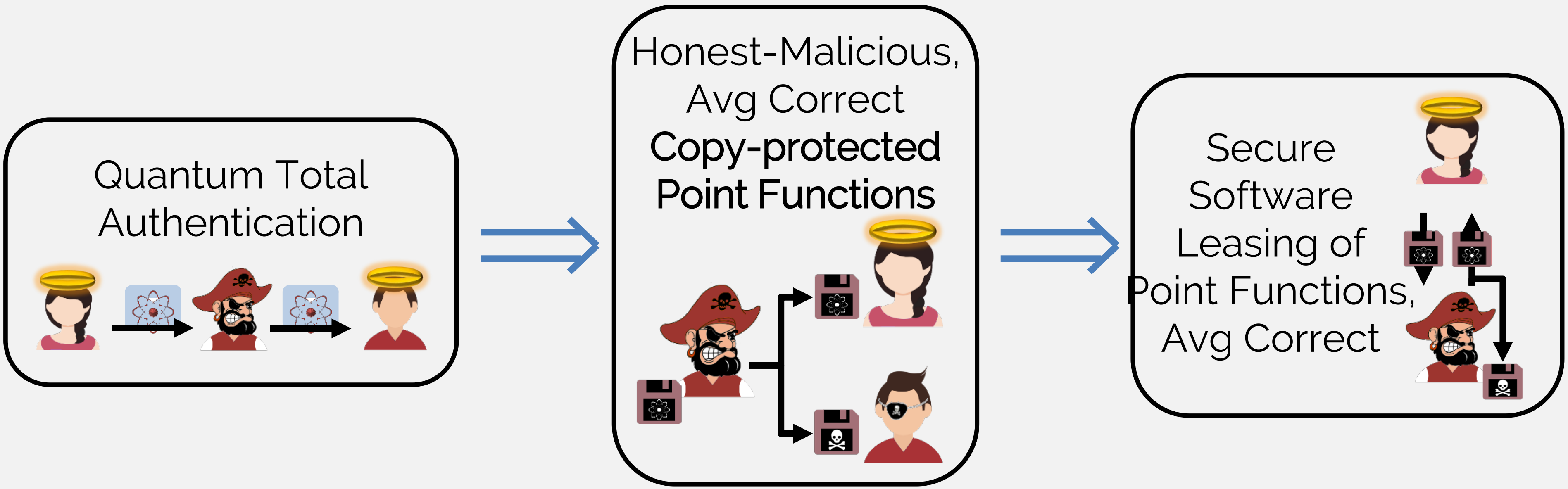
Ananth and La Placa (2020):
- impossibility of SSL in general
- Construction of SSL for point functions, against honest evaluators assuming:
    - quantum-secure subspace obfuscators
    - a common reference string,
    - difficulty of Learning With Errors (LWE)

Kitagawa, Nishimaki, and Yamakawa (2020):
- SSL against honest evaluators for point functions (and more)
    - Assuming LWE (only)

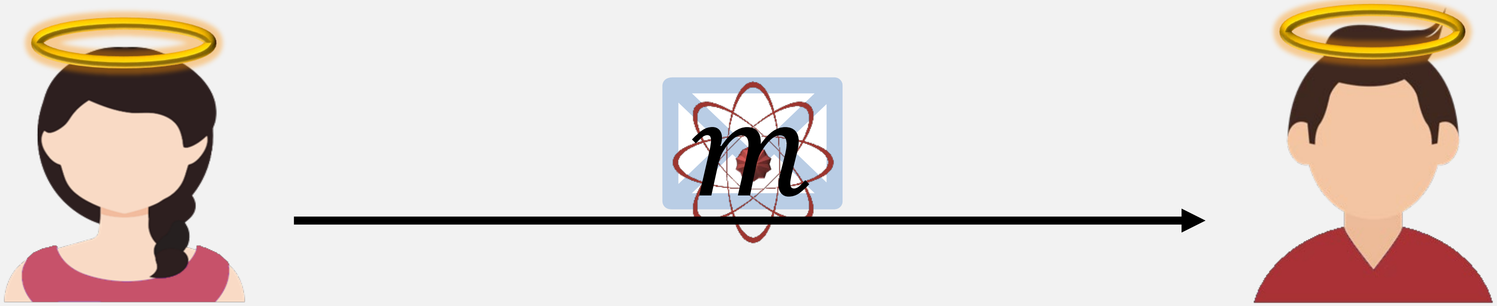
Coladangelo, Majenz and Poremba (2020):
- SSL for point functions, assuming:
    - Quantum Random Oracle

Broadbent, Jeffery, Lord, Podder,Sundaram (2021):
- SSL for point functions, average correctness
    - no assumptions

