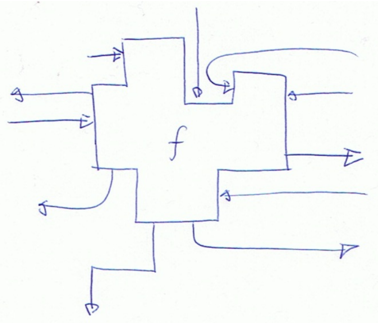
Cryptographic Primitives

Jürg Wullschleger

Université de Montréal
McGill University

What are cryptographic primitives?


f

Focus of This Talk:

Focus of This Talk:

Importance to Quantum Information.

Focus of This Talk:

Importance to Quantum Information.

Bias of the speaker...

Importance to Quantum Information

Importance to Quantum Information

Is it secure in the quantum setting?

Importance to Quantum Information

Is it secure in the quantum setting?

Can we do better in the quantum setting?

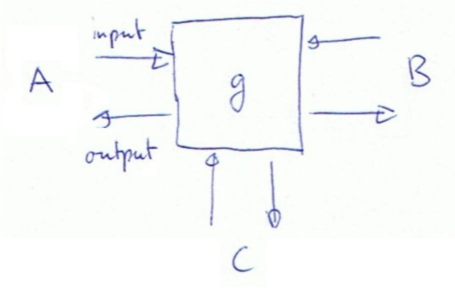
This Talk: Overview

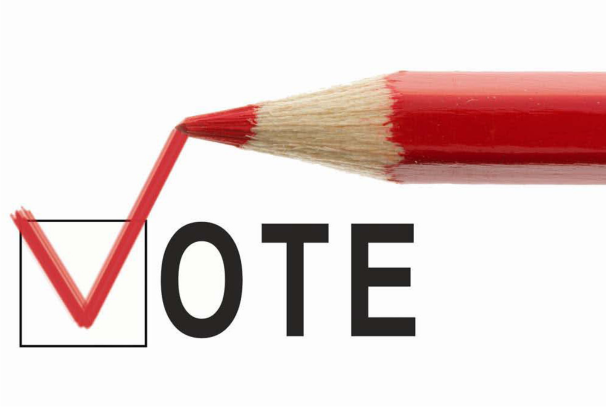
- Basics of Secure Multi Party Computation
- Oblivious Transfer (OT)
- Bit Commitment (BC)
- Coin Flip (CF)

Secure Multi Party Computation (MPC)

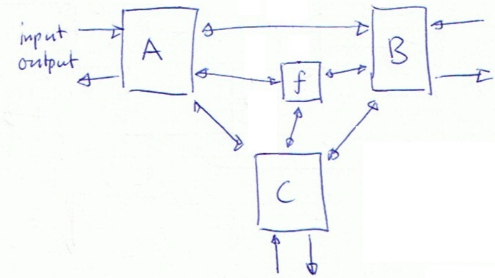
Secure Multi Party Computation (MPC)

Introduced by [Yao 82]

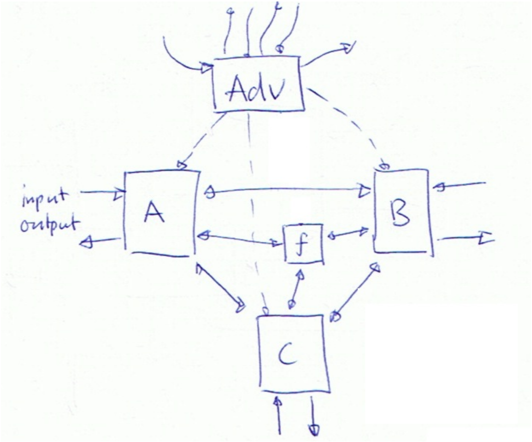

input
A
g
B
output
C


VOTE

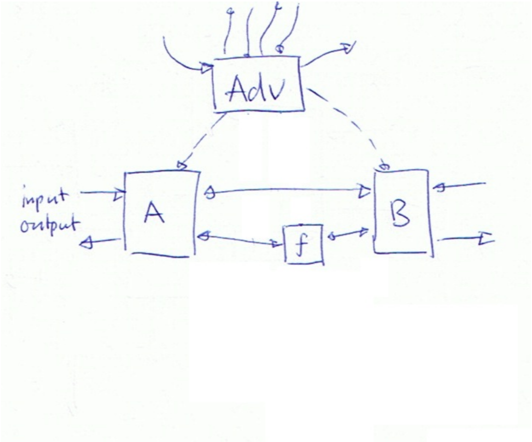
Cryptographic Protocol



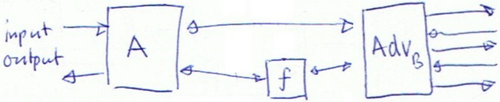
Cryptographic Protocol



Cryptographic Protocol



Cryptographic Protocol



Security?

Security?

List of Conditions:

- (Correctness) If both are honest, the protocol calculates g.
- (Sec. for B) Malicious A should not learn ... , except ... .
- (Sec. for A) ...

Security?

List of Conditions:

- (Correctness) If both are honest, the protocol calculates g.
- (Sec. for B) Malicious A should not learn ... , except ... .
- (Sec. for A) ...

Problems:

Security?

List of Conditions:

- (Correctness) If both are honest, the protocol calculates g.
- (Sec. for B) Malicious A should not learn . . . , except . . . .
- (Sec. for A) . . .

Problems:

- Difficult to formalize.

Security?

List of Conditions:

- (Correctness) If both are honest, the protocol calculates g.
- (Sec. for B) Malicious A should not learn ... , except ... .
- (Sec. for A) ...

Problems:

- Difficult to formalize.
- Ad hoc. Did we think of everything?

Security?

List of Conditions:

- (Correctness) If both are honest, the protocol calculates g.
- (Sec. for B) Malicious A should not learn . . . , except . . . .
- (Sec. for A) . . .

Problems:

- Difficult to formalize.
- Ad hoc. Did we think of everything?
- How to use the primitive?

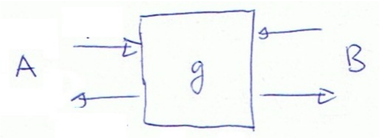
Security: Real vs. Ideal

Security: Real vs. Ideal

What do we want to achieve?

Security: Real vs. Ideal

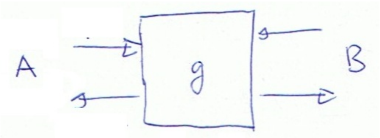
What do we want to achieve?



Show: the protocol implements g, **but nothing else**.

Security: Real vs. Ideal

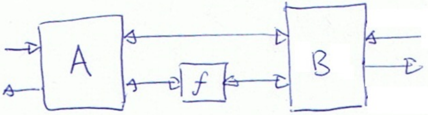
What do we want to achieve?



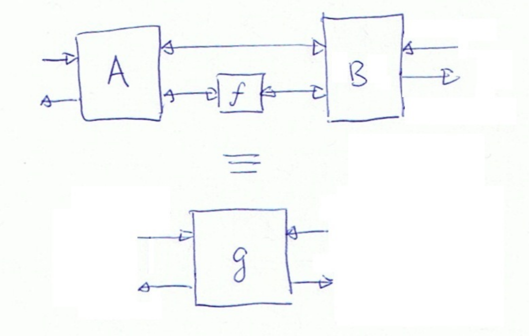
Show: the protocol implements g, **but nothing else**.

Anything the Adv can do in the protocol, he could also do with g.

