Quantum Uncloneability

Anne Broadbent

uOttawa

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

Extreme Universe colloquium
Kyoto University
November 14 2023

Quantum States Can't be Copied

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

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.

Qubits ("quantum states")

A *pure qubit* can be in one of the basis states:

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

It can also be in a *superposition,*

$$\alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

where .

$$\alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

Systems of qubits are combined with the tensor product:

$$\begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \equiv \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix} \qquad |0\rangle \otimes |1\rangle \equiv |0\rangle\,|1\rangle \equiv |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Measurements: qubits $\longrightarrow$ bits

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \;\rightarrow\; \begin{cases} \textbf{measurement outcomes:} \\ \;0 \text{ with probability } |\alpha|^2 \\ \;1 \text{ with probability } |\beta|^2 \end{cases}$$

$$e.g. \;\; \text{measure } |0\rangle \rightarrow 0$$

Let $|+\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$.

$$e.g. \;\; \text{measure } |+\rangle \rightarrow \begin{cases} 0 \;, \text{ prob. } \frac{1}{2} \\ 1 \;, \text{ prob. } \frac{1}{2} \end{cases}$$

Measuring a quantum system will not, in general, give a complete description of the state.

Measurement destroys the quantum state.

Transformations

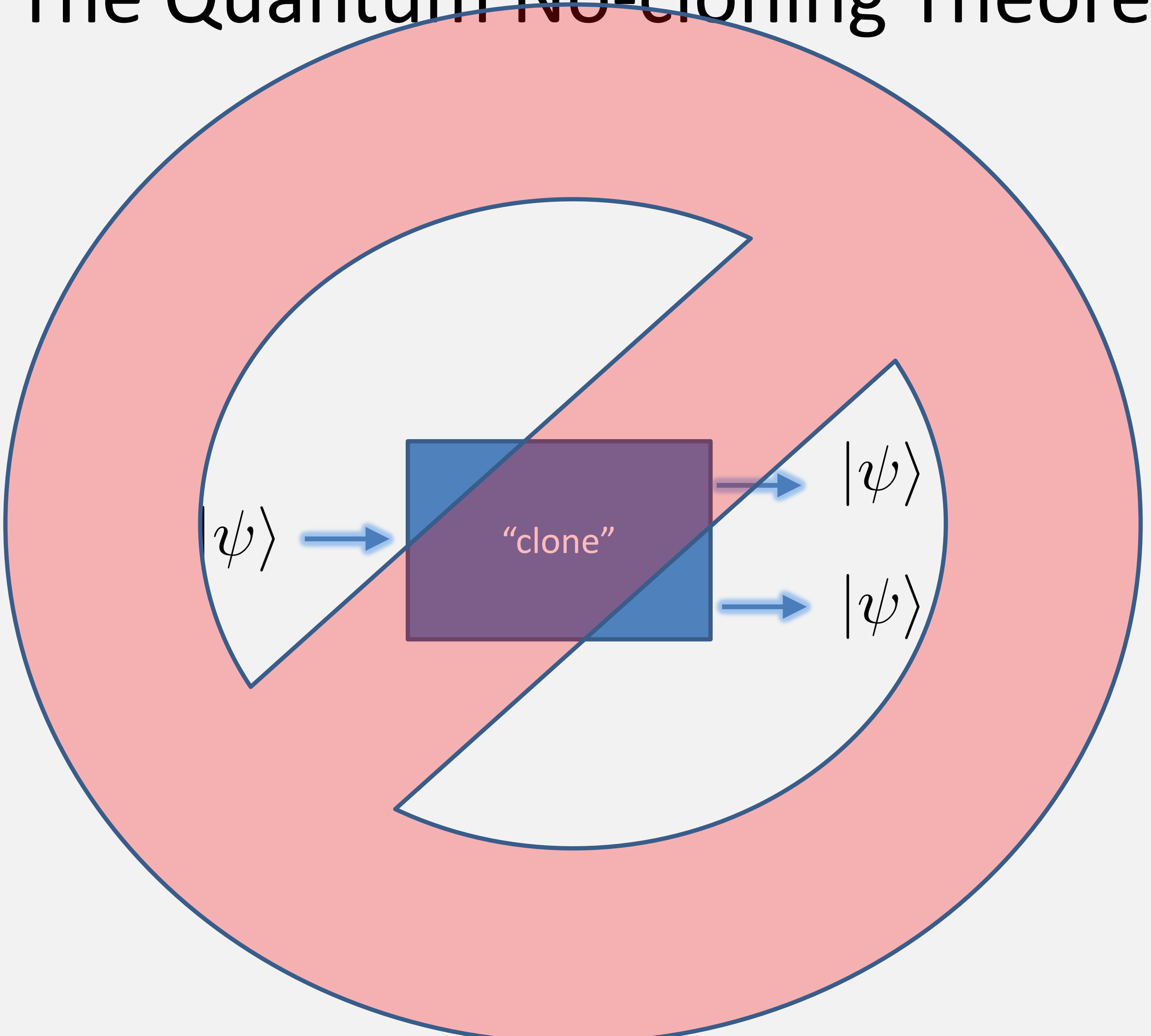
Postulate: quantum evolutions are linear

$\Longrightarrow$transformations are given by matrix multiplication.

Unitary matrices are the valid quantum transformations, since they are the transformations that preserve Euclidean norm.

Theorem: U unitary if and only if $UU^\dagger = I$, where $U^\dagger = (U^T)^*$

The Quantum No-cloning Theorem



The Quantum No-cloning Theorem

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

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

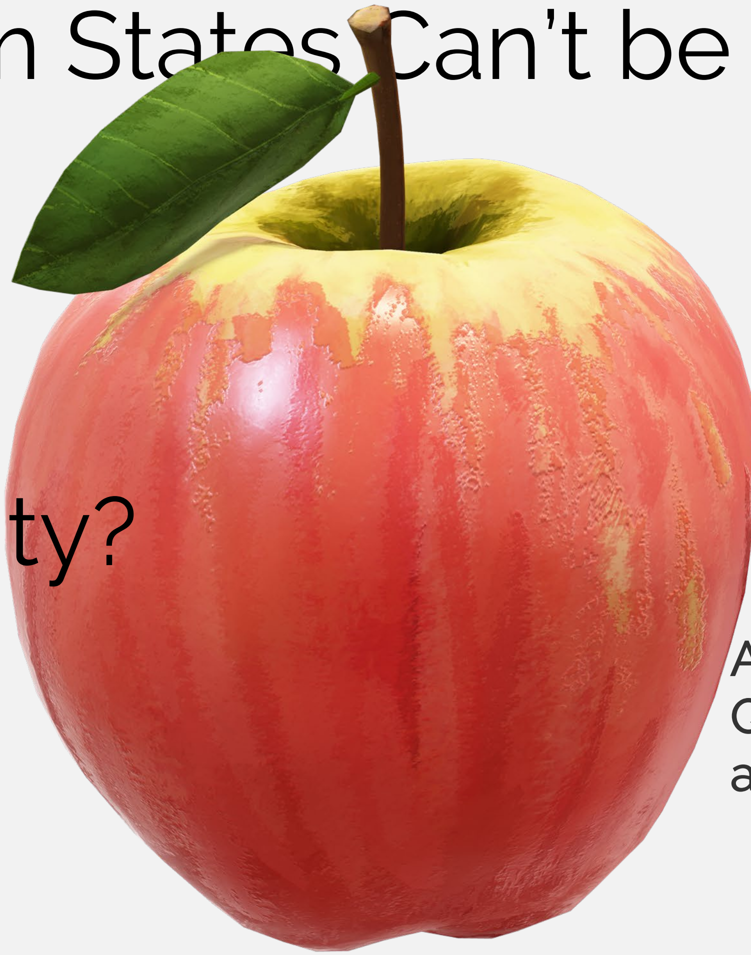
$$\begin{aligned} U|\psi\rangle|0\rangle &= |\psi\rangle|\psi\rangle \\ &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \\ &= \boxed{\alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle} \qquad (*) \end{aligned}$$

