Quantum Oblivious Transfer from One-way Functions


ALEX GRILO


HUIJIA LIN

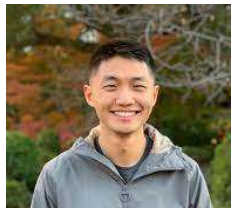

JAMES BARTUSEK


ANDREA COLADANGELO

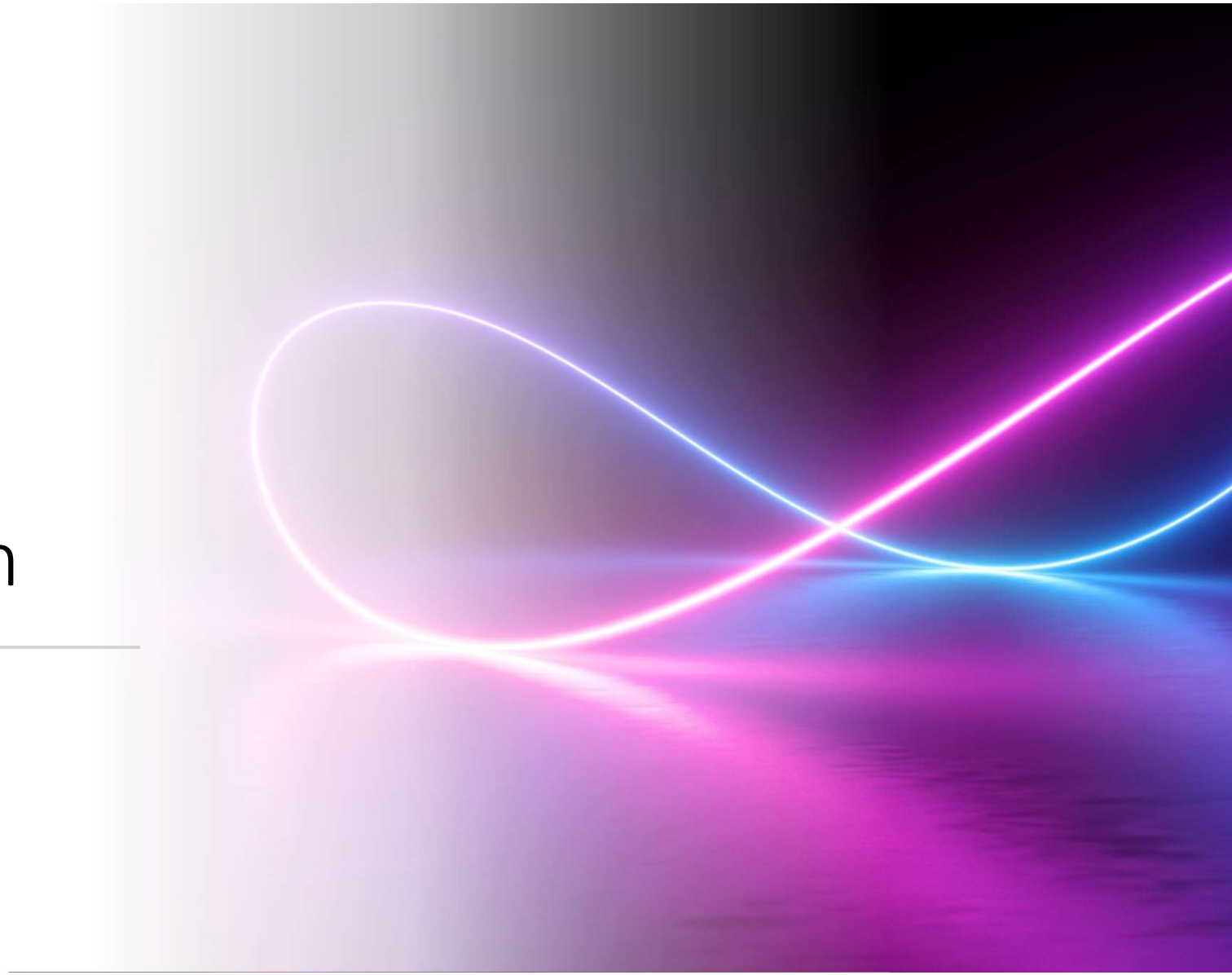

FANG SONG


VINOD VAIKUNTANATHAN

DAKSHITA KHURANA


FERMI MA

Introduction



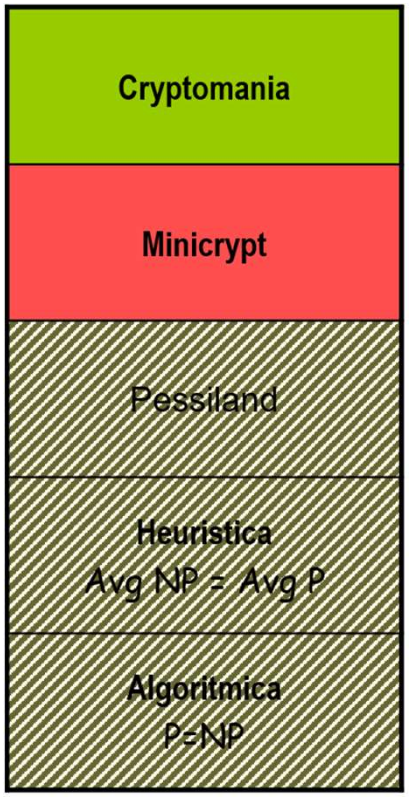
Impagliazzo's Five Worlds

- 5 possibilities
  - based on different crypto-computational assumptions.

- The top two worlds:

  - **Minicrypt** – One Way Functions exist, some crypto possible (symmetric encryption, commitments, signatures…)

  - **Cryptomania** – Oblivious Transfer (OT) exists, *almost* anything imaginable is possible.



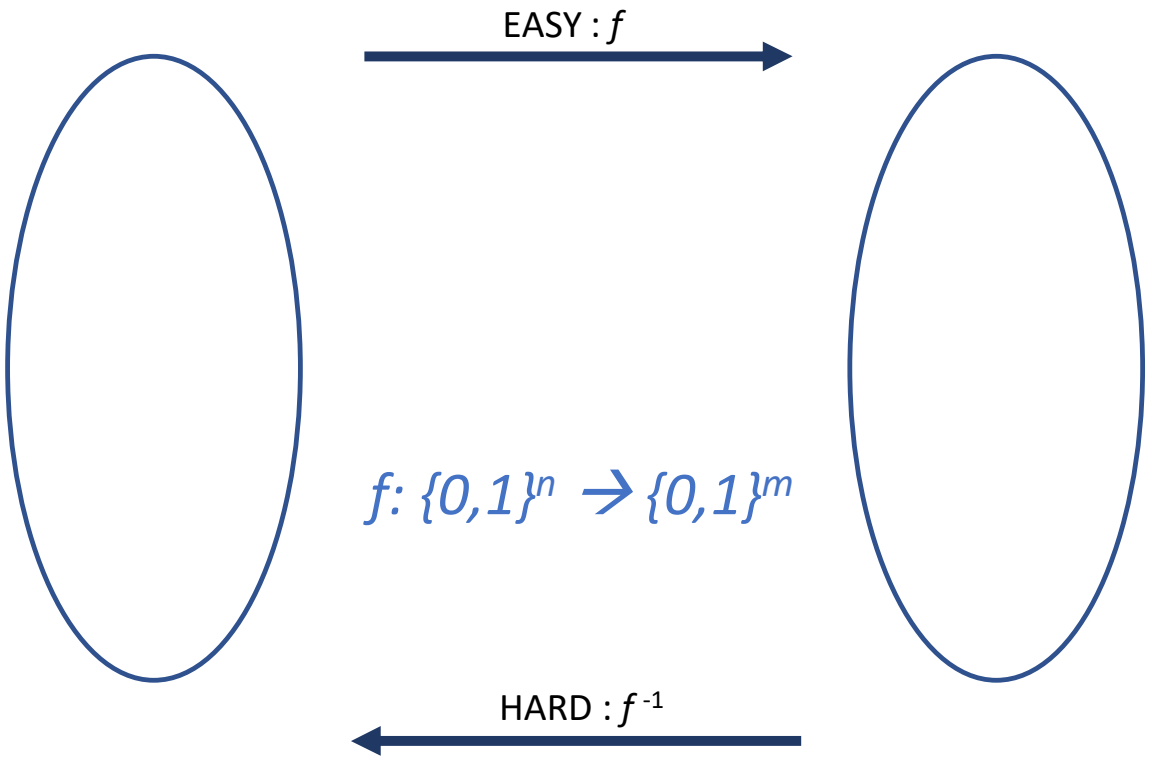
Slide courtesy: Moni Naor, 2006. Talk at Weizmann on *How to Prove that Minicrypt=Cryptomania (in the future)*

One-Way Functions

EASY

HARD

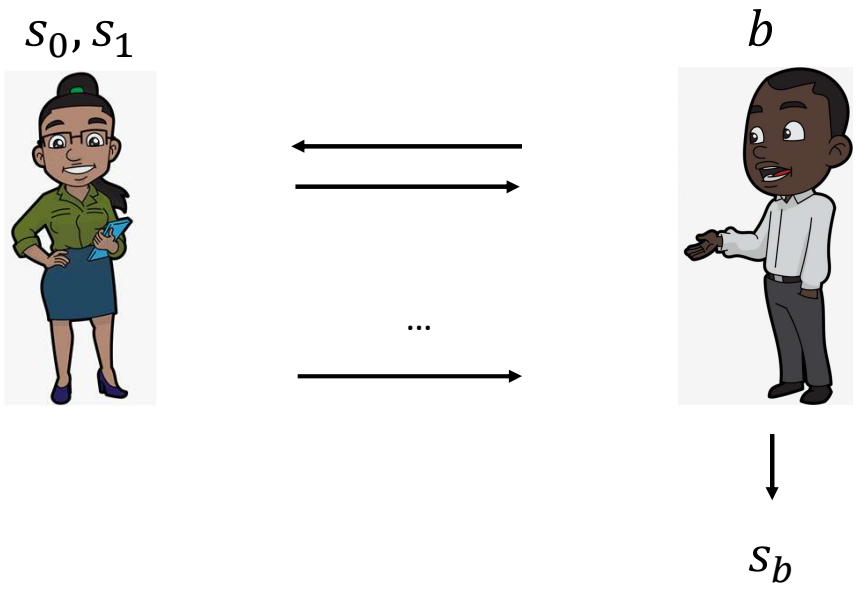
One-Way Functions



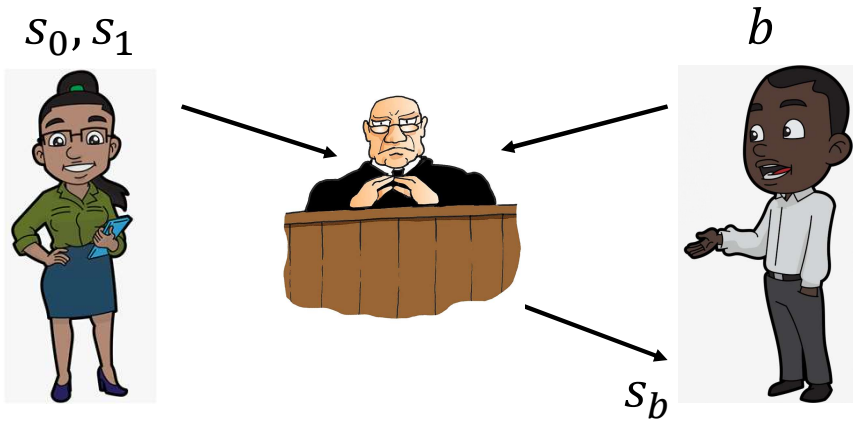
Sample $x \leftarrow \{0,1\}^n$, $y = f(x)$.

