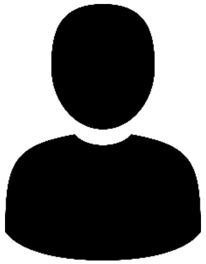
Impossibility of quantum bit commitment

Bit Commitment

A “physical” representation:

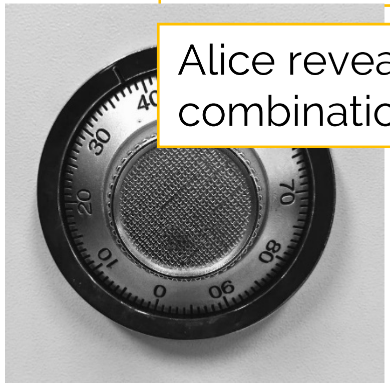
$b \in \{0,1\}$

Alice inserts a bit b into a safe, closes it and sends it to Bob. **(commit stage)**



Bob receives the safe. It is now guaranteed that:

- Alice cannot modify b **(binding)**
- Bob cannot read learn b **(concealing)**



Alice reveals the combination to the safe

Bob receives the combination and opens the safe **(reveal stage)**

Bit Commitment

Importance of bit commitment (BC)

Early work (Bennett, Brassard, Crépeau, Skubiszewska, 2001) showed that quantumly,

$$\boxed{BC} \longrightarrow \boxed{OT}$$

The importance of Oblivious Transfer (OT) is that it is universal for multi-party computation.

Can we achieve bit commitment in a digital world?

Quantum Bit Commitment

Historical Context

1984 Quantum Key Distribution (BB84)

1992 Superdense coding

1993 “Provably Unbreakable Bit Commitment”

1995 Quantum Teleportation

1997 Impossibility of Quantum Bit Commitment

Contradiction !

Proceedings of
FOCS 2013

A Quantum Bit Commitment Scheme
Provably Unbreakable by both Parties

Gilles Brassard [*]
Université de Montréal [†]

Claude Crépeau [‡]
École Normale Supérieure [§]

Richard Jozsa
Université de Montréal [†]

Denis Langlois [‡]
Université Paris–Sud [¶]

Abstract

Assume that a party, *Alice*, has a bit x in mind, to which she would like to be committed toward another party, *Bob*. That is, *Alice* wishes, through a procedure *commit*(x), to provide *Bob* with a piece of evidence that she has a bit x in mind and that she cannot change it. Meanwhile, *Bob* should not be able to tell from that evidence what x is. At a later time, *Alice* can reveal, through a procedure *unveil*(x), the value

1 Introduction

Assume that a party, *Alice*, has a bit x in mind, to which she would like to be committed toward another party, *Bob*. That is, *Alice* wishes, through a procedure *commit*(x), to provide *Bob* with a piece of evidence that she has a bit x in mind and that she cannot change it. Meanwhile, *Bob* should not be able to tell from that evidence what x is. At a later time, *Alice* can reveal, through a procedure *unveil*(x), the value

Mistake: assume that, if Alice can cheat the binding property, then she knows how to open both a commitment to 0 and a commitment to 1.

Theorem 3.7 *There exists a positive constant $\alpha < 1$ with the following property: the probability that Alice is able to announce either pair (c^0, b^0) or pair (c^1, b^1) at her choosing in protocol unveil leading Bob to accept a 0 and a 1, is less than α^n.*

Proof. Let (c^0, b^0) and (c^1, b^1) be any pairs of n-bit strings such that $c^0 \odot r = 0$ and $c^1 \odot r = 1$. Since $c^0 \odot r \neq c^1 \odot r$, it must be that $c^0 \neq c^1$. By construction of the code C, any two codewords must be at distance at least $10\epsilon n$ from each other. Let I be the set of indices on which c^0 and c^1 disagree: $I = \{i \mid c_i^0 \neq c_i^1\}$. We show that whatever *Alice* does, with high probability, $I_0 \leftarrow \{i \in I \mid c_i^0 \neq c_i' \wedge b_i^0 = b_i'\}$ or $I_1 \leftarrow \{i \in I \mid c_i^1 \neq c_i' \wedge b_i^1 = b_i'\}$ has size more than $0.7\epsilon n$. Since $I_0 \cap I_1 = \emptyset$, and thus $|I_0 \cup I_1| = |I_0| + |I_1|$, it suffices to show

VOLUME 78, NUMBER 17 PHYSICAL REVIEW LETTERS 28 APRIL 1997

Unconditionally Secure Quantum Bit Commitment is Impossible

Dominic Mayers

Département IRO, Université de Montréal, C.P. 6128, Succursale Centre-Ville, Montréal, Québec, Canada H3C 3J7

(Received 21 March 1996; revised manuscript received 25 July 1996)

The claim of quantum cryptography has always been that it can provide protocols that are unconditionally secure, that is, for which the security does not depend on any restriction on the time, space, or technology available to the cheaters. We show that this claim does not hold for any quantum bit commitment protocol. Since many cryptographic tasks use bit commitment as a basic primitive, this result implies a severe setback for quantum cryptography. The model used encompasses all reasonable implementations of quantum bit commitment protocols in which the participants have not met before, including those that make use of the theory of special relativity. [S0031-9007(97)02996-7]

VOLUME 78, NUMBER 17 PHYSICAL REVIEW LETTERS 28 APRIL 1997

Is Quantum Bit Commitment Really Possible?

Hoi-Kwong Lo* and H. F. Chau†

School of Natural Sciences, Institute for Advanced Study, Olden Lane, Princeton, New Jersey 08540

(Received 8 March 1996)

We show that all proposed quantum bit commitment schemes are insecure because the sender, Alice, can almost always cheat successfully by using an Einstein-Podolsky-Rosen–type of attack and delaying her measurement until she opens her commitment. [S0031-9007(97)02967-0]

Schmidt decomposition:

Let $|\psi\rangle \in A \otimes B$ (a pure state). Then there exist orthonormal bases $\{|a_i\rangle\}$ for A and $\{|b_i\rangle\}$ for B, and non-negative real numbers $\{p_i\}$ such that:

$$|\psi\rangle = \sum_i \sqrt{p_i}\, |a_i\rangle \otimes |b_i\rangle$$

Corollary:

Let $|\phi\rangle, |\psi\rangle \in A \otimes B$. Suppose that

$$\mathrm{Tr}_B(|\phi\rangle\langle\phi|) = \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$$

Then there exists unitary U such that

$$(I_A \otimes U)|\phi\rangle = |\psi\rangle$$

Impossibility of **Quantum** Bit Commitment

Theorem:
There is no perfectly concealing and perfectly binding Quantum Bit Commitment protocol

Recall:
- Alice cannot modify b **(binding)**
- Bob cannot read learn b **(concealing)**

Proof: Suppose such a scheme exists. Suppose WLOG that all operations are unitary in the protocol (follows from purification)
Consider the joint state after the commit phase:

$|\psi_0\rangle \in A \otimes B$, if $b = 0$
$|\psi_1\rangle \in A \otimes B$, if $b = 1$

By the hiding property, $\mathrm{Tr}_A(|\psi_0\rangle\langle\psi_0|) = \mathrm{Tr}_A(|\psi_1\rangle\langle\psi_1|)$
By the Corollary, there exists unitary U such that $(U \otimes I)|\psi_0\rangle = |\psi_1\rangle$
Therefore, the binding property is completely broken – Alice can change her mind about the committed bit, even after the commit phase.

