Secure Computation is in MiniQCrypt

Merge of:

Oblivious Transfer is in MiniQCrypt

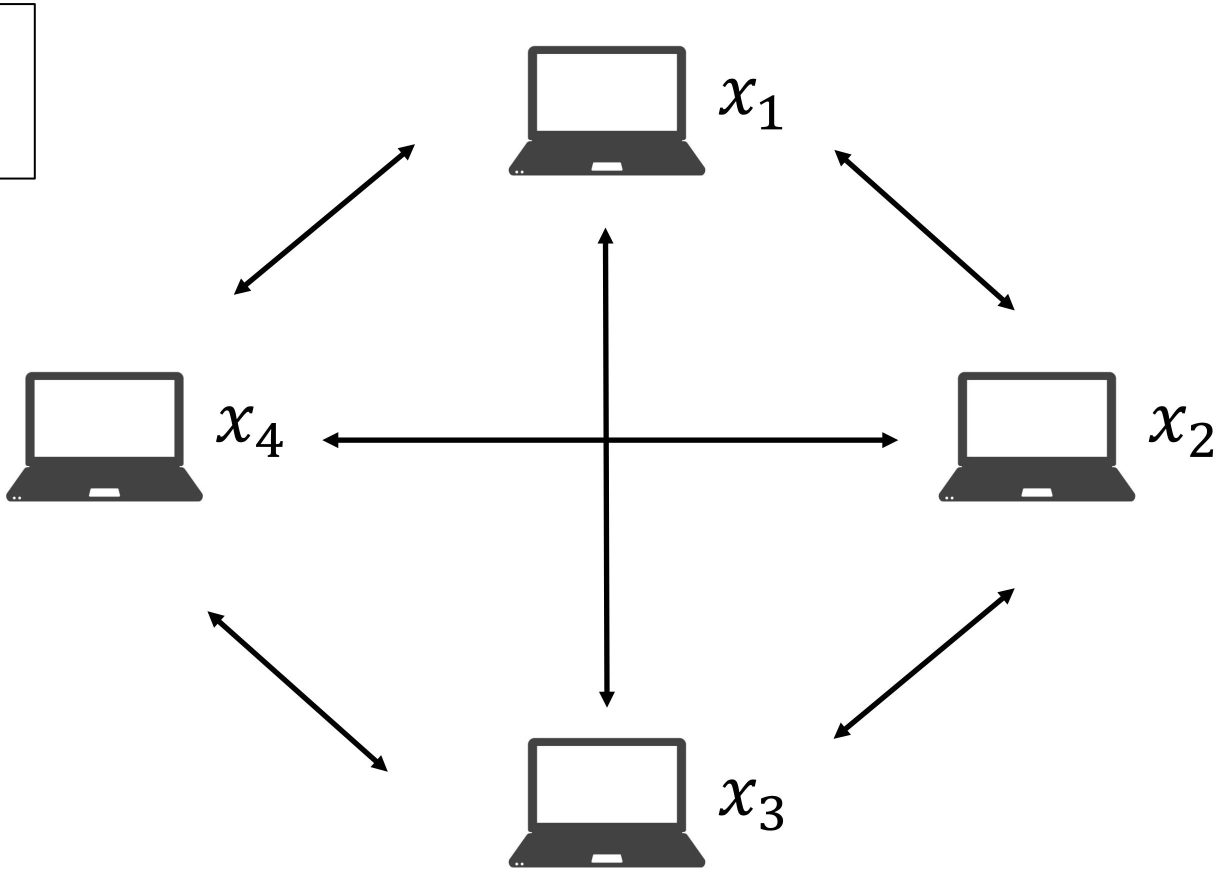
Alex Bredariol Grilo (LIP6, CNRS/Sorbonne Université)
Huijia Lin (University of Washington)
Fang Song (Portland State University)
Vinod Vaikuntanathan (MIT)

One-Way Functions Imply Secure Computation In a Quantum World

James Bartusek (UC Berkeley)
Andrea Coladangelo (UC Berkeley)
Dakshita Khurana (UIUC)
Fermi Ma (Princeton and NTT Research)

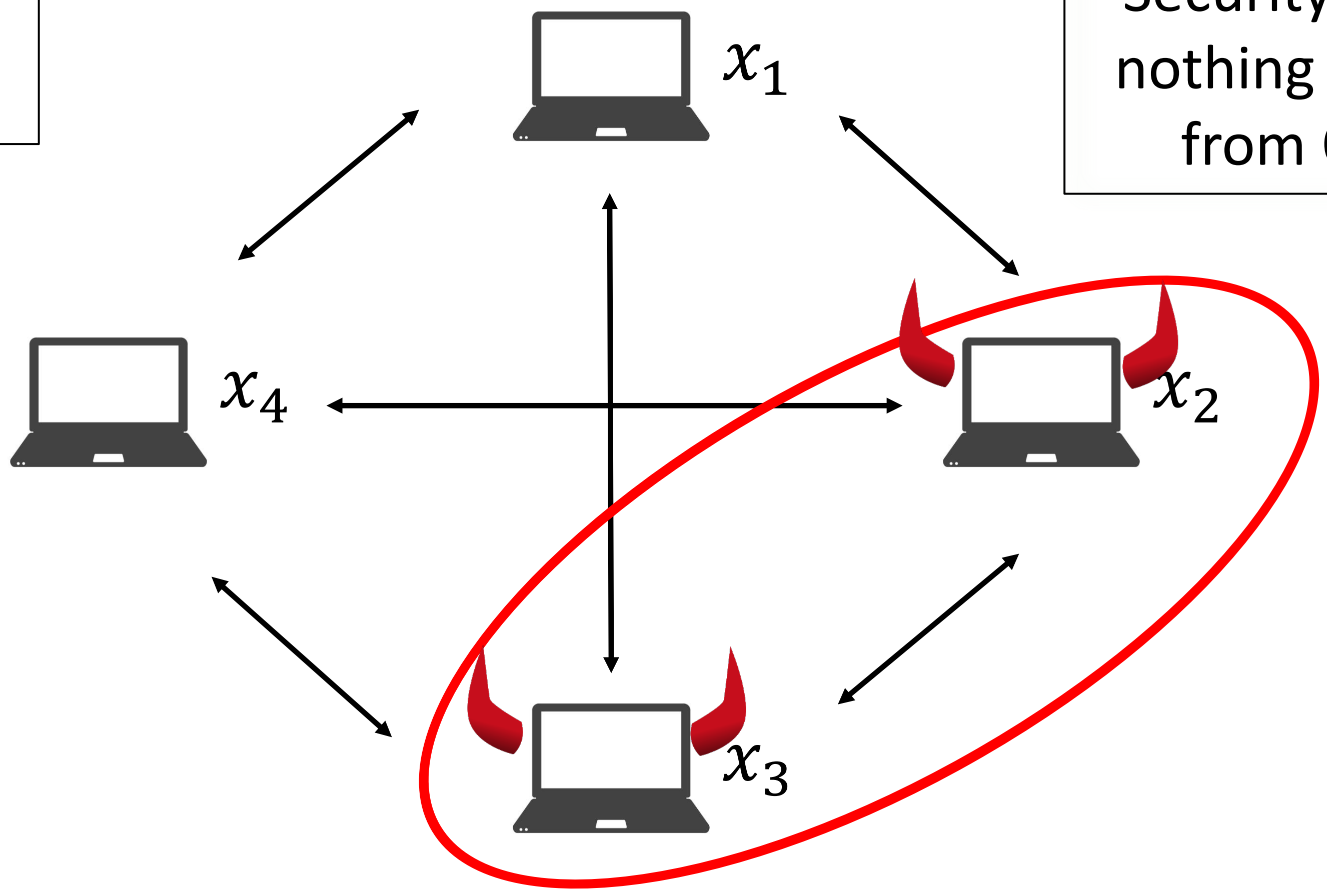
Secure Multi-Party Computation

Goal: Compute
$\mathrm{C}(x_1, x_2, x_3, x_4)$



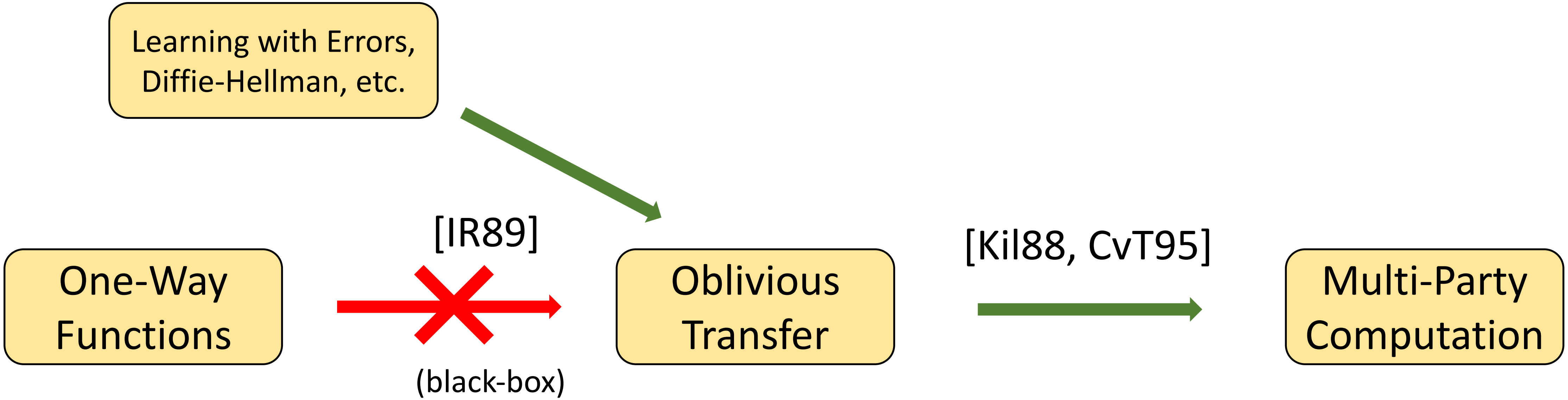
Secure Multi-Party Computation

Goal: Compute $C(x_1, x_2, x_3, x_4)$



Security: adversary learns nothing about x_1, x_4 apart from $C(x_1, x_2, x_3, x_4)$

In a Classical World



Learning with Errors, Diffie-Hellman, etc.

One-Way Functions

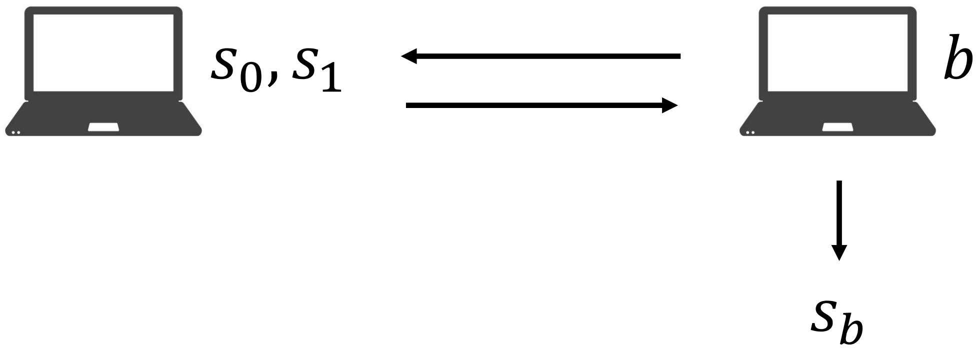
[IR89]

(black-box)

Oblivious Transfer

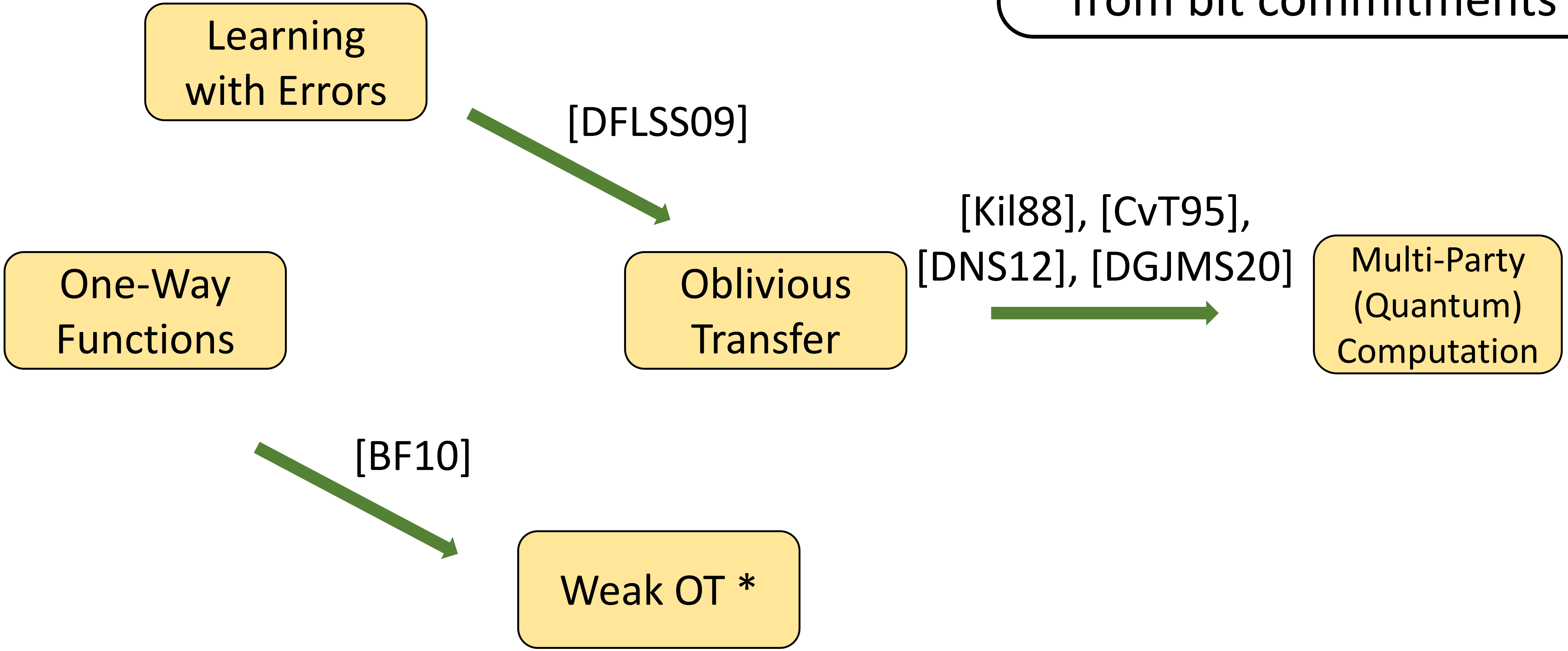
[Kil88, CvT95]

Multi-Party Computation



In a Quantum World

[CK88], [BBCS92]:
Template for building OT from bit commitments



Learning with Errors

[DFLSS09]

One-Way Functions

Oblivious Transfer

[Kil88], [CvT95], [DNS12], [DGJMS20]

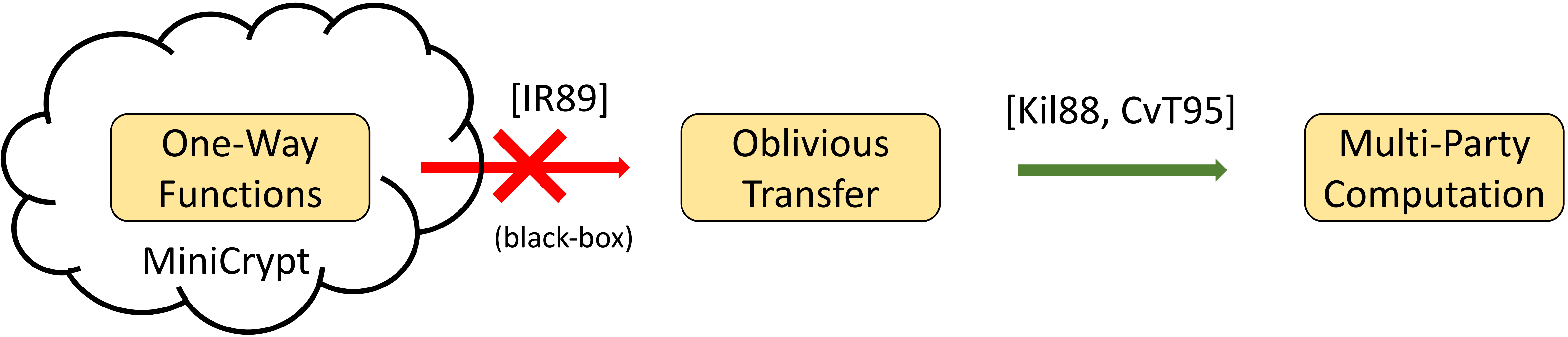
Multi-Party (Quantum) Computation

[BF10]

Weak OT *

* Not known to imply MPC

In a Classical World:



One-Way Functions

MiniCrypt

[IR89]

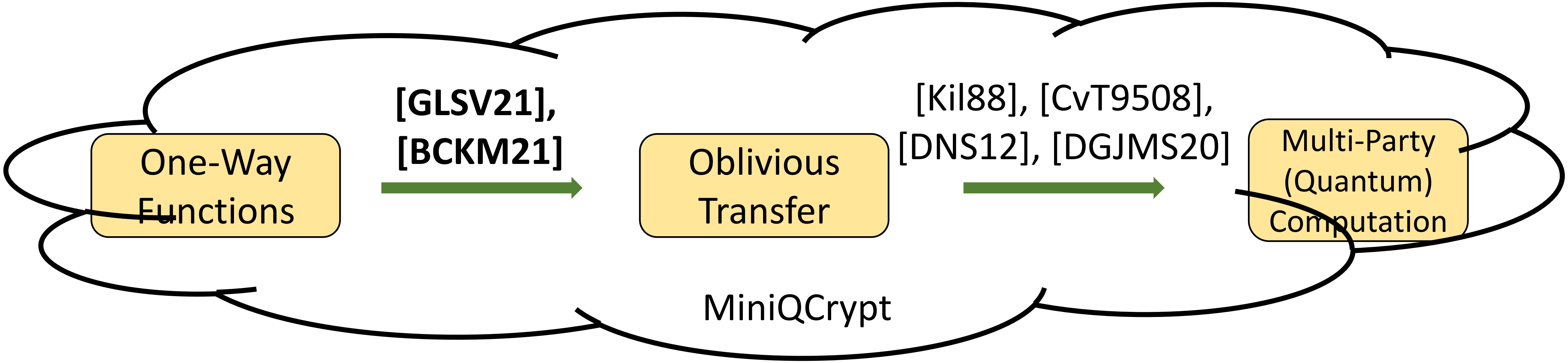
(black-box)

Oblivious Transfer

[Kil88, CvT95]

Multi-Party Computation

In a Quantum World:



One-Way Functions

[GLSV21], [BCKM21]

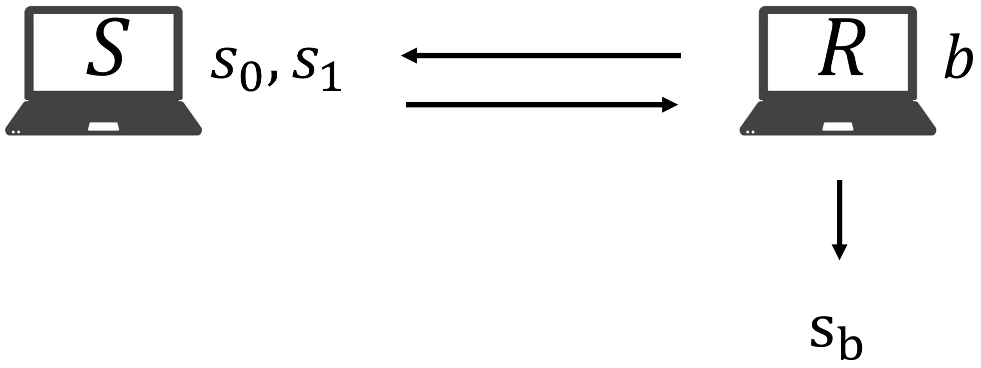
Oblivious Transfer

[Kil88], [CvT9508], [DNS12], [DGJMS20]

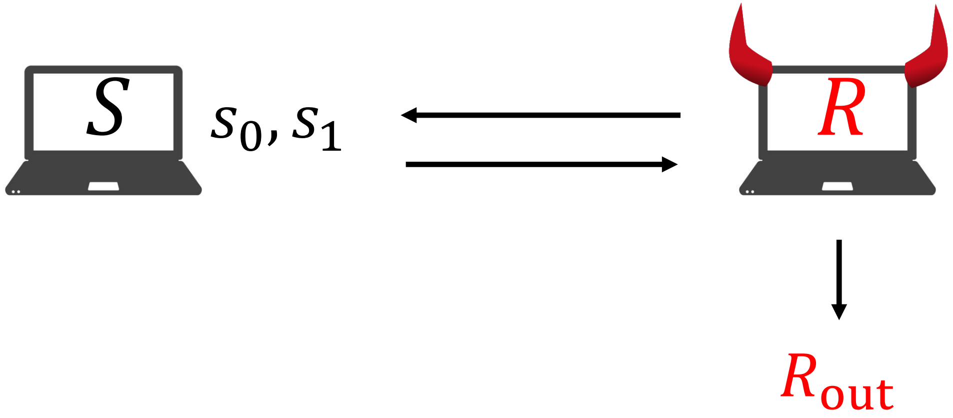
Multi-Party (Quantum) Computation

MiniQCrypt

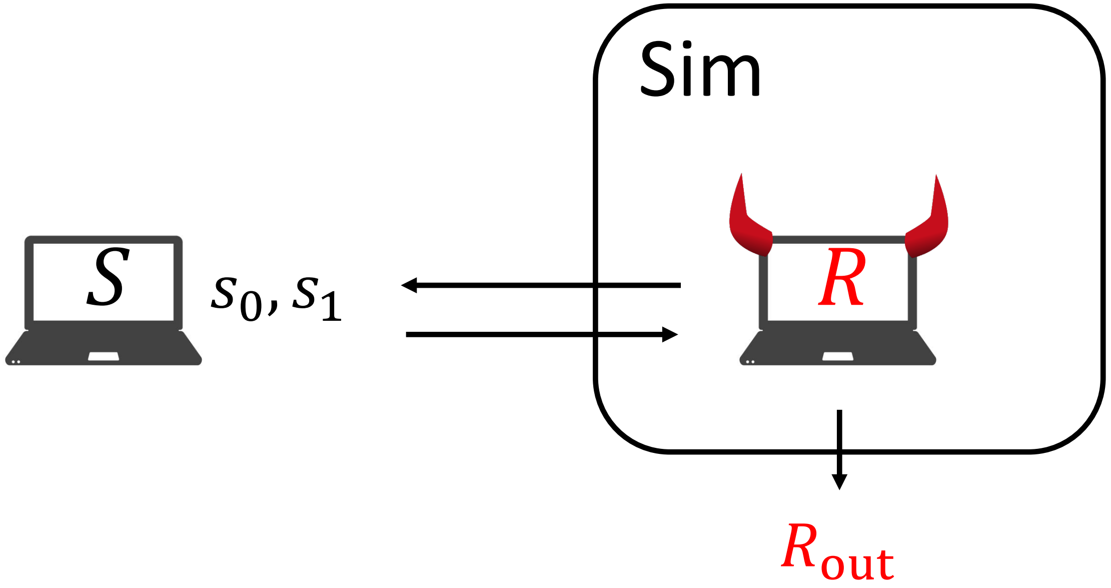
Oblivious Transfer



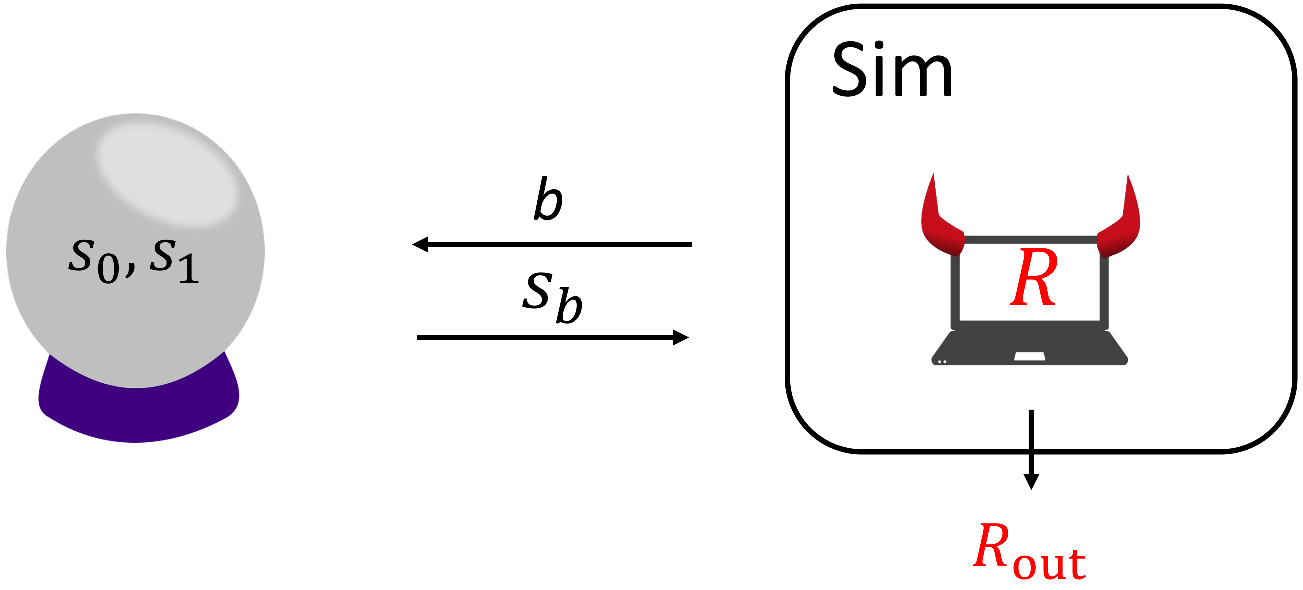
Security Against Malicious Receiver



Security Against Malicious Receiver



Security Against Malicious Receiver

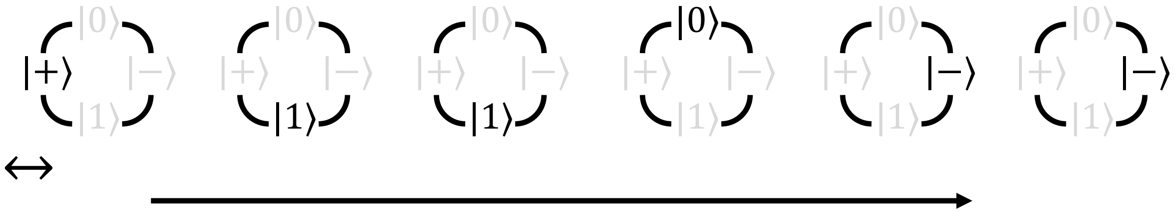


Sim must **extract** implicit choice bit *b* from *R*

[CK88], [BBCS92] Template for OT from Bit Commitment

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

$\underline{R(b)}$


$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$

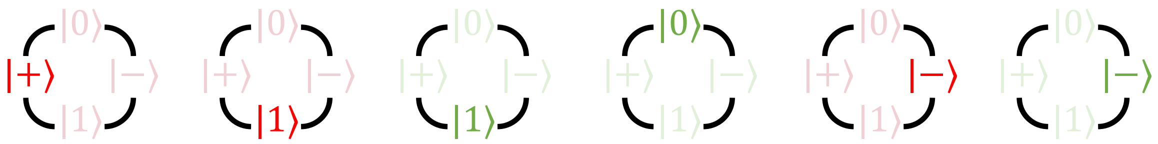
Sample bases $\theta = \leftrightarrow\updownarrow\updownarrow\updownarrow\leftrightarrow\leftrightarrow$

Sample bits $x = 011011$

[CK88], [BBCS92] Template for OT from Bit Commitment

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

$\underline{R(b)}$



$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$

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

Sample bits $x = 011011$

$\xrightarrow{\hspace{5em}}$

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

Measure $x' = 111001$

$\xrightarrow{\theta}$

$I_b = \{3,4,6\}$

$I_{1-b} = \{1,2,5\}$

$\xleftarrow{I_0, I_1}$

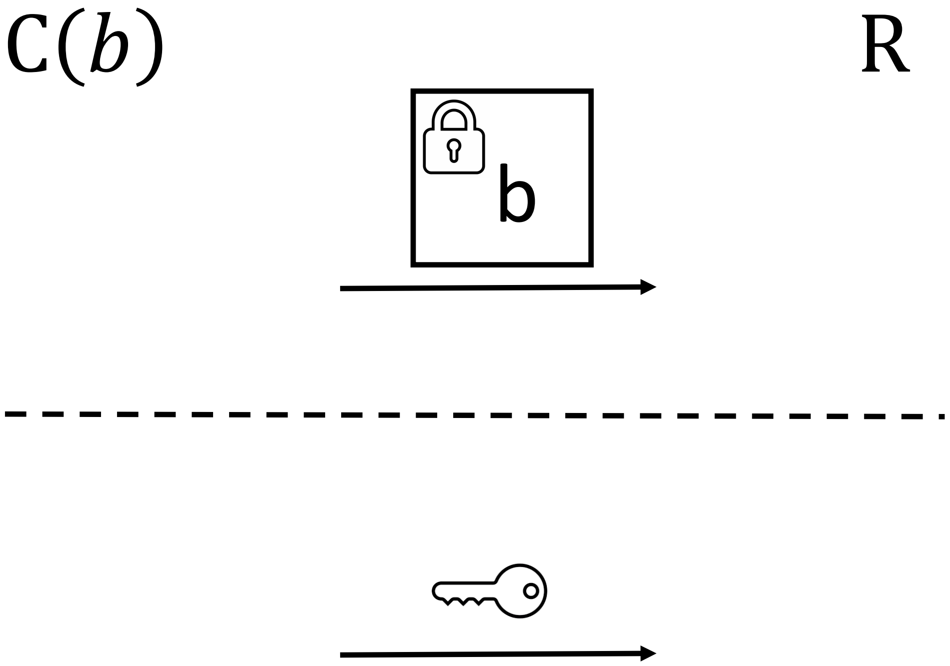
$x^{(0)} = (x_i)_{i \in I_0}$

$x^{(1)} = (x_i)_{i \in I_1}$

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

Cheating R can wait until receiving θ to measure

Aside: Bit Commitment



Hiding: R does not learn b

Binding: C can only make box open to b

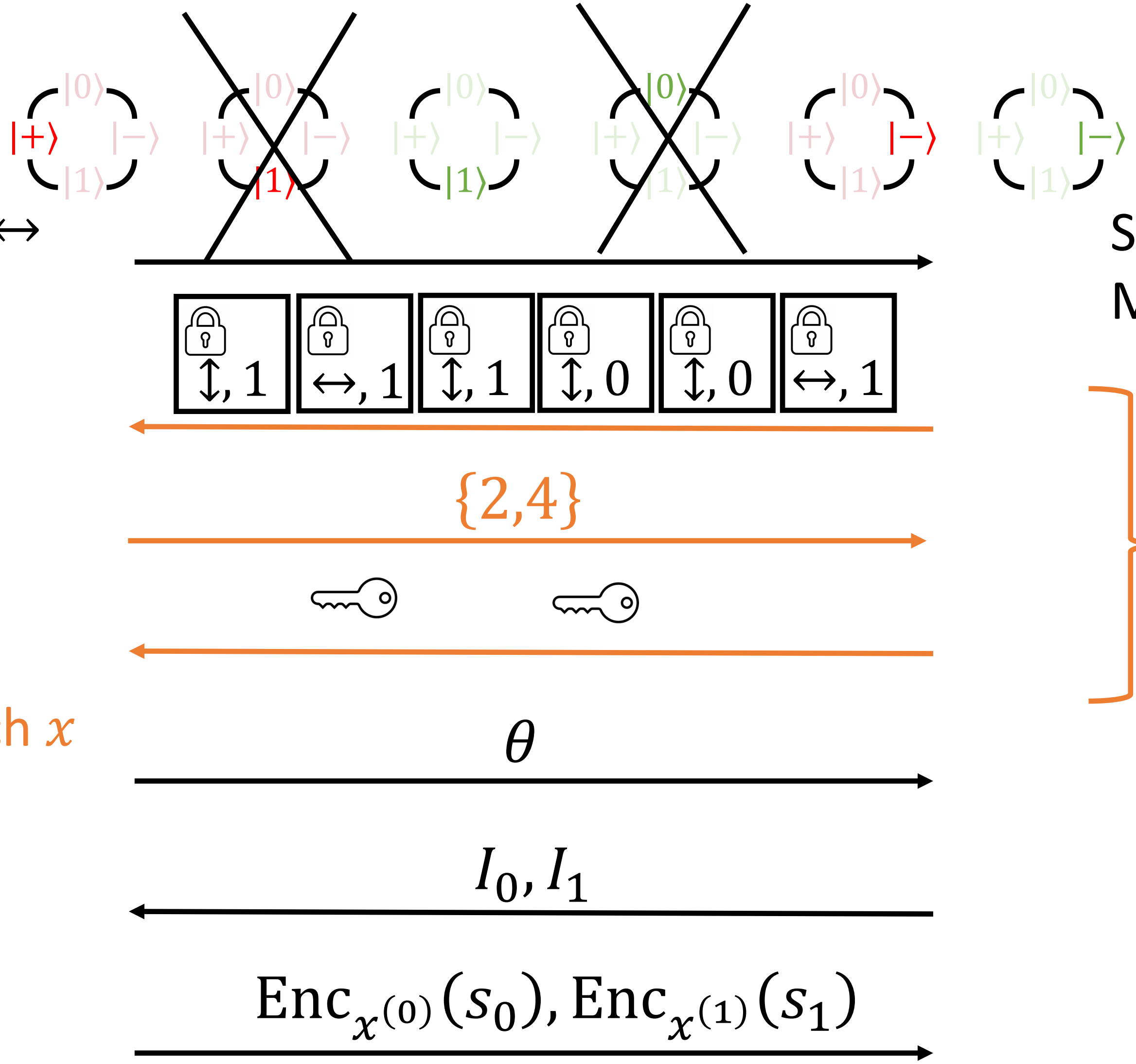
[CK88], [BBCS92] Template for OT from Bit Commitment

