Quantum Unclonability

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
*additional thanks for providing materials for this presentation

QCrypt 2021
Amsterdam, Netherlands
(online)
August 26, 2021

Quantum States Can't be Cloned

Quantum rewinding
Quantum oracle queries

Quantum money
Quantum encodings
Copy-protected software

What is unclonability?

"Uncloneability"vs.
"unclonability"?

Aaronson (2016)
Qcrypt 2016 after-
dinner speech

Quantum Information

Can be tasted, but this leaves a mark.

Can be shared, but there is a total of
1 item to be shared.

Cannot be copied.

Conventional Information

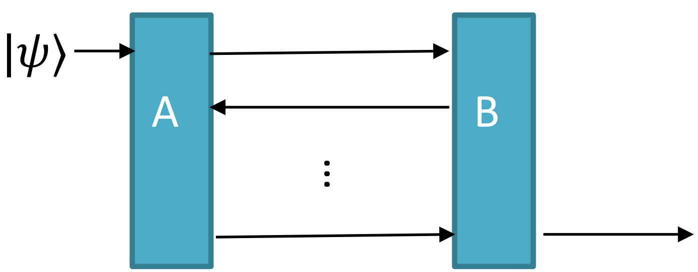
Can be observed without changing it.

Can be shared at will.

Can be copied.

Annoyances of quantum unclonability

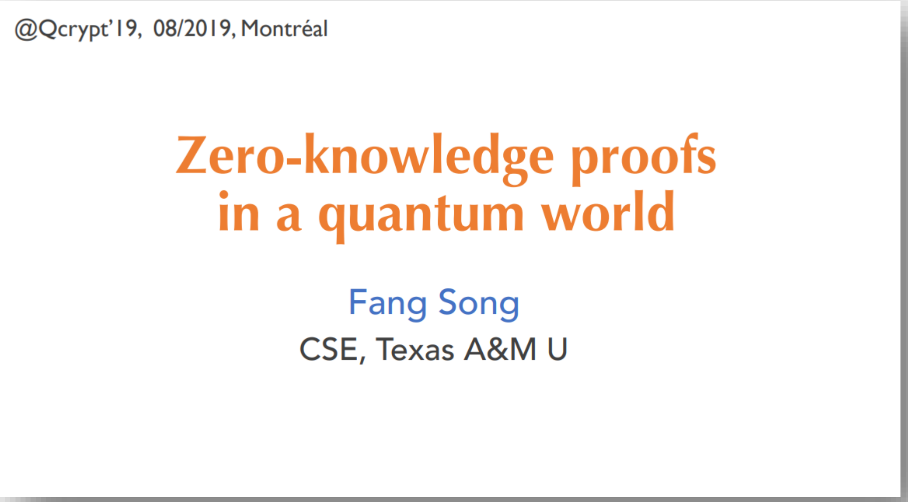
Contrary to the classical case, We cannot in general keep a transcript of a quantum interaction.



Unclonability and Zero-Knowledge

In Zero-Knowledge (ZK), a common technique is **rewinding** (returning to a prior point in the interaction whenever some “wrong” path is taken)

- **not** directly applicable in the quantum case (measurement disturbs the rewinding process)
- Watrous (2009): A quantum rewinding technique: “Quantum-secure ZK for all NP”.



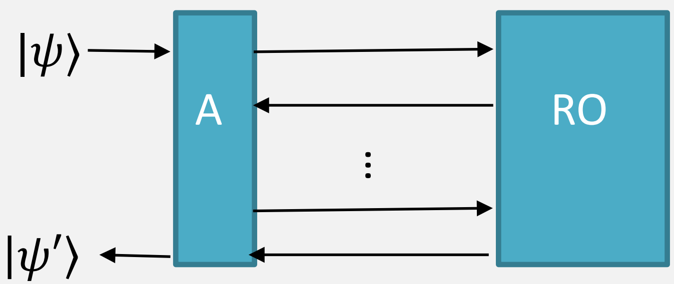
Post-Quantum Succinct Arguments
Alessandro Chiesa; Fermi Ma; Nicholas Spooner; Mark Zhandry

A Black-Box Approach to Post-Quantum Zero-Knowledge in Constant Rounds
Nai-Hui Chia; Kai-Min Chung; Takashi Yamakawa
merged with
On the Impossibility of Post-Quantum Black-Box Zero-Knowledge in Constant Rounds
Nai-Hui Chia; Kai-Min Chung; Qipeng Liu; Takashi Yamakawa

Post-quantum Resettably-Sound Zero Knowledge
Nir Bitansky; Michael Kellner; Omri Shmueli

Unclonability and Quantum Random Oracle (QROM)

f uniformly random



Recording barrier: not possible in general to record quantum oracle queries

Mark L. Zhandry: Quantum techniques in post-quantum crypto (invited talk @ Qcrypt 2019) + " How to record quantum queries" (Crypto 2019)

On the Compressed-Oracle Technique, and Post-Quantum Security of Proofs of Sequential Work
Kai-Min Chung; Serge Fehr; Yu-Hsuan Huang; Tai-Ning Liao

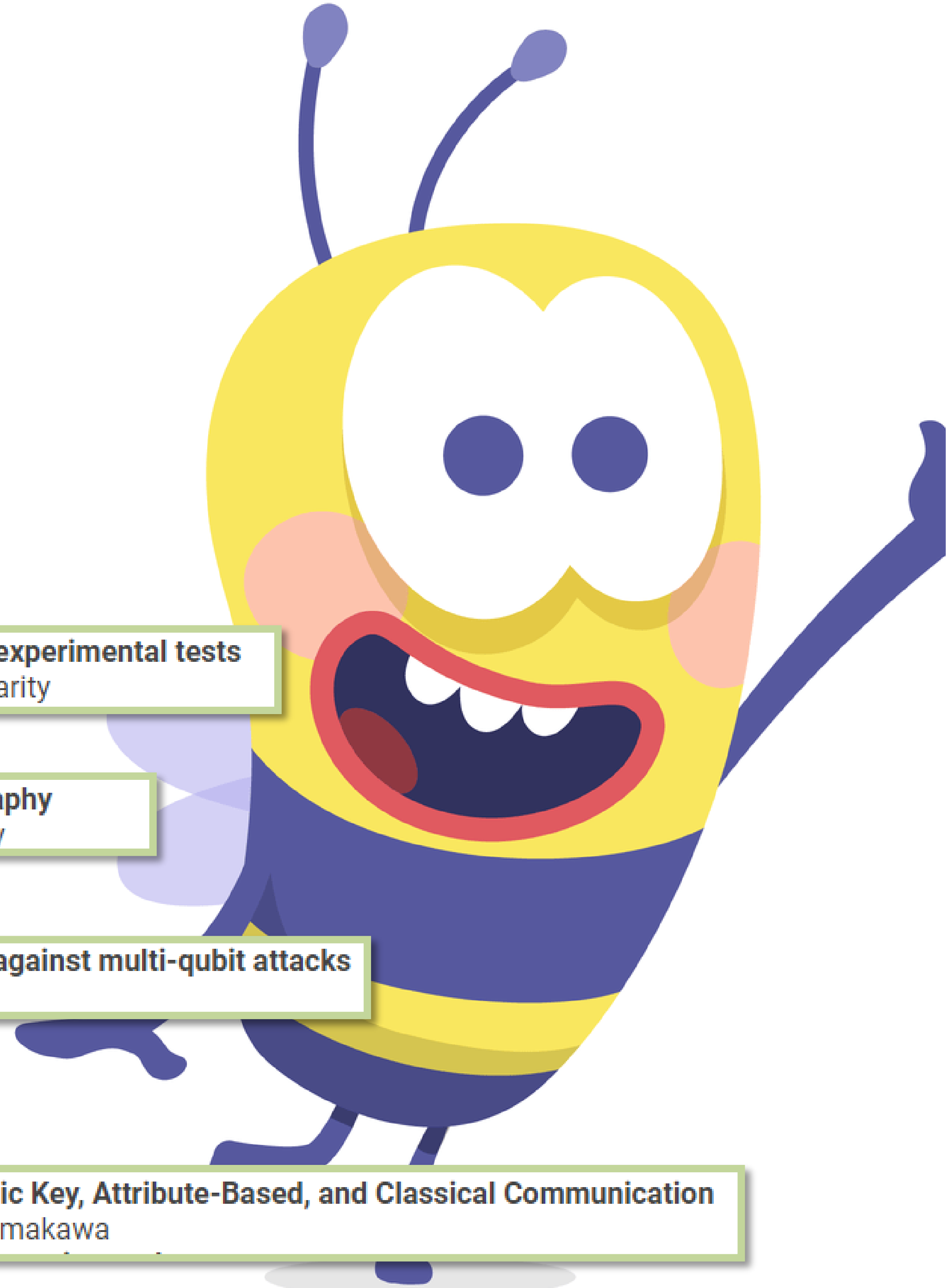
Advantages of quantum unclonability

All of QKD

Practical quantum tokens without quantum memories and experimental tests
Adrian Kent; David Lowndes; Damián Pitalúa-García; John Rarity

Hidden Cosets and Applications to Unclonable Cryptography
Andrea Coladangelo; Jiahui Liu; Qipeng Liu; Mark Zhandry

Position-based cryptography: Single-qubit protocol secure against multi-qubit attacks
Andreas Bluhm; Matthias Christandl; Florian Speelman



Quantum Encryption with Certified Deletion, Revisited: Public Key, Attribute-Based, and Classical Communication
Taiga Hiroka; Tomoyuki Morimae; Ryo Nishimaki; Takashi Yamakawa

Written in 1968
Published 1983

Shtetl-Optimized

The Blog of Scott Aaronson

If you take nothing else from this blog: quantum computers won't solve hard problems instantly by just trying all solutions in parallel.

Also, next pandemic, let's approve the vaccines faster!

PSPACE
PostBQP
NP
BQP
P

« Yet more mistakes in papers

Stephen Wiesner (1942-2021)

Photo credit: Lev Vaidman

Wiesner's conjugate coding

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

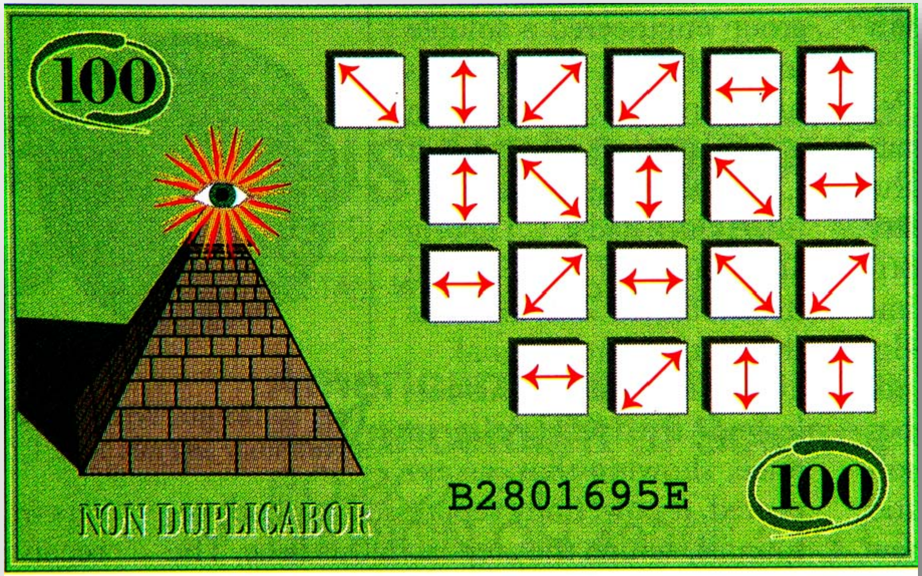
$\boldsymbol{\theta}$	$\boldsymbol{b}$	$\boldsymbol{|b\rangle_\theta}$
0	0	$|0\rangle$
0	1	$|1\rangle$
1	0	$|+\rangle$
1	1	$|-\rangle$

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 $\theta = \theta_1\theta_2 \dots \theta_n$, $b = b_1 b_2 \dots b_n$, define
$|b\rangle_\theta = |b_1\rangle_{\theta_1} \otimes |b_2\rangle_{\theta_2} \dots \otimes |b_n\rangle_{\theta_n}$

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.

