Quantum Cryptography

Anne Broadbent

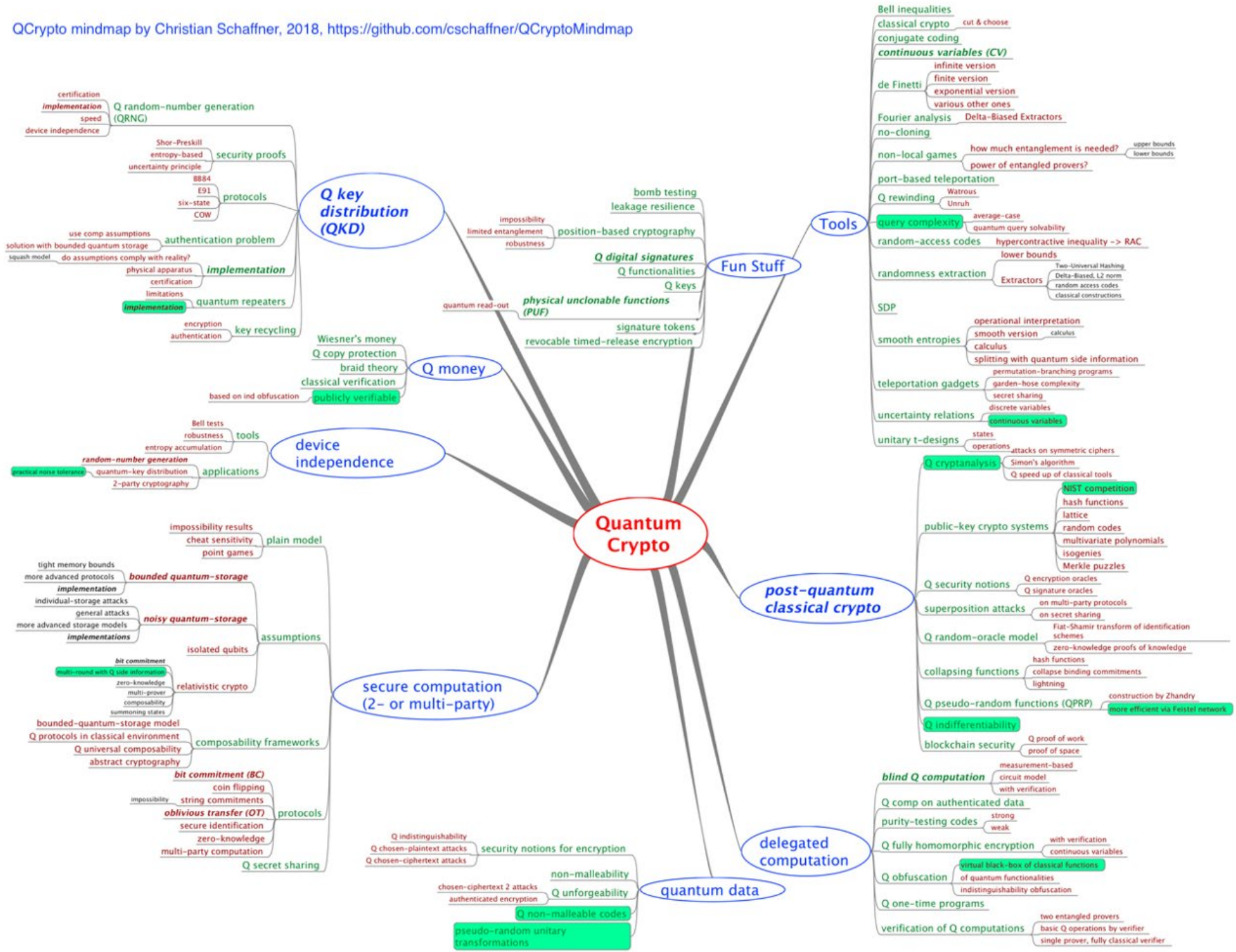

uOttawa

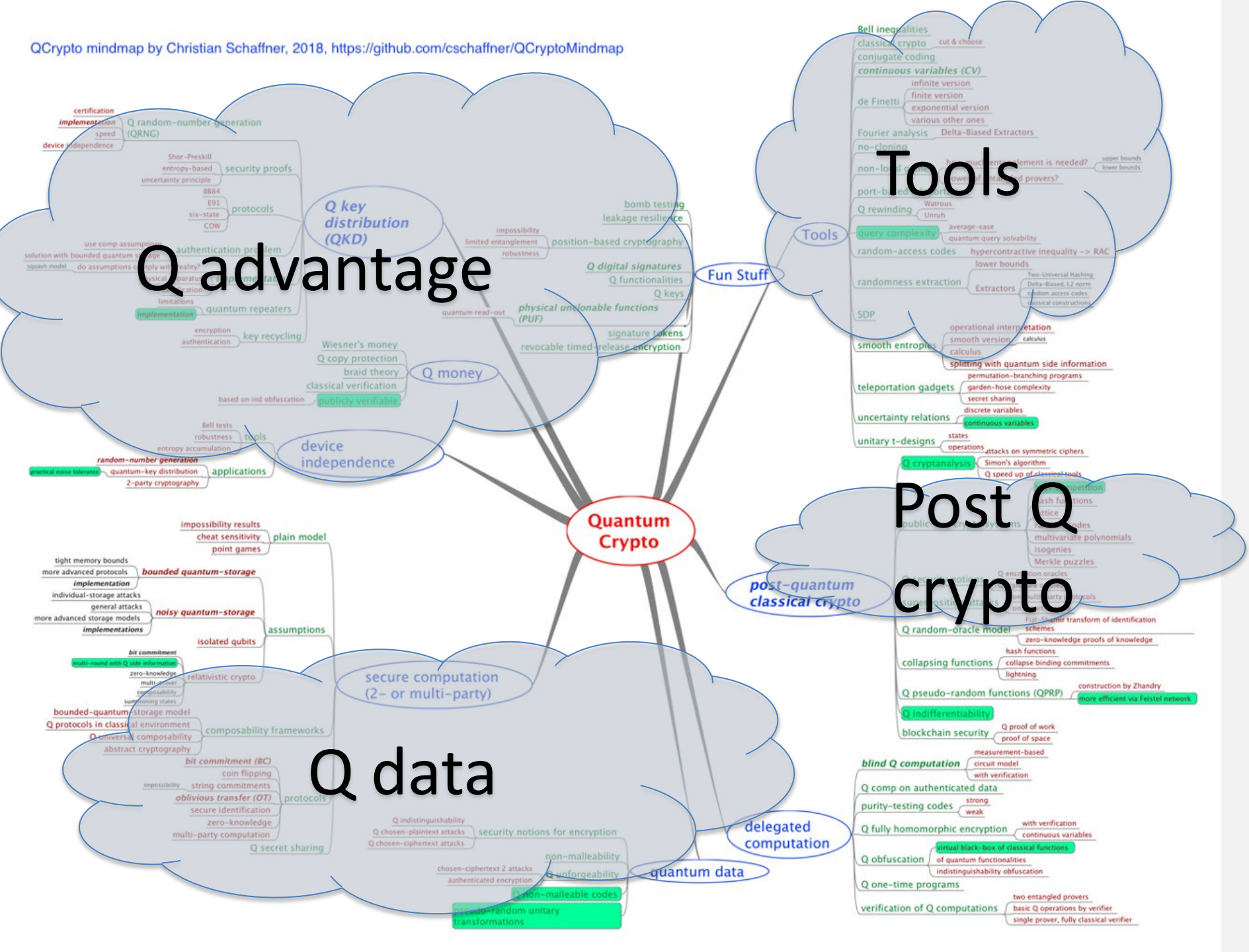
SAC 2024 Tutorial
August 25 2024

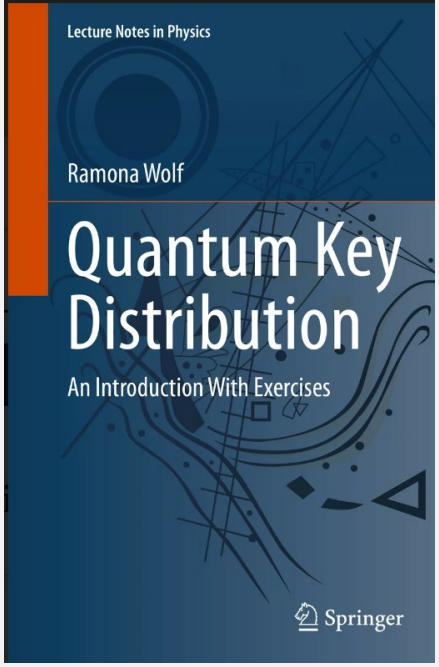
What is quantum cryptography?

- Classical cryptography:
  - Information processing in the presence of an adversary.
- Quantum cryptography:
  - Information processing in the presence of an adversary where at least one party has quantum capabilities.

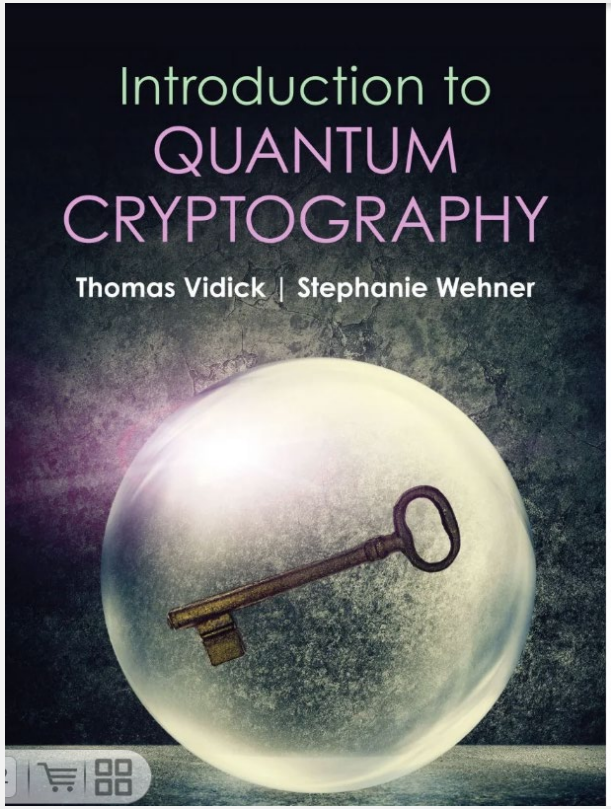
QCrypto mindmap by Christian Schaffner, 2018, https://github.com/cschaffner/QCryptoMindmap




QCrypto mindmap by Christian Schaffner, 2018, https://github.com/cschaffner/QCryptoMindmap
Q advantage
Tools
Post Q crypto
Q data
Quantum Crypto
Fun Stuff
Q key distribution (QKD)
Q money
device independence
post-quantum classical crypto
secure computation (2- or multi-party)
delegated computation
quantum data
Q random-number generation (QRNG)
security proofs
protocols
authentication problem
quantum repeaters
key recycling
Wiesner's money
Q copy protection
braid theory
classical verification
publicly verifiable
tools
applications
bomb testing
leakage resilience
position-based cryptography
Q digital signatures
Q functionalities
Q keys
physical unclonable functions (PUF)
signature tokens
revocable timed-release encryption
Bell inequalities
classical crypto
conjugate coding
continuous variables (CV)
de Finetti
Fourier analysis
Delta-Biased Extractors
no-cloning
Q rewinding
query complexity
random-access codes
randomness extraction
Extractors
SDP
smooth entropies
teleportation gadgets
uncertainty relations
unitary t-designs
Q cryptanalysis
multivariate polynomials
isogenies
Merkle puzzles
Q random-oracle model
collapsing functions
Q pseudo-random functions (QPRP)
Q indifferentiability
blockchain security
plain model
assumptions
bounded quantum-storage
noisy quantum-storage
isolated qubits
relativistic crypto
composability frameworks
bounded-quantum-storage model
Q protocols in classical environment
Q universal composability
abstract cryptography
protocols
bit commitment (BC)
coin flipping
string commitments
oblivious transfer (OT)
secure identification
zero-knowledge
multi-party computation
Q secret sharing
security notions for encryption
non-malleability
Q unforgeability
Q non-malleable codes
pseudo-random unitary transformations
blind Q computation
Q comp on authenticated data
purity-testing codes
Q fully homomorphic encryption
Q obfuscation
Q one-time programs
verification of Q computations



https://ramonawolf.com/qkdtextbook/



https://www.cambridge.org/highereducation/books/introduction-to-quantum-cryptography

Des. Codes Cryptogr. (2016) 78:351–382
DOI 10.1007/s10623-015-0157-4

CrossMark

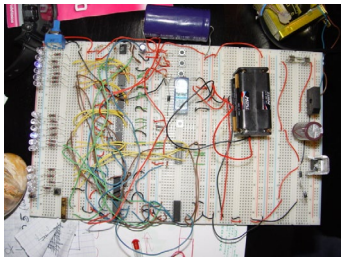
Quantum cryptography beyond quantum key distribution

Anne Broadbent[1] · **Christian Schaffner**[2]

https://arxiv.org/abs/1510.06120

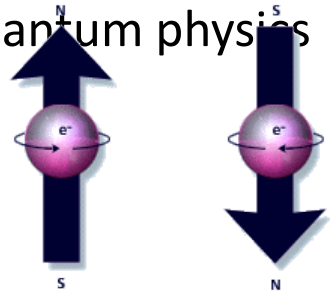
Information is physical

- bit: can be represented by an electrical voltage in an electronic circuit.
- Obeys the laws of classical physics



Conventional computers

- **qu**antum **bit** (qubit): can be represented by electron spin, photon polarization, quantum dot, etc.
- Obeys the laws of quantum physics



Quantum computers

In this tutorial:

- How to use quantum information to build cool stuff
- unforgeable money
- perfectly secure communication
- …and more!

Quantum States Can't be Cloned

"Quantum no-cloning theorem"
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.

But first, some basics

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 .

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

Measurements: qubits ⟶ bits

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

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

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

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

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

Measurement destroys the quantum state.

Measurement destroys the quantum state.

Sounds Annoying!
Can this principle be useful?

Answer: YES!
But first, let's see another related principle.

Transformations

Postulate: quantum evolutions are linear

$\Longrightarrow$transformations are given by matrix multiplication.

Q: Which types of matrices are valid quantum transformations?

A: Those that map quantum states to quantum states!

e.g. Suppose $U(\alpha|0\rangle + \beta|1\rangle) = \alpha'|0\rangle + \beta'|1\rangle$

Then U is a valid quantum operation if:

$$|\alpha|^2 + |\beta|^2 = 1 \Rightarrow |\alpha'|^2 + |\beta'|^2 = 1$$

Definition: A matrix is unitary if it preserves the Euclidean norm. Thus unitary matrices are the valid quantum transformations

Claim: A matrix U over $\mathbb{C}$ is unitary if and only if $UU^\dagger = I$ where $U^\dagger = (U^T)^*$.

Multi-qubit systems

Systems of qubits are combined with the tensor product:

$$\begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix}\otimes\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix}\equiv\begin{pmatrix}\alpha_1\alpha_2\\ \alpha_1\beta_2\\ \beta_1\alpha_2\\ \beta_1\beta_2\end{pmatrix}\quad \text{e.g. } |0\rangle\otimes|1\rangle\equiv|0\rangle|1\rangle\equiv|01\rangle=\begin{pmatrix}0\\ 1\\ 0\\ 0\end{pmatrix}$$

More generally, an *n*-qubit system can be in an arbitrary superposition of 2^n basis states, $|00\cdots0\rangle, |00\cdots1\rangle, \ldots, |11\cdots1\rangle$

$$\sum_{x\in\{0,1\}^n}\alpha_x|x\rangle, \sum_x|\alpha_x|^2=1$$

Once more, unitary matrices are the valid quantum transformations.
For an *n*-qubit system, we have a 2^n-dimensional vector, therefore the unitaries are matrices of size $2^n \times 2^n$.