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

$\underline{R(b)}$

Sample bases $\theta =$ ↔↕↕↕↔↔

Sample bits $x = 011011$



$\{2,4\}$

θ

I_0, I_1

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

Sample bases $\theta' =$ ↕↔↕↕↕↔

Measure $x' = 111001$

Sample subset {2,4}

Open (↔, 1), (↕, 0),

Check that green bits match x

Measurement check sub-protocol

$I_b = \{3,6\}$

$I_{1-b} = \{1,5\}$

$$x^{(0)} = (x_i)_{i \in I_0}$$

$$x^{(1)} = (x_i)_{i \in I_1}$$

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

- **Extractability** → security against malicious receiver
- **Equivocality** → security against malicious sender

Security against malicious receiver: extract *b* from *R*

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

$\underline{R(b)}$

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

Sample bits $x = 011011$

Extract

(θ', x')

Sample subset $\{2,4\}$

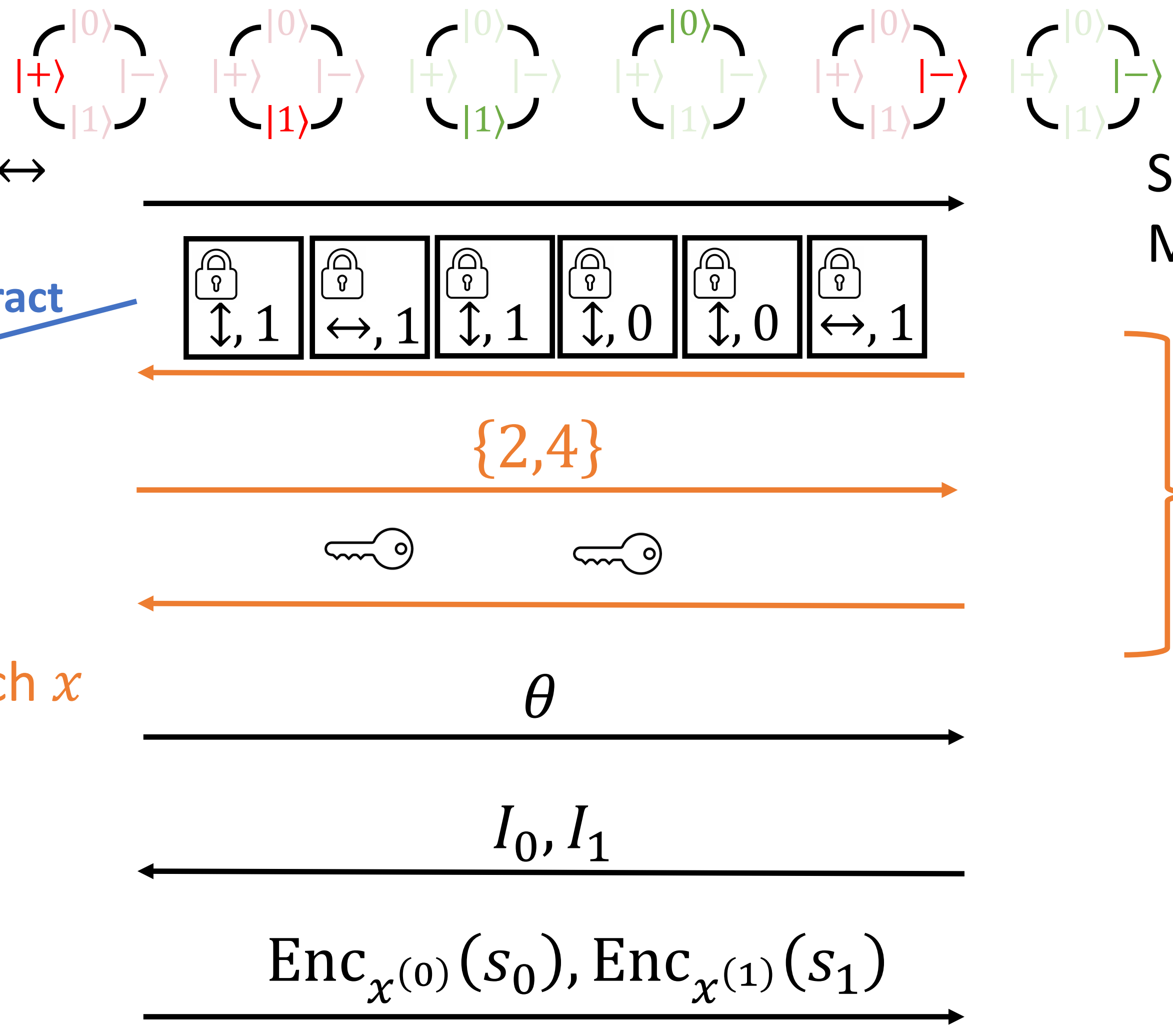
Open $(\leftrightarrow, 1), (\updownarrow, 0)$,

Check that green bits match x

$b \leftarrow \{\theta, \theta', I_0, I_1\}$

$x^{(0)} = (x_i)_{i \in I_0}$

$x^{(1)} = (x_i)_{i \in I_1}$



$\{2,4\}$

θ

I_0, I_1

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

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

Measure $x' = 111001$

Measurement check sub-protocol

$I_b = \{3,6\}$

$I_{1-b} = \{1,5\}$

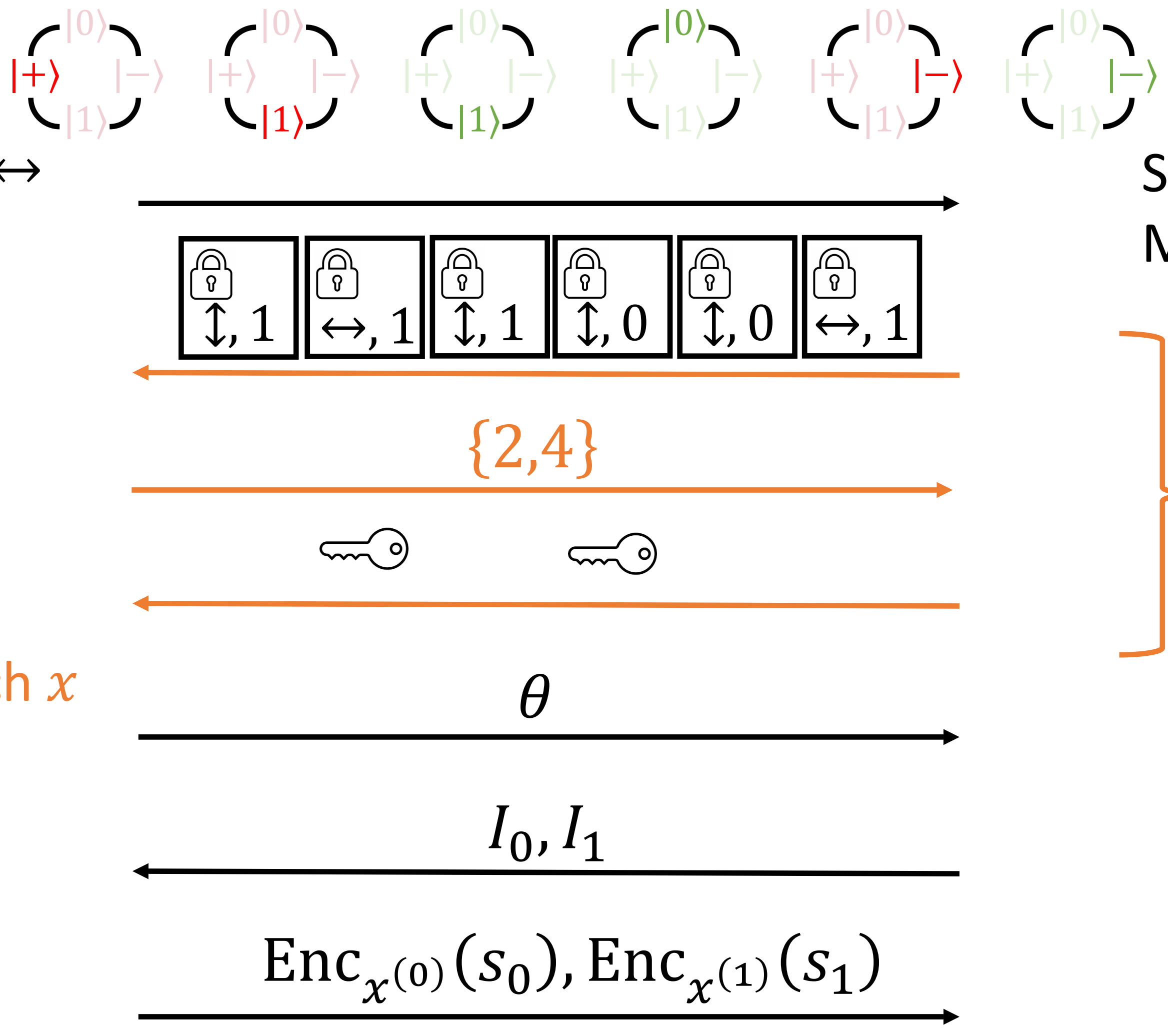
Security against malicious sender: extract (s_0, s_1) from S

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

$\underline{R(b)}$

Sample bases $\theta = \leftrightarrow\updownarrow\updownarrow\updownarrow\leftrightarrow\leftrightarrow$
Sample bits $x = 011011$

Sample bases $\theta' = \updownarrow\leftrightarrow\updownarrow\updownarrow\updownarrow\leftrightarrow$
Measure $x' = 111001$


$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$\updownarrow$, 1
$\leftrightarrow$, 1
$\updownarrow$, 1
$\updownarrow$, 0
$\updownarrow$, 0
$\leftrightarrow$, 1

$\{2,4\}$

θ

I_0, I_1

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

Sample subset $\{2,4\}$

Measurement check sub-protocol

Open $(\leftrightarrow, 1), (\updownarrow, 0)$,
Check that green bits match x

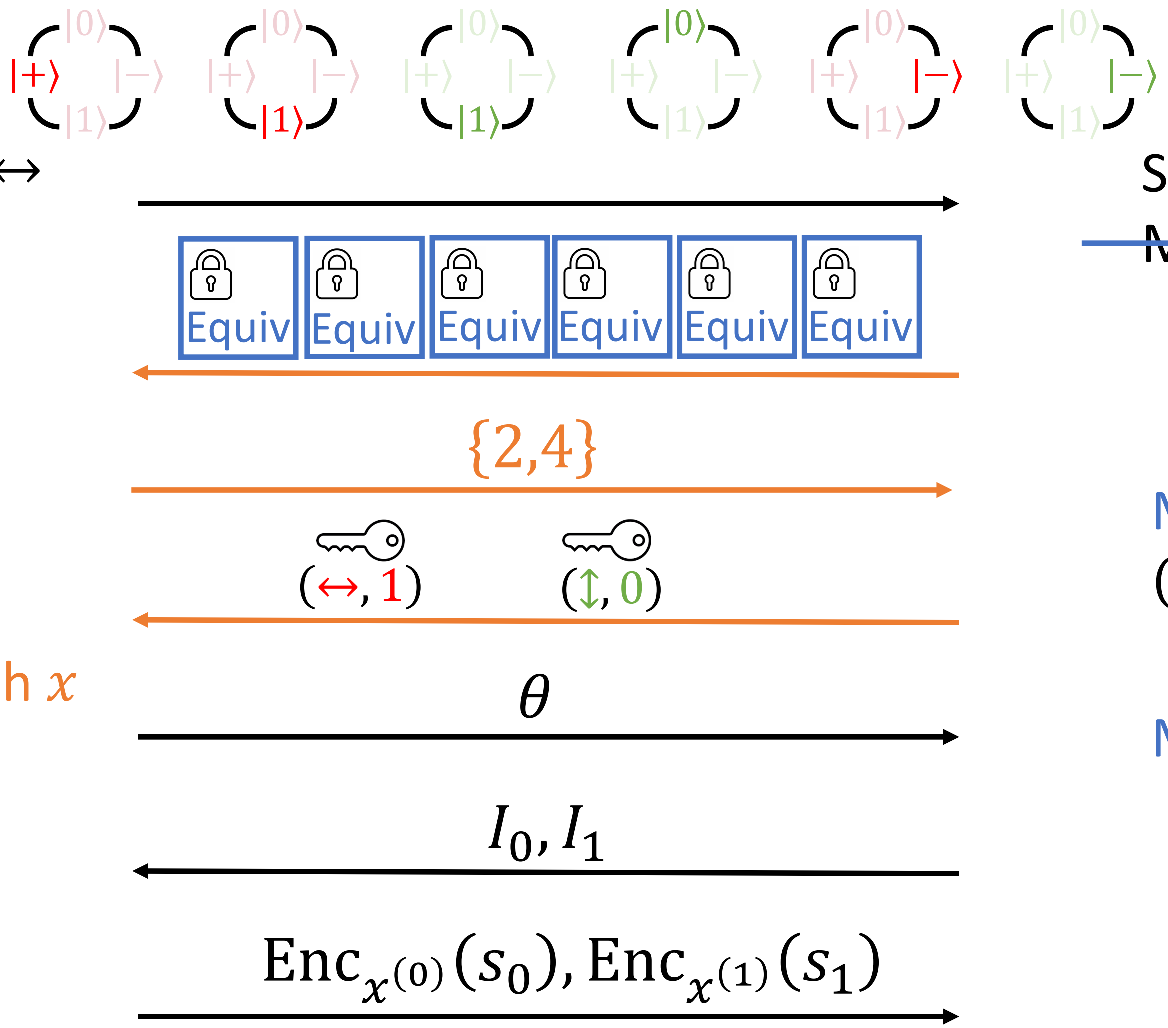
$I_b = \{3,6\}$
$I_{1-b} = \{1,5\}$

$$x^{(0)} = (x_i)_{i \in I_0}$$
$$x^{(1)} = (x_i)_{i \in I_1}$$

Security against malicious sender: extract (s_0, s_1) from S

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

$\underline{R(b)}$



$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
Equiv
Equiv
Equiv
Equiv
Equiv
Equiv
$\{2,4\}$
$(\leftrightarrow, 1)$
$(\updownarrow, 0)$
θ
I_0, I_1
$\mathrm{Enc}_{x^{(0)}}(s_0), \mathrm{Enc}_{x^{(1)}}(s_1)$

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

Sample bits $x = 011011$

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

~~Measure $x' = 111001$~~

Sample subset $\{2,4\}$

Measure qubits 2 and 4: $(\leftrightarrow, 1), (\updownarrow, 0)$

Open $(\leftrightarrow, 1), (\updownarrow, 0)$,
Check that green bits match x

Measure qubits 1,3,5,6 in θ

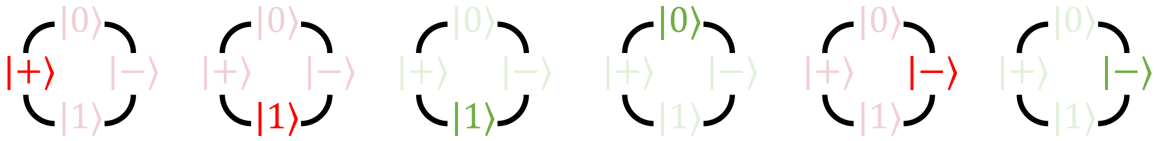
$I_b = \{3,6\}$
$I_{1-b} = \{1,5\}$

$$x^{(0)} = (x_i)_{i \in I_0}$$
$$x^{(1)} = (x_i)_{i \in I_1}$$

Security against malicious sender: extract (s_0, s_1) from S

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

$\underline{R(b)}$



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

Sample bits $x = 011011$

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

~~Measure $x' = 111001$~~

Equiv Equiv Equiv Equiv Equiv Equiv

Sample subset {2,4}

{2,4}

Measure qubits 2 and 4:
(↔, 1), (↕, 0)

(↔, 1) (↕, 0)

Open (↔, 1), (↕, 0),
Check that green bits match x

θ

Measure qubits 1,3,5,6 in θ

I_0, I_1

$I_b = \{3,6\}$
$I_{1-b} = \{1,5\}$

$x^{(0)} = (x_i)_{i \in I_0}$
$x^{(1)} = (x_i)_{i \in I_1}$

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

Obtain (s_0, s_1)