*A generalization to the approximate case also holds.

Possibilities for Bit Commitment

1. Using a computational assumption, classical bit commitment is possible
   - Statistical binding, computational hiding
   - Computational binding, statistical hiding
2. Using a physical assumption, information-theoretic **quantum** bit commitment is possible
   - Bounded quantum-storage
   - Noisy quantum-storage
   - Isolated qubits (no multi-qubit operations)

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

Delegating Private Quantum Computations

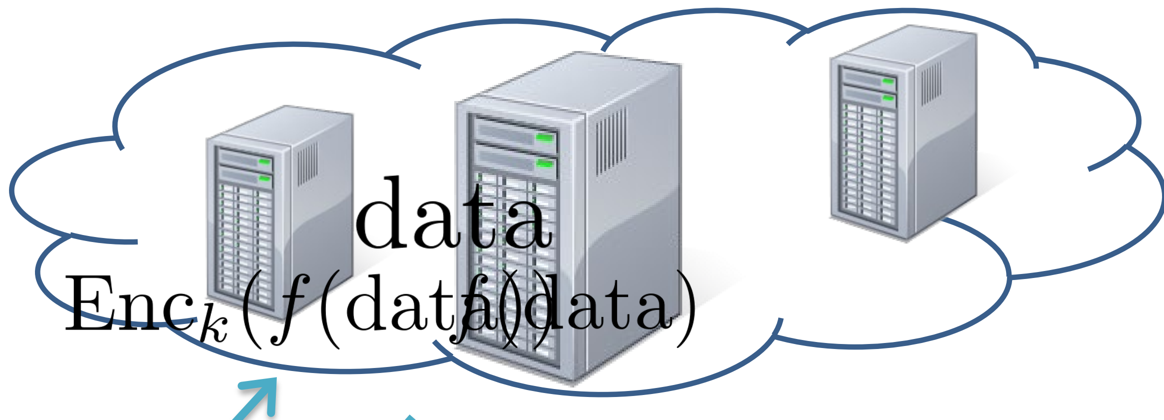
Anne Broadbent

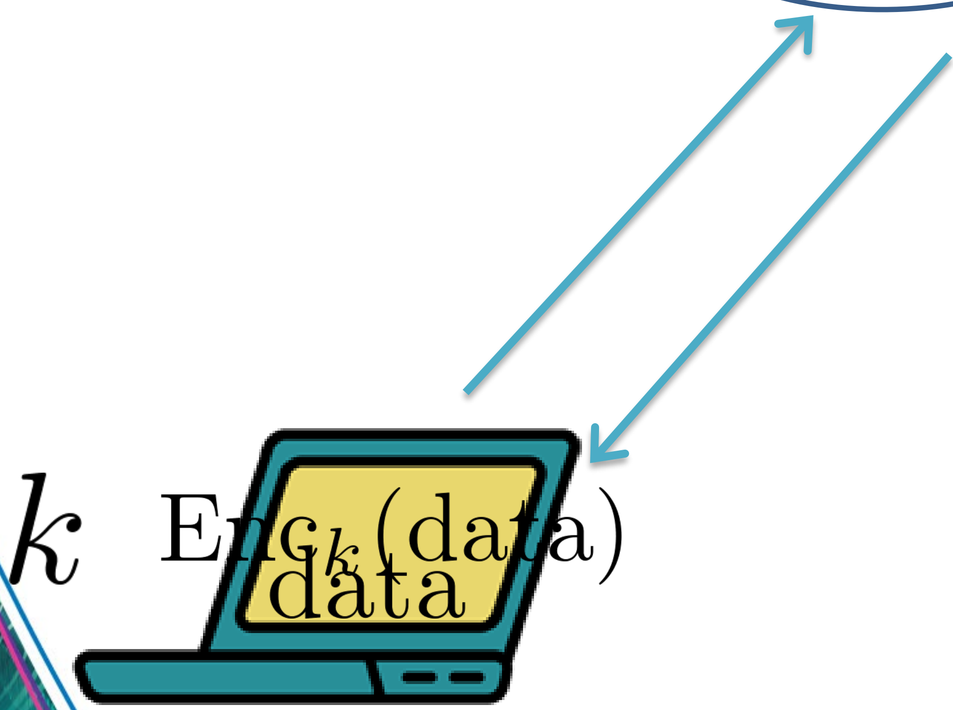
IPAM

July 2022

Delegating Computations

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

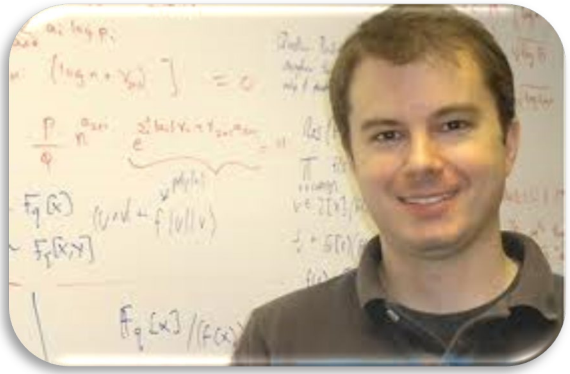
Massachusetts Institute of Technology
Cambridge, Massachusetts

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



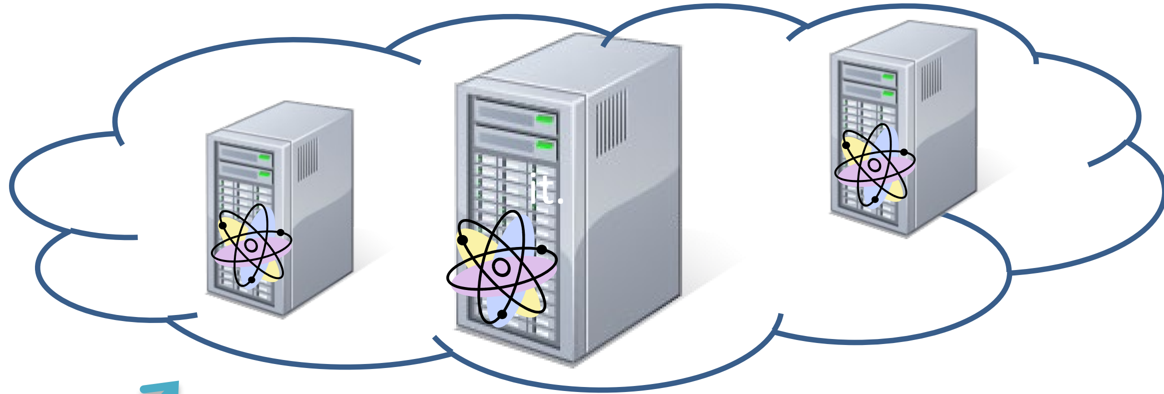
"Fully Homomorphic Encryption Using Ideal Lattices"
by Craig Gentry (STOC 2009)

