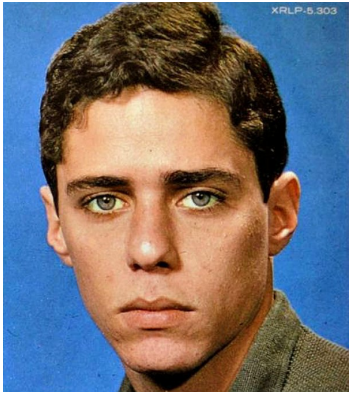
Improving quantum cryptography with computational assumptions

Alex Bredariol Grilo

Quantum information vs. cryptography

Quantum information vs. cryptography



Quantum helps malicious parties

Quantum information vs. cryptography

Quantum helps honest parties

Quantum helps malicious parties

Quantum information vs. cryptography

Quantum helps honest parties Quantum helps malicious parties

How do quantum resources allow us to achieve better cryptographic protocols?

Quantum 101 (simplified)

Quantum mechanics

Quantum states | Evolution | Measurements

Quantum 101 (simplified)

Quantum mechanics

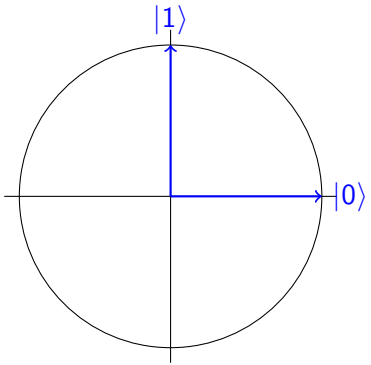
Quantum states | Evolution | Measurements

Quantum 101 (simplified)

Quantum mechanics

Quantum states | Evolution | Measurements

States

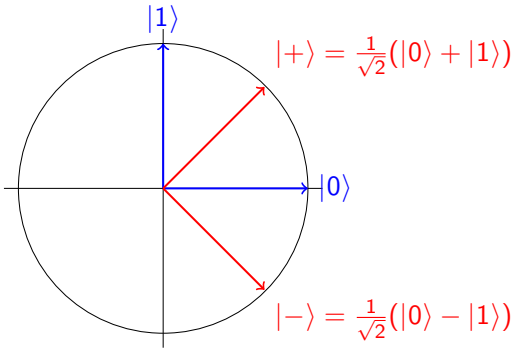


Quantum 101 (simplified)

Quantum mechanics

Quantum states | Evolution | Measurements

States

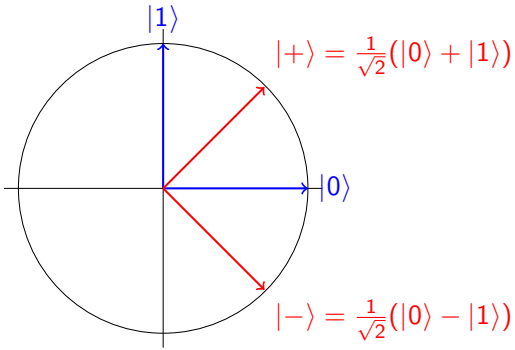


Quantum 101 (simplified)

Quantum mechanics

Quantum states | Evolution | Measurements

States



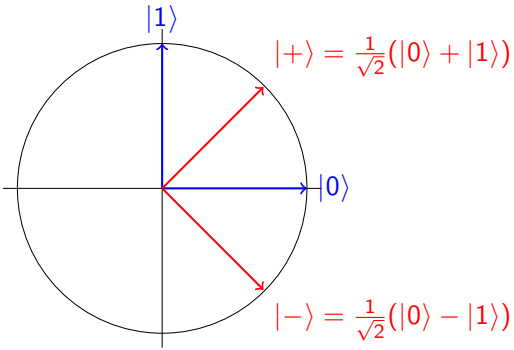
Measurements

Quantum 101 (simplified)

Quantum mechanics

Quantum states | Evolution | Measurements

States



Measurements

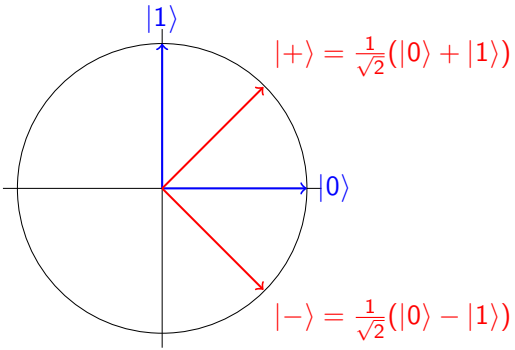
- Computational basis $\rightarrow$
  - Meas. $|0\rangle$, the outcome is 0 w.p. 1
  - Meas. $|1\rangle$, the outcome is 1 w.p. 1

Quantum 101 (simplified)

Quantum mechanics

Quantum states | Evolution | Measurements

States



Measurements

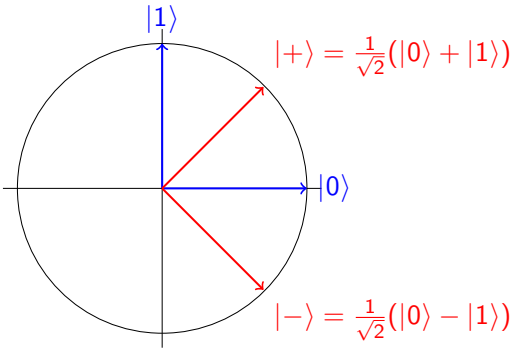
- Computational basis $\rightarrow$
  - Meas. $|0\rangle$, the outcome is 0 w.p. 1
  - Meas. $|1\rangle$, the outcome is 1 w.p. 1
  - Meas. $|+\rangle$, the outcome is 0/1 w.p. 1/2
  - Meas. $|-\rangle$, the outcome is 0/1 w.p. 1/2

Quantum 101 (simplified)

Quantum mechanics

Quantum states | Evolution | Measurements

States



Measurements

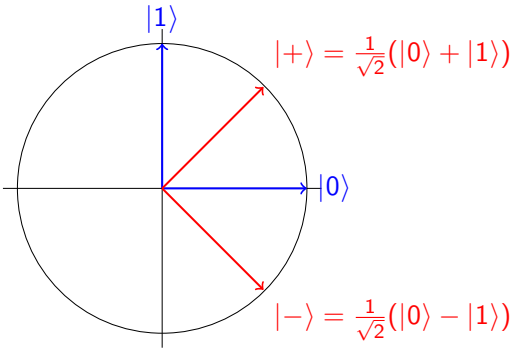
- Computational basis $\rightarrow$
  - Meas. $|0\rangle$, the outcome is 0 w.p. 1
  - Meas. $|1\rangle$, the outcome is 1 w.p. 1
  - Meas. $|+\rangle$, the outcome is 0/1 w.p. 1/2
  - Meas. $|-\rangle$, the outcome is 0/1 w.p. 1/2
- Hadamard basis $\nearrow$

Quantum 101 (simplified)

Quantum mechanics

Quantum states | Evolution | Measurements

States



Measurements

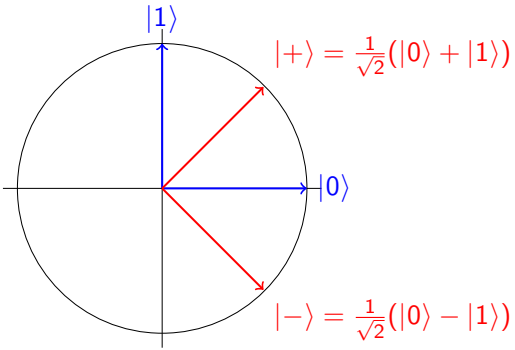
- Computational basis $\rightarrow$
  - Meas. $|0\rangle$, the outcome is 0 w.p. 1
  - Meas. $|1\rangle$, the outcome is 1 w.p. 1
  - Meas. $|+\rangle$, the outcome is 0/1 w.p. 1/2
  - Meas. $|-\rangle$, the outcome is 0/1 w.p. 1/2
- Hadamard basis $\nearrow$
  - Meas. $|0\rangle$, the outcome is $+/-$ w.p. 1/2
  - Meas. $|1\rangle$, the outcome is $+/-$ w.p. 1/2

Quantum 101 (simplified)