Examples of 1-qubit unitaries

Identity

$$\mathsf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Not (aka Pauli-X)

$$\mathsf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \begin{aligned} \mathsf{X}|0\rangle &= |1\rangle \\ \mathsf{X}|1\rangle &= |0\rangle \end{aligned}$$

Hadamard

$$\mathsf{H} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

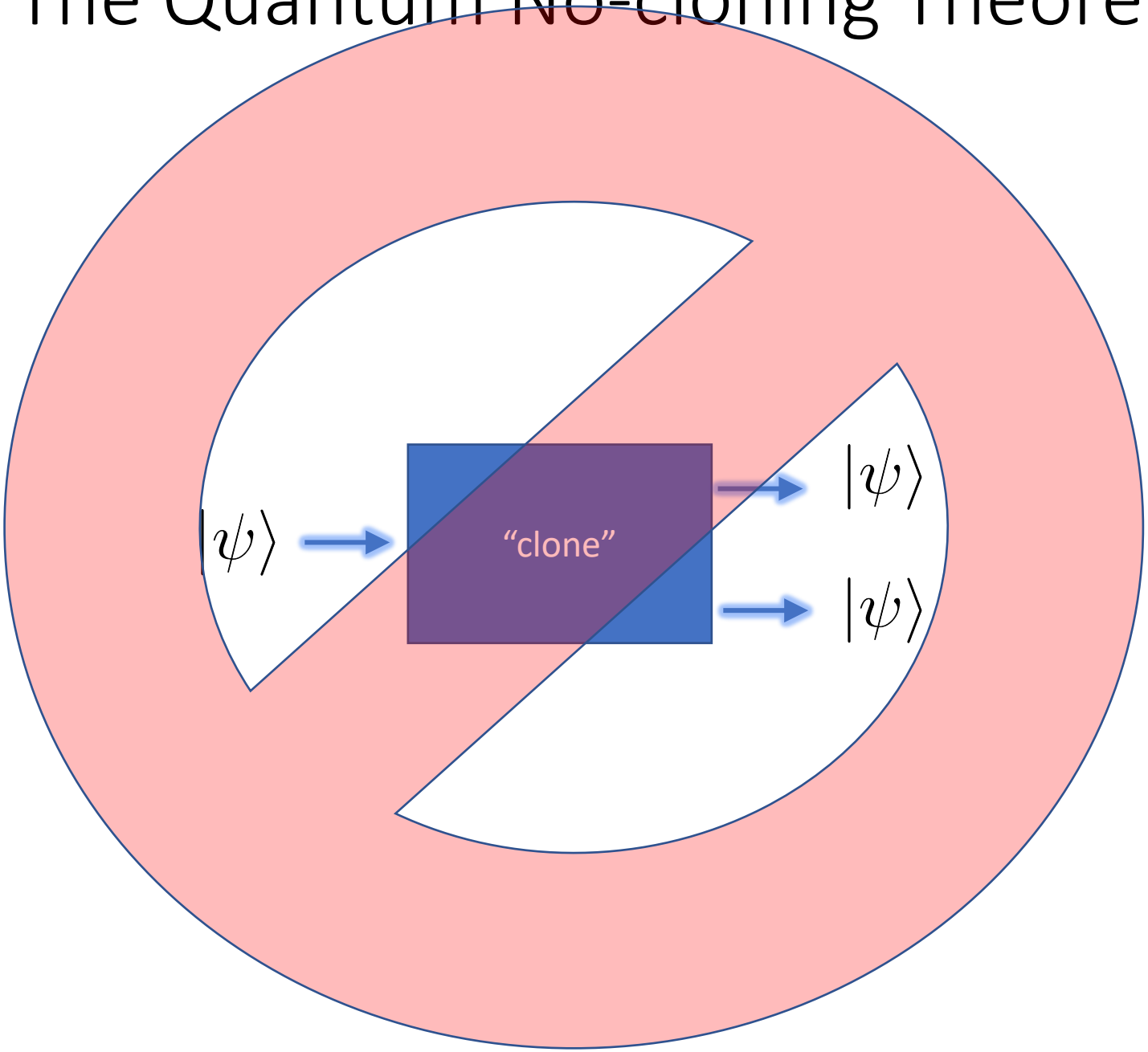
$$\mathsf{H}\mathsf{H}^\dagger = \tfrac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \tfrac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \mathsf{I}$$

$$\begin{aligned} \mathsf{H}|0\rangle &= \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle \equiv |+\rangle \\ \mathsf{H}|1\rangle &= \tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle \equiv |-\rangle \end{aligned}$$

Pauli-Z

$$\mathsf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \begin{aligned} \mathsf{Z}|+\rangle &= |-\rangle \\ \mathsf{Z}|-\rangle &= |+\rangle \end{aligned}$$

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 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

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

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

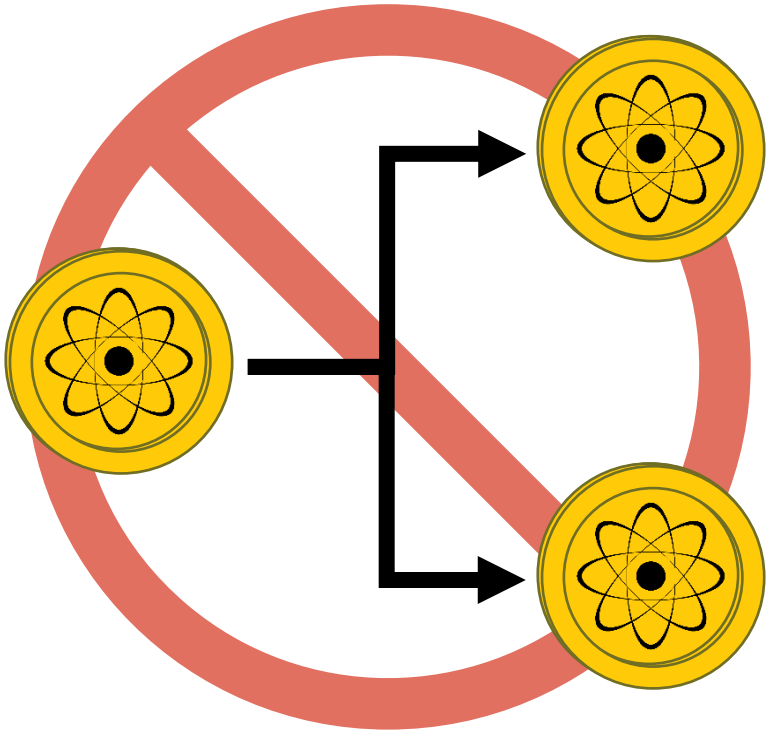
$$U|00\rangle = |00\rangle$$
$$U|10\rangle = |11\rangle$$

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 $\alpha = \beta = \frac{1}{\sqrt{2}}$).

In general, it is not possible to copy an unknown quantum state.

Sounds Annoying!
Can this principle be useful?

Unclonable 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 $|b\rangle_\theta = H^\theta |b\rangle$

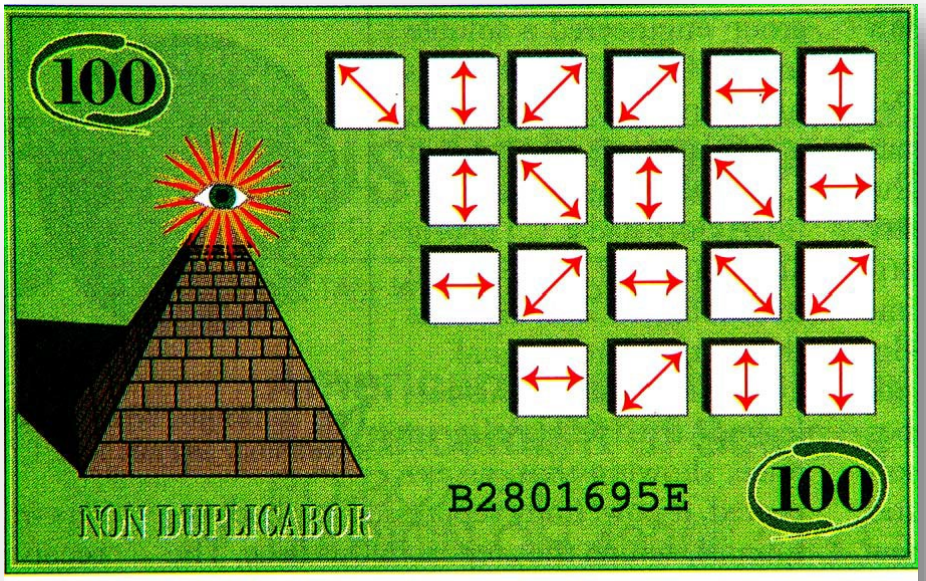
θ	b	$\|b\rangle_\theta$
0	0	$\|0\rangle$
0	1	$\|1\rangle$
1	0	$\|+\rangle$
1	1	$\|-\rangle$

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

- Can easily verify $|b\rangle_\theta$ if b, θ are known.
- Intuitively: without knowledge of the encoding basis, and given $|b\rangle_\theta$, no third party can create two quantum states that **both** 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 $b, \theta \in \{0,1\}^n$:

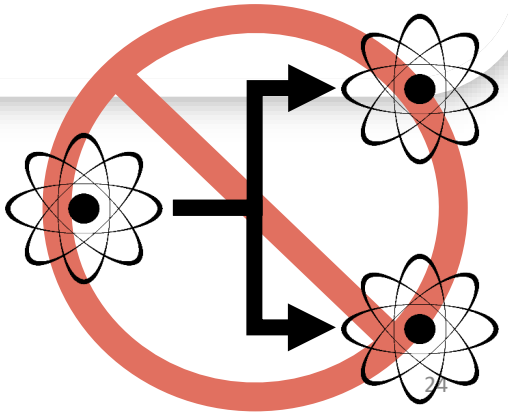


A quantum banknote, containing particles in a secret set of quantum states, cannot be copied by counterfeiters, who would disturb the particles by attempting to observe them.

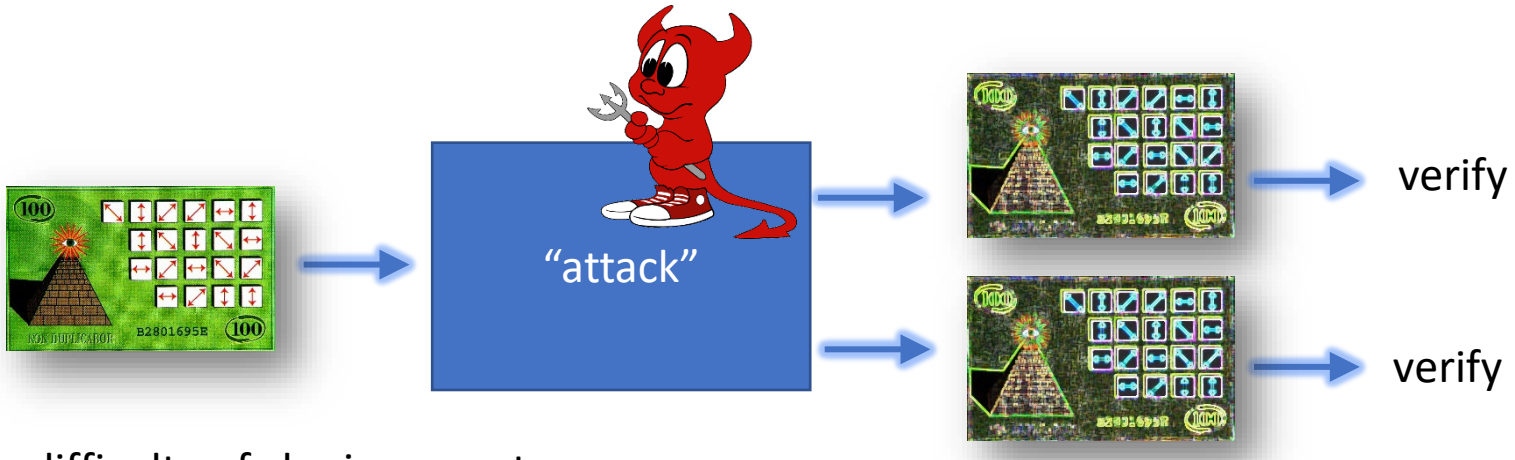
©AAAS (1992)

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?

For a single qubit, one possible attack is to guess a basis θ uniformly, measure in θ, and re-send two identical qubits encoded in θ that correspond to this measurement outcome.

What is the success prob. of this attack?

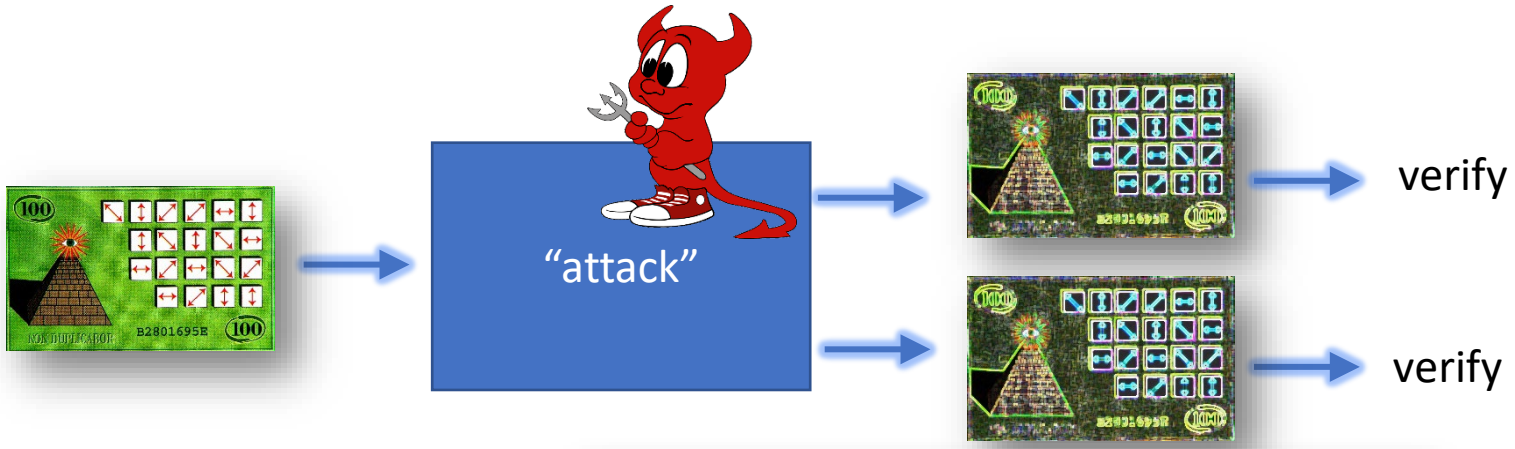
A) 1
B) 1 /2
C) 5/8

- If the basis is correct (prob= ½), the attack succeeds with prob. 1.
- If the basis is incorrect, the attack success with prob. 1/4 since the attack prepares qubits in the complementary basis, and the probability that both verifiers accept is ½*½ = ¼.

Success prob. of attack = ½ + ½*¼ = 5/8.

Can actually achieve ¾ (and this is optimal).

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.