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

[BCKM21]

1. (Black-box) equivocality compiler
2. Extractable commitment from equivocal commitment and quantum communication

[GLSV21]

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

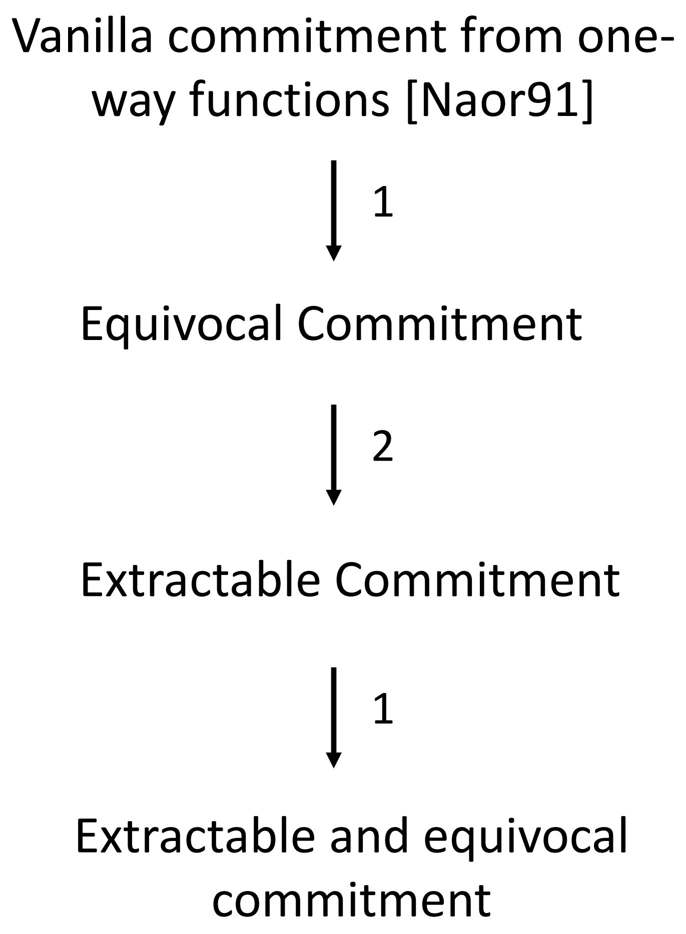
[BCKM21]	[GLSV21]
1. (Black-box) equivocality compiler 2. Extractable commitment from equivocal commitment and quantum communication	1. Equivocal commitment from Naor’s commitment and zero-knowledge 2. Unbounded-simulator OT from equivocal commitment 3. Extractable and equivocal commitment from unbounded-simulator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

Alex’s talk

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

[BCKM21]

1. (Black-box) equivocality compiler
2. Extractable commitment from equivocal commitment and quantum communication



Vanilla commitment from one-way functions [Naor91]

1

Equivocal Commitment

2

Extractable Commitment

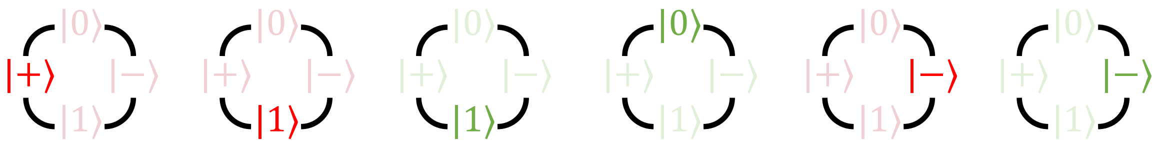
1

Extractable and equivocal commitment

2. Extractable Commitment from Equivocal Commitment

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

$\underline{R(b)}$



Sample bases $\theta = $ ↔↕↕↕↔↔

Sample bits $x = 011011$

Sample bases $\theta' = $ ↕↔↕↕↕↔

~~Measure $x' = 111001$~~

Equiv Equiv Equiv Equiv Equiv Equiv

Sample subset {2,4}

{2,4}

Measure qubits 2 and 4:
(↔, 1), (↕, 0)

(↔, 1) (↕, 0)

Open (↔, 1), (↕, 0),
Check that green bits match x

θ

Measure qubits 1,3,5,6 in θ

I_0, I_1

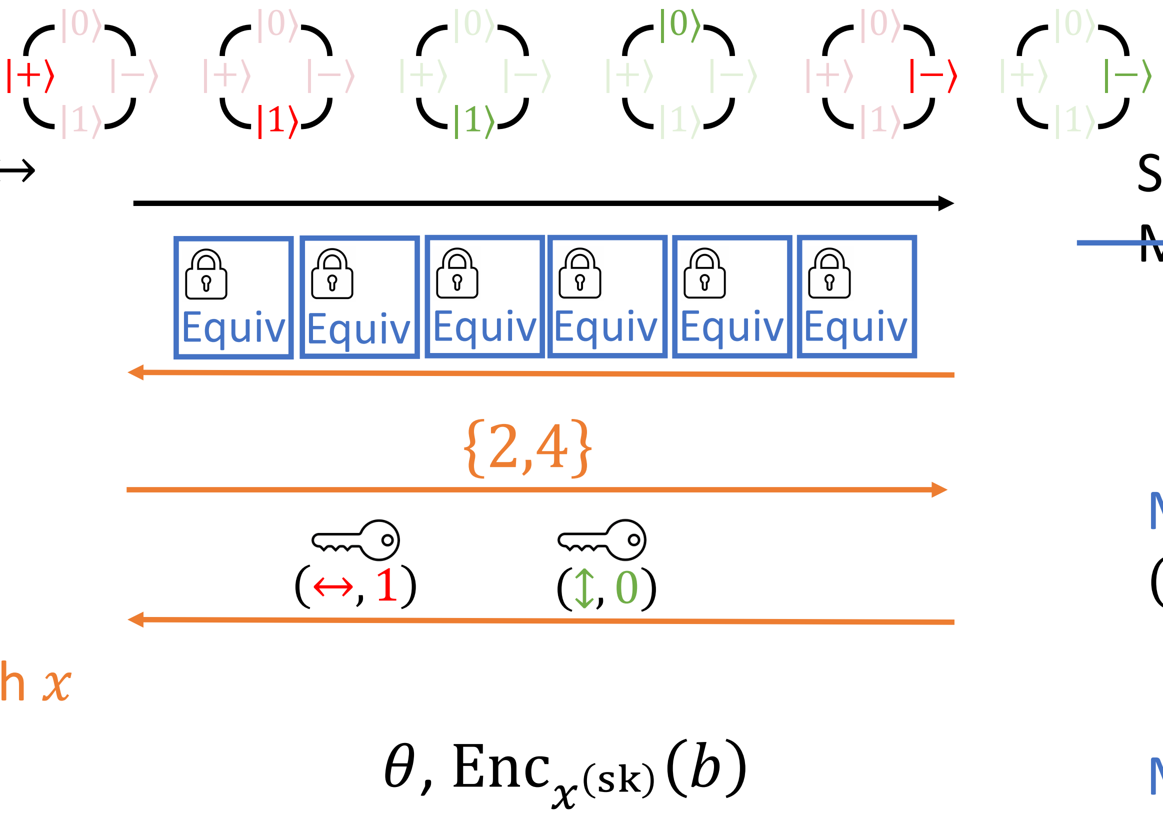
$I_b = \{3,6\}$
$I_{1-b} = \{1,5\}$

$x^{(0)} = (x_i)_{i \in I_0}$
$x^{(1)} = (x_i)_{i \in I_1}$

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

Obtain (s_0, s_1)

2. Extractable Commitment from Equivocal Commitment



$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
$|0\rangle$ $|+\rangle$ $|-\rangle$ $|1\rangle$
Equiv
Equiv
Equiv
Equiv
Equiv
Equiv

ExtractCom(b)

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

Sample bits $x = 011011$

Sample subset $\{2,4\}$

$\{2,4\}$

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

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

Check that green bits match x

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

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

R

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

~~Measure $x' = 111001$~~

Measure qubits 2 and 4:

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

Measure qubits 1,3,5,6 in θ

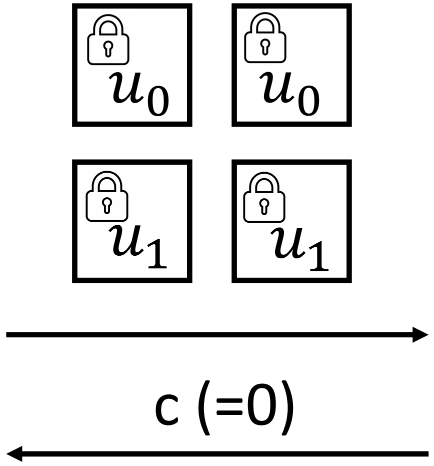
to obtain $x^{(\mathrm{sk})}$

1. Black-Box Equivocality Compiler: Com → EquivCom

$\underline{\mathrm{EquivCom}(b)}$

<u>Rec</u>

Sample $u_0, u_1 \leftarrow \{0,1\}$



Sample c $\leftarrow \{0,1\}$

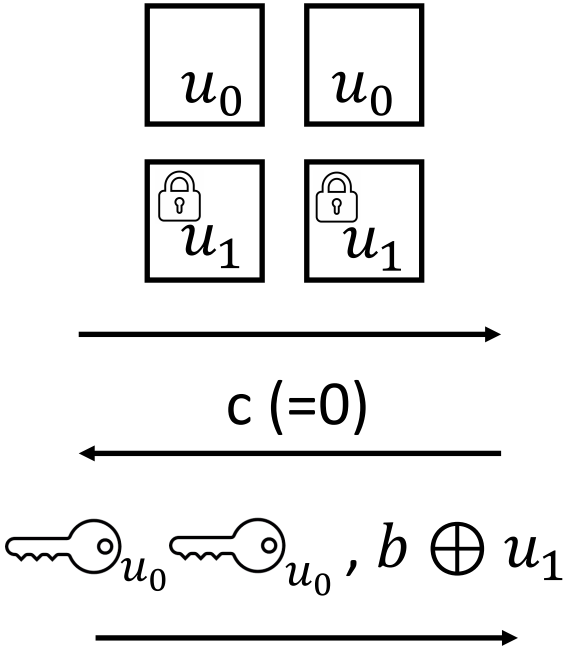
1. Black-Box Equivocality Compiler: Com → EquivCom

$\underline{\text{EquivCom}(b)}$

Rec

Sample $u_0, u_1 \leftarrow \{0,1\}$

Sample c $\leftarrow \{0,1\}$



$\underline{\text{EquivOpen}}$

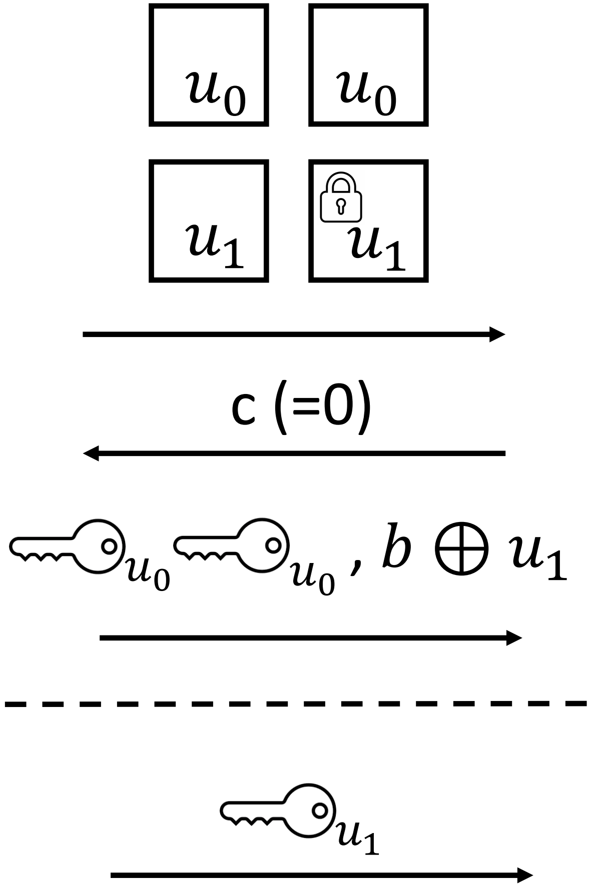
1. Black-Box Equivocality Compiler: Com → EquivCom

EquivCom(b)

Rec

Sample $u_0, u_1 \leftarrow \{0,1\}$

Sample c $\leftarrow \{0,1\}$



EquivOpen

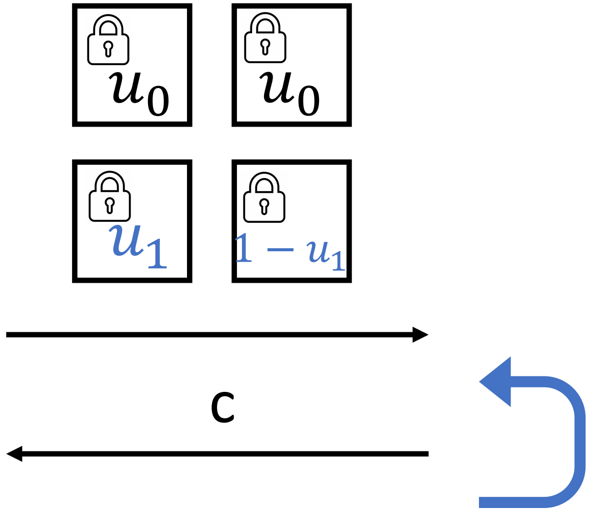
1. Black-Box Equivocality Compiler: Com → EquivCom

EquivCom

Rec

Sample $u_0, u_1 \leftarrow \{0,1\}$

Sample c $\leftarrow \{0,1\}$



Rewind until c $= 0$

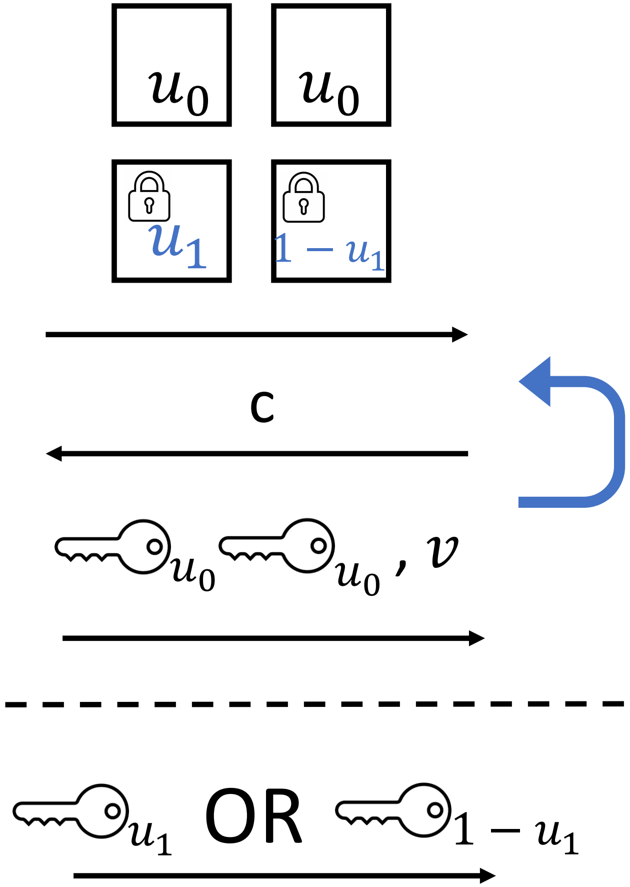
1. Black-Box Equivocality Compiler: Com → EquivCom

EquivCom

Rec

Sample $u_0, u_1 \leftarrow \{0,1\}$

Sample c $\leftarrow \{0,1\}$



Rewind until c = 0

Watrous Rewinding Lemma

Sample $v \leftarrow \{0,1\}$

EquivOpen

	[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
Features:	• **Black-Box** use of one-way functions • **Statistical** security against malicious receiver	• **Constant-Round** OT in the CRS model • **Statistically binding** extractable commitment

Secure Computation is in MiniQCrypt

Merge of:

Oblivious Transfer is in MiniQCrypt

Alex Bredariol Grilo
Huijia Lin
Fang Song
Vinod Vaikuntanathan

One-Way Functions Imply Secure Computation In a Quantum World

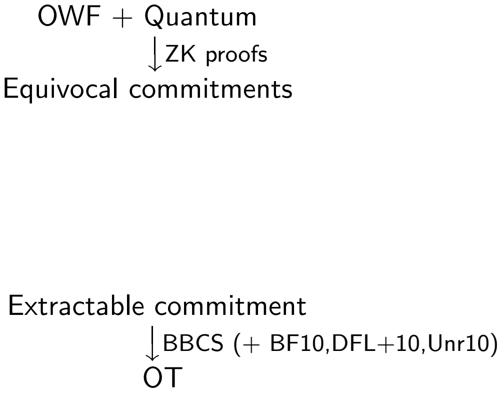
James Bartusek
Andrea Coladangelo
Dakshita Khurana
Fermi Ma