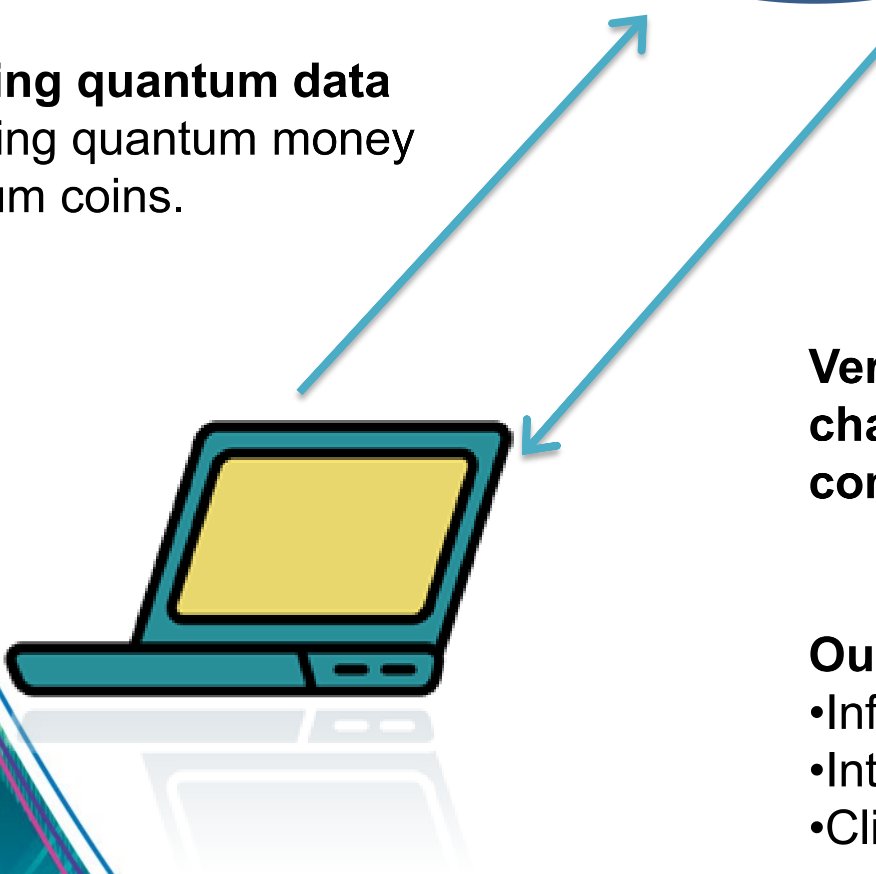
Delegating Private Quantum Computations

Applications

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

Processing quantum data
•Processing quantum money or quantum coins.





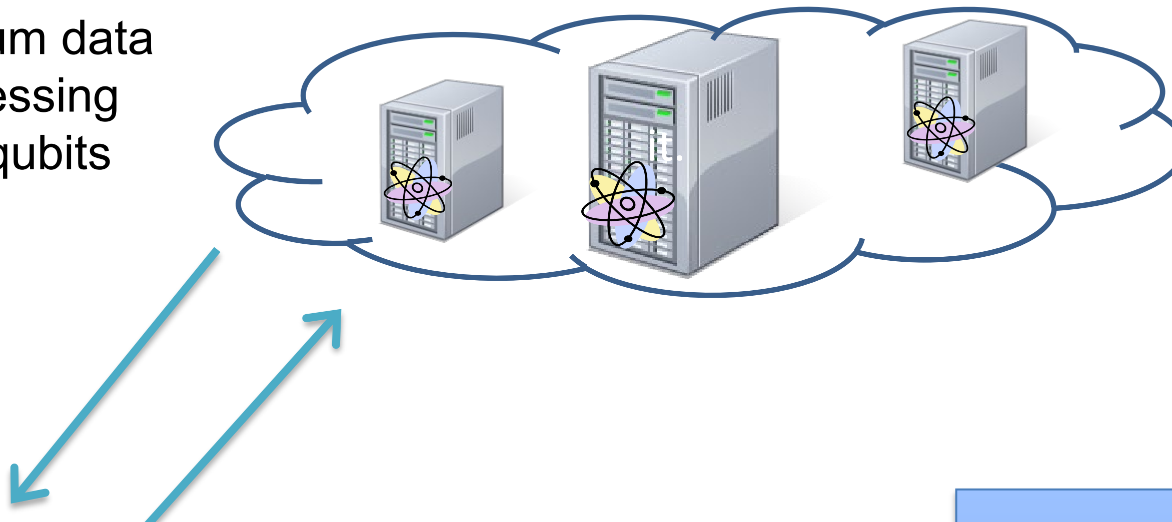
Very relevant given current challenges in building quantum computers!

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



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

Same technology used for quantum key distribution

- Broadbent, A. (2015). Delegating private quantum computations. *Canadian Journal of Physics*, *93*(9), 941-946.
- Fisher, K. A., Broadbent, A., Shalm, L. K., Yan, Z., Lavoie, J., Prevedel, R., Jennewein, T.& Resch, K. J. (2014). Quantum computing on encrypted data. *Nature communications*, *5*(1), 1-7.

Universal set of quantum gates

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

Pauli gates

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

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

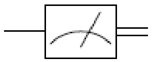
Clifford group gates

+

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

Non-Clifford group gate

+

- Single-qubit preparation $|0\rangle$
- Single-qubit measurement 

=

Universal Quantum Computation

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]

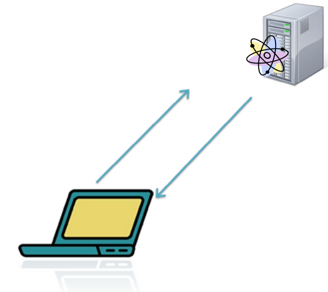
Plaintext	$\lvert\psi\rangle = \alpha\lvert 0\rangle + \beta\lvert 1\rangle$
Key	$(a,b) \in_R \{0,1\}^2$
Ciphertext	$\mathsf{Z}^a\mathsf{X}^b\lvert\psi\rangle$

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

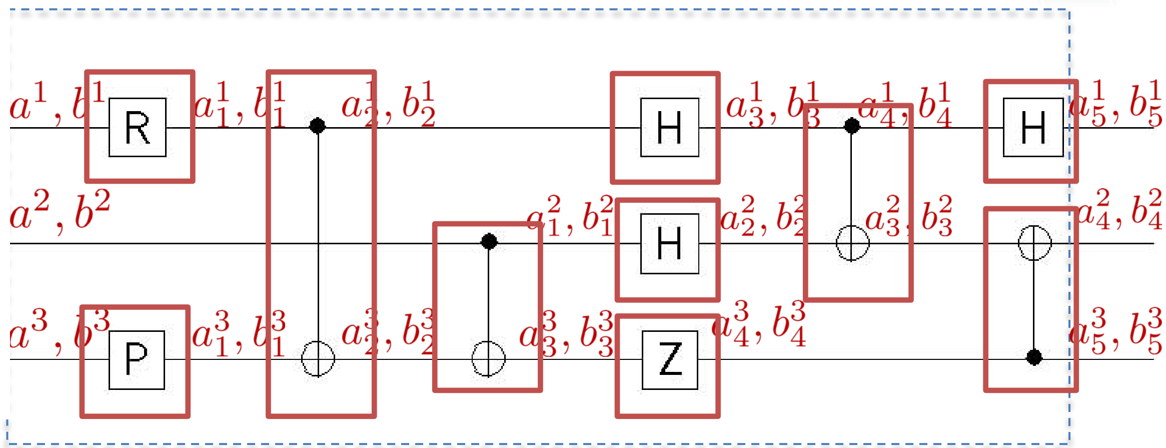
Pauli gates

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

The protocol



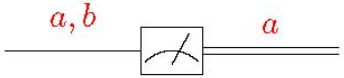
ρ_{in}



ρ_{out}

Protocol for single-qubit preparation

Protocol for single-qubit measurement



Protocols for Clifford group gates

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

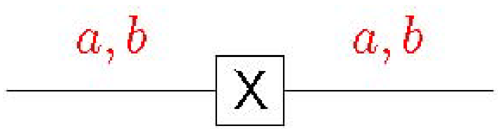
Pauli gates

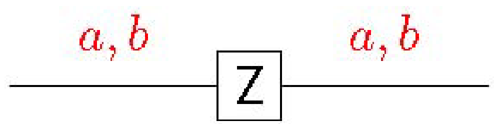
$$P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