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

Quantum States Can't be Copied



What is uncloneability?

Aaronson (2009)
Quantum Copy-Protection and Quantum Money

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

What is uncloneability?

What is security?

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

Probabilistic Encryption*

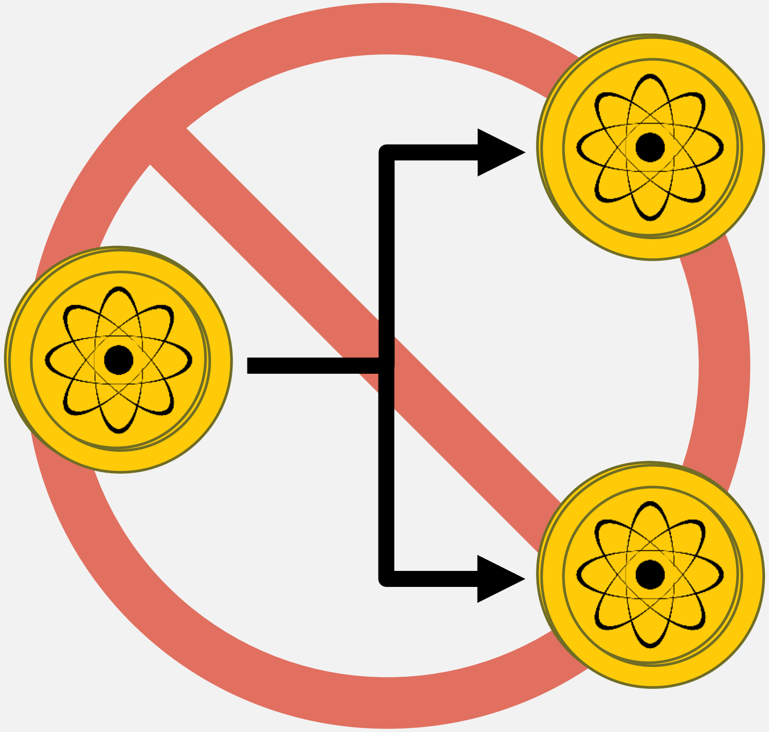
SHAFI GOLDWASSER AND SILVIO MICALI

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"

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 $r \in \{0,1\}$.
let $|r\rangle_\theta = H^\theta |r\rangle$

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

$r=0$: Computational basis : $\{|0\rangle, |1\rangle\}$
$r=1$: Diagonal basis: $\{|+\rangle, |-\rangle)$

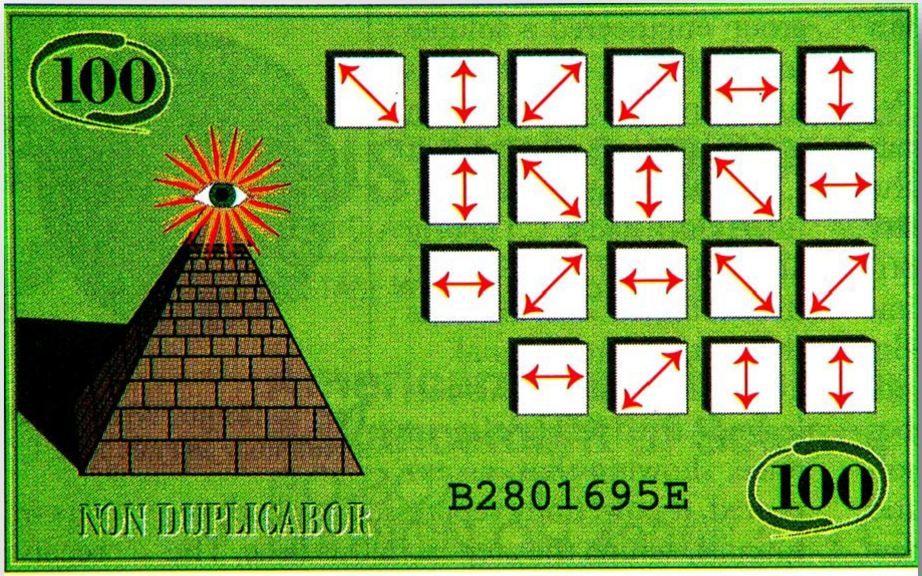
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

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

- Can easily verify $|r\rangle_\theta$ if r, 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 $\theta = \theta_1\theta_2 \ldots \theta_n$, $r = r_1 r_2 \ldots r_n$, define
$|r\rangle_\theta = |r_1\rangle_{\theta_1} \otimes |r_2\rangle_{\theta_2} \ldots \otimes |r_n\rangle_{\theta_n}$