Bird's-eye view

OWF + Quantum

$$\begin{tikzcd}
\text{Extractable commitment} \arrow[d, "\text{BBCS (+ BF10,DFL+10,Unr10)}"] \\
\text{OT}
\end{tikzcd}$$

Bird's-eye view



OWF + Quantum

↓ ZK proofs

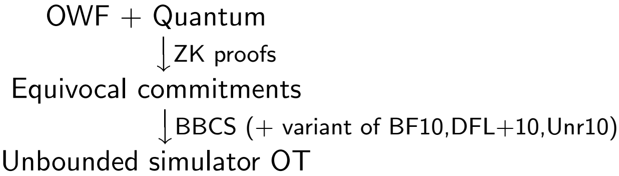
Equivocal commitments

Extractable commitment

↓ BBCS (+ BF10,DFL+10,Unr10)

OT

Bird's-eye view



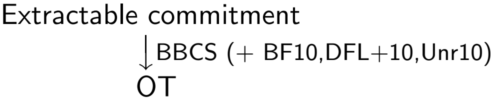
OWF + Quantum

↓ ZK proofs

Equivocal commitments

↓ BBCS (+ variant of BF10,DFL+10,Unr10)

Unbounded simulator OT

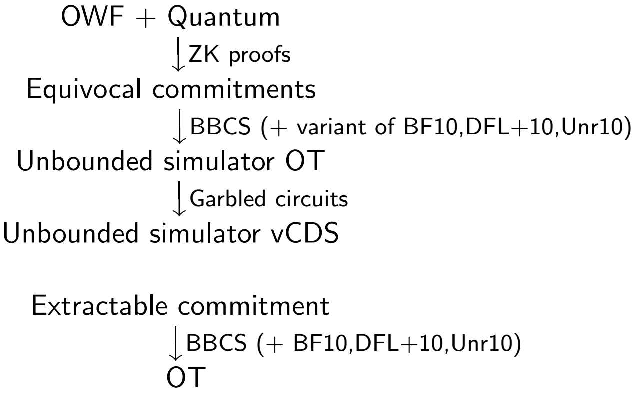


Extractable commitment

↓ BBCS (+ BF10,DFL+10,Unr10)

OT

Bird's-eye view



OWF + Quantum

ZK proofs

Equivocal commitments

BBCS (+ variant of BF10,DFL+10,Unr10)

Unbounded simulator OT

Garbled circuits

Unbounded simulator vCDS

Extractable commitment

BBCS (+ BF10,DFL+10,Unr10)

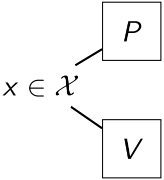
OT

Bird's-eye view

$$\begin{tikzcd}
\text{OWF + Quantum} \arrow[d, "\text{ZK proofs}"] \\
\text{Equivocal commitments} \arrow[d, "\text{BBCS (+ variant of BF10,DFL+10,Unr10)}"] \\
\text{Unbounded simulator OT} \arrow[d, "\text{Garbled circuits}"] \\
\text{Unbounded simulator vCDS} \arrow[d] \\
\text{Extractable commitment} \arrow[d, "\text{BBCS (+ BF10,DFL+10,Unr10)}"] \\
\text{OT}
\end{tikzcd}$$

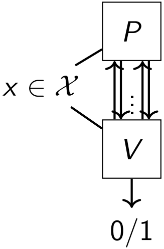
(post-quantum) Zero-knowledge protocol for relations

$$\mathcal{R} \subseteq \mathcal{X} \times \mathcal{W}$$



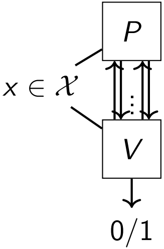
(post-quantum) Zero-knowledge protocol for relations

$$\mathcal{R} \subseteq \mathcal{X} \times \mathcal{W}$$



(post-quantum) Zero-knowledge protocol for relations

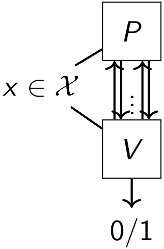
$\mathcal{R} \subseteq \mathcal{X} \times \mathcal{W}$



1. If P knows w s.t. $(x, w) \in \mathcal{R}$, V accepts whp

(post-quantum) Zero-knowledge protocol for relations

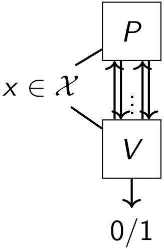
$$\mathcal{R} \subseteq \mathcal{X} \times \mathcal{W}$$



1. If P knows w s.t. $(x, w) \in \mathcal{R}$, V accepts whp
2. If $\nexists w$ s.t. $(x, w) \in \mathcal{R}$, V rejects whp

(post-quantum) Zero-knowledge protocol for relations

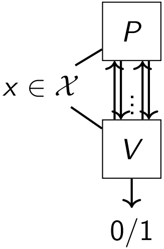
$$\mathcal{R} \subseteq \mathcal{X} \times \mathcal{W}$$



1. If P knows w s.t. $(x, w) \in \mathcal{R}$, V accepts whp
2. If $\nexists w$ s.t. $(x, w) \in \mathcal{R}$, V rejects whp
3. $\tilde{V}$ does not learn w s.t. $(x, w) \in \mathcal{R}$

(post-quantum) Zero-knowledge protocol for relations

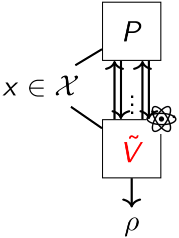
$$\mathcal{R} \subseteq \mathcal{X} \times \mathcal{W}$$



1. If P knows w s.t. $(x, w) \in \mathcal{R}$, V accepts whp
2. If $\nexists w$ s.t. $(x, w) \in \mathcal{R}$, V rejects whp
3. $\tilde{V}$ does not learn w s.t. $(x, w) \in \mathcal{R}$

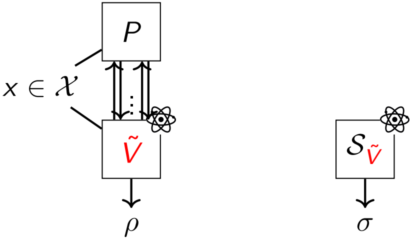
(post-quantum) Zero-knowledge protocol for relations

$$\mathcal{R} \subseteq \mathcal{X} \times \mathcal{W}$$



(post-quantum) Zero-knowledge protocol for relations

$$\mathcal{R} \subseteq \mathcal{X} \times \mathcal{W}$$



P

$x \in \mathcal{X}$

$\tilde{V}$

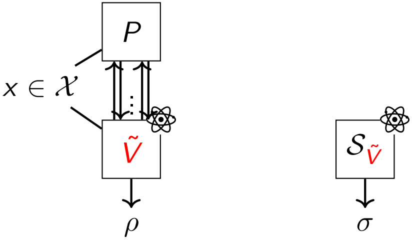
ρ

$\mathcal{S}_{\tilde{V}}$

σ

(post-quantum) Zero-knowledge protocol for relations

$$\mathcal{R} \subseteq \mathcal{X} \times \mathcal{W}$$



Quantum computational zero-knowledge

ρ and σ cannot be **efficiently** distinguished:

$$\forall \text{ quantum poly-time } \mathcal{A} : |Pr[\mathcal{A}(\rho) = 1] - Pr[\mathcal{A}(\sigma) = 1]| \leq negl(n)$$

post-quantum ZK for NP relations

post-quantum ZK for NP relations

NP relations

$\mathcal{R} \subseteq \mathcal{X} \times \mathcal{W}$ is an NP-relation if there exists a polynomial-time algorithm V s.t.

$$V(x, w) = 1 \text{ iff } (x, w) \in \mathcal{R}.$$

post-quantum ZK for NP relations

NP relations

$\mathcal{R} \subseteq \mathcal{X} \times \mathcal{W}$ is an NP-relation if there exists a polynomial-time algorithm V s.t.

$$V(x, w) = 1 \text{ iff } (x, w) \in \mathcal{R}.$$

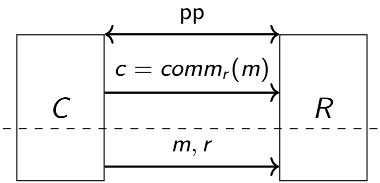
Theorem (Watrous'09)

Assuming the existence of post-quantum secure one-way functions, there is a post-quantum zero-knowledge protocol for all NP relations.

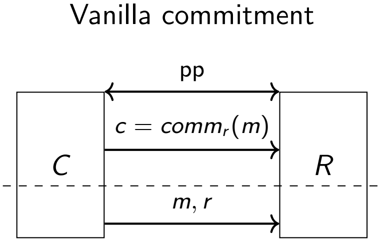
Equivocal commitments

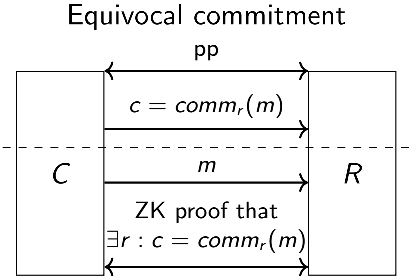
Equivocal commitments

Vanilla commitment

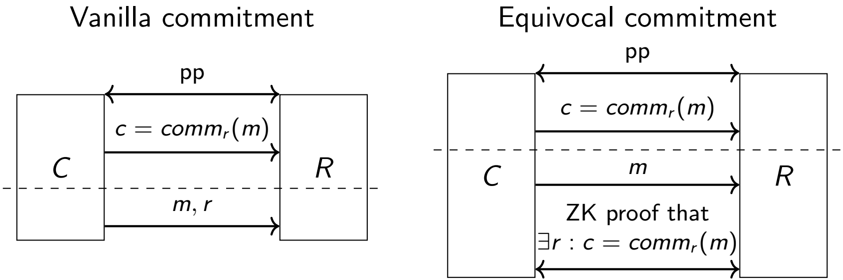


Equivocal commitments





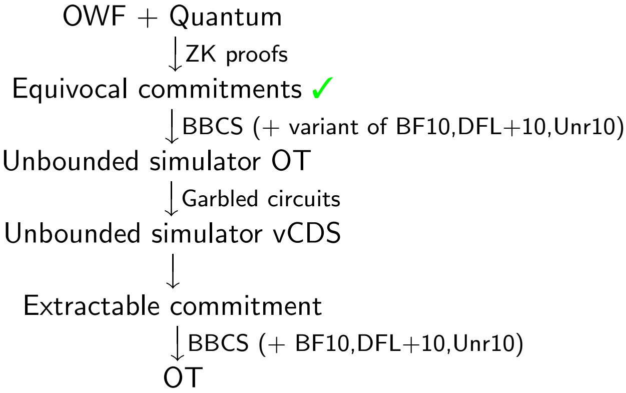
Equivocal commitments



Equivocator

1. Sends $c = comm_r(m)$
2. Sends m'
3. Use ZK simulator to convince R that $c = comm_r(m')$

Bird's-eye view



OWF + Quantum

↓ ZK proofs

Equivocal commitments ✓

↓ BBCS (+ variant of BF10,DFL+10,Unr10)

Unbounded simulator OT

↓ Garbled circuits

Unbounded simulator vCDS

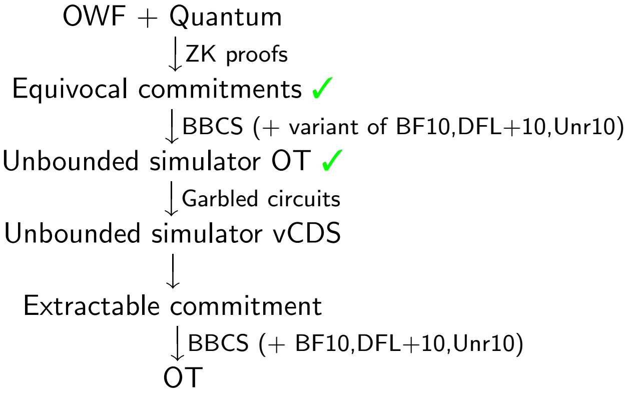
↓

Extractable commitment

↓ BBCS (+ BF10,DFL+10,Unr10)

OT

Bird's-eye view



OWF + Quantum

ZK proofs

Equivocal commitments ✓

BBCS (+ variant of BF10,DFL+10,Unr10)

Unbounded simulator OT ✓

Garbled circuits

Unbounded simulator vCDS

Extractable commitment

BBCS (+ BF10,DFL+10,Unr10)

OT

Conditional Disclosure of Secrets (CDS)

Conditional Disclosure of Secrets (CDS)

NP relations

$\mathcal{R} \subseteq \mathcal{X} \times \mathcal{W}$ is an NP-relation if there exists a polynomial-time algorithm V s.t.

$$V(x, w) = 1 \text{ iff } (x, w) \in \mathcal{R}.$$

Conditional Disclosure of Secrets (CDS)

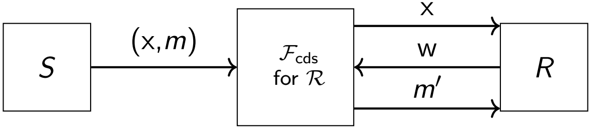
NP relations

$\mathcal{R} \subseteq \mathcal{X} \times \mathcal{W}$ is an NP-relation if there exists a polynomial-time algorithm V s.t.

$$V(x, w) = 1 \text{ iff } (x, w) \in \mathcal{R}.$$

CDS for $\mathcal{R}$

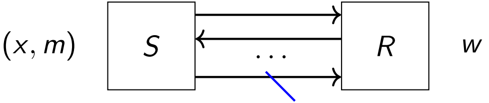
For a chosen $x \in \mathcal{X}$ and message m, S will reveal m to R iff R knows w s.t. $(x, w) \in \mathcal{R}$



$$m' = \begin{cases} m, & \text{if } (x, w) \in \mathcal{R} \\ \perp, & \text{otherwise} \end{cases}$$

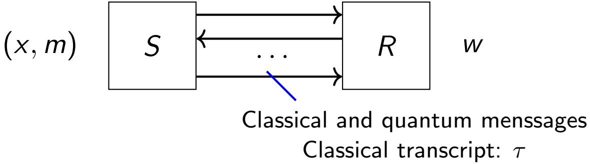
Verifiable CDS protocol

Verifiable CDS protocol



Classical and quantum menssages
Classical transcript: τ

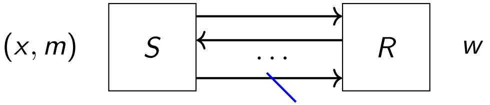
Verifiable CDS protocol



The protocol is a verifiable CDS if

1. It implements $\mathcal{F}_{\text{cds}}$

Verifiable CDS protocol

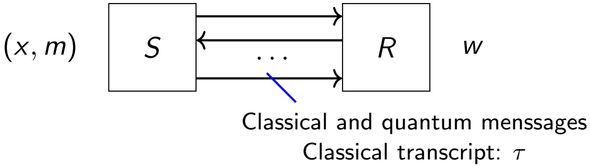


Classical and quantum menssages
Classical transcript: τ

The protocol is a verifiable CDS if

1. It implements $\mathcal{F}_{\text{cds}}$
2. The protocols binds (x, m) that a malicious sender uses and this is verifiable

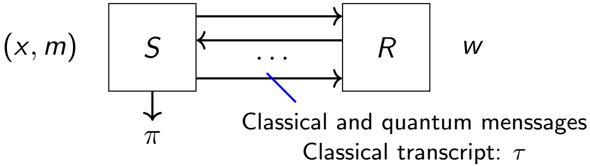
Verifiable CDS protocol



The protocol is a verifiable CDS if

1. It implements $\mathcal{F}_{\mathsf{cds}}$
2. The protocols binds (x, m) that a malicious sender uses and this is verifiable

Verifiable CDS protocol

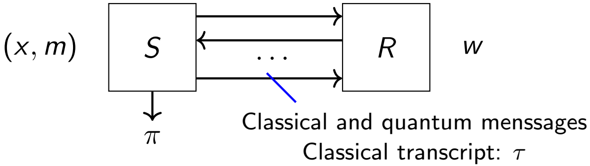


The protocol is a verifiable CDS if

1. It implements $\mathcal{F}_{\text{cds}}$
2. The protocols binds (x, m) that a malicious sender uses and this is verifiable

   After interacting with R, S outputs π such that

Verifiable CDS protocol



Classical and quantum menssages
Classical transcript: τ

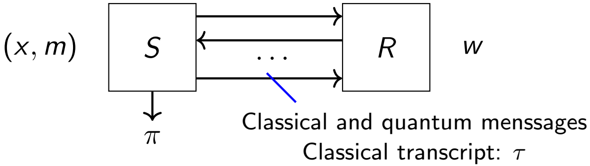
The protocol is a verifiable CDS if

1. It implements $\mathcal{F}_{\text{cds}}$
2. The protocols binds (x, m) that a malicious sender uses and this is verifiable

