Zero-knowledge and multi-party (quantum) computation in the quantum world

Alex Bredariol Grilo

Primitives

Public-key encryption

Functional encryption

Oblivious transfer

indistinguishable Obfuscation

Secret-key encryption

Two-party computation

Witness encryption

Multi-party computation

One-way functions

Pseudo-random number generators

Zero-knowledge proof systems

How to propose implementations and prove their security?

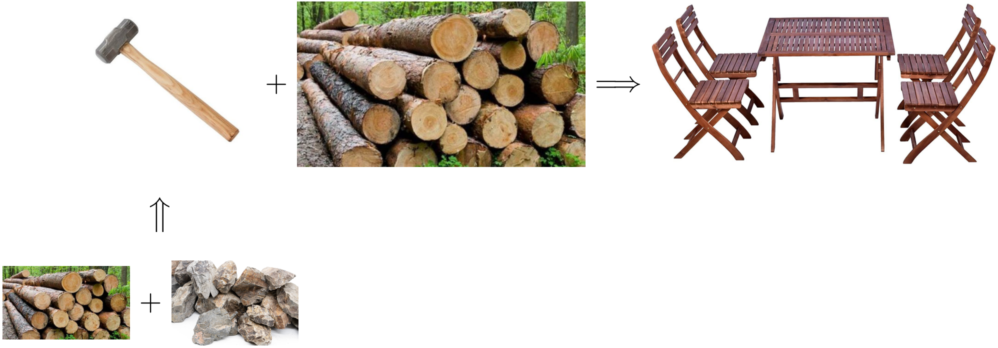
Reductions

Reductions

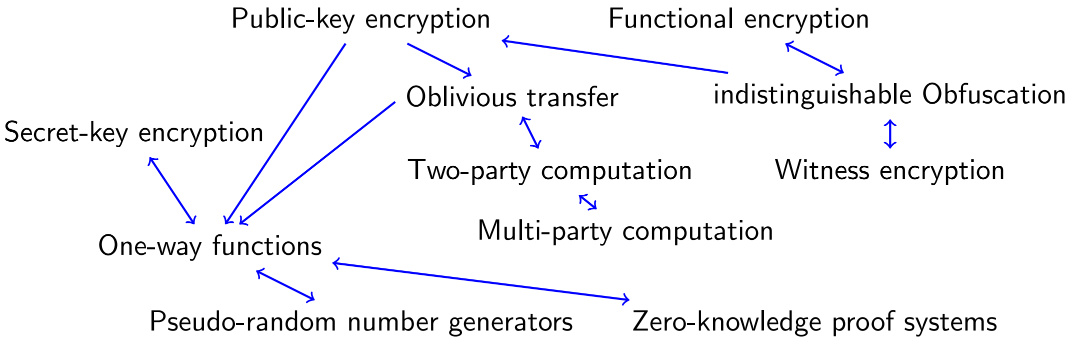
$+$

$\Longrightarrow$

Reductions



Primitives



Public-key encryption

Functional encryption

Oblivious transfer

indistinguishable Obfuscation

Secret-key encryption

Two-party computation

Witness encryption

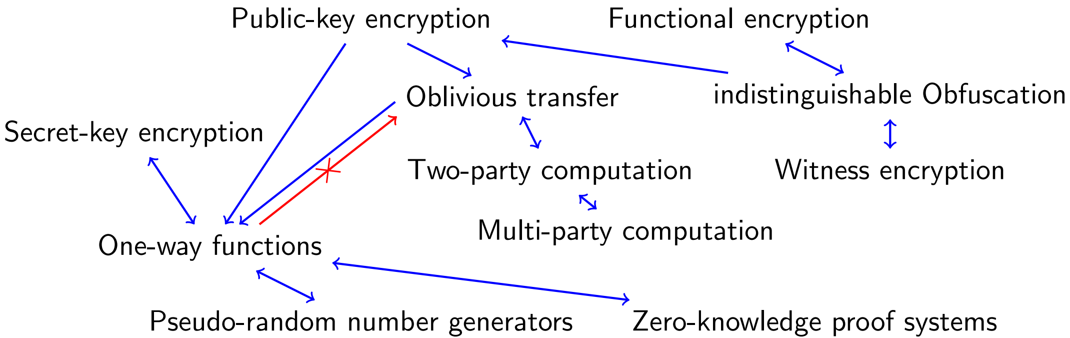
Multi-party computation

One-way functions

Pseudo-random number generators

Zero-knowledge proof systems

Primitives



Public-key encryption

Functional encryption

Oblivious transfer

indistinguishable Obfuscation

Secret-key encryption

Two-party computation

Witness encryption

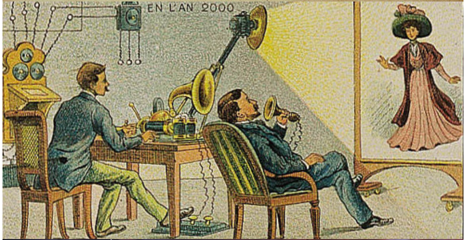
Multi-party computation

One-way functions

Pseudo-random number generators

Zero-knowledge proof systems

Minicrypt: OWFs exist



Cryptomania: PKE schemes exist

Obfutopia: iO exists

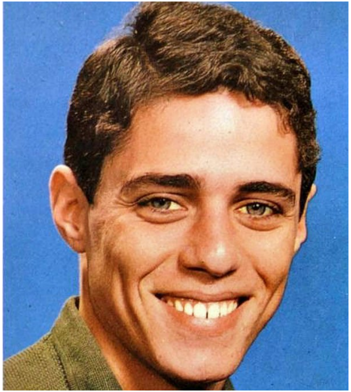
… if crypto is possible

Algorithmica(+Heuristica): We can solve NP (in practice)

Pessiland: We cannot solve NP and OWFs do not exist

How do quantum resources affect these reductions/worlds?

How do quantum resources affect these reductions/worlds?



Quantum helps honest parties

How do quantum resources affect these reductions/worlds?

Quantum helps honest parties

Quantum helps malicious parties

How do quantum resources affect these reductions/worlds?

Quantum helps honest parties

Quantum helps malicious parties

What are the minimal assumptions for quantum functionalities?

ZK and MPC in the quantum world

ZK and MPC in the quantum world

Zero-knowledge proofs

Central tool in crypto toolbox

ZK and MPC in the quantum world

Zero-knowledge proofs
Central tool in crypto toolbox

Multi-party computation
Most-general functionality (modulo #rounds)

ZK and MPC in the quantum world

Zero-knowledge proofs

Central tool in crypto toolbox

1. ZK for NP in MiniCrypt
2. ZK against quantum adversaries
3. ZK for QMA (“quantum NP”)

Multi-party computation

Most-general functionality (modulo #rounds)

ZK and MPC in the quantum world

Zero-knowledge proofs

Central tool in crypto toolbox

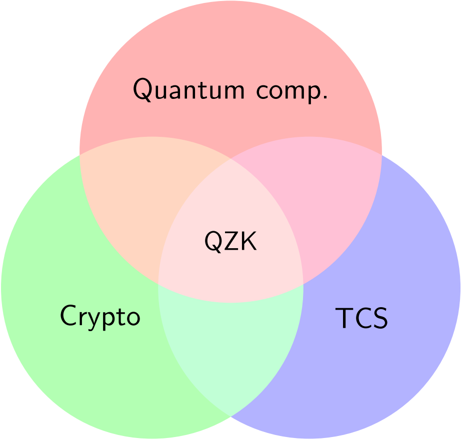
1. ZK for NP in MiniCrypt
2. ZK against quantum adversaries
3. ZK for QMA ("quantum NP")

Multi-party computation

Most-general functionality (modulo #rounds)

1. MPC from Oblivious transfer
2. OT is in Mini**Q**Crypt
3. Multi-party quantum computation

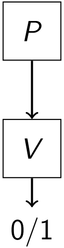
Zero-knowledge in the quantum world


Quantum comp.
QZK
Crypto
TCS

Interactive proofs

Interactive proofs

$L \in \mathrm{NP}$



P

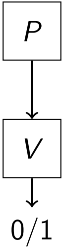
V

$0/1$

for $x \in L$, $\exists P$
V accepts
for $x \notin L$, $\forall P$
V rejects

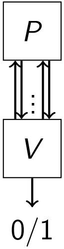
Interactive proofs

$L \in \mathrm{NP}$



for $x \in L$, $\exists P$
V accepts
for $x \notin L$, $\forall P$
V rejects

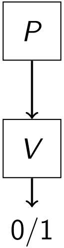
$L \in \mathrm{IP}$



for $x \in L$, $\exists P$
V accepts
for $x \notin L$, $\forall P$
V rejects whp

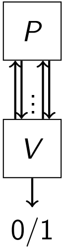
Interactive proofs

$L \in \mathrm{NP}$



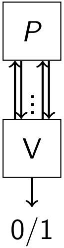
for $x \in L$, $\exists P$
V accepts
for $x \notin L$, $\forall P$
V rejects

$L \in \mathrm{IP} = \mathrm{PSPACE}$



for $x \in L$, $\exists P$
V accepts
for $x \notin L$, $\forall P$
V rejects whp

Zero-knowledge

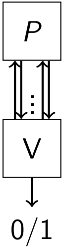


$L \in \mathrm{IP}$

for $x \in L$, $\exists P$
V accepts

for $x \notin L$, $\forall P$
V rejects whp

Zero-knowledge



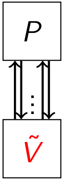
$L \in \mathsf{ZK}$

for $x \in L$, $\exists P$
V accepts

for $x \notin L$, $\forall P$
V rejects whp

Zero-knowledge: V "learns nothing" when $x \in L$

Zero-knowledge



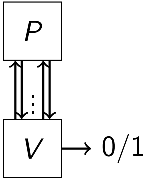
$L \in$ ZK

for $x \in L$, $\exists P$
V accepts

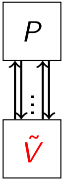
for $x \notin L$, $\forall P$
V rejects whp

Zero-knowledge: $\tilde{V}$ "learns nothing" when $x \in L$

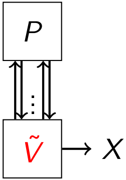
Zero-knowledge



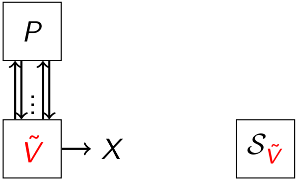
Zero-knowledge



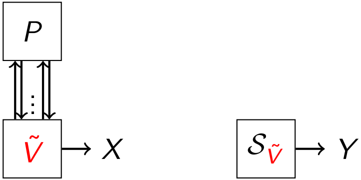
Zero-knowledge



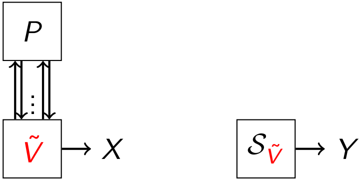
Zero-knowledge



Zero-knowledge



Zero-knowledge

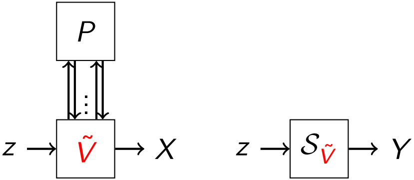


Zero-knowledge property: X is indistinguishable from Y

(**Computational**) ZK: No **efficient distinguishers** for the distributions

$$\forall \text{ poly-time } \mathcal{A} : |Pr_{x \sim X}[\mathcal{A}(x) = 1] - Pr_{y \sim Y}[\mathcal{A}(y) = 1]| \leq negl(n)$$

Zero-knowledge

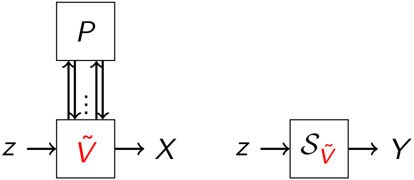


Zero-knowledge property: X is indistinguishable from Y

(**Computational**) ZK: $\forall z$, No **efficient distinguishers** for the distributions

$$\forall \text{ poly-time } \mathcal{A} : |Pr_{x \sim X}[\mathcal{A}(x) = 1] - Pr_{y \sim Y}[\mathcal{A}(y) = 1]| \leq negl(n)$$

Zero-knowledge



Zero-knowledge property: X is indistinguishable from Y

(**Computational**) ZK: $\forall z$, No **efficient distinguishers** for the distributions

$$\forall \text{ poly-time } \mathcal{A} : |Pr_{x \sim X}[\mathcal{A}(x) = 1] - Pr_{y \sim Y}[\mathcal{A}(y) = 1]| \leq negl(n)$$

Statistical ZK: $\forall z$, Distribution X is **statistically close** to distribution Y
Perfect ZK: $\forall z$, Distribution X **=** distribution Y

ZK: bread-and-butter of cryptography

- **Applications:** authentication schemes, building block of several cryptographic compilers, blockchains,...