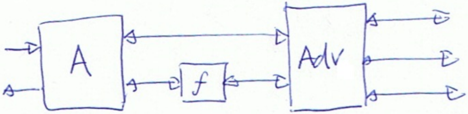
Security: Real vs. Ideal



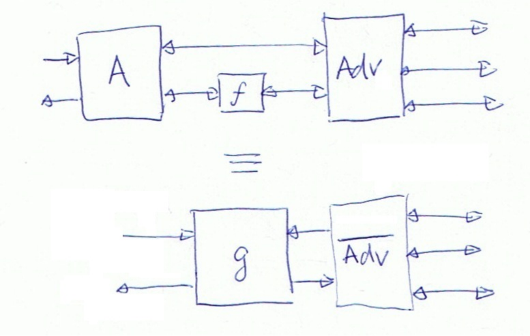
Security: Real vs. Ideal



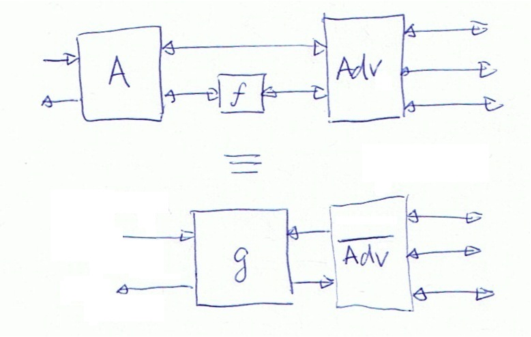
Security: Real vs. Ideal



Security: Real vs. Ideal

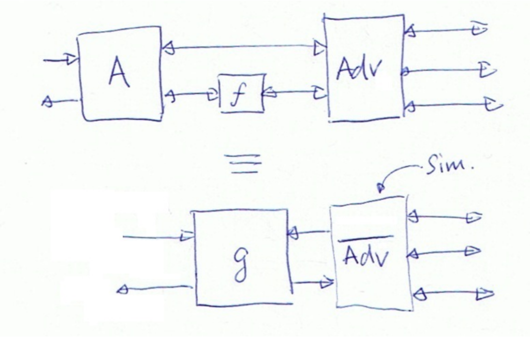


Security: Real vs. Ideal



$$\forall\, Adv\ \exists\, \overline{Adv}$$

Security: Real vs. Ideal



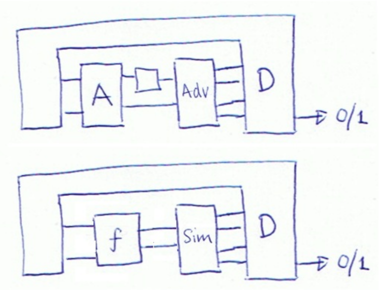
$$\forall\ Adv\ \exists\ \overline{Adv}$$

Distinguishers

What do we mean with $\equiv$?

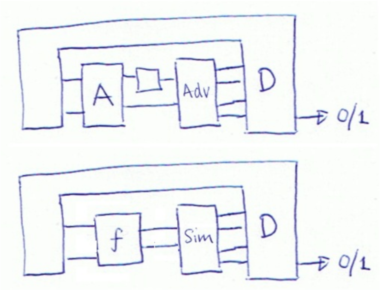
Distinguishers

What do we mean with $\equiv$?



Distinguishers

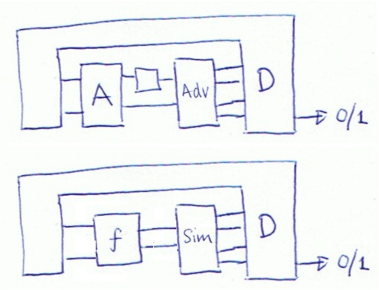
What do we mean with $\equiv$?



$$\forall D : |\Pr[D(real) = 1] - \Pr[D(ideal) = 1]| \leq \varepsilon \; .$$

Distinguishers

What do we mean with $\equiv$?

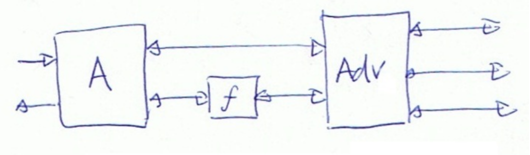


$$\forall D : |\Pr[D(real) = 1] - \Pr[D(ideal) = 1]| \leq \varepsilon \ .$$

$$\frac{1}{2}\|\rho_{real} - \rho_{ideal}\|_1 \leq \varepsilon \ .$$

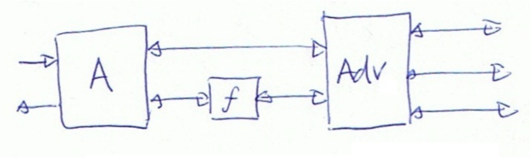
Sequential vs. Universal Composability

Sequential vs. Universal Composability

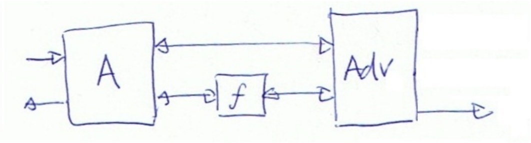


Online

Sequential vs. Universal Composability

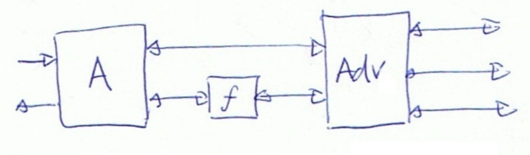


Online

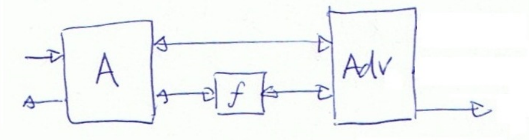


Offline

Sequential vs. Universal Composability

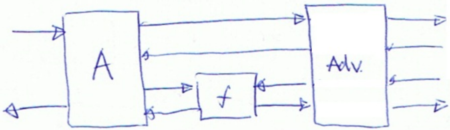


Online / Universal Composability (UC) [Canetti 01]

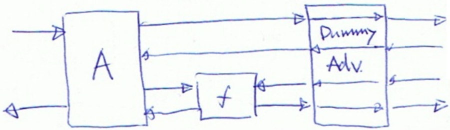


Offline / Sequential Composability [Beaver 92, Canetti 96]