Quantum mechanics

Quantum states | Evolution | Measurements

States



Measurements

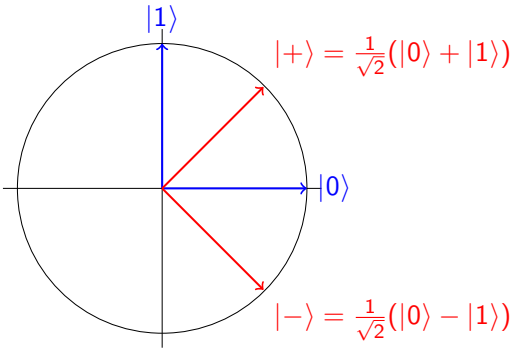
- Computational basis $\rightarrow$
  - Meas. $|0\rangle$, the outcome is 0 w.p. 1
  - Meas. $|1\rangle$, the outcome is 1 w.p. 1
  - Meas. $|+\rangle$, the outcome is 0/1 w.p. 1/2
  - Meas. $|-\rangle$, the outcome is 0/1 w.p. 1/2
- Hadamard basis $\nearrow$
  - Meas. $|0\rangle$, the outcome is $+/-$ w.p. 1/2
  - Meas. $|1\rangle$, the outcome is $+/-$ w.p. 1/2
  - Meas. $|+\rangle$, the outcome is $+$ w.p. 1
  - Meas. $|-\rangle$, the outcome is $-$ w.p. 1

Quantum 101 (simplified)

Quantum mechanics

Quantum states | Evolution | Measurements

States



Measurements

- Computational basis $\rightarrow$
  - Meas. $|0\rangle$, the outcome is 0 w.p. 1
  - Meas. $|1\rangle$, the outcome is 1 w.p. 1
  - Meas. $|+\rangle$, the outcome is 0/1 w.p. 1/2
  - Meas. $|-\rangle$, the outcome is 0/1 w.p. 1/2
- Hadamard basis $\nearrow$
  - Meas. $|0\rangle$, the outcome is $+/-$ w.p. 1/2
  - Meas. $|1\rangle$, the outcome is $+/-$ w.p. 1/2
  - Meas. $|+\rangle$, the outcome is $+$ w.p. 1
  - Meas. $|-\rangle$, the outcome is $-$ w.p. 1

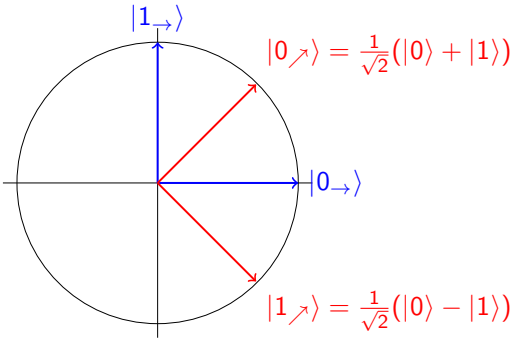
State collapses after measurements

Quantum 101 (simplified)

Quantum mechanics

Quantum states | Evolution | Measurements

States



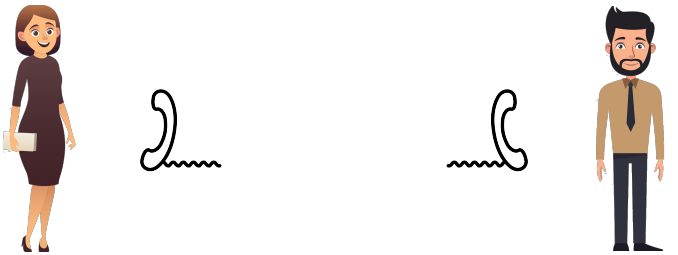
Measurements

- Computational basis $\rightarrow$
  - Meas. $|0\rangle$, the outcome is 0 w.p. 1
  - Meas. $|1\rangle$, the outcome is 1 w.p. 1
  - Meas. $|+\rangle$, the outcome is 0/1 w.p. 1/2
  - Meas. $|-\rangle$, the outcome is 0/1 w.p. 1/2
- Hadamard basis $\nearrow$
  - Meas. $|0\rangle$, the outcome is $+/-$ w.p. 1/2
  - Meas. $|1\rangle$, the outcome is $+/-$ w.p. 1/2
  - Meas. $|+\rangle$, the outcome is $+$ w.p. 1
  - Meas. $|-\rangle$, the outcome is $-$ w.p. 1

State collapses after measurements

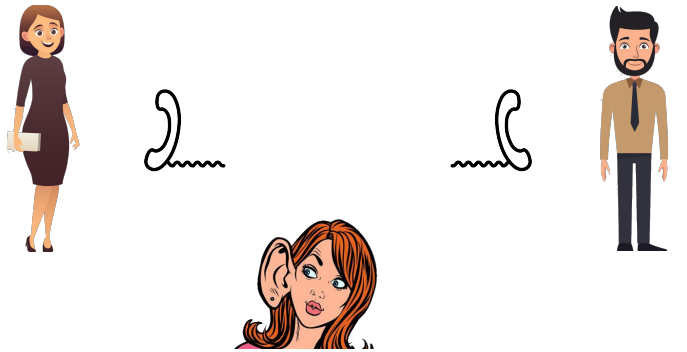
Key agreement

Key agreement



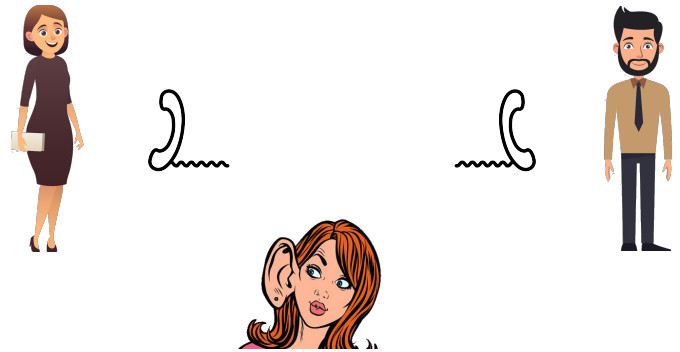
Goal: Alice and Bob want to share a common random key k over the phone

Key agreement



Goal: Alice and Bob want to share a common random key k over the phone
Security: They want k to be unknown to potential eavesdroppers

Key agreement



Goal: Alice and Bob want to share a common random key k over the phone
Security: They want k to be unknown to potential eavesdroppers
Classical information-theoretically secure key agreement is impossible!

Quantum-key distribution (simplified)

Quantum-key distribution (simplified)

Quantum-key distribution (simplified)

	Basis
$\|\phi_1\rangle = \|+\rangle$	$\nearrow$
$\|\phi_2\rangle = \|0\rangle$	$\rightarrow$
$\|\phi_3\rangle = \|1\rangle$	$\rightarrow$
$\|\phi_4\rangle = \|0\rangle$	$\rightarrow$
$\|\phi_5\rangle = \|-\rangle$	$\nearrow$
$\|\phi_6\rangle = \|-\rangle$	$\nearrow$

Quantum-key distribution (simplified)

	Basis
$\|\phi_1\rangle = \|+\rangle$	$\nearrow$
$\|\phi_2\rangle = \|0\rangle$	$\rightarrow$
$\|\phi_3\rangle = \|1\rangle$	$\rightarrow$
$\|\phi_4\rangle = \|0\rangle$	$\rightarrow$
$\|\phi_5\rangle = \|-\rangle$	$\nearrow$
$\|\phi_6\rangle = \|-\rangle$	$\nearrow$

$|+010--\rangle$

Quantum-key distribution (simplified)

	Basis
$\|\phi_1\rangle = \|+\rangle$	$\nearrow$
$\|\phi_2\rangle = \|0\rangle$	$\rightarrow$
$\|\phi_3\rangle = \|1\rangle$	$\rightarrow$
$\|\phi_4\rangle = \|0\rangle$	$\rightarrow$
$\|\phi_5\rangle = \|-\rangle$	$\nearrow$
$\|\phi_6\rangle = \|-\rangle$	$\nearrow$

$|+010--\rangle$

Basis	Outcome
$\nearrow$	$+$
$\nearrow$	$-$
0	1
$\rightarrow$	0
$\rightarrow$	0
$\nearrow$	$-$

Quantum-key distribution (simplified)