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



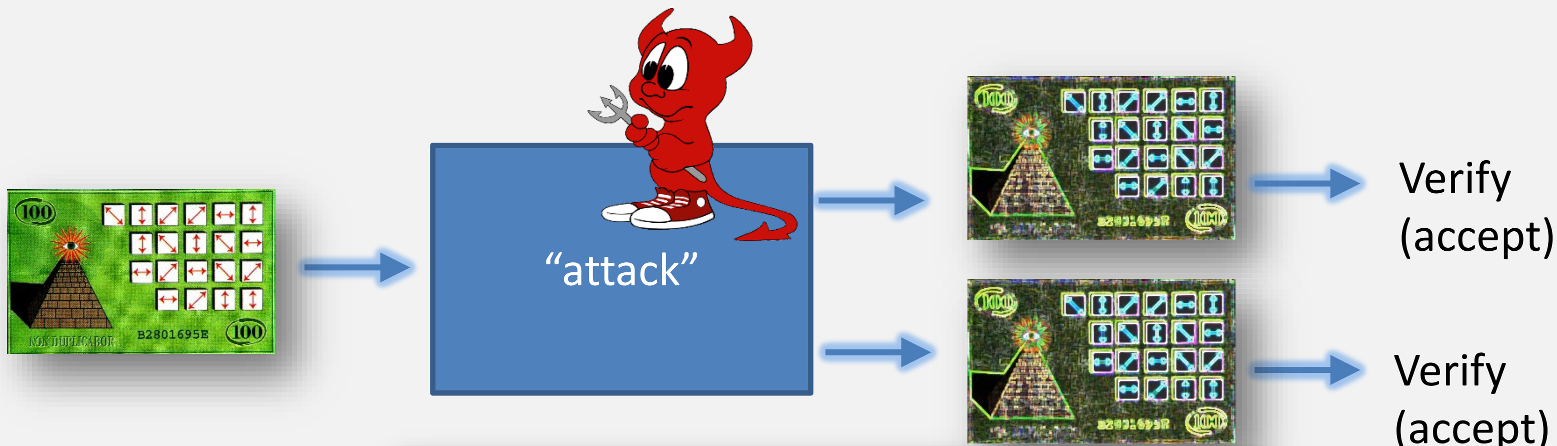
A quantum banknote, containing particles in a secret set of quantum states, cannot be copied by counterfeiters, who would disturb the particles by attempting to observe them.

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.

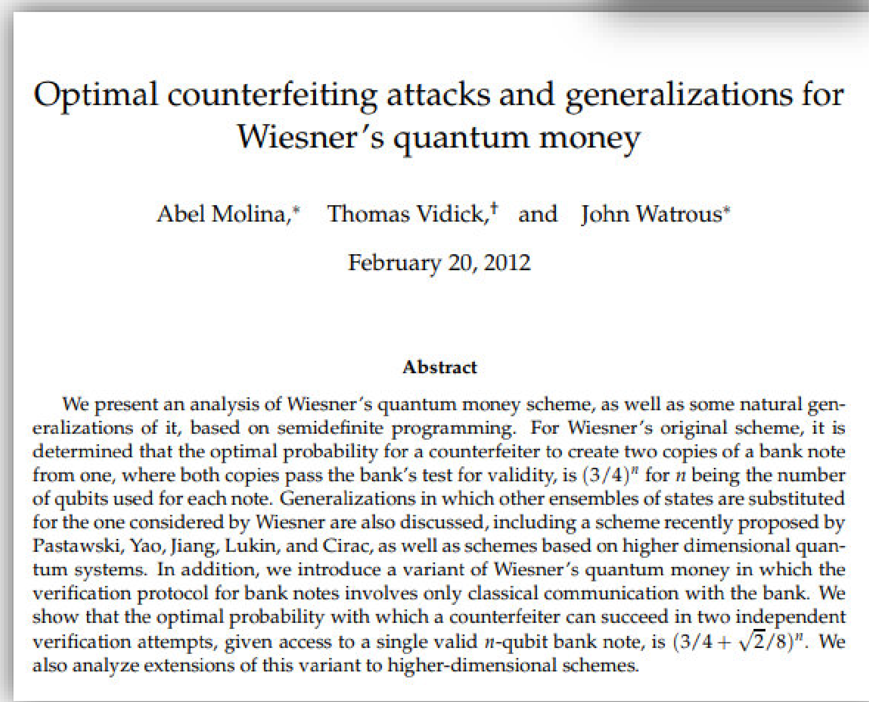
Security of Wiesner’s quantum money



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 SINCE WIESNER

Noise-tolerant ('feasible with current technology') quantum money

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

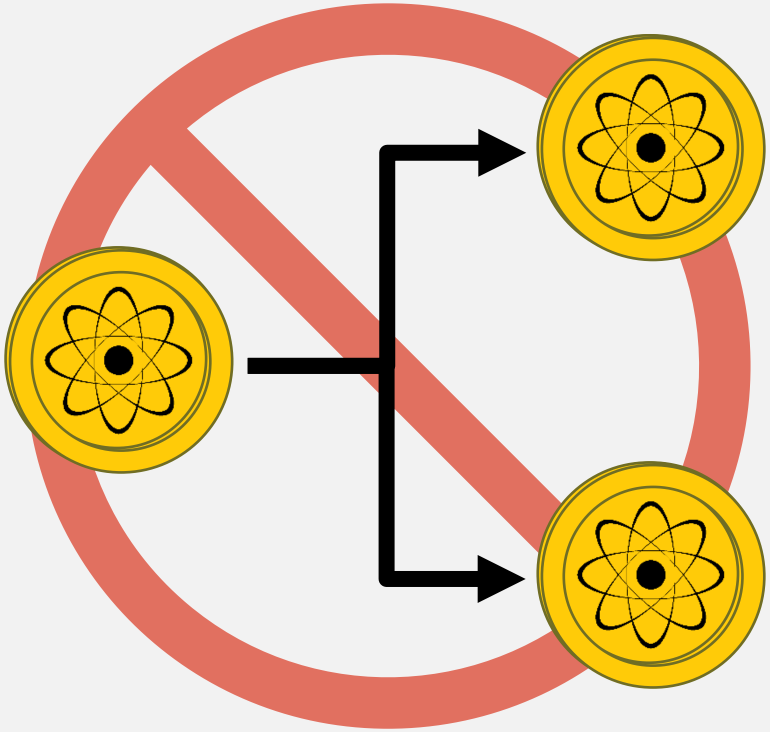
Quantum Money with classical verification

- Gavinsky (2012)

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

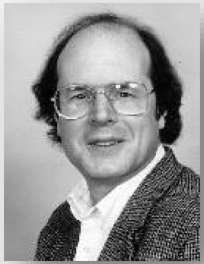
- Farhi, Gosset, Hassidim, Lutomirski, and Shor (2012)
- Aaronson and Christiano (2012)
- Zhandry (2017)

Quantum Money = "Uncloneable Authenticity"

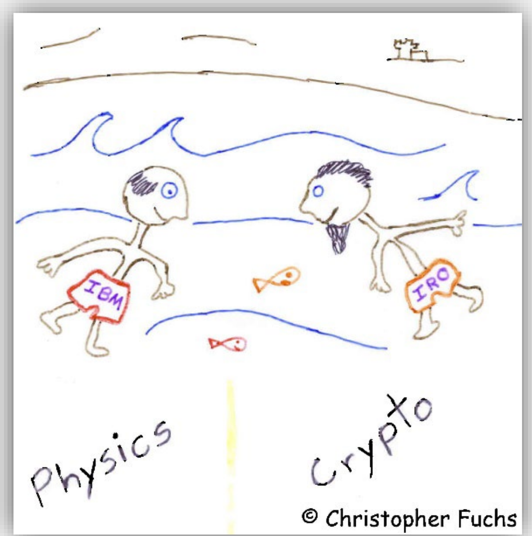


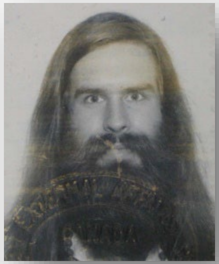
Quantum money does not encode any data;
Can the no-cloning principle be used to secure information?