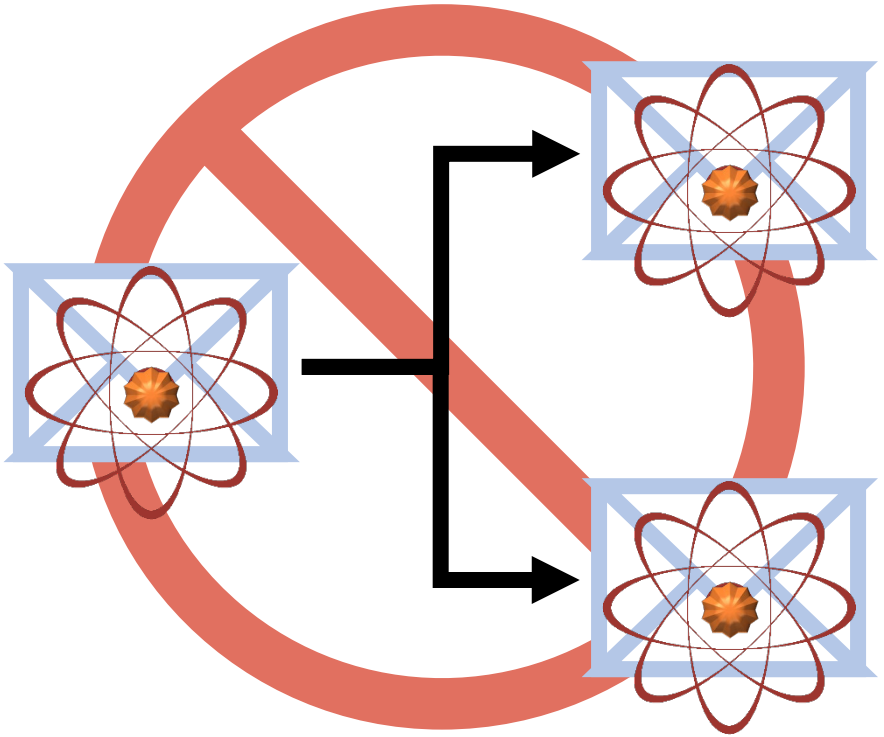
Quantum Money “revival”

- **Noise-tolerant** (‘feasible with current technology’) quantum money
  - Pastawski, Yao, Jiang, Lukin, Cirac (2012)

- Quantum Money with **classical verification**
  - Gavinsky (2012)

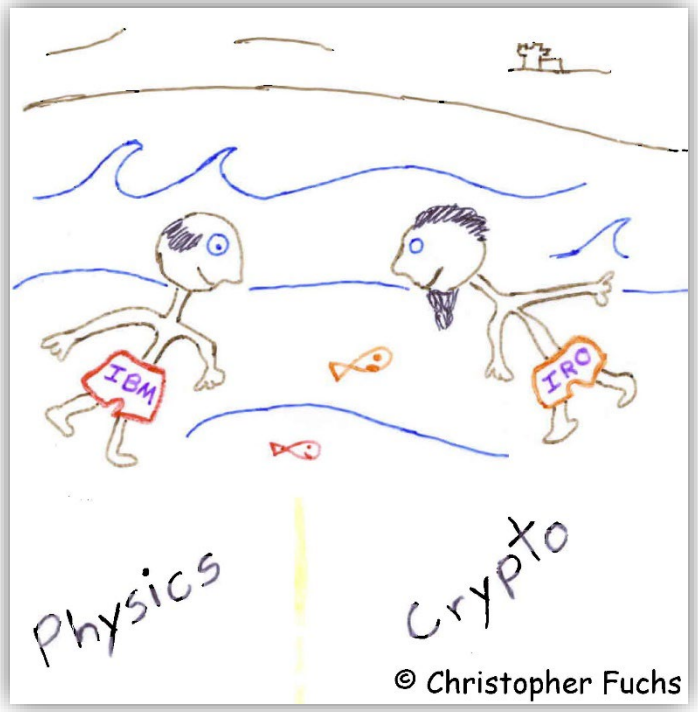
- **Public-key** quantum money (can be verified by any user)
  - Farhi, Gosset, Hassidim, Lutomirski, and Shor (2012)
  - Aaronson and Christiano (2012)
  - Zhandry (2019)
  - Schmueli (2022)

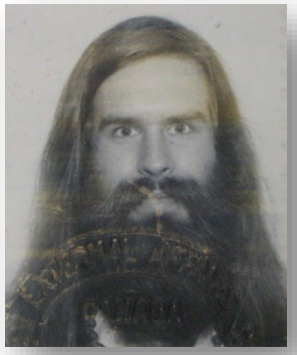
Unclonable Information



1979

Charles
Bennett
Physicist
IBM, USA





Gilles
Brassard
Computer
Scientist
Université
de Montréal,
Canada

Ultimate goal:
Information-theoretic security

AES ?

No !

RSA ?

No !

The One-time Pad Encryption Scheme

Plaintext	$x \in \{0,1\}$
Key	$k \in_R \{0,1\}$
Ciphertext	$x \oplus k$

Since the ciphertext is uniformly random (as long as *k* is random, unknown and used only once), the plaintext is perfectly concealed.

The Washington-Moscow Hot Line (est.1963)

Conjugate coding to the rescue!

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"

BB84 QKD

- Version 1
- A very high-level

Quantum Key Distribution

Bennett and Brassard (1984)

Quantum Key Distribution

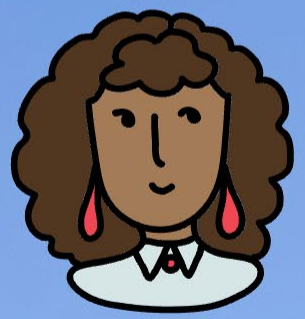
Bennett and Brassard (1984)

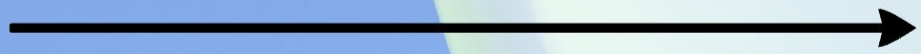
Quantum Key Distribution

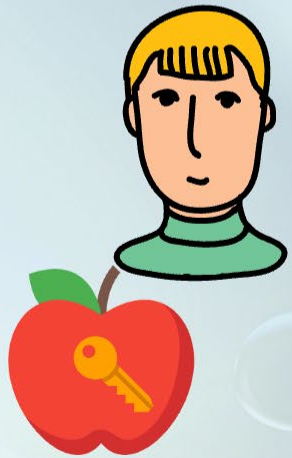
Bennett and Brassard (1984)

Quantum Key Distribution

Bennett and Brassard (1984)

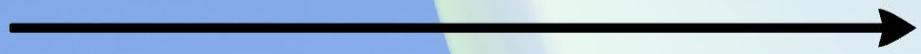


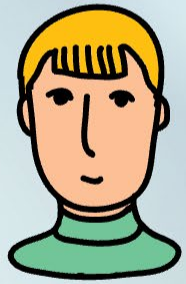




Quantum Key Distribution

Bennett and Brassard (1984)



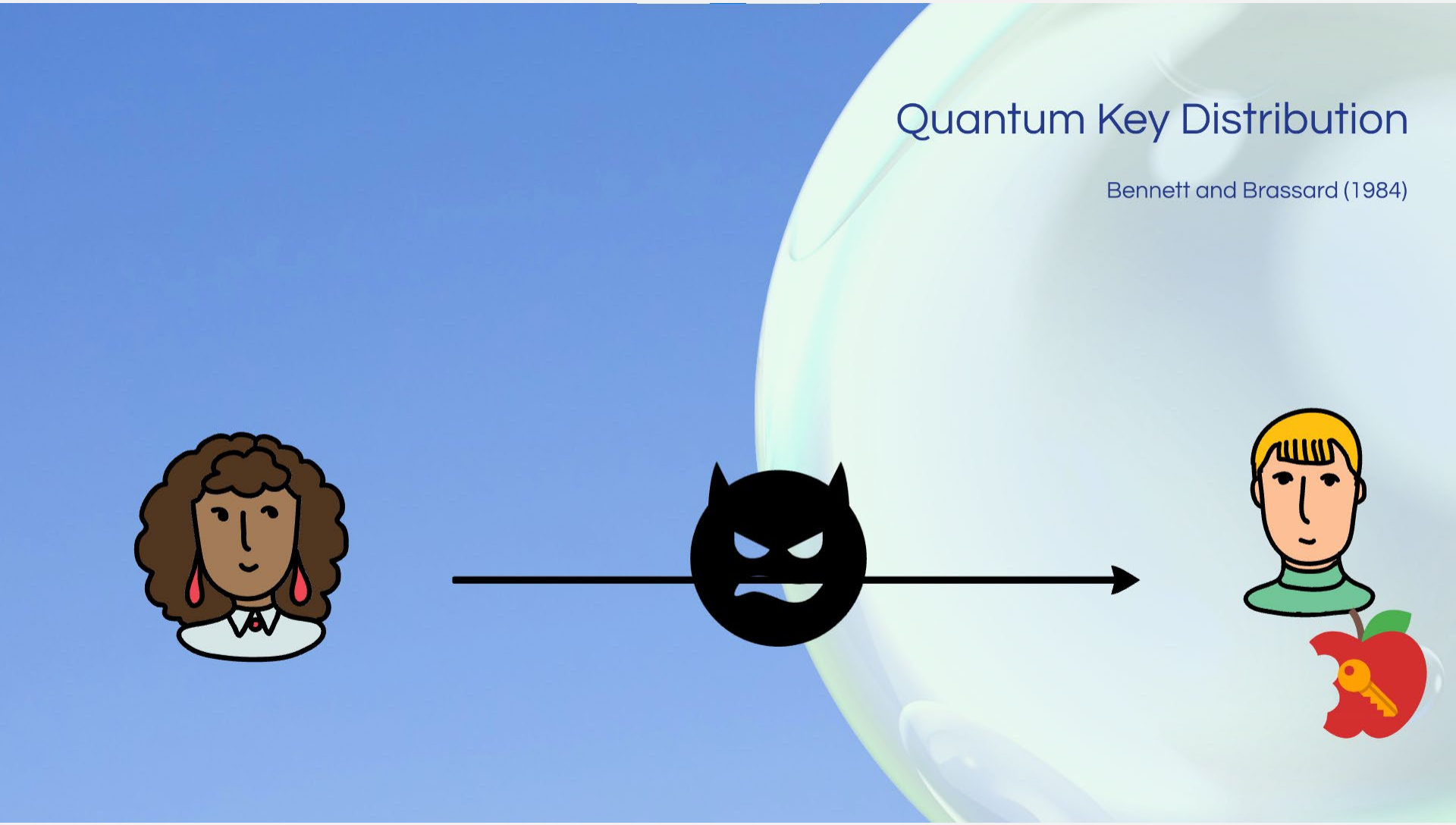


Quantum Key Distribution

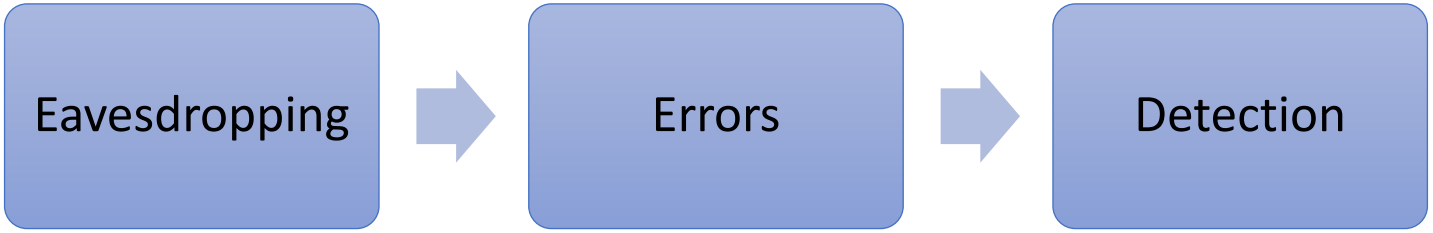
Bennett and Brassard (1984)

Quantum Key Distribution

Bennett and Brassard (1984)



Quantum Key Distribution



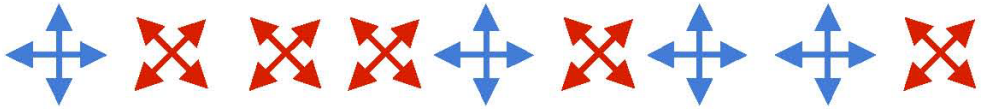
- Use quantum channel to send a random key
- If no eavesdropping detected, use the established key in the one-time pad scheme.

BB84 QKD

- Version 2
- A high-level

« BB84 » Protocol (Bennett & Brassard, 1984)

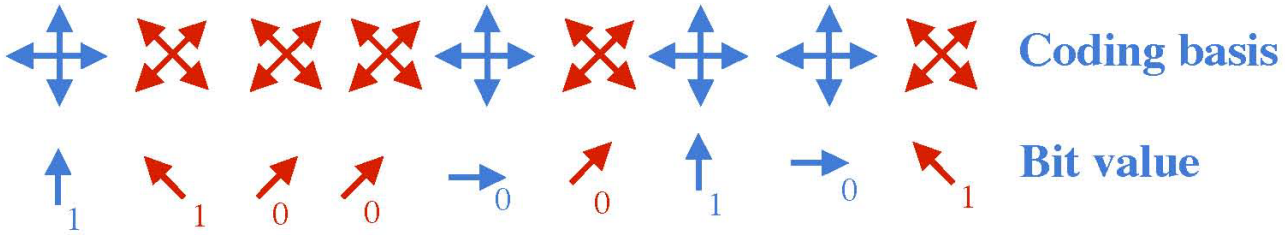
Alice



Coding basis

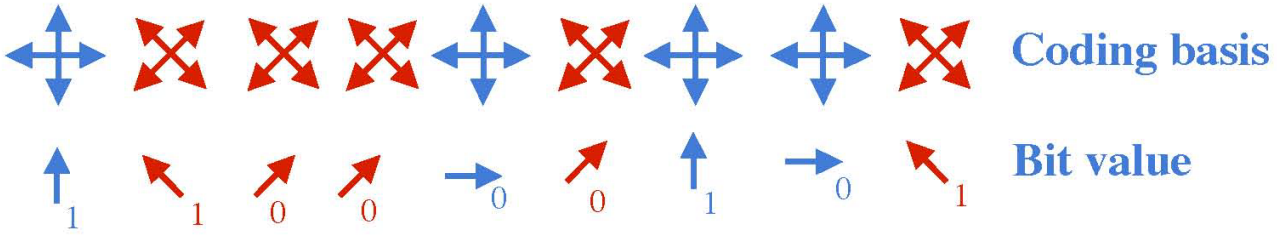
« BB84 » Protocol (Bennett & Brassard, 1984)

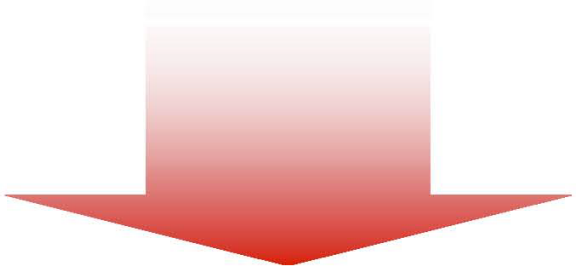
Alice



« BB84 » Protocol (Bennett & Brassard, 1984)

Alice

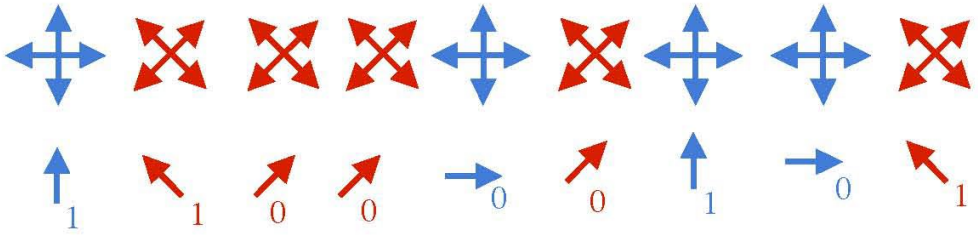


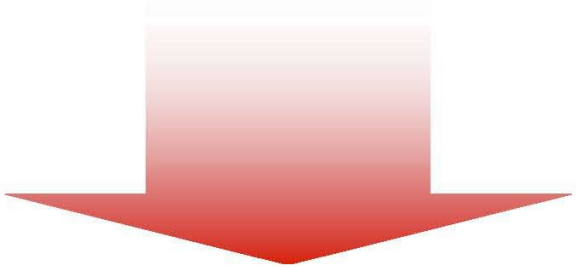


Bob

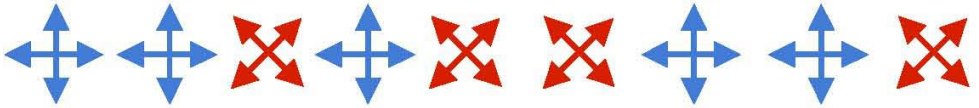
« BB84 » Protocol (Bennett & Brassard, 1984)