	Basis
$\|\phi_1\rangle = \|+\rangle$	$\nearrow$
$\|\phi_2\rangle = \|0\rangle$	$\rightarrow$
$\|\phi_3\rangle = \|1\rangle$	$\rightarrow$
$\|\phi_4\rangle = \|0\rangle$	$\rightarrow$
$\|\phi_5\rangle = \|-\rangle$	$\nearrow$
$\|\phi_6\rangle = \|-\rangle$	$\nearrow$

$|+010--\rangle$

$\nearrow\nearrow\rightarrow\rightarrow\rightarrow\nearrow$

Basis	Outcome
$\nearrow$	$+$
$\nearrow$	$-$
0	1
$\rightarrow$	0
$\rightarrow$	0
$\nearrow$	$-$

Quantum-key distribution (simplified)

	Basis
$\|\phi_1\rangle = \|+\rangle$	$\nearrow$
$\|\phi_2\rangle = \|0\rangle$	$\rightarrow$
$\|\phi_3\rangle = \|1\rangle$	$\rightarrow$
$\|\phi_4\rangle = \|0\rangle$	$\rightarrow$
$\|\phi_5\rangle = \|-\rangle$	$\nearrow$
$\|\phi_6\rangle = \|-\rangle$	$\nearrow$

$|+010--\rangle$

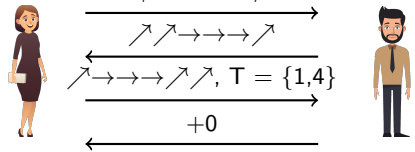
$\nearrow\nearrow\rightarrow\rightarrow\rightarrow\nearrow$

$\nearrow\rightarrow\rightarrow\rightarrow\nearrow\nearrow$, $\mathsf{T} = \{1,4\}$

Basis	Outcome
$\nearrow$	$+$
$\nearrow$	$-$
0	1
$\rightarrow$	0
$\rightarrow$	0
$\nearrow$	$-$

Quantum-key distribution (simplified)

	Basis
$\|\phi_1\rangle = \|+\rangle$	↗
$\|\phi_2\rangle = \|0\rangle$	→
$\|\phi_3\rangle = \|1\rangle$	→
$\|\phi_4\rangle = \|0\rangle$	→
$\|\phi_5\rangle = \|-\rangle$	↗
$\|\phi_6\rangle = \|-\rangle$	↗



Basis	Outcome
↗	+
↗	−
0	1
→	0
→	0
↗	−

Quantum-key distribution (simplified)

	Basis
$\|\phi_1\rangle = \|+\rangle$	$\nearrow$
$\|\phi_2\rangle = \|0\rangle$	$\rightarrow$
$\|\phi_3\rangle = \|1\rangle$	$\rightarrow$
$\|\phi_4\rangle = \|0\rangle$	$\rightarrow$
$\|\phi_5\rangle = \|-\rangle$	$\nearrow$
$\|\phi_6\rangle = \|-\rangle$	$\nearrow$

$|+010--\rangle$

$\nearrow\nearrow\rightarrow\rightarrow\rightarrow\nearrow$

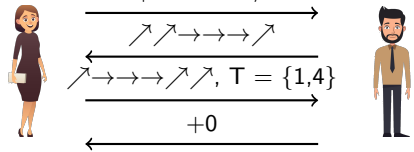
$\nearrow\rightarrow\rightarrow\rightarrow\nearrow\nearrow$, $\mathsf{T} = \{1,4\}$

$+0$

Basis	Outcome
$\nearrow$	$+$
$\nearrow$	$-$
0	1
$\rightarrow$	0
$\rightarrow$	0
$\nearrow$	$-$

Quantum-key distribution (simplified)

	Basis
$\|\phi_1\rangle = \|+\rangle$	$\nearrow$
$\|\phi_2\rangle = \|0\rangle$	$\rightarrow$
$\|\phi_3\rangle = \|1\rangle$	$\rightarrow$
$\|\phi_4\rangle = \|0\rangle$	$\rightarrow$
$\|\phi_5\rangle = \|-\rangle$	$\nearrow$
$\|\phi_6\rangle = \|-\rangle$	$\nearrow$

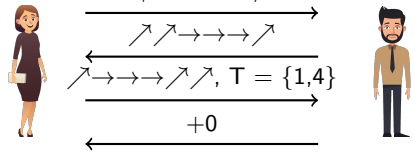


Basis	Outcome
$\nearrow$	+
$\nearrow$	−
0	1
$\rightarrow$	0
$\rightarrow$	0
$\nearrow$	−

Intuitively, if Eve tries to eavesdrop the quantum state, it collapses

Quantum-key distribution (simplified)

	Basis
$\|\phi_1\rangle = \|+\rangle$	↗
$\|\phi_2\rangle = \|0\rangle$	→
$\|\phi_3\rangle = \|1\rangle$	→
$\|\phi_4\rangle = \|0\rangle$	→
$\|\phi_5\rangle = \|-\rangle$	↗
$\|\phi_6\rangle = \|-\rangle$	↗



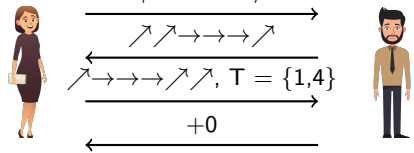
Basis	Outcome
↗	+
↗	−
0	1
→	0
→	0
↗	−

Intuitively, if Eve tries to eavesdrop the quantum state, it collapses

- Complete protocol and formal security proof is more cumbersome

Quantum-key distribution (simplified)

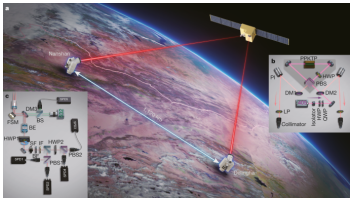
	Basis
$\|\phi_1\rangle = \|+\rangle$	↗
$\|\phi_2\rangle = \|0\rangle$	→
$\|\phi_3\rangle = \|1\rangle$	→
$\|\phi_4\rangle = \|0\rangle$	→
$\|\phi_5\rangle = \|-\rangle$	↗
$\|\phi_6\rangle = \|-\rangle$	↗



Basis	Outcome
↗	+
↗	−
0	1
→	0
→	0
↗	−

Intuitively, if Eve tries to eavesdrop the quantum state, it collapses

- Complete protocol and formal security proof is more cumbersome



Beyond QKD

Beyond QKD

- Can we achieve other protocols such as bit-commitment, MPC,... unconditionally?

Beyond QKD

- Can we achieve other protocols such as bit-commitment, MPC,... unconditionally?
- No! [M'97, LC'97]

Beyond QKD

- Can we achieve other protocols such as bit-commitment, MPC,... unconditionally?
- No! [M'97, LC'97]

What if we use computational assumptions?

Beyond QKD

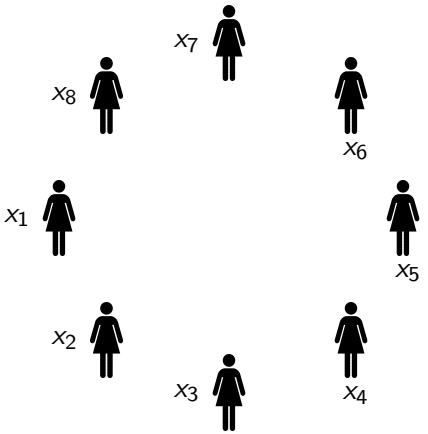
- Can we achieve other protocols such as bit-commitment, MPC,... unconditionally?
- No! [M'97, LC'97]

What if we use computational assumptions?