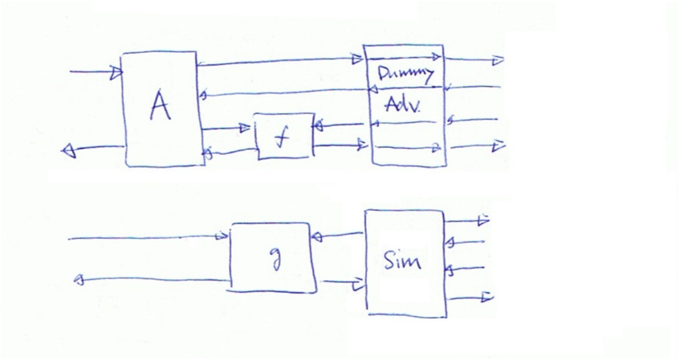
Dummy Adversary



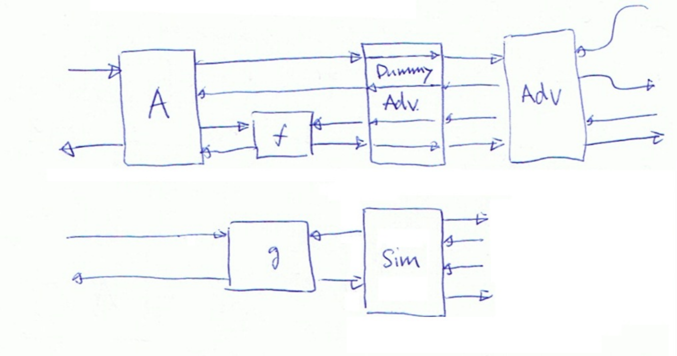
Dummy Adversary



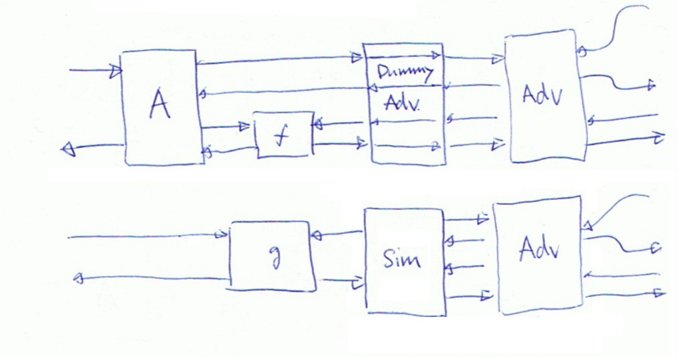
Dummy Adversary



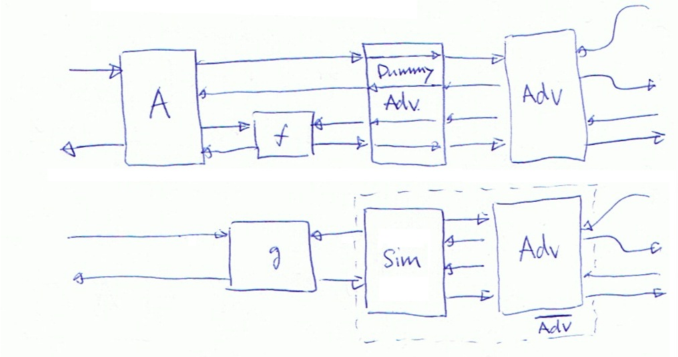
Dummy Adversary



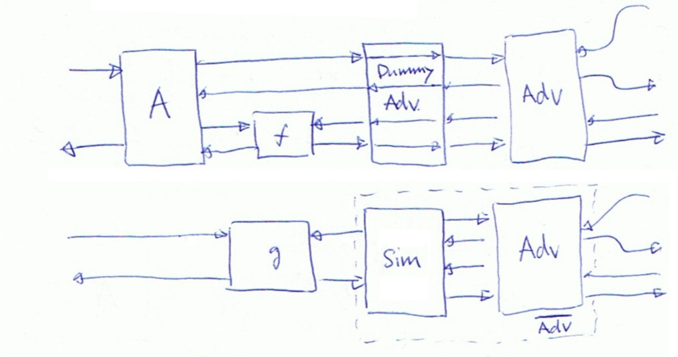
Dummy Adversary



Dummy Adversary

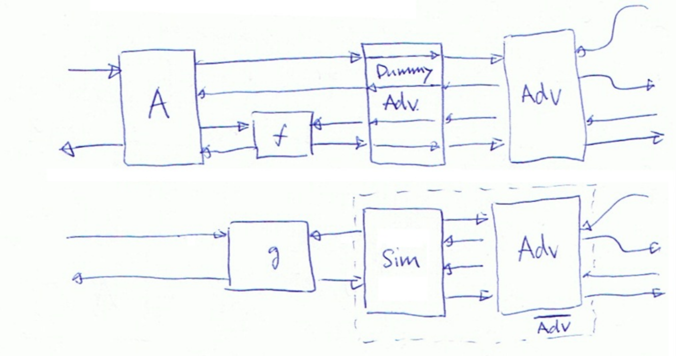


Dummy Adversary



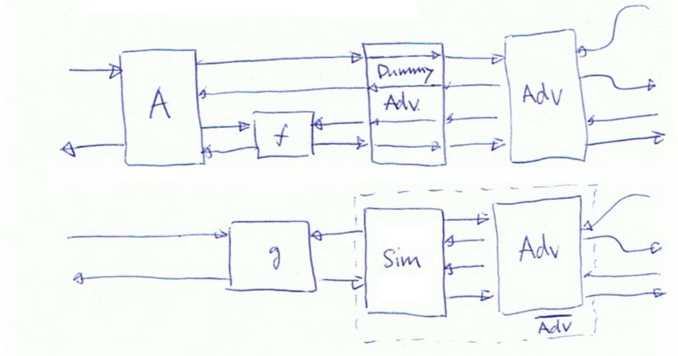
Sec. against dummy $\Rightarrow$ Sec. against **any** Adv!

Dummy Adversary



Sec. against dummy $\Rightarrow$ Sec. against **any** Adv! Even Quantum.

Dummy Adversary



Sec. against dummy ⇒ Sec. against **any** Adv! Even Quantum.

Quantum Lifting Theorem: [Unruh10]

Classical UC implies Quantum UC.

The Semi-Honest Adversary

Semi-Honest / Honest-but-curious Adversary:

- Follows the protocol.
- Remembers everything.

The Semi-Honest Adversary

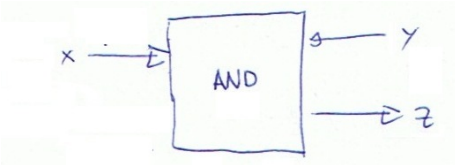
Semi-Honest / Honest-but-curious Adversary:

- Follows the protocol.
- Remembers everything.

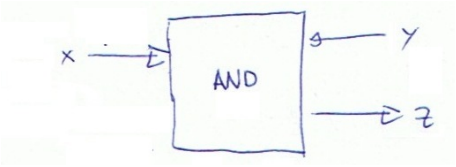
Attention: Also the simulator must be semi-honest!

Malicious $\not\rightarrow$ Semi-Honest Security

Malicious $\not\rightarrow$ Semi-Honest Security



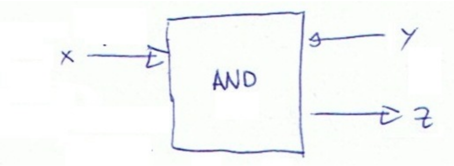
Malicious $\not\Rightarrow$ Semi-Honest Security



Malicious Model:

Protocol "A sends x to B" is secure!

Malicious $\not\Rightarrow$ Semi-Honest Security

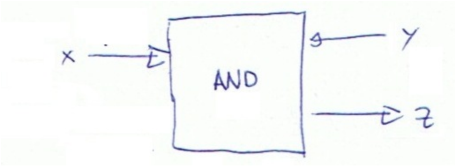


Malicious Model:

Protocol "A sends x to B" is secure!

...since B can always get x by choosing $y = 1$.

Malicious $\not\Rightarrow$ Semi-Honest Security



Malicious Model:

Protocol "A sends x to B" is secure!

...since B can always get x by choosing $y = 1$.

Semi-Honest Model:

OT required.

Summary MPC

- Real vs. Ideal
- UC (Online) / Sequential (Offline)
- Classical UC $\Rightarrow$ Quantum UC

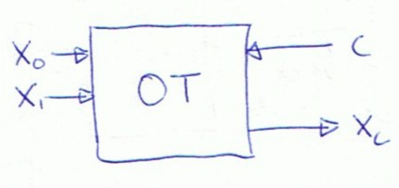
Further reading:

D. Unruh: "Universally Composable Quantum Multi-Party Computation", arXiv:0910.2912

S. Fehr, C. Schaffner: "Composing Quantum Protocols in a Classical Environment", arXiv:0804.1059

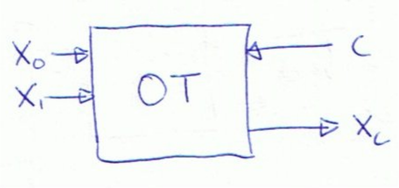
Oblivious Transfer

Oblivious Transfer



[Wiesner ∼69], [Rabin 83], [Even Lempel Goldreich 85].

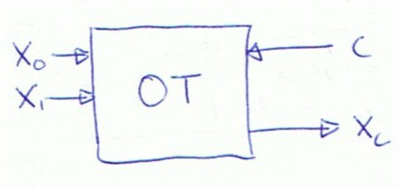
Oblivious Transfer



[Wiesner ∼69], [Rabin 83], [Even Lempel Goldreich 85].

Interesting, because:

Oblivious Transfer



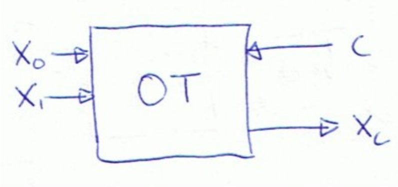
[Wiesner ∼69], [Rabin 83], [Even Lempel Goldreich 85].

Interesting, because:

- Simple.
- Powerful: Build **any*** primitive [Kilian 88].

* some fine print

Oblivious Transfer

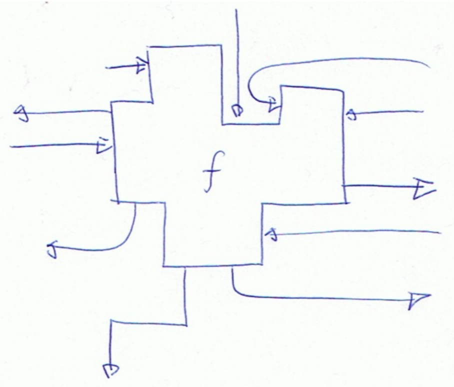


[Wiesner ~69], [Rabin 83], [Even Lempel Goldreich 85].