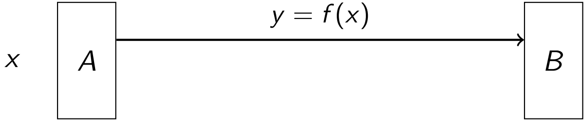
ZK: bread-and-butter of cryptography

- **Applications:** authentication schemes, building block of several cryptographic compilers, blockchains,...
- Example:

x A B

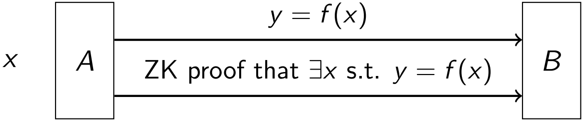
ZK: bread-and-butter of cryptography

- **Applications:** authentication schemes, building block of several cryptographic compilers, blockchains,...
- Example:



ZK: bread-and-butter of cryptography

- **Applications:** authentication schemes, building block of several cryptographic compilers, blockchains,...
- Example:



x

A

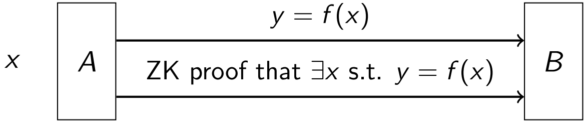
$y = f(x)$

ZK proof that $\exists x$ s.t. $y = f(x)$

B

ZK: bread-and-butter of cryptography

- **Applications:** authentication schemes, building block of several cryptographic compilers, blockchains,…
- Example:



x

A

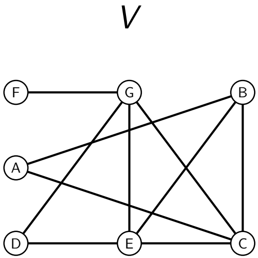
$y = f(x)$

ZK proof that $\exists x$ s.t. $y = f(x)$

B

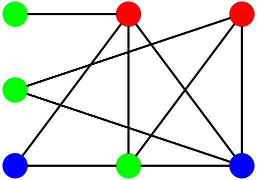
- Zero-knowledge protocols for problems in NP
  - ZK proof of 3-coloring

ZK proof for 3-coloring: attempt 1

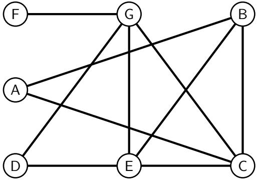


ZK proof for 3-coloring: attempt 1

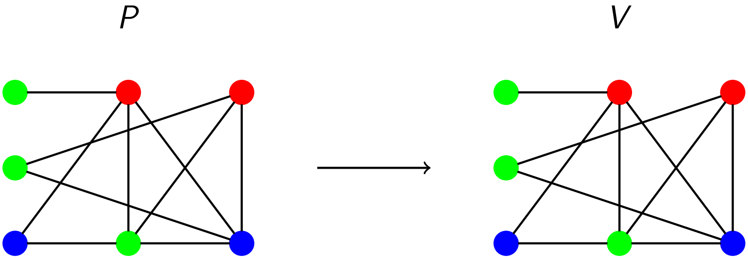
P



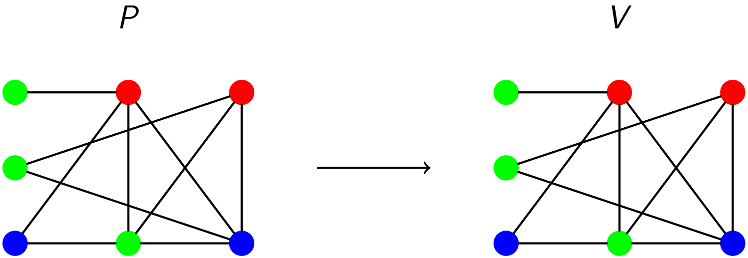
V



ZK proof for 3-coloring: attempt 1



ZK proof for 3-coloring: attempt 1



Completeness ✓ Soundness ✓ ZK ✗

Bit-commitment

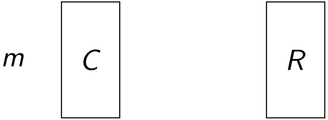
"Cryptographic safe"

C

R

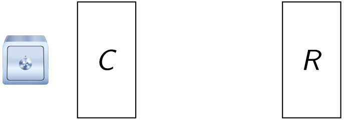
Bit-commitment

"Cryptographic safe"



Bit-commitment

"Cryptographic safe"

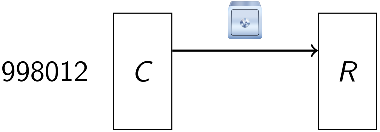


C

R

Bit-commitment

“Cryptographic safe”

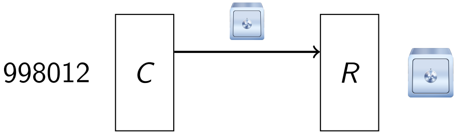


998012

C

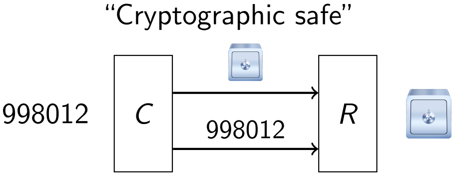
R

Bit-commitment



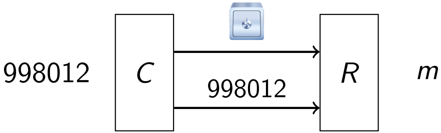
“Cryptographic safe”

Bit-commitment



Bit-commitment

“Cryptographic safe”



998012

C

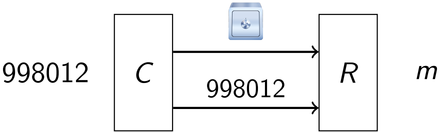
998012

R

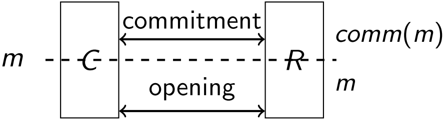
m

Bit-commitment

“Cryptographic safe”

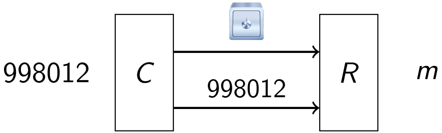


More concretely...



Bit-commitment

"Cryptographic safe"



998012

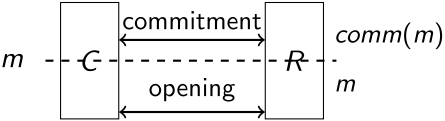
C

998012

R

m

More concretely...



m

C

commitment

opening

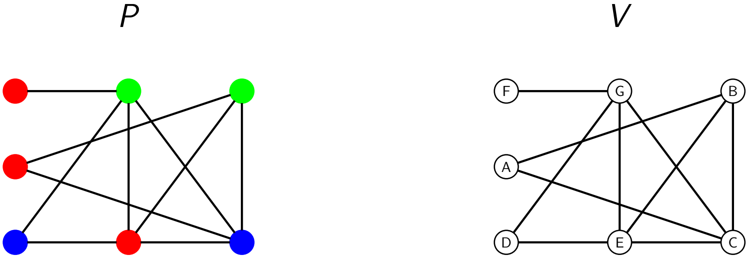
R

$comm(m)$

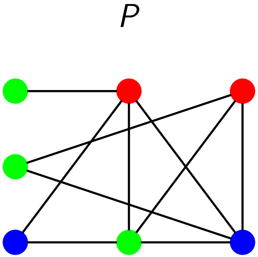
m

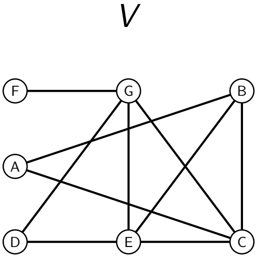
Hiding: R cannot learn m from $comm(m)$
Binding: C cannot successfully open $comm(m)$ to a message $m' \neq m$

ZK proof for 3-coloring: GMW'91

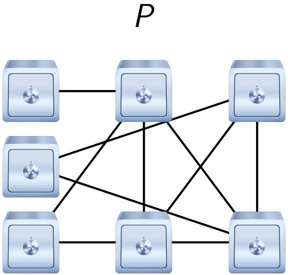


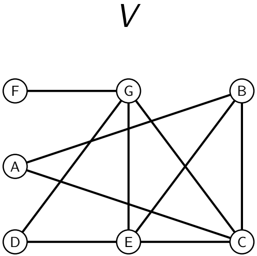
ZK proof for 3-coloring: GMW'91





ZK proof for 3-coloring: GMW'91



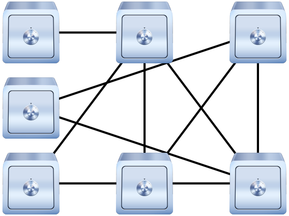


ZK proof for 3-coloring: GMW'91

P

$A \to 564651$
$B \to 867132$
$C \to 984565$
$D \to 894102$
$E \to 069732$
$F \to 873210$
$G \to 897966$

V

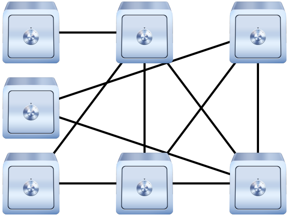


ZK proof for 3-coloring: GMW'91

P

$A \rightarrow$ 564651
$B \rightarrow$ 867132
$C \rightarrow$ 984565
$D \rightarrow$ 894102
$E \rightarrow$ 069732
$F \rightarrow$ 873210
$G \rightarrow$ 897966

V



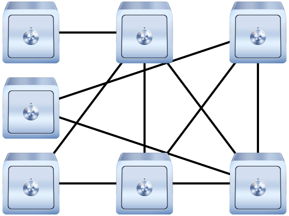
ZK proof for 3-coloring: GMW'91

P

$A \to 564651$
$B \to 867132$
$C \to 984565$
$D \to 894102$
$E \to 069732$
$F \to 873210$
$G \to 897966$

$\xleftarrow{\{A, C\}}$

V



ZK proof for 3-coloring: GMW'91

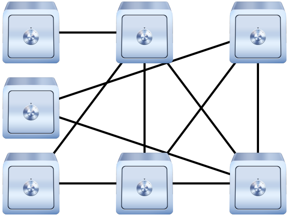
P

$A \to 564651$
$B \to 867132$
$C \to 984565$
$D \to 894102$
$E \to 069732$
$F \to 873210$
$G \to 897966$

$\xleftarrow{\quad \{A, C\} \quad}$

$\xrightarrow[\quad 564651, 984565 \quad]{}$

V



ZK proof for 3-coloring: GMW'91

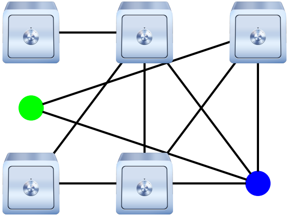
P

$A \rightarrow 564651$
$B \rightarrow 867132$
$C \rightarrow 984565$
$D \rightarrow 894102$
$E \rightarrow 069732$
$F \rightarrow 873210$
$G \rightarrow 897966$

$\xleftarrow{\{A, C\}}$

$\xrightarrow[564651,\, 984565]{}$

V



ZK proof for 3-coloring: GMW'91

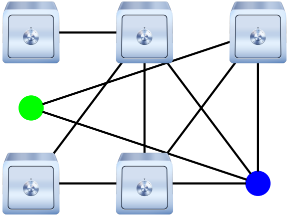
P

$A \rightarrow 564651$
$B \rightarrow 867132$
$C \rightarrow 984565$
$D \rightarrow 894102$
$E \rightarrow 069732$
$F \rightarrow 873210$
$G \rightarrow 897966$

$\xleftarrow{\{A, C\}}$

$\xrightarrow[564651,\, 984565]{}$

V



Completeness ✓ Soundness ✓ CZK

Simulator

Simulator

Sim(z):

1. Give z to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$ *rewind* to step 2
6. Otherwise, open the commitment of nodes in e'
7. Forward output from $\tilde{V}$

Simulator

Sim(z):

1. Give z to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$ *rewind* to step 2
6. Otherwise, open the commitment of nodes in e'
7. Forward output from $\tilde{V}$

Sketch of the proof

Simulator

Sim(z):

1. Give z to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$ *rewind* to step 2
6. Otherwise, open the commitment of nodes in e'
7. Forward output from $\tilde{V}$

Sketch of the proof

$e = e' \Rightarrow$ output of Sim(z) is computationally indistinguishable of $(\tilde{V} \leftrightarrow P)$ by the hiding property of the commitment scheme.

Simulator

Sim(z):

1. Give z to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$ *rewind* to step 2
6. Otherwise, open the commitment of nodes in e'
7. Forward output from $\tilde{V}$

Sketch of the proof

$e = e' \Rightarrow$ output of Sim(z) is computationally indistinguishable of $(\tilde{V} \leftrightarrow P)$ by the hiding property of the commitment scheme.

Simulator

Sim(z):

1. Give z to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$ *rewind* to step 2
6. Otherwise, open the commitment of nodes in e'
7. Forward output from $\tilde{V}$

Sketch of the proof

$e = e' \Rightarrow$ output of Sim(z) is computationally indistinguishable of $(\tilde{V} \leftrightarrow P)$ by the hiding property of the commitment scheme.

$\tilde{V}$ is computationally bounded $\Rightarrow$ distribution of e' does not depend on the commited values.

Simulator

Sim(z):

1. Give z to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$ *rewind* to step 2
6. Otherwise, open the commitment of nodes in e'
7. Forward output from $\tilde{V}$

Sketch of the proof

$e = e' \Rightarrow$ output of Sim(z) is computationally indistinguishable of $(\tilde{V} \leftrightarrow P)$ by the hiding property of the commitment scheme.

$\tilde{V}$ is computationally bounded $\Rightarrow$ distribution of e' does not depend on the commited values.

$Pr[e = e'] \geq \frac{1}{m} - negl(n)$.

Simulator

Sim(z):

1. Give z to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$ *rewind* to step 2
6. Otherwise, open the commitment of nodes in e'
7. Forward output from $\tilde{V}$

Sketch of the proof

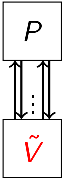
$e = e' \Rightarrow$ output of Sim(z) is computationally indistinguishable of $(\tilde{V} \leftrightarrow P)$ by the hiding property of the commitment scheme.