1. Quantum protocol for multi-party computation from weaker computational assumptions
2. Improving the round complexity of QKD

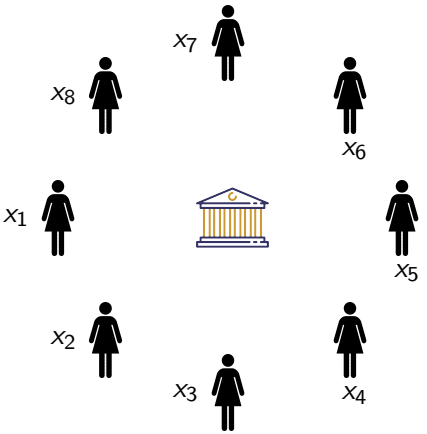
Quantum protocol for multi-party computation from weaker computational assumptions

Multi-party computation



Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

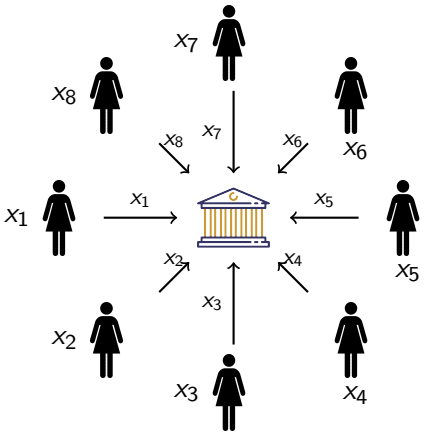
Multi-party computation



Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

Ideal world

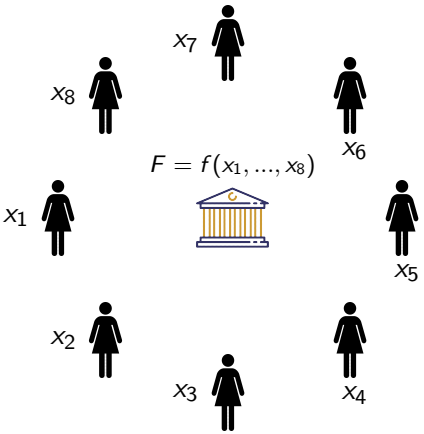
Multi-party computation



Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

Ideal world

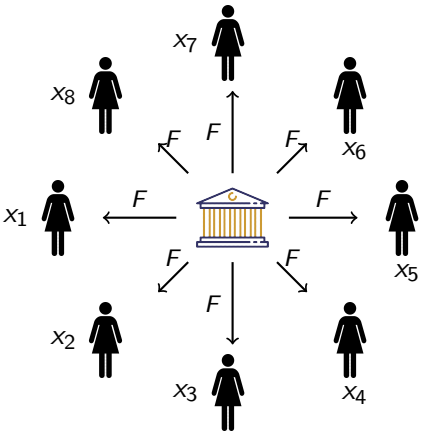
Multi-party computation



Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

Ideal world

Multi-party computation

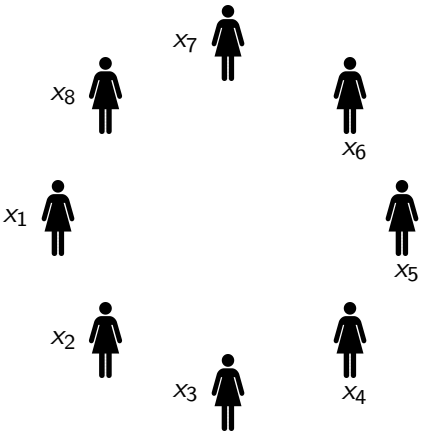


Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

Ideal world

- Each party learns $F = f(x_1, ..., x_8)$ and nothing else

Multi-party computation



Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

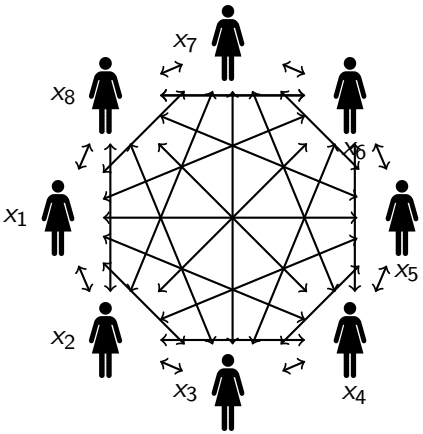
Ideal world

- Each party learns $F = f(x_1, ..., x_8)$ and nothing else

Real world

- Goal: implement the ideal functionality

Multi-party computation



Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

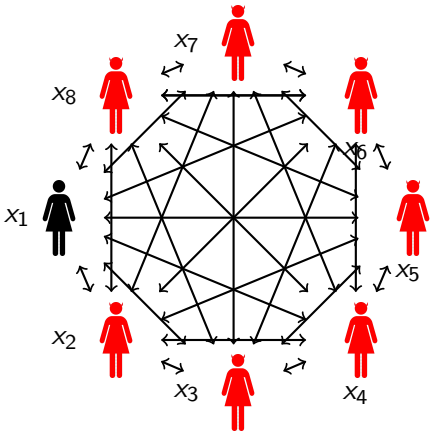
Ideal world

- Each party learns $F = f(x_1, ..., x_8)$ and nothing else

Real world

- Goal: implement the ideal functionality
- Protocols where parties interact, but still they only learn F

Multi-party computation



Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

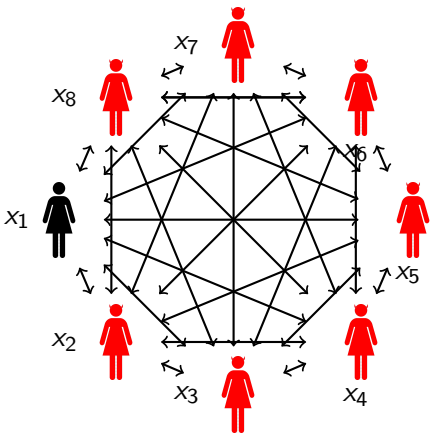
Ideal world

- Each party learns $F = f(x_1, ..., x_8)$ and nothing else

Real world

- Goal: implement the ideal functionality
- Protocols where parties interact, but still they only learn F
- Even if they behave disonestly

Multi-party computation



Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

Ideal world

- Each party learns $F = f(x_1, ..., x_8)$ and nothing else

Real world

- Goal: implement the ideal functionality
- Protocols where parties interact, but still they only learn F
- Even if they behave disonestly

Theorem [MMP'12]

MPC cannot be built from OWF in a black-box way

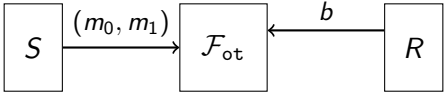
Oblivious transfer

Oblivious transfer

Ideal functionality

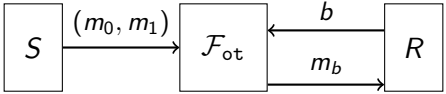
Oblivious transfer

Ideal functionality



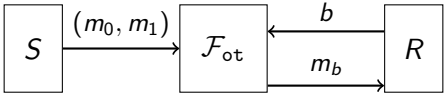
Oblivious transfer

Ideal functionality

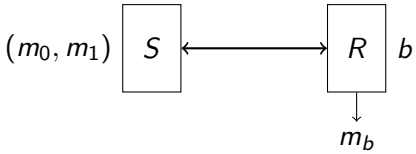


Oblivious transfer

Ideal functionality



Real world



MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$

MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- U'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world

MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- U'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world
- CK'88/BBCS'92: Quantum protocol for OT based on commitment schemes

MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- U'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world
- CK'88/BBCS'92: Quantum protocol for OT based on commitment schemes
- DFLSS'09 BF'10: Security proof of CK/BBCS protocol based on strong classical commitment schemes (likely to lie outside of MiniCrypt)

MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- U'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world
- CK'88/BBCS'92: Quantum protocol for OT based on commitment schemes
- DFLSS'09 BF'10: Security proof of CK/BBCS protocol based on strong classical commitment schemes (likely to lie outside of MiniCrypt)
- BCKM'21 and **G**LSV'21: Quantum protocol for strong commitment from OWF

MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- U'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world
- CK'88/BBCS'92: Quantum protocol for OT based on commitment schemes
- DFLSS'09 BF'10: Security proof of CK/BBCS protocol based on strong classical commitment schemes (likely to lie outside of MiniCrypt)
- BCKM'21 and **G**LSV'21: Quantum protocol for strong commitment from OWF

Corollary

Quantum protocol for MPC from OWF

MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- U'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world
- CK'88/BBCS'92: Quantum protocol for OT based on commitment schemes
- DFLSS'09 BF'10: Security proof of CK/BBCS protocol based on strong classical commitment schemes (likely to lie outside of MiniCrypt)
- BCKM'21 and **G**LSV'21: Quantum protocol for strong commitment from OWF

Corollary

Quantum protocol for MPC from OWF

vs.