    After interacting with R, S outputs π such that

    Correctness: $\exists$ poly-time algorithm Ver s.t. for honest R, S $Ver(\tau, x, m, \pi) = 1$

Verifiable CDS protocol



The protocol is a verifiable CDS if

1. It implements $\mathcal{F}_{\mathsf{cds}}$
2. The protocols binds (x, m) that a malicious sender uses and this is verifiable

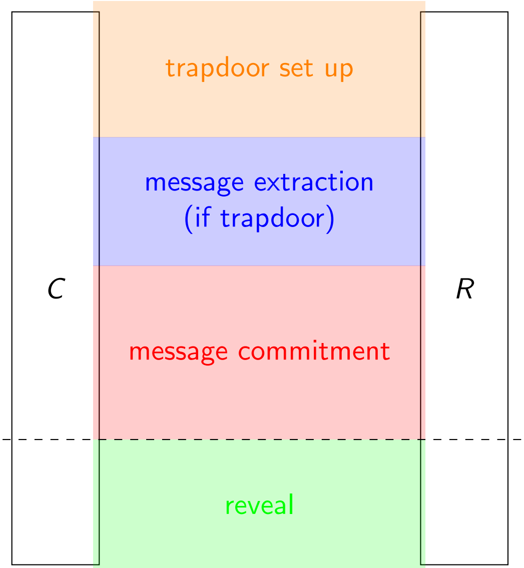
   After interacting with R, S outputs π such that

   Correctness: $\exists$ poly-time algorithm Ver s.t. for honest R, S $Ver(\tau, x, m, \pi) = 1$

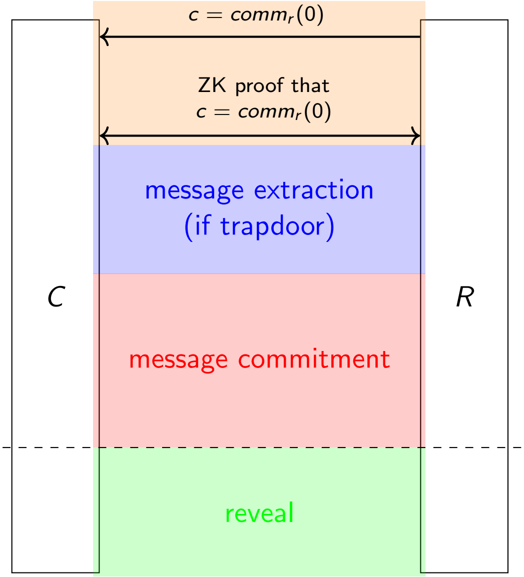
   Binding: For every malicious $\tilde{S}$ that interacts with R and outputs $(\tilde{m}, \tilde{\pi})$ then with negl. probability we have

$$Ver(\tau, x, \tilde{m}, \tilde{\pi}) = 1 \quad \text{and} \quad R \text{ gets } m' \neq \begin{cases} \tilde{m}, & \text{if } (x, w) \in \mathcal{R} \\ \perp, & \text{otherwise} \end{cases}$$

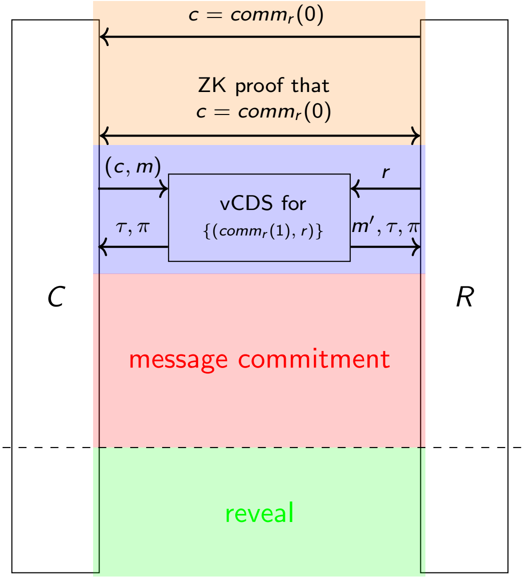
Extractable commitments from unbounded simulator vCDS



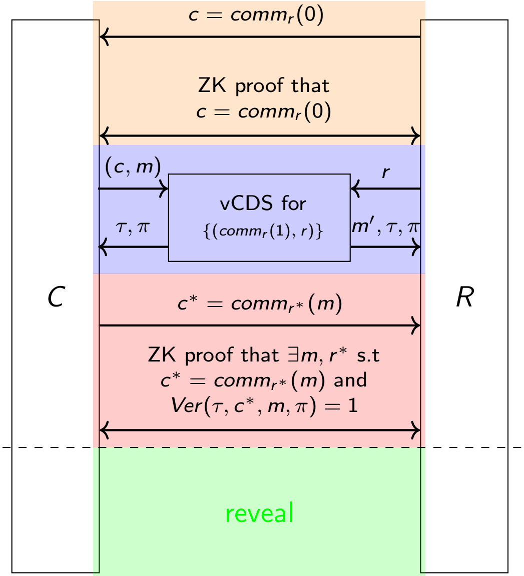
Extractable commitments from unbounded simulator vCDS



Extractable commitments from unbounded simulator vCDS



Extractable commitments from unbounded simulator vCDS



$c = comm_r(0)$

ZK proof that
$c = comm_r(0)$

(c, m)

r

vCDS for
$\{(comm_r(1), r)\}$

τ, π

m', τ, π

C

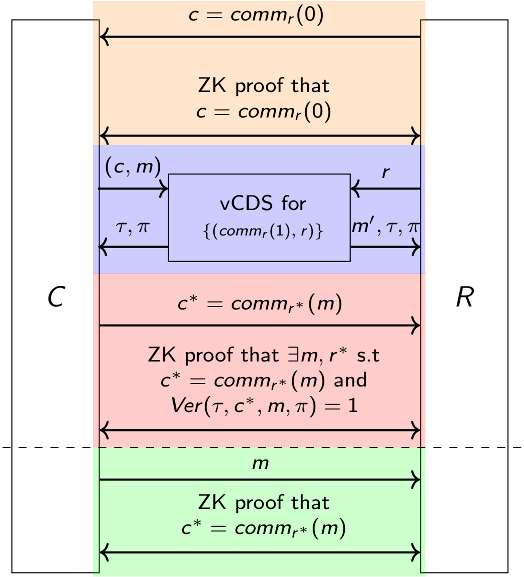
R

$c^* = comm_{r^*}(m)$

ZK proof that $\exists m, r^*$ s.t
$c^* = comm_{r^*}(m)$ and
$Ver(\tau, c^*, m, \pi) = 1$

reveal

Extractable commitments from unbounded simulator vCDS



C

R

$c = comm_r(0)$

ZK proof that
$c = comm_r(0)$

(c, m)

r

vCDS for
$\{(comm_r(1), r)\}$

τ, π

m', τ, π

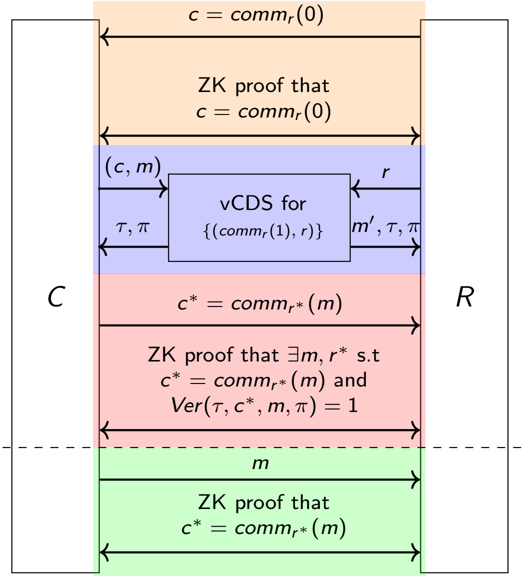
$c^* = comm_{r^*}(m)$

ZK proof that $\exists m, r^*$ s.t
$c^* = comm_{r^*}(m)$ and
$Ver(\tau, c^*, m, \pi) = 1$

m

ZK proof that
$c^* = comm_{r^*}(m)$

Extractable commitments from unbounded simulator vCDS



$c = comm_r(0)$

ZK proof that $c = comm_r(0)$

(c, m)

r

vCDS for $\{(comm_r(1), r)\}$

τ, π

m', τ, π

C

R

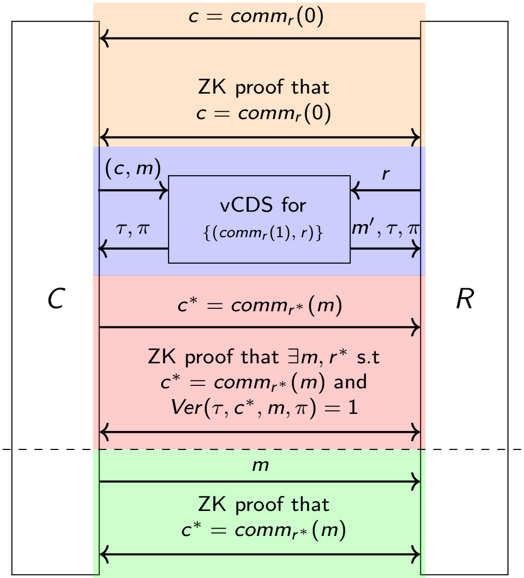
$c^* = comm_{r^*}(m)$

ZK proof that $\exists m, r^*$ s.t $c^* = comm_{r^*}(m)$ and $Ver(\tau, c^*, m, \pi) = 1$

m

ZK proof that $c^* = comm_{r^*}(m)$

Extractable commitments from unbounded simulator vCDS



C

R

$c = comm_r(0)$

ZK proof that $c = comm_r(0)$

(c, m)

r

vCDS for $\{(comm_r(1), r)\}$

τ, π

m', τ, π

$c^* = comm_{r^*}(m)$

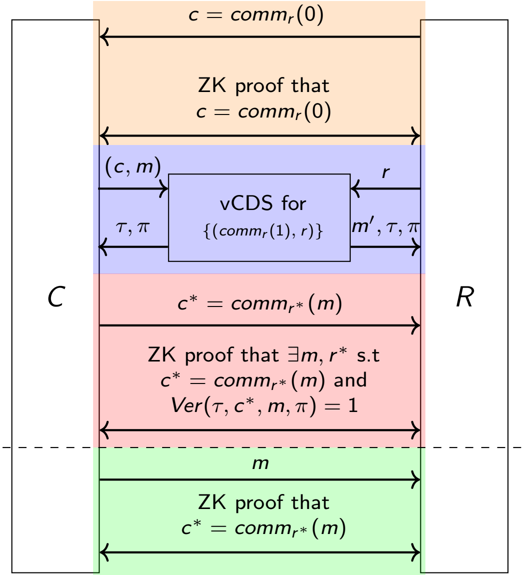
ZK proof that $\exists m, r^*$ s.t $c^* = comm_{r^*}(m)$ and $Ver(\tau, c^*, m, \pi) = 1$

m

ZK proof that $c^* = comm_{r^*}(m)$

Binding ✓

Extractable commitments from unbounded simulator vCDS



$c = comm_r(0)$

ZK proof that
$c = comm_r(0)$

(c, m)

r

vCDS for
$\{(comm_r(1), r)\}$

τ, π

m', τ, π

C

R

$c^* = comm_{r^*}(m)$

ZK proof that $\exists m, r^*$ s.t
$c^* = comm_{r^*}(m)$ and
$Ver(\tau, c^*, m, \pi) = 1$

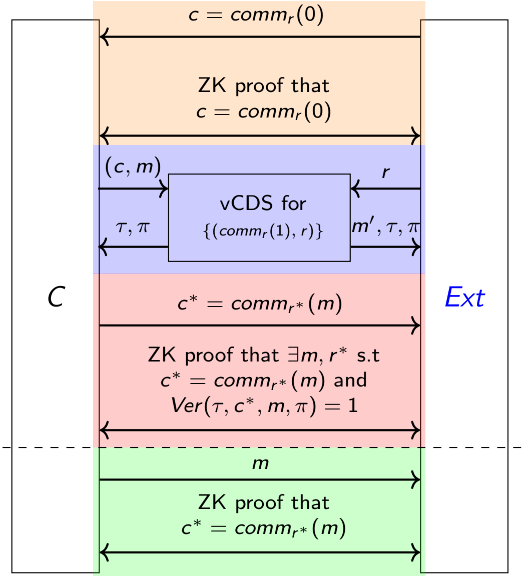
m

ZK proof that
$c^* = comm_{r^*}(m)$

Binding ✓

Hiding ✓

Extractable commitments from unbounded simulator vCDS

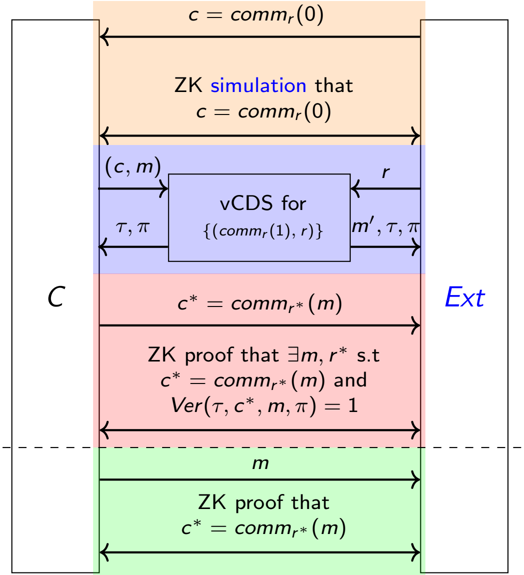

$c = comm_r(0)$
ZK proof that $c = comm_r(0)$
(c, m)
r
vCDS for $\{(comm_r(1), r)\}$
τ, π
m', τ, π
C
Ext
$c^* = comm_{r^*}(m)$
ZK proof that $\exists m, r^*$ s.t $c^* = comm_{r^*}(m)$ and $Ver(\tau, c^*, m, \pi) = 1$
m
ZK proof that $c^* = comm_{r^*}(m)$

Binding ✓

Hiding ✓

Extractability

Extractable commitments from unbounded simulator vCDS

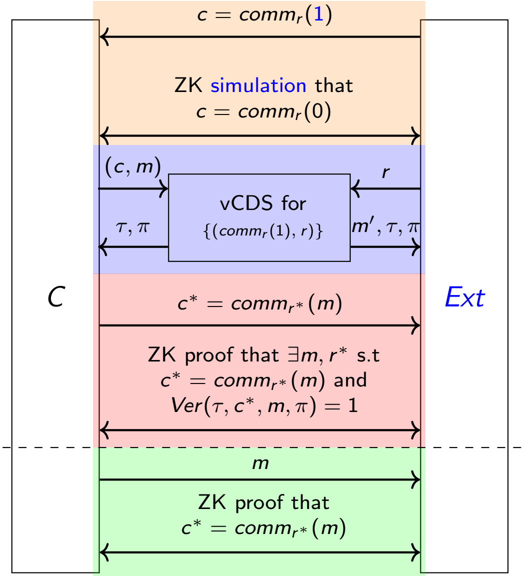


Binding ✓

Hiding ✓

Extractability

Extractable commitments from unbounded simulator vCDS

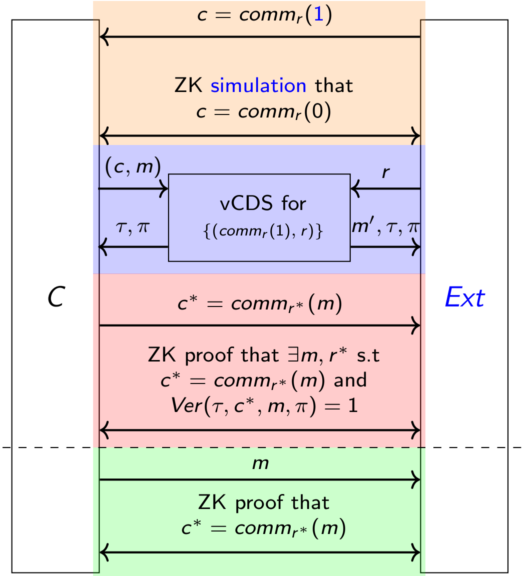


Binding ✓

Hiding ✓

Extractability

Extractable commitments from unbounded simulator vCDS



$c = comm_r(1)$

ZK simulation that $c = comm_r(0)$

(c, m)

r

vCDS for $\{(comm_r(1), r)\}$

τ, π

m', τ, π

C

Ext

$c^* = comm_{r^*}(m)$

ZK proof that $\exists m, r^*$ s.t $c^* = comm_{r^*}(m)$ and $Ver(\tau, c^*, m, \pi) = 1$

m

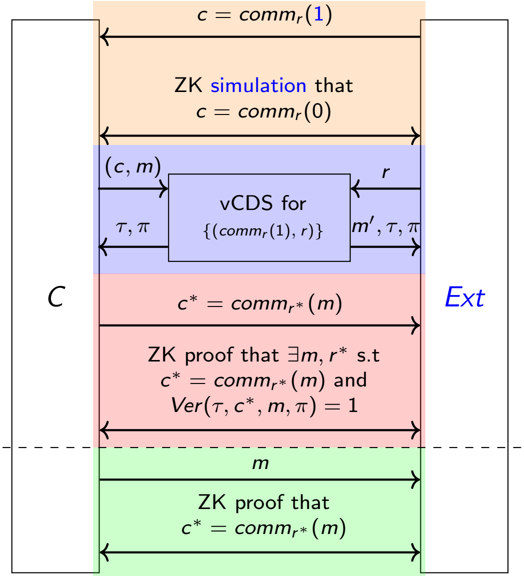
ZK proof that $c^* = comm_{r^*}(m)$

Binding ✓

Hiding ✓

Extractability ✓

Extractable commitments from unbounded simulator vCDS



$c = comm_r(1)$

ZK simulation that $c = comm_r(0)$

(c, m)

r

vCDS for $\{(comm_r(1), r)\}$

τ, π

m', τ, π

C

Ext

$c^* = comm_{r^*}(m)$

ZK proof that $\exists m, r^*$ s.t $c^* = comm_{r^*}(m)$ and $Ver(\tau, c^*, m, \pi) = 1$

m

ZK proof that $c^* = comm_{r^*}(m)$

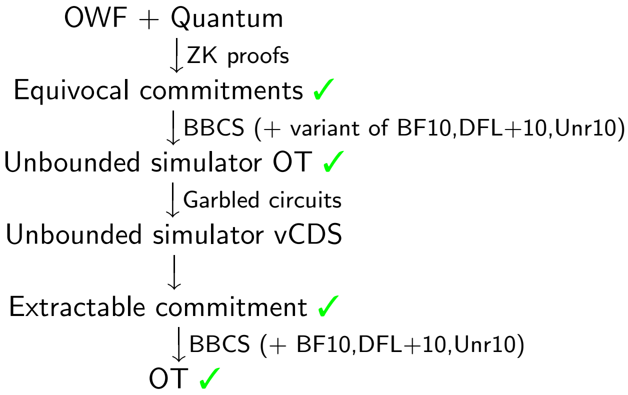
Binding ✓

Hiding ✓

Extractability ✓

Equivocality ✓

Bird's-eye view



OWF + Quantum

↓ ZK proofs

Equivocal commitments ✓

↓ BBCS (+ variant of BF10,DFL+10,Unr10)