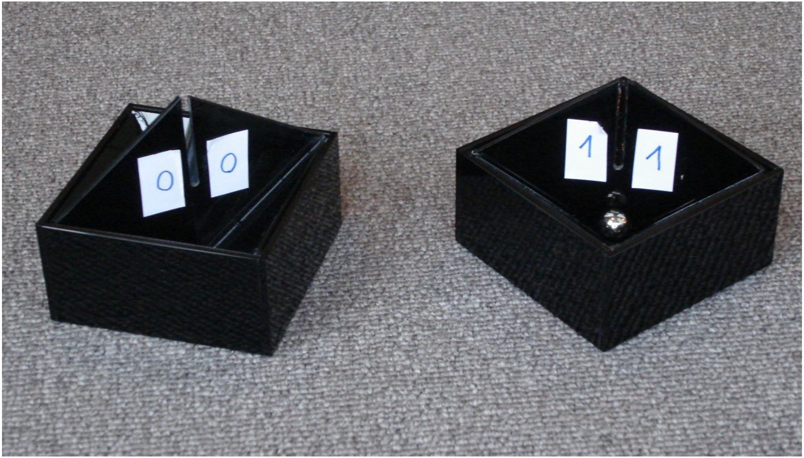
Interesting, because:

- Simple.
- Powerful: Build **any*** primitive [Kilian 88]. Quantum: [Dupuis Salvail Nielsen 12]

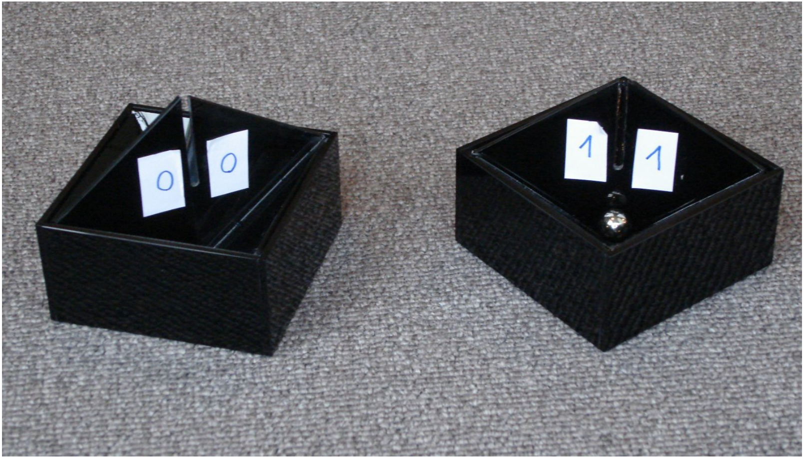
* some fine print


f

Oblivious Transfer - Model



Oblivious Transfer - Model



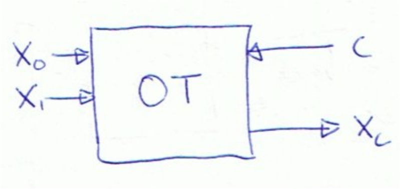
Note: OT does **not** allow input delay!

Oblivious Transfer Impossibility (Classically)

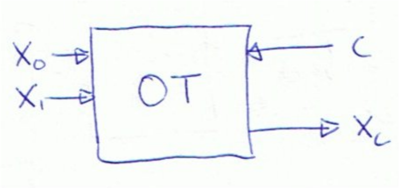
Oblivious Transfer Impossibility (Classically)

Boils down to:
If Bob doesn't leak his input c, but learns the output x_c, then Alice must send both x_0 and x_1.

Quantum OT?



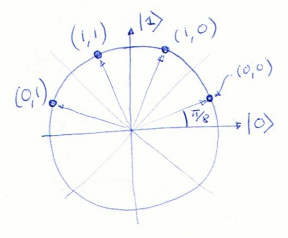
Quantum OT?



Wiesner: Invented OT to be implemented by a quantum protocol!

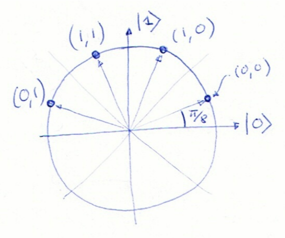
Quantum OT?

Encode 2 bits in one qubit:



Quantum OT?

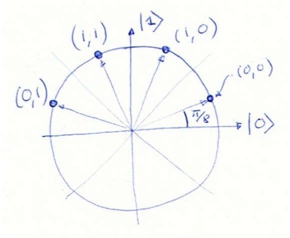
Encode 2 bits in one qubit:



Works with prob. 85 %.

Quantum OT?

Encode 2 bits in one qubit:

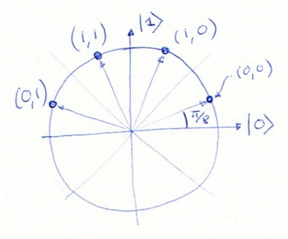


Works with prob. 85 %.

Wiesner's scheme: Error correction. No error, but not secure.

Quantum OT?

Encode 2 bits in one qubit:



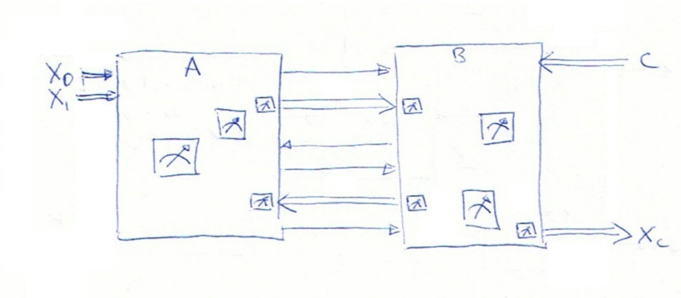
Works with prob. 85 %.

Wiesner's scheme: Error correction. No error, but not secure.

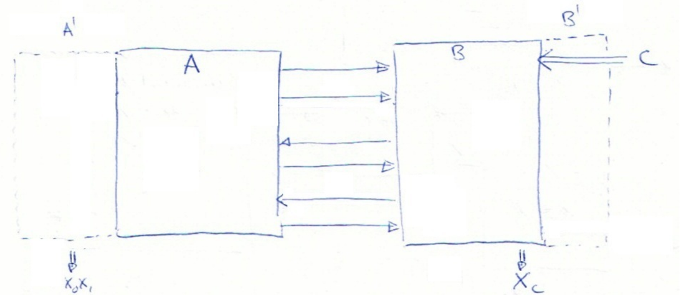
...

Impossibility of Quantum OT

Impossibility of Quantum OT - Purified Protocol



Impossibility of Quantum OT - Purified Protocol



After the protocol execution: pure state $|\rho_c^{AA'BB'}\rangle$.

Equivalence of Purifications

For any $|\rho^{AB}\rangle$, $|\phi^{AB}\rangle$:
If $\rho^A = \phi^A$, then there exists an U^B, such that

$$|\rho^{AB}\rangle = (\mathbb{1}^A \otimes U^B)|\phi^{AB}\rangle \ .$$

Equivalence of Purifications

For any $|\rho^{AB}\rangle$, $|\phi^{AB}\rangle$:
If $\rho^{A} = \phi^{A}$, then there exists an U^{B}, such that

$$|\rho^{AB}\rangle = (\mathbb{1}^{A} \otimes U^{B})|\phi^{AB}\rangle \ .$$

ε: Uhlmann's Theorem.

Impossibility of Quantum OT [Lo97]

Impossibility of Quantum OT [Lo97]

- After the protocol execution: pure state $|\rho_c^{AA'BB'}\rangle$.

Impossibility of Quantum OT [Lo97]

- After the protocol execution: pure state $|\rho_c^{AA'BB'}\rangle$.
- Alice does not learn c: $\rho_0^{AA'} = \rho_1^{AA'}$.