CONJUGATE CODING GOES BIG TIME

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

“BB84 quantum key distribution”

Quantum Key Distribution

Bennett and Brassard (1984)

Quantum Key Distribution

Bennett and Brassard (1984)

Quantum Key Distribution

Bennett and Brassard (1984)

Quantum Key Distribution

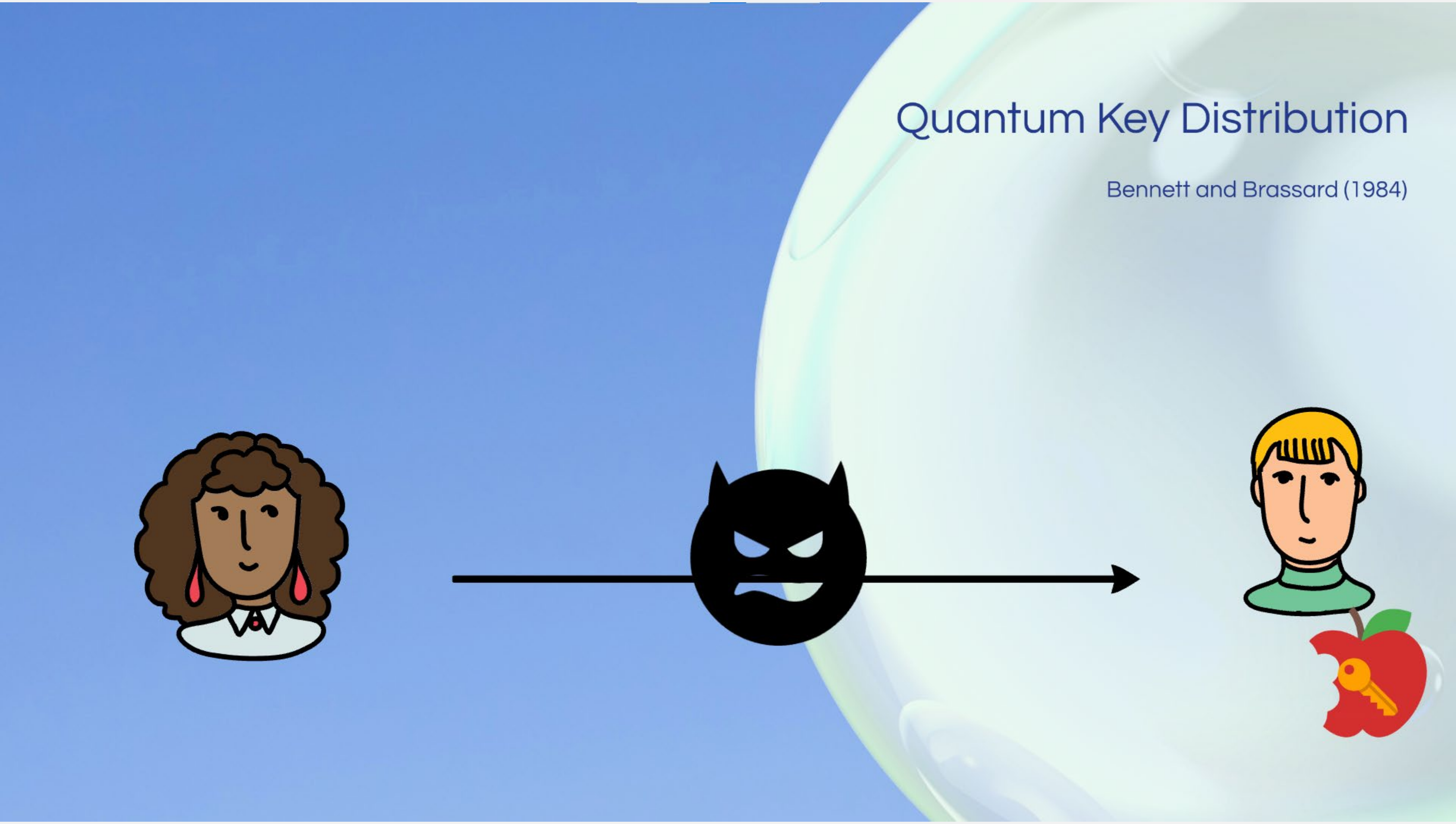
Bennett and Brassard (1984)

Quantum Key Distribution

Bennett and Brassard (1984)

Quantum Key Distribution

Bennett and Brassard (1984)



Assumption: trusted apples

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.

Wiesner's security argument

Could there be some way of duplicating the money without learning the sequence N_i? No, because if one copy can be made (so that there are two pieces of the money) then many copies can be made by making copies of copies. Now given an unlimited supply of systems in the same state, that state can be determined. Thus, the sequence N_i could be recovered. But this is impossible.

Written in 1968
Published 1983

The Quantum No-cloning Theorem

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

Theorem: No 2-qubit unitary U exists such that for all single-qubit states $|\psi\rangle$, $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$.

Proof by contradiction.
Suppose such a U exists.
Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

$$\begin{aligned} U|\psi\rangle|0\rangle &= |\psi\rangle|\psi\rangle \\ &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle \qquad (*) \end{aligned}$$

Buy U also clones $|0\rangle$ and $|1\rangle$:

$$\begin{aligned} U|00\rangle &= |00\rangle \\ U|10\rangle &= |11\rangle \end{aligned}$$

By linearity, $U(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha U|00\rangle + \beta U|10\rangle = \alpha|00\rangle + \beta|11\rangle$
This contradicts (*) (*e.g.*, take $\alpha = \beta = \frac{1}{\sqrt{2}}$).

What is uncloneability?

What is security?

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

Probabilistic Encryption*

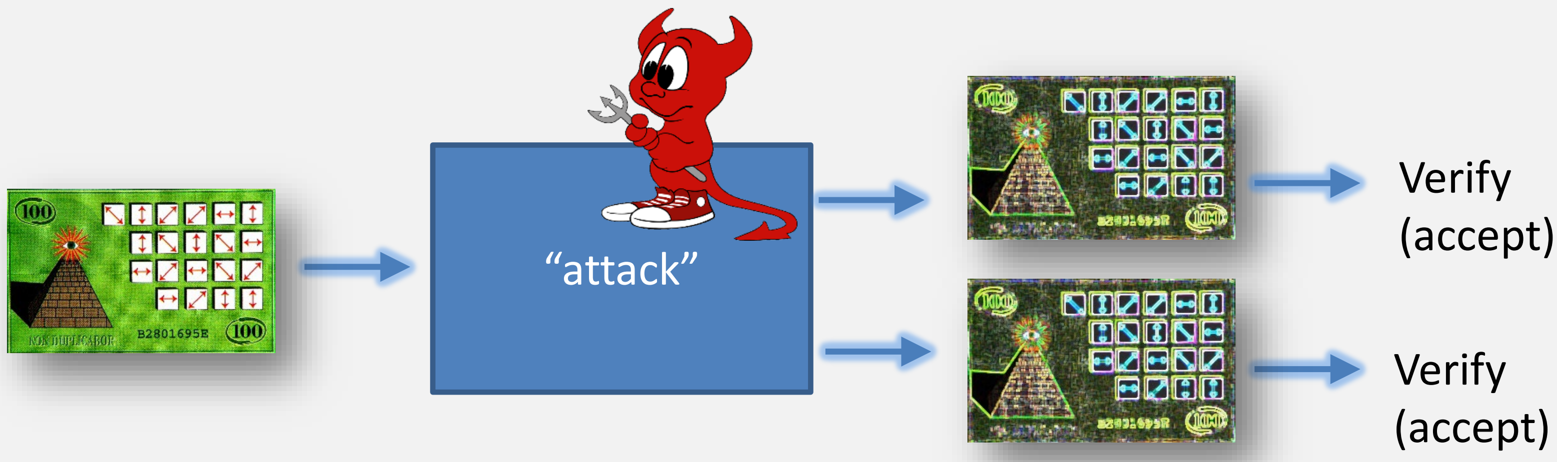
SHAFI GOLDWASSER AND SILVIO MICALI

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”

Security of Wiesner’s quantum money

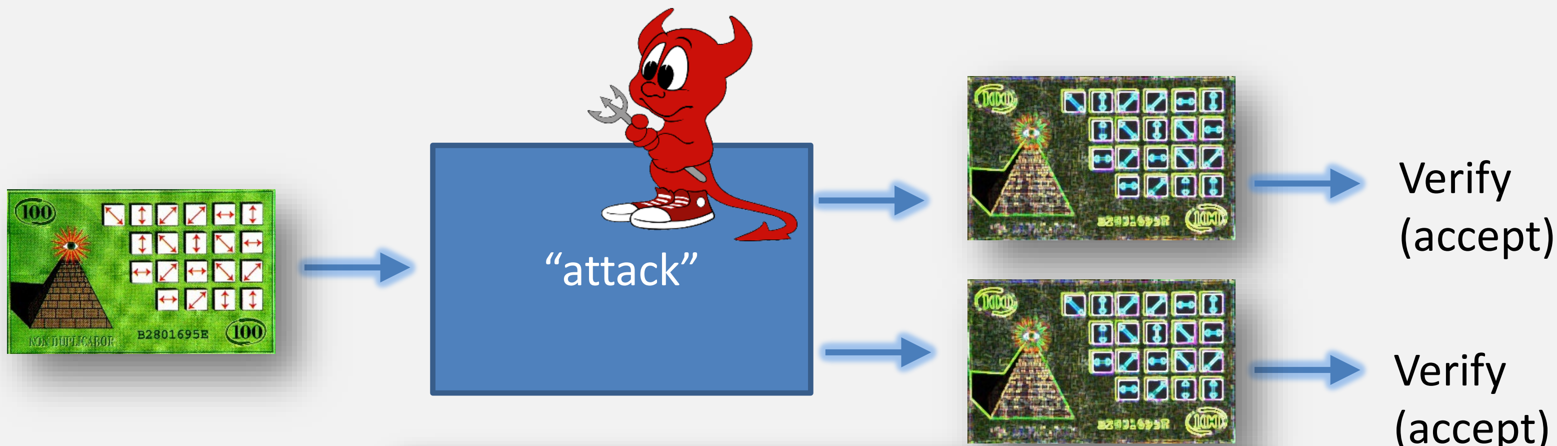


How does the difficulty of cloning quantum money scale with the number of qubits, n?

*special case of the “quantum cloning” problem.

“Universal Quantum Cloner”: optimize over **all possible** inputs.
(see survey by Scarani, Gisin, Acin (2005))

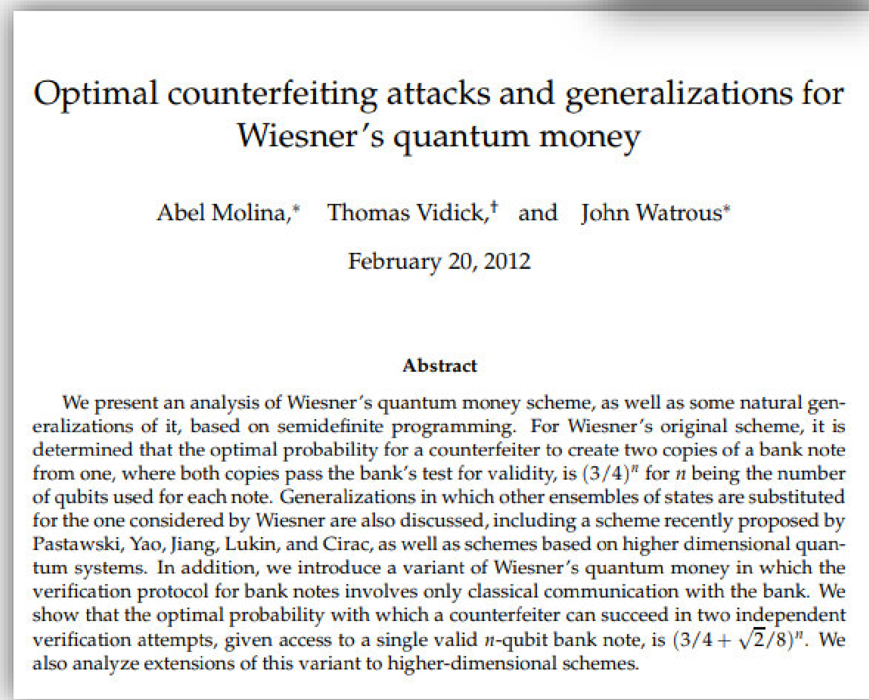
Security of Wiesner’s quantum money



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)

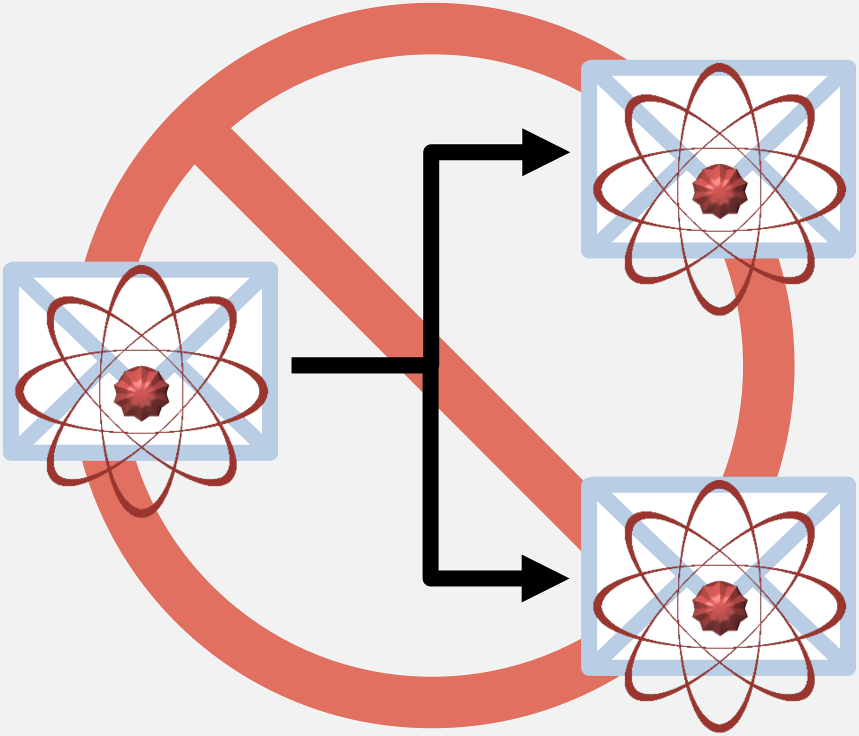
Quantum Money with classical verification