1979



Charles
Bennett
Physicist
IBM, USA





Gilles
Brassard
Computer
Scientist
Université
de Montréal,
Canada

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

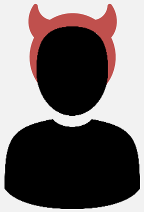
Bennett and Brassard (1984)

Quantum Key Distribution

Bennett and Brassard (1984)

Quantum Key Distribution

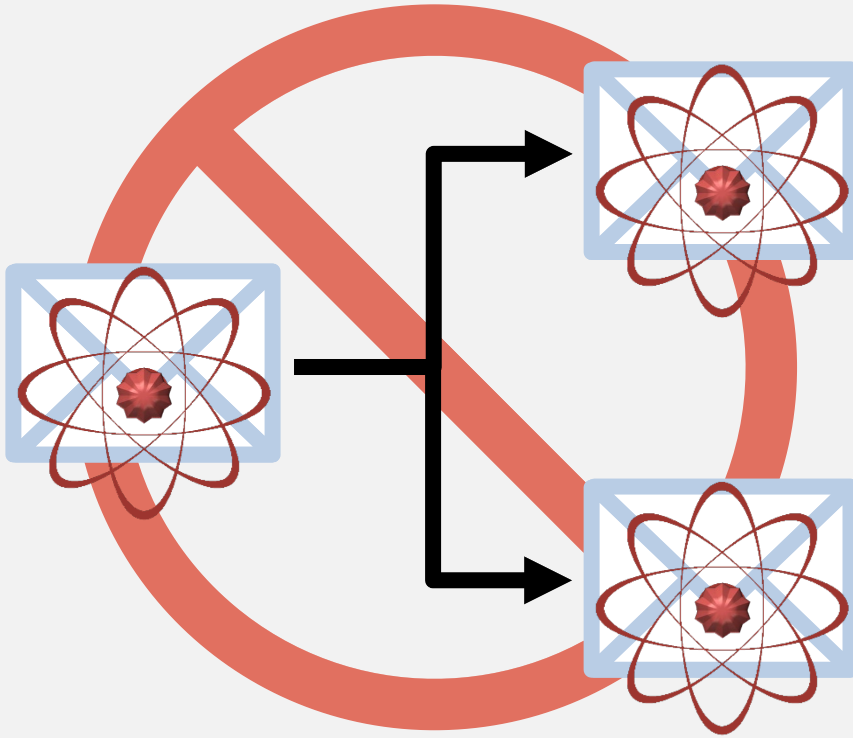
Bennett and Brassard (1984)



- BB84 uses conjugate coding in order to detect eavesdropping.
  - No eavesdropping detected → shared key is secret.
  - Impossible to achieve with classical information alone

- In what other areas of cryptography could quantum information provide a qualitative advantage?

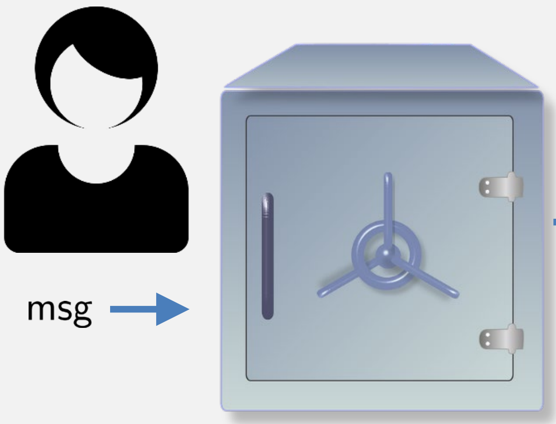
Quantum Encodings for Classical Messages

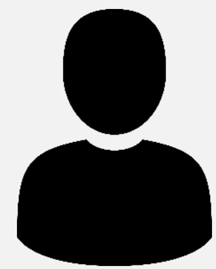


1. Certified Deletion (Broadbent, Islam 2020)
2. Unclonable Encryption (Broadbent, Lord 2020)

Certified Deletion

A “physical” type of encryption:





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

Bob decides

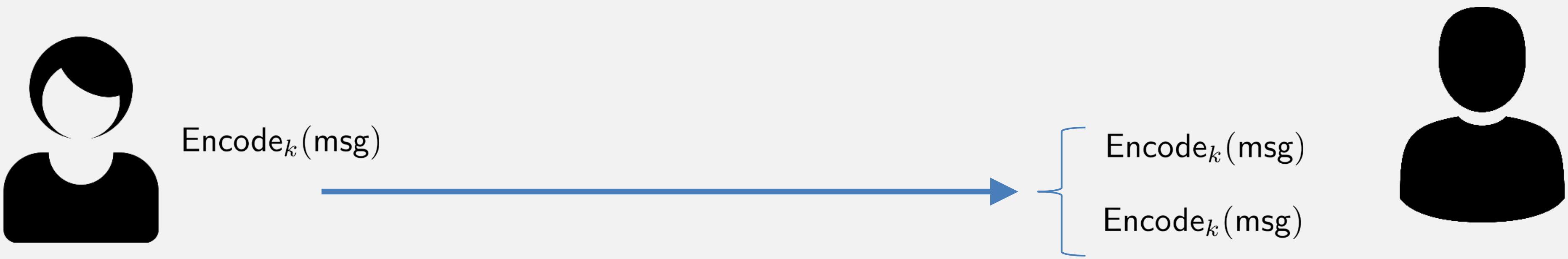
- return the closed safe before the combination is revealed as a proof that message was not read

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?
No!
Proof by contradiction…



Bob can :

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

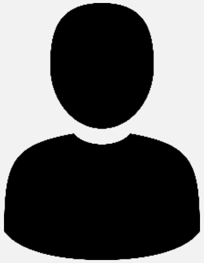
AND

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

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



Application:

Basic certified deletion scheme by example:

θ random	**θ**	**0**	**1**	**0**	**1**
r random	r	0	1	1	0
Wiesner encoding	$\|r\rangle_\theta$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$
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;
  - honest behaviour obtains $y =* 1 * 0$.
- 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
$\vert r\rangle_\theta$	$\vert 0\rangle$	$\vert -\rangle$	$\vert 1\rangle$	$\vert +\rangle$
r_{comp}	0		1	
r_{diag}		1		0