Impossibility of Quantum OT [Lo97]

- After the protocol execution: pure state $|\rho_c^{AA'BB'}\rangle$.
- Alice does not learn c: $\rho_0^{AA'} = \rho_1^{AA'}$.
- There exists a $U^{BB'}$, such that

$$|\rho_1^{AA'BB'}\rangle = (\mathbb{1}^{AA'} \otimes U^{BB'})|\rho_0^{AA'BB'}\rangle \ .$$

Impossibility of Quantum OT [Lo97]

- After the protocol execution: pure state $|\rho_c^{AA'BB'}\rangle$.
- Alice does not learn c: $\rho_0^{AA'} = \rho_1^{AA'}$.
- There exists a $U^{BB'}$, such that

$$|\rho_1^{AA'BB'}\rangle = (\mathbb{1}^{AA'} \otimes U^{BB'})|\rho_0^{AA'BB'}\rangle \ .$$

Therefore, Bob can change c **after** the protocol is over!

Impossibility of Quantum OT [Lo97]

- After the protocol execution: pure state $|\rho_c^{AA'BB'}\rangle$.
- Alice does not learn c: $\rho_0^{AA'} = \rho_1^{AA'}$.
- There exists a $U^{BB'}$, such that

$$|\rho_1^{AA'BB'}\rangle = (\mathbb{1}^{AA'} \otimes U^{BB'})|\rho_0^{AA'BB'}\rangle \; .$$

Therefore, Bob can change c **after** the protocol is over! **Insecure.**

Impossibility of Quantum OT [Lo97]

- After the protocol execution: pure state $|\rho_c^{AA'BB'}\rangle$.
- Alice does not learn c: $\rho_0^{AA'} = \rho_1^{AA'}$.
- There exists a $U^{BB'}$, such that

$$|\rho_1^{AA'BB'}\rangle = (\mathbb{1}^{AA'} \otimes U^{BB'})|\rho_0^{AA'BB'}\rangle .$$

Therefore, Bob can change c **after** the protocol is over! **Insecure.**

Stronger: Bob can also get x_0, apply $U^{BB'}$, and get x_1.

Extending OT?

Extending OT?

Without authenticated channels, even QKD is impossible!

Extending OT?

Without authenticated channels, even QKD is impossible!
We need a short key to start with.

Extending OT?

Without authenticated channels, even QKD is impossible!
We need a short key to start with.

What if we are given a small number of OTs?
Can we make $n+1$ from n? OTs?

Impossibility of Extending OT [Winkler W. 10]

Given: n OT's. Create $m > n$ OT's.

Impossibility of Extending OT [Winkler W. 10]

Given: n OT's. Create $m > n$ OT's.

- Purify the n OT's with a system E of $3n$ qubits.

Impossibility of Extending OT [Winkler W. 10]

Given: n OT's. Create $m > n$ OT's.

- Purify the n OT's with a system E of $3n$ qubits.
- After the protocol execution: pure state $|\rho_c^{AA'BB'E}\rangle$.

Impossibility of Extending OT [Winkler W. 10]

Given: n OT's. Create $m > n$ OT's.

- Purify the n OT's with a system E of $3n$ qubits.
- After the protocol execution: pure state $|\rho_c^{AA'BB'E}\rangle$.
- Without E, the protocol is secure, but given E, Bob can break it.

Impossibility of Extending OT [Winkler W. 10]

Given: n OT's. Create $m > n$ OT's.

- Purify the n OT's with a system E of $3n$ qubits.
- After the protocol execution: pure state $|\rho_c^{AA'BB'E}\rangle$.
- Without E, the protocol is secure, but given E, Bob can break it.
- Entropic argument: $m \leq 2|E| = 6n$.

Impossibility of Extending OT [Winkler W. 10]

Given: n OT's. Create $m > n$ OT's.

- Purify the n OT's with a system E of $3n$ qubits.
- After the protocol execution: pure state $|\rho_c^{AA'BB'E}\rangle$.
- Without E, the protocol is secure, but given E, Bob can break it.
- Entropic argument: $m \leq 2|E| = 6n$.

Implies that $n + 1$ from n OTs is impossible.

Impossibility of Extending OT [Winkler W. 10]

Given: n OT's. Create $m > n$ OT's.

- Purify the n OT's with a system E of $3n$ qubits.
- After the protocol execution: pure state $|\rho_c^{AA'BB'E}\rangle$.
- Without E, the protocol is secure, but given E, Bob can break it.
- Entropic argument: $m \leq 2|E| = 6n$.

Implies that $n+1$ from n OTs is impossible.

Note: Bound is weaker than in the classical setting.

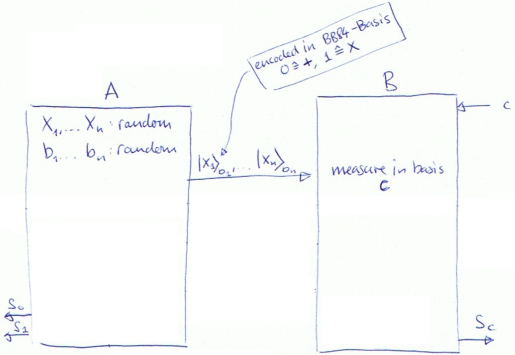
We need Additional Assumptions

We need Additional Assumptions

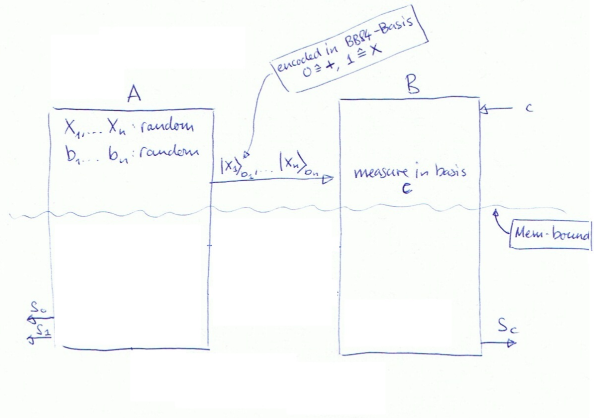
Bounded/Noisy Quantum Storage Model:

Adversary does not have an unlimited, perfect quantum storage.

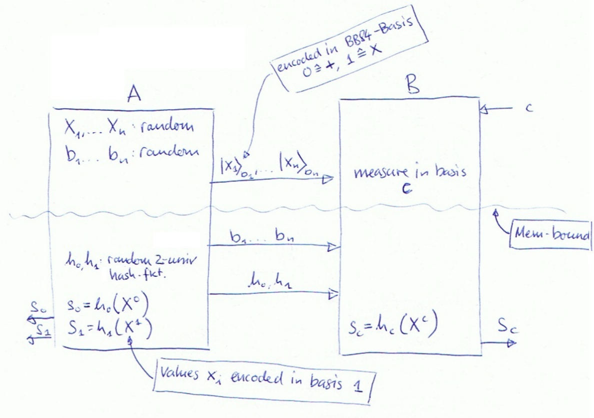
OT in the Bounded Quantum Storage Model [. . . ,DFRSS07]



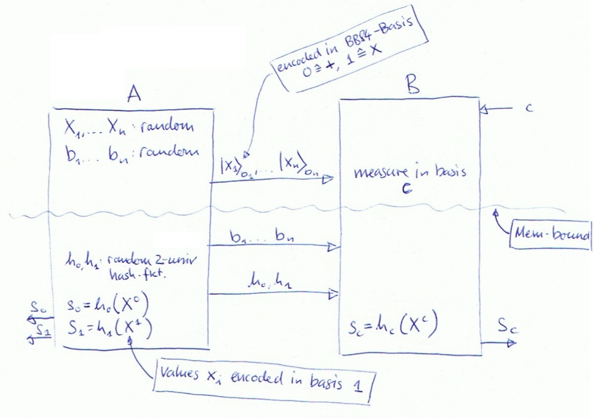
OT in the Bounded Quantum Storage Model [. . . ,DFRSS07]



OT in the Bounded Quantum Storage Model [. . . ,DFRSS07]



OT in the Bounded Quantum Storage Model [. . . ,DFRSS07]



Proof: Uncertainty relation + privacy amplification.

Use OTs from MPC

Use OTs from MPC

Semi-Honest Model

Share Secrets. Evaluate circuit gates, one-by-one.

Use OTs from MPC

Semi-Honest Model

Share Secrets. Evaluate circuit gates, one-by-one.