Alice



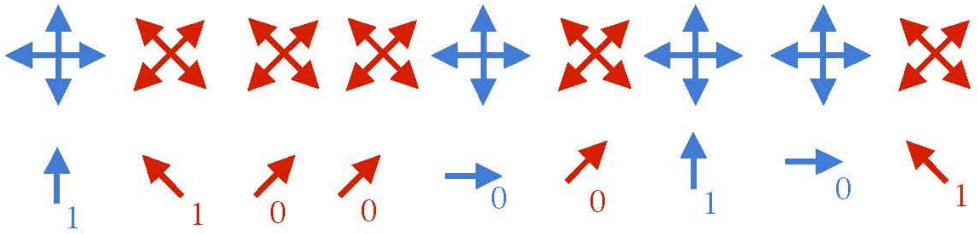


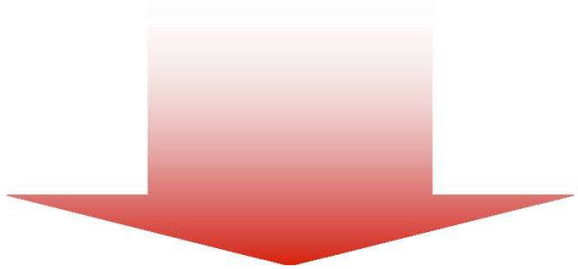
Bob



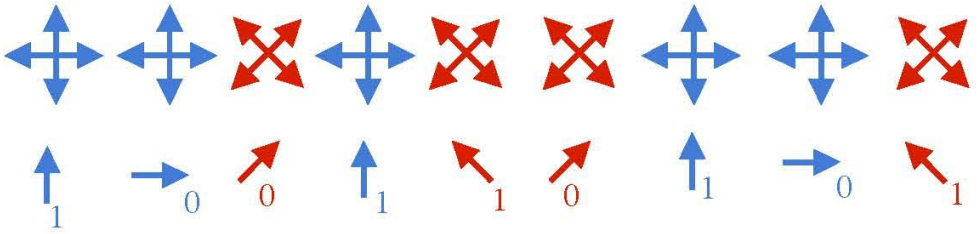
« BB84 » Protocol (Bennett & Brassard, 1984)

Alice



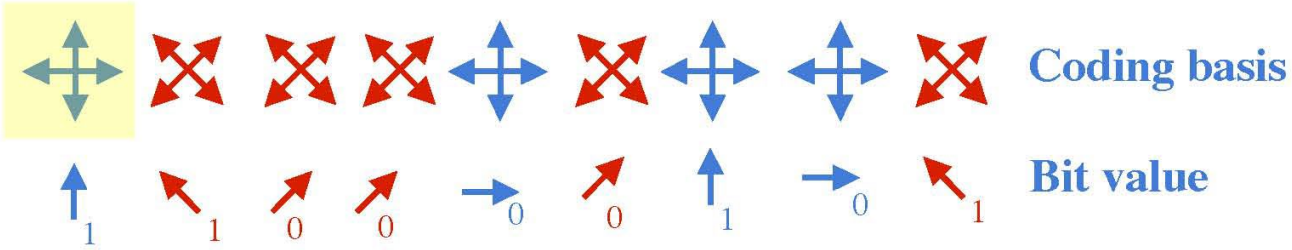


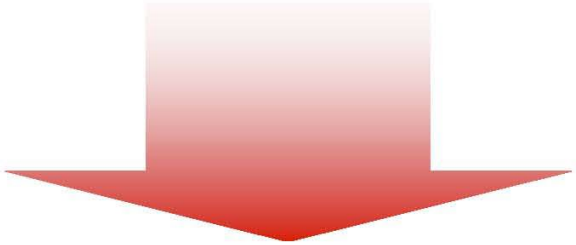
Bob



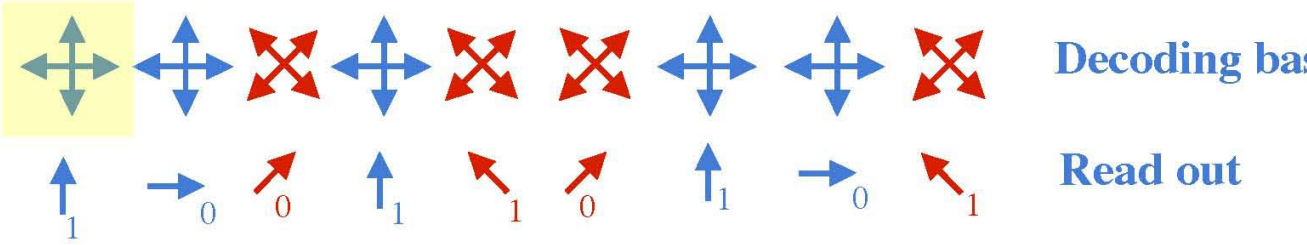
« BB84 » Protocol (Bennett & Brassard, 1984)

Alice



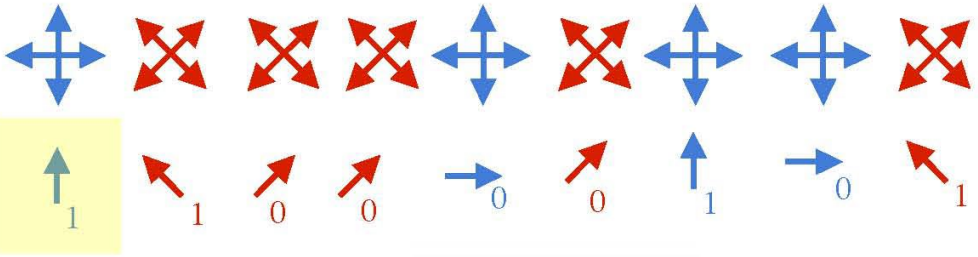


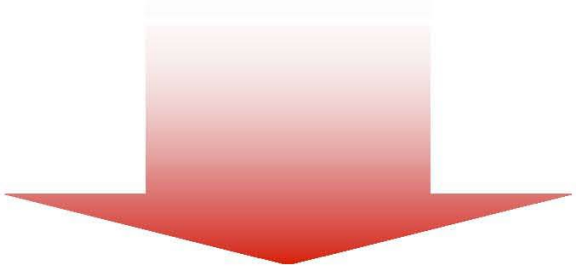
Bob



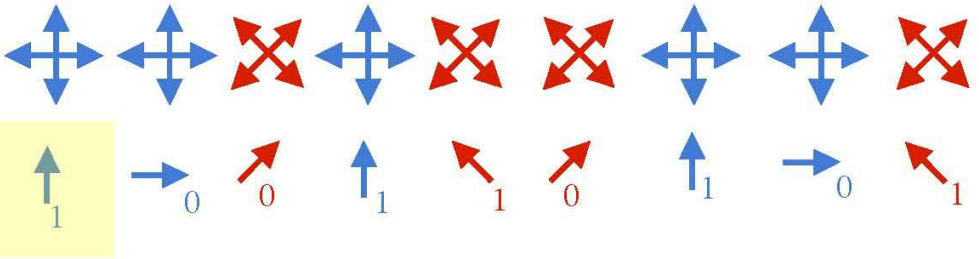
« BB84 » Protocol (Bennett & Brassard, 1984)

Alice



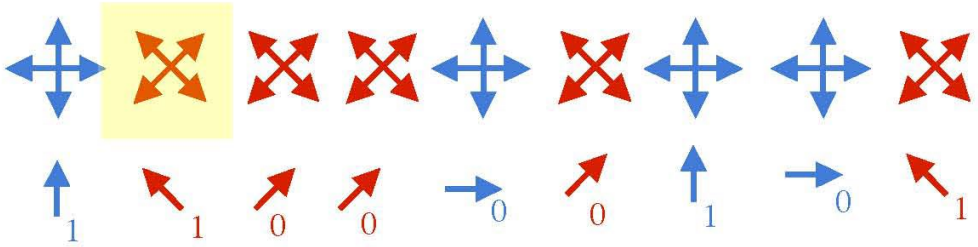


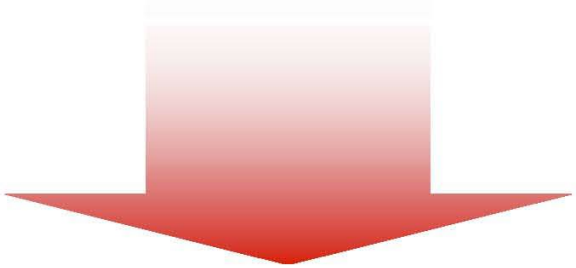
Bob



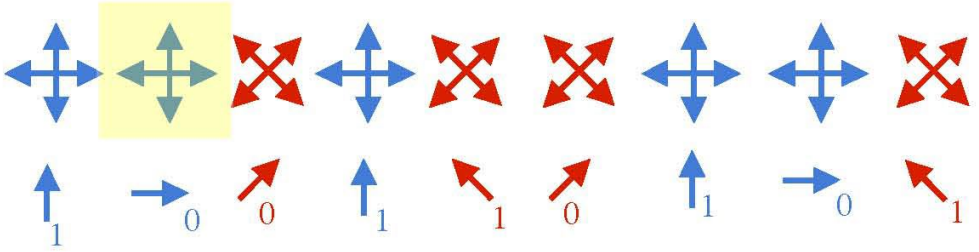
« BB84 » Protocol (Bennett & Brassard, 1984)

Alice



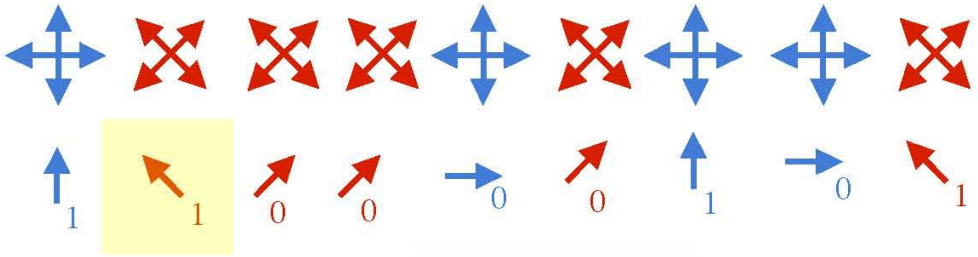


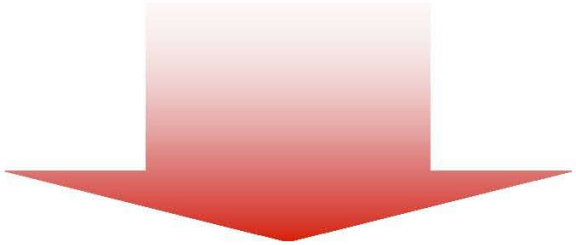
Bob



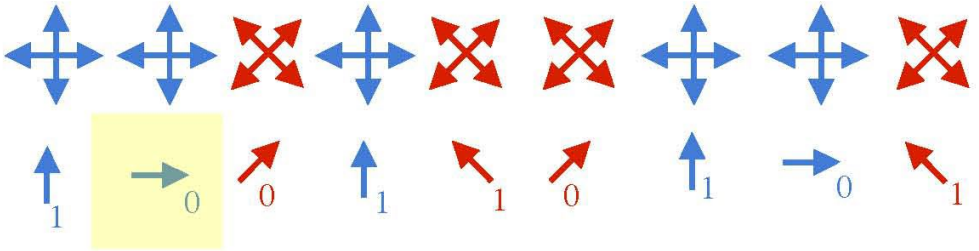
« BB84 » Protocol (Bennett & Brassard, 1984)

Alice



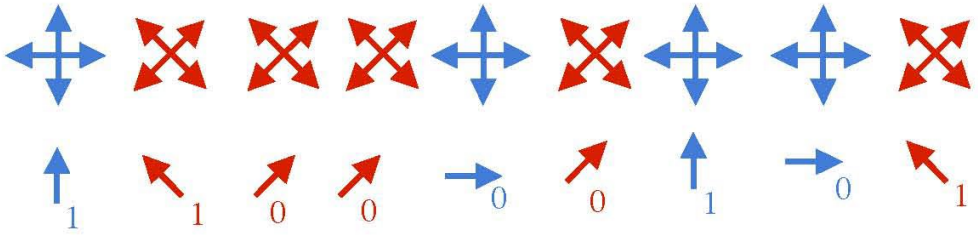


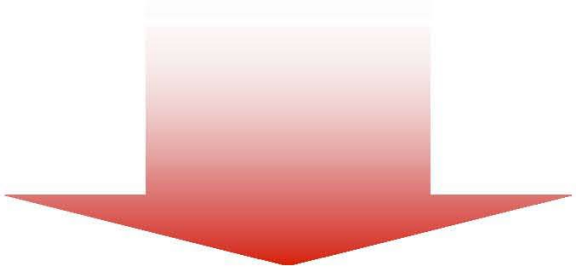
Bob

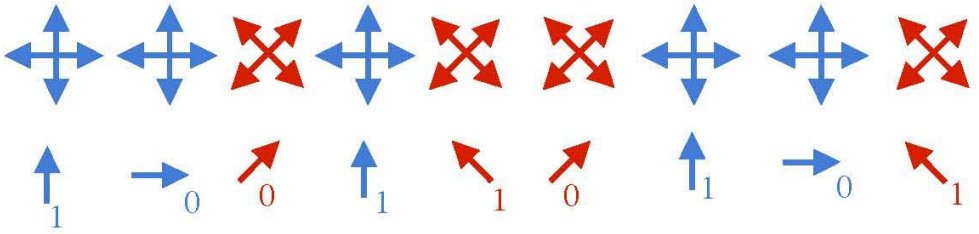


« BB84 » Protocol (Bennett & Brassard, 1984)

Alice



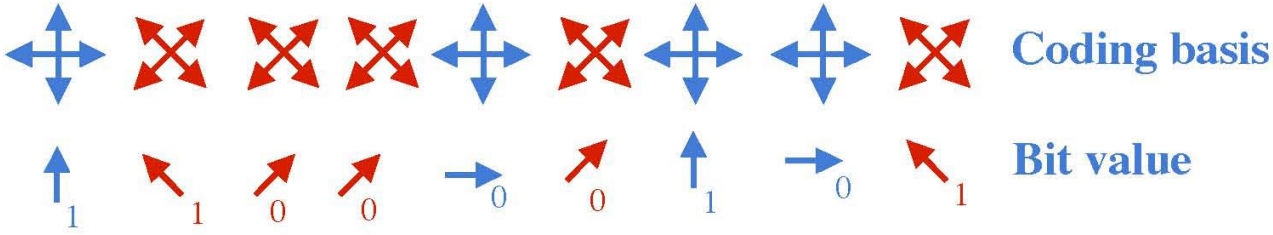


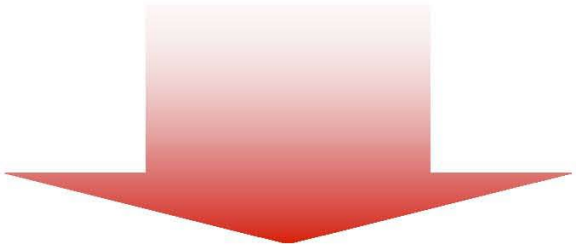


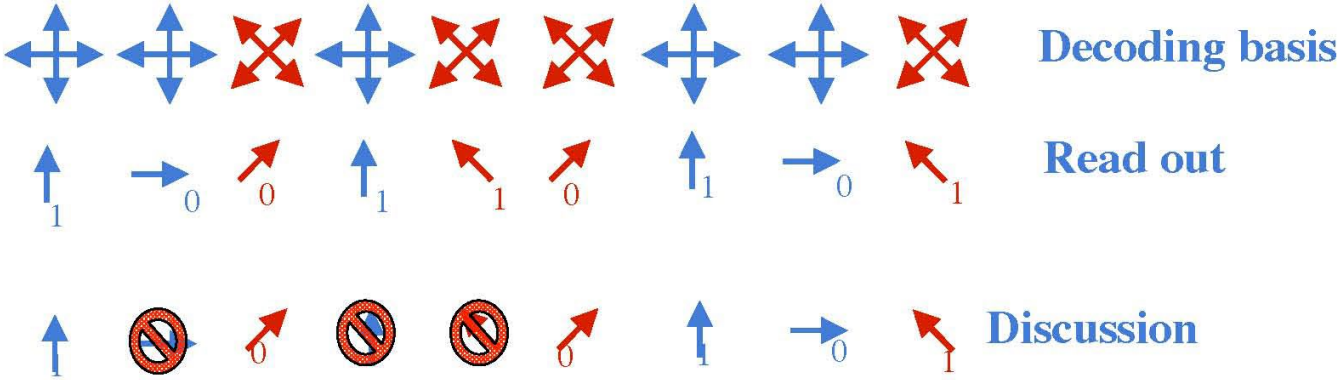
Bob

« BB84 » Protocol (Bennett & Brassard, 1984)