$\tilde{V}$ is computationally bounded $\Rightarrow$ distribution of e' does not depend on the commited values.

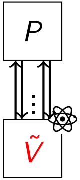
$Pr[e = e'] \geq \frac{1}{m} - negl(n)$.

What happens if $\tilde{V}$ is quantum?

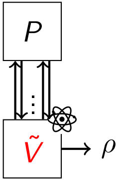
Classical zero-knowledge against quantum adversaries



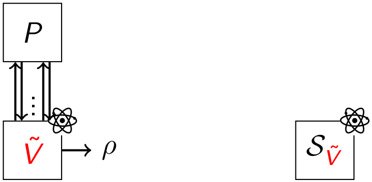
Classical zero-knowledge against quantum adversaries



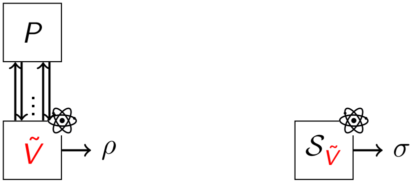
Classical zero-knowledge against quantum adversaries



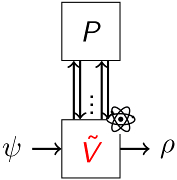
Classical zero-knowledge against quantum adversaries

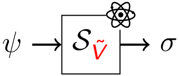


Classical zero-knowledge against quantum adversaries

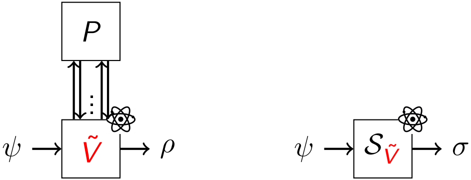


Classical zero-knowledge against quantum adversaries





Classical zero-knowledge against quantum adversaries

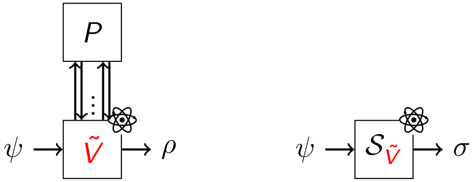


Zero-knowledge property: ρ is indistinguishable from σ

Quantum (**Computational**) ZK: $\forall \psi$, No **efficient distinguishers** for ρ and σ

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

Classical zero-knowledge against quantum adversaries



Zero-knowledge property: ρ is indistinguishable from σ

Quantum (**Computational**) ZK: $\forall\psi$, No **efficient distinguishers** for ρ and σ

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

Quantum **Statistical** ZK: $\forall\psi$, $\|\rho - \sigma\|_{\mathrm{tr}} \leq negl(n)$ for ρ and σ

Quantum **Perfect** ZK: $\forall\psi$, $\rho \mathbf{=} \sigma$

Quantum simulator for classical protocol: warm-up

Sim($\psi = |z\rangle\langle z|$):

1. Give z to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$ *rewind* to step 2
6. Otherwise, open the commitment of nodes in e'
7. Forward output from $\tilde{V}$

Quantum simulator for classical protocol: warm-up

Sim($\psi = |z\rangle\langle z|$):

1. Give z to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$ *rewind* to step 2
6. Otherwise, open the commitment of nodes in e'
7. Forward output from $\tilde{V}$

State of $\tilde{V}$ right before sending challenge:
$|\phi\rangle = \sum_{e'} \alpha_{e'} |e'\rangle_M |\gamma_{e'}\rangle_V$

Quantum simulator for classical protocol: warm-up

Sim($\psi = |z\rangle\langle z|$):

1. Give z to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$ *rewind* to step 2
6. Otherwise, open the commitment of nodes in e'
7. Forward output from $\tilde{V}$

State of $\tilde{V}$ right before sending challenge:
$|\phi\rangle = \sum_{e'} \alpha_{e'} |e'\rangle_M |\gamma_{e'}\rangle_V$

Sim measures register M and gets e' w.p. $|\alpha_{e'}|^2$ and post-meas. state is $|e'\rangle|\gamma'_e\rangle$:

$e' = e$: all is good

$e' \neq e$: rewinding does not work

$$V^\dagger |e'\rangle|\gamma'_e\rangle \text{ vs. } V^\dagger|\phi\rangle$$

Quantum simulator for classical protocol: warm-up

Sim($\psi = |z\rangle\langle z|$):

1. Give z to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$ ~~*rewind* to step 2~~ reset $\tilde{V}$ and go to step 1
6. Otherwise, open the commitment of nodes in e'
7. Forward output from $\tilde{V}$

Quantum simulator for classical protocol: warm-up

Sim($\psi = |z\rangle\langle z|$):

1. Give z to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$ ~~*rewind* to step 2~~ reset $\tilde{V}$ and go to step 1
6. Otherwise, open the commitment of nodes in e'
7. Forward output from $\tilde{V}$

Sketch of the proof

$e = e' \Rightarrow$ output of Sim(z) is computationally indistinguishable of ($\tilde{V} \leftrightarrow P$) by the hiding property of the commitment scheme.

$\tilde{V}$ is computationally bounded $\Rightarrow$ distribution of e' does not depend on the commited values.

$Pr[e = e'] \geq \frac{1}{m} - negl(n)$.

Quantum simulator for classical protocol: warm-up

Sim($\psi = |z\rangle\langle z|$):

1. Give z to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$ ~~*rewind* to step 2~~ reset $\tilde{V}$ and go to step 1
6. Otherwise, open the commitment of nodes in e'
7. Forward output from $\tilde{V}$

Sketch of the proof

$e = e' \Rightarrow$ output of Sim(z) is computationally indistinguishable of $(\tilde{V} \leftrightarrow P)$ by the hiding property of the commitment scheme.

$\tilde{V}$ is computationally bounded $\Rightarrow$ distribution of e' does not depend on the commited values.

$Pr[e = e'] \geq \frac{1}{m} - negl(n)$.

Does not work with quantum side information!

Quantum simulator for classical protocol: warm-up

Sim($\psi = |z\rangle\langle z|$):

1. Give z to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$ ~~*rewind to step 2*~~ reset $\tilde{V}$ and go to step 1
6. Otherwise, open the commitment of nodes in e'
7. Forward output from $\tilde{V}$

Sketch of the proof

$e = e' \Rightarrow$ output of Sim(z) is computationally indistinguishable of $(\tilde{V} \leftrightarrow P)$ by the hiding property of the commitment scheme.

$\tilde{V}$ is computationally bounded $\Rightarrow$ distribution of e' does not depend on the commited values.

$Pr[e = e'] \geq \frac{1}{m} - negl(n)$.

Does not work with quantum side information!

We cannot sequentially repeat this protocol!

Watrous's rewinding

Theorem

Let Q be a quantum circuit such that $\exists p \forall |\psi\rangle$

$$Q|\psi\rangle|0\rangle = \sqrt{p}|0\rangle|\phi_0(\psi)\rangle + \sqrt{1-p}|1\rangle|\phi_1(\psi)\rangle$$

Watrous's rewinding

Theorem

Let Q be a quantum circuit such that $\exists p \forall |\psi\rangle$

$$Q|\psi\rangle|0\rangle = \sqrt{p}|0\rangle|\phi_0(\psi)\rangle + \sqrt{1-p}|1\rangle|\phi_1(\psi)\rangle$$

Then $\forall \varepsilon > 0$, we can construct a circuit R of size $poly(|Q|, \log 1/\varepsilon, 1/p)$ that receives an input $|\psi\rangle$ and outputs $|\phi_0(\psi)\rangle$ w.p. $1-\varepsilon$

Watrous's rewinding

Theorem

Let Q be a quantum circuit such that $\exists p \forall |\psi\rangle$

$$Q|\psi\rangle|0\rangle = \sqrt{p}|0\rangle|\phi_0(\psi)\rangle + \sqrt{1-p}|1\rangle|\phi_1(\psi)\rangle$$

Then $\forall \varepsilon > 0$, we can construct a circuit R of size $poly(|Q|, \log 1/\varepsilon, 1/p)$ that receives an input $|\psi\rangle$ and outputs $|\phi_0(\psi)\rangle$ w.p. $1-\varepsilon$

- Similar statement holds for the non-exact case

Watrous's rewinding - idea of the proof

- $|1\rangle|\phi_1(\psi)\rangle$ has all the information that we need to get $|0\rangle|\phi_0(\psi)\rangle$

Watrous's rewinding - idea of the proof

- $|1\rangle|\phi_1(\psi)\rangle$ has all the information that we need to get $|0\rangle|\phi_0(\psi)\rangle$

  We can "extract" $|0\rangle|\phi_0(\psi)\rangle$ efficiently

Watrous's rewinding - idea of the proof

- $|1\rangle|\phi_1(\psi)\rangle$ has all the information that we need to get $|0\rangle|\phi_0(\psi)\rangle$

  We can "extract" $|0\rangle|\phi_0(\psi)\rangle$ efficiently
- Quantum rewinding operator: $Q(2\Delta - I)Q^\dagger$

  Δ is the projection onto the valid initial states of Q

Watrous's rewinding - idea of the proof

- $|1\rangle|\phi_1(\psi)\rangle$ has all the information that we need to get $|0\rangle|\phi_0(\psi)\rangle$

  We can "extract" $|0\rangle|\phi_0(\psi)\rangle$ efficiently
- Quantum rewinding operator: $Q(2\Delta - I)Q^\dagger$

  Δ is the projection onto the valid initial states of Q

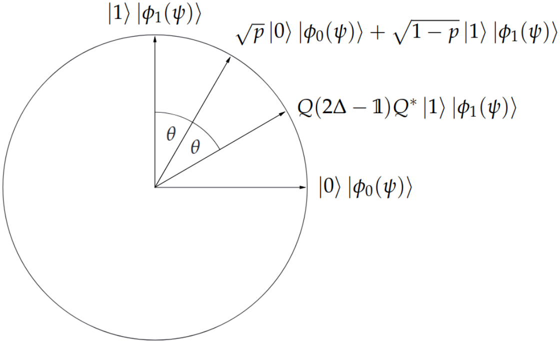


Figure from Watrous'09

Watrous's rewinding - wrapping up

Watrous's rewinding - wrapping up

$R(\psi)$

1. Run $Q(\psi)$
2. Repeat T times
   1. Measure first qubit
   2. If outcome is 0, output second register
   3. Apply $Q(2\Delta - I)Q^*$
3. Output $\perp$

Watrous's rewinding - wrapping up

$R(\psi)$

1. Run $Q(\psi)$
2. Repeat T times
   1. Measure first qubit
   2. If outcome is 0, output second register
   3. Apply $Q(2\Delta - I)Q^*$
3. Output $\perp$

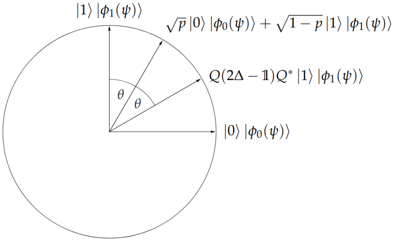


Figure from Watrous'09

Watrous's rewinding - wrapping up

$R(\psi)$

1. Run $Q(\psi)$
2. Repeat T times
   1. Measure first qubit
   2. If outcome is 0, output second register
   3. Apply $Q(2\Delta - I)Q^*$
3. Output $\perp$

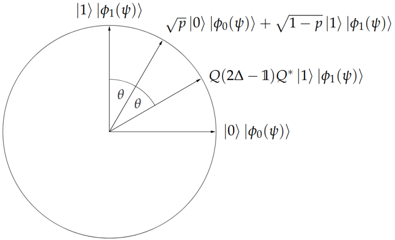


Figure from Watrous'09

Theorem

Let Q be a quantum circuit such that $\exists p \forall |\psi\rangle\ Q|\psi\rangle|0\rangle = \sqrt{p}|0\rangle|\phi_0(\psi)\rangle + \sqrt{1-p}|1\rangle|\phi_1(\psi)\rangle$

Then $\forall \varepsilon > 0$, we can pick some $T = poly(|Q|, \log 1/\varepsilon, 1/p)$ and $R(\psi)$ outputs $|\phi_0(\psi)\rangle$ w.p. $1 - \varepsilon$

Quantum simulator for classical protocol

Quantum simulator for classical protocol

$\mathrm{Sim}_1(\psi)$:

1. Give ψ to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$, open the commitment of nodes in e', and forward output
6. Output $\perp$ from $\tilde{V}$

- If $e = e'$, output of Sim_1 is good
- Sim_1 succeeds with probability $\frac{1}{m}$ $(+\ negl(n))$

Quantum simulator for classical protocol

$\mathrm{Sim}_1(\psi)$:

1. Give ψ to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$, open the commitment of nodes in e', and forward output
6. Output $\perp$ from $\tilde{V}$

$\mathrm{Sim}_2(\psi)$:

1. Watrous' rewinding on Sim_1 with $\varepsilon = negl(n)$

- If $e = e'$, output of Sim_1 is good
- Sim_1 succeeds with probability $\frac{1}{m}$ $(+\ negl(n))$

Quantum simulator for classical protocol

$\mathrm{Sim}_1(\psi)$:

1. Give ψ to $\tilde{V}$.
2. Pick $e \in E$ uniformly at random
3. Commit to a random coloring that is correct on edge e
4. Receive a challenge e' from $\tilde{V}$
5. If $e \neq e'$, open the commitment of nodes in e', and forward output
6. Output $\perp$ from $\tilde{V}$

$\mathrm{Sim}_2(\psi)$:

1. Watrous' rewinding on Sim_1 with $\varepsilon = negl(n)$

- If $e = e'$, output of Sim_1 is good
- Sim_1 succeeds with probability $\frac{1}{m}$ $(+\ negl(n))$

- Output of Sim_2 is $\mathrm{negl}(n)$ close to the output when we have $e = e'$
- Runtime of Sim_2 is $poly(|\tilde{V}|, n)$

Classical ZK - wrap up

Classical ZK - wrap up

Theorem

Assuming post-quantum commitment schemes, GMW'91 is secure against quantum adversaries.