Malicious Model

Use OTs from MPC

Semi-Honest Model
Share Secrets. Evaluate circuit gates, one-by-one.

Malicious Model
Somehow force players to follow protocol.

Use OTs from MPC

Semi-Honest Model
Share Secrets. Evaluate circuit gates, one-by-one.

Malicious Model
Somehow force players to follow protocol.

[Crépeau van de Graaf Tapp 95]: Use bit commitments.

Use OTs from MPC

Semi-Honest Model

Share Secrets. Evaluate circuit gates, one-by-one.

Malicious Model

Somehow force players to follow protocol.

[Crépeau van de Graaf Tapp 95]: Use bit commitments.

[Ishai Prabhakaran Sahai 08]: Use an MPC-in-the-head.

Summary OT

- OT: Simple + Useful.
- Creating / Extending OT is impossible.
- OT is possible in BQS model.

Further reading:

S. Winkler, J. Wullschleger: "On the Efficiency of Classical and Quantum Secure Function Evaluation", arXiv:1205.5136

I. Damgaard, S. Fehr, R. Renner, L. Salvail, C. Schaffner: "A Tight High-Order Entropic Quantum Uncertainty Relation With Applications", arXiv:quant-ph/0612014

Y. Ishai, M. Prabhakaran, and A. Sahai: "Founding Cryptography on Oblivious Transfer - Efficiently", CRYPTO 08.

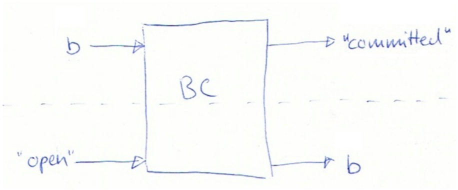
Bit Commitment (BC)

Bit Commitment (BC)

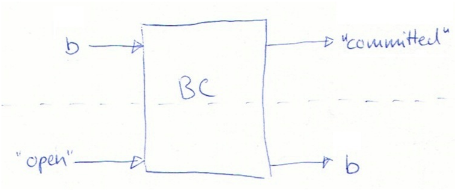
First formally defined in [Bennett Brassard Crépeau 88]

aka: Commitment, Commitment Scheme, Commit-and-Open, Commit-and-Reveal, ...

Bit Commitment



Bit Commitment



Mostly used to force players to follow the protocol.

BC implementations

Quantum protocol for creating BC

[Mayers 97, Lo Chau 97]: Impossible. Basically the same proof as for OT.

BC implementations

Quantum protocol for creating BC

[Mayers 97, Lo Chau 97]: Impossible. Basically the same proof as for OT.

Quantum protocol for extending BC

[Winkler W. 10, Winkler Tomamichel Hengl Renner 11]: Impossible.

BC implementations

Quantum protocol for creating BC

[Mayers 97, Lo Chau 97]: Impossible. Basically the same proof as for OT.

Quantum protocol for extending BC

[Winkler W. 10, Winkler Tomamichel Hengl Renner 11]: Impossible.

OT $\rightarrow$ BC

BC implementations

Quantum protocol for creating BC

[Mayers 97, Lo Chau 97]: Impossible. Basically the same proof as for OT.

Quantum protocol for extending BC

[Winkler W. 10, Winkler Tomamichel Hengl Renner 11]: Impossible.

OT $\rightarrow$ BC

Easy.

BC implementations

Quantum protocol for creating BC

[Mayers 97, Lo Chau 97]: Impossible. Basically the same proof as for OT.

Quantum protocol for extending BC

[Winkler W. 10, Winkler Tomamichel Hengl Renner 11]: Impossible.

OT $\rightarrow$ BC

Easy.

BC $\rightarrow$ OT

BC implementations

Quantum protocol for creating BC

[Mayers 97, Lo Chau 97]: Impossible. Basically the same proof as for OT.

Quantum protocol for extending BC

[Winkler W. 10, Winkler Tomamichel Hengl Renner 11]: Impossible.

OT $\rightarrow$ BC

Easy.

BC $\rightarrow$ OT

Impossible classically.

BC implementations

Quantum protocol for creating BC

[Mayers 97, Lo Chau 97]: Impossible. Basically the same proof as for OT.

Quantum protocol for extending BC

[Winkler W. 10, Winkler Tomamichel Hengl Renner 11]: Impossible.

OT $\rightarrow$ BC

Easy.

BC $\rightarrow$ OT

Impossible classically.
Quantumly?

Quantum Protocol of BC $\rightarrow$ OT

Quantum Protocol of BC $\rightarrow$ OT

[Crépeau Kilian 88, Bennett Brassard Crépeau Skubiszewska 91, Mayers Salvail 94, Yao 95, Crépeau Dumais Mayers Salvail 04, Damgård Fehr Lunemann Salvail Schaffner 09, Bouman Fehr 09, Unruh 10]

Quantum Protocol of BC $\rightarrow$ OT

[Crépeau Kilian 88, Bennett Brassard Crépeau Skubiszewska 91, Mayers Salvail 94, Yao 95, Crépeau Dumais Mayers Salvail 04, Damgård Fehr Lunemann Salvail Schaffner 09, Bouman Fehr 09, Unruh 10]

Basic Idea:

- Use a protocol very similar to the BQSM-protocol from before.
- Bob commits to **all** his measurement basis and outcome.
- Cut-And-Choose: Alice asks Bob to open a small subset and checks.

Summary BC

- Quantum BC is impossible.
- OT $\rightarrow$ BC.
- Quantum: BC $\rightarrow$ OT.

Further reading:

C. Crépeau, J. van de Graaf, A. Tapp: "Committed Oblivious Transfer and Private Multi-Party Computation", www.cs.mcgill.ca/∼crepeau/PS/CGT95.ps

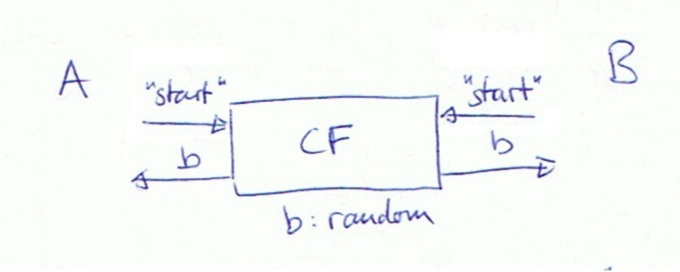
Niek J. Bouman, Serge Fehr: "Sampling in a Quantum Population, and Applications", arXiv:0907.4246

Coin Flip

Coin Flip

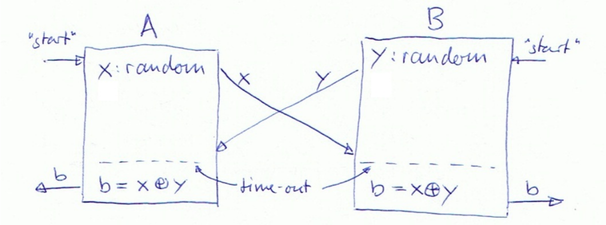
Introduced by [Blum 81]

Coin Flip



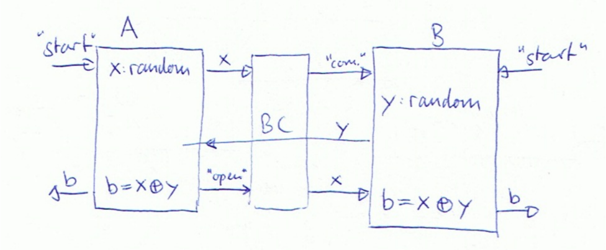
Relativistic Coin Flip

Relativistic Coin Flip

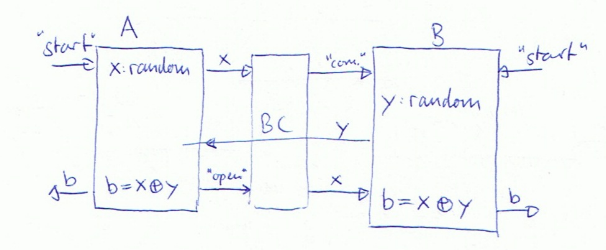


Coin Flip from BC

Coin Flip from BC

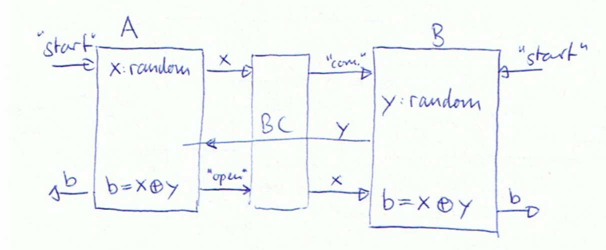


Coin Flip from BC



Secure?