Alice





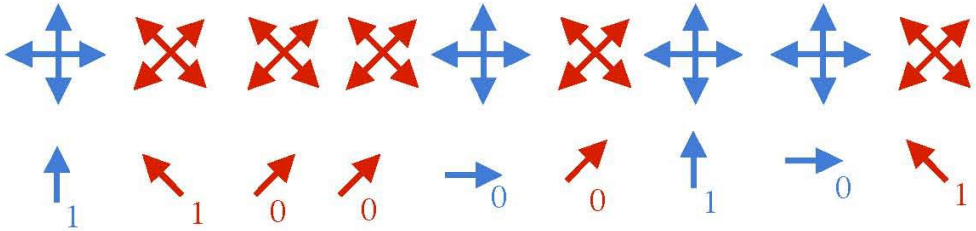


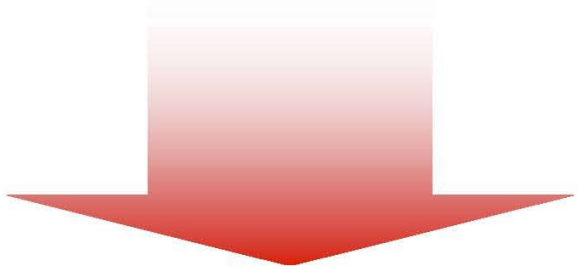
Bob

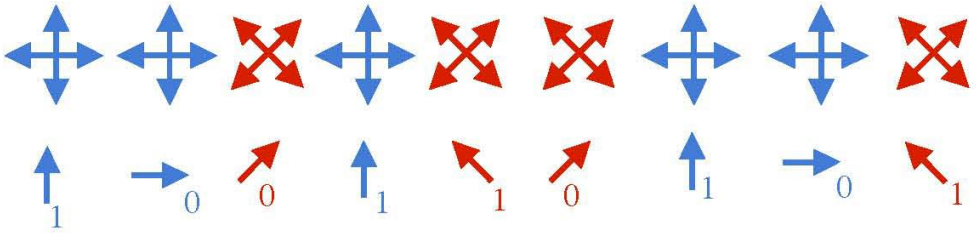
« BB84 » Protocol (Bennett & Brassard, 1984)

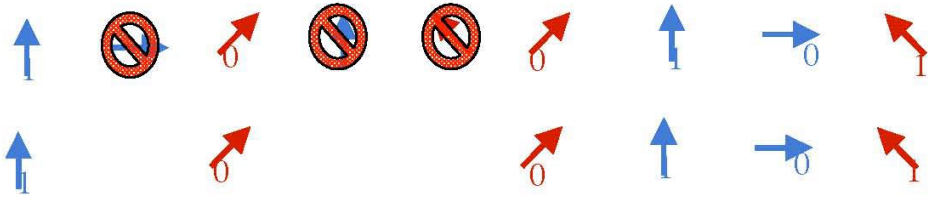
Alice

Bob





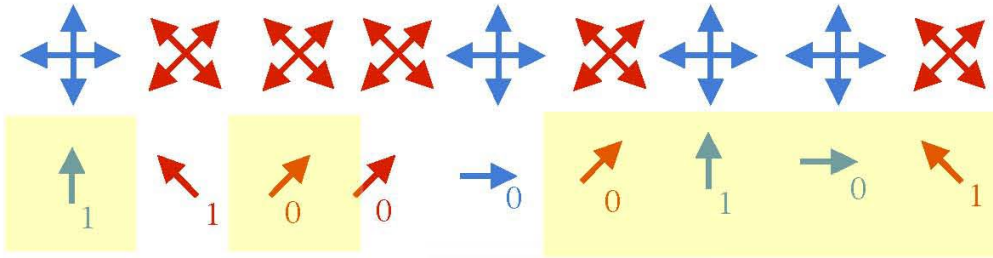


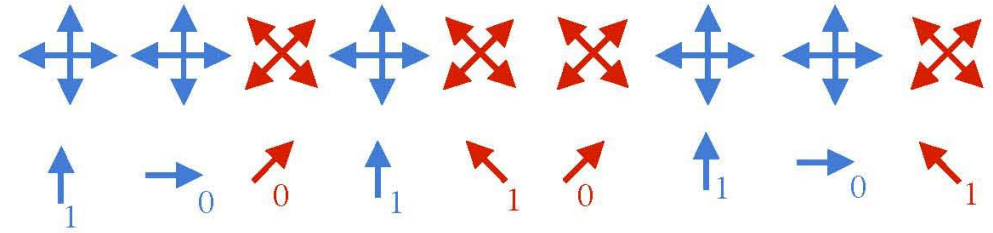


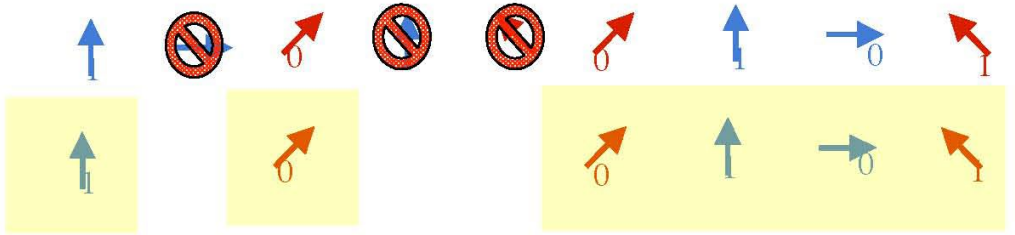
« BB84 » Protocol (Bennett & Brassard, 1984)

Alice

Bob



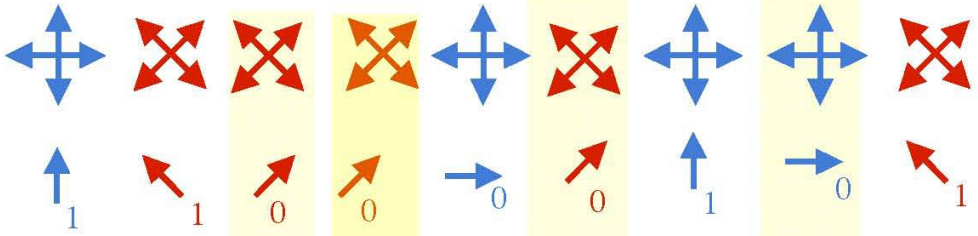




« BB84 » Protocol (Bennett & Brassard, 1984)

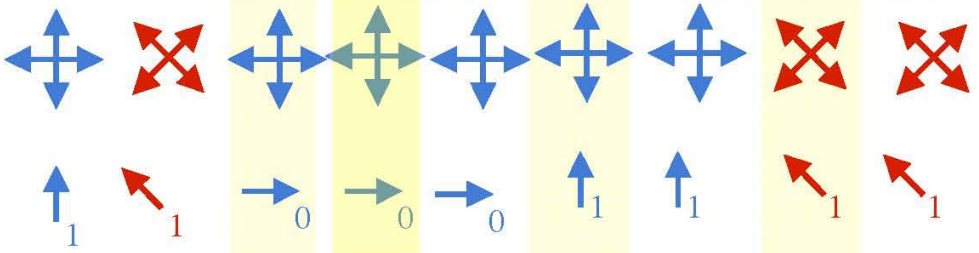
Alice

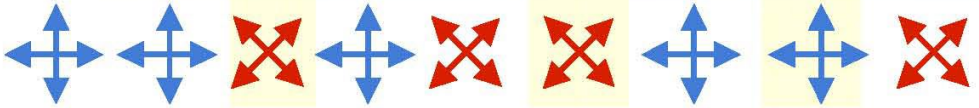
Bob



Coding basis

Bit value





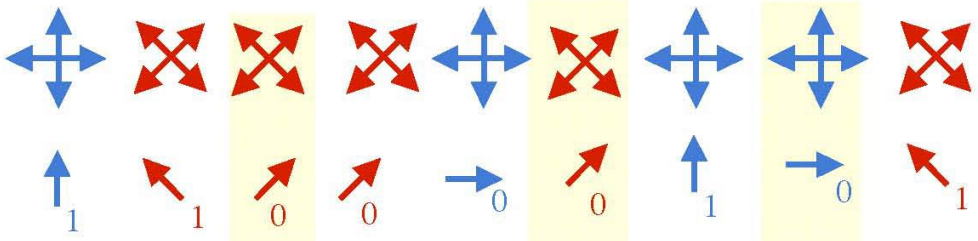
Decoding basis

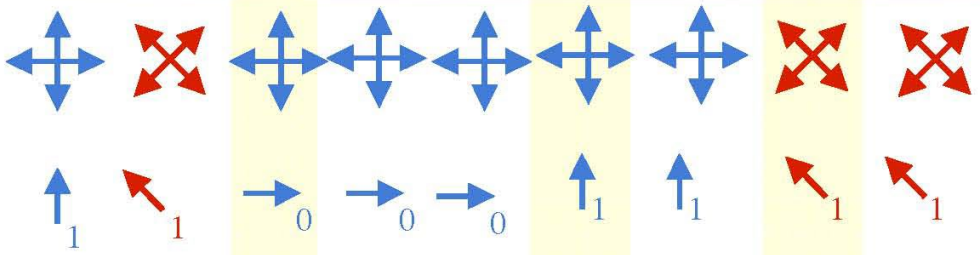
Eve

« BB84 » Protocol (Bennett & Brassard, 1984)

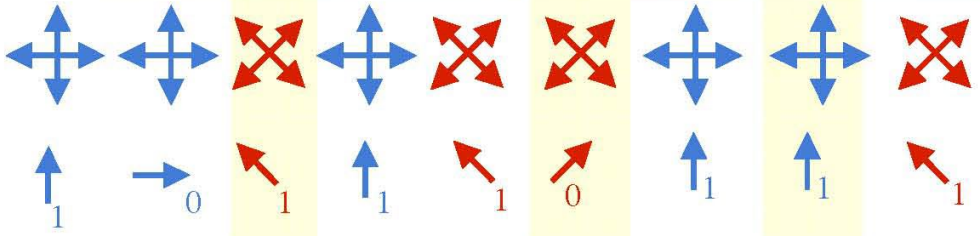
Alice

Bob

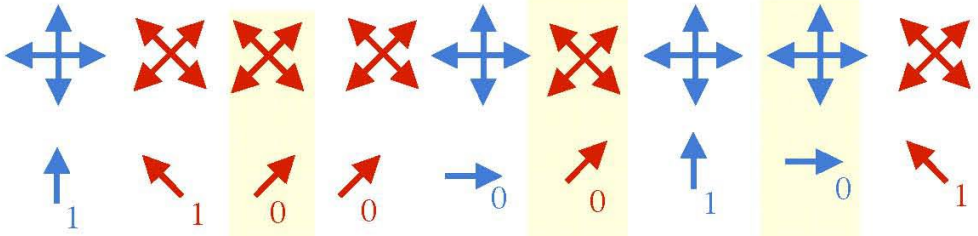


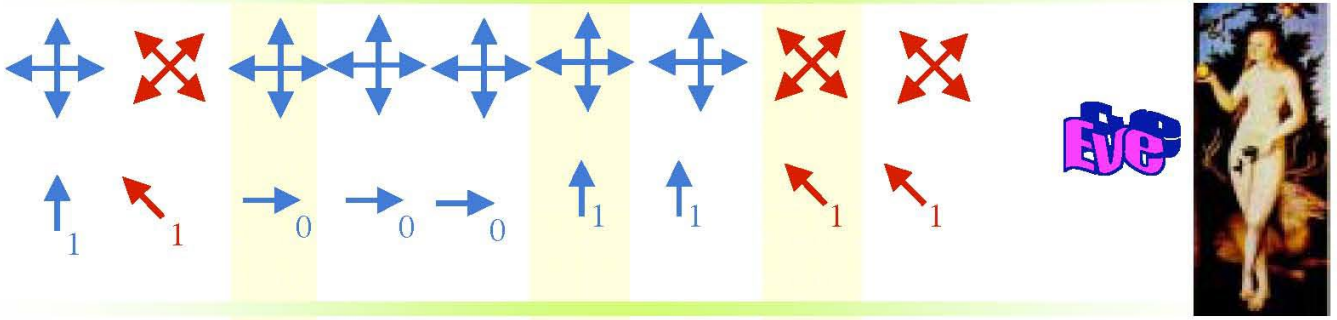


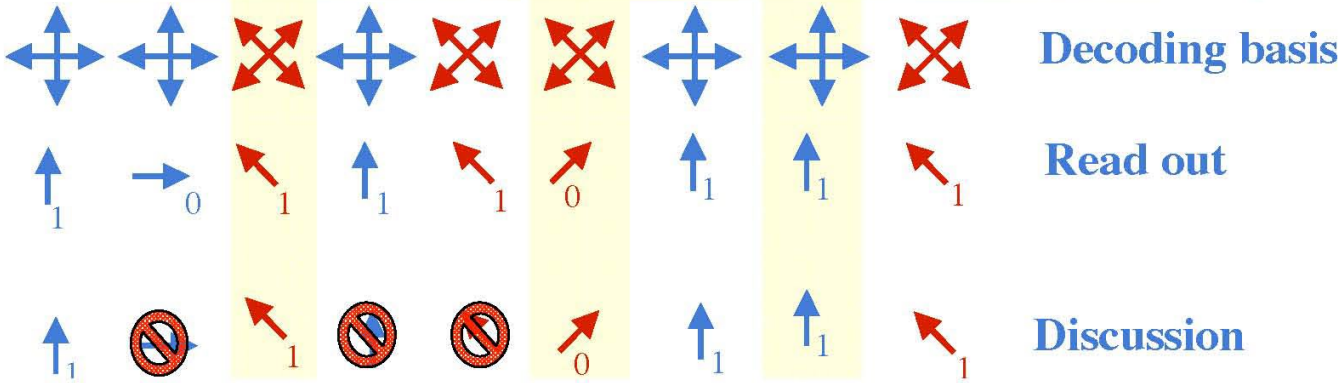
Eve



« BB84 » Protocol (Bennett & Brassard, 1984)







« BB84 » Protocol (Bennett & Brassard, 1984)

Alice

Bob

Coding basis

Bit value

Eve

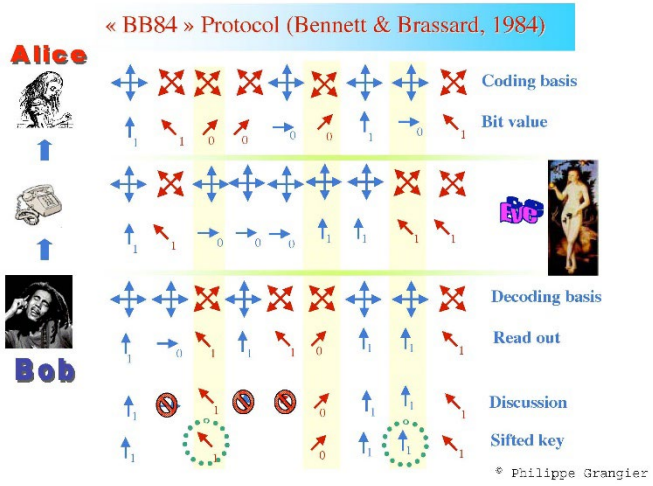
Decoding basis

Read out

Discussion

Sifted key

- QKD Assumes authenticated classical communication
  - Information-theoretic authentication can be achieved with a short initial shared secret (Wegman-Carter authentication)
  - Thus, QKD is more accurately described as a **key expansion** protocol.