$\forall$ *polynomial-time A*, $Pr[\, A(y) \in f^{-1}(y) \,] = negl$.

Oblivious Transfer

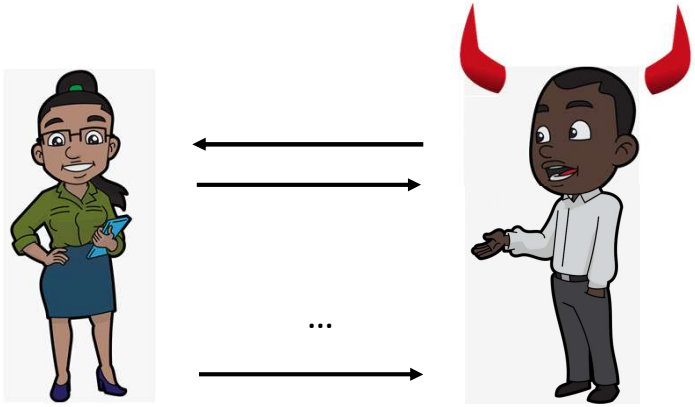


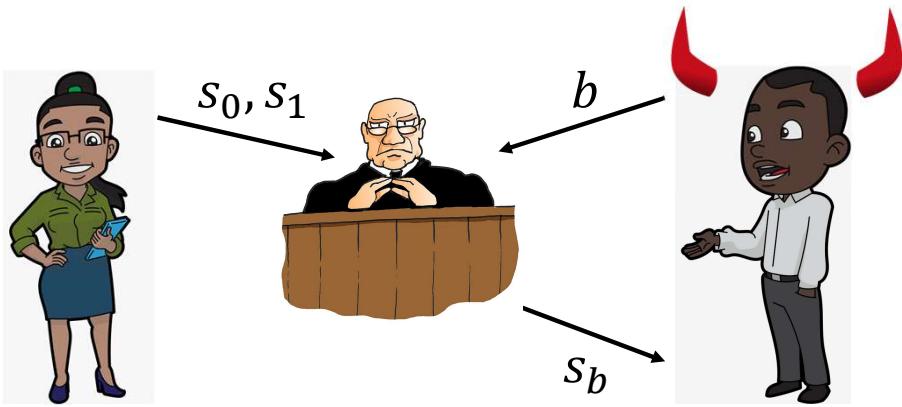
Oblivious Transfer: Security



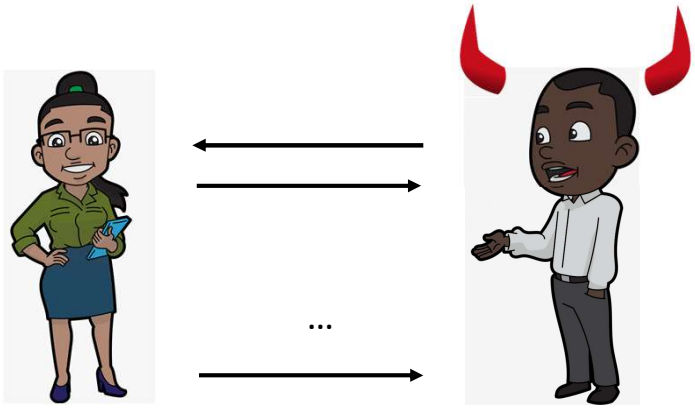
"learn no more than what they would if they were interacting with a trusted third party."

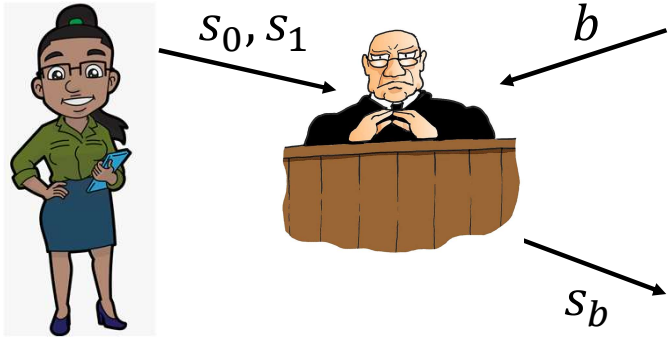
Oblivious Transfer: Security against a malicious Receiver B

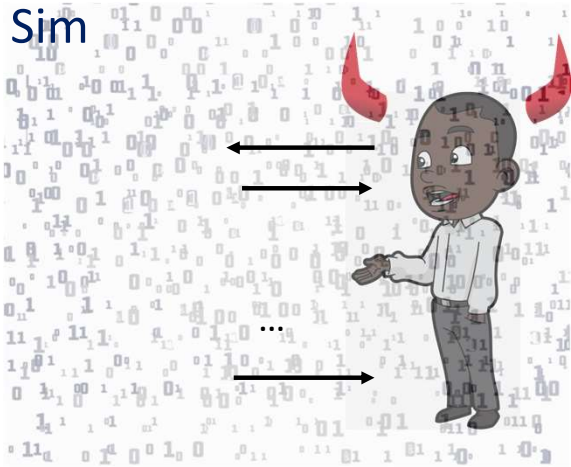




Oblivious Transfer: Security against a malicious Receiver B

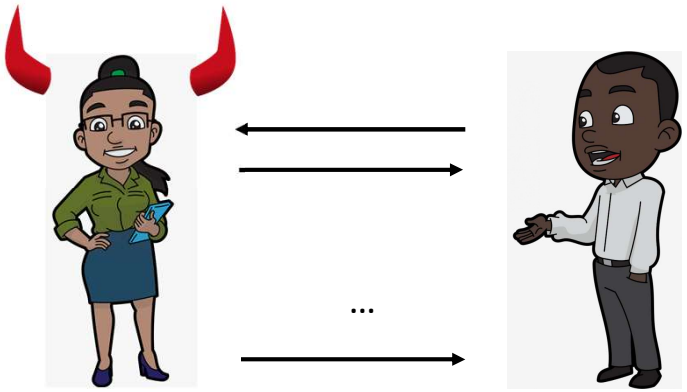


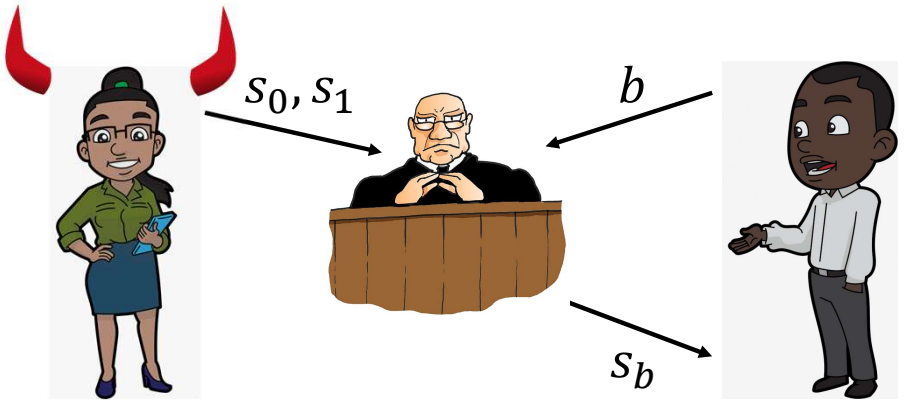




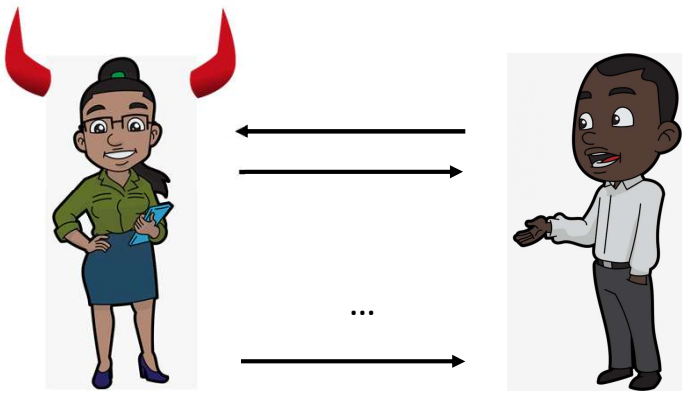
Sim must extract B's implicit input b without knowing A's input s_0, s_1

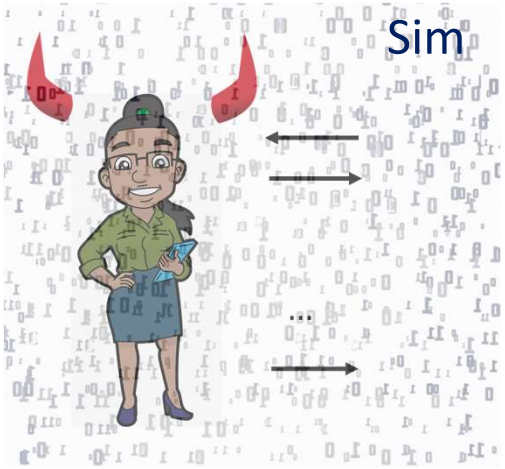
Oblivious Transfer: Security against a malicious Sender A