- Gavinsky (2012)

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

- Farhi, Gosset, Hassidim, Lutomirski, and Shor (2012)
- Aaronson and Christiano (2012)
- Zhandry (2019)

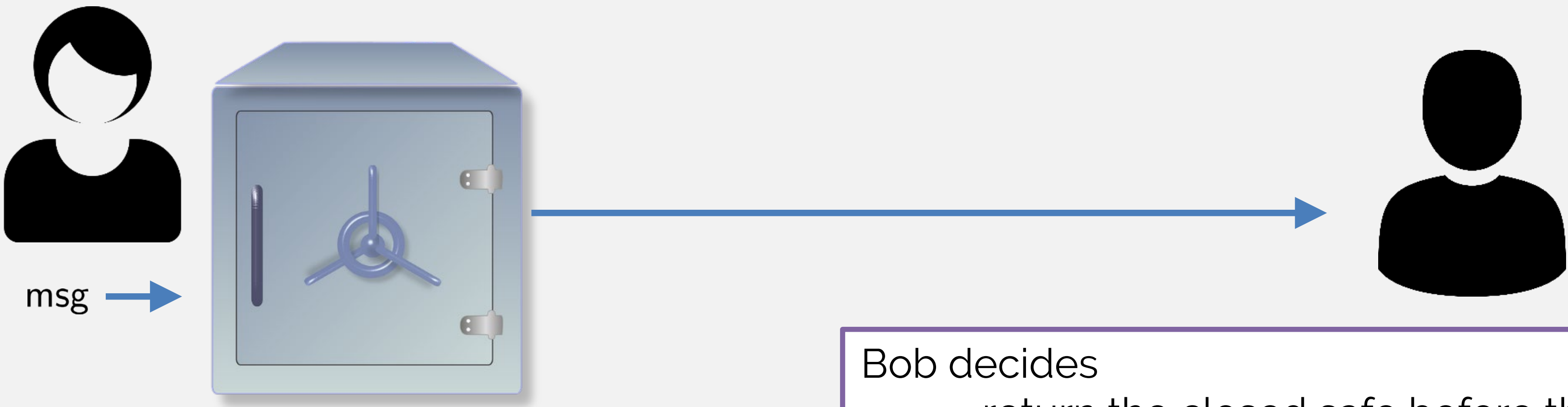
Uncloneable Information



1. Certified Deletion
2. Unclonable Encryption
3. Unclonable Decryption

1. 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

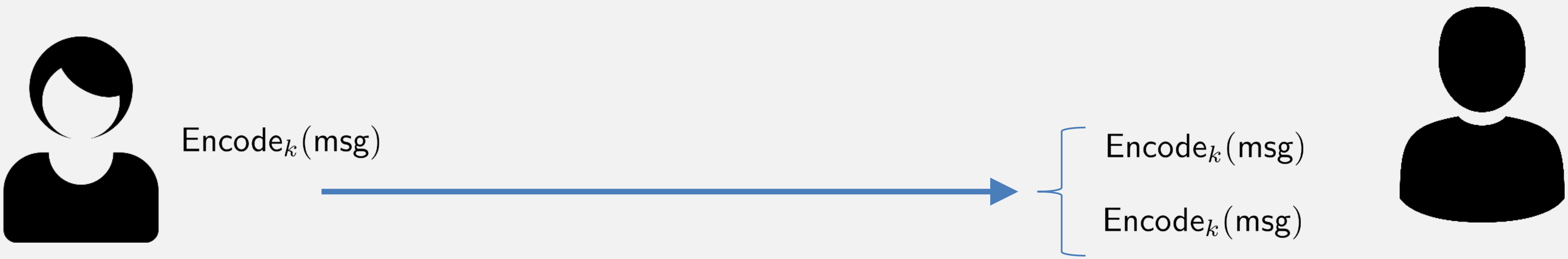
XOR

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

Can we achieve this in a digital world?

Broadbent, Islam (2020)

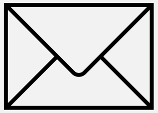
Can we achieve this in a digital world?
No!
Proof by contradiction…



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

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

Certified Deletion
-application



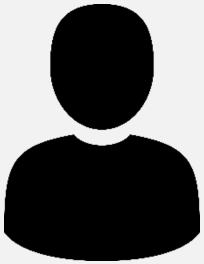
Alice's
Last Will and Testament

1. Alice can use Certified Deletion to store her will with a lawyer.
   - When she wants to **update** to a new will, the lawyer first **proves deletion.**

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 $\lvert r\rangle_\theta, m \oplus r_{comp}$

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

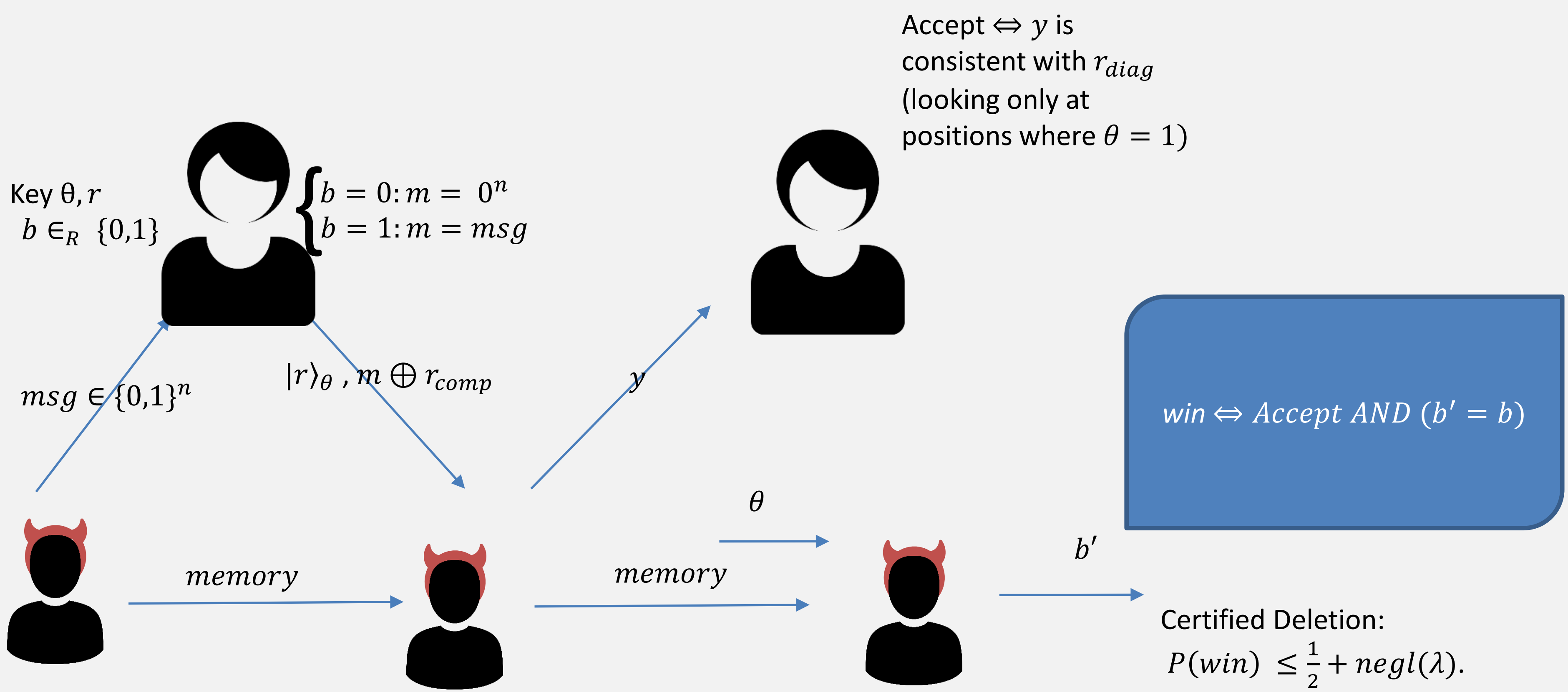
As the probability of predicting r_{diag} increases (i.e. adversary produces convincing "proof of deletion")

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

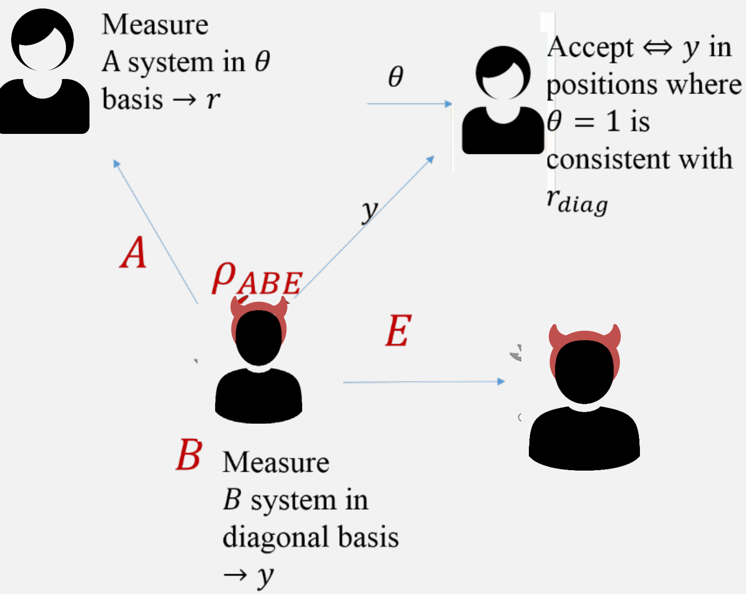
The probability of guessing r_{comp} decreases (i.e. adversary is unable to decrypt, even given the key)

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:

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

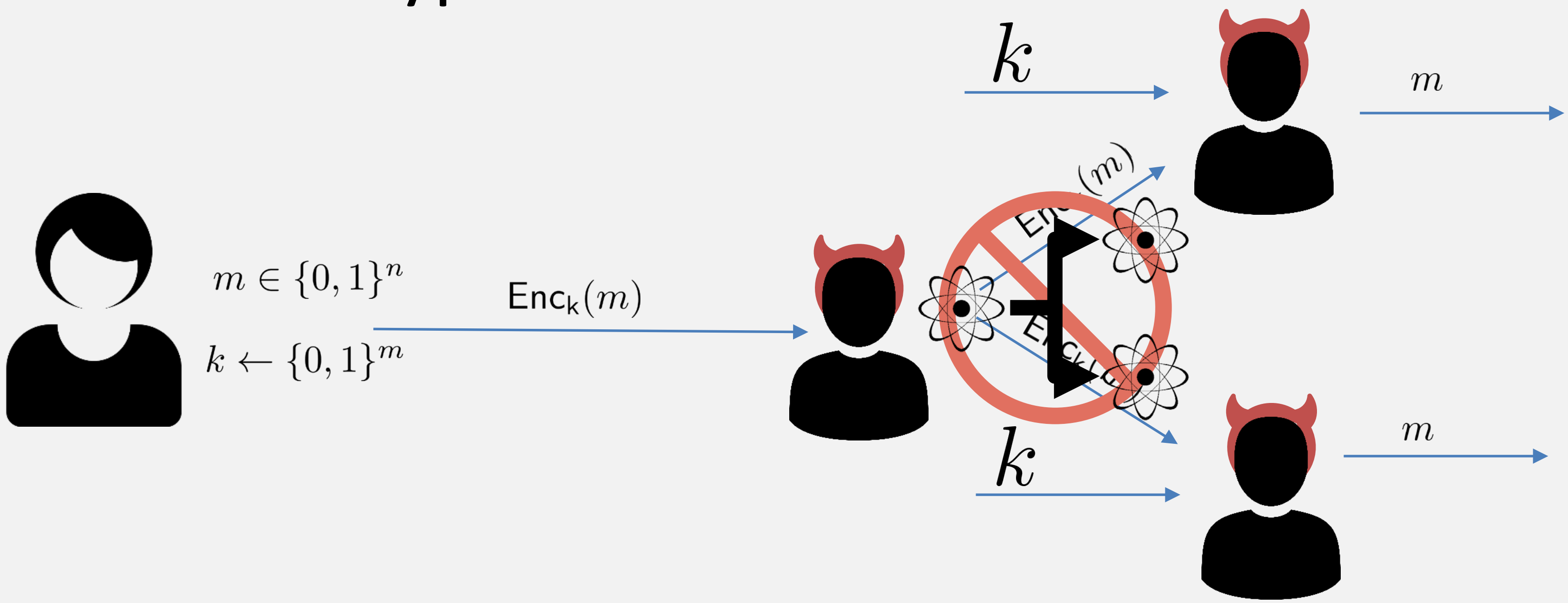
-noise tolerance: Accept y if less than $k\delta$ bits are wrong; use **error correction**.