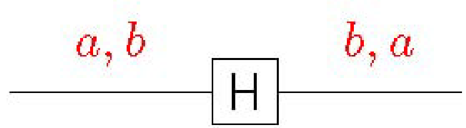
$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

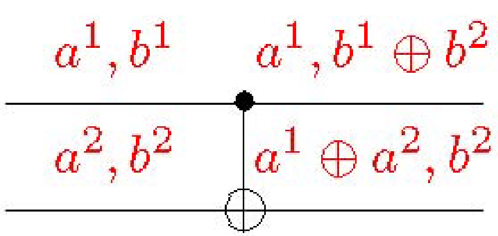
Clifford group gates

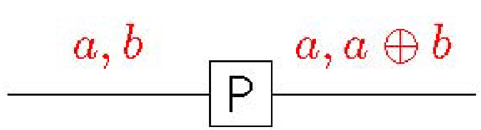
The Clifford Group is the set of operators that conjugate Pauli operators into Pauli operators.









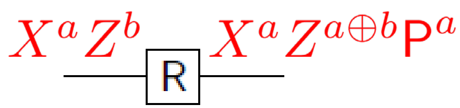


Protocol for non-Clifford group gate

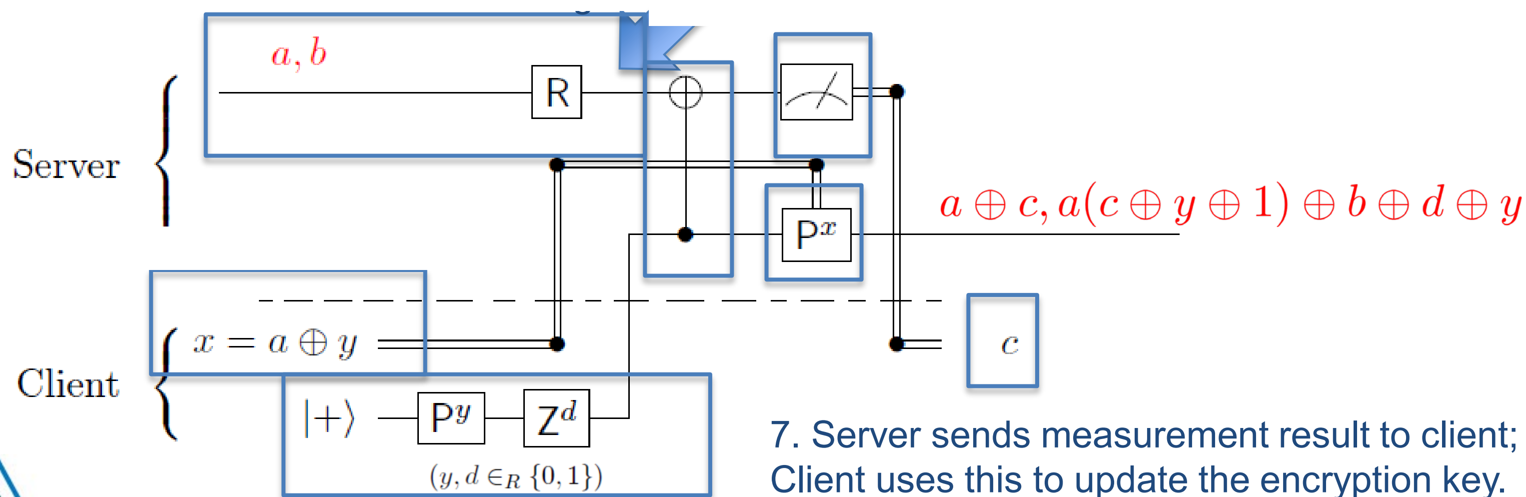
$$\mathsf{R} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Non-Clifford group gate

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



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

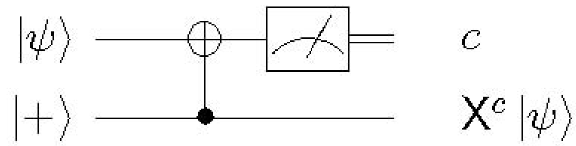


7. Server sends measurement result to client; Client uses this to update the encryption key.

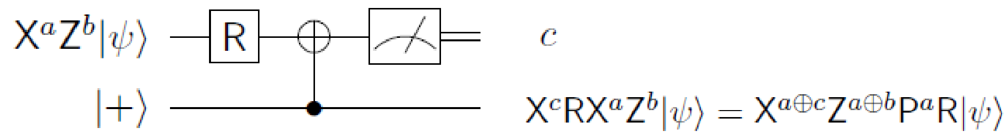
Correctness of the R-gate protocol

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

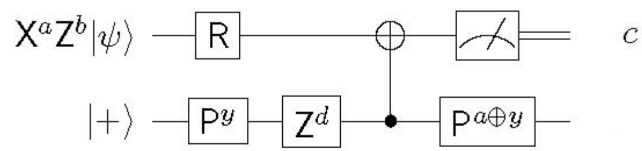
1. Start with X-teleportation circuit of Zhou, Leung and Chuang (PRA 2000):



2. modify the input:



3. add rotations on the bottom wire:



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

$P^{a\oplus y} = Z^{a\cdot y}P^{a+y}$

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

$PX = XZP$

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

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

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

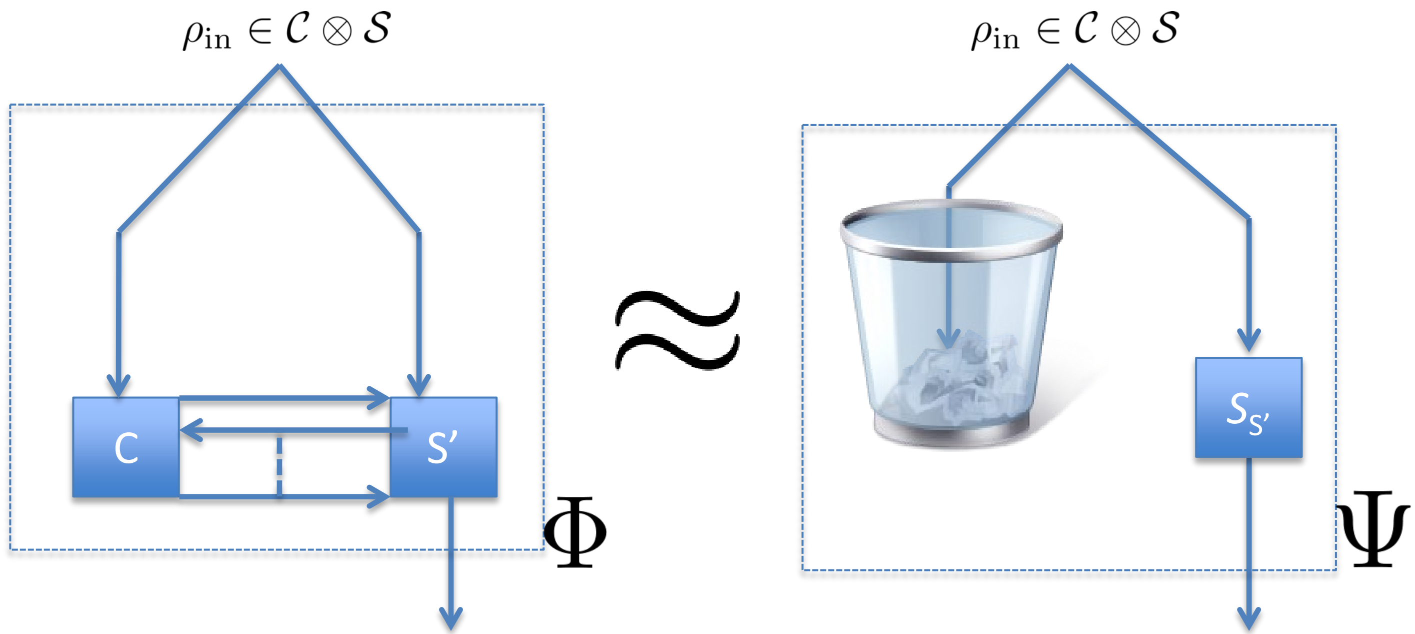
$$= Z^{d\oplus a\cdot y\oplus y}X^{a\oplus c}Z^{a(a\oplus c)}P^aZ^{a\oplus b}P^aR|\psi\rangle$$