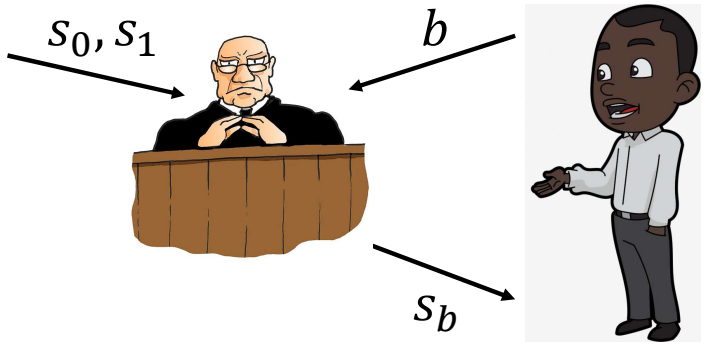




Oblivious Transfer: Security against a malicious Sender A

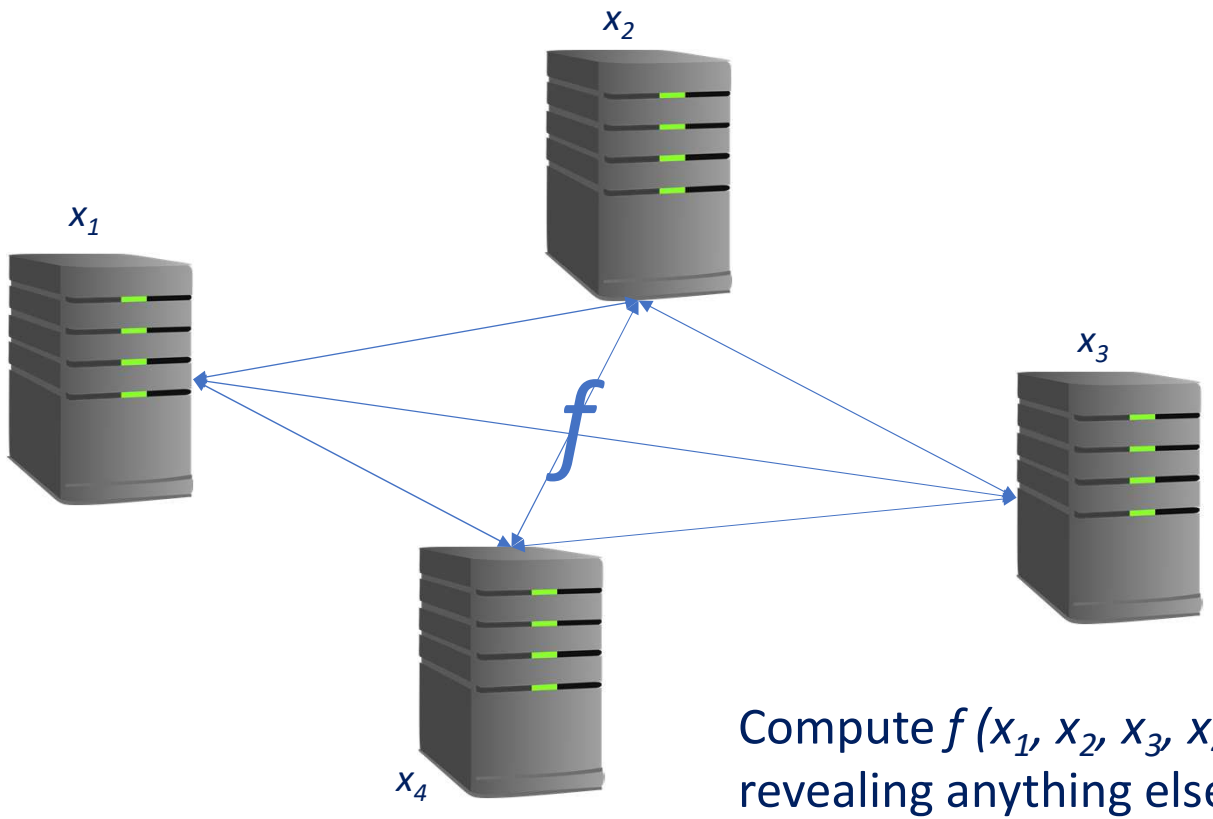






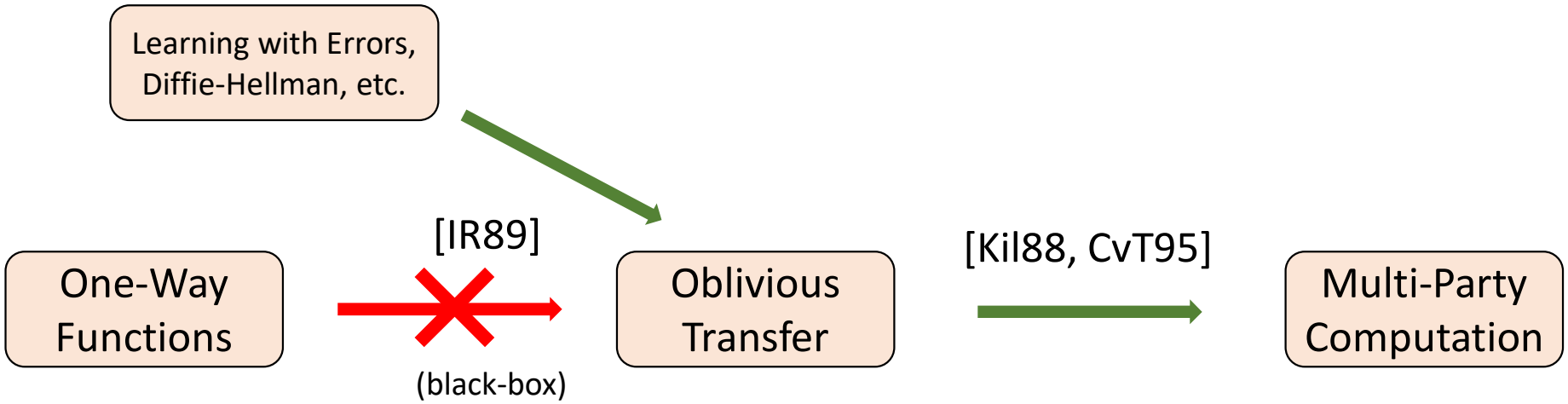
Sim must extract A's implicit inputs s_0, s_1 without knowing B's input b

Secure Multi-Party Computation

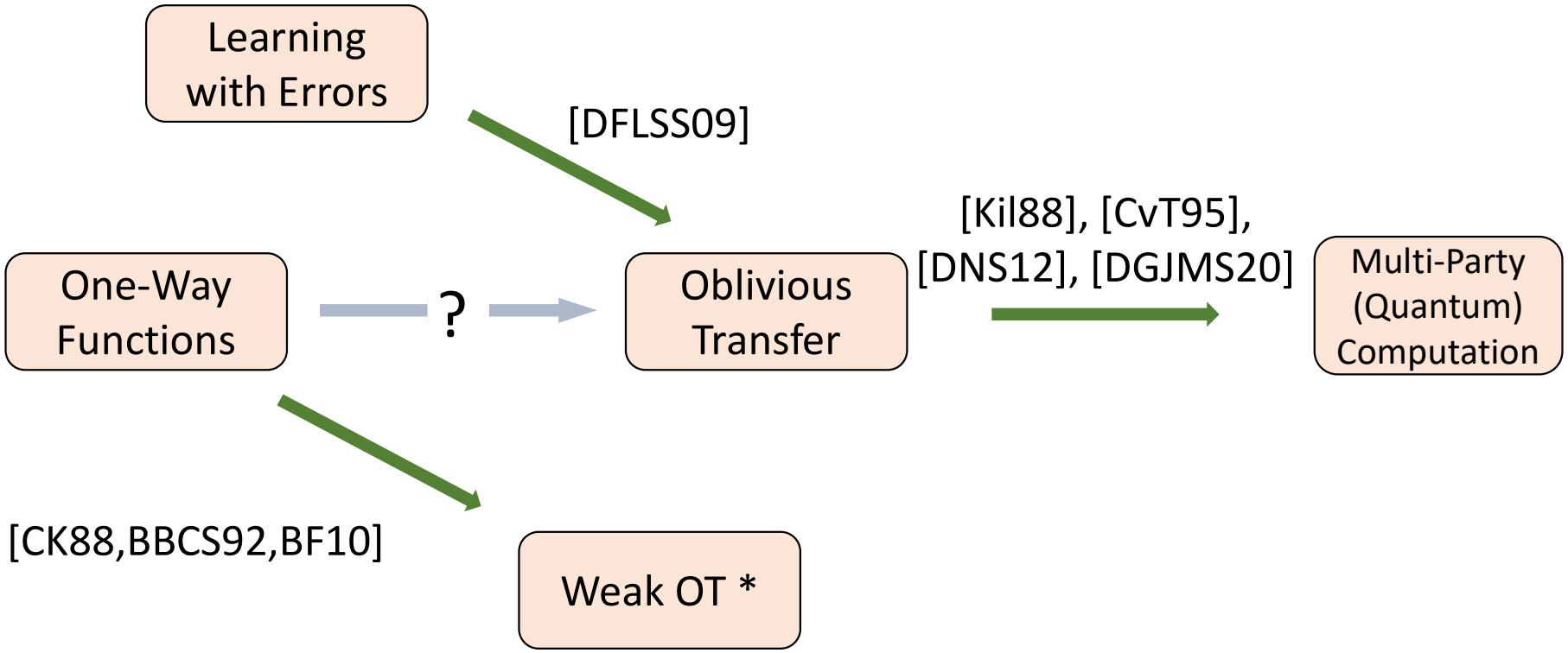


Compute $f(x_1, x_2, x_3, x_4)$ without revealing anything else about x_1, x_2, x_3, x_4