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

Quantum Encryption with Certified Deletion, Revisited: Public Key, Attribute-Based, and Classical Communication
Taiga Hiroka; Tomoyuki Morimae; Ryo Nishimaki; Takashi Yamakawa

2. Unclonable Encryption

When encryption is classical:

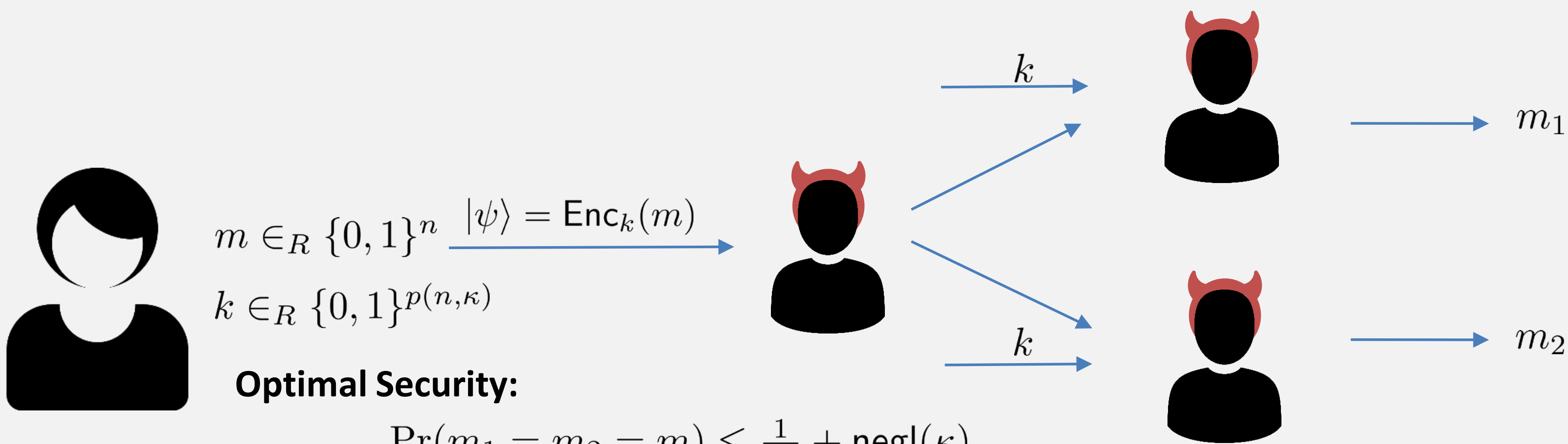


Classical ciphertexts can be copied, hence it is always possible for the adversary and the honest party to perfectly decrypt, given k.

Gottesman (2002)
Broadbent, Lord (2020)

Uncloneable Encryption Security Game

Figure of merit is how well two adversaries can predict m (different from quantum cloning)



Optimal Security:

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

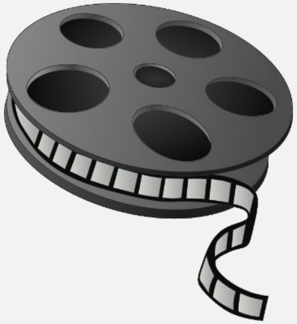
Conjugate-encoding based scheme (in the Quantum Random Oracle Model (QROM): [Broadbent, Lord 2020]

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

117. **Limitations on Uncloneable Encryption and Simultaneous One-Way-to-Hiding**
Christian Majenz (CWI, QuSoft); Christian Schaffner (University of Amsterdam, QuSoft); Mehrdad Tahmasbi (University of Amsterdam, QuSoft)

➢ Bound could be tightened, but not below 9/8.

Uncloneable Encryption -application

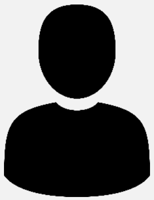


1. Alice uses uncloneable encryption and distributes an encrypted movie ahead of the movie release date.
2. The day of release, she reveals the key.
3. Thanks to uncloneable encryption, she is sure that at most one recipient* can decrypt the movie.

*assuming no communication after key reveal

Uncloneable Encryption Basic Protocol

θ, b



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

$|b \oplus m\rangle_\theta$

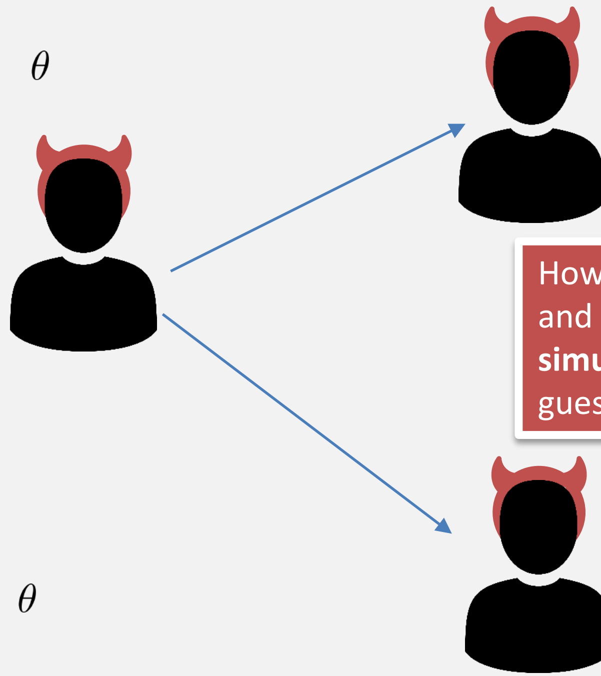
Measure received qubits in basis θ;
Let the result be y.

Output $y \oplus b = m$

Uncloneable Encryption Scheme + Security

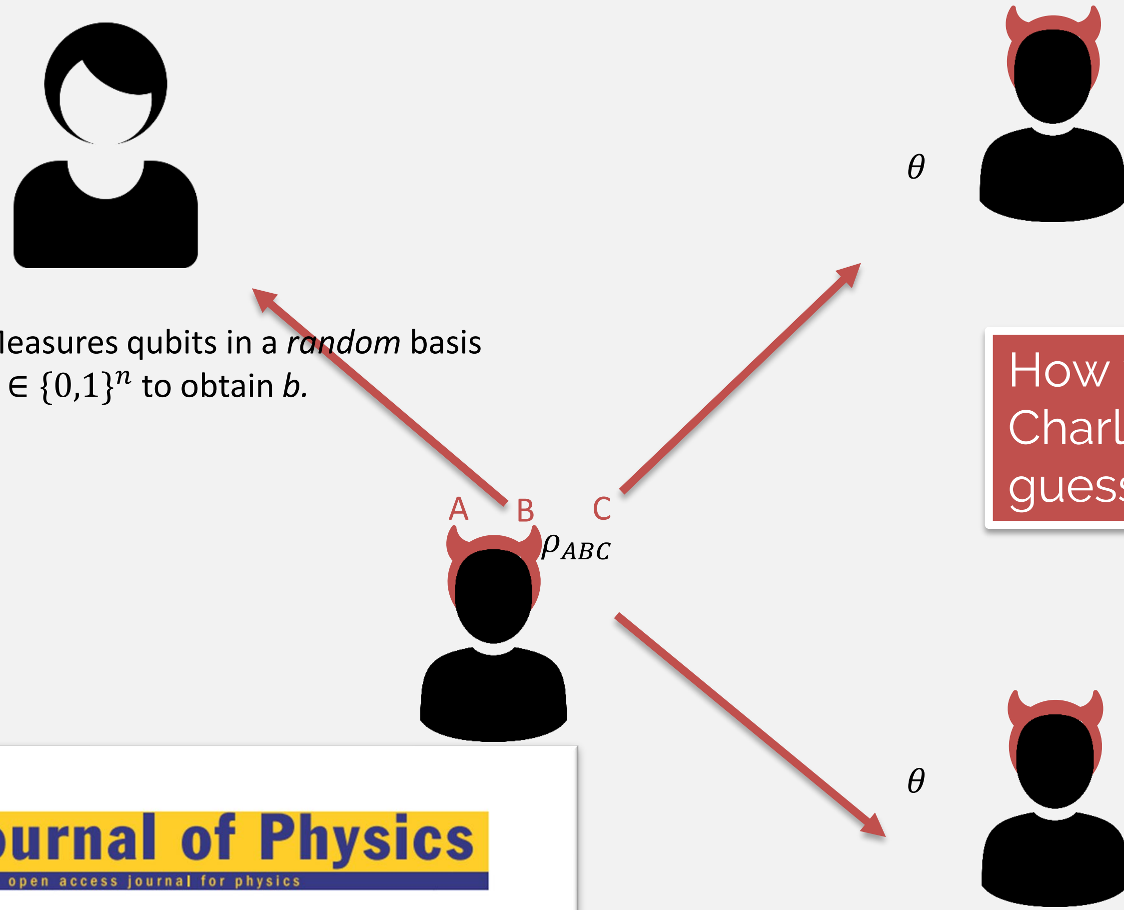
To encrypt $m \in \{0,1\}^n$,
Prepare $|b\rangle_\theta$ for random $b, \theta \in \{0,1\}^n$

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

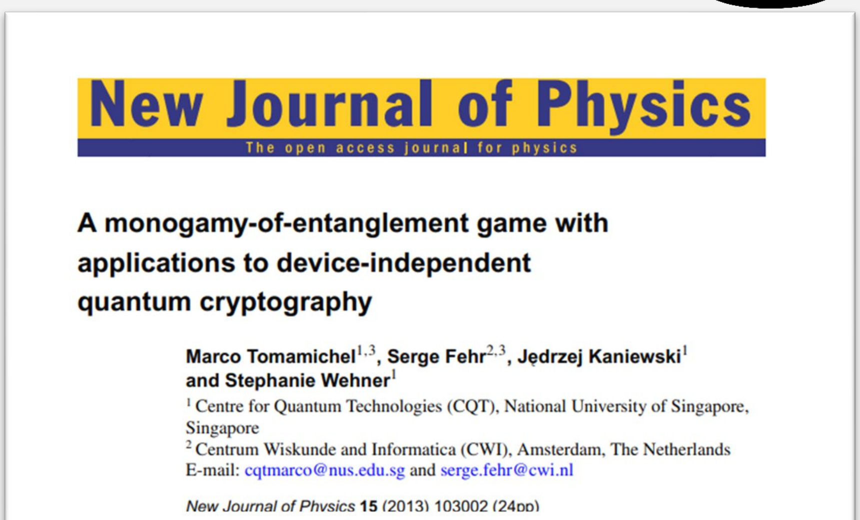


How well can Bob and Charlie **simultaneously** guess *m*?

Measures qubits in a *random* basis $\theta \in \{0,1\}^n$ to obtain *b*.



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


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

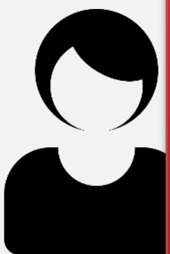
E-mail: cqtmarco@nus.edu.sg and serge.fehr@cwi.nl

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

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.



Intuitive security argument:
Producing m is equivalent to producing QROM(y), which 'should'* require full knowledge of y; Bob and Charlie can simultaneously produce y with probability at most $\left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)^{\lambda}$

*formally proved using a novel ``simultaneous one-way-to-hiding'' lemma.

To encrypt $m \in \{0,1\}^n$,
Prepare $|b\rangle_\theta$ for random
$b, \theta \in \{0,1\}^\lambda$
Let QROM be a quantum-secure random oracle
QROM: $\{0,1\}^\lambda \rightarrow \{0,1\}^n$

Output:
$|b\rangle_\theta$, $m \oplus QROM(b)$

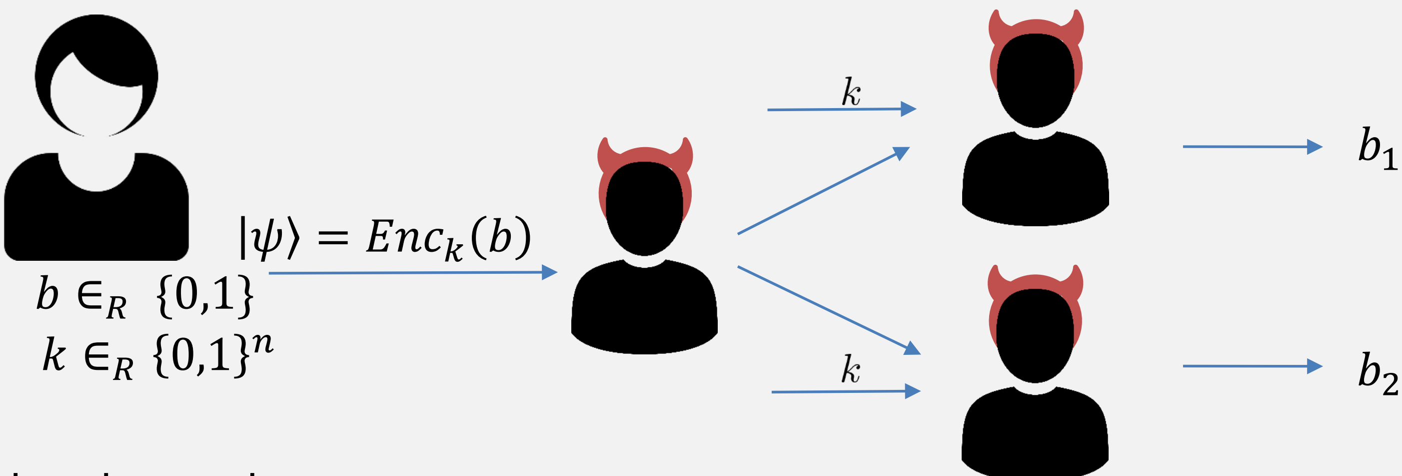
To decrypt:
Measure received qubits in basis θ;
Let the result be y.