- From a sifted key to a private key (in a nutshell)
  - **Publicly compare** half of the sifted bits to obtain an estimate of the **error rate**. Abort if the error rate is too high (specific rate depends on parameter choice; approx. 11% is the theoretical maximum)
  - **Information Reconciliation (aka Error Correction):** corrects the remaining strings so that they agree in all positions with high probability.
    - Can be done via a series of parity checks, or more generally, using error correcting codes.
  - **Privacy amplification:** Eve has some information about the key (from eavesdropping and Information Reconciliation).
    - Alice and Bob apply a **random hash function** $\{0,1\}^n \rightarrow \{0,1\}^l$ $(l < n)$

Security of BB84 Quantum Key distribution?

- Security of QKD is often informally attributed to the no-cloning theorem.
- Actual proofs (which appeared 15 years later or more) use much more sophisticated techniques
  - Quantum error correcting codes
  - De Finetti reductions
  - Entropic uncertainty relations
  - Sampling

QKD Firsts

- 1989: First Experimental demonstration
- 1998-2000: First proofs of security for QKD
- 2004: First bank transfer using QKD
- 2008: First network secured with QKD (200km, 6 nodes)
- 2016: First quantum satellite for space-to-ground quantum communication.

QKD Commercial Products

IDQ
FROM VISION TO TECHNOLOGY

TOSHIBA

国盾量子
QuantumCTek

Quintessence Labs
Data Uncompromised

MagiQ

KETS

Practicality of BB84 Quantum Key

- Alice only needs to prepare & send single qubits.
- Bob only needs to measure single qubits in a random basis
- Error correction is integrated into the protocol so that under a small amount of noise:
  - The protocol does not abort
  - The noise is corrected and the final keys agree.

Noise-tolerant, single-qubit prepare-and-measure

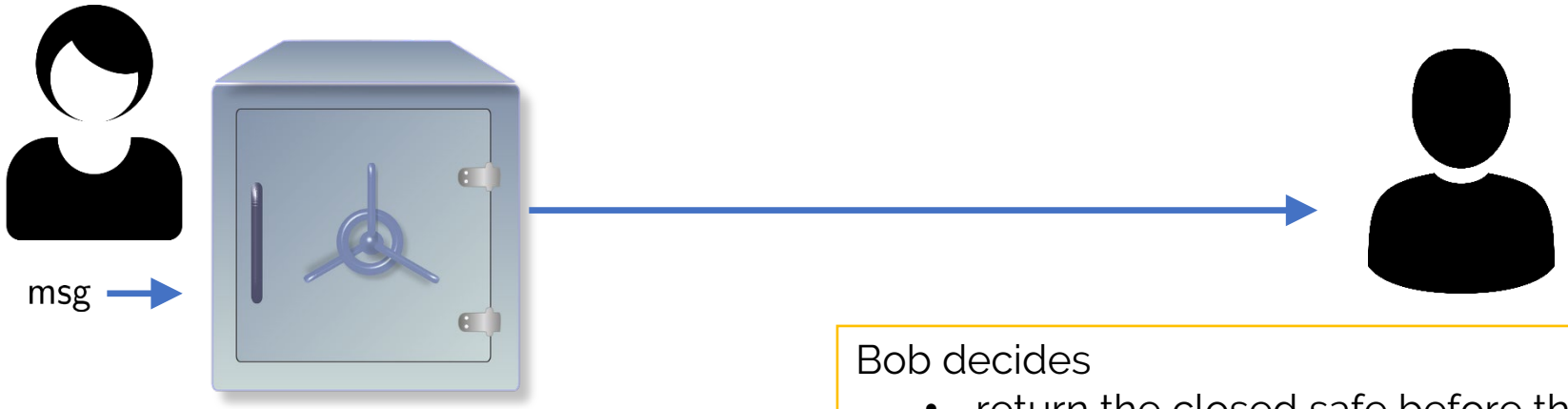
Recent Direction in QKD

- Device-independent and one-sided device-independent QKD
  - See Qcrypt 2019 Tutorial by Rotem Arnon Friedman (https://youtu.be/5KsW0d9JeqQ)
- Continuous-Variable QKD
- Finite-size effects in QKD
- Side-channel attacks
- ….

Certified Deletion

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…

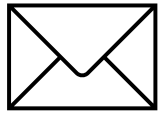
Bob can :

- 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



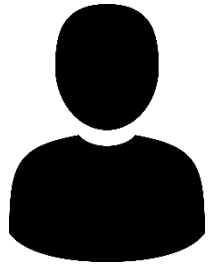
Alice's
Last Will and Testament

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 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 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

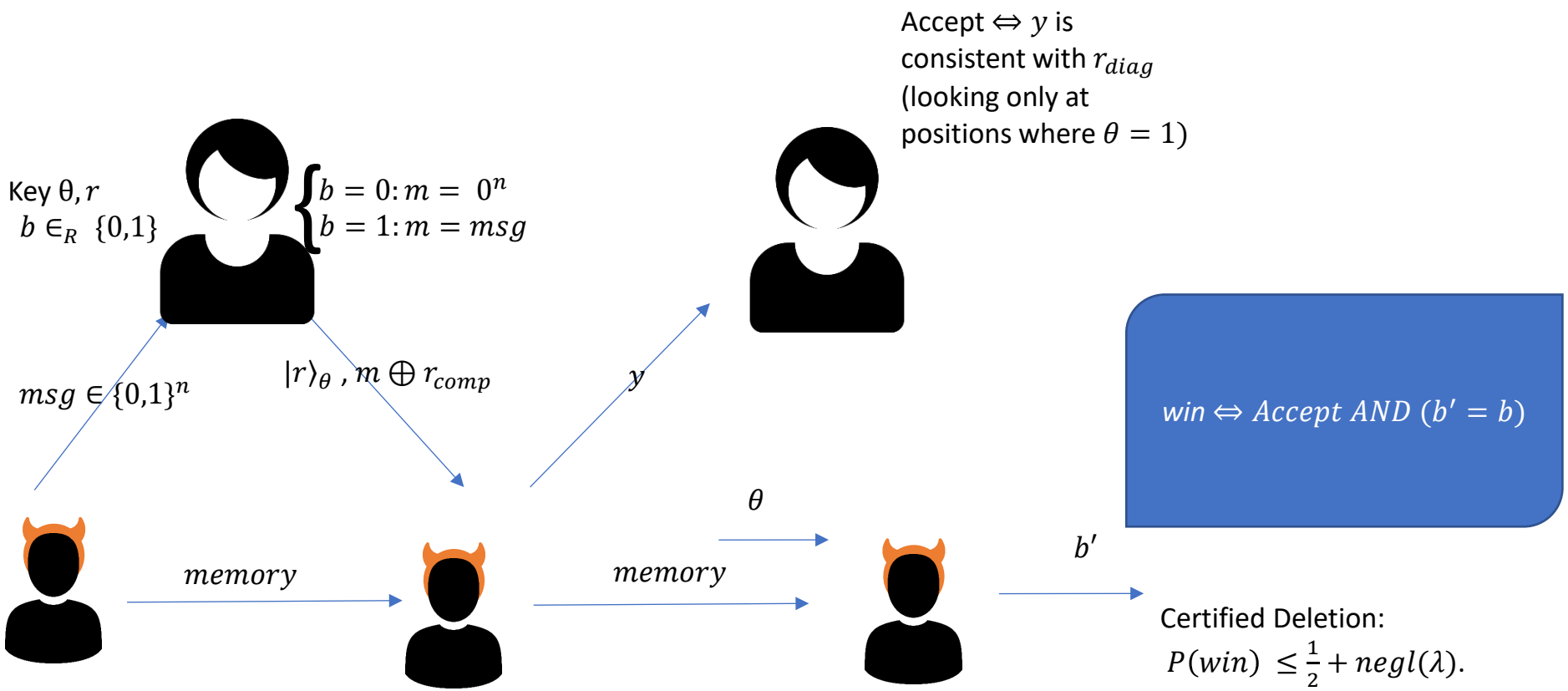
As the probability of predicting r_{diag} increases (i.e. adversary produces convincing "proof of deletion")

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

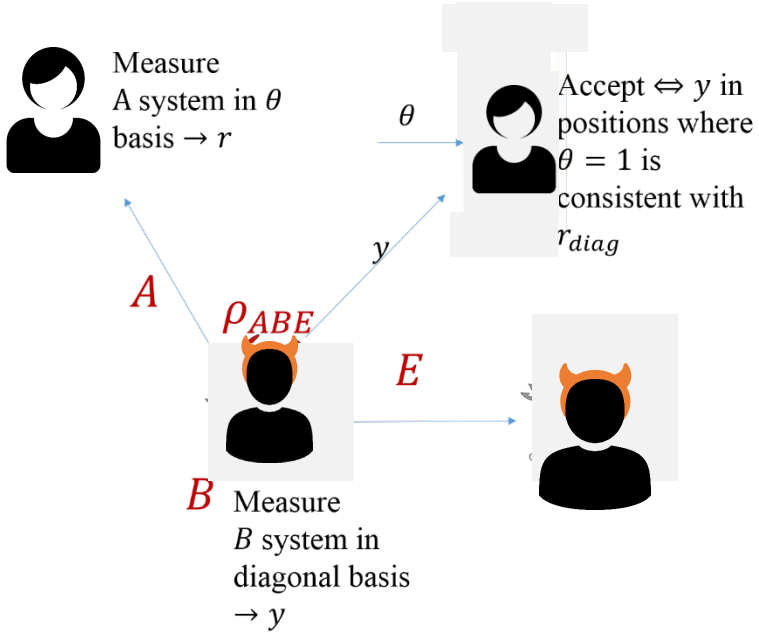
The probability of guessing r_{comp} decreases (i.e. adversary is unable to decrypt, even given the key)

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

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

$H_{min}^{\epsilon}(X \mid E)$: average prob. that Eve guesses X correctly
$H_{max}^{\epsilon}(Z \mid Z')$: # 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:

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

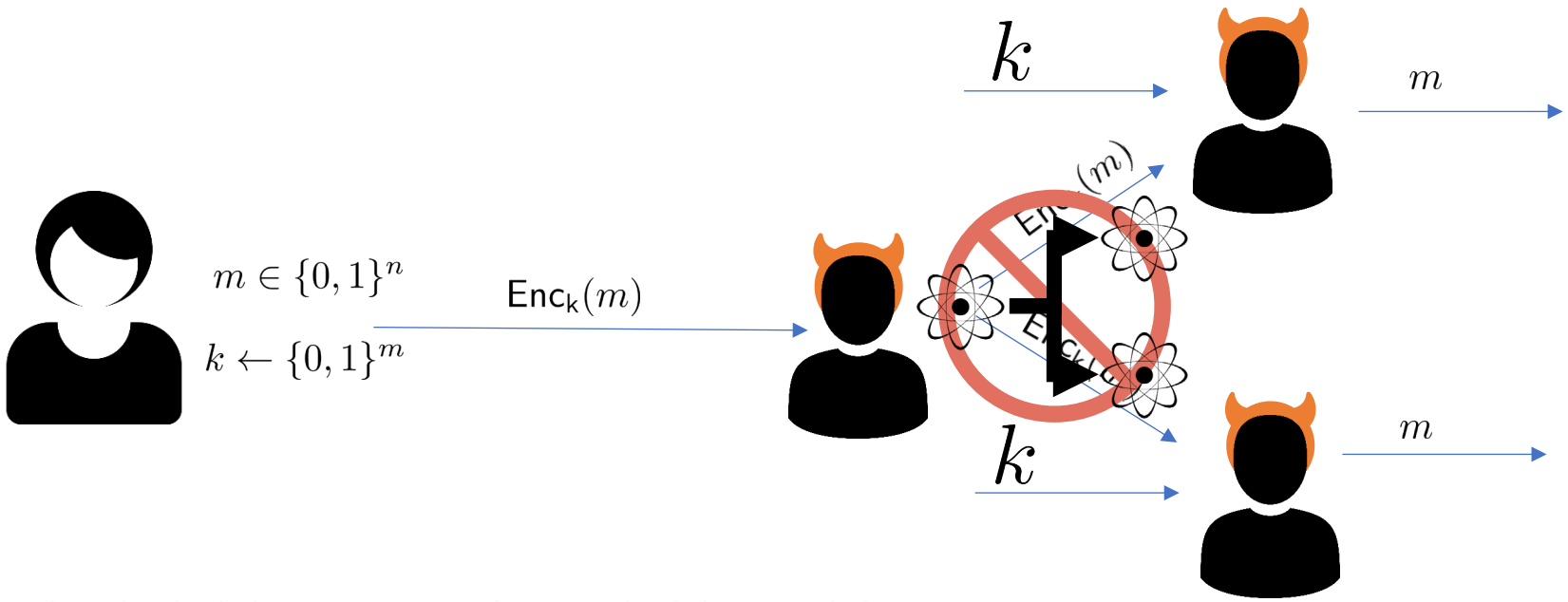
-noise tolerance: Accept y if less than $k\delta$ bits are wrong; use **error correction**.

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:

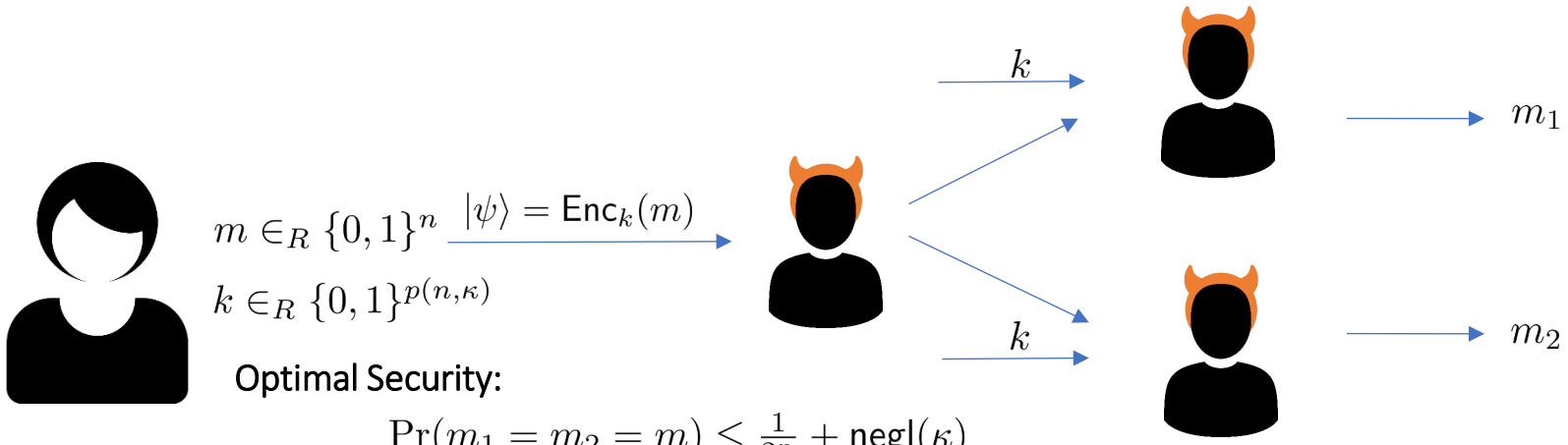


Classical ciphertexts can be copied, hence it is always possible for the adversary and the honest party to perfectly decrypt, given k.