In a Classical World

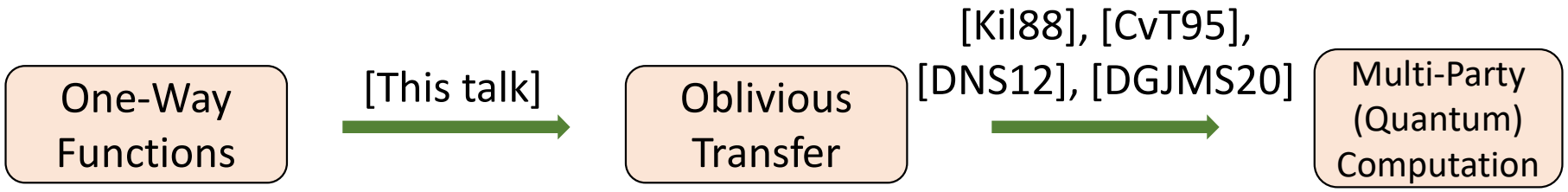


In a Quantum World

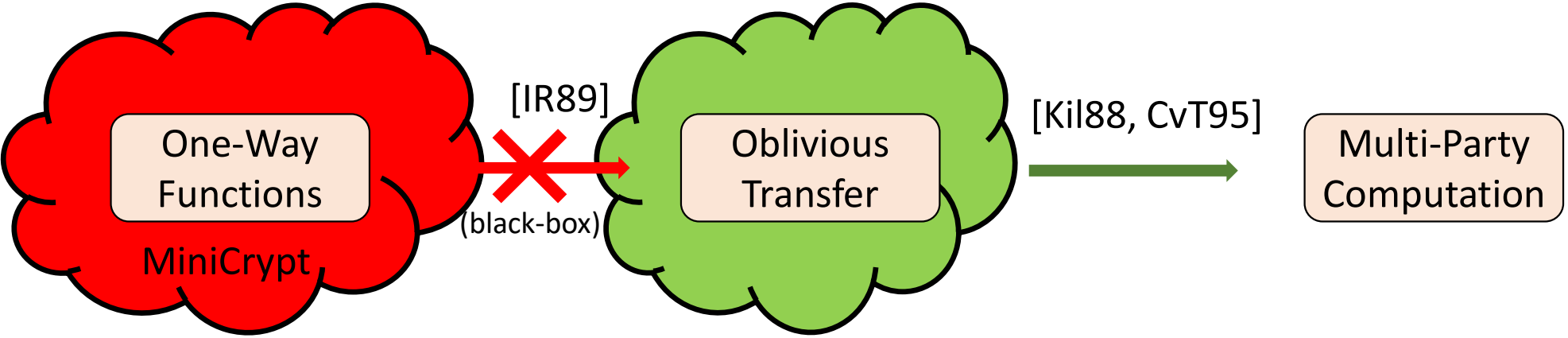


* Not known to imply MPC

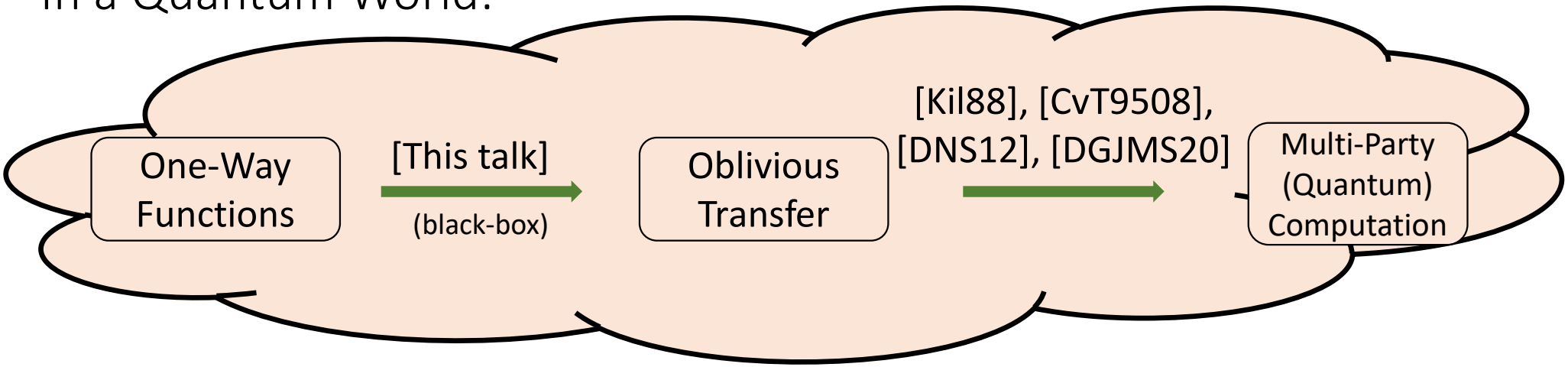
In a Quantum World



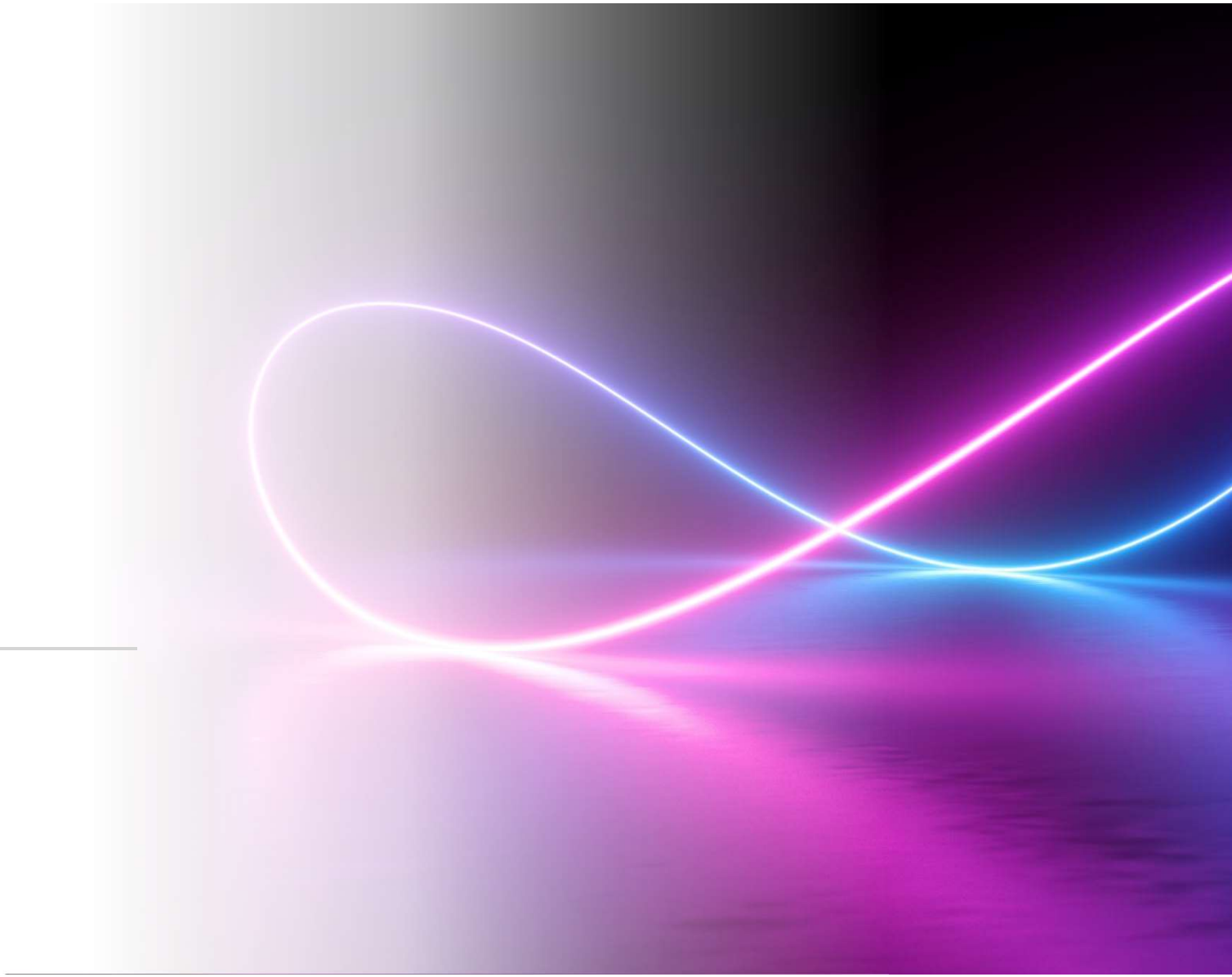
In a Classical World:



In a Quantum World:

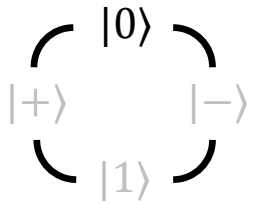


Techniques

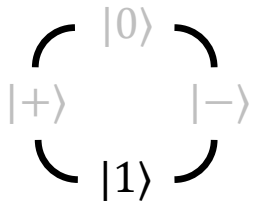


Quantum Mechanics

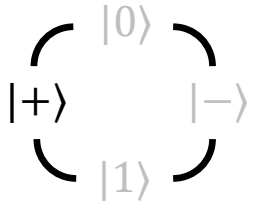
- BB84 states



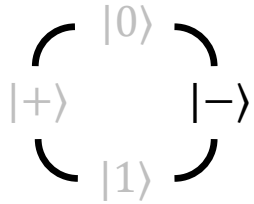
Basis θ: ↕
Bit x: 0



Basis θ: ↕
Bit x: 1



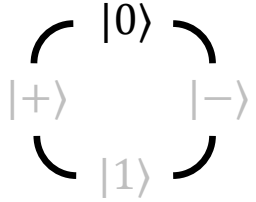
Basis θ: ↔
Bit x: 0



Basis θ: ↔
Bit x: 1

Quantum Mechanics

- BB84 states



Basis θ:↔
Bit x: 0 w.p. ½, 1 w.p. ½

Given random BB84 state (θ, x), measure in basis θ':

- If $\theta' = \theta$: observe x
- If $\theta' \neq \theta$: observe random bit

BB84 states + crypto
= erasure channel

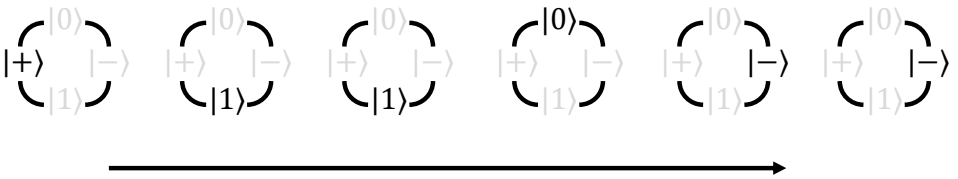
The [CK88, BBCS92] OT template

- Step 1: Establish an erasure channel

$\underline{S(s_0, s_1)}$

Sample bases $\theta = \leftrightarrow\updownarrow\updownarrow\updownarrow\leftrightarrow\leftrightarrow$