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

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

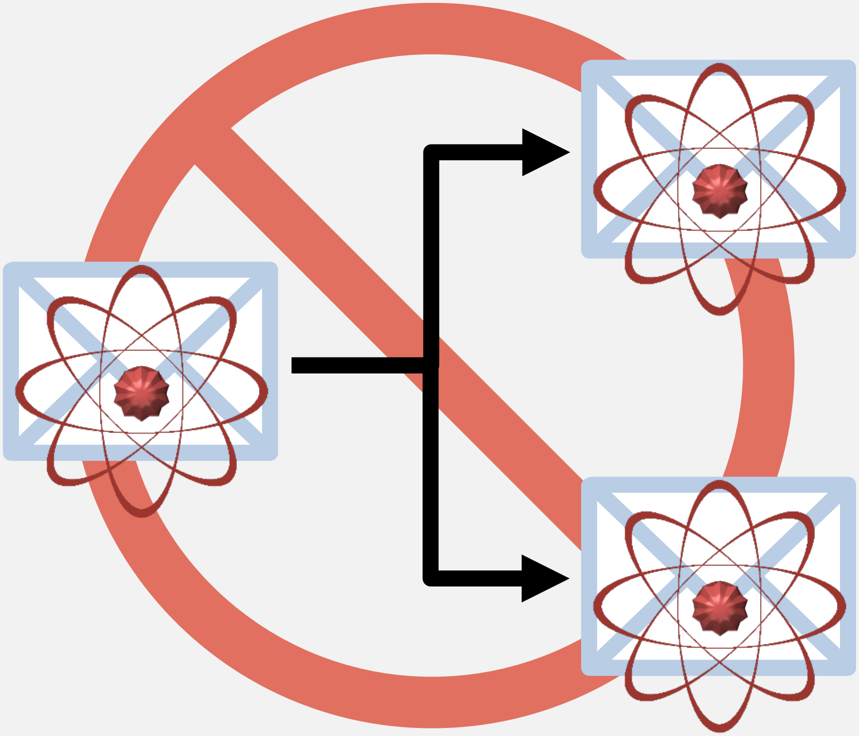
The probability of guessing r_{comp} decreases (i.e. adversary is unable to decrypt, even given the key)

Maassen & Uffink, 1988

More on certified deletion

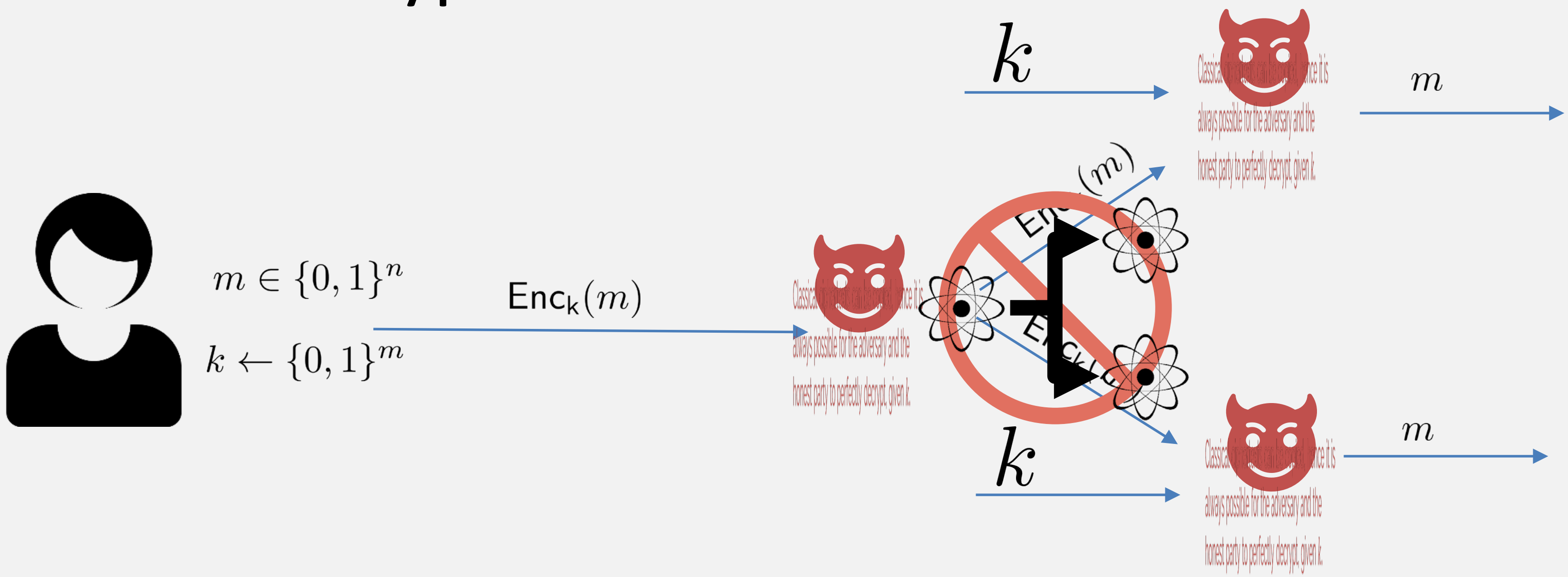
- Device-independent
  - Kundu & Tan 2020
- Re-usable encryption key; classical communication
  - Hiroka, Morimae, Nishimaki & Yamakawa 2021
- For fully homomorphic encryption
  - Poremba 2022
- Commitments and zero-knowledge
  - Hiroka, Morimae, Nishimaki, & Yamakawa 2022

Unclonable Information



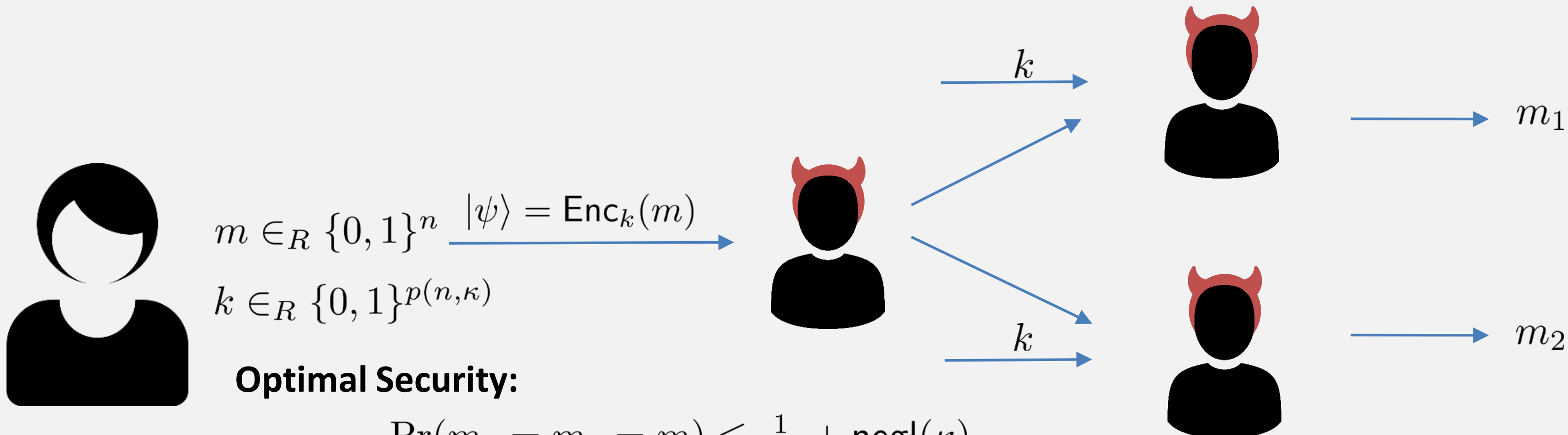
Example 2: Unclonable Encryption

When encryption is classical:



Classical ciphertexts can be copied, hence it is always possible for multiple adversaries to perfectly decrypt, given k.