Output
$QROM(b) \oplus (m \oplus QROM(b)) = m$

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

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 *both* be able to distinguish an encryption of *m* from an encryption of a fixed message.
- Solve the "Uncloneable bit" problem:



Find a scheme where

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

2. Unclonable Decryption

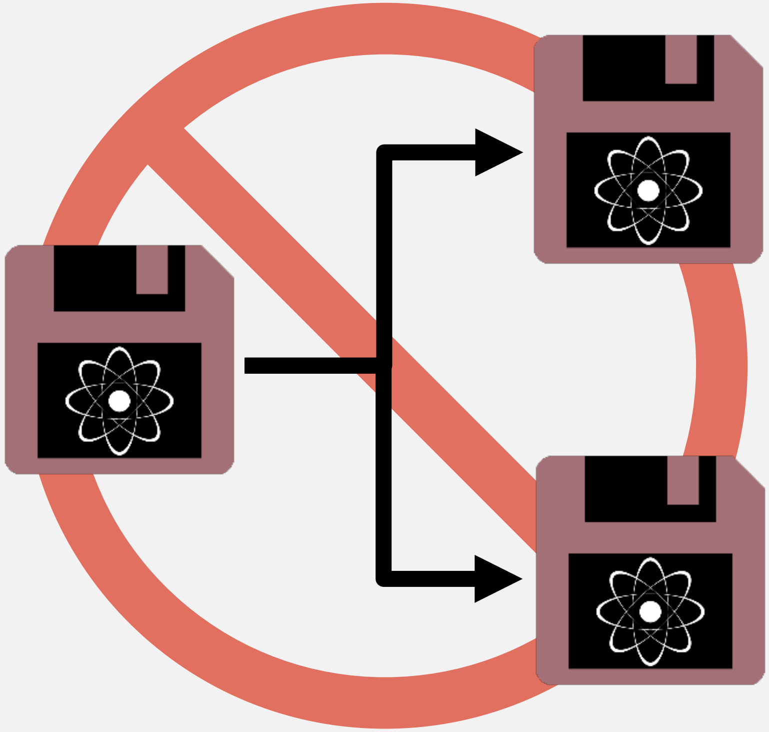
Unclonable Decryption Keys

Marios Georgiou[1] and Mark Zhandry[2,3]

- Also known as: ``single-decryptor encryption'':
  - public-key encryption, with a quantum secret key.
  - Given the secret key, cannot create two registers, both of which can be used for decryption.

Hidden Cosets and Applications to Unclonable Cryptography
Andrea Coladangelo; Jiahui Liu; Qipeng Liu; Mark Zhandry

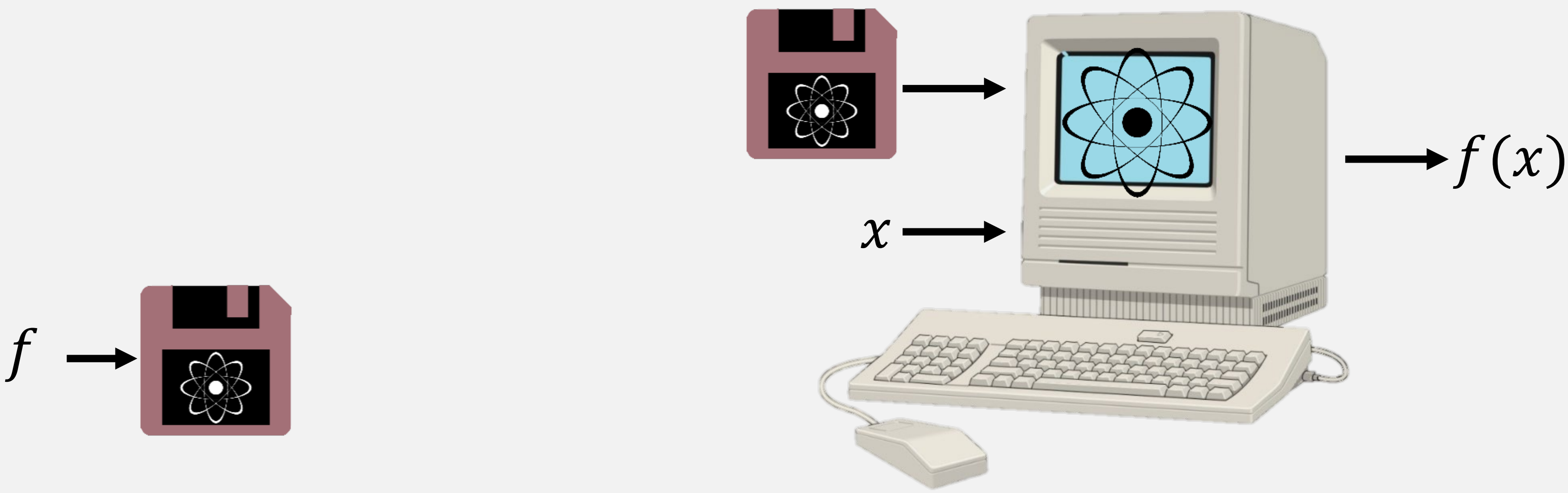
Uncloneable Functionality



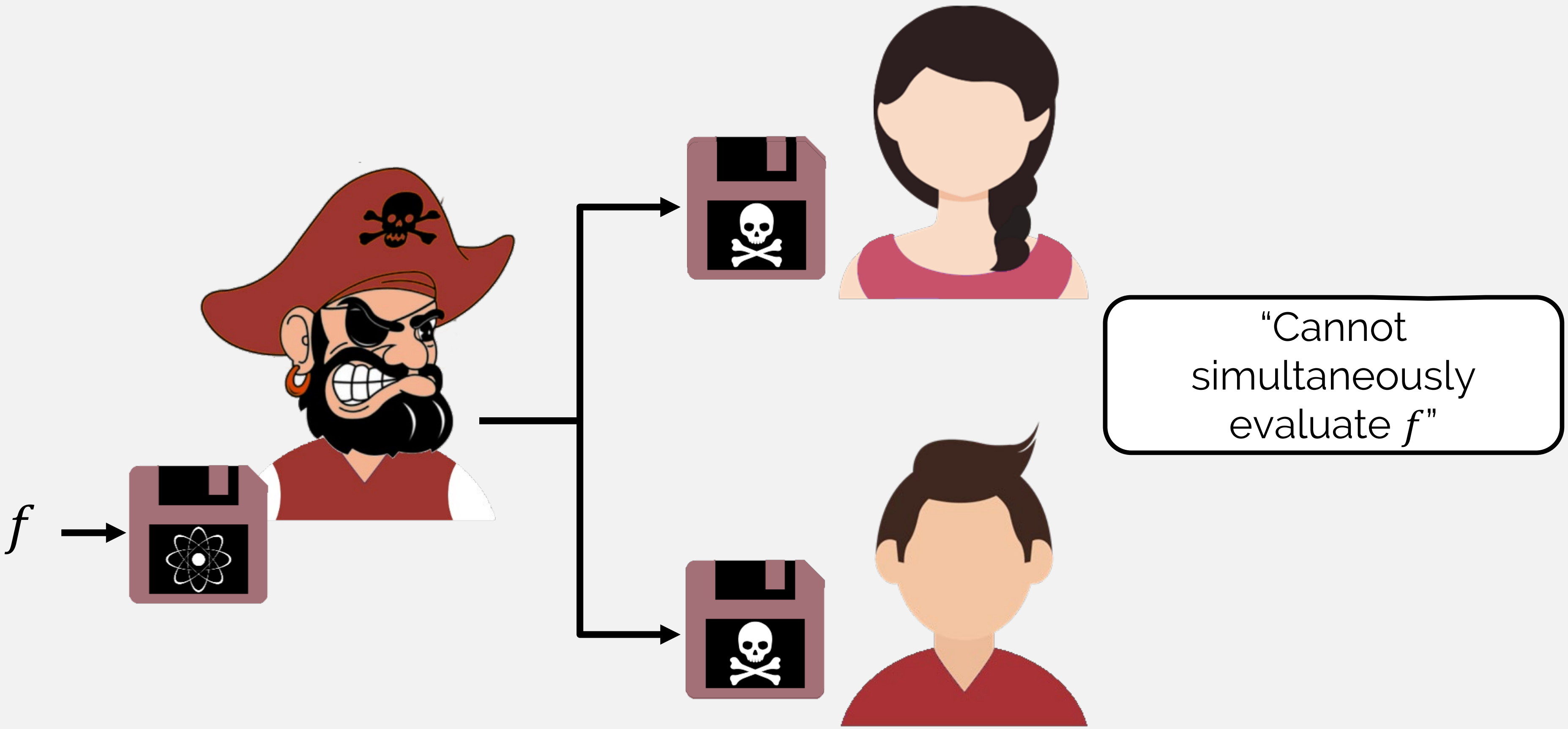
Copy-protected Software

Aaronson (2009)

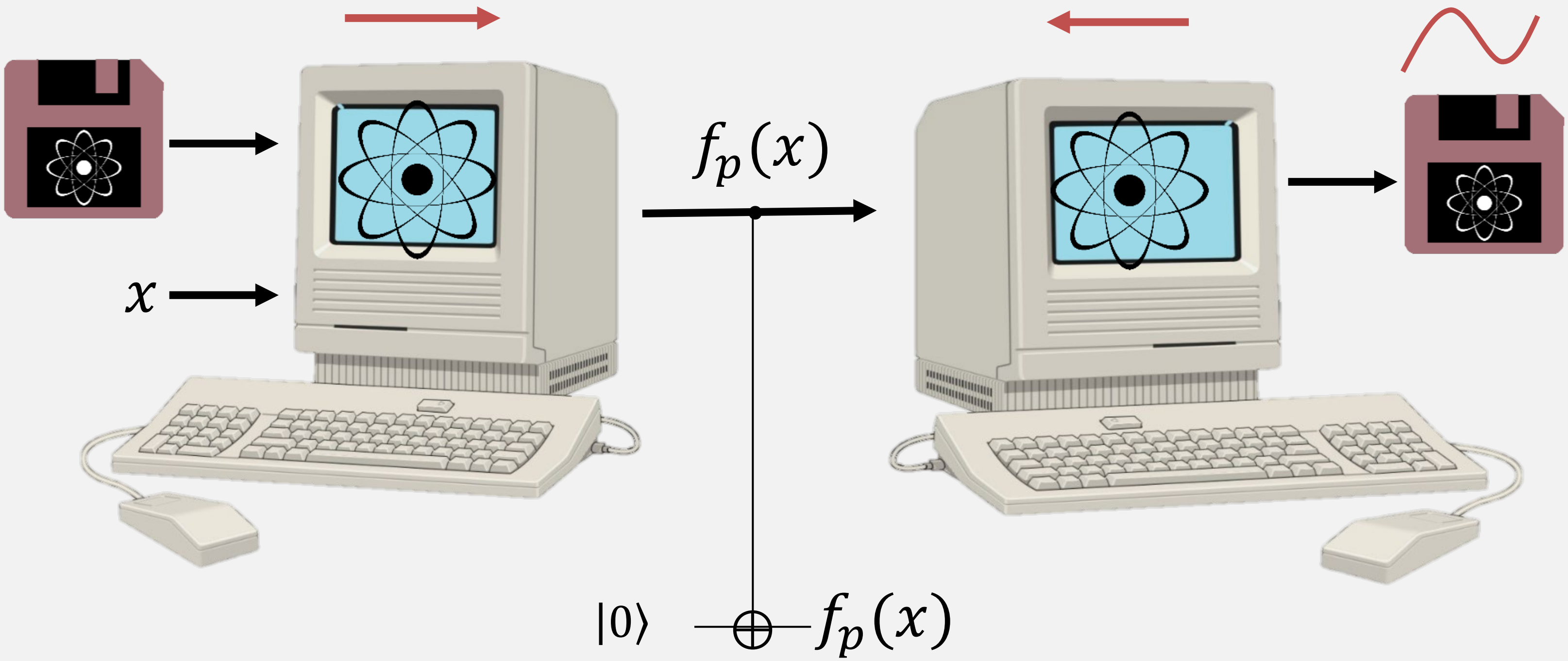
What is quantum copy protection?



What is quantum copy protection?