Classical ZK - wrap up

Theorem

Assuming post-quantum commitment schemes, GMW'91 is secure against quantum adversaries.

Theorem

Naor's commitment scheme implemented with post-quantum OWF is secure against quantum adversaries.

Classical ZK - wrap up

Theorem

Assuming post-quantum commitment schemes, GMW'91 is secure against quantum adversaries.

Theorem

Naor's commitment scheme implemented with post-quantum OWF is secure against quantum adversaries.

Corollary

Zero-knowledge proofs for NP is in MiniQCrypt

Classical ZK - wrap up

Theorem

Assuming post-quantum commitment schemes, GMW'91 is secure against quantum adversaries.

Theorem

Naor's commitment scheme implemented with post-quantum OWF is secure against quantum adversaries.

Corollary

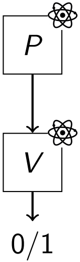
Zero-knowledge proofs for NP is in $MiniQCrypt$

Can we have (simple) zero-knowledge protocols for quantum proofs?

Quantum proofs

Quantum proofs

$L \in \mathrm{QMA}$



P

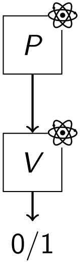
V

$0/1$

for $x \in L$, $\exists P$
V accepts whp
for $x \notin L$, $\forall P$
V rejects whp

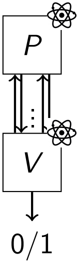
Quantum proofs

$L \in \text{QMA}$



for $x \in L$, $\exists P$
V accepts whp
for $x \notin L$, $\forall P$
V rejects whp

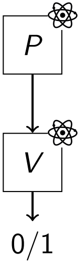
$L \in \text{QIP}$



for $x \in L$, $\exists P$
V accepts
for $x \notin L$, $\forall P$
V rejects whp

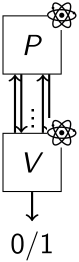
Quantum proofs

$L \in \mathrm{QMA}$



for $x \in L$, $\exists P$
V accepts whp
for $x \notin L$, $\forall P$
V rejects whp

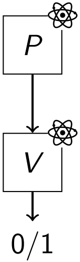
$L \in \mathrm{QIP} = \mathrm{PSPACE}$



for $x \in L$, $\exists P$
V accepts
for $x \notin L$, $\forall P$
V rejects whp

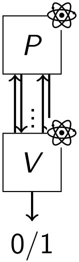
Quantum proofs

$L \in \mathrm{QMA}$



for $x \in L$, $\exists P$
V accepts whp
for $x \notin L$, $\forall P$
V rejects whp

$L \in \mathrm{QIP} = \mathrm{PSPACE}$

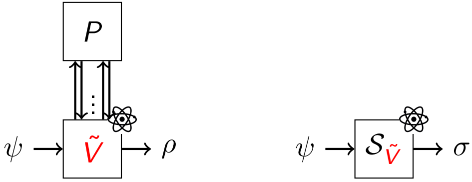


for $x \in L$, $\exists P$
V accepts
for $x \notin L$, $\forall P$
V rejects whp

Expected: $\mathrm{NP} \subsetneq \mathrm{QMA} \subsetneq \mathrm{IP} = \mathrm{QIP} = \mathrm{PSPACE}$

Quantum Zero-knowledge

Quantum Zero-knowledge



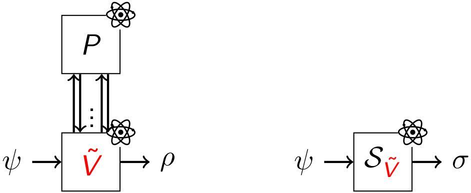
Zero-knowledge property: ρ is indistinguishable from σ

Quantum (Computational) ZK: $\forall\psi$, No efficient distinguishers for ρ and σ

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

Quantum Statistical ZK: $\forall\psi$, $\|\rho - \sigma\|_{\mathrm{tr}} \leq negl(n)$ for ρ and σ
Quantum Perfect ZK: $\forall\psi$, $\rho = \sigma$

Quantum Zero-knowledge



Zero-knowledge property: ρ is indistinguishable from σ

Quantum (Computational) ZK: $\forall \psi$, No efficient distinguishers for ρ and σ

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

Quantum Statistical ZK: $\forall \psi$, $\|\rho - \sigma\|_{\mathrm{tr}} \leq negl(n)$ for ρ and σ
Quantum Perfect ZK: $\forall \psi$, $\rho = \sigma$

Quantum ZK protocols for QMA

Option 1: ZK from generic problem in QMA.

Quantum ZK protocols for QMA

Option 1: ZK from generic problem in QMA. We need structure.

Quantum ZK protocols for QMA

Option 1: ZK from generic problem in QMA. We need structure.

Option 2: ZK from Local Hamiltonian problem.

Quantum ZK protocols for QMA

Option 1: ZK from generic problem in QMA. We need structure.

Option 2: ZK from Local Hamiltonian problem. We need **more** structure.

Quantum ZK protocols for QMA

Option 1: ZK from generic problem in QMA. We need structure.

Option 2: ZK from Local Hamiltonian problem. We need **more** structure.

Option 3: ZK from Clifford Local Hamiltonian problem.

Quantum ZK protocols for QMA

Option 1: ZK from generic problem in QMA. We need structure.

Option 2: ZK from Local Hamiltonian problem. We need **more** structure.

Option 3: ZK from Clifford Local Hamiltonian problem. It works [BJSW'20].

Quantum ZK protocols for QMA

Option 1: ZK from generic problem in QMA. We need structure.

Option 2: ZK from Local Hamiltonian problem. We need **more** structure.

Option 3: ZK from Clifford Local Hamiltonian problem. It works [BJSW'20]. It is somewhat complicated.

Quantum ZK protocols for QMA

Option 1: ZK from generic problem in QMA. We need structure.

Option 2: ZK from Local Hamiltonian problem. We need **more** structure.

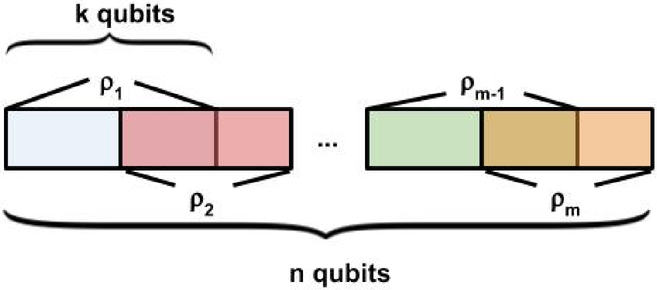
Option 3: ZK from Clifford Local Hamiltonian problem. It works [BJSW'20]. It is somewhat complicated.

Option 4: **ZK from Consistency of Local density matrices**

Consistency of local density matrices problem

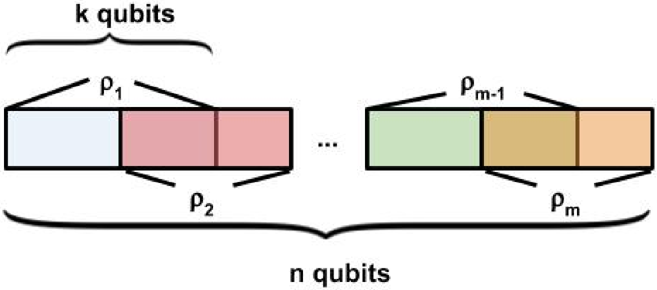
Consistency of local density matrices problem

Do “pieces” of quantum state come from the same global state?



Consistency of local density matrices problem

Do “pieces” of quantum state come from the same global state?

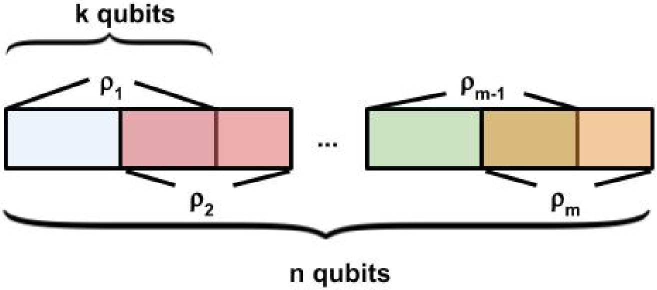


Input: Reduced density matrices $\rho_1, \ldots, \rho_m$ on k-qubits

Output: yes: $\exists \psi$ such that $\forall i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \leq \varepsilon$
no: $\forall \psi$, $\exists i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \geq \frac{1}{poly(n)}$

Consistency of local density matrices problem

Do "pieces" of quantum state come from the same global state?



Input: Reduced density matrices $\rho_1, \ldots, \rho_m$ on k-qubits

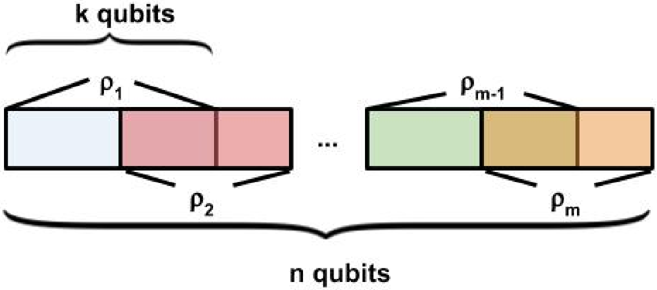
Output: yes: $\exists \psi$ such that $\forall i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \leq \varepsilon$

no: $\forall \psi, \exists i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \geq \frac{1}{poly(n)}$

- Liu'06: containment in QMA, and QMA-hardness under Turing reduction

Consistency of local density matrices problem

Do "pieces" of quantum state come from the same global state?



Input: Reduced density matrices $\rho_1, ..., \rho_m$ on k-qubits

Output: yes: $\exists \psi$ such that $\forall i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \leq \varepsilon$

no: $\forall \psi, \exists i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \geq \frac{1}{poly(n)}$

- Liu'06: containment in QMA, and QMA-hardness under Turing reduction
- Broadbent-**G**'20: QMA-hardness under Karp reductions

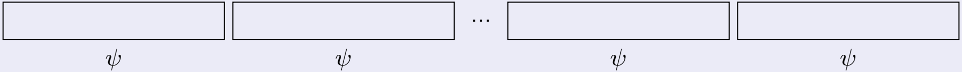
CLDM is in QMA - overview

Completeness:

CLDM is in QMA - overview

Completeness:

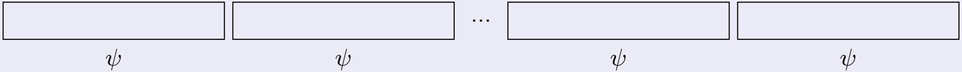
1. Prover sends $\psi^{\otimes\ell}$



CLDM is in QMA - overview

Completeness:

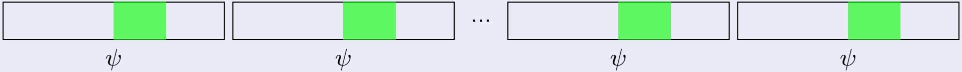
1. Prover sends $\psi^{\otimes \ell}$
2. Verifier chooses $i \in [m]$ uniformly at random



CLDM is in QMA - overview

Completeness:

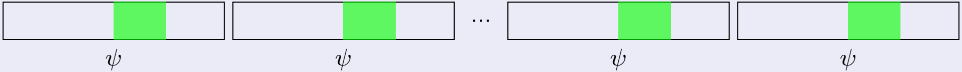
1. Prover sends $\psi^{\otimes \ell}$
2. Verifier chooses $i \in [m]$ uniformly at random
3. Verifier performs checks on qubits corresponding to ρ_i



CLDM is in QMA - overview

Completeness: Verifier accepts w.p. $\geq 1 - negl(n)$

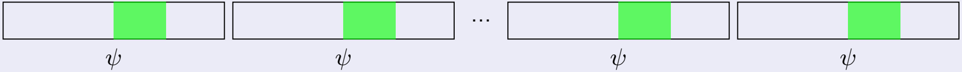
1. Prover sends $\psi^{\otimes \ell}$
2. Verifier chooses $i \in [m]$ uniformly at random
3. Verifier performs checks on qubits corresponding to ρ_i



CLDM is in QMA - overview

Completeness: Verifier accepts w.p. $\geq 1 - negl(n)$

1. Prover sends $\psi^{\otimes \ell}$
2. Verifier chooses $i \in [m]$ uniformly at random
3. Verifier performs checks on qubits corresponding to ρ_i

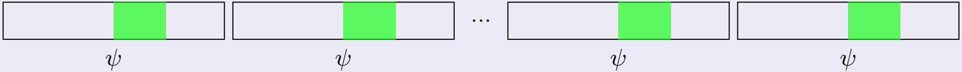


Soundness:

CLDM is in QMA - overview

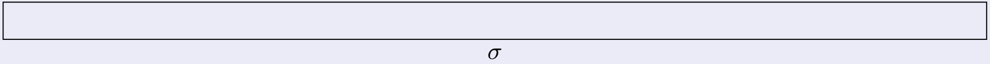
Completeness: Verifier accepts w.p. $\geq 1 - negl(n)$

1. Prover sends $\psi^{\otimes \ell}$
2. Verifier chooses $i \in [m]$ uniformly at random
3. Verifier performs checks on qubits corresponding to ρ_i



Soundness:

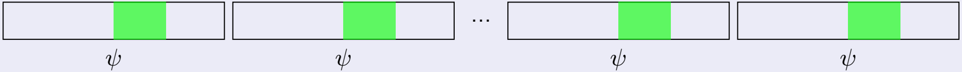
1. Prover sends σ



CLDM is in QMA - overview

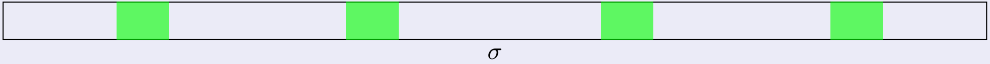
Completeness: Verifier accepts w.p. $\geq 1 - \mathit{negl}(n)$

1. Prover sends $\psi^{\otimes \ell}$
2. Verifier chooses $i \in [m]$ uniformly at random
3. Verifier performs checks on qubits corresponding to ρ_i



Soundness:

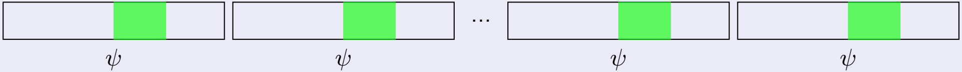
1. Prover sends σ
2. Verifier chooses $i \in [m]$ uniformly at random
3. Verifier performs checks on qubits corresponding to ρ_i



CLDM is in QMA - overview

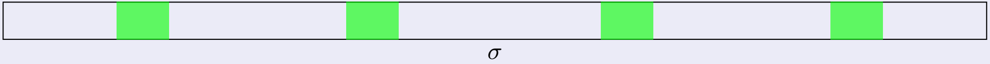
Completeness: Verifier accepts w.p. $\geq 1 - negl(n)$

1. Prover sends $\psi^{\otimes \ell}$
2. Verifier chooses $i \in [m]$ uniformly at random
3. Verifier performs checks on qubits corresponding to ρ_i



Soundness: Verifier accepts w.p. $\leq 1 - \frac{1}{m} - negl(n)$

1. Prover sends σ
2. Verifier chooses $i \in [m]$ uniformly at random
3. Verifier performs checks on qubits corresponding to ρ_i



ZK proof for CLDM: BG'20

P V

$\rho_1, \ldots, \rho_m$

ZK proof for CLDM: BG'20

P

V

$\psi^{\otimes \ell}$

$\rho_1, \ldots, \rho_m$

ZK proof for CLDM: BG'20

P

V

$X^a Z^b \psi^{\otimes \ell} Z^b X^a$

$\rho_1, \ldots, \rho_m$

a_1, b_1

a_2, b_2

$\ldots$

a_{n-1}, b_{n-1}

a_n, b_n

ZK proof for CLDM: BG'20

P

V

$X^a Z^b \psi^{\otimes \ell} Z^b X^a$

$\rho_1, \ldots, \rho_m$

ZK proof for CLDM: BG'20

P

$a_1, b_1 \rightarrow 564651$
$a_2, b_2 \rightarrow 984565$
$\dots$
$a_n, b_n \rightarrow 894102$

V

$\rho_1, \dots, \rho_m$

$X^a Z^b \psi^{\otimes \ell} X^a Z^b$

…

ZK proof for CLDM: BG'20

P

$a_1, b_1 \rightarrow 564651$

$a_2, b_2 \rightarrow 984565$

$\cdots$

$a_n, b_n \rightarrow 894102$

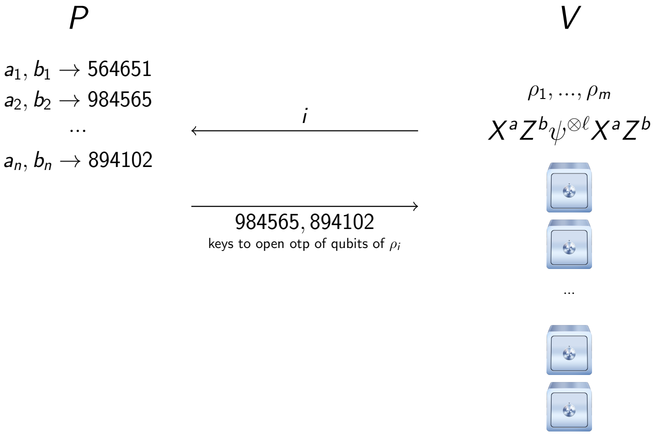
$$\xleftarrow{\quad i \quad}$$

V

$\rho_1, \ldots, \rho_m$

$X^a Z^b \psi^{\otimes \ell} X^a Z^b$

ZK proof for CLDM: BG'20



P

$a_1, b_1 \to 564651$

$a_2, b_2 \to 984565$

$\dots$

$a_n, b_n \to 894102$

V

$\rho_1, \dots, \rho_m$

$X^a Z^b \psi^{\otimes \ell} X^a Z^b$

$$\xleftarrow{\quad i \quad}$$

$$\xrightarrow[\text{984565, 894102}]{}$$

keys to open otp of qubits of ρ_i

ZK proof for CLDM: BG'20

P

$a_1, b_1 \to 564651$

$a_2, b_2 \to 984565$

$\ldots$

$a_n, b_n \to 894102$

$\xleftarrow{\quad i \quad}$

$\xrightarrow{\quad 984565, 894102 \quad}$

keys to open otp of qubits of ρ_i

V

$\rho_1, \ldots, \rho_m$

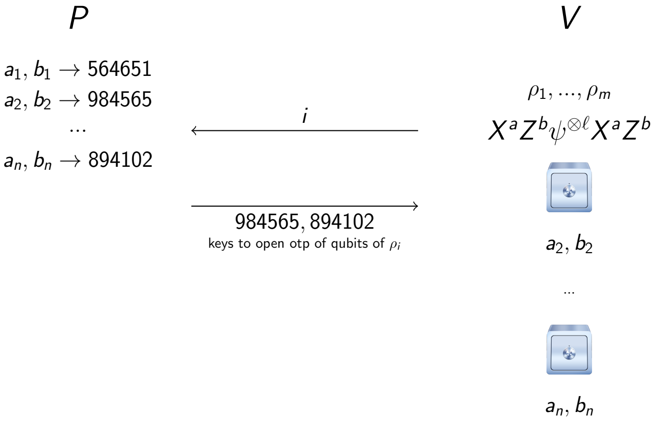
$X^a Z^b \psi^{\otimes \ell} X^a Z^b$

a_2, b_2

...

a_n, b_n

ZK proof for CLDM: BG'20



P

$a_1, b_1 \rightarrow 564651$

$a_2, b_2 \rightarrow 984565$

$\dots$

$a_n, b_n \rightarrow 894102$

V

$\rho_1, \dots, \rho_m$

$X^a Z^b \psi^{\otimes \ell} X^a Z^b$

$\xleftarrow{\quad i \quad}$

$\xrightarrow{\quad\quad\quad}$

$984565, 894102$

keys to open otp of qubits of ρ_i

a_2, b_2

...

a_n, b_n

Completeness ✓ Soundness ✓ CZK

Zero-knowledge (sketch of the proof)

Zero-knowledge (sketch of the proof)

$\mathrm{Sim}_1(\psi)$:

1. Give ψ to $\tilde{V}$.
2. Pick $i \in [m]$ uniformly at random
3. Commit to a state that has ρ_i in the right position
4. Receive a challenge i' from $\tilde{V}$
5. If $i \neq i'$, open the commitment of OTP of the corresponding qubits, and forward output
6. Output $\perp$ from $\tilde{V}$

- If $i = i'$, output of Sim_1 is good
- Sim_1 succeeds with probability $\frac{1}{m}$ $(+\ negl(n))$

Zero-knowledge (sketch of the proof)

$\mathrm{Sim}_1(\psi)$:

1. Give ψ to $\tilde{V}$.
2. Pick $i \in [m]$ uniformly at random
3. Commit to a state that has ρ_i in the right position
4. Receive a challenge i' from $\tilde{V}$
5. If $i \neq i'$, open the commitment of OTP of the corresponding qubits, and forward output
6. Output $\perp$ from $\tilde{V}$

$\mathrm{Sim}_2(\psi)$:

1. Watrous' rewinding on Sim_1 with $\varepsilon = negl(n)$

- If $i = i'$, output of Sim_1 is good
- Sim_1 succeeds with probability $\frac{1}{m}$ $(+\ negl(n))$

Zero-knowledge (sketch of the proof)

$\mathrm{Sim}_1(\psi)$:

1. Give ψ to $\tilde{V}$.
2. Pick $i \in [m]$ uniformly at random
3. Commit to a state that has ρ_i in the right position
4. Receive a challenge i' from $\tilde{V}$
5. If $i \neq i'$, open the commitment of OTP of the corresponding qubits, and forward output
6. Output $\perp$ from $\tilde{V}$

$\mathrm{Sim}_2(\psi)$:

1. Watrous' rewinding on Sim_1 with $\varepsilon = negl(n)$

- If $i = i'$, output of Sim_1 is good
- Sim_1 succeeds with probability $\frac{1}{m}$ $(+\ negl(n))$

- Output of Sim_2 is $\mathrm{negl}(n)$ close to the output when we have $i = i'$
- Runtime of Sim_2 is $poly(|\tilde{V}|, n)$

Zero-knowledge (sketch of the proof)

Sim$_1(\psi)$:

1. Give ψ to $\tilde{V}$.
2. Pick $i \in [m]$ uniformly at random
3. Commit to a state that has ρ_i in the right position
4. Receive a challenge i' from $\tilde{V}$
5. If $i \neq i'$, open the commitment of OTP of the corresponding qubits, and forward output
6. Output $\perp$ from $\tilde{V}$

Sim$_2(\psi)$:

1. Watrous' rewinding on Sim$_1$ with $\varepsilon = negl(n)$

- If $i = i'$, output of Sim$_1$ is good
- Sim$_1$ succeeds with probability $\frac{1}{m}$ $(+\ negl(n))$

- Output of Sim$_2$ is negl(n) close to the output when we have $i = i'$
- Runtime of Sim$_2$ is $poly(|\tilde{V}|, n)$

Corollary

Quantum zero-knowledge proofs for QMA is in MiniQCrypt

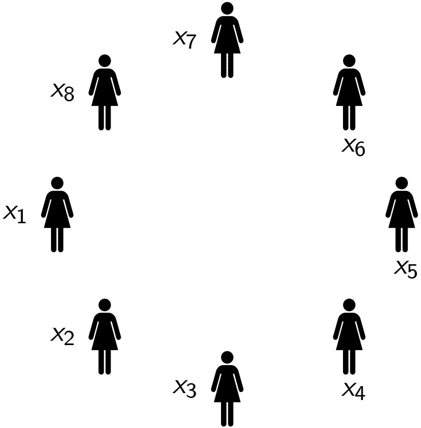
Further development

1. Perfect ZK for multi-prover entangled proof systems (MIP*) [**G**SY'19]
2. Constant round post-quantum ZK for NP/QMA [Bitansky-S'20]
3. Proof of Knowledge
   - Usual soundness: there is no good strategy for no-instance
   - PoK: If Prover passes with high enough probability, then a NP-witness is known

     There is an extractor K, such that if $\tilde{P}$ passes with probability $\geq \kappa$, $K^{\tilde{P}}$ outputs a witness
   - Proof of Knowledge against quantum provers [Unruh'12]
   - Proof of Quantum Knowledge [Broadbent-**G**'20,Coladangelo-VZ'20, Ananth-CLP'20]
4. Classical ZK *arguments* for QMA
   - Computational soundness: no poly-time adversary can make V accept a no-instance
   - Classical argument system for QMA [Mahadev'18,Alagic-C**G**H'20, Chia-CY'20]
   - Classical ZK protocols for QMA [Vidick-Z'20]
5. NIZKs in the quantum setting
   - Post-quantum NIZK for NP [Peikert-S'19]
   - Quantum NIZK for QMA [Broadbent-**G**'20,Coladangelo-VZ'20]
   - Classical NIZK arguments for QMA [Alagic-C**G**H'20]

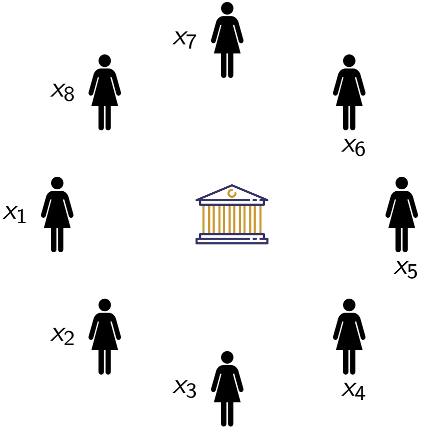
Multi-party (quantum) computation in the quantum world