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

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

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 Φ and Ψ are indistinguishable.

Indistinguishability of channels

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

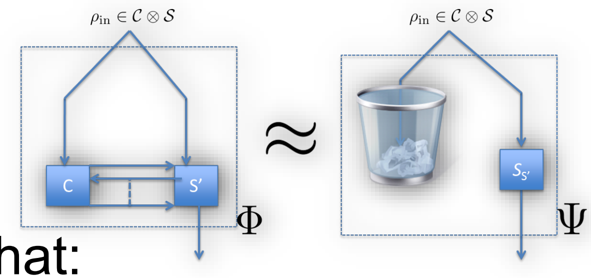
Operational Definition:

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

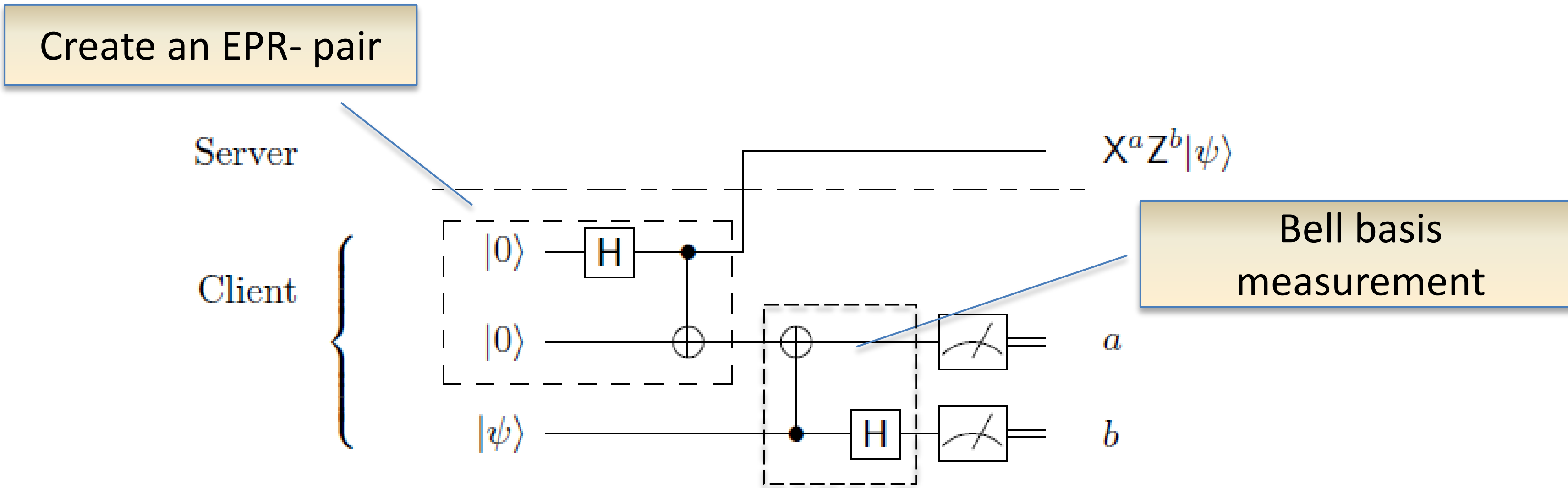
Method: allow the client to share entanglement with the server

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: Shor-Preskill proof of security for quantum key distribution (PRL 2000).

Proof /1

Instead of sending an encrypted qubit, the client sends a half-EPR pair and “teleports in” her input by performing a Bell basis measurement.

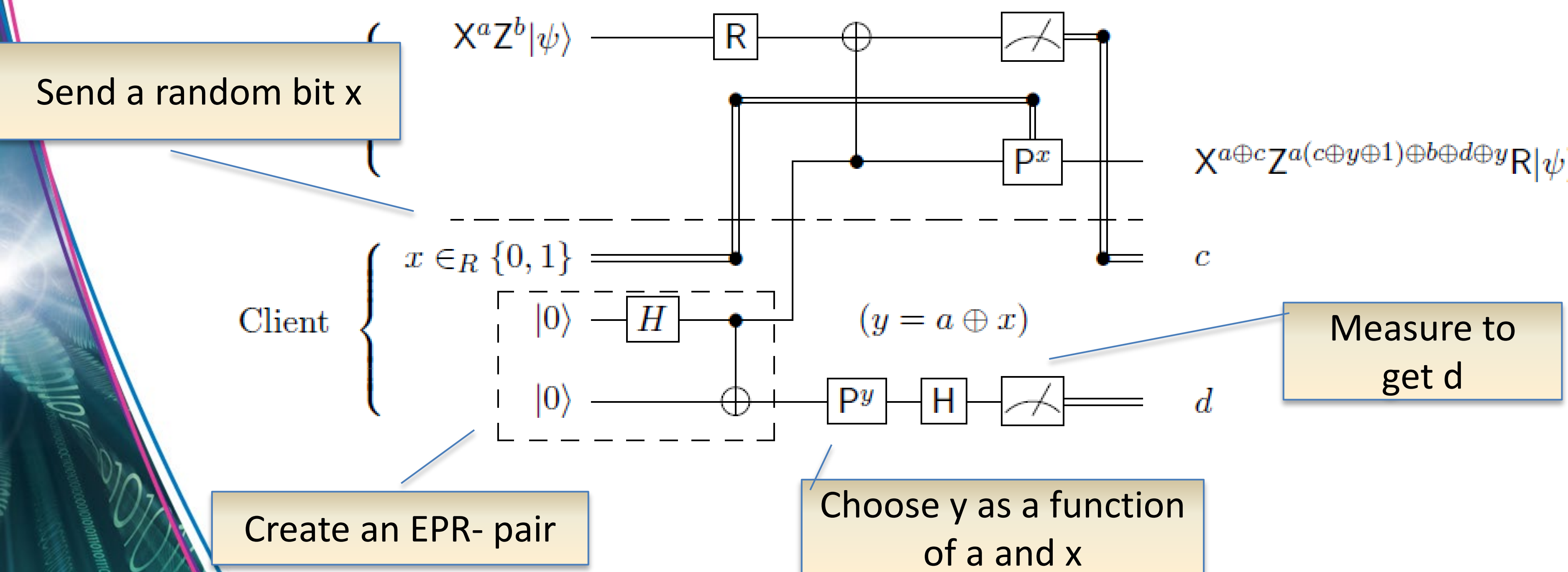


Do this for each input qubit.
The server’s view and the effect of the protocol is unchanged.