Sample bits $x = 011011$



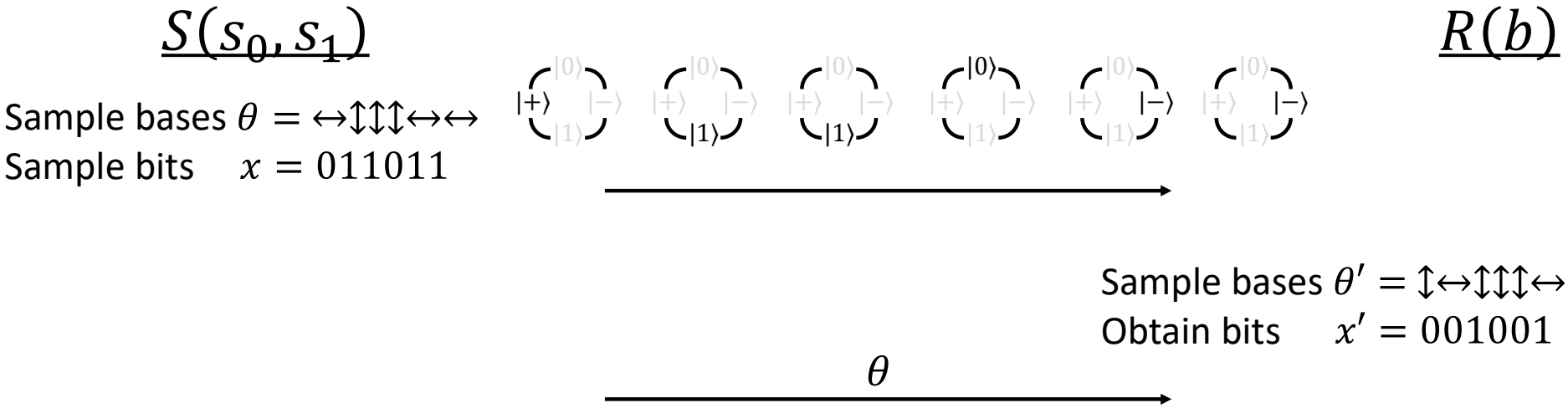
$\underline{R(b)}$

Sample bases $\theta' = \updownarrow\leftrightarrow\updownarrow\updownarrow\updownarrow\leftrightarrow$

Obtain bits $x' = 001001$

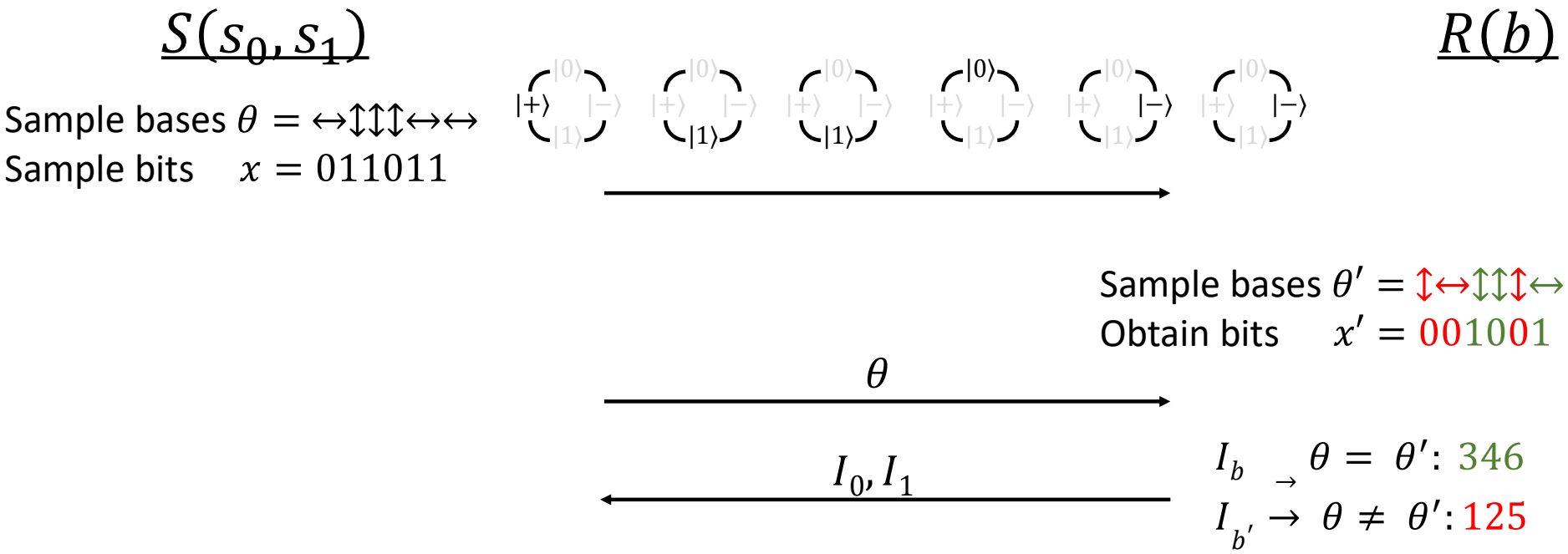
The [CK88, BBCS92] OT template

- Step 1: Establish an erasure channel



The [CK88, BBCS92] OT template

- Step 1: Establish an erasure channel

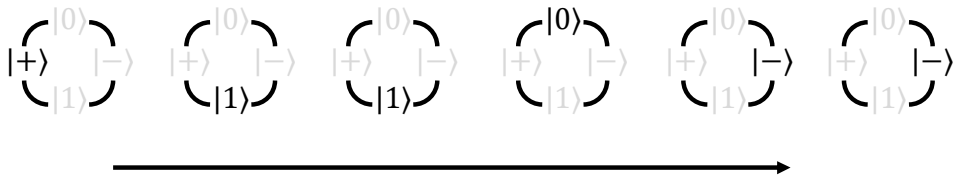


The [CK88, BBCS92] OT template

$\underline{S(s_0, s_1)}$

Sample bases $\theta = \leftrightarrow\updownarrow\updownarrow\updownarrow\leftrightarrow\leftrightarrow$

Sample bits $x = 011011$



$\underline{R(b)}$

Sample bases $\theta' = \updownarrow\leftrightarrow\updownarrow\updownarrow\updownarrow\leftrightarrow$

Obtain bits $x' = 001001$

θ

I_0, I_1

$I_b \rightarrow \theta = \theta'$: 346

$I_{b'} \rightarrow \theta \neq \theta'$: 125

$x^{(0)} = 101$

$x^{(1)} = 000$

$z_0 = \mathrm{Enc}_{x^{(0)}}(s_0),\ z_1 = \mathrm{Enc}_{x^{(1)}}(s_1)$

$s_b = \mathrm{Dec}_{x^{(b)}}(z_b)$

The [CK88, BBCS92] OT template: Malicious R

$\underline{S(s_0, s_1)}$

$\underline{R(b)}$

Sample bases $\theta = \leftrightarrow\updownarrow\updownarrow\leftrightarrow\leftrightarrow$

Sample bits $x = 011011$

θ

Obtain values $x' = x$

by measuring in basis $\theta' = \theta$

I_0, I_1

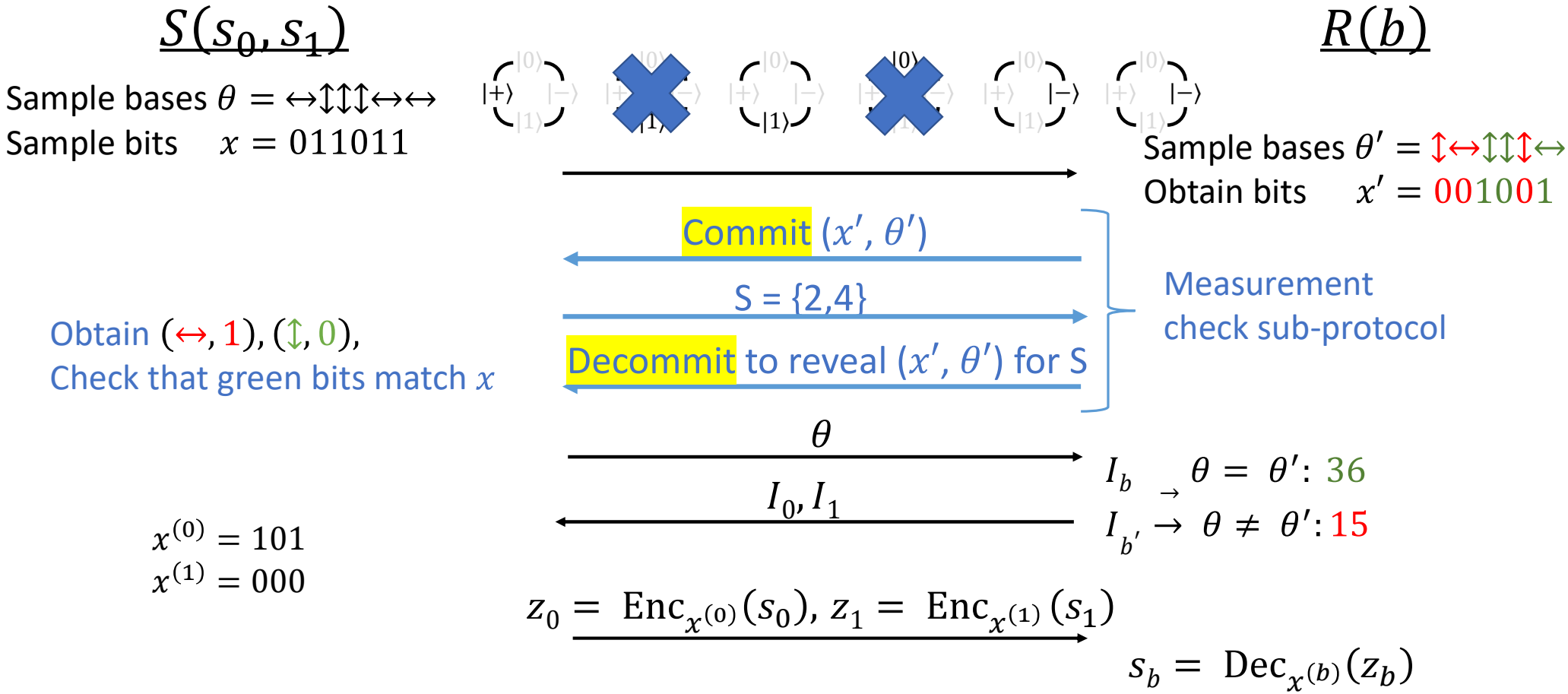
$x^{(0)} = 101$

$x^{(1)} = 000$

$z_0 = \mathrm{Enc}_{x^{(0)}}(s_0),\ z_1 = \mathrm{Enc}_{x^{(1)}}(s_1)$

Recover both s_0, s_1

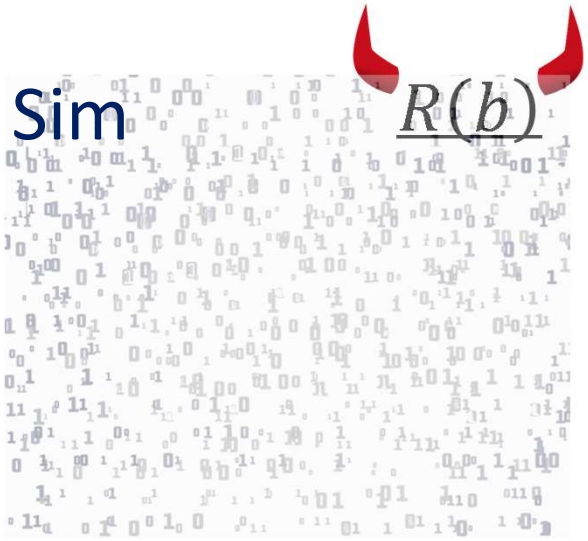
Fix: The Measurement-Check Subprotocol



[DFLSS09]: Simulation security of OT follows from using commitment with certain properties:

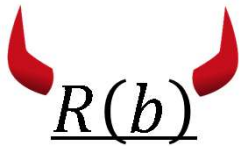
- **Extractability** → security against malicious receiver

Security against Malicious R



Sim must extract R's implicit input *b*

Security against Malicious R

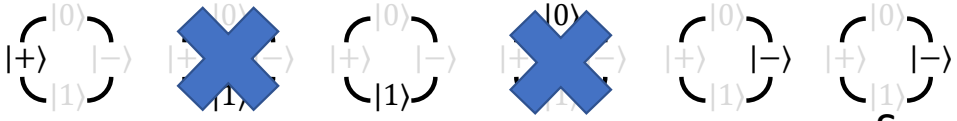


$R(b)$

Sim

Sample bases $\theta = \leftrightarrow\updownarrow\updownarrow\updownarrow\leftrightarrow\leftrightarrow$

Sample bits $x = 011011$



Sample bases $\theta' = \updownarrow\leftrightarrow\updownarrow\updownarrow\updownarrow\leftrightarrow$

Obtain bits $x' = 001001$

Extract

(θ', x')

Commit (x', θ')

$S = \{2,4\}$

Decommit to reveal (x', θ') for S

Measurement check sub-protocol

Obtain $(\leftrightarrow, 1), (\updownarrow, 0)$,

Check that green bits match x

θ

I_0, I_1

$I_b \rightarrow \theta = \theta'$: 36

$I_{b'} \rightarrow \theta \neq \theta'$: 15

$x^{(0)} = 101$

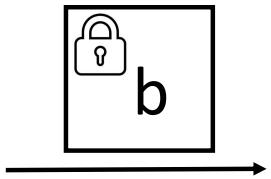
$x^{(1)} = 000$

$z_0 = \mathrm{Enc}_{x^{(0)}}(s_0),\ z_1 = \mathrm{Enc}_{x^{(1)}}(s_1)$

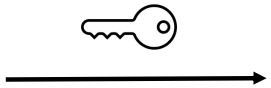
$s_b = \mathrm{Dec}_{x^{(b)}}(z_b)$

Extractable (Bit) Commitment

$\mathrm{C}(b)$ R



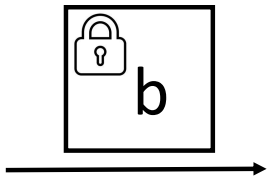
Hiding: R does not learn b



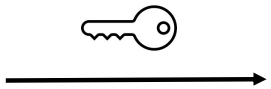
Binding: C can only make box open to b

Extractable (Bit) Commitment

$\mathrm{C}(b)$ Sim



Extraction: Sim can recover b

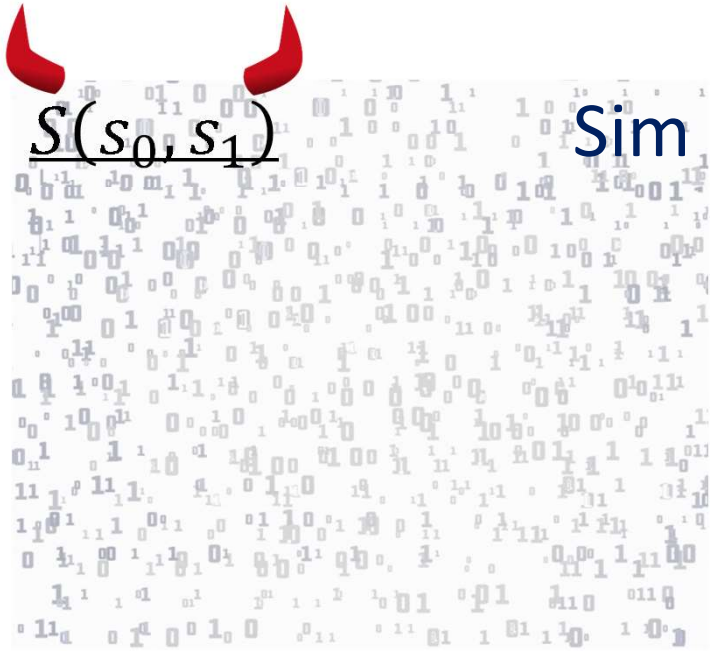


C can only make box open to b

[DFLSS09]: Simulation security of OT follows from using commitment with certain properties:

- **Equivocality** → security against malicious sender

Security against Malicious S



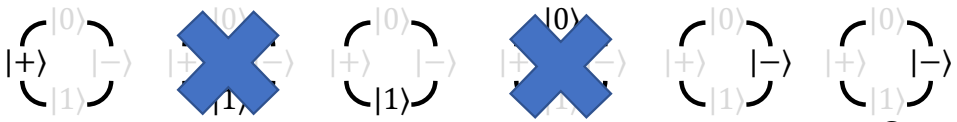
Sim must extract S's implicit inputs

Security against Malicious S

$\underline{S(s_0, s_1)}$

Sample bases $\theta = \leftrightarrow\updownarrow\updownarrow\updownarrow\leftrightarrow\leftrightarrow$

Sample bits $x = 011011$



$\underline{Sim}$

~~Sample bases $\theta' = \updownarrow\leftrightarrow\updownarrow\updownarrow\updownarrow\leftrightarrow$~~

~~Obtain bits $x' = 001001$~~

Commit (x', θ')

S = {2,4}

Decommit to (x', θ') for S

Measure *only in* S

Obtain $(\leftrightarrow, 1), (\updownarrow, 0)$,

Check that green bits match x

θ

I_0, I_1

$I_b \rightarrow \theta = \theta'$: 36

$I_{b'} \rightarrow \theta \neq \theta'$: 15

$x^{(0)} = 101$

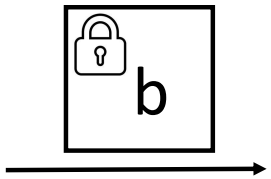
$x^{(1)} = 000$

$z_0 = \mathrm{Enc}_{x^{(0)}}(s_0),\ z_1 = \mathrm{Enc}_{x^{(1)}}(s_1)$

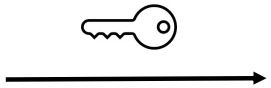
$s_b = \mathrm{Dec}_{x^{(b)}}(z_b)$

Equivocal (Bit) Commitment

$\mathrm{C}(b)$ R



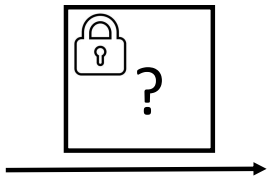
Hiding: R does not learn b



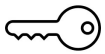
Binding: C can only make box open to b

Equivocal (Bit) Commitment

Sim R



b



Equivocality: Sim can make box open to b

Goal: (quantum-secure) Extractable and Equivocal bit commitment from one-way functions

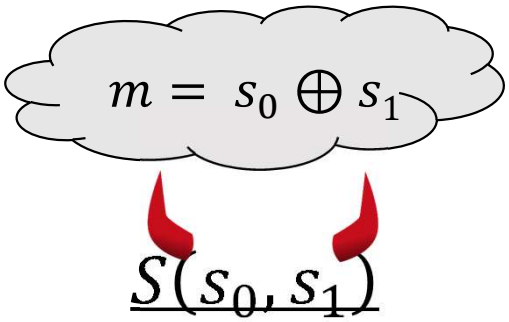
[BCKM21]	[GLSV21]
1. Black-box equivocality compiler 2. Extractable commitment from equivocal commitment and quantum communication	1. Equivocal commitment from Naor's commitment and zero-knowledge 2. Unbounded-simulator OT from equivocal commitment 3. Extractable and equivocal commitment from unbounded-simulator OT and quantum communication

Goal:

Extractable and Equivocal bit commitment from one-way functions

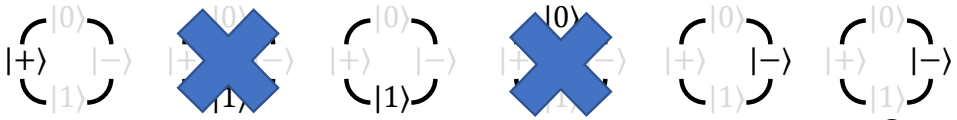
Key Obstacle: Extractable (bit) Commitment

Extractable Bit Commitments: Approach 1 [BCKM]



Sample bases $\theta = \leftrightarrow\updownarrow\updownarrow\updownarrow\leftrightarrow\leftrightarrow$

Sample bits $x = 011011$



Sim

~~Sample bases $\theta' = \updownarrow\leftrightarrow\updownarrow\updownarrow\updownarrow\leftrightarrow$~~

~~Obtain bits $x' = 001001$~~

Commit (x', θ')

S = {2,4}

Decommit to (x', θ') for S

Measure *only in* S

Obtain $(\leftrightarrow, 1), (\updownarrow, 0)$,

Check that green bits match x

θ

I_b → $\theta = \theta'$: 36

I_0, I_1

$I_{b'}$ → $\theta \neq \theta'$: 15

$x^{(0)} = 101$

$x^{(1)} = 000$

$z_0 = \mathrm{Enc}_{x^{(0)}}(s_0),\ z_1 = \mathrm{Enc}_{x^{(1)}}(s_1)$

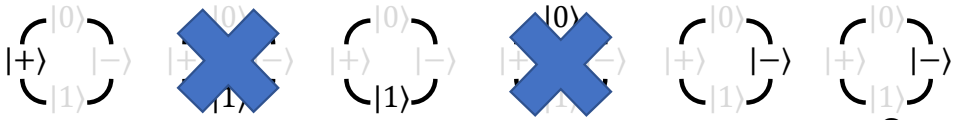
$s_b = \mathrm{Dec}_{x^{(b)}}(z_b)$

Extractable (Bit) Commitments from Equivocal (Bit) Commitments

$\underline{C(m)}$

Sample bases $\theta = \leftrightarrow\updownarrow\updownarrow\updownarrow\leftrightarrow\leftrightarrow$

Sample bits $x = 011011$



$\underline{R}$

Sample bases $\theta' = \updownarrow\leftrightarrow\updownarrow\updownarrow\updownarrow\leftrightarrow$