Uncloneable Encryption Security Game



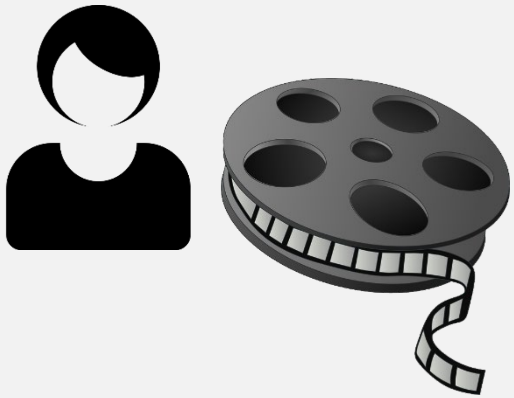
Optimal Security:

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

Wiesner-encoding based scheme: [Broadbent, Lord 2020]

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

Uncloneable Encryption -application



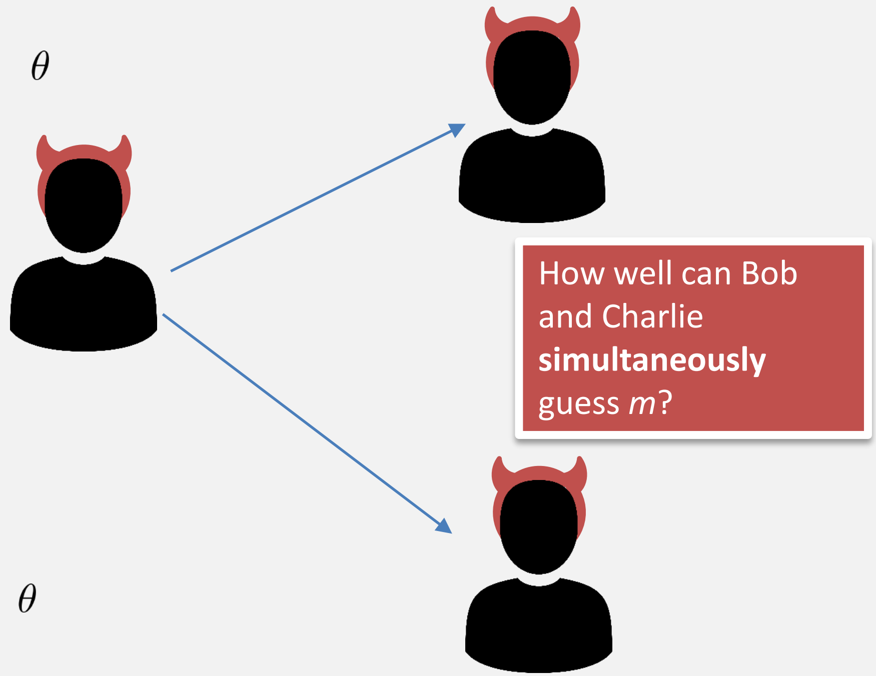
1. Alice uses uncloneable encryption and distributes an encrypted movie ahead of the movie release date.
2. The day of release, she reveals the key.
3. Thanks to uncloneable encryption, she is sure that at most one recipient* can decrypt the movie.

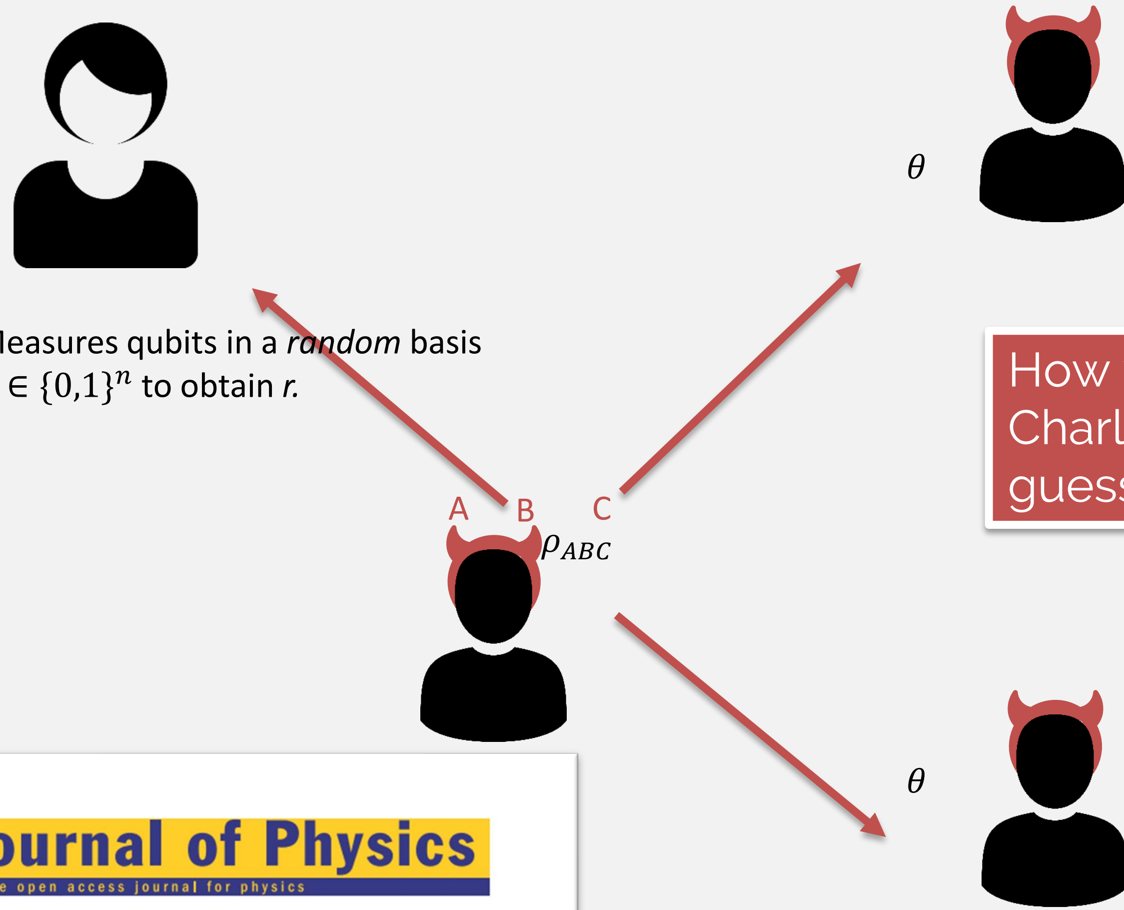
*assuming no communication after key reveal