Proof /2

For the R- gate protocol:

1. Instead of sending an auxiliary qubit, the client sends a half-EPR pair
2. Instead of sending bit x, a random bit is sent
3. The "hidden P gate" is now chosen as a function of a and x.
4. The value d is now determined by a measurement

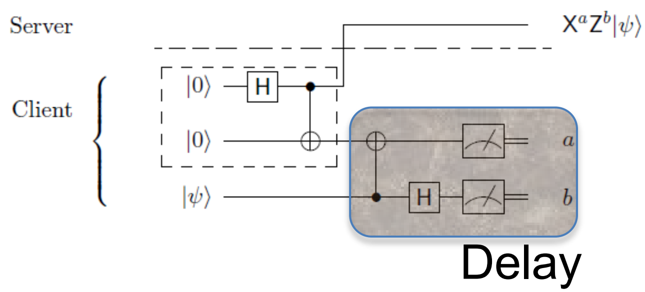


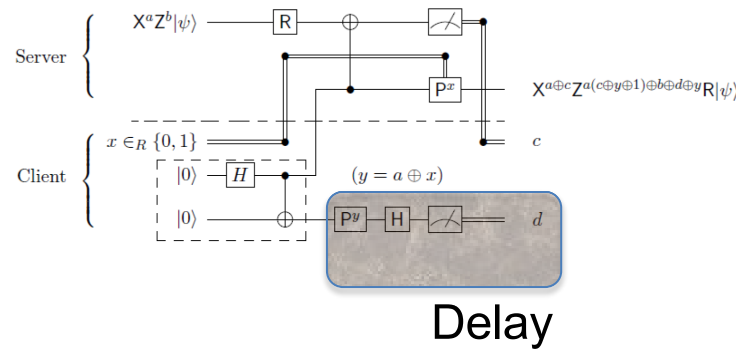
Do this for each R- gate protocol.

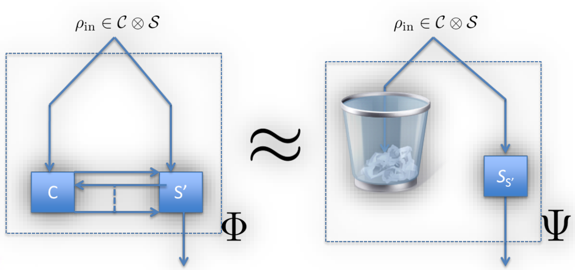
The server's view and the effect of the protocol is unchanged.

Proof /3

In both sub-protocols (encryption and R-gate), delay all of the client's measurements until the output register is returned by the server.





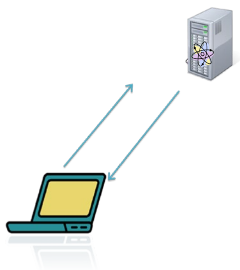


- We construct the simulator $S_{S'}$ that generates the transmissions that the client would send in this protocol and feeds them to S' (which it then internallly simulates), *but that never performs any measurements.*

- Access to the actual input is not required. By the previous slides, S' view is unchanged. It follows that the two channels are identical.

$$\|\Phi - \Psi\|_{\diamond} = 0$$

Conclusion



Main result: method to compute on encrypted data

- Client uses quantum encryption and sends Wiesner states; otherwise is classical.
- Information-theoretically secure against any cheating server, even with quantum side information.

Related work

Universal Blind Quantum Computation. A. Broadbent, J. Fitzsimons and E. Kashefi. “(FOCS, 2009)

- Auxiliary qubits in $\{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle \mid \theta = 0, \frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}, \pi, \frac{3\pi}{2}, \frac{7\pi}{4}\}$
- Correctness in terms of *measurement-based quantum computing*
- *Each gate: 8 auxiliary qubits, 24 bits of communication in each direction.*

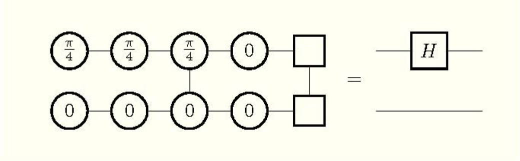


Figure 3: Implementation of a Hadamard gate.

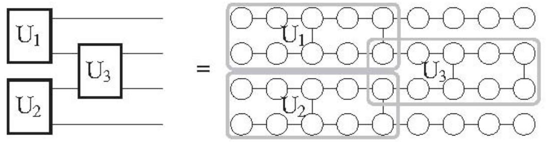
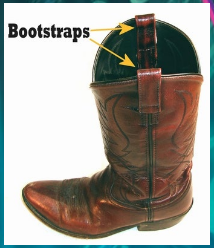


Figure 7: Tiling for a 4-qubit circuit with three gates.

Verifying a Quantum Computation

[Aharonov, Ben-Or & Eban 2010]
[Aharonov & Vazirani 2012]

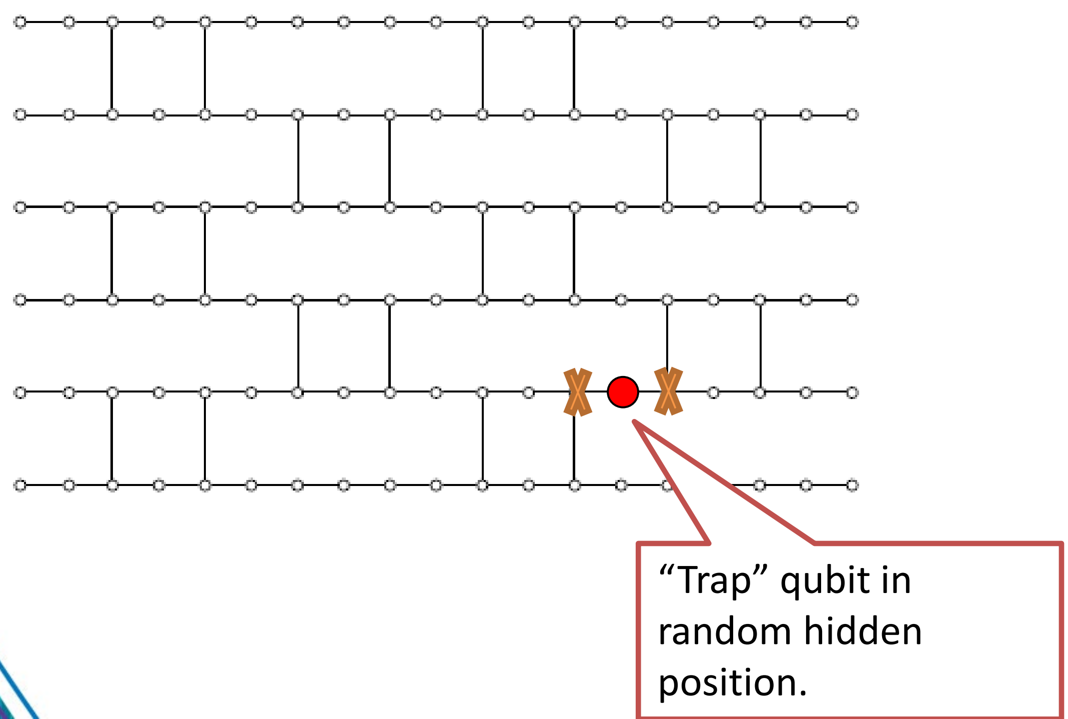
- How do you know that the outcome of a delegated quantum computation is correct?
  - In general, we cannot predict the output of a quantum computation.
  - Is the scientific method of predict-and-verify doomed?
- There is hope…
  - Consider factoring. The experimentalist can efficiently verify the solution.
- More generally, we want the experimentalist to be convinced of the correctness of the solution even though she cannot compute the solution herself.
  - We know of bootstrapping methods
    - If experimentalist is convinced she can characterize and control a small quantum system (e.g. single qubits) then we can expand this to an entire quantum system.