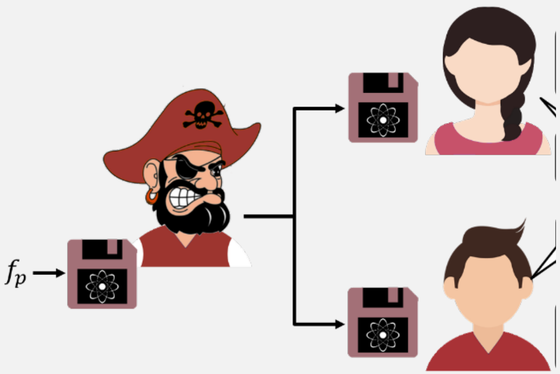


Quantum software is reusable to a certain extent



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

Limitations of Quantum Copy-Protection



Learnable Functions

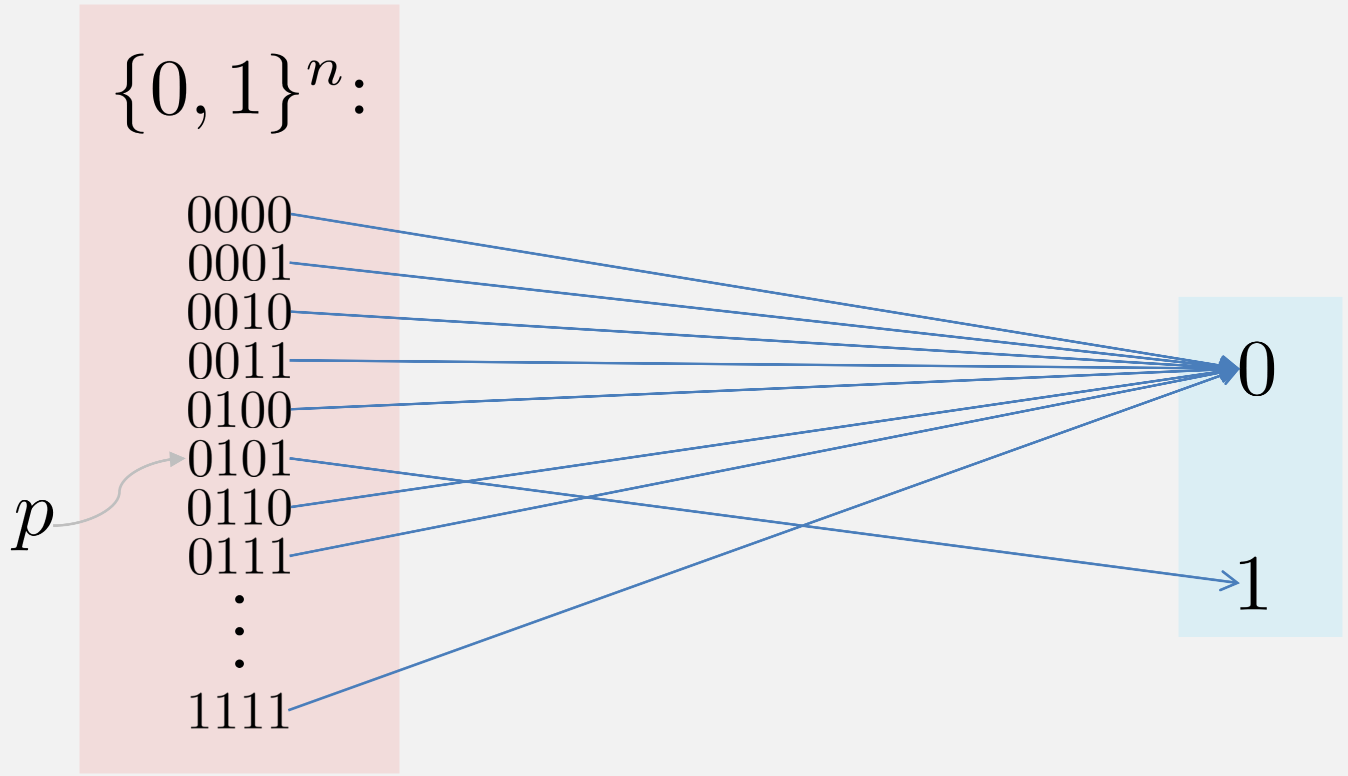
- Cannot be copy-protected

Perfectly correct ($\boldsymbol{\eta} = \mathbf{0}$)

- Cannot be secure against unbounded adversaries

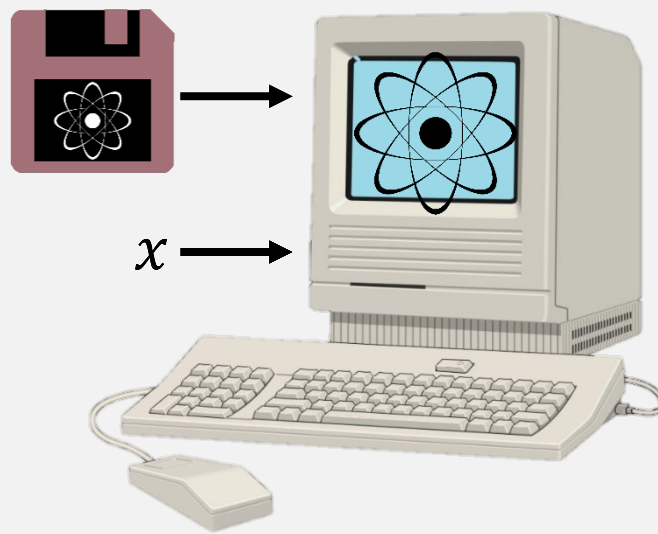
Point Functions

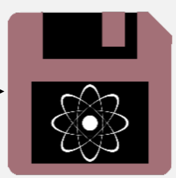
$$f_p : \{0,1\}^n \to \{0,1\}$$



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

What is quantum copy protection?



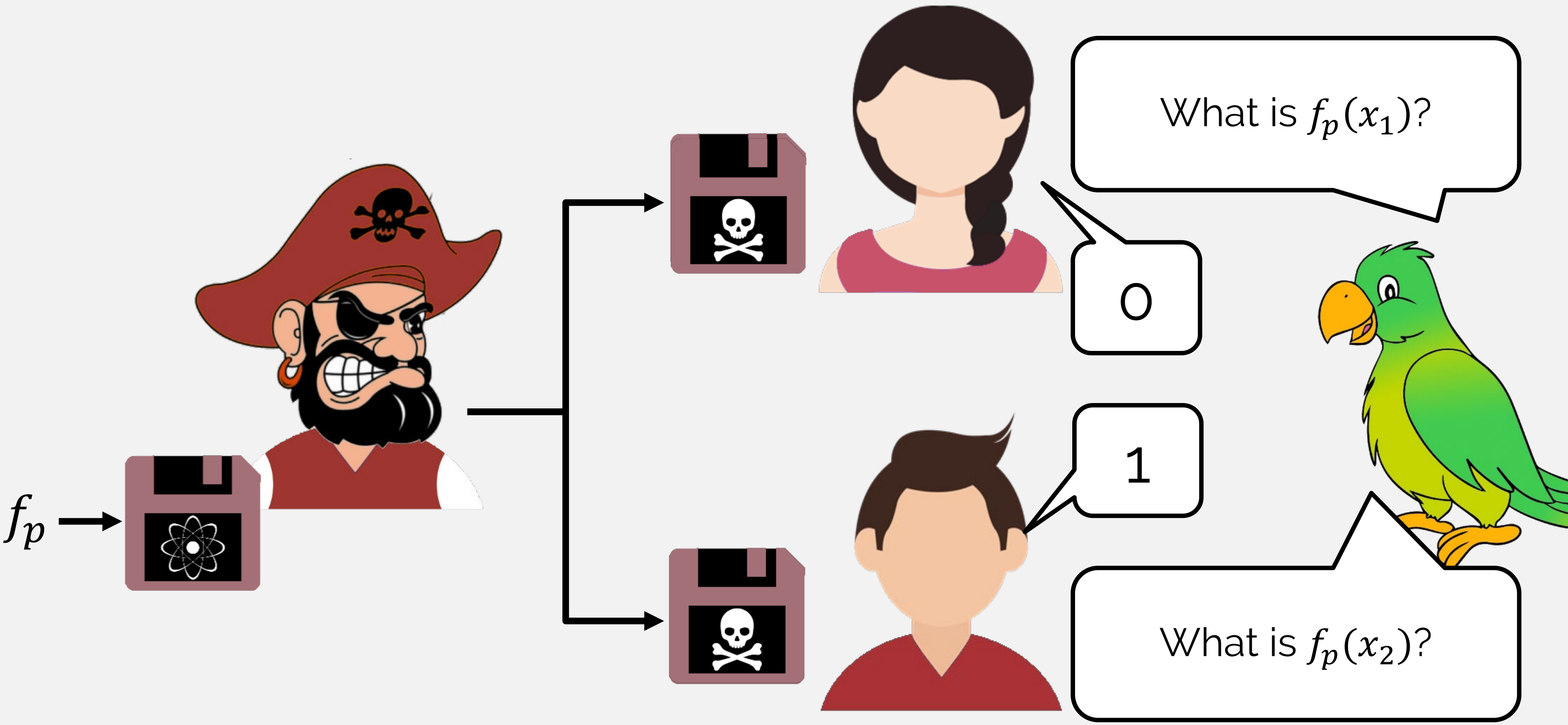
f_p 

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

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

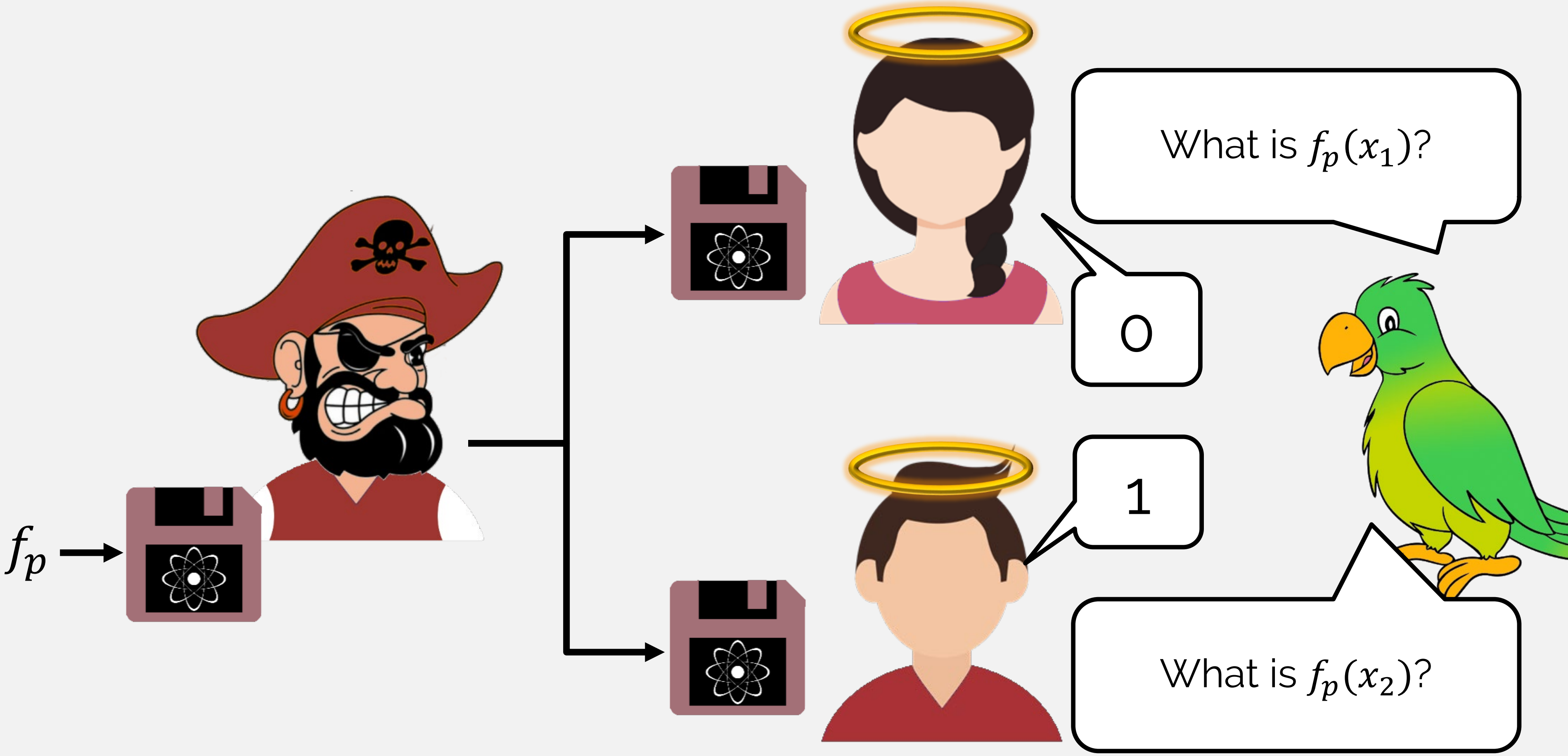
<u>Average Correctness</u>:
Up to some error term η, outcome is correct in expectation over choice of x.

What is quantum copy protection?