Classical protocols require PKE assumptions

MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- U'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world
- CK'88/BBCS'92: Quantum protocol for OT based on commitment schemes
- DFLSS'09 BF'10: Security proof of CK/BBCS protocol based on strong classical commitment schemes (likely to lie outside of MiniCrypt)
- BCKM'21 and **G**LSV'21: Quantum protocol for strong commitment from OWF
- D**G**ILYY'24+IYYL**G**D'25: Implementing quantum OT in the lab

Corollary

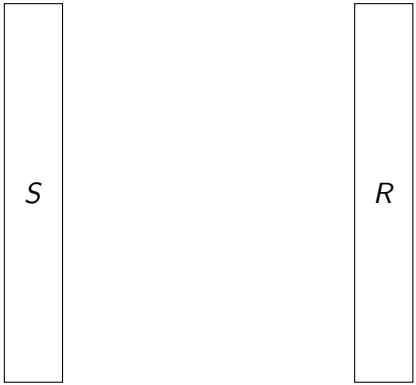
(Practical?) Quantum protocol for MPC from OWF

vs.

Classical protocols require PKE assumptions

CK/BBCS protocol (I)

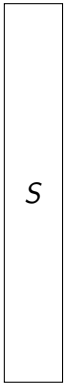
CK/BBCS protocol (I)



CK/BBCS protocol (I)

$\vec{x} \in \{0,1\}^\lambda$

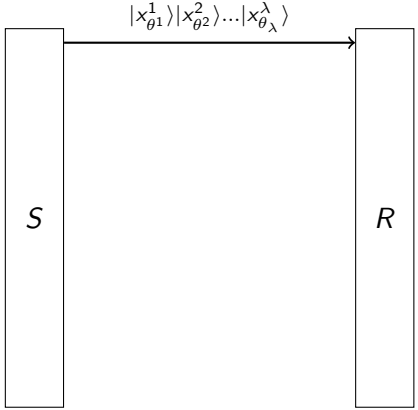
$\vec{\theta} \in \{\rightarrow, \nearrow\}^\lambda$



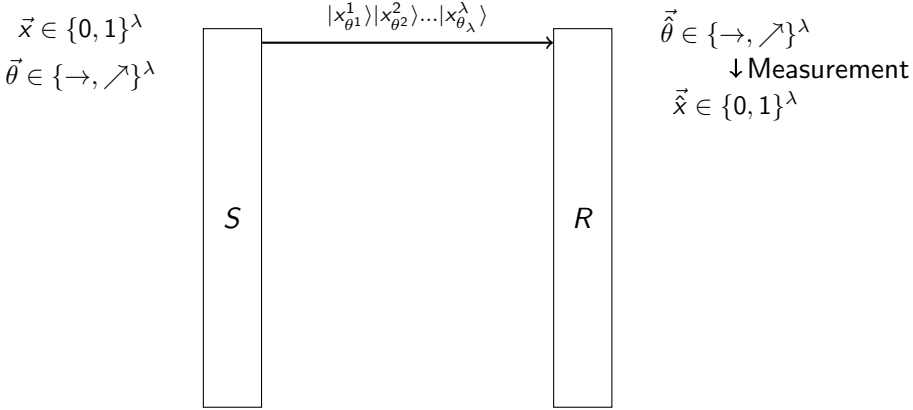
CK/BBCS protocol (I)

$\vec{x} \in \{0,1\}^{\lambda}$

$\vec{\theta} \in \{\rightarrow, \nearrow\}^{\lambda}$



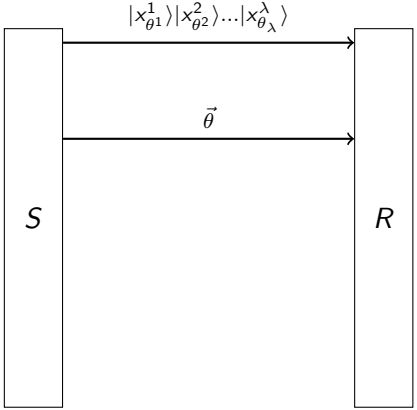
CK/BBCS protocol (I)



CK/BBCS protocol (I)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{\rightarrow, \nearrow\}^\lambda$



$\vec{\hat{\theta}} \in \{\rightarrow, \nearrow\}^\lambda$

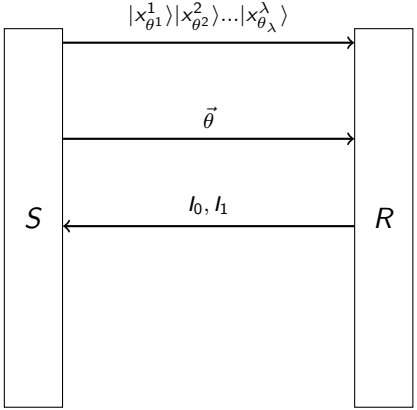
$\downarrow$Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

CK/BBCS protocol (I)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{\rightarrow, \nearrow\}^\lambda$



$\vec{\hat{\theta}} \in \{\rightarrow, \nearrow\}^\lambda$

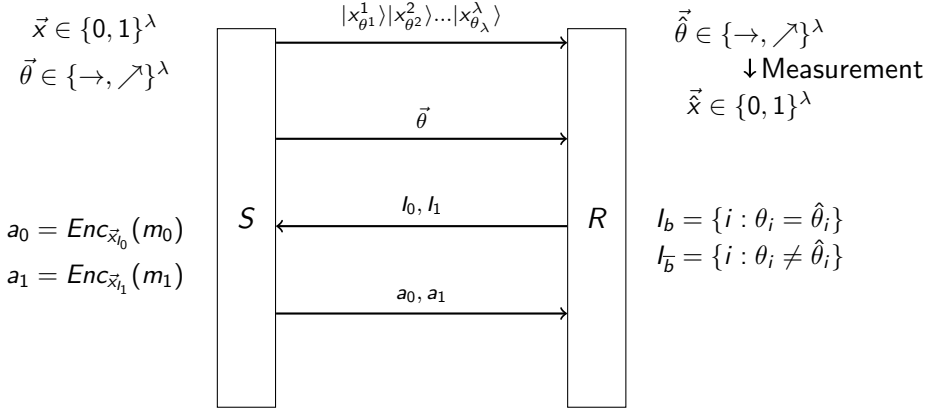
$\downarrow$ Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

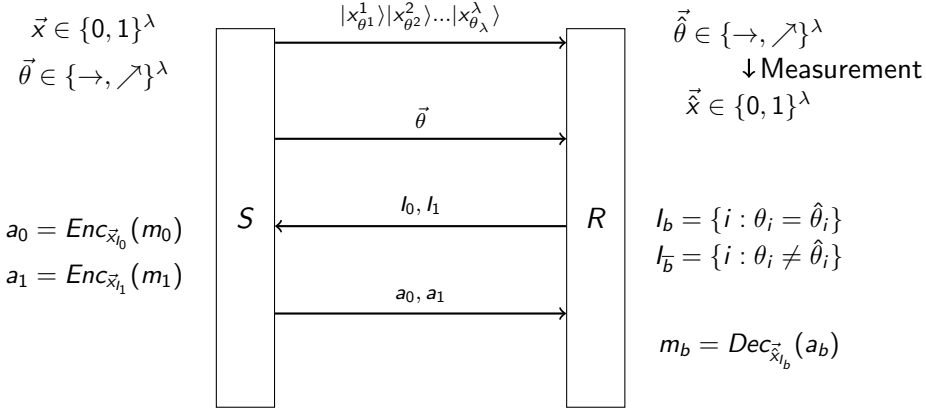
$I_b = \{i : \theta_i = \hat{\theta}_i\}$

$I_{\overline{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

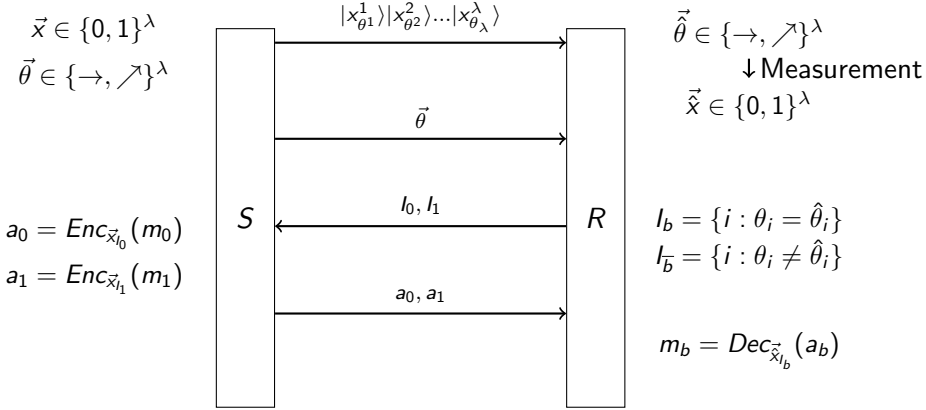
CK/BBCS protocol (I)