Multi-party computation



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

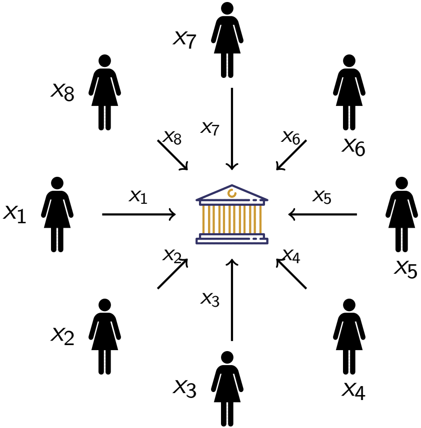
Multi-party computation



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

Ideal world

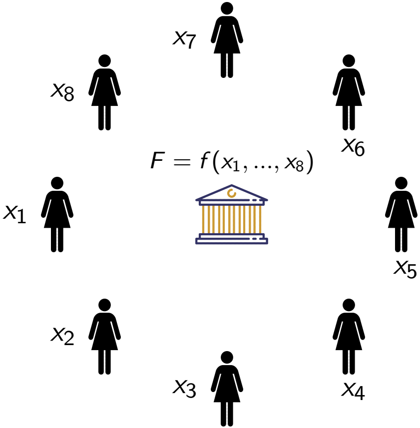
Multi-party computation



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

Ideal world

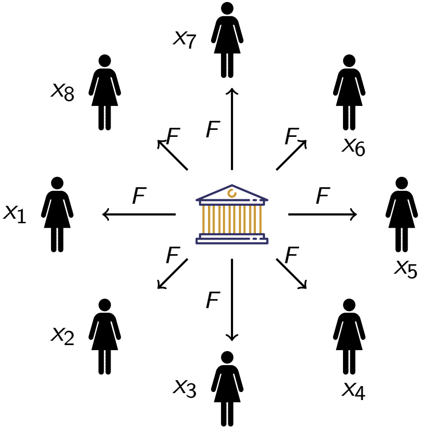
Multi-party computation



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

Ideal world

Multi-party computation

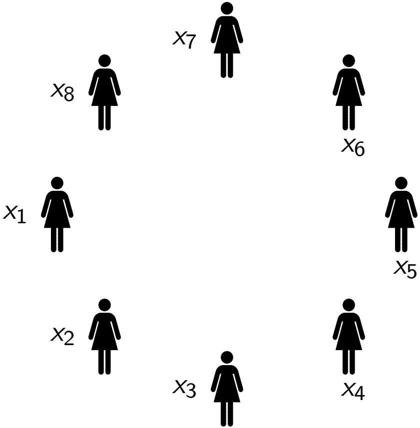


Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

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

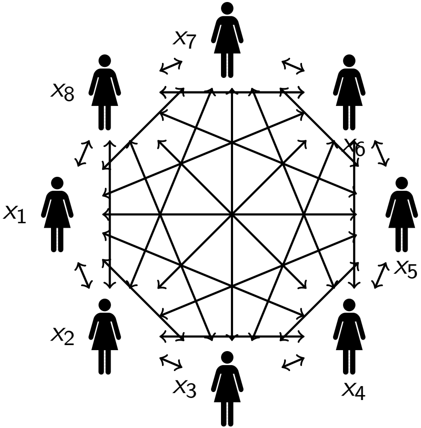
Ideal world

- 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

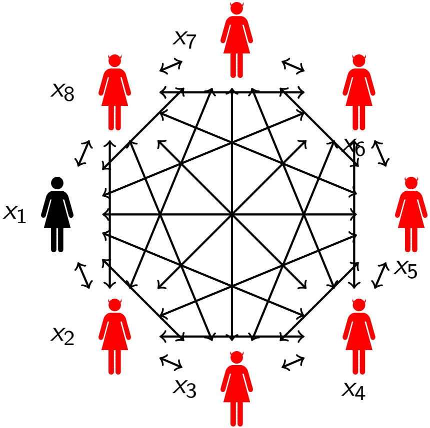
Ideal world

- 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

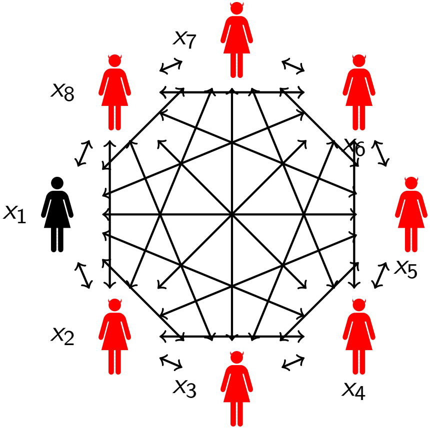
Ideal world

- 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



Are classical protocols secure against quantum adversaries?

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

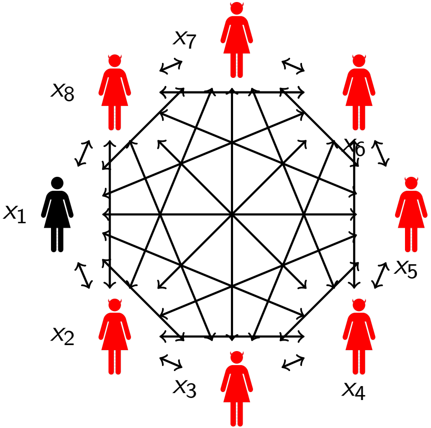
Ideal world

- 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

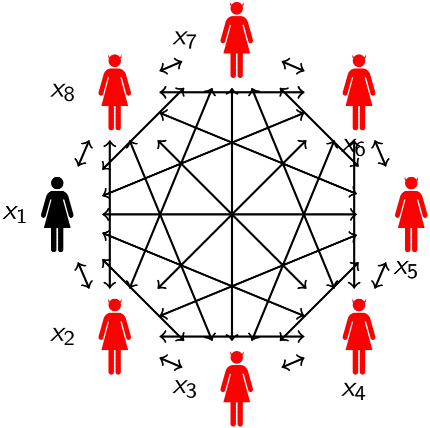
Real world

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

Are classical protocols secure against quantum adversaries?

Are there *better* quantum protocols for MPC?

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

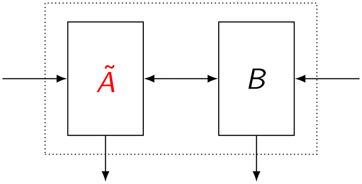
- Goal: implement the ideal functionality
- Protocols where parties interact, but still they only learn F
- Even if they behave disonestly

Are classical protocols secure against quantum adversaries?

Are there *better* quantum protocols for MPC?

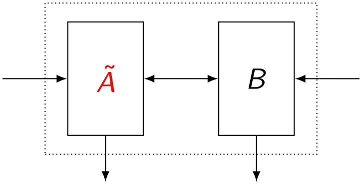
Are there protocols for MP**Q**C?

Security definition (two-party case)

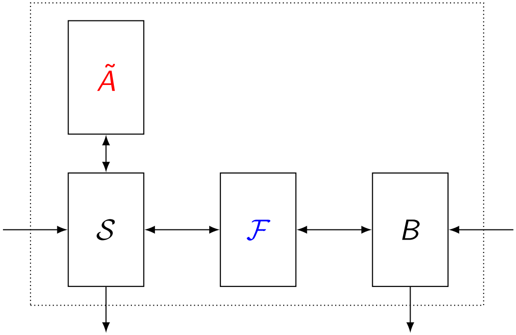


Real world

Security definition (two-party case)

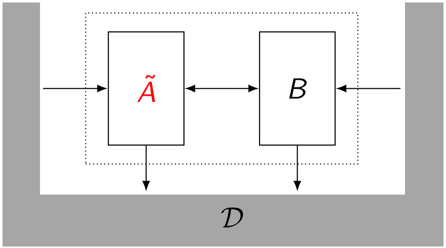


Real world

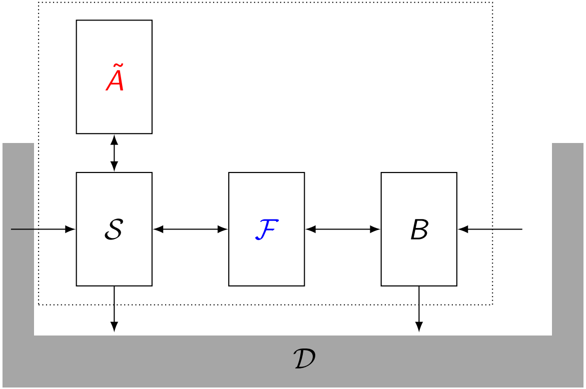


Ideal world

Security definition (two-party case)

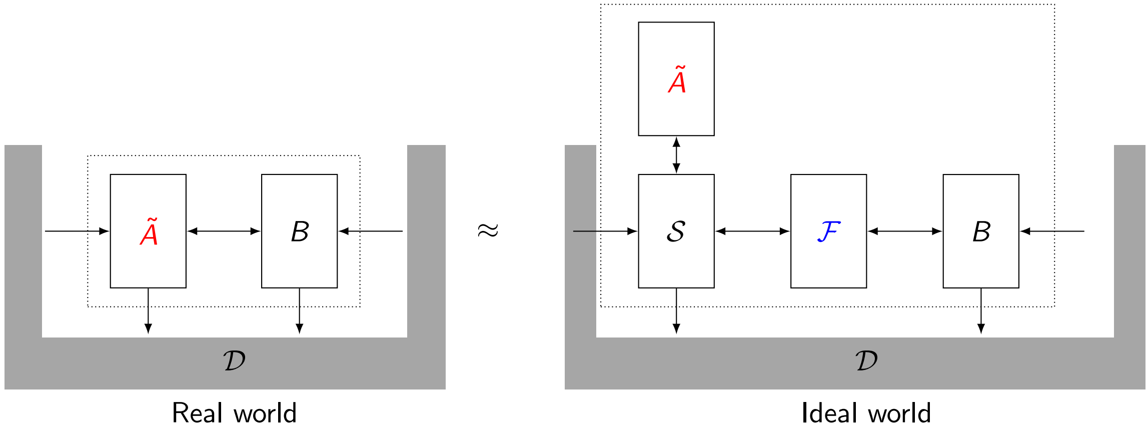


Real world



Ideal world

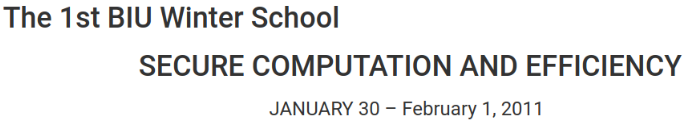
Security definition (two-party case)



For every polynomial-time $\mathcal{D}$, $|Pr[\mathcal{D}(\text{real})] - Pr[\mathcal{D}(\text{ideal})]| \leq negl(\lambda)$

Classical MPC protocols

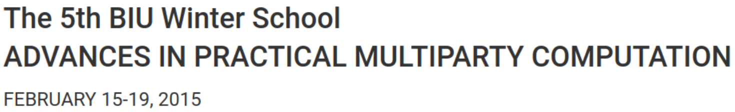
Classical MPC protocols



The 1st BIU Winter School

SECURE COMPUTATION AND EFFICIENCY

JANUARY 30 – February 1, 2011



The 5th BIU Winter School

ADVANCES IN PRACTICAL MULTIPARTY COMPUTATION

FEBRUARY 15-19, 2015

Classical MPC protocols

Classical MPC protocols

GMW family

Honest MPC + $\mathcal{F}_{ZK}$

Classical MPC protocols

GMW family
Honest MPC + $\mathcal{F}_{ZK}$

IPS family
Honest MPC + $\mathcal{F}_{OT}$

Classical MPC protocols

GMW family
Honest MPC + $\mathcal{F}_{ZK}$

IPS family
Honest MPC + $\mathcal{F}_{OT}$

- Unruh'10: protocols are secure against quantum adversaries in the ideal world

Classical MPC protocols

GMW family
Honest MPC + $\mathcal{F}_{ZK}$

IPS family
Honest MPC + $\mathcal{F}_{OT}$

- Unruh'10: protocols are secure against quantum adversaries in the ideal world
- Implementation of ideal functionalities
    - Classically: from PKE assumptions
    - Quantumly: extraction without disturbing internal state of adversaries is cumbersome

Classical MPC protocols

GMW family
Honest MPC + $\mathcal{F}_{ZK}$

IPS family
Honest MPC + $\mathcal{F}_{OT}$

- Unruh'10: protocols are secure against quantum adversaries in the ideal world
- Implementation of ideal functionalities
  - Classically: from PKE assumptions
  - Quantumly: extraction without disturbing internal state of adversaries is cumbersome
- Solutions

Classical MPC protocols

GMW family
Honest MPC + $\mathcal{F}_{ZK}$

IPS family
Honest MPC + $\mathcal{F}_{OT}$

- Unruh'10: protocols are secure against quantum adversaries in the ideal world
- Implementation of ideal functionalities
  - Classically: from PKE assumptions
  - Quantumly: extraction without disturbing internal state of adversaries is cumbersome
- Solutions
  1. Implementations from trusted setup (e.g. Garg-S'18)

Classical MPC protocols

GMW family
Honest MPC + $\mathcal{F}_{ZK}$

IPS family
Honest MPC + $\mathcal{F}_{OT}$

- Unruh'10: protocols are secure against quantum adversaries in the ideal world
- Implementation of ideal functionalities
  - Classically: from PKE assumptions
  - Quantumly: extraction without disturbing internal state of adversaries is cumbersome
- Solutions
  1. Implementations from trusted setup (e.g. Garg-S'18)
  2. Implementations from stronger functionalities/assumptions (Bitansky-S'20, Agarwal-BGKM'20)

Classical MPC protocols

GMW family
Honest MPC + $\mathcal{F}_{ZK}$

IPS family
Honest MPC + $\mathcal{F}_{OT}$

- Unruh'10: protocols are secure against quantum adversaries in the ideal world
- Implementation of ideal functionalities
  - Classically: from PKE assumptions
  - Quantumly: extraction without disturbing internal state of adversaries is cumbersome
- Solutions
  1. Implementations from trusted setup (e.g. Garg-S'18)
  2. Implementations from stronger functionalities/assumptions (Bitansky-S'20, Agarwal-BGKM'20)
  3. Implementations with quantum protocols

Classical MPC protocols

GMW family
Honest MPC + $\mathcal{F}_{ZK}$

IPS family
Honest MPC + $\mathcal{F}_{OT}$

- Unruh'10: protocols are secure against quantum adversaries in the ideal world
- Implementation of ideal functionalities
  - Classically: from PKE assumptions
  - Quantumly: extraction without disturbing internal state of adversaries is cumbersome
- Solutions
  1. Implementations from trusted setup (e.g. Garg-S'18)
  2. Implementations from stronger functionalities/assumptions (Bitansky-S'20, Agarwal-BGKM'20)
  3. Implementations with quantum protocols (from <u>weaker</u> assumptions!)