Obtain bits $x' = 001001$

Commit (x', θ')

S = {2,4}

Decommit to (x', θ') for S

Obtain $(\leftrightarrow, 1), (\updownarrow, 0)$,

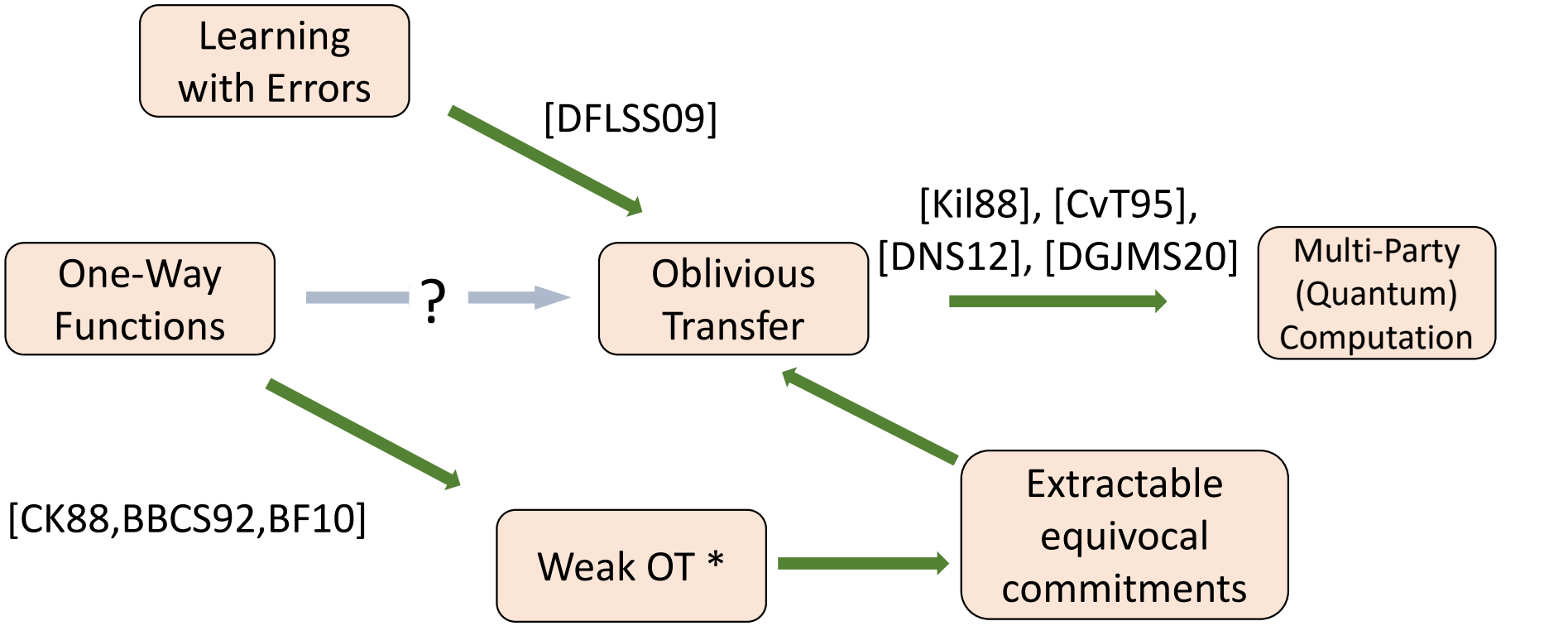
Check that green bits match x

$x^{(\mathrm{sk})} = (x_i)_{i \notin T}$

$\theta, \mathrm{Enc}_{x^{(\mathrm{sk})}}(m)$

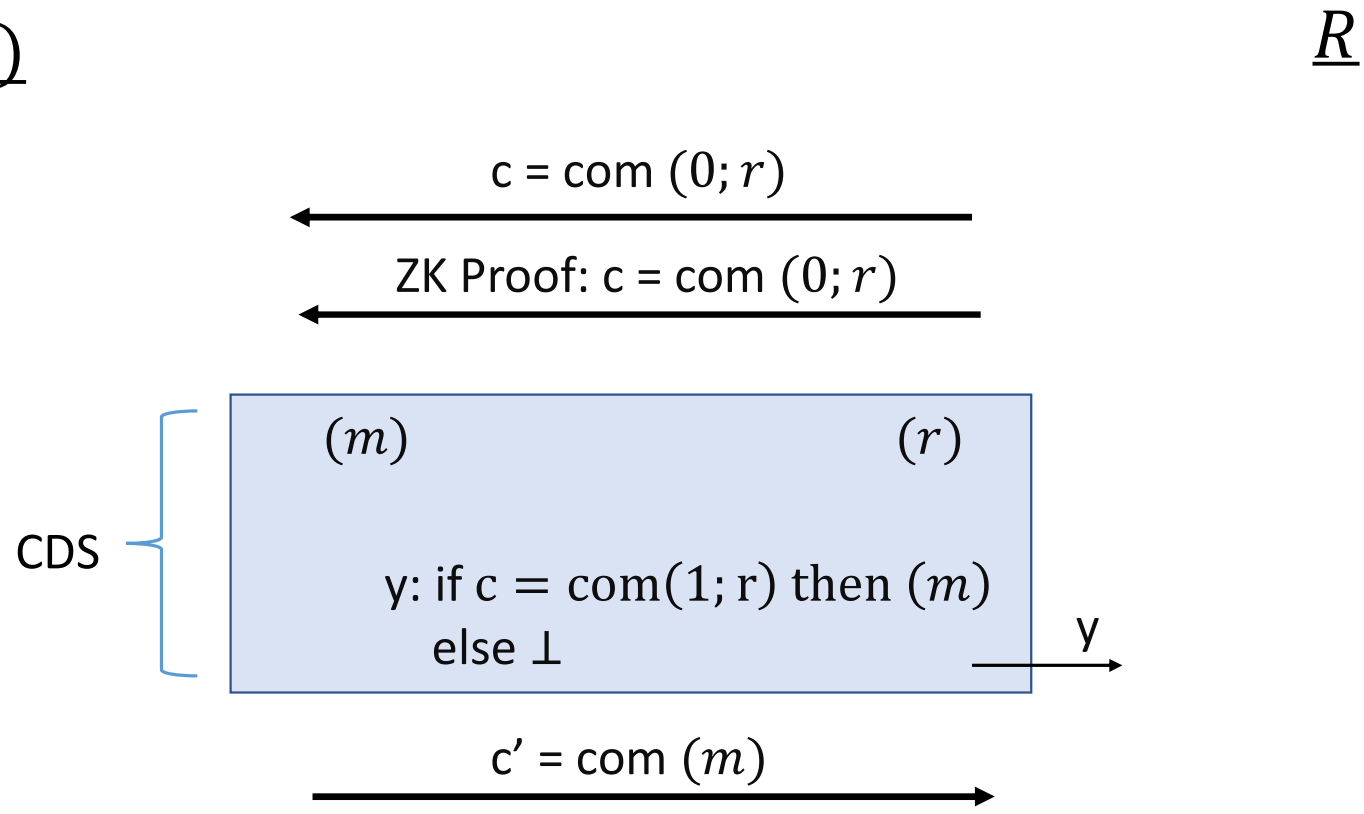
Extractable Bit Commitments: Approach 2 [GLSV]

In a Quantum World



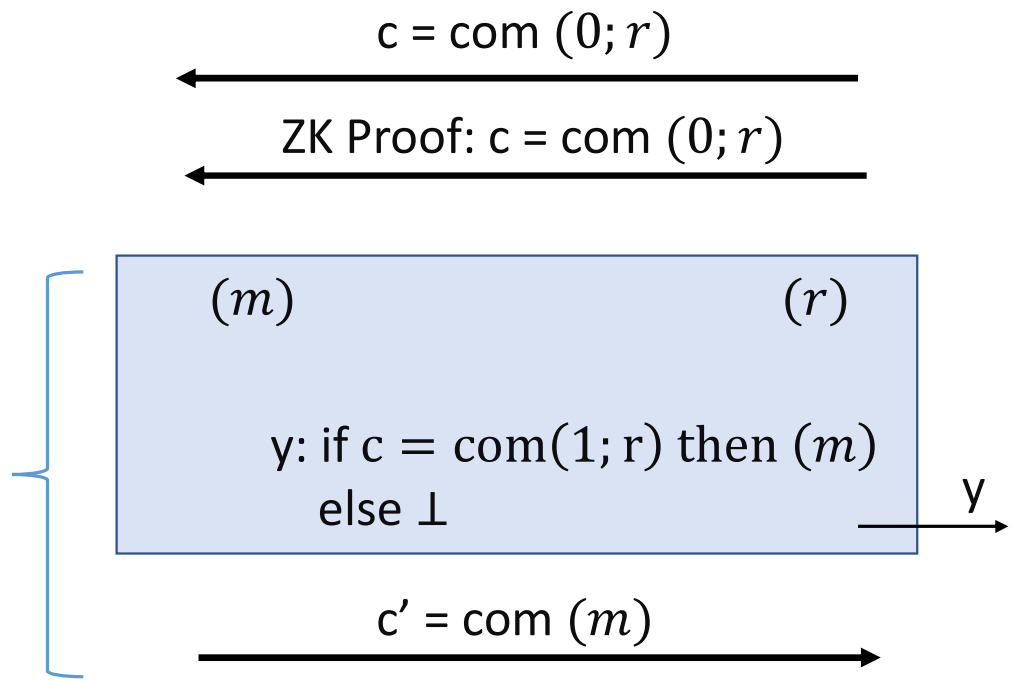
* Not known to imply MPC

Extractable (Bit) Commitments from Weak OT



Extractable (Bit) Commitments from Weak OT

$\underline{C(m)}$ $\underline{R}$



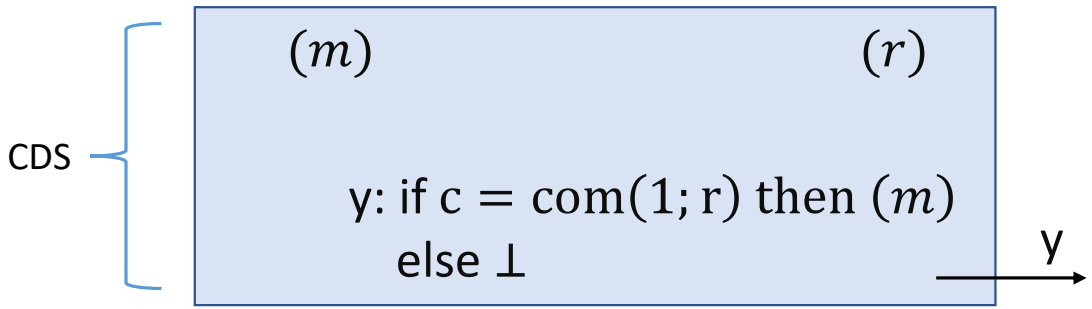
Verifiable CDS:

Can verify given the classical transcript that CDS outputs the right *m*

CDS from Weak OT

$\underline{C(m)}$

$\underline{R}$

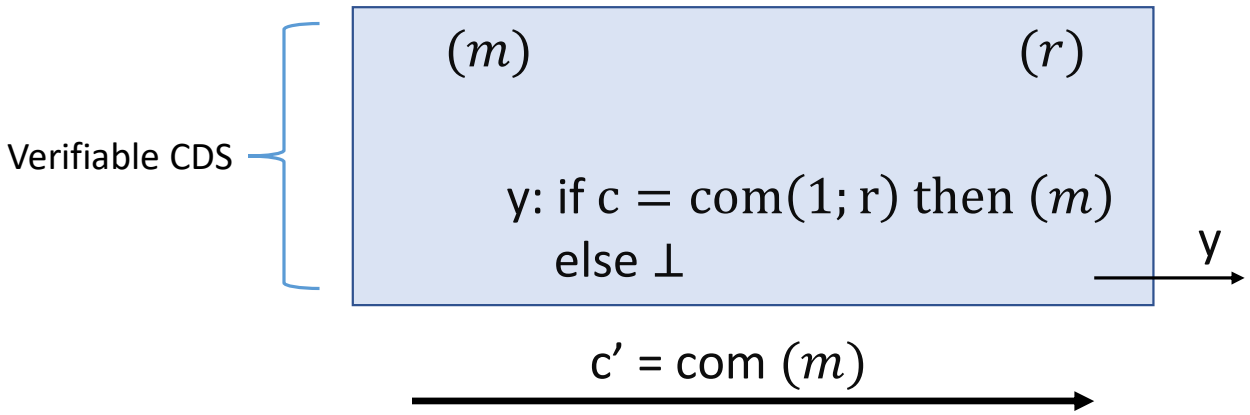


Garbled circuits + weak OT

Verifiable CDS from Weak OT

$\underline{C(m)}$

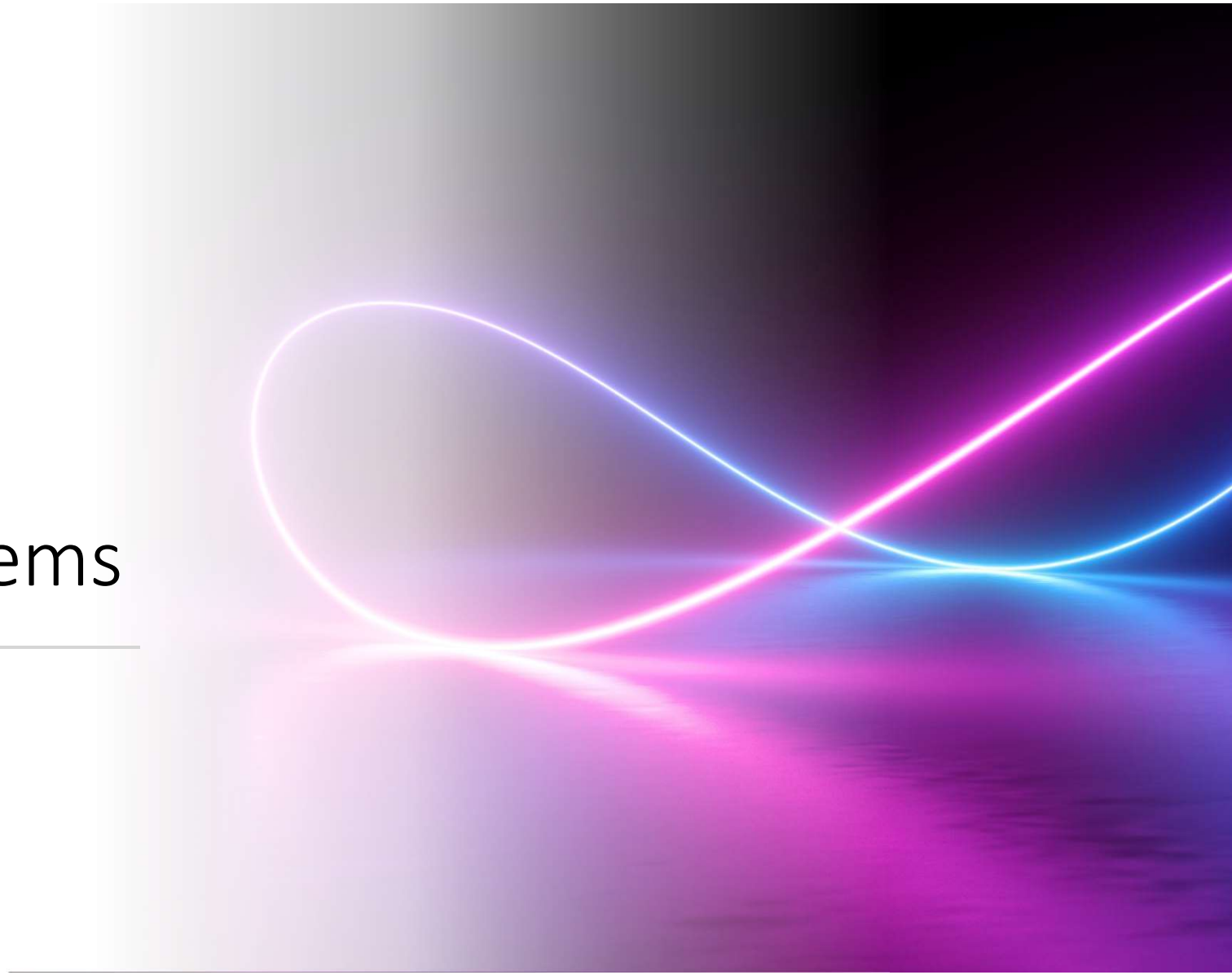
$\underline{R}$



Garbled circuits + weak OT

+ cut-and-choose + error correction

Open Problems



Open Problems

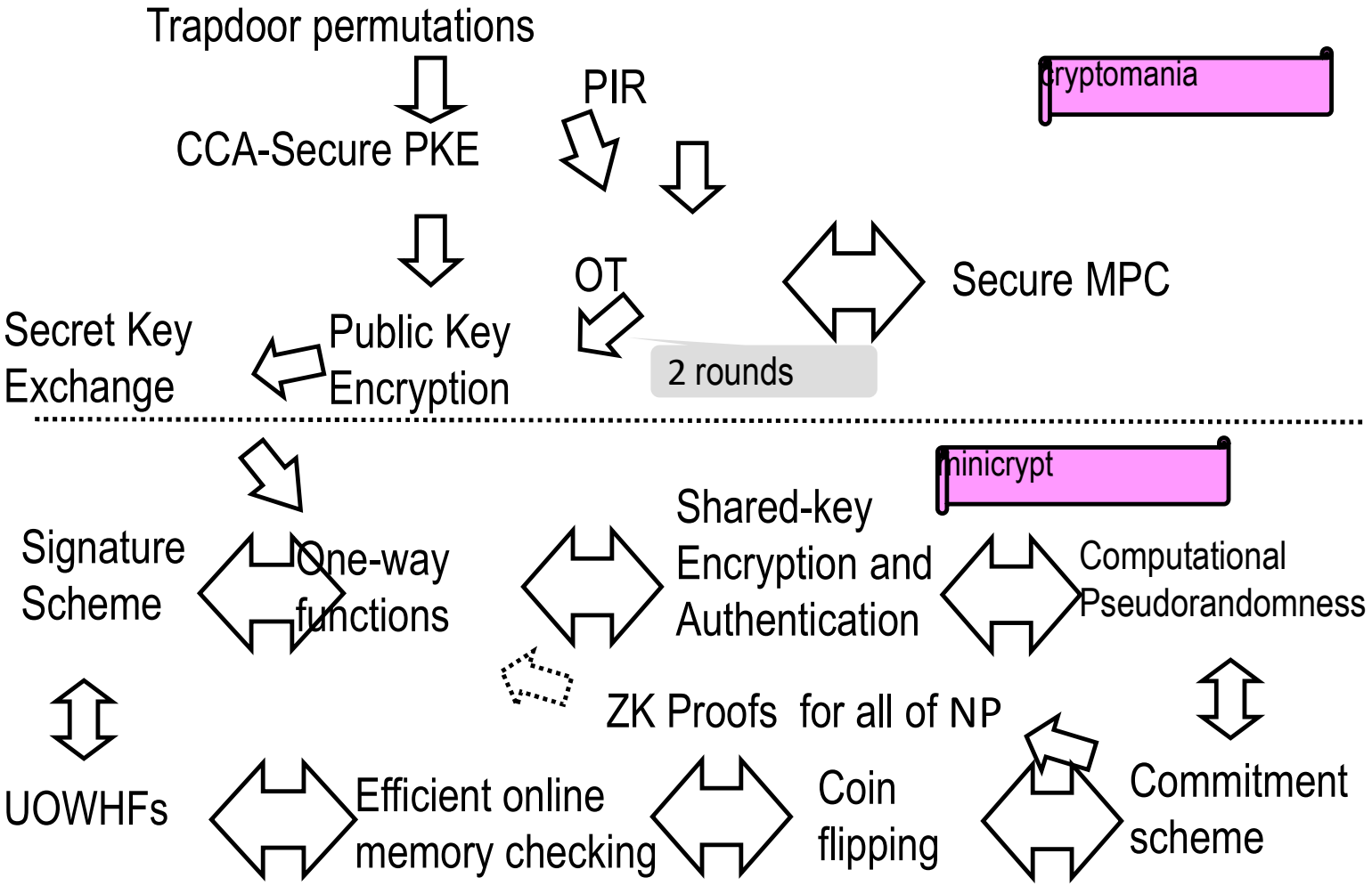
1. What does the landscape of cryptographic complexity look like in the presence of quantum communication?

2. Can cryptography with quantum communication be based on better complexity-theoretic foundations (e.g., $P \neq NP$)?

3. Which two-party functionalities are complete for secure computation with quantum communication?

4. Can we minimize the number of quantum resources/qubits consumed per OT while still only relying on one-way functions? Random Oracles?

A more refined view



Slide courtesy: Moni Naor, 2006. Talk at Weizmann on *How to Prove that Minicrypt=Cryptomania (in the future)*

Thank You