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:

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

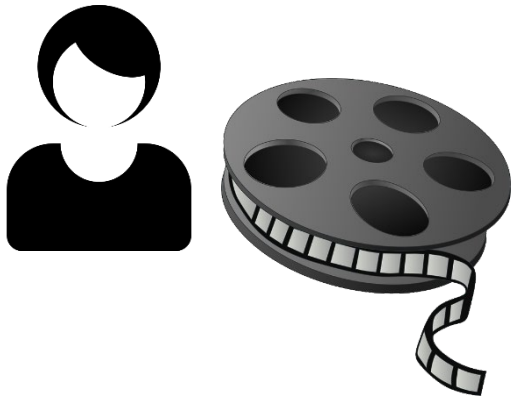
Conjugate-encoding based scheme (in the Quantum Random Oracle Model (QROM): [Broadbent, Lord 2020]

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

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

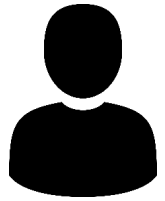


1. Alice uses uncloneable encryption and distributes an encrypted movie ahead of the movie release date.
2. The day of release, she reveals the key.
3. Thanks to uncloneable encryption, she is sure that at most one recipient* can decrypt the movie.

*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.

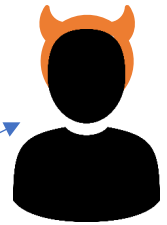
Output $y \oplus b = m$

Uncloneable Encryption Scheme + Security

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

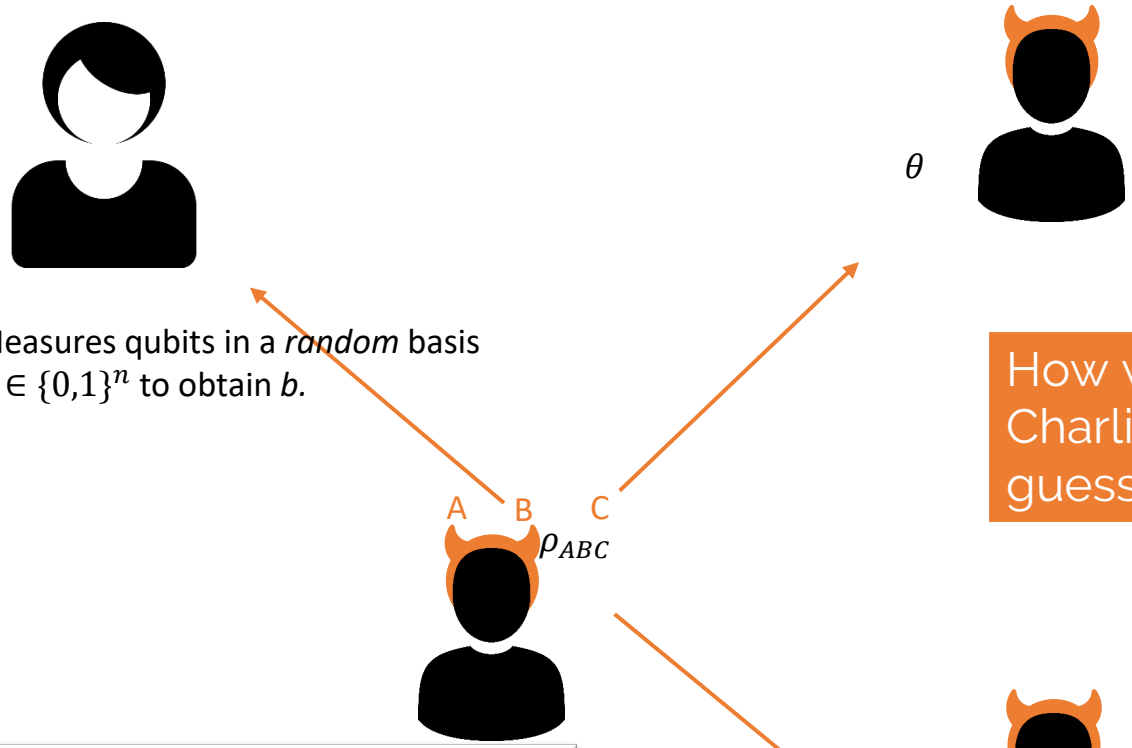
$|b\rangle_\theta$, $m \oplus b$

θ

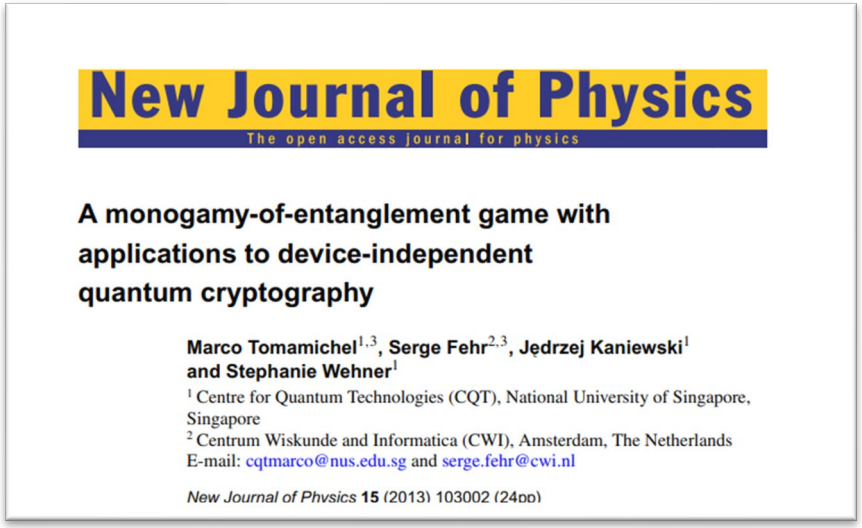


How well can Bob and Charlie **simultaneously** guess m?

θ



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

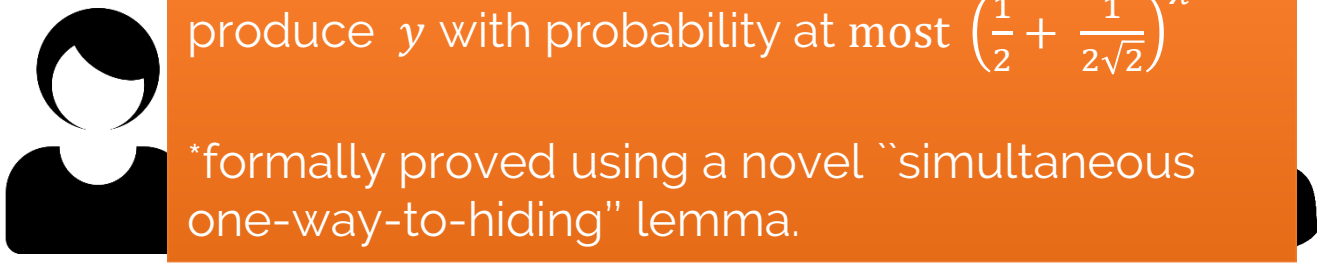
E-mail: cqtmarco@nus.edu.sg and serge.fehr@cwi.nl

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

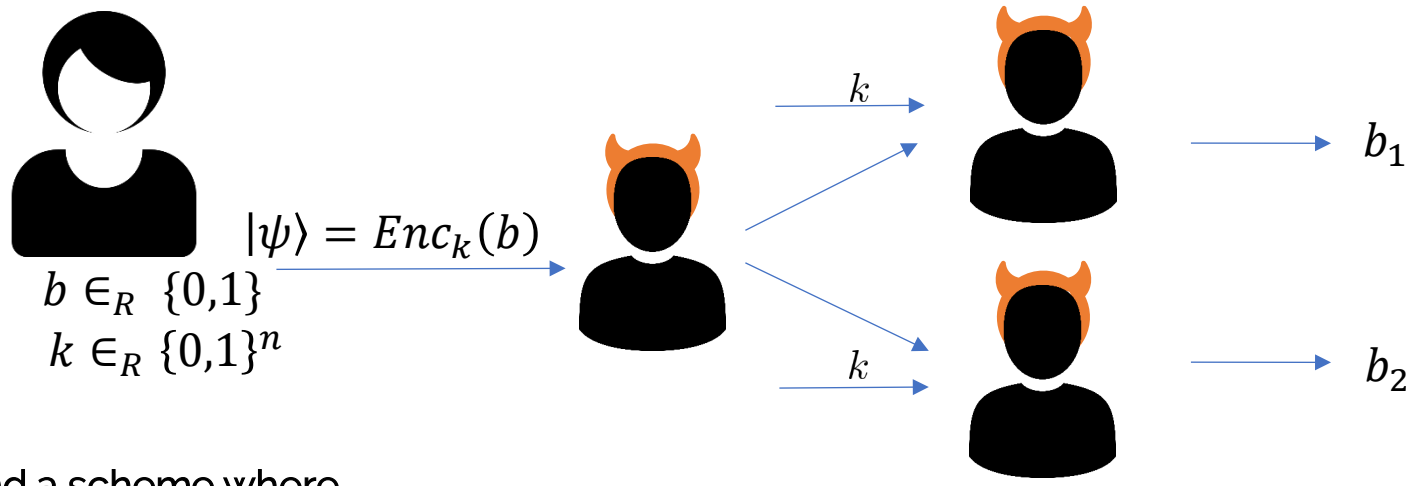
To decrypt:
Measure received qubits in basis θ;
Let the result be y.

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

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

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

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

Delegated Quantum Computation

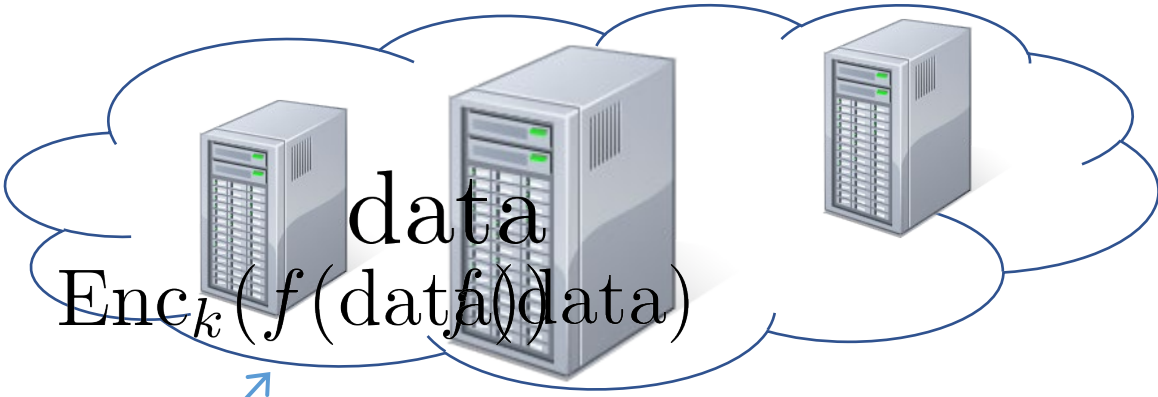
What are quantum computers good for?

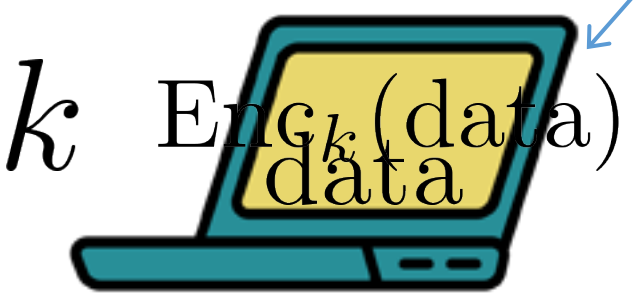
- Factoring and Discrete Log (Shor's algorithm)
- Simulating Quantum Systems
- Approximating the Jones polynomial
- Solving Pell's equation

- Unsorted search (Grover's algorithm) [quadratic speedup over brute-force search]
- …?

➢ Current world-wide effort to build a quantum computer!

Delegating Private Computations





- online data storage
- web-based email
- online income tax software

Homomorphic Encryption

Foundations of Secure Computation (1978)

ON DATA BANKS AND PRIVACY HOMOMORPHISMS

Ronald L. Rivest
Len Adleman
Michael L. Dertouzos

Massachusetts Institute of Technology
Cambridge, Massachusetts

I. INTRODUCTION

Encryption is a well-known technique for preserving the privacy of sensitive information. One of the basic, apparently inherent, limitations of this technique is that an information system working with encrypted data can at most store or retrieve the data for the user; any more complicated operations seem to require that the data be decrypted before being operated on. This limitation follows from the choice of encryption functions used, however, and although there are some truly inherent limitations on what can be accomplished, we shall see that it appears likely that there exist encryption functions which permit encrypted data to be operated on without preliminary decryption of the operands, for many sets of interesting operations. These special encryption functions we call "privacy homomorphisms"; they form an interesting subset of arbitrary encryption schemes (called "privacy transformations").

Plain RSA is multiplicatively homomorphic:

Given $x^e \pmod m$ and $y^e \pmod m$, server can compute $x^e y^e \pmod m = (x \cdot y)^e \pmod m$.

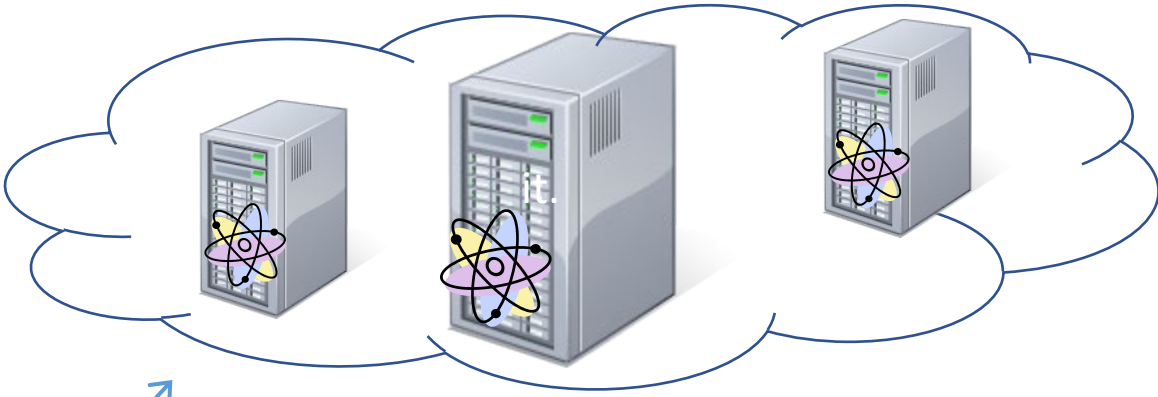
"Fully Homomorphic Encryption Using Ideal Lattices" by Craig Gentry (STOC 2009)

Delegating Private Quantum Computations

Applications

Shor's factoring algorithm:
•Server helps client crack an RSA public key without finding out the key.

Processing quantum data
•Processing quantum money.



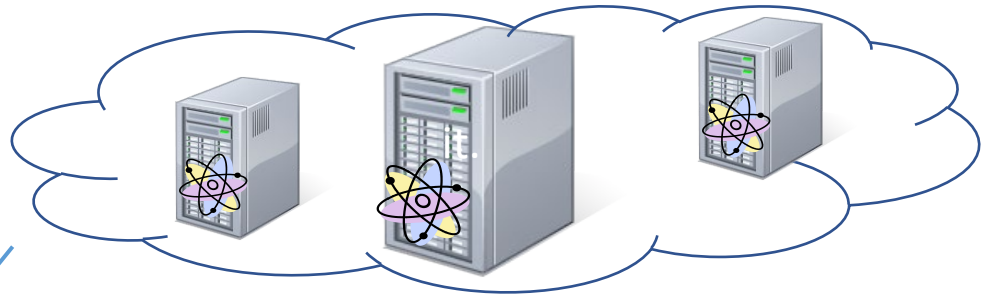
Very relevant given current challenges in building quantum computers!