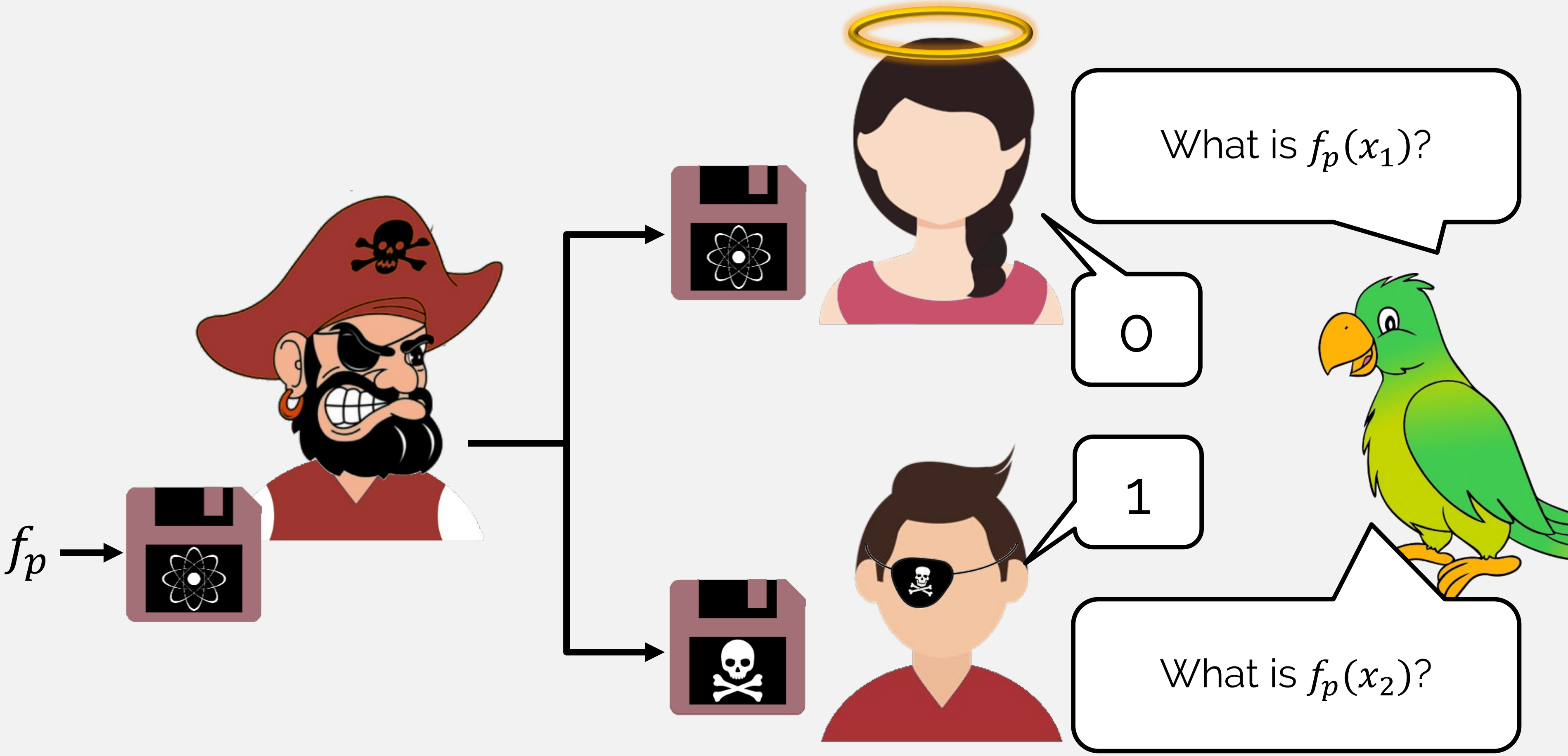


Coladangelo, Majenz and Poremba (2020)

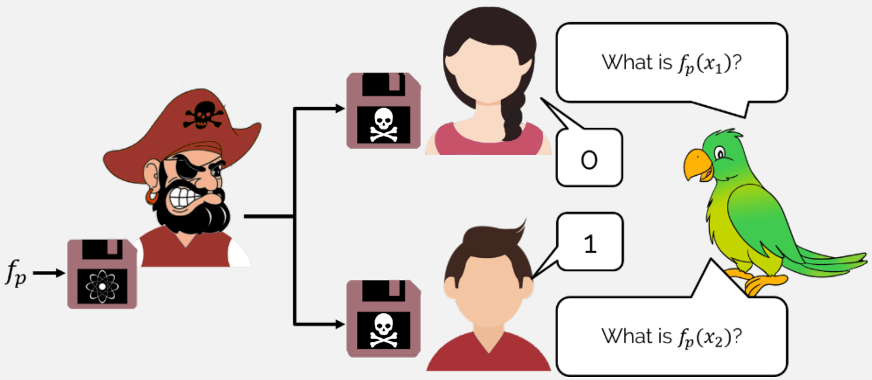
Honest-user Copy Protection



Honest-Malicious Copy Protection



What is copy protection?



Challenge Distribution

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

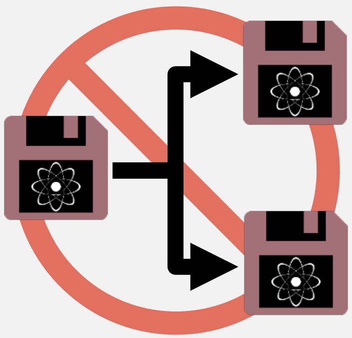
$$\Pr[x_i = p'] = \frac{1}{2(2^n - 1)}$$

$win \Leftrightarrow$ 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:

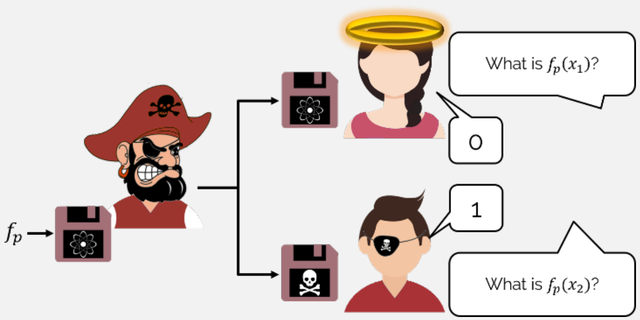
- All functions (not learnable)
- Assumes a classical oracle

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"
- Information-theoretic security

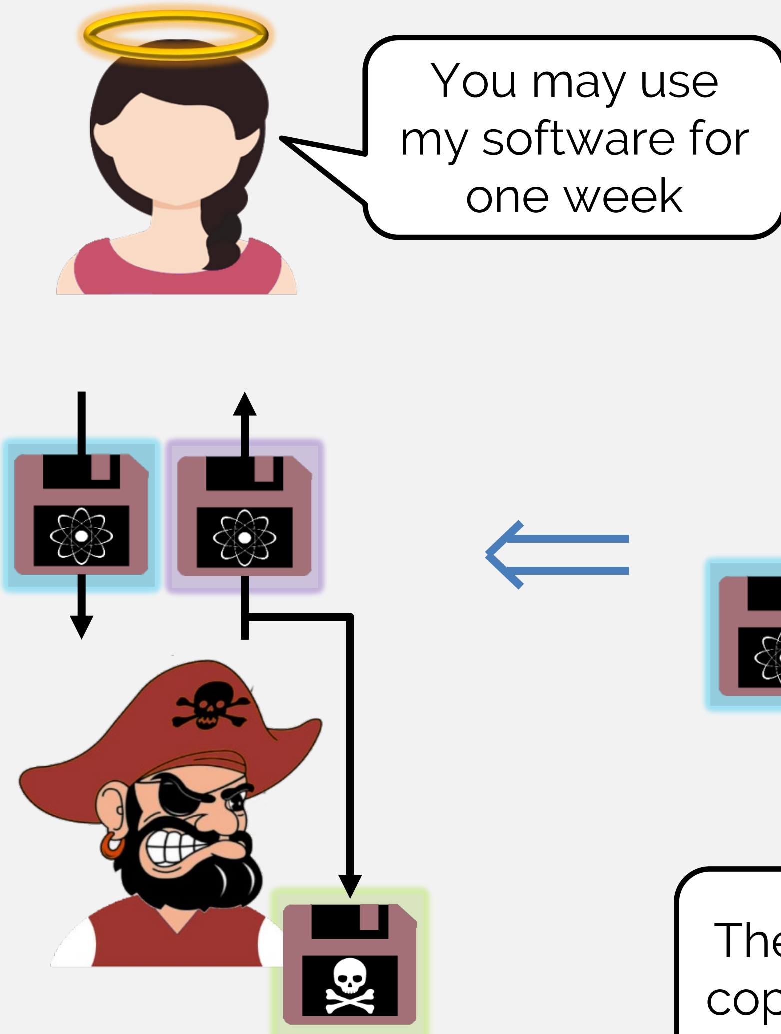


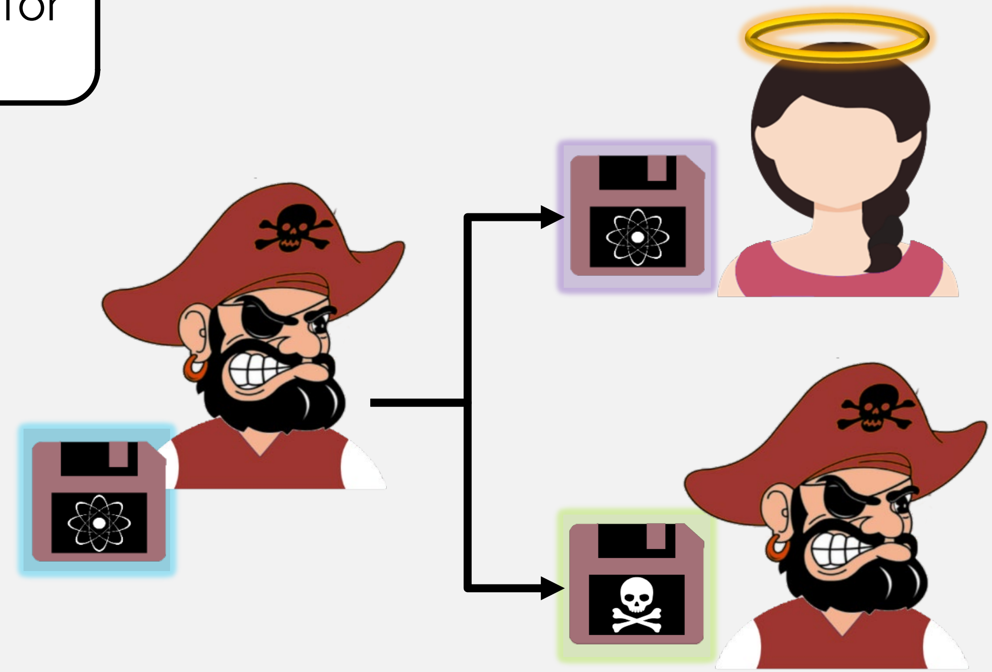
Coladangelo, Liu, Liu, Zhandry 2021:

- Pseudo-Random Functions

*(actually, compute-and-compare)

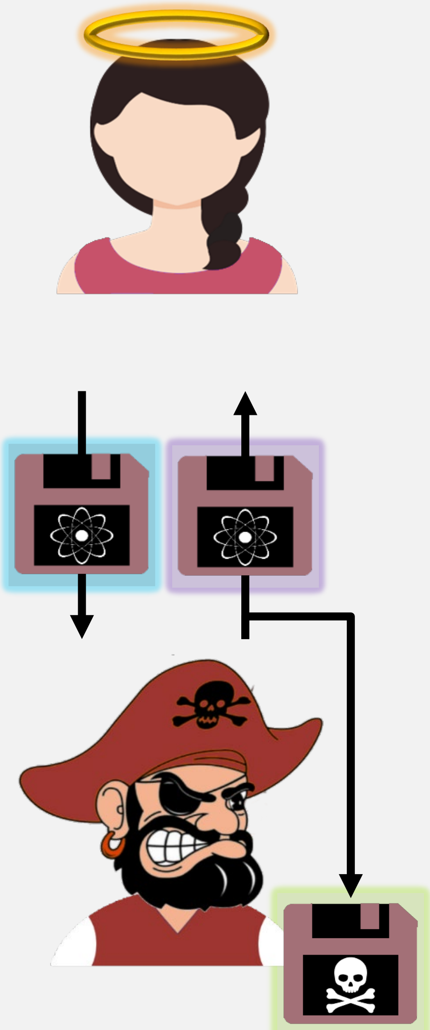
Secure Software Leasing





Theorem: Honest-Malicious copy-protection implies SSL

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

*(actually, compute-and-compare)