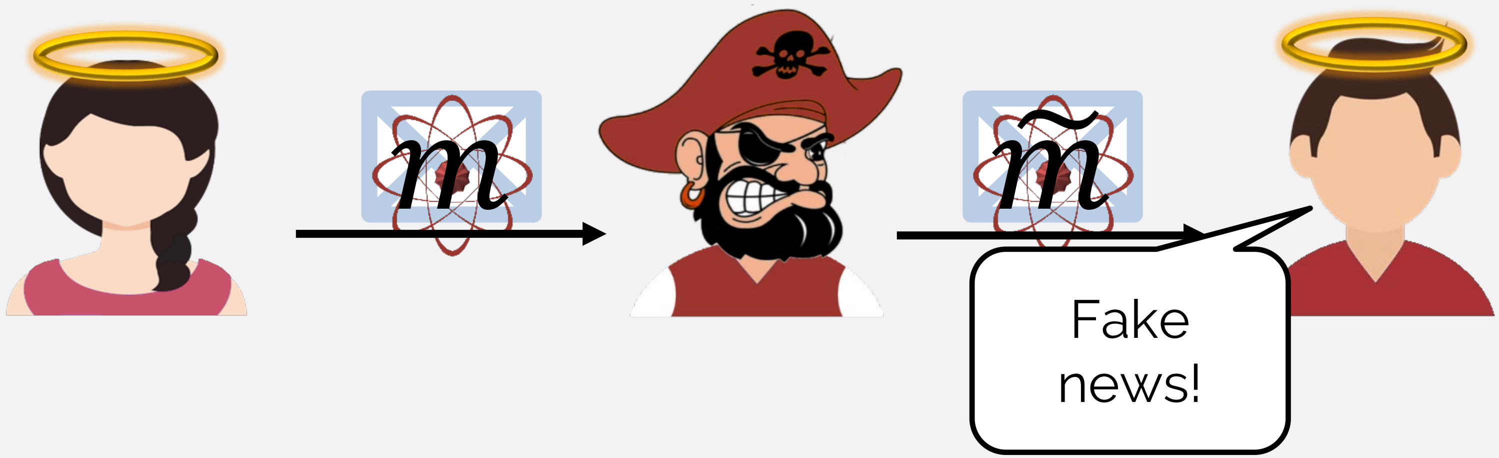
Achieving Honest-Malicious Copy-Protection



Quantum Message Authentication

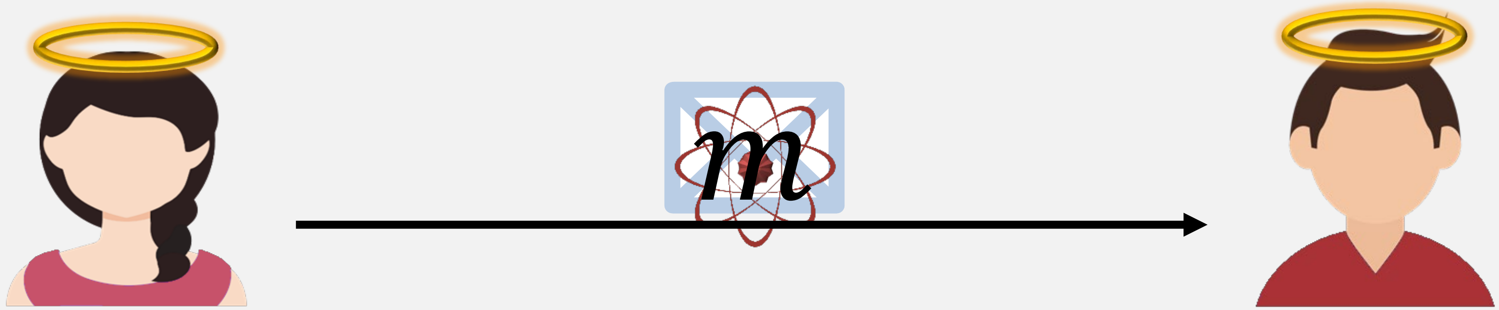


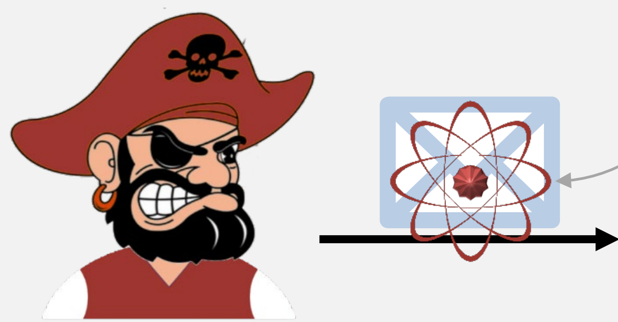
Quantum Message Authentication



Quantum Message Authentication

Quantum **Total** Authentication





nothing to
do with m
or with k

Garg, Yuen, and Zhandry (2017)