Classical MPC protocols

GMW family
Honest MPC + $\mathcal{F}_{ZK}$

IPS family
Honest MPC + $\mathcal{F}_{OT}$

- Unruh'10: protocols are secure against quantum adversaries in the ideal world
- Implementation of ideal functionalities
  - Classically: from PKE assumptions
  - Quantumly: extraction without disturbing internal state of adversaries is cumbersome
- Solutions
  1. Implementations from trusted setup (e.g. Garg-S'18)
  2. Implementations from stronger functionalities/assumptions (Bitansky-S'20, Agarwal-BGKM'20)
  3. **Implementations with quantum protocols (from <u>weaker</u> assumptions!)**

Oblivious transfer

Oblivious transfer

Ideal functionality

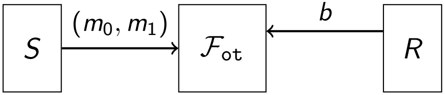
S

$\mathcal{F}_{\mathtt{ot}}$

R

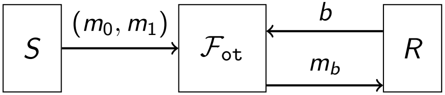
Oblivious transfer

Ideal functionality



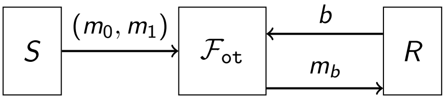
Oblivious transfer

Ideal functionality

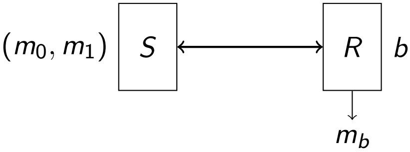


Oblivious transfer

Ideal functionality



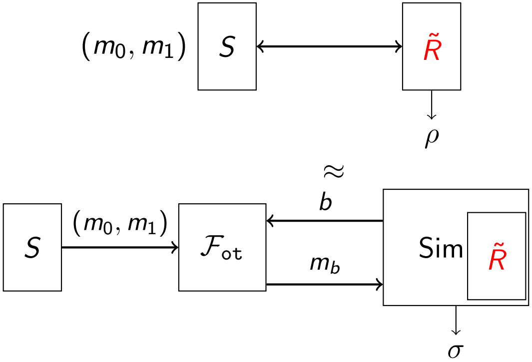
Real world



Oblivious transfer - security definitions

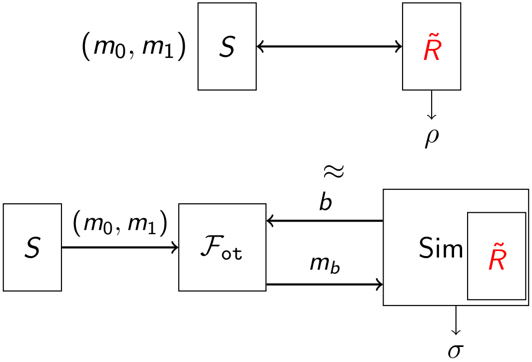
Oblivious transfer - security definitions

Security against malicious receiver

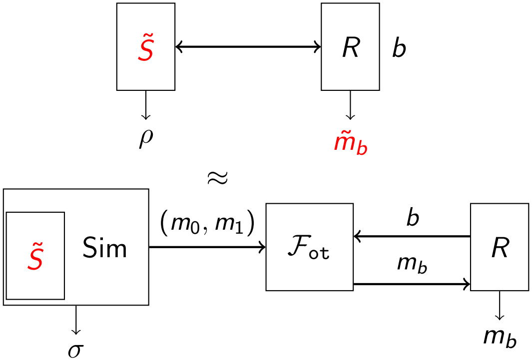


Oblivious transfer - security definitions

Security against malicious receiver



Security against malicious sender



MPC from Quantum+OWF

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

MPC from Quantum+OWF

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

MPC from Quantum+OWF

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

MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- Unruh'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world
- Bennet-BCS'92: Quantum protocol for OT based on commitment schemes
- Damgard-FLSS'09 Bouman-F'10: Security proof of BBCS protocol based on strong classical commitment schemes (likely to lie outside of MiniCrypt)

MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- Unruh'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world
- Bennet-BCS'92: Quantum protocol for OT based on commitment schemes
- Damgard-FLSS'09 Bouman-F'10: Security proof of BBCS protocol based on strong classical commitment schemes (likely to lie outside of MiniCrypt)
- Bartusek-CKM'21 and **G**LSV'21: Quantum protocol for strong commitment from OWF

MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- Unruh'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world
- Bennet-BCS'92: Quantum protocol for OT based on commitment schemes
- Damgard-FLSS'09 Bouman-F'10: Security proof of BBCS protocol based on strong classical commitment schemes (likely to lie outside of MiniCrypt)
- Bartusek-CKM'21 and **G**LSV'21: Quantum protocol for strong commitment from OWF

Corollary

Quantum protocol for MPC from OWF (i.e. MPC is in Mini**Q**Crypt)

MPC from Quantum+OWF

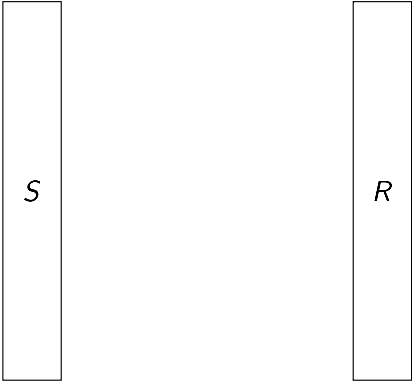
- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- Unruh'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world
- Bennet-BCS'92: Quantum protocol for OT based on commitment schemes
- Damgard-FLSS'09 Bouman-F'10: Security proof of BBCS protocol based on strong classical commitment schemes (likely to lie outside of MiniCrypt)
- Bartusek-CKM'21 and **G**LSV'21: Quantum protocol for strong commitment from OWF

Corollary

Quantum protocol for MPC from OWF (i.e. MPC is in Mini**Q**Crypt)
vs.
Impagliazzo-R'91: We don't expect MPC in MiniCrypt!

BBCS protocol (I)

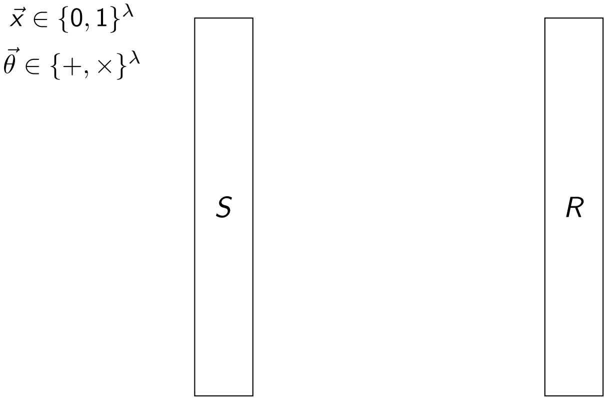
BBCS protocol (I)



S

R

BBCS protocol (I)



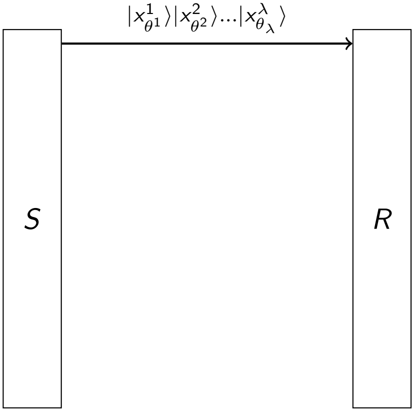
$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{+,\times\}^\lambda$

BBCS protocol (I)

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

$\vec{\theta} \in \{+,\times\}^\lambda$

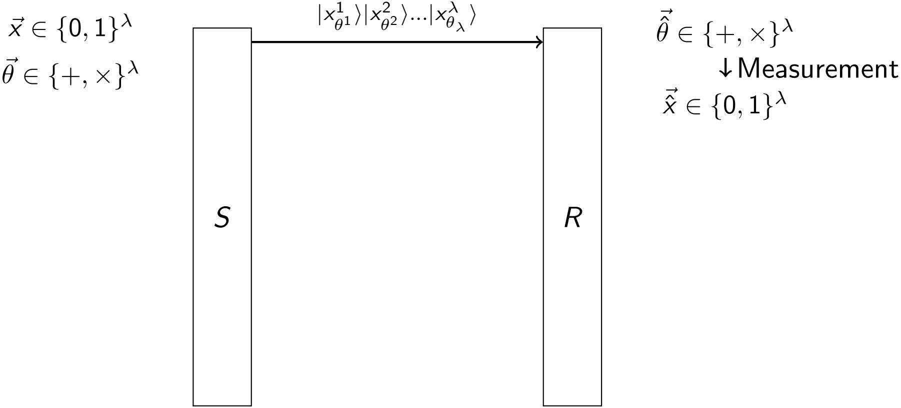


$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle...|x^\lambda_{\theta_\lambda}\rangle$

S

R

BBCS protocol (I)



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

$\vec{\theta} \in \{+,\times\}^\lambda$

$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle\ldots|x^\lambda_{\theta_\lambda}\rangle$

$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

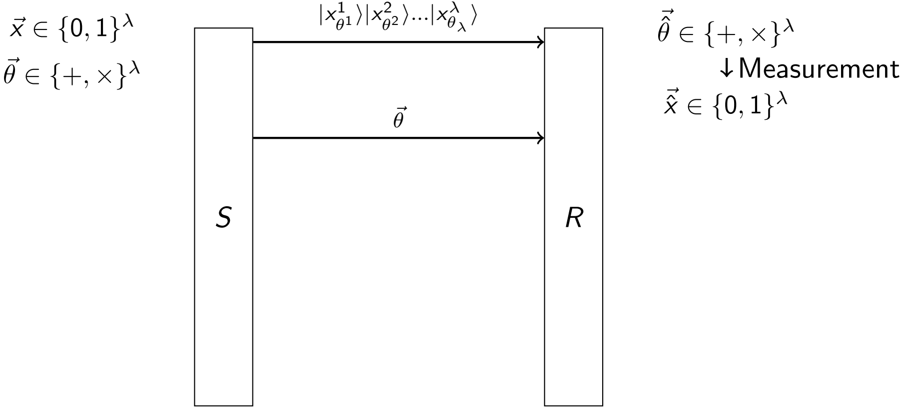
$\downarrow$Measurement

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

S

R

BBCS protocol (I)



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

$\vec{\theta} \in \{+, \times\}^\lambda$

$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle \dots |x^\lambda_{\theta_\lambda}\rangle$

$\vec{\theta}$

S

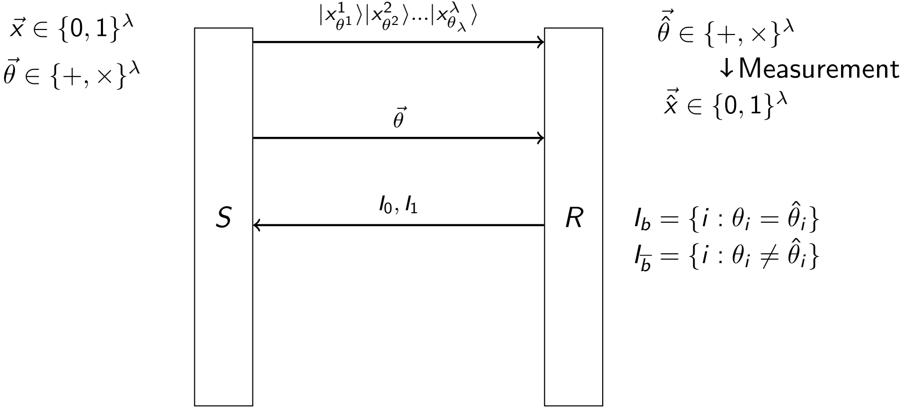
R

$\vec{\hat{\theta}} \in \{+, \times\}^\lambda$

$\downarrow$Measurement

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

BBCS protocol (I)



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

$\vec{\theta} \in \{+,\times\}^\lambda$

$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle ... |x^\lambda_{\theta_\lambda}\rangle$