Uncloneable Encryption Scheme + Security

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

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





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

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

New Journal of Physics
The open access journal for physics

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

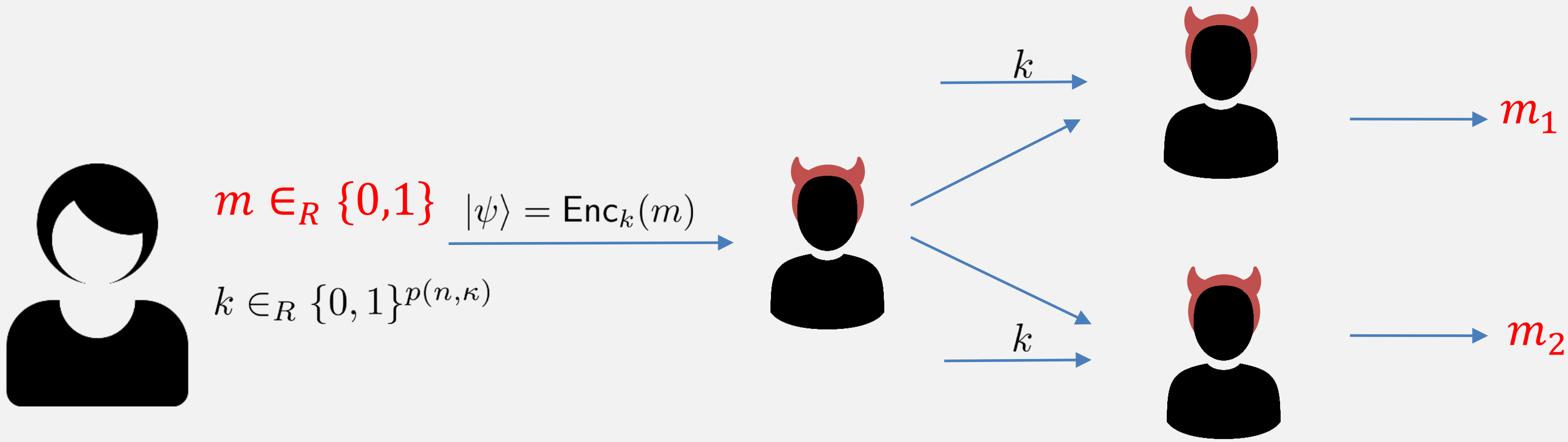
Marco Tomamichel[1,3], Serge Fehr[2,3], Jędrzej Kaniewski[1] and Stephanie Wehner[1]
[1] Centre for Quantum Technologies (CQT), National University of Singapore, Singapore
[2] Centrum Wiskunde and Informatica (CWI), Amsterdam, The Netherlands
E-mail: cqtmarco@nus.edu.sg and serge.fehr@cwi.nl

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

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

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

Uncloneable Bit Security Game



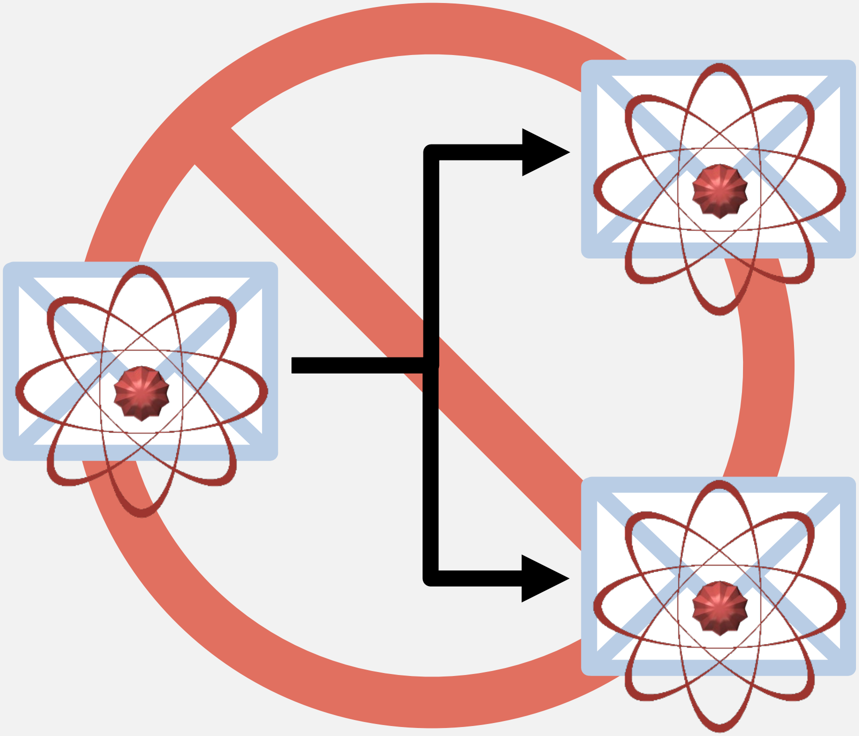
Open Question: does there exist a scheme Enc with:

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

Important step towards Unclonable Indistinguishability

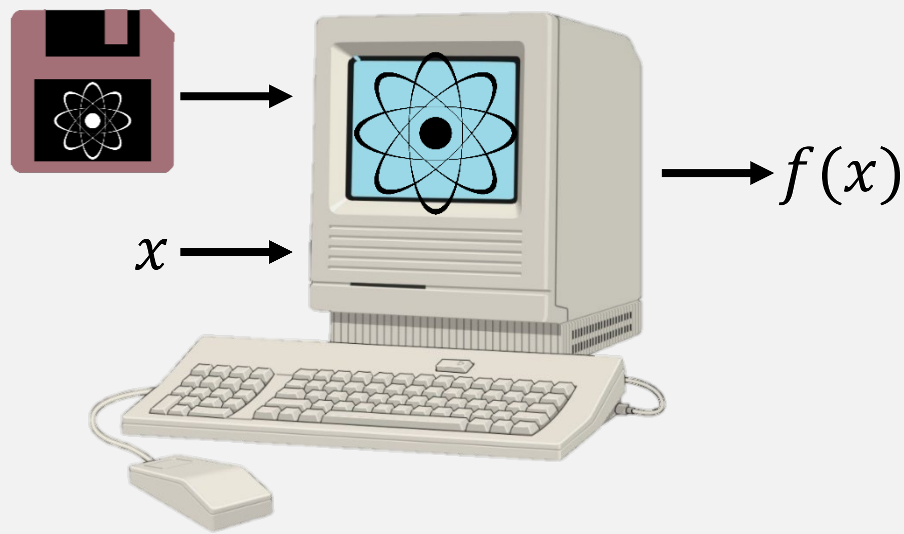
(see Ananth, Kaleoglu, Li, Liu & Zhandry 2022)