Coin Flip from BC

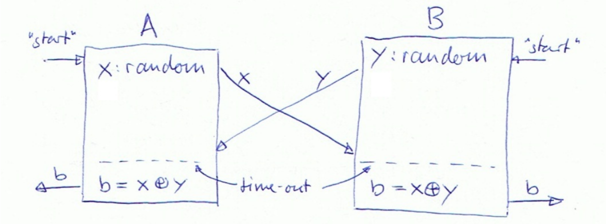


Secure?

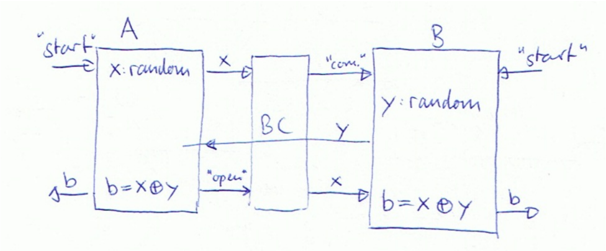
Alice can refuse to open!

Coin Flip from BC

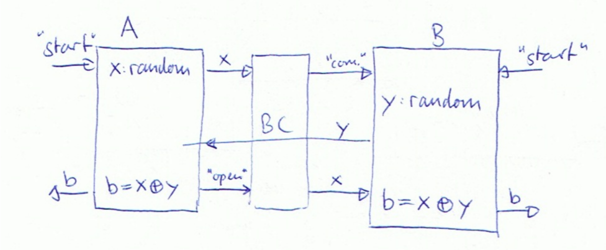
But we can also abort here!



Coin Flip from BC - Problem

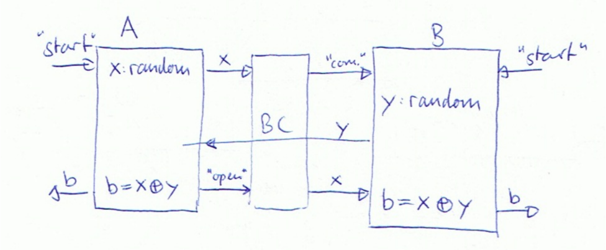


Coin Flip from BC - Problem



Unfair, because Alice can **SELECTIVELY** abort. E.g., for $y = 0$.

Coin Flip from BC - Problem

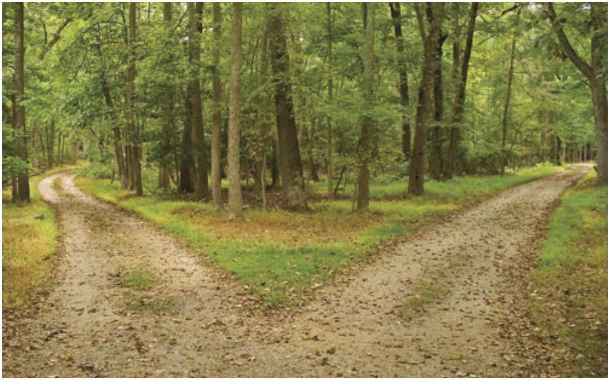


Unfair, because Alice can **SELECTIVELY** abort. E.g., for $y = 0$.

But should we care! We then know that she is cheating!

Forest-Crossing Problem

Forest-Crossing Problem



Coin Flip from BC - Problem

What can we do?

Coin Flip from BC - Problem

What can we do? It's complicated.

Coin Flip from BC - Problem

What can we do? It's complicated.

[Cleve 86]:

Any protocol with n rounds has an error of at least $\Omega(1/n)$.

Coin Flip from BC - Problem

What can we do? It's complicated.

[Cleve 86]:

Any protocol with n rounds has an error of at least $\Omega(1/n)$.
(Classical proof, but can be generalized to quantum.)

Coin Flip from BC - Problem

What can we do? It's complicated.

[Cleve 86]:

Any protocol with n rounds has an error of at least $\Omega(1/n)$.
(Classical proof, but can be generalized to quantum.)

There exists a protocol using BC with n rounds and error $O(1/\sqrt{n})$.
(Protocol: n times the 1-round protocol + majority)

Coin Flip from BC - Problem

What can we do? It's complicated.

[Cleve 86]:

Any protocol with n rounds has an error of at least $\Omega(1/n)$.
(Classical proof, but can be generalized to quantum.)

There exists a protocol using BC with n rounds and error $O(1/\sqrt{n})$.
(Protocol: n times the 1-round protocol + majority)

[Moran Naor Segev 09]

There exists a protocol using OT with n rounds and error $O(1/n)$.

Coin Flip from BC - Problem

What can we do? It's complicated.

[Cleve 86]:

Any protocol with n rounds has an error of at least $\Omega(1/n)$.
(Classical proof, but can be generalized to quantum.)

There exists a protocol using BC with n rounds and error $O(1/\sqrt{n})$.
(Protocol: n times the 1-round protocol + majority)

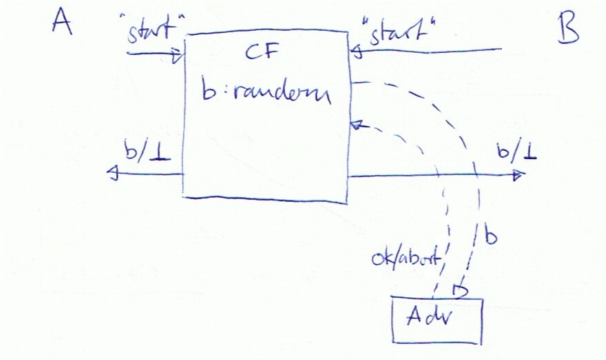
[Moran Naor Segev 09]

There exists a protocol using OT with n rounds and error $O(1/n)$.

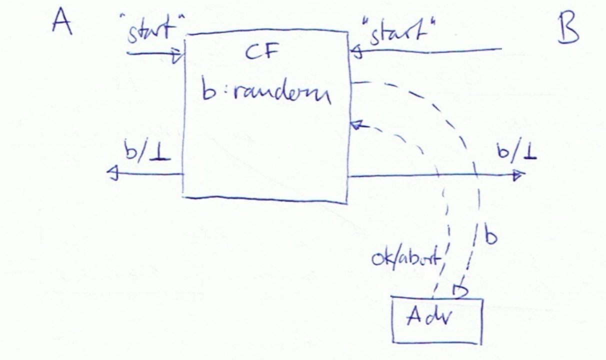
Most Fkt. with 2 outputs have this problem.

Unfair Version of CF

Unfair Version of CF



Unfair Version of CF



Equivalent to "Strong Coin Flip".

Coin Flip Variants

- (Fair) Coin Flip (CF).
- Unfair Coin Flip / Strong Coin Flip (SCF).

Coin Flip Variants

- (Fair) Coin Flip (CF).
- Unfair Coin Flip / Strong Coin Flip (SCF).
- Weak Coin Flip (WCF): Players have preferred value.

Coin Flip Variants

- (Fair) Coin Flip (CF).
- Unfair Coin Flip / Strong Coin Flip (SCF).
- Weak Coin Flip (WCF): Players have preferred value.

Note: WCF cannot be unfair.

Weak and Strong Coin Flip: Results

Results:

Weak and Strong Coin Flip: Results

Results:

- WCF + SCF are impossible in the classical setting.