CK/BBCS protocol (I)

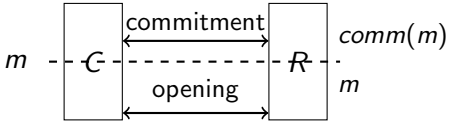


CK/BBCS protocol (I)

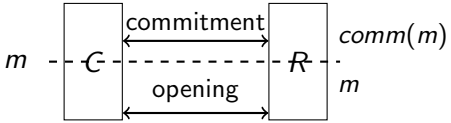


Attack for malicious receiver: $\tilde{R}$ waits $\vec{\theta}$ to measure the qubits using the right basis

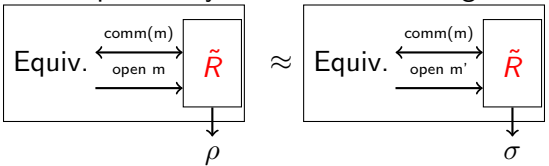
Bit-commitment with simulation security



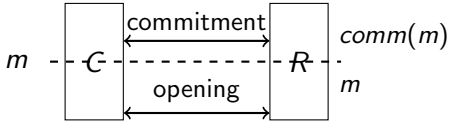
Bit-commitment with simulation security



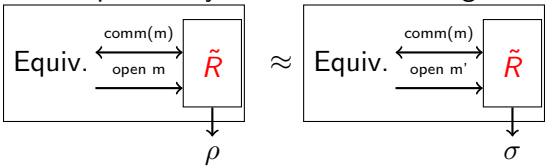
Equivocality: "simulation" hiding



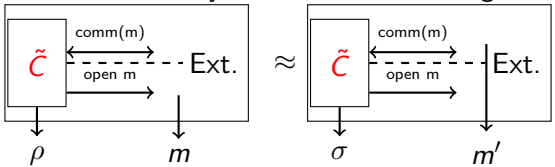
Bit-commitment with simulation security



Equivocality: "simulation" hiding



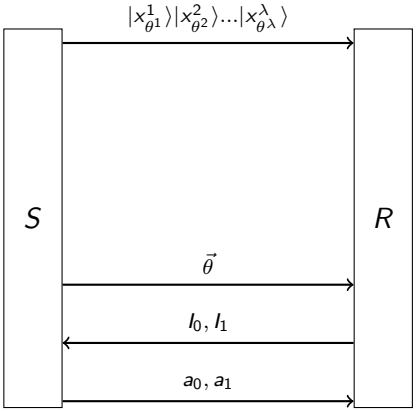
Extractability: "simulation" binding



CK/BBCS protocol (II)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{\rightarrow, \nearrow\}^\lambda$



$\vec{\hat{\theta}} \in \{\rightarrow, \nearrow\}^\lambda$

$\downarrow$ Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

$a_1 = Enc_{\vec{x}_{I_1}}(m_1)$

$I_b = \{i : \theta_i = \hat{\theta}_i\}$

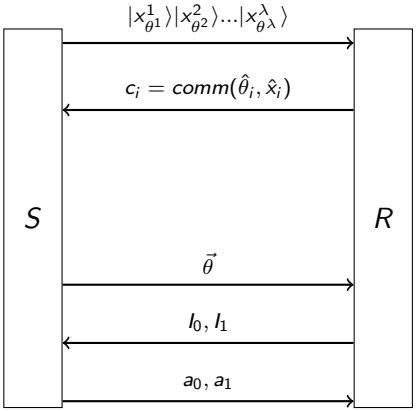
$I_{\overline{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

$m_b = Dec_{\vec{\hat{x}}_{I_b}}(a_b)$

CK/BBCS protocol (II)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{\rightarrow, \nearrow\}^\lambda$



$\vec{\hat{\theta}} \in \{\rightarrow, \nearrow\}^\lambda$

↓Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

$a_1 = Enc_{\vec{x}_{I_1}}(m_1)$

$I_b = \{i : \theta_i = \hat{\theta}_i\}$

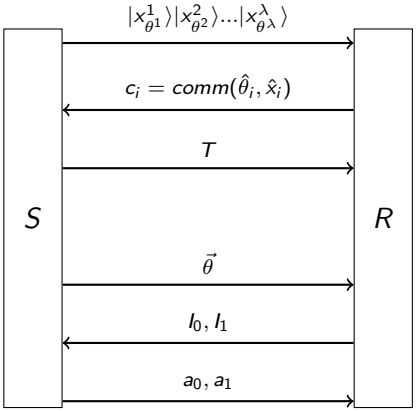
$I_{\overline{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

$m_b = Dec_{\vec{\hat{x}}_{I_b}}(a_b)$

CK/BBCS protocol (II)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{\rightarrow, \nearrow\}^\lambda$



$\vec{\hat{\theta}} \in \{\rightarrow, \nearrow\}^\lambda$

$\downarrow$ Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

$a_1 = Enc_{\vec{x}_{I_1}}(m_1)$

$I_b = \{i : \theta_i = \hat{\theta}_i\}$

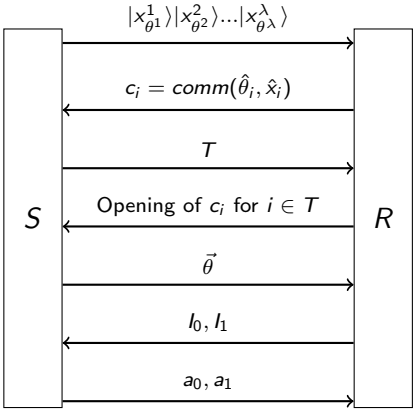
$I_{\overline{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

$m_b = Dec_{\vec{\hat{x}}_{I_b}}(a_b)$

CK/BBCS protocol (II)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{\rightarrow, \nearrow\}^\lambda$



$\vec{\hat{\theta}} \in \{\rightarrow, \nearrow\}^\lambda$

↓Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

$a_1 = Enc_{\vec{x}_{I_1}}(m_1)$

$I_b = \{i : \theta_i = \hat{\theta}_i\}$

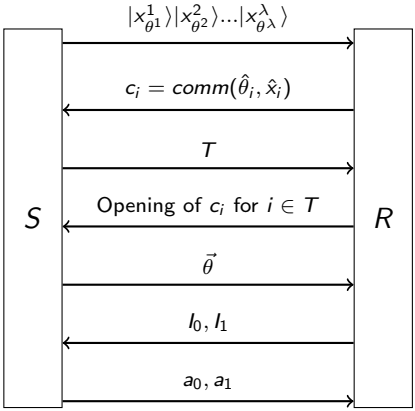
$I_{\overline{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

$m_b = Dec_{\vec{\hat{x}}_{I_b}}(a_b)$

CK/BBCS protocol (II)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{\rightarrow, \nearrow\}^\lambda$



$\vec{\hat{\theta}} \in \{\rightarrow, \nearrow\}^\lambda$

↓Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

check consistency

$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

$a_1 = Enc_{\vec{x}_{I_1}}(m_1)$

$I_b = \{i : \theta_i = \hat{\theta}_i\}$

$I_{\overline{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

$m_b = Dec_{\vec{\hat{x}}_{I_b}}(a_b)$

CK/BBCS protocol (II)

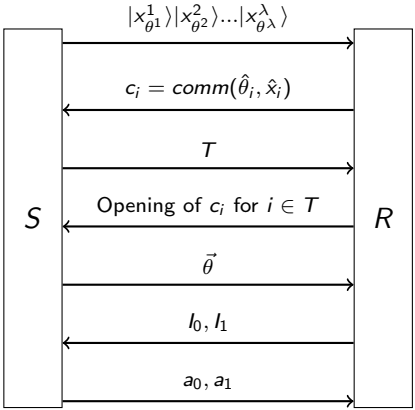
$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{\rightarrow, \nearrow\}^\lambda$

check consistency

$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

$a_1 = Enc_{\vec{x}_{I_1}}(m_1)$



$\vec{\hat{\theta}} \in \{\rightarrow, \nearrow\}^\lambda$

↓Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

$I_b = \{i : \theta_i = \hat{\theta}_i\} \setminus T$

$I_{\overline{b}} = \{i : \theta_i \neq \hat{\theta}_i\} \setminus T$

$m_b = Dec_{\vec{\hat{x}}_{I_b}}(a_b)$

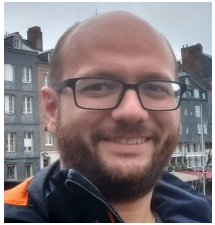
Implemententing commitment scheme with simulation security from OWF