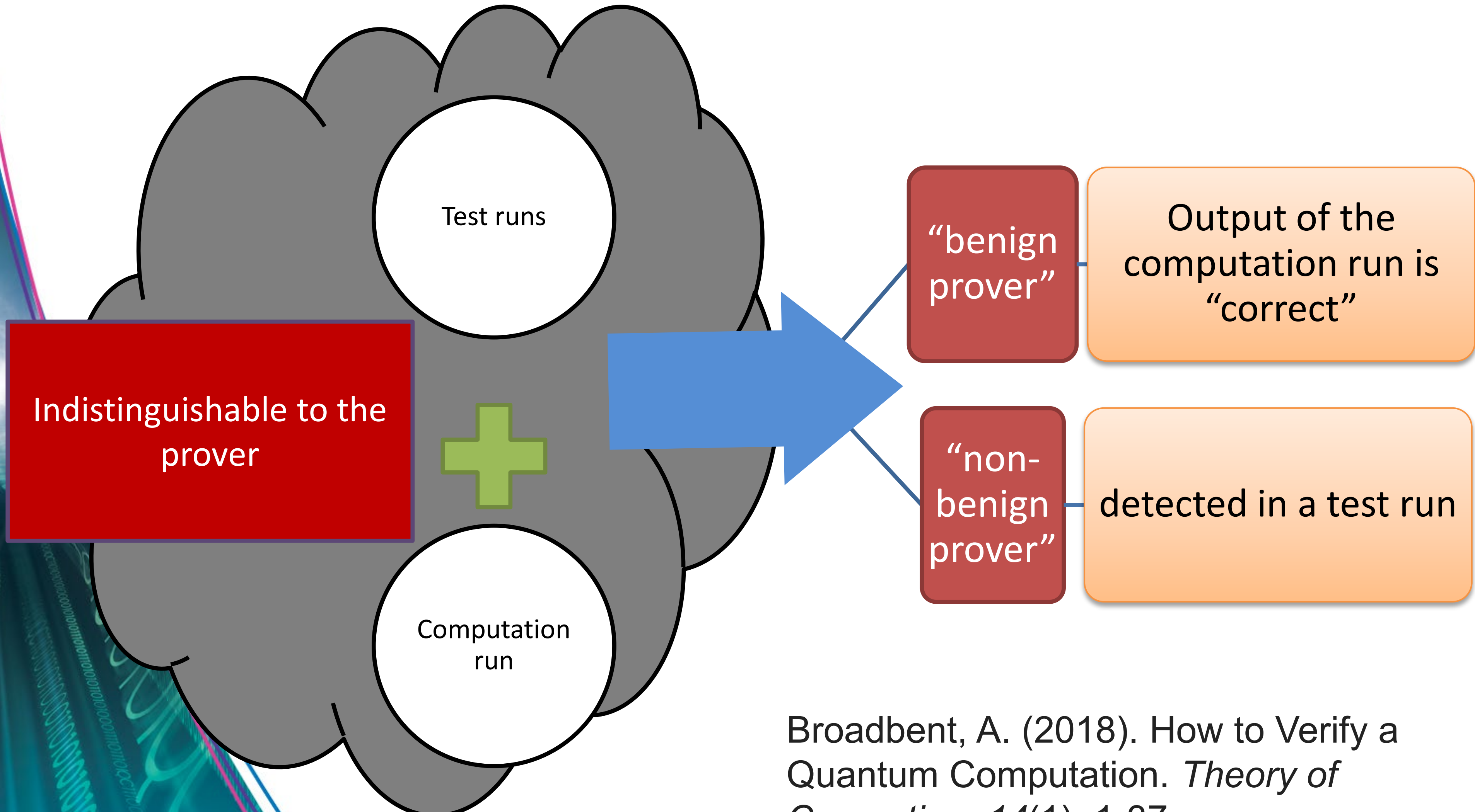
Verifiability

Unconditionally Verifiable Blind Quantum Computation

Joseph F. Fitzsimons[1,2] and Elham Kashefi[3,4]



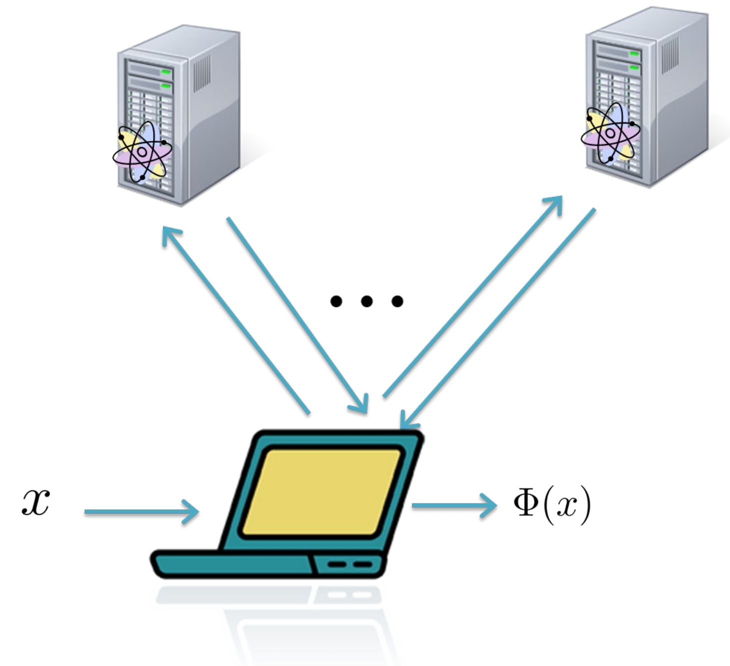
Interactive verification of quantum computations



Broadbent, A. (2018). How to Verify a Quantum Computation. *Theory of Computing*, *14*(1), 1-37.