Unbounded simulator OT ✓

↓ Garbled circuits

Unbounded simulator vCDS

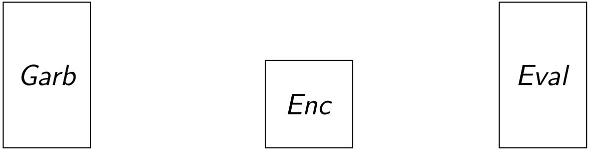
↓

Extractable commitment ✓

↓ BBCS (+ BF10,DFL+10,Unr10)

OT ✓

Garbled circuits



Garb

Enc

Eval

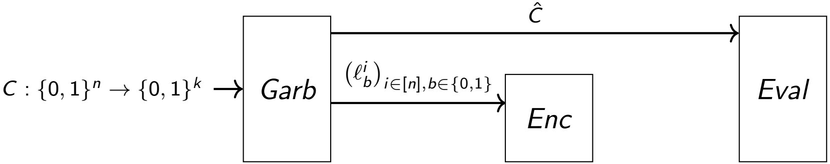
Garbled circuits

$C : \{0,1\}^n \to \{0,1\}^k \longrightarrow$ *Garb*

Enc

Eval

Garbled circuits



$C : \{0,1\}^n \to \{0,1\}^k$

Garb

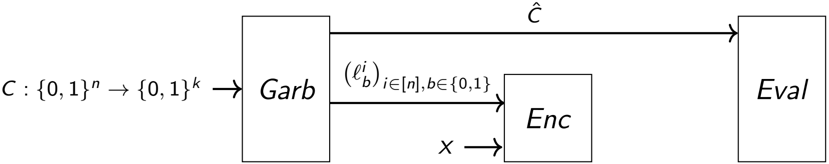
$\hat{C}$

$\left(\ell^i_b\right)_{i\in[n],b\in\{0,1\}}$

Enc

Eval

Garbled circuits



$C : \{0,1\}^n \to \{0,1\}^k$

$Garb$

$\hat{C}$

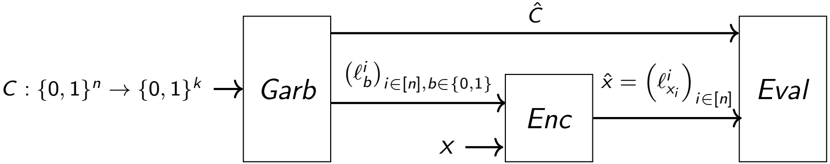
$(\ell_b^i)_{i \in [n], b \in \{0,1\}}$

x

Enc

$Eval$

Garbled circuits



$C : \{0,1\}^n \to \{0,1\}^k$

Garb

$\hat{C}$

$\left(\ell^i_b\right)_{i\in[n],b\in\{0,1\}}$

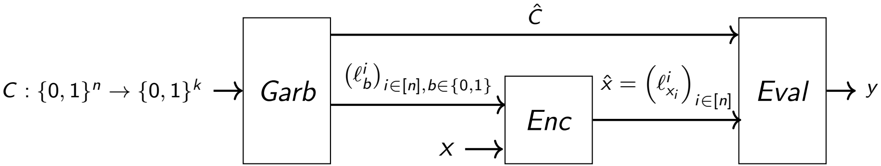
Enc

x

$\hat{x} = \left(\ell^i_{x_i}\right)_{i\in[n]}$

Eval

Garbled circuits



$C : \{0,1\}^n \to \{0,1\}^k$

Garb

$\hat{C}$

$\left(\ell_b^i\right)_{i\in[n],b\in\{0,1\}}$

x

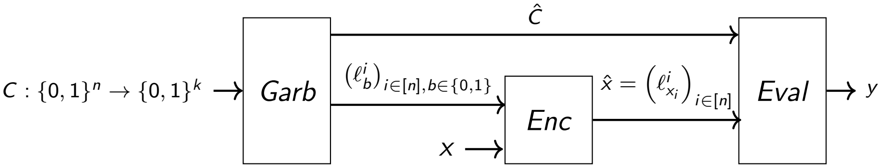
Enc

$\hat{x} = \left(\ell_{x_i}^i\right)_{i\in[n]}$

Eval

y

Garbled circuits



$C : \{0,1\}^n \to \{0,1\}^k$

Garb

$\hat{C}$

$\left(\ell^i_b\right)_{i\in[n],b\in\{0,1\}}$

x

Enc

$\hat{x} = \left(\ell^i_{x_i}\right)_{i\in[n]}$

Eval

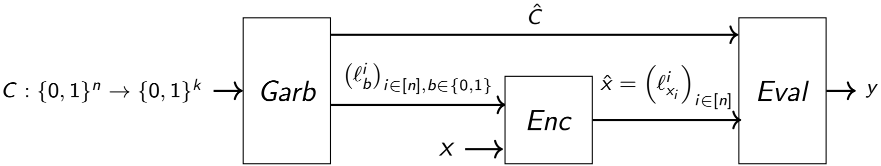
y

Correctness: $y = Eval(\hat{C}, \hat{x}) = C(x)$

Security: There exists *GarbSim* such that

$$(\hat{C}, \hat{x}) \approx_c GarbSim(C(x))$$

Garbled circuits


$C : \{0,1\}^n \to \{0,1\}^k$
$Garb$
$\hat{C}$
$(\ell_b^i)_{i\in[n],b\in\{0,1\}}$
x
Enc
$\hat{x} = \left(\ell_{x_i}^i\right)_{i\in[n]}$
$Eval$
y

Correctness: $y = Eval(\hat{C}, \hat{x}) = C(x)$

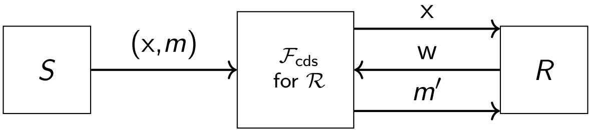
Security: There exists $GarbSim$ such that

$$(\hat{C}, \hat{x}) \approx_c GarbSim(C(x))$$

Theorem [Yao86]

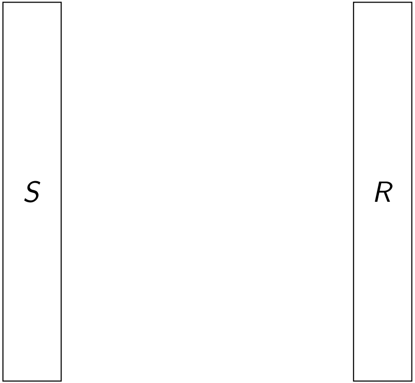
Assuming the existence of post-quantum secure one-way functions, there is a post-quantum secure garbling scheme for polynomial-size circuits.

Protocol for vCDS from OWF + unbounded simulation OT



$$m' = \begin{cases} m, & \text{if } (x, w) \in \mathcal{R} \\ \perp, & \text{otherwise} \end{cases}$$

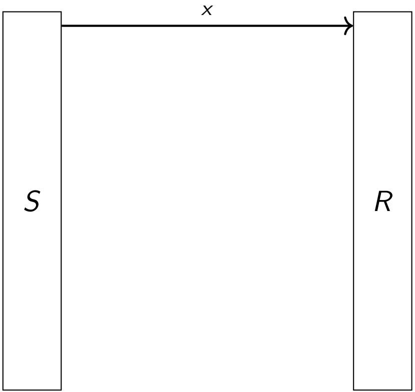
Protocol for vCDS from OWF + unbounded simulation OT



S

R

Protocol for vCDS from OWF + unbounded simulation OT



x

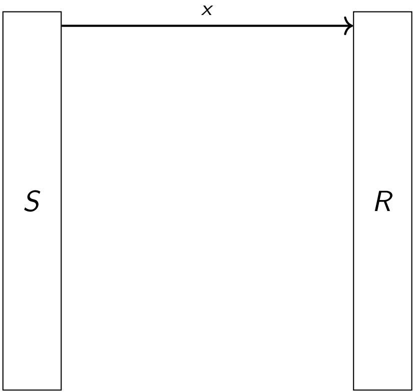
S

R

Protocol for vCDS from OWF + unbounded simulation OT

$$G(w) = \begin{cases} m, & \text{if } (x, w) \in \mathcal{R} \\ \perp, & \text{otherwise} \end{cases}$$

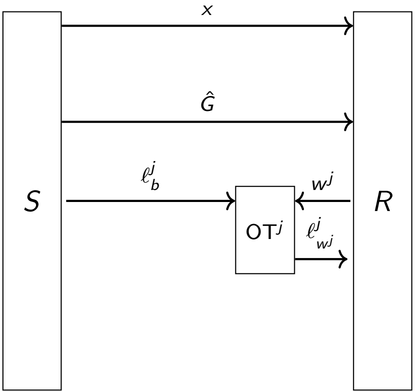
$$\hat{G}, \left(\ell_b^j\right)_{j,b}$$



Protocol for vCDS from OWF + unbounded simulation OT

$$G(w) = \begin{cases} m, & \text{if } (x, w) \in \mathcal{R} \\ \perp, & \text{otherwise} \end{cases}$$

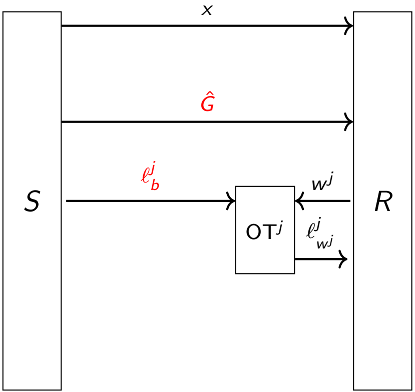
$$\hat{G}, \left(\ell_b^j\right)_{j,b}$$



Protocol for vCDS from OWF + unbounded simulation OT

$$G(w) = \begin{cases} m, & \text{if } (x, w) \in \mathcal{R} \\ \perp, & \text{otherwise} \end{cases}$$

$$\hat{G}, \left(\ell_b^j\right)_{j,b}$$



Protocol for vCDS from OWF + unbounded simulation OT

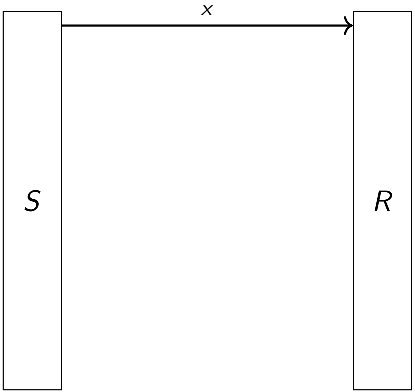
$$G(w) = \begin{cases} m, & \text{if } (x, w) \in \mathcal{R} \\ \perp, & \text{otherwise} \end{cases}$$

$$\hat{G}^1, \left(\ell_b^{1,j}\right)_{j,b}$$

$$\hat{G}^2, \left(\ell_b^{2,j}\right)_{j,b}$$

$$\dots$$

$$\hat{G}^{2\lambda}, \left(\ell_b^{2\lambda,j}\right)_{j,b}$$



Protocol for vCDS from OWF + unbounded simulation OT

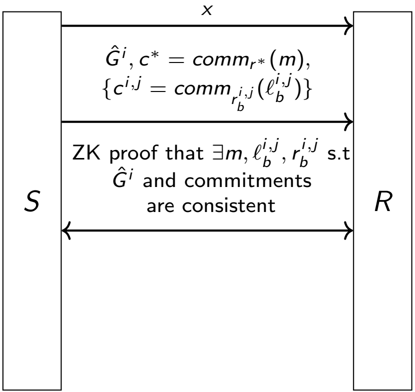
$$G(w) = \begin{cases} m, & \text{if } (x, w) \in \mathcal{R} \\ \perp, & \text{otherwise} \end{cases}$$

$$\hat{G}^1, \left(\ell_b^{1,j}\right)_{j,b}$$

$$\hat{G}^2, \left(\ell_b^{2,j}\right)_{j,b}$$

$\ldots$

$$\hat{G}^{2\lambda}, \left(\ell_b^{2\lambda,j}\right)_{j,b}$$



x

$\hat{G}^i, c^* = comm_{r^*}(m),$
$\{c^{i,j} = comm_{r_b^{i,j}}(\ell_b^{i,j})\}$

ZK proof that $\exists m, \ell_b^{i,j}, r_b^{i,j}$ s.t
$\hat{G}^i$ and commitments
are consistent

S

R

Protocol for vCDS from OWF + unbounded simulation OT

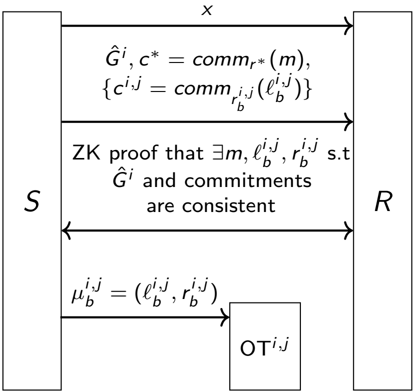
$$G(w) = \begin{cases} m, & \text{if } (x, w) \in \mathcal{R} \\ \bot, & \text{otherwise} \end{cases}$$

$$\hat{G}^1, \left(\ell_b^{1,j}\right)_{j,b}$$

$$\hat{G}^2, \left(\ell_b^{2,j}\right)_{j,b}$$

$$\ldots$$

$$\hat{G}^{2\lambda}, \left(\ell_b^{2\lambda,j}\right)_{j,b}$$



x

$\hat{G}^i, c^* = comm_{r^*}(m)$,

$\{c^{i,j} = comm_{r_b^{i,j}}(\ell_b^{i,j})\}$

ZK proof that $\exists m, \ell_b^{i,j}, r_b^{i,j}$ s.t

$\hat{G}^i$ and commitments

are consistent

$\mu_b^{i,j} = (\ell_b^{i,j}, r_b^{i,j})$

Protocol for vCDS from OWF + unbounded simulation OT

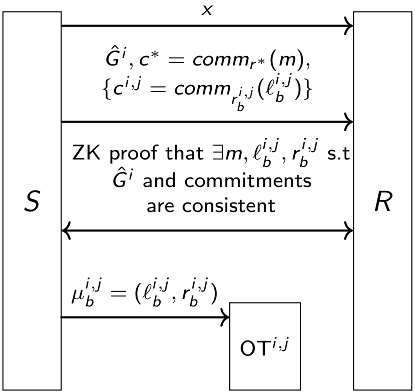
$$G(w) = \begin{cases} m, & \text{if } (x, w) \in \mathcal{R} \\ \perp, & \text{otherwise} \end{cases}$$

$$\hat{G}^1, \left(\ell_b^{1,j}\right)_{j,b}$$

$$\hat{G}^2, \left(\ell_b^{2,j}\right)_{j,b}$$

...