Implemententing commitment scheme with simulation security from OWF

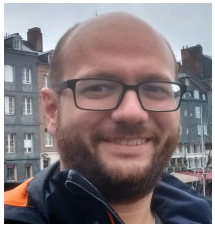
[BCKM21]	[GLSV21]
1. (Black-box) equivocality compiler	1. Equivocal commitment from Naor's commitment and zero-knowledge
2. Extractable commitment from equivocal commitment and quantum communication	2. Unbounded-simulator OT from equivocal commitment
	3. Extractable and equivocal commitment from unbounded-simulator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

Features:

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

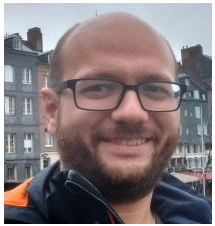


We have a protocol that only uses BB84 states.



We have a protocol that only uses BB84 states.

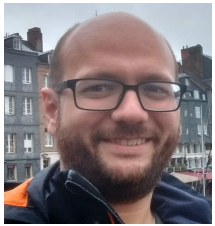
Great, let's implement it!



We have a protocol that only uses BB84 states.

Great, let's implement it!

How much noise you can tolerate?

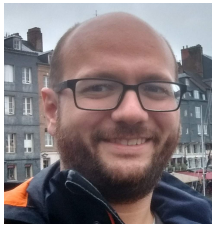


We have a protocol that only uses BB84 states.

Great, let's implement it!

How much noise you can tolerate?

No noise



We have a protocol that only uses BB84 states.

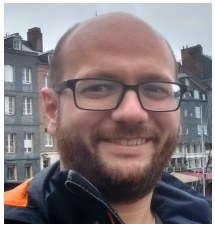
Great, let's implement it!

How much noise you can tolerate?

No noise

Hmmm.. OK.

How many states do you need to send?



We have a protocol that only uses BB84 states.

Great, let's implement it!

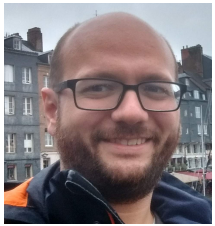
How much noise you can tolerate?

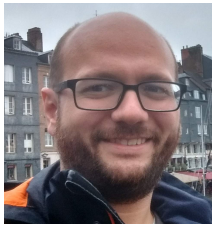
No noise

Hmmm.. OK.

How many states do you need to send?

poly(λ)





We have a protocol that only uses BB84 states.

Great, let's implement it!

How much noise you can tolerate?

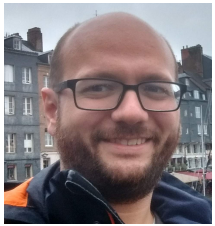
No noise

Hmmm.. OK.

How many states do you need to send?

poly(λ)

What is λ?



We have a protocol that only uses BB84 states.

Great, let's implement it!

How much noise you can tolerate?

No noise

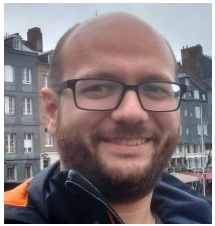
Hmmm.. OK.

How many states do you need to send?

poly(λ)

What is λ?

The security parameter.



We have a protocol that only uses BB84 states.

Great, let's implement it!

How much noise you can tolerate?

No noise

Hmmm.. OK.

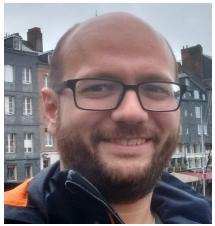
How many states do you need to send?

poly(λ)

What is λ?

The security parameter.

How many bits of security do you achieve?



We have a protocol that only uses BB84 states.

Great, let's implement it!

How much noise you can tolerate?

No noise

Hmmm.. OK.

How many states do you need to send?

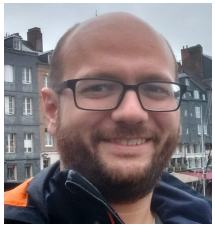
poly(λ)

What is λ?

The security parameter.

How many bits of security do you achieve?

poly(λ)



We have a protocol that only uses BB84 states.

Great, let's implement it!

How much noise you can tolerate?

No noise

Hmmm.. OK.

How many states do you need to send?

poly(λ)

What is λ?

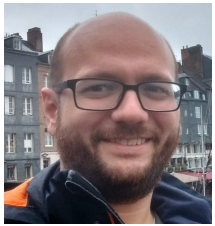
The security parameter.

How many bits of security do you achieve?

poly(λ)

This λ again...

And the classical post-processing?



We have a protocol that only uses BB84 states.

Great, let's implement it!

How much noise you can tolerate?

No noise

Hmmm.. OK.

How many states do you need to send?

poly(λ)

What is λ?

The security parameter.

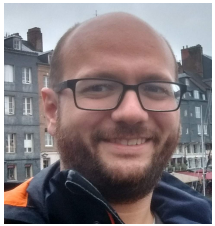
How many bits of security do you achieve?

poly(λ)

This λ again...

And the classical post-processing?

No idea how to implement it.



We have a protocol that only uses BB84 states.

Great, let's implement it!

How much noise you can tolerate?

No noise

Hmmm.. OK.

How many states do you need to send?

poly(λ)

What is λ?

The security parameter.

How many bits of security do you achieve?

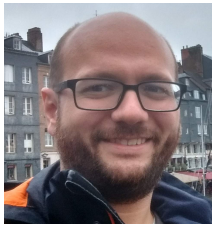
poly(λ)

This λ again...

And the classical post-processing?

No idea how to implement it.

...



We have a protocol that only uses BB84 states.

Great, let's implement it!

How much noise you can tolerate?

No noise

Hmmm.. OK.

How many states do you need to send?

poly(λ)

What is λ?

The security parameter.

How many bits of security do you achieve?

poly(λ)

This λ again...

And the classical post-processing?

No idea how to implement it.

...

...

Practical OT from OWF

- Difficulties in implementation
  - Fragility against errors
  - Practical hash functions and zero knowledge proofs
  - Inefficiency

Practical OT from OWF

- Difficulties in implementation
  - Fragility against errors
  - Practical hash functions and zero knowledge proofs
  - Inefficiency

Practical protocol [D**G**ILYY'24] $\leftrightarrow$ Experimental implementation [IYYL**G**D'24 – on-going]

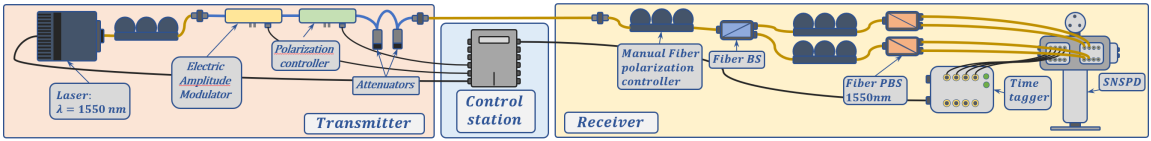
Practical OT from OWF

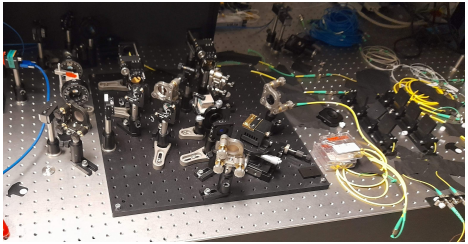
- Difficulties in implementation
  - Fragility against errors
  - Practical hash functions and zero knowledge proofs
  - Inefficiency

Practical protocol [D**G**ILYY'24] $\leftrightarrow$ Experimental implementation [IYYL**G**D'24 – on-going]