Compute-and-compare functions

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

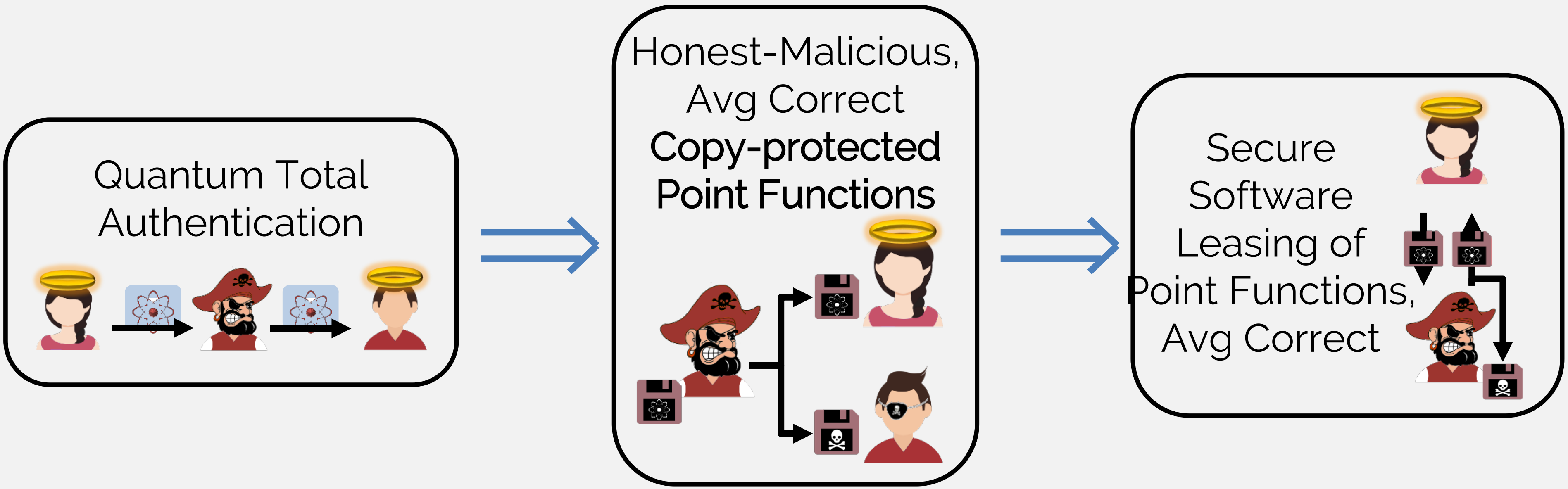
$$f_p^g(x) = \begin{cases} 1 & \text{if } g(x) = p \\ 0 & \text{otherwise} \end{cases}$$

Lemma (CMP20):

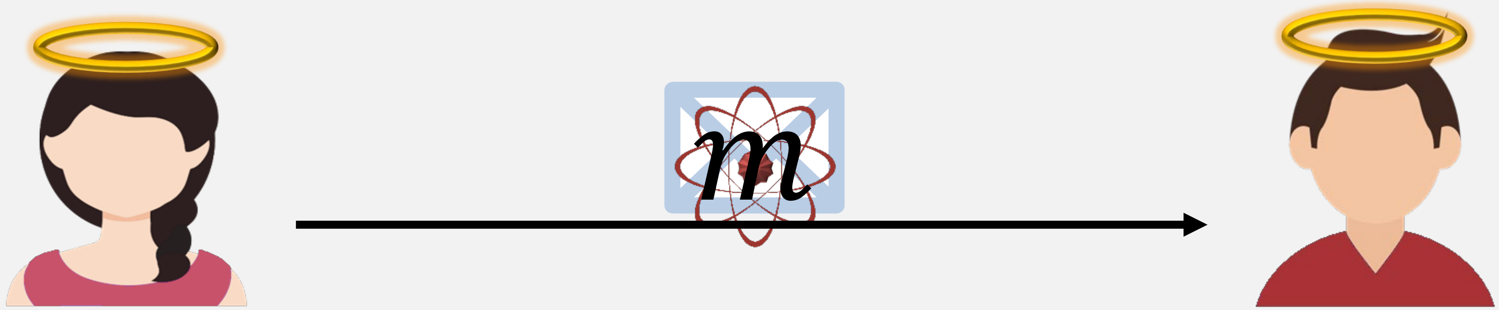
SSL for point functions implies SSL for compute-and compare functions.

Idea: Include function g (in the clear) as part of the program. Use point-function SSL on $f_p(x)$. In order to evaluate $f_p^g(x)$, first evaluate $g(x)$, and then use the SSL evaluation to compute $f_p(g(x))$. Intuition: knowing $g(x)$ does not help a pirate if they don't have access to $f_p(x)$.

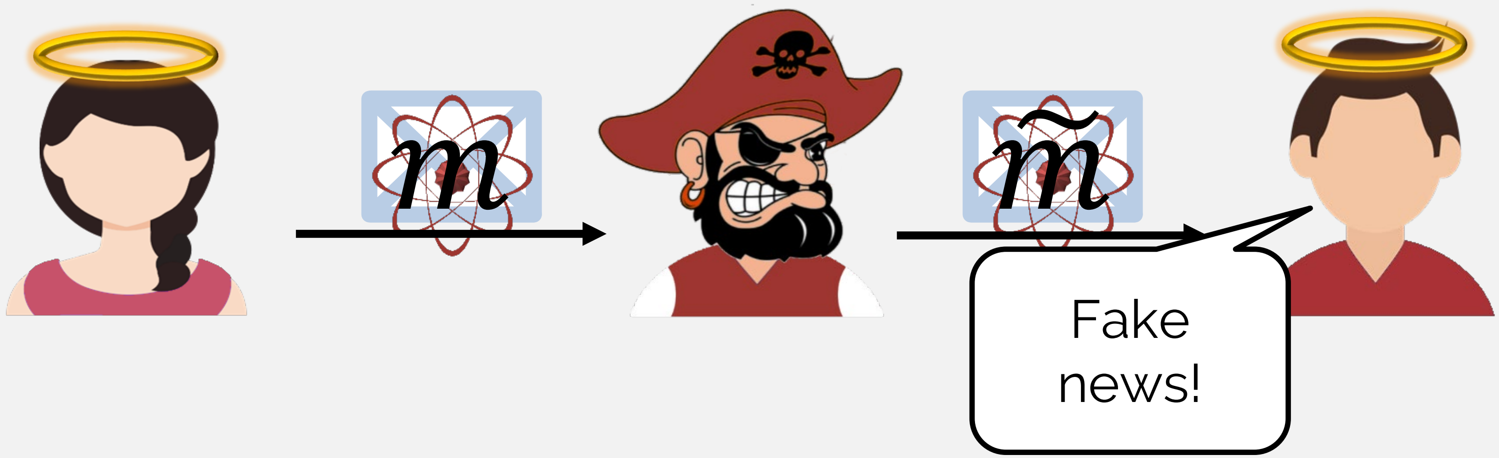
Achieving Honest-Malicious Copy-Protection



Quantum Message Authentication

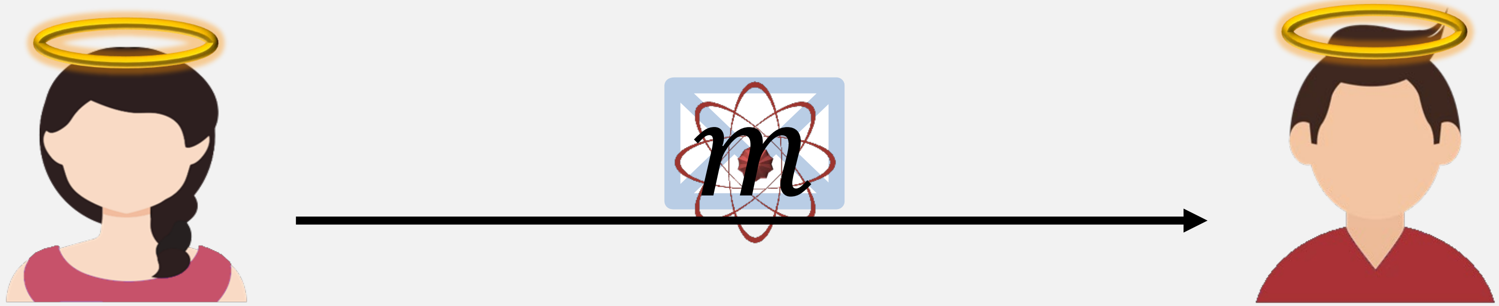


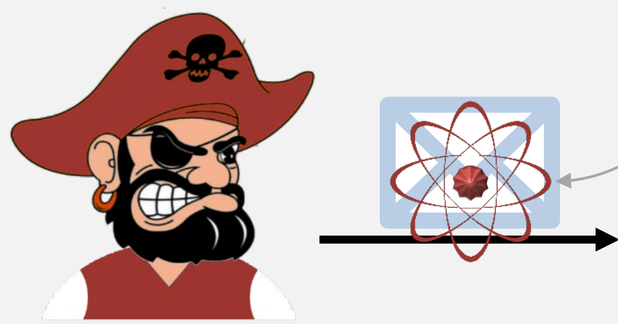
Quantum Message Authentication



Quantum Message Authentication

Quantum **Total** Authentication





nothing to
do with m
or with k

Garg, Yuen, and Zhandry (2017)

realized by 2-designs (Alagic, Majenz 2017) , 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 $\mathbf{Auth}_k, \mathbf{Verf}_k$ 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 $\mathsf{Auth}_p(|\psi\rangle\langle\psi|)$.

CP.Eval

On input of σ and q:

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

Correctness

- By correctness of the authentication scheme:

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

- By properties of the authentication scheme:

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

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

Copy Protection from Quantum Total Authentication

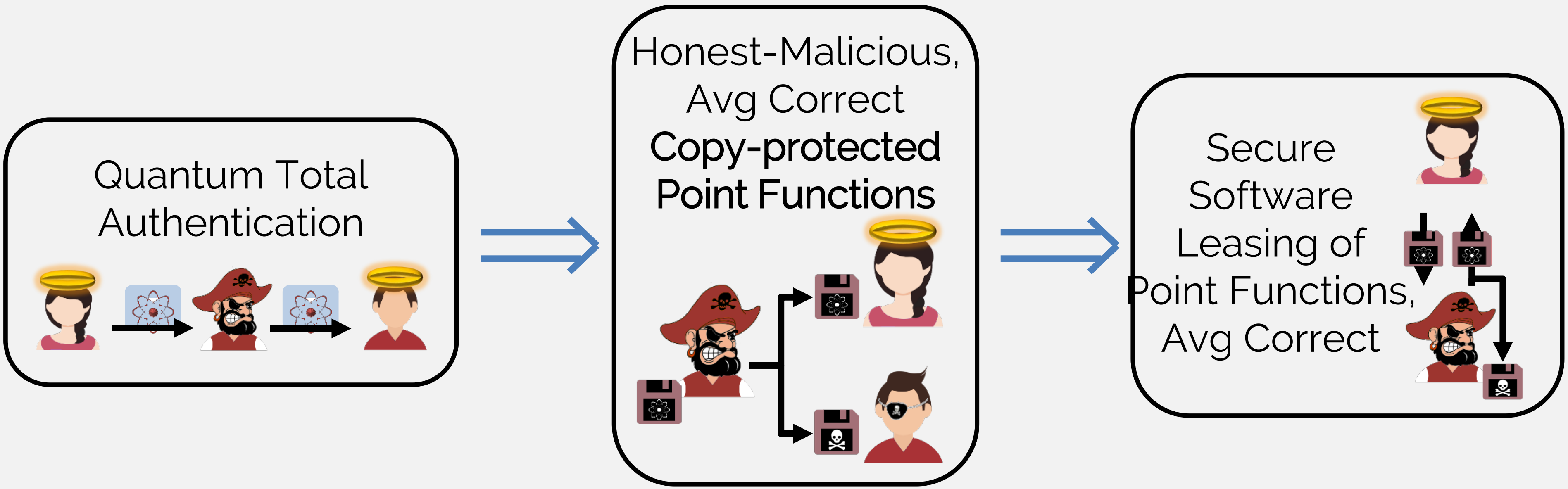
Scheme

$\mathrm{CP.Protect}(f_p) = \mathrm{Auth}_p(|\psi\rangle\langle\psi|)$ and $\mathrm{CP.Eval}(\sigma, q) = \mathrm{Ver}_q(\sigma)$ for an ϵ-secure QAS.

Security

- "Honest evaluator correctly evaluating f_p on p." $\leftrightarrow$ "Accepting an authenticated state".
- QAS: Conditioned on acceptance, the attacker knows essentially nothing on the key.
- QAS Key $\leftrightarrow$ CP Function QAS Attacker $\leftrightarrow$ CP Pirate and CP Malicious Evaluator
- If the honest evaluator is correct, the malicious evaluator knows essentialy nothing on p.
- We show that $\Pr[\text{Advs. win.}] \leq p^{\text{guess}} + \frac{3}{2}\epsilon + \sqrt{2\epsilon}$ with distributions where $p^{\text{guess}} = \frac{1}{2}$.

Achieving Honest-Malicious Copy-Protection



Questions on quantum uncloneability

1. Unconditional security for copy protection:
   - against **two** malicious evaluators?
   - With multiple copies of the program?

2. Unconditional copy-protection for functions beyond compute-and-compare?

3. Foundations of uncloneability:
   - What is it?
   - Simple primitive?

4. NISQ-era uncloneable schemes?

Thank you!