Weak and Strong Coin Flip: Results

Results:

- WCF + SCF are impossible in the classical setting.
- WCF is possible in the quantum setting, for any $\varepsilon > 0$. [Mochon 07]

Weak and Strong Coin Flip: Results

Results:

- WCF + SCF are impossible in the classical setting.
- WCF is possible in the quantum setting, for any $\varepsilon > 0$. [Mochon 07]
- SCF is impossible in the quantum setting. [Kitaev 02]

Weak and Strong Coin Flip: Results

Results:

- WCF + SCF are impossible in the classical setting.
- WCF is possible in the quantum setting, for any $\varepsilon > 0$. [Mochon 07]
- SCF is impossible in the quantum setting. [Kitaev 02]

How much possible / impossible?

Weak and Strong Coin Flip: Results

Results:

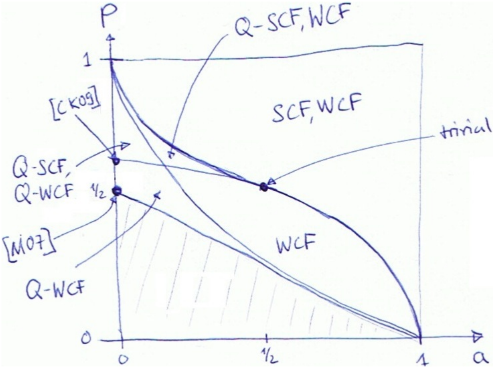
- WCF + SCF are impossible in the classical setting.
- WCF is possible in the quantum setting, for any $\varepsilon > 0$. [Mochon 07]
- SCF is impossible in the quantum setting. [Kitaev 02]

How much possible / impossible?

Long line of research: [Aharanov Ta-Shma Vazirani Yao 00, Ambainis 01, Spekkens Rudolph 01, Kitaev 02, Spekkens Rudolph 02, Mochon 04, Hofheinz Müller-Quade Unruh 06, Mochon 07, Nguyen Frison Huy Massar 08, Chailloux Kerenidis 09, Hänggi W. 11]

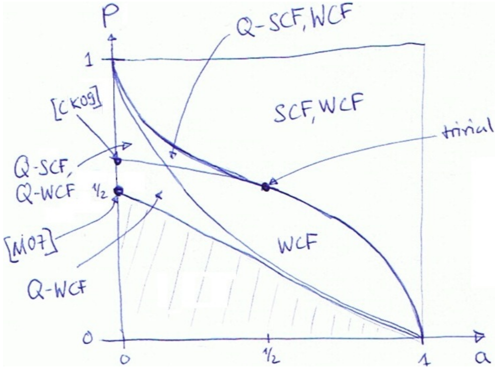
WCF and SCF Bounds.

a: abort probability, p: max. probability of a value.



WCF and SCF Bounds.

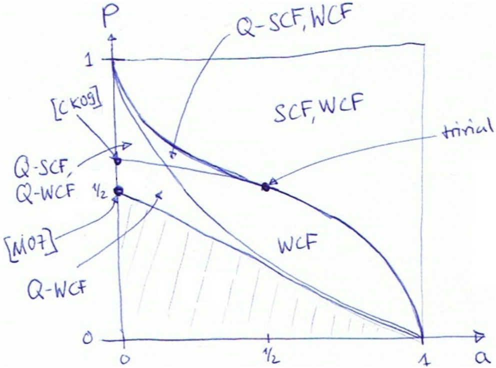
a: abort probability, *p*: max. probability of a value.



All protocols are classical + really simple, except [M 07].

WCF and SCF Bounds.

a: abort probability, p: max. probability of a value.



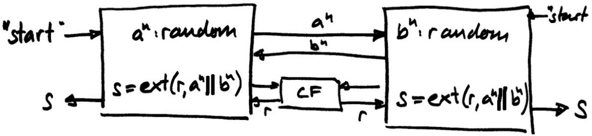
All protocols are classical + really simple, except [M 07].

Fair CF???

Extending Coin Flips?

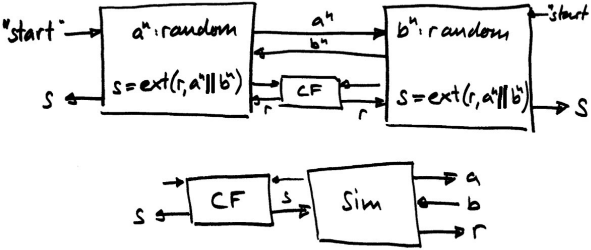
Extending Coin Flips?

Can even be done classically [Hofheinz Müller-Quade Unruh 06]:



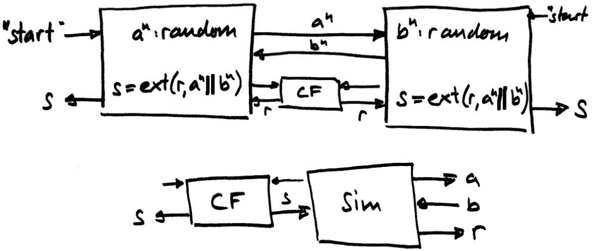
Extending Coin Flips?

Can even be done classically [Hofheinz Müller-Quade Unruh 06]:



Extending Coin Flips?

Can even be done classically [Hofheinz Müller-Quade Unruh 06]:

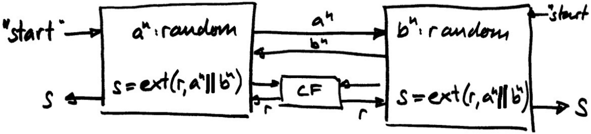


It is unlikely that Sim can find a r with:

$$s = ext(r, a^n \| b^n) \; .$$

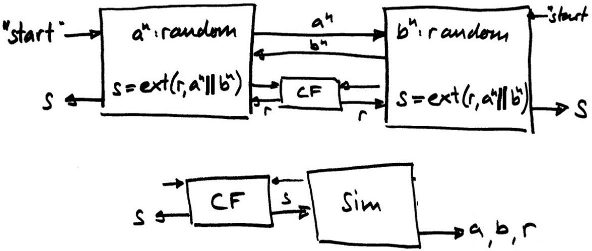
Extending Coin Flips?

Can even be done classically [Hofheinz Müller-Quade Unruh 06]:



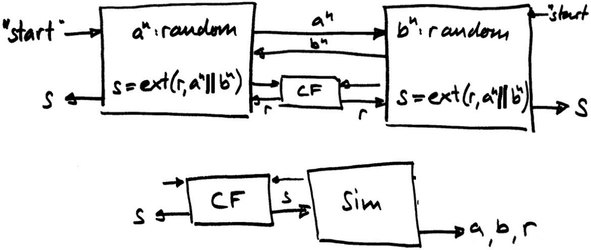
Extending Coin Flips?

Can even be done classically [Hofheinz Müller-Quade Unruh 06]:



Extending Coin Flips?

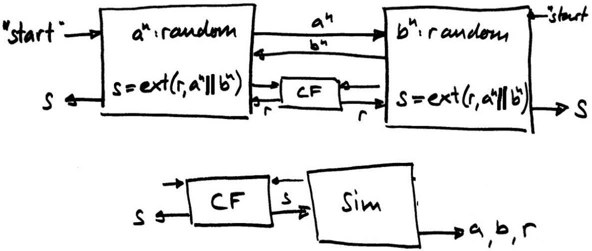
Can even be done classically [Hofheinz Müller-Quade Unruh 06]:



Works also against quantum adversary.

Extending Coin Flips?

Can even be done classically [Hofheinz Müller-Quade Unruh 06]:



Works also against quantum adversary. UC?

Summary Coin Flip

- Three types: fair CF, (unfair) SCF, WCF.
- BC $\rightarrow$ SCF.
- Quantum WCF possible, others not.
- Optimal quantum SCF achieved by classical protocol using WCF.

Further reading:

R. Cleve: "Limits on the security of coin flips when half the processors are faulty", STOC 86

C. Mochon: "Quantum weak coin flipping with arbitrarily small bias", arXiv:0711.4114

D. Hofheinz, J. Müller-Quade, D. Unruh: "On the (Im-)Possibility of Extending Coin Toss", on eprint.iacr.org/2006/177

Last Slide

Some interesting open problems:

- Efficiency bounds for WCF.
- [Cleve 86] in quantum setting.
- Improve OT impossibility bounds.
- Q/C bounds for fair (non-aborting) coin flip.
- Improve OT protocols: many bit-OT instead of one string-OT.

Thanks.