	BCKM21 numerical analysis	**DGILYY24 implementation profiling**
N_{BB84}	$1.7 \cdot 10^{13}$	$2.1 \cdot 10^{6}$
N_{RNG}	$1.3 \cdot 10^{16}$	$1.5 \cdot 10^{9}$
N_{PRG}	$6.6 \cdot 10^{15}$	$1.7 \cdot 10^{7}$
M_{seed}	$8.5 \cdot 10^{17}$ *bytes*	$2.5 \cdot 10^{10}$ *bytes*
$T_{acqBB84}$	197 *days*	2.1 *s*
T_{exec}	–	13 *min* 5 *s*

Implementation





Improving the round complexity of QKD

Number of rounds in QKD

Number of rounds in QKD

QKD

- quantum communication: technologically challenging but round-efficient
- classical post-processing: at best, 2 extra rounds
  1. sifting
  2. error correction
  3. privacy amplification

Number of rounds in QKD

QKD

- quantum communication: technologically challenging but round-efficient
- classical post-processing: at best, 2 extra rounds
  1. sifting
  2. error correction
  3. privacy amplification

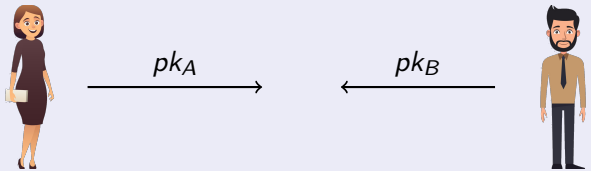
DH Key exchange

Number of rounds in QKD

QKD

- quantum communication: technologically challenging but round-efficient
- classical post-processing: at best, 2 extra rounds
  1. sifting
  2. error correction
  3. privacy amplification

DH Key exchange



Is it possible to improve the round complexity of QKD?

- 1-round QKD is impossible information theoretically

Is it possible to improve the round complexity of QKD?

- 1-round QKD is impossible information theoretically
- 1-round QKD is possible with OWF [MW'24,KMNY'24]

Is it possible to improve the round complexity of QKD?

- 1-round QKD is impossible information theoretically
- 1-round QKD is possible with OWF [MW'24,KMNY'24]
  - Need quantum computers...

Is it possible to improve the round complexity of QKD?

- 1-round QKD is impossible information theoretically
- 1-round QKD is possible with OWF [MW'24,KMNY'24]
  - Need quantum computers...

Our results [GMWK'25]

QKD with simultaneous messages and simple quantum states

Is it possible to improve the round complexity of QKD?

- 1-round QKD is impossible information theoretically
- 1-round QKD is possible with OWF [MW'24,KMNY'24]
  - Need quantum computers...

Our results [GMWK'25]

QKD with simultaneous messages and simple quantum states

- Cryptographic assumption: classical KA

Is it possible to improve the round complexity of QKD?

- 1-round QKD is impossible information theoretically
- 1-round QKD is possible with OWF [MW'24,KMNY'24]
  - Need quantum computers...

Our results [**G**MWK'25]

QKD with simultaneous messages and simple quantum states

- Cryptographic assumption: classical KA
- Everlasting security

Is it possible to improve the round complexity of QKD?

- 1-round QKD is impossible information theoretically
- 1-round QKD is possible with OWF [MW'24,KMNY'24]
  - Need quantum computers...

Our results [**G**MWK'25]

QKD with simultaneous messages and simple quantum states

- Cryptographic assumption: classical KA
- Everlasting security
  - Online phase: attacker is computationally bounded

Is it possible to improve the round complexity of QKD?

- 1-round QKD is impossible information theoretically
- 1-round QKD is possible with OWF [MW'24,KMNY'24]
  - Need quantum computers...

Our results [**G**MWK'25]

QKD with simultaneous messages and simple quantum states

- Cryptographic assumption: classical KA
- Everlasting security
  - Online phase: attacker is computationally bounded
  - Offline phase: attacker is unbounded

Is it possible to improve the round complexity of QKD?

- 1-round QKD is impossible information theoretically
- 1-round QKD is possible with OWF [MW'24,KMNY'24]
  - Need quantum computers...

Our results [**G**MWK'25]

QKD with simultaneous messages and simple quantum states

- Cryptographic assumption: classical KA
- Everlasting security
  - Online phase: attacker is computationally bounded
  - Offline phase: attacker is unbounded
- Search security

Is it possible to improve the round complexity of QKD?

- 1-round QKD is impossible information theoretically
- 1-round QKD is possible with OWF [MW'24,KMNY'24]
  - Need quantum computers...

Our results [**G**MWK'25]

QKD with simultaneous messages and simple quantum states

- Cryptographic assumption: classical KA
- Everlasting security
  - Online phase: attacker is computationally bounded
  - Offline phase: attacker is unbounded
- Search security
  - extra round of simultaneous messages to have indistinguishability security

Our protocol

EPR pairs

Our protocol

EPR pairs

- Entanglement: quantum states that cannot be seen “individually”

Our protocol

EPR pairs

- Entanglement: quantum states that cannot be seen "individually"
- EPR pair $\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$

Our protocol

EPR pairs

- Entanglement: quantum states that cannot be seen "individually"
- EPR pair $\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$
  - If A and B measure in *any* basis, they both have perfect correlation

Our protocol

EPR pairs

- Entanglement: quantum states that cannot be seen "individually"
- EPR pair $\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$
  - If A and B measure in *any* basis, they both have perfect correlation
  - Outcome is perfectly random

Our protocol

EPR pairs

- Entanglement: quantum states that cannot be seen "individually"
- EPR pair $\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$
  - If A and B measure in *any* basis, they both have perfect correlation
  - Outcome is perfectly random
  - Source of quantum spookyness

Our protocol

EPR pairs

- Entanglement: quantum states that cannot be seen "individually"
- EPR pair $\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$
  - If A and B measure in *any* basis, they both have perfect correlation
  - Outcome is perfectly random
  - Source of quantum spookyness

Protocol

Our protocol

EPR pairs

- Entanglement: quantum states that cannot be seen "individually"
- EPR pair $\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$
  - If A and B measure in *any* basis, they both have perfect correlation
  - Outcome is perfectly random
  - Source of quantum spookyness

Protocol

1. Alice and Bob perform classical KA

Our protocol

EPR pairs

- Entanglement: quantum states that cannot be seen "individually"
- EPR pair $\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$
  - If A and B measure in *any* basis, they both have perfect correlation
  - Outcome is perfectly random
  - Source of quantum spookyness

Protocol

1. Alice and Bob perform classical KA
2. In parallel, Alice sends halves of EPR pairs to Bob

Our protocol

EPR pairs

- Entanglement: quantum states that cannot be seen "individually"
- EPR pair $\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$
  - If A and B measure in *any* basis, they both have perfect correlation
  - Outcome is perfectly random
  - Source of quantum spookyness

Protocol

1. Alice and Bob perform classical KA
2. In parallel, Alice sends halves of EPR pairs to Bob
3. Classically shared key is used for choosing the basis measurement of the EPR pair

QKD with simultaneous messages

- Correctness comes from the properties of EPR pairs

QKD with simultaneous messages

- Correctness comes from the properties of EPR pairs
- Security: reduction to attack to classical KA

QKD with simultaneous messages

- Correctness comes from the properties of EPR pairs
- Security: reduction to attack to classical KA
  - Challenge: offline attacker cannot be run in the reduction

QKD with simultaneous messages

- Correctness comes from the properties of EPR pairs
- Security: reduction to attack to classical KA
  - Challenge: offline attacker cannot be run in the reduction
  - Offline attacker characterizes the structure of the entanglement shared between Alice, Bob and Eve

QKD with simultaneous messages

- Correctness comes from the properties of EPR pairs
- Security: reduction to attack to classical KA
  - Challenge: offline attacker cannot be run in the reduction
  - Offline attacker characterizes the structure of the entanglement shared between Alice, Bob and Eve
  - Alice and Bob's quantum state in the offline phase is sufficient for breaking classical KA

Conclusions and open questions

Conclusions and open questions

- Quantum resources + post-quantum cryptography has a lot of potential (at least in theory)

Conclusions and open questions

- Quantum resources + post-quantum cryptography has a lot of potential (at least in theory)

- More practical protocols?
- New impossibility results?
- Simultaneous messages KA with everlasting security?

Conclusions and open questions

- Quantum resources + post-quantum cryptography has a lot of potential (at least in theory)

- More practical protocols?
- New impossibility results?
- Simultaneous messages KA with everlasting security?

Thank you for your attention!