Our Scenario
•Information-theoretic security
•Interactive
•Client is almost-classical

Client's power

Client *only* needs to:

- Encrypt quantum data
- Decrypt quantum data
- Classical processing
- Send random qubits



random qubits $\begin{cases} |0\rangle \\ |1\rangle \\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$

Same technology used for quantum key distribution

- Broadbent, A. (2015). Delegating private quantum computations. *Canadian Journal of Physics*, *93*(9), 941-946.

The One-time Pad Encryption Scheme

1. **The classical one-time pad**

Plaintext	$x \in \{0,1\}$
Key	$k \in_R \{0,1\}$
Ciphertext	$x \oplus k$

Since the ciphertext is uniformly random (as long as *k* is random and unknown), the plaintext is perfectly concealed.

2. **The quantum one-time pad** [Ambainis, Mosca, Tapp, de Wolf 2000]

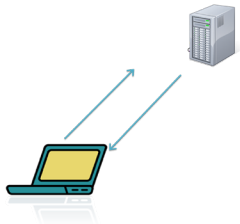
Plaintext	$\lvert\psi\rangle = \alpha \lvert 0\rangle + \beta \lvert 1\rangle$
Key	$(a,b) \in_R \{0,1\}^2$
Ciphertext	$\mathsf{Z}^a\mathsf{X}^b \lvert\psi\rangle$

$$\mathsf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \mathsf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

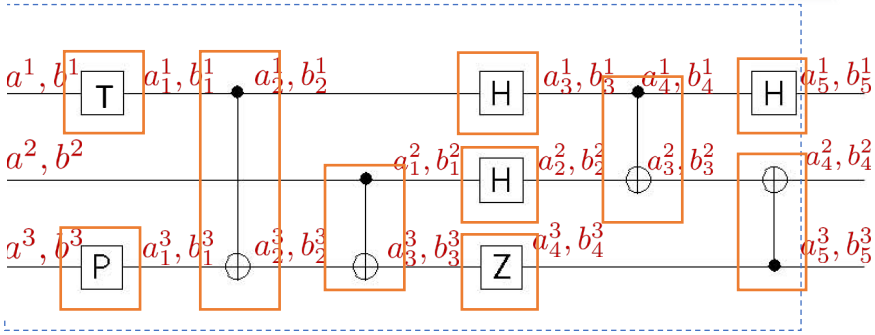
Pauli gates

Without knowledge of the key, the ciphertext always appears as the maximally mixed state, $\frac{\mathbb{I}}{2}$.

The protocol



ρ_{in}



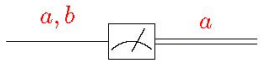
ρ_{out}

At each slice of time, applying the decryption key would produce the same (unencrypted) system that we would get in the execution of the original circuit.

To hide the computation, use a universal circuit.

Protocol for single-qubit preparation

Protocol for single-qubit measurement



Protocols for Clifford group gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

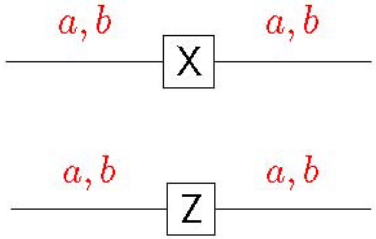
Pauli gates

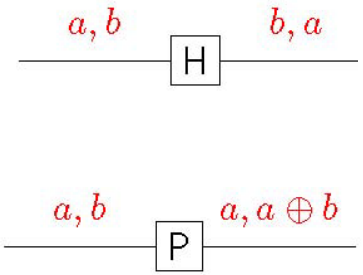
$$P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

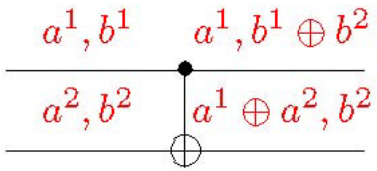
$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Clifford group gates

The Clifford Group is the set of operators that conjugate Pauli operators into Pauli operators.







Protocol for non-Clifford group gate

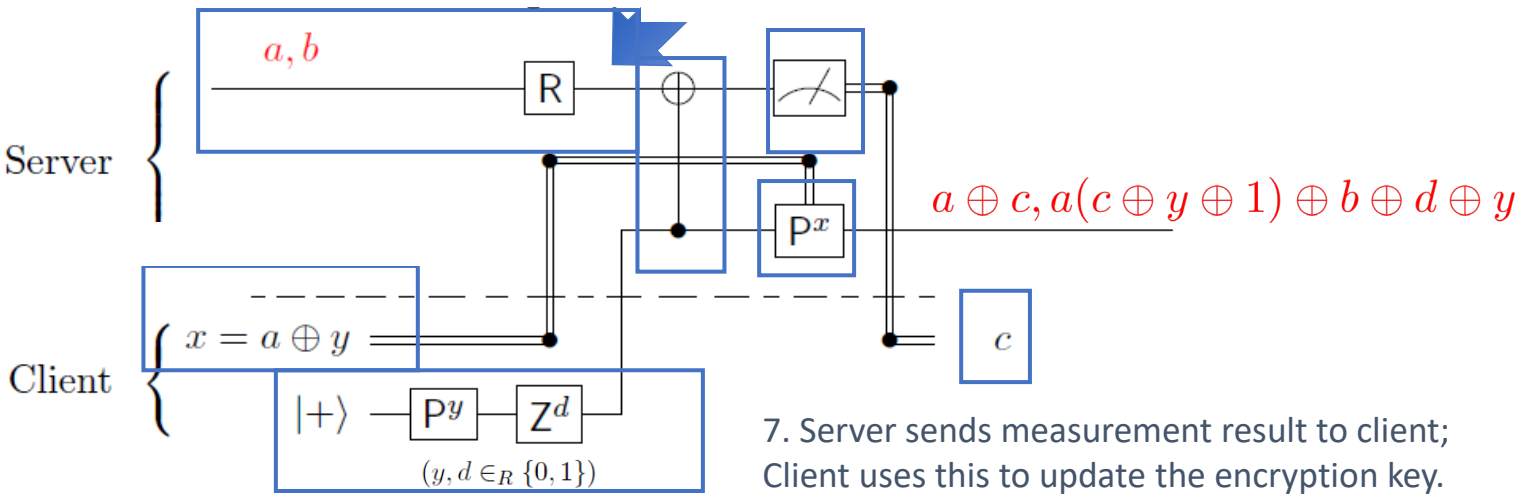
$$\mathsf{R} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Non-Clifford group gate

Applying the R gate on encrypted data causes a *Clifford* error in the key:

$$X^a Z^b \;\boxed{\mathsf{R}}\; X^a Z^{a\oplus b} \mathsf{P}^a$$

Main Idea: the client makes the server "correct" this error by making him apply a hidden P correction.

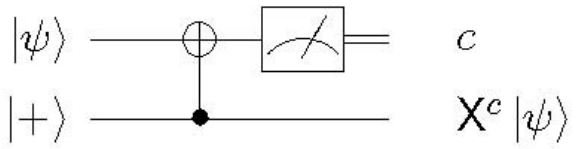


7. Server sends measurement result to client; Client uses this to update the encryption key.

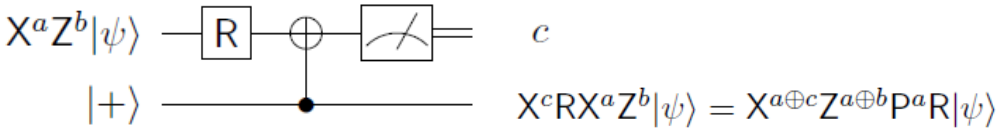
Correctness of the R-gate protocol

(Circuit derivation techniques inspired by [Childs, Leung, Nielsen, PRA 2005])

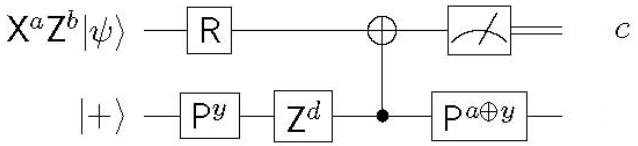
1. Start with X-teleportation circuit of Zhou, Leung and Chuang (PRA 2000):



2. modify the input:



3. add rotations on the bottom wire:



4. Since P *and* Z *commute with control, the output is:*

$P^{a\oplus y} = Z^{a\cdot y}P^{a+y}$ $\qquad$ $ZP = PZ;\ P^2 = Z$ $\qquad$ $PX = XZP$

$$P^{a\oplus y}Z^dP^yX^{a\oplus c}Z^{a\oplus b}P^aR|\psi\rangle = Z^{a\cdot y}P^{a+y}Z^dP^yX^{a\oplus c}Z^{a\oplus b}P^aR|\psi\rangle$$

$ZP = PZ;\ P^2 = Z$

$$= Z^{d\oplus a\cdot y\oplus y}P^aX^{a\oplus c}Z^{a\oplus b}P^aR|\psi\rangle$$

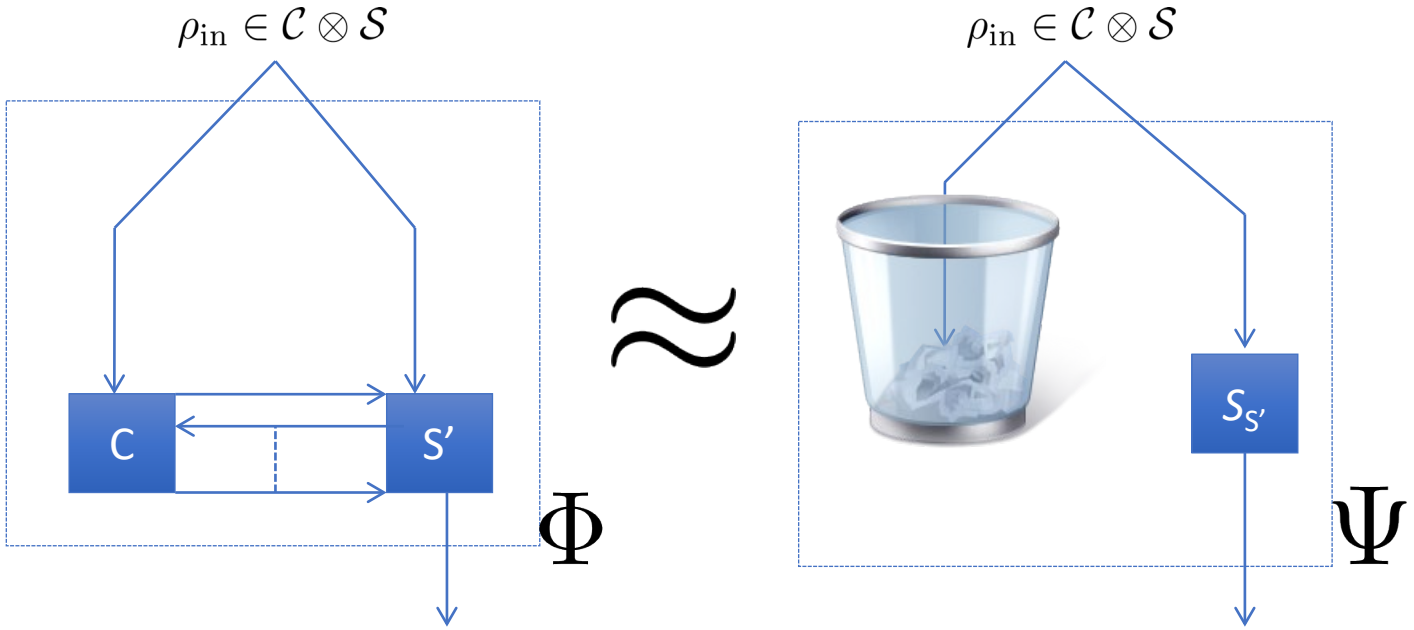
$$= Z^{d\oplus a\cdot y\oplus y}X^{a\oplus c}Z^{a(a\oplus c)}P^aZ^{a\oplus b}P^aR|\psi\rangle$$

$$= X^{a\oplus c}Z^{d\oplus a\cdot y\oplus y\oplus a^2\oplus a\cdot c}Z^bR|\psi\rangle$$

$$= X^{a\oplus c}Z^{a(c\oplus y\oplus 1)\oplus b\oplus d\oplus y}R|\psi\rangle$$

Security definition

How to formalize that “the server learns nothing from its interaction with the client”?



Let S’ be any deviating server.

A *simulator* $S_{S'}$ for S’ is any general quantum circuit that agrees with S’ on the input and output dimensions.

We say that a protocol for delegated quantum computation is *secure* if for every S’ there exists a simulator $S_{S'}$ such that the channels and Φ are Ψ indistinguishable.

Indistinguishability of channels

The *diamond norm* is a measure of indistinguishability of two quantum channels.

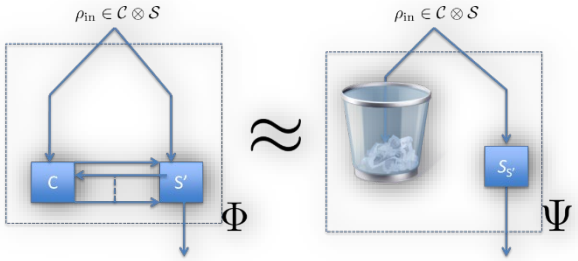
Operational Definition:

Suppose quantum channels Φ and Ψ agree their input and output spaces. Given that Φ or Ψ is applied with equal probability, the optimal procedure to determine the identity of the channel with only one use succeeds with probability

$$\frac{1}{2} + \frac{\|\Phi - \Psi\|_\diamond}{4}.$$

$$\|\Phi - \Psi\|_\diamond = \max\{\|(\Phi \otimes \mathbf{1}_\mathcal{W})(\rho) - (\Psi \otimes \mathbf{1}_\mathcal{W})(\rho)\|_1 : \rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{W})\}$$

Proof Outline



Main Idea: change the client's protocol such that:

1. The server cannot notice the change
2. The protocol is easily proven secure

Method: allow the client to share entanglement with the server

1. Instead of sending encrypted qubits, client sends half-EPR pairs
2. Instead of sending auxiliary qubits, client sends half-EPR pairs
3. The client delays inserting her actual input until the ***after*** the interaction with the server is complete: the protocol is trivially secure!

Inspiration: entanglement-based proof approach for QKD.

$$|EPR\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Summary:

We can use quantum information to build cool stuff

- unforgeable money
- perfectly secure communication
- … and more!

Thank you!

Some References

- Broadbent, A., Schaffner, C. Quantum cryptography beyond quantum key distribution. *Des. Codes Cryptogr.* **78,** 351–382 (2016). https://doi.org/10.1007/s10623-015-0157-4
- Wiesner, S. (1983). Conjugate coding. ACM Sigact News, 15(1), 78-88. https://dl.acm.org/doi/pdf/10.1145/1008908.1008920
- Watrous, J. Lecture 19: Impossibility of Quantum Bit Commitment. https://cs.uwaterloo.ca/~watrous/QC-notes/QC-notes.19.pdf
- Broadbent, A. (2015). Delegating private quantum computations. Canadian Journal of Physics, 93(9), 941-946. https://doi.org/10.1139/cjp-2015-0030
- Bouman, N. J., & Fehr, S. (2010, August). Sampling in a quantum population, and applications. In Annual Cryptology Conference (pp. 724-741). https://link.springer.com/chapter/10.1007/978-3-642-14623-7_39
- Bennett, C. H., & Brassard, G. (2020). Quantum cryptography: Public key distribution and coin tossing. https://arxiv.org/ftp/arxiv/papers/2003/2003.06557.pdf
- Broadbent, A., & Islam, R. (2020, November). Quantum encryption with certified deletion. In Theory of Cryptography Conference (pp. 92-122). https://link.springer.com/chapter/10.1007/978-3-030-64381-2_4
- Fehr, S. (2010). Quantum cryptography. *Foundations of Physics*, *40*(5), 494-531.
- James Bartusek, Dakshita Khurana. Cryptography with Certified Deletion, https://arxiv.org/abs/2207.01754
- And many more…