$$\hat{G}^{2\lambda}, \left(\ell_b^{2\lambda,j}\right)_{j,b}$$



x

$\hat{G}^i, c^* = comm_{r^*}(m)$,
$\{c^{i,j} = comm_{r_b^{i,j}}(\ell_b^{i,j})\}$

ZK proof that $\exists m, \ell_b^{i,j}, r_b^{i,j}$ s.t
$\hat{G}^i$ and commitments
are consistent

$\mu_b^{i,j} = (\ell_b^{i,j}, r_b^{i,j})$

S

R

$\mathrm{OT}^{i,j}$

$$\Lambda \subseteq [2\lambda]$$
$$|\Lambda| = \lambda$$

$$\sigma^i = \begin{cases} w, & \text{if } i \in \Lambda \\ s^i \text{ u.a.r}, & \text{o.w.} \end{cases}$$

Protocol for vCDS from OWF + unbounded simulation OT

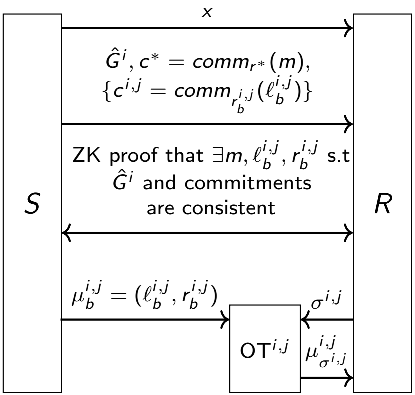
$$G(w) = \begin{cases} m, & \text{if } (x, w) \in \mathcal{R} \\ \perp, & \text{otherwise} \end{cases}$$

$$\hat{G}^1, \left(\ell_b^{1,j}\right)_{j,b}$$

$$\hat{G}^2, \left(\ell_b^{2,j}\right)_{j,b}$$

$$\ldots$$

$$\hat{G}^{2\lambda}, \left(\ell_b^{2\lambda,j}\right)_{j,b}$$



x

$\hat{G}^i, c^* = comm_{r^*}(m),$
$\{c^{i,j} = comm_{r_b^{i,j}}(\ell_b^{i,j})\}$

ZK proof that $\exists m, \ell_b^{i,j}, r_b^{i,j}$ s.t
$\hat{G}^i$ and commitments
are consistent

S

R

$\mu_b^{i,j} = (\ell_b^{i,j}, r_b^{i,j})$

$\text{OT}^{i,j}$

$\sigma^{i,j}$

$\mu^{i,j}_{\sigma^{i,j}}$

$$\Lambda \subseteq [2\lambda]$$
$$|\Lambda| = \lambda$$

$$\sigma^i = \begin{cases} w, & \text{if } i \in \Lambda \\ s^i \text{ u.a.r}, & \text{o.w.} \end{cases}$$

Protocol for vCDS from OWF + unbounded simulation OT

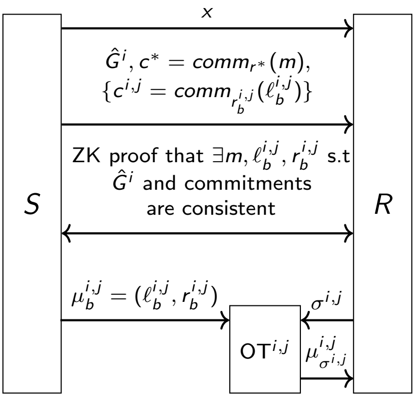
$$G(w) = \begin{cases} m, & \text{if } (x, w) \in \mathcal{R} \\ \perp, & \text{otherwise} \end{cases}$$

$\hat{G}^1, \left(\ell_b^{1,j}\right)_{j,b}$

$\hat{G}^2, \left(\ell_b^{2,j}\right)_{j,b}$

...

$\hat{G}^{2\lambda}, \left(\ell_b^{2\lambda,j}\right)_{j,b}$



x

$\hat{G}^i, c^* = comm_{r^*}(m),$
$\{c^{i,j} = comm_{r_b^{i,j}}(\ell_b^{i,j})\}$

ZK proof that $\exists m, \ell_b^{i,j}, r_b^{i,j}$ s.t $\hat{G}^i$ and commitments are consistent

S

R

$\mu_b^{i,j} = (\ell_b^{i,j}, r_b^{i,j})$

$\mathrm{OT}^{i,j}$

$\sigma^{i,j}$

$\mu_{\sigma^{i,j}}^{i,j}$

$\Lambda \subseteq [2\lambda]$
$|\Lambda| = \lambda$

$$\sigma^i = \begin{cases} w, & \text{if } i \in \Lambda \\ s^i \text{ u.a.r}, & \text{o.w.} \end{cases}$$

Aborts if:

1. ZK fails
2. $\exists i \notin \Lambda, j$:
   $c^{i,j} \neq comm_{r_b^{i,j}}(\ell_b^{i,j})$
3. $\forall i \in \Lambda, \exists j$:
   $c^{i,j} \neq comm_{r_b^{i,j}}(\ell_b^{i,j})$

Otherwise

Output $Eval(\hat{G}^{i^*}, \hat{w})$

Protocol for vCDS from OWF + unbounded simulation OT

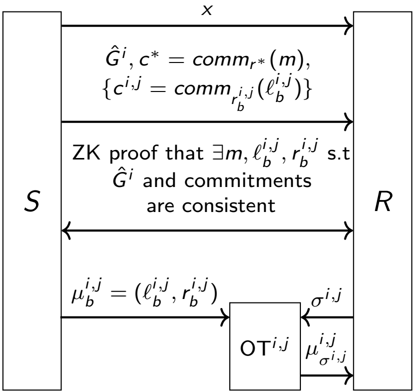
$$G(w) = \begin{cases} m, & \text{if } (x, w) \in \mathcal{R} \\ \perp, & \text{otherwise} \end{cases}$$

$$\hat{G}^1, \left(\ell_b^{1,j}\right)_{j,b}$$

$$\hat{G}^2, \left(\ell_b^{2,j}\right)_{j,b}$$

$$\dots$$

$$\hat{G}^{2\lambda}, \left(\ell_b^{2\lambda,j}\right)_{j,b}$$



S

R

x

$\hat{G}^i, c^* = comm_{r^*}(m),$

$\{c^{i,j} = comm_{r_b^{i,j}}(\ell_b^{i,j})\}$

ZK proof that $\exists m, \ell_b^{i,j}, r_b^{i,j}$ s.t $\hat{G}^i$ and commitments are consistent

$\mu_b^{i,j} = (\ell_b^{i,j}, r_b^{i,j})$

$\mathrm{OT}^{i,j}$

$\sigma^{i,j}$

$\mu_{\sigma^{i,j}}^{i,j}$

$$\Lambda \subseteq [2\lambda]$$

$$|\Lambda| = \lambda$$

$$\sigma^i = \begin{cases} w, & \text{if } i \in \Lambda \\ s^i \text{ u.a.r,} & \text{o.w.} \end{cases}$$

Aborts if:

1. ZK fails
2. $\exists i \notin \Lambda, j$:

   $c^{i,j} \neq comm_{r_b^{i,j}}(\ell_b^{i,j})$
3. $\forall i \in \Lambda, \exists j$:

   $c^{i,j} \neq comm_{r_b^{i,j}}(\ell_b^{i,j})$

Otherwise

Output $Eval(\hat{G}^{i^*}, \hat{w})$

CDS ✓

Protocol for vCDS from OWF + unbounded simulation OT

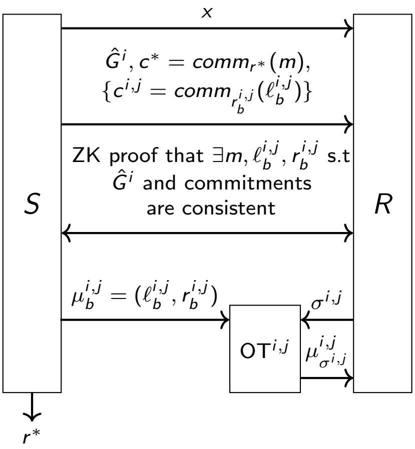
$$G(w) = \begin{cases} m, & \text{if } (x,w) \in \mathcal{R} \\ \bot, & \text{otherwise} \end{cases}$$

$\hat{G}^1, \left(\ell_b^{1,j}\right)_{j,b}$

$\hat{G}^2, \left(\ell_b^{2,j}\right)_{j,b}$

...

$\hat{G}^{2\lambda}, \left(\ell_b^{2\lambda,j}\right)_{j,b}$



S

R

x

$\hat{G}^i, c^* = comm_{r^*}(m),$

$\{c^{i,j} = comm_{r_b^{i,j}}(\ell_b^{i,j})\}$

ZK proof that $\exists m, \ell_b^{i,j}, r_b^{i,j}$ s.t $\hat{G}^i$ and commitments are consistent

$\mu_b^{i,j} = (\ell_b^{i,j}, r_b^{i,j})$

$\text{OT}^{i,j}$

$\sigma^{i,j}$

$\mu_{\sigma^{i,j}}^{i,j}$

r^*

$\Lambda \subseteq [2\lambda]$

$|\Lambda| = \lambda$

$$\sigma^i = \begin{cases} w, & \text{if } i \in \Lambda \\ s^i \text{ u.a.r}, & \text{o.w.} \end{cases}$$

Aborts if:

1. ZK fails
2. $\exists i \notin \Lambda, j$: $c^{i,j} \neq comm_{r_b^{i,j}}(\ell_b^{i,j})$
3. $\forall i \in \Lambda, \exists j$: $c^{i,j} \neq comm_{r_b^{i,j}}(\ell_b^{i,j})$

Otherwise

Output $Eval(\hat{G}^{i^*}, \hat{w})$

CDS ✓
Verifiability: $Ver(\tau, x, m, r^*) = 1$ iff $c^* = comm_{r^*}(m)$

Protocol for vCDS from OWF + unbounded simulation OT

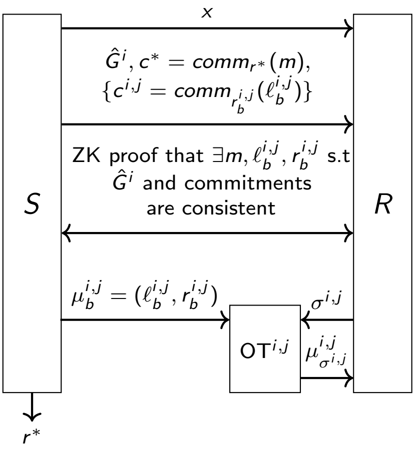
$$G(w) = \begin{cases} m, & \text{if } (x, w) \in \mathcal{R} \\ \bot, & \text{otherwise} \end{cases}$$

$$\hat{G}^1, \left(\ell_b^{1,j}\right)_{j,b}$$

$$\hat{G}^2, \left(\ell_b^{2,j}\right)_{j,b}$$

...

$$\hat{G}^{2\lambda}, \left(\ell_b^{2\lambda,j}\right)_{j,b}$$


x
$\hat{G}^i, c^* = comm_{r^*}(m)$,
$\{c^{i,j} = comm_{r_b^{i,j}}(\ell_b^{i,j})\}$
ZK proof that $\exists m, \ell_b^{i,j}, r_b^{i,j}$ s.t
$\hat{G}^i$ and commitments
are consistent
S
R
$\mu_b^{i,j} = (\ell_b^{i,j}, r_b^{i,j})$
$\sigma^{i,j}$
$\text{OT}^{i,j}$
$\mu_{\sigma^{i,j}}^{i,j}$
r^*

$$\Lambda \subseteq [2\lambda]$$
$$|\Lambda| = \lambda$$

$$\sigma^i = \begin{cases} w, & \text{if } i \in \Lambda \\ s^i \text{ u.a.r,} & \text{o.w.} \end{cases}$$

Aborts if:

1. ZK fails
2. $\exists i \notin \Lambda, j$: $c^{i,j} \neq comm_{r_b^{i,j}}(\ell_b^{i,j})$
3. $\forall i \in \Lambda, \exists j$: $c^{i,j} \neq comm_{r_b^{i,j}}(\ell_b^{i,j})$

Otherwise

Output $Eval(\hat{G}^{i^*}, \hat{w})$

CDS ✓
Verifiability: $Ver(\tau, x, m, r^*) = 1$ iff $c^* = comm_{r^*}(m)$

1. **Correctness** ✓

Protocol for vCDS from OWF + unbounded simulation OT

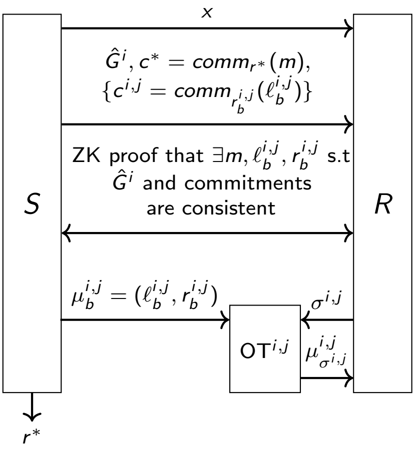
$$G(w) = \begin{cases} m, & \text{if } (x, w) \in \mathcal{R} \\ \bot, & \text{otherwise} \end{cases}$$

$\hat{G}^1, \left(\ell_b^{1,j}\right)_{j,b}$

$\hat{G}^2, \left(\ell_b^{2,j}\right)_{j,b}$

...

$\hat{G}^{2\lambda}, \left(\ell_b^{2\lambda,j}\right)_{j,b}$



x

$\hat{G}^i, c^* = comm_{r^*}(m),$
$\{c^{i,j} = comm_{r_b^{i,j}}(\ell_b^{i,j})\}$

ZK proof that $\exists m, \ell_b^{i,j}, r_b^{i,j}$ s.t $\hat{G}^i$ and commitments are consistent

$\mu_b^{i,j} = (\ell_b^{i,j}, r_b^{i,j})$

$\sigma^{i,j}$

$\mathsf{OT}^{i,j}$

$\mu_{\sigma^{i,j}}^{i,j}$

S

R

r^*

$\Lambda \subseteq [2\lambda]$
$|\Lambda| = \lambda$

$$\sigma^i = \begin{cases} w, & \text{if } i \in \Lambda \\ s^i \text{ u.a.r}, & \text{o.w.} \end{cases}$$

Aborts if:

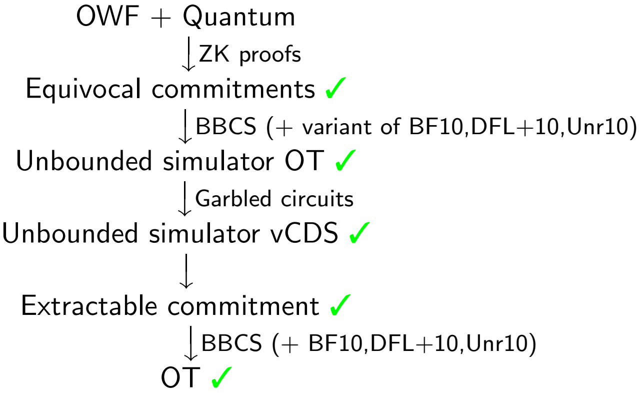
1. ZK fails
2. $\exists i \notin \Lambda, j$: $c^{i,j} \neq comm_{r_b^{i,j}}(\ell_b^{i,j})$
3. $\forall i \in \Lambda, \exists j$: $c^{i,j} \neq comm_{r_b^{i,j}}(\ell_b^{i,j})$

Otherwise

Output $Eval(\hat{G}^{i^*}, \hat{w})$

CDS ✓
Verifiability: $Ver(\tau, x, m, r^*) = 1$ iff $c^* = comm_{r^*}(m)$
1. **Correctness** ✓
2. **Binding** ✓

Bird's-eye view



OWF + Quantum

↓ ZK proofs

Equivocal commitments ✓

↓ BBCS (+ variant of BF10,DFL+10,Unr10)

Unbounded simulator OT ✓

↓ Garbled circuits

Unbounded simulator vCDS ✓

↓

Extractable commitment ✓

↓ BBCS (+ BF10,DFL+10,Unr10)

OT ✓

[BCKM21]

1. (Black-box) equivocality compiler
2. Extractable commitment from equivocal commitment and quantum communication

Features:

- **Black-Box** use of one-way functions
- **Statistical** security against malicious receiver

[GLSV21]

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

- **Constant-Round** OT in the CRS model
- **Statistically binding** extractable commitment

Conclusions and open problems

Secure (quantum) multi-party computation is in MiniQCrypt (OWF+quantum).

Conclusions and open problems

Secure (quantum) multi-party computation is in MiniQCrypt (OWF+quantum).
What else?

Conclusions and open problems

Secure (quantum) multi-party computation is in MiniQCrypt (OWF+quantum).
What else?

Thank you for your attention