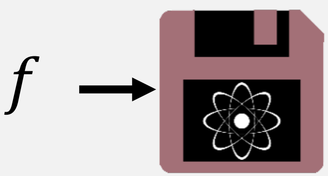
Unclonable Functionality



Quantum Copy-Protection:
Unclonable Software

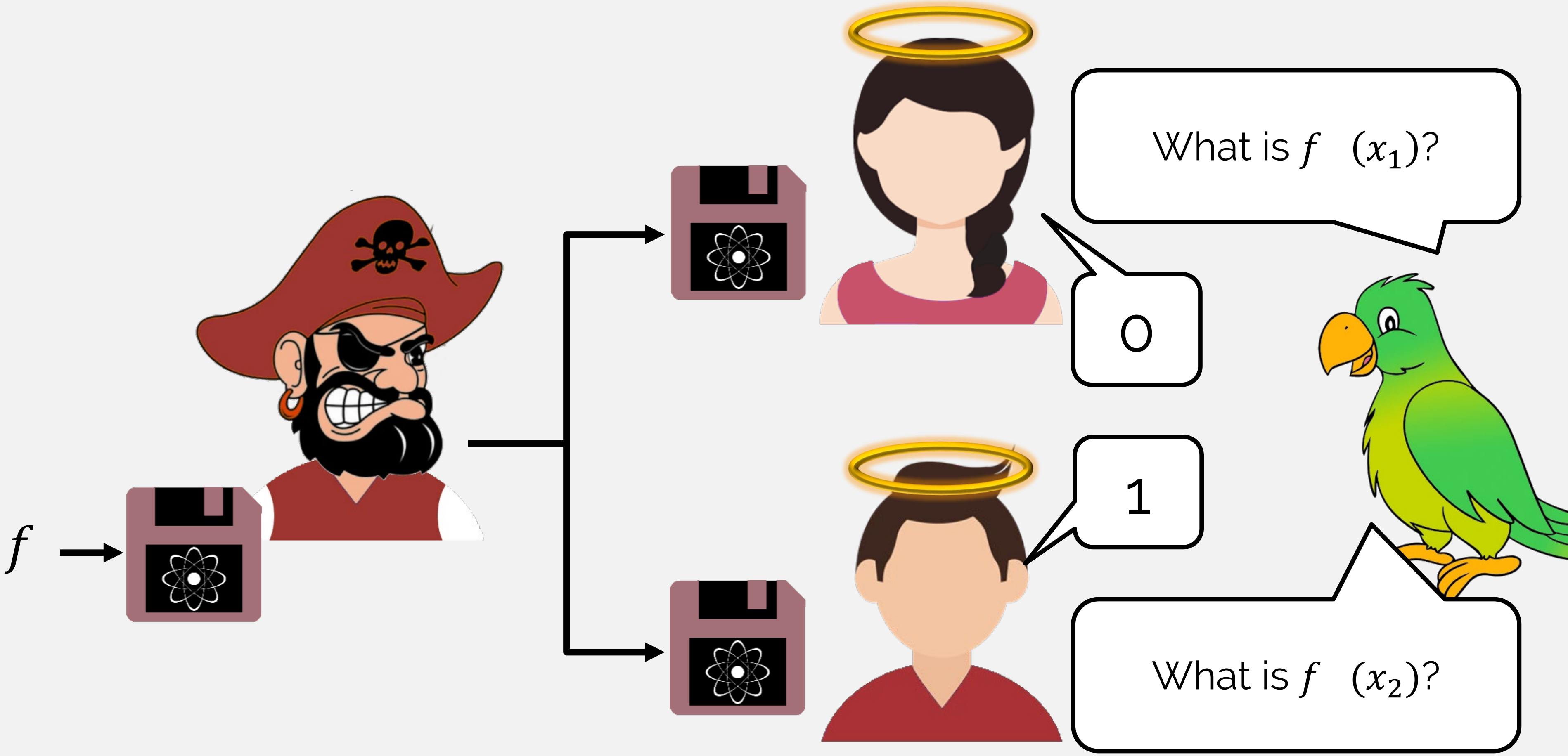
What is quantum copy protection?



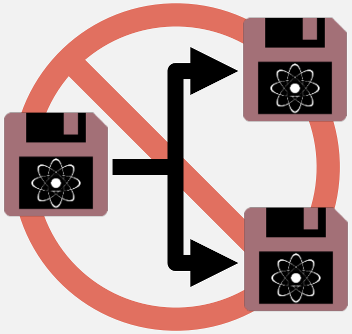


<u>Average Correctness</u>:
Up to some error term η, outcome is correct in expectation over choice of x.

Honest-user Copy Protection



Results on Quantum Copy Protection

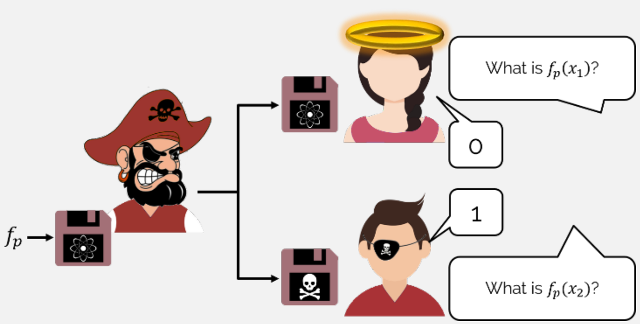


Aaronson 2009:
- All functions (not learnable)
- Assumes a quantum oracle

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

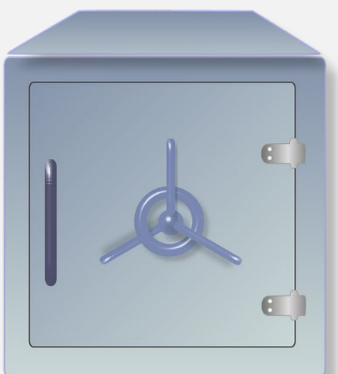
Broadbent, Jeffery, Lord, Podder, Sundaram 2021:
- Point Functions
- Restricted Class of Adversaries
  - "Honest-Malicious"
- No other assumptions



Conclusion

Quantum Unclonability is inspired by the physical world

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.



What else can we make uncloneable?

Thank you!