Classical verifier

Using two isolated provers
[Reichardt, Unger & Vazirani 2013]



Using computational assumptions
[Mahadev 2018]

Certified Deletion

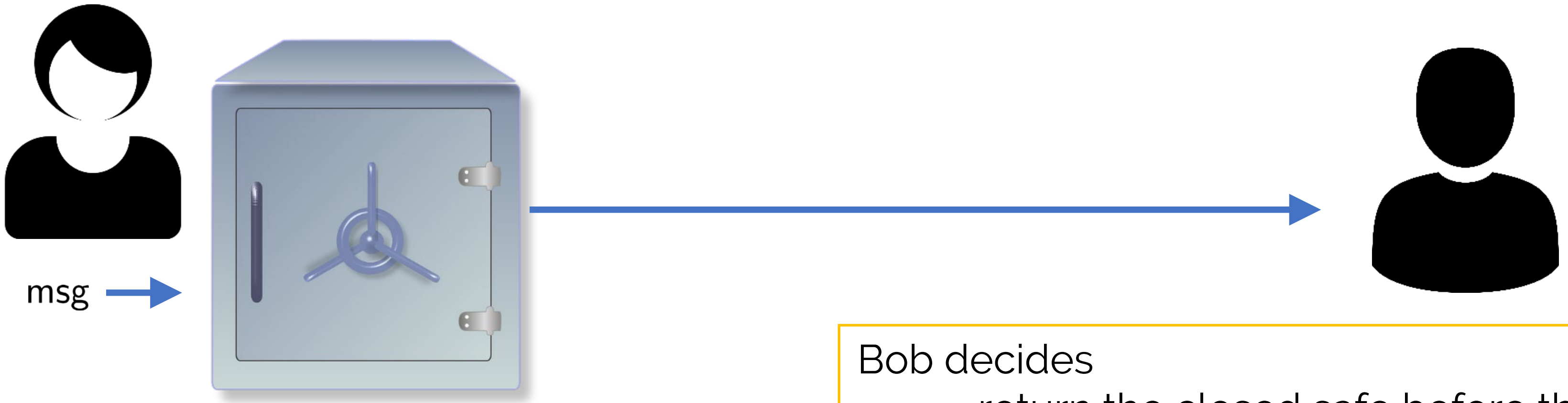
Anne Broadbent

IPAM

July 2022

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?
<u>No</u>!
Proof by contradiction…

Bob can :

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

AND

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

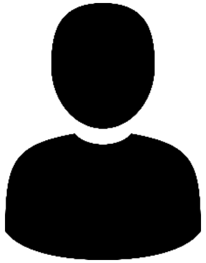
Certified Deletion
-application

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	$\boldsymbol{\theta}$	**0**	**1**	**0**	**1**
r random	r	0	1	1	0
Wiesner encoding	$\vert r\rangle_\theta$	$\vert 0\rangle$	$\vert -\rangle$	$\vert 1\rangle$	$\vert +\rangle$
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
$\lvert r\rangle_\theta$	$\lvert 0\rangle$	$\lvert -\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$
r_{comp}	0		1	
r_{diag}		1		0

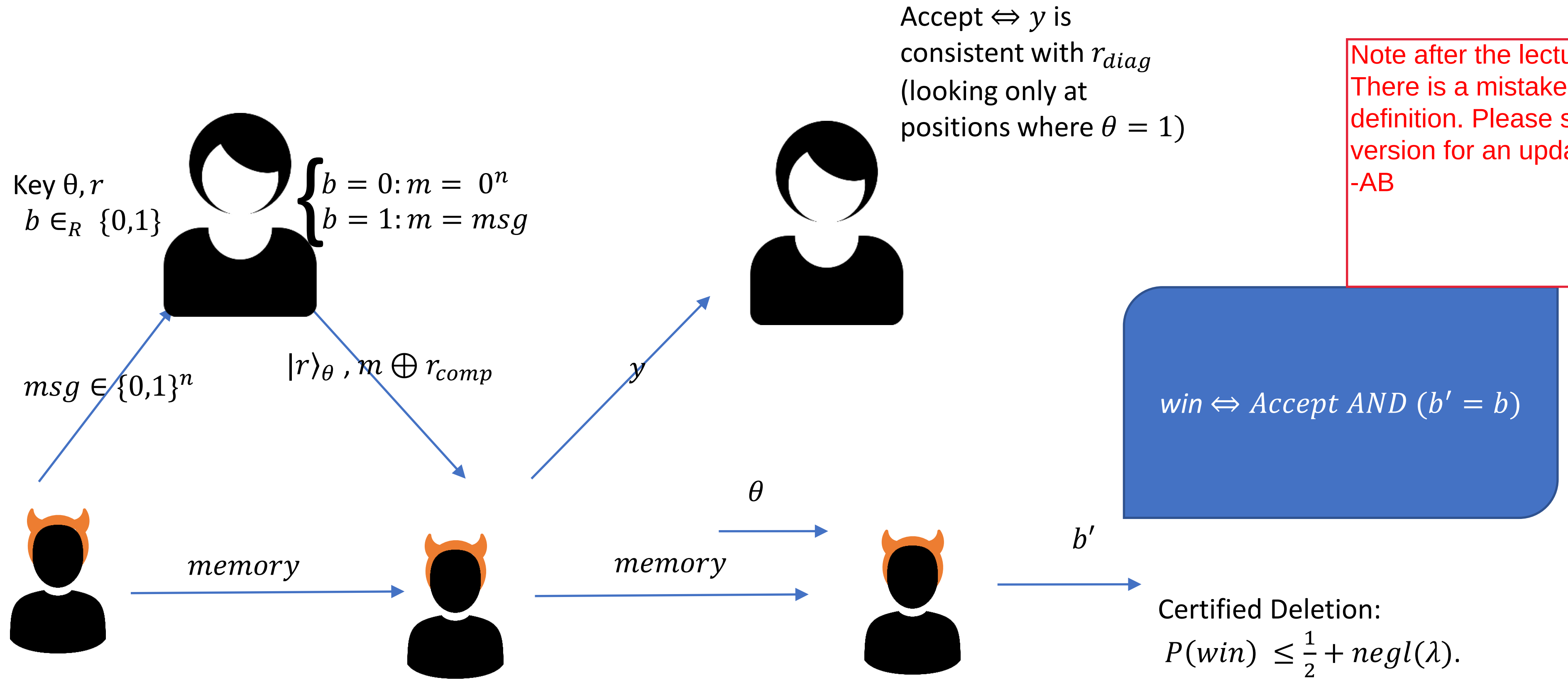
As the probability of predicting r_{diag} increases (i.e. adversary produces convincing "proof of deletion")

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

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

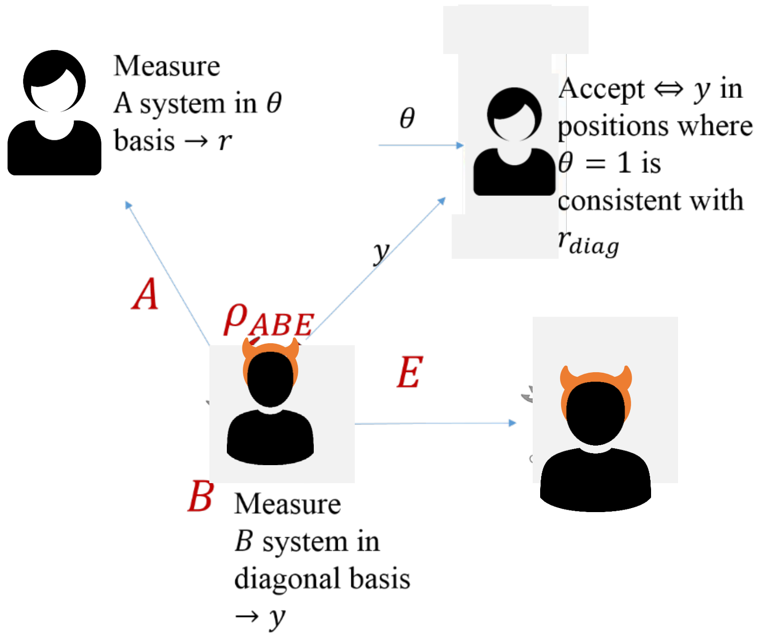
Maassen & Uffink, 1988

Certified Deletion Security Game



Note after the lecture:
There is a mistake in this definition. Please see latest arXiv version for an update.
-AB

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