Quantum **Total** Authentication

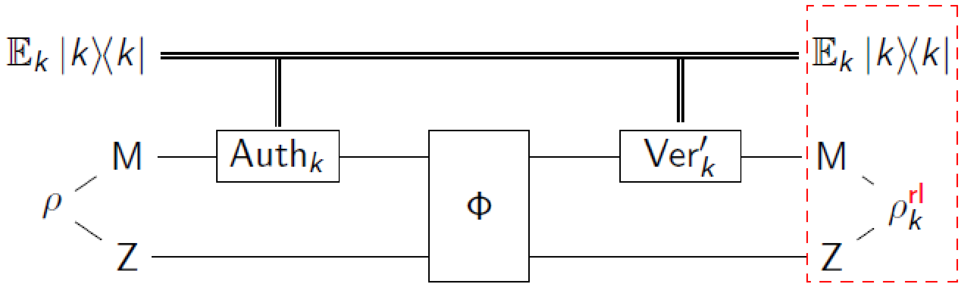


Figure: A real adversary, conditioned on acceptance.

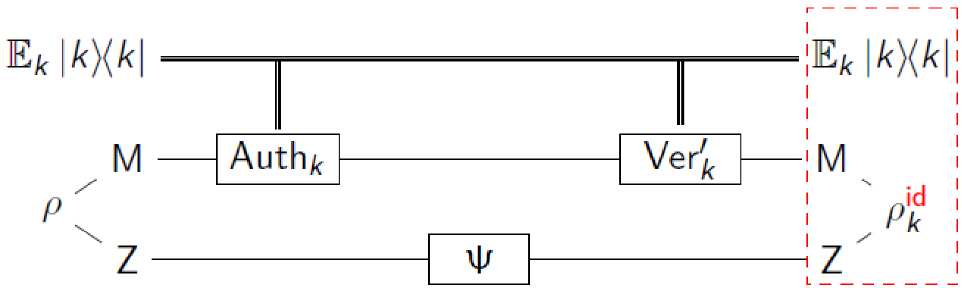


Figure: An ideal adversary, conditioned on acceptance.

- Correctness:

$$\mathrm{Ver}_k \circ \mathrm{Auth}_k(\rho) = \rho \otimes |\mathrm{A}\rangle\langle\mathrm{A}|$$

- $\mathrm{Ver}'_k = \mathrm{Ver}_k$ cond. on accept.
- Security:
  Real and ideal outputs are ϵ-close in trace distance:

$$\mathop{\mathbb{E}}_k |k\rangle\langle k| \otimes \rho_k^{\mathrm{rl}} \approx_\epsilon \mathop{\mathbb{E}}_k |k\rangle\langle k| \otimes \rho_k^{\mathrm{id}}$$

Total authentication is realized by 2-designs (Alagic and Majenz 2017) ,
and the strong trap code (Dulek, Speelman 2018).

Copy Protection from Quantum Total Authentication

Point function f_p: $\{0,1\}^n \to \{0,1\}, f_p(q) = 1 \Leftrightarrow p = q$
Let $\mathrm{Auth}_k, \mathrm{Verf}_k$ be ϵ- secure Quantum Total Authentication Scheme
Idea: Point function on point $p \leftrightarrow \mathrm{Auth}_p$ and Verf_p on fixed state $|\psi\rangle$

CP.Protect

On input of $f_p : \{0,1\}^n \to \{0,1\}$:

1. Output $\mathrm{Auth}_p(|\psi\rangle\langle\psi|)$.

CP.Eval

On input of σ and q:

1. Compute $\mathrm{Verf}_q(\sigma)$.
2. Output 1 if and only if the verification accepts.

Correctness

- By correctness of the authentication scheme:

$$\Pr[\mathrm{CP.Eval}(\mathrm{CP.Protect}(f_p), p) = 1] = 1$$

- By properties of the authentication scheme:

$$\mathop{\mathbb{E}}_{q} \Pr[\mathrm{CP.Eval}(\mathrm{CP.Protect}(f_p), q) = 0] \geq 1 - 2\epsilon$$

- Note: We achieve correctness averaged over all inputs, not necessarily for all inputs.

Quantum Copy-Protection Open Problems

1. Standard correctness for copy protection without assumptions?
2. Security for copy protection without assumptions, against **two** malicious evaluators?
3. Unconditional SSL for functions beyond compute-and-compare?
4. NISQ-ready Quantum Copy-Protection?