$\vec{\theta}$

I_0, I_1

S

R

$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

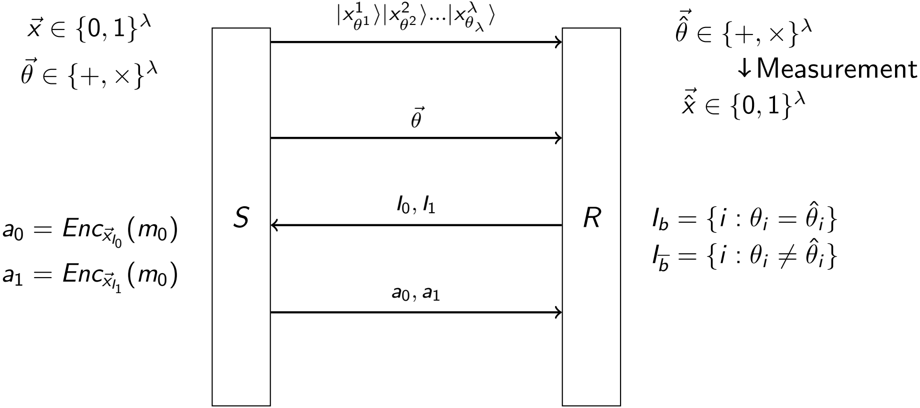
↓Measurement

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

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

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

BBCS protocol (I)



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

$\vec{\theta} \in \{+,\times\}^\lambda$

$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle\dots|x^\lambda_{\theta_\lambda}\rangle$

$\hat{\vec{\theta}} \in \{+,\times\}^\lambda$

↓Measurement

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

$\vec{\theta}$

I_0, I_1

S

R

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

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

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

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

a_0, a_1

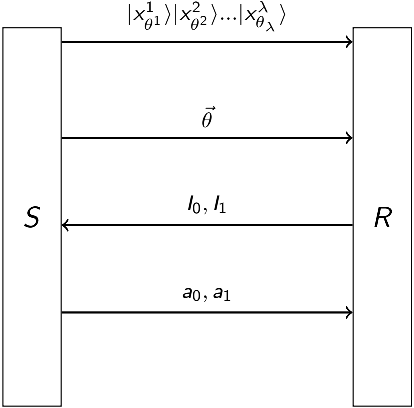
BBCS protocol (I)

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

$\vec{\theta} \in \{+,\times\}^\lambda$

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

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$



$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle\ldots|x^\lambda_{\theta_\lambda}\rangle$

$\vec{\theta}$

I_0, I_1

a_0, a_1

S

R

$\hat{\vec{\theta}} \in \{+,\times\}^\lambda$

$\downarrow$Measurement

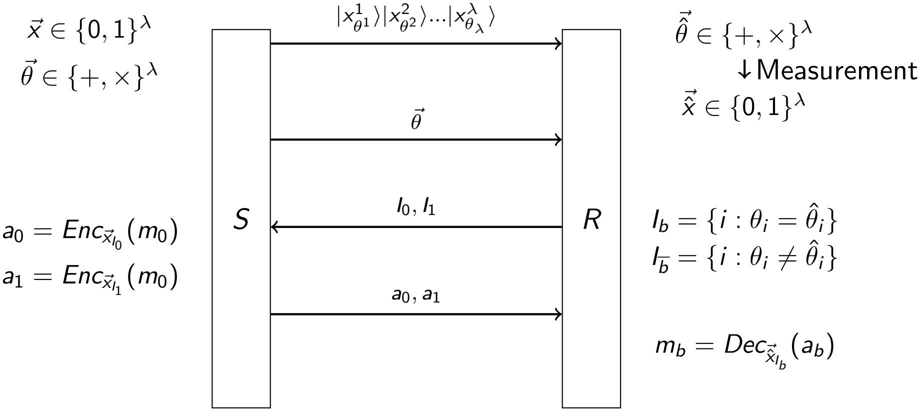
$\hat{\vec{x}} \in \{0,1\}^\lambda$

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

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

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

BBCS protocol (I)



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

$\vec{\theta} \in \{+,\times\}^\lambda$

$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle...|x^\lambda_{\theta_\lambda}\rangle$

$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

↓Measurement

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

$\vec{\theta}$

S

I_0, I_1

R

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

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

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

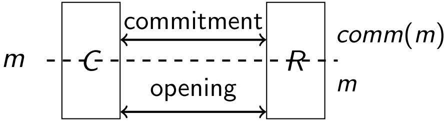
$I_{\overline{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

a_0, a_1

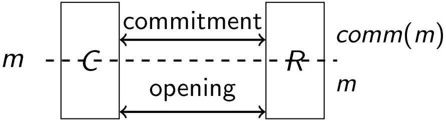
$m_b = Dec_{\vec{\hat{x}}_{I_b}}(a_b)$

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

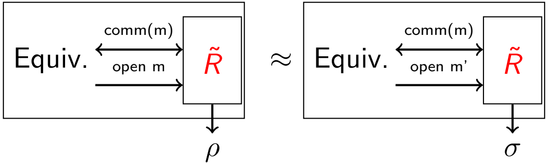
Bit-commitment with simulation security



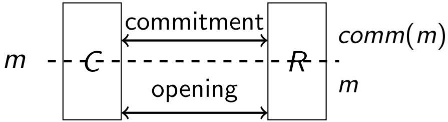
Bit-commitment with simulation security



Equivocality: “simulation” hiding

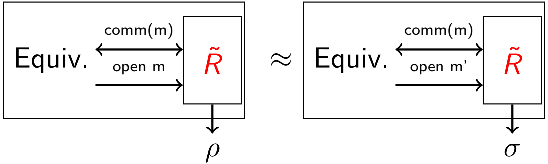


Bit-commitment with simulation security



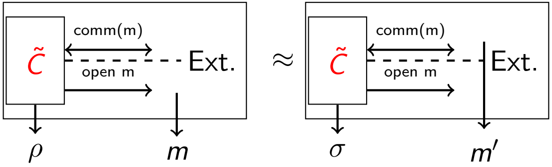
m C commitment opening R $comm(m)$ m

Equivocality: “simulation” hiding



Equiv. comm(m) open m $\tilde{R}$ ρ $\approx$ Equiv. comm(m) open m’ $\tilde{R}$ σ

Extractability: “simulation” binding

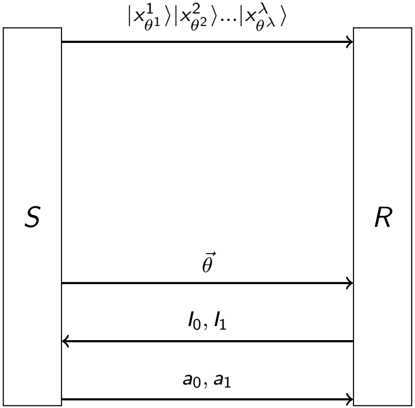


$\tilde{C}$ comm(m) open m Ext. ρ m $\approx$ $\tilde{C}$ comm(m) open m Ext. σ m'

BBCS protocol (II)

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

$\vec{\theta} \in \{+,\times\}^\lambda$



S

R

$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle\ldots|x^\lambda_{\theta^\lambda}\rangle$

$\vec{\theta}$

I_0, I_1

a_0, a_1

$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

↓Measurement

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

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

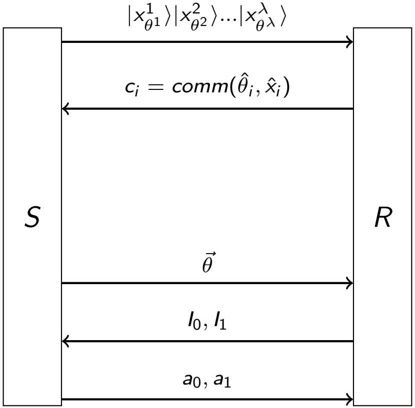
$I_{\bar{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

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

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

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

BBCS protocol (II)



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

$\vec{\theta} \in \{+,\times\}^{\lambda}$

$|x^{1}_{\theta^{1}}\rangle|x^{2}_{\theta^{2}}\rangle\ldots|x^{\lambda}_{\theta^{\lambda}}\rangle$

$\vec{\hat{\theta}} \in \{+,\times\}^{\lambda}$

↓Measurement

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

$c_i = comm(\hat{\theta}_i, \hat{x}_i)$

S

R

$\vec{\theta}$

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

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

I_0, I_1

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

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

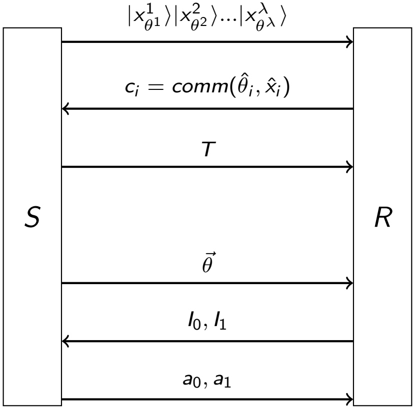
a_0, a_1

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

BBCS protocol (II)

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

$\vec{\theta} \in \{+,\times\}^\lambda$



S

R

$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle...|x^\lambda_{\theta^\lambda}\rangle$

$c_i = comm(\hat{\theta}_i, \hat{x}_i)$

T

$\vec{\theta}$

I_0, I_1

a_0, a_1

$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

↓Measurement

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

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

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

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

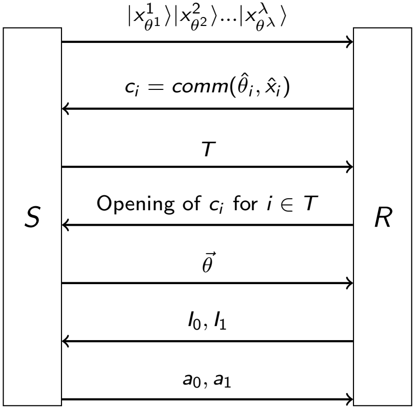
$$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$$

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

BBCS protocol (II)

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

$\vec{\theta} \in \{+,\times\}^\lambda$



$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle\ldots|x^\lambda_{\theta^\lambda}\rangle$

$c_i = comm(\hat{\theta}_i, \hat{x}_i)$

T

Opening of c_i for $i \in T$

$\vec{\theta}$

I_0, I_1

a_0, a_1

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

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

↓Measurement

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

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

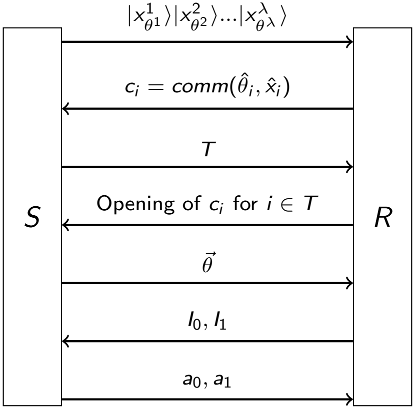
$I_{\overline{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

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

BBCS protocol (II)

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

$\vec{\theta} \in \{+,\times\}^\lambda$



$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

$\downarrow$Measurement

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

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

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

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

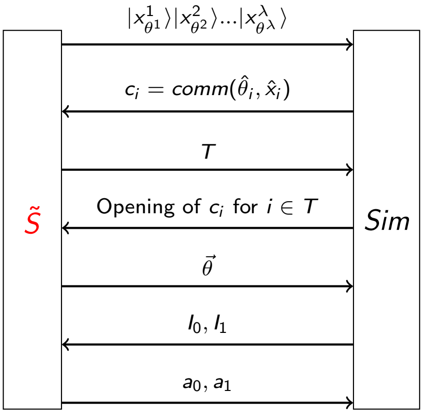
$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

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

Security of BBCS against malicious sender

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

$\vec{\theta} \in \{+,\times\}^\lambda$



$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle...|x^\lambda_{\theta^\lambda}\rangle$

$c_i = comm(\hat{\theta}_i, \hat{x}_i)$

T

Opening of c_i for $i \in T$

$\tilde{S}$

Sim

$\vec{\theta}$

I_0, I_1

a_0, a_1

$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

↓Measurement

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

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

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

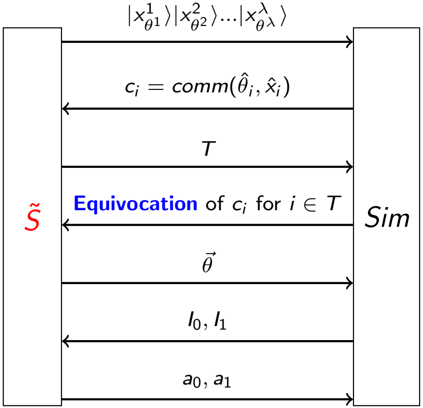
$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

Security of BBCS against malicious sender

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

$\vec{\theta} \in \{+,\times\}^\lambda$



$\tilde{S}$

Sim

$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle...|x^\lambda_{\theta^\lambda}\rangle$

$c_i = comm(\hat{\theta}_i, \hat{x}_i)$

T

Equivocation of c_i for $i \in T$

$\vec{\theta}$

I_0, I_1

a_0, a_1

$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

↓Measurement

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

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

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

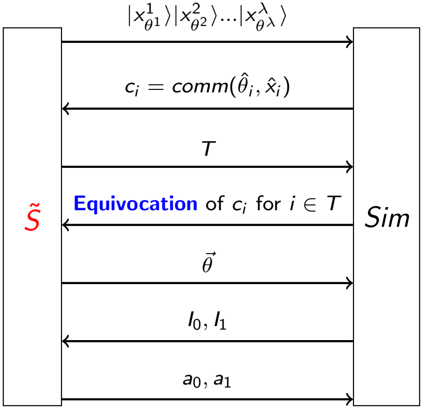
$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

Security of BBCS against malicious sender

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

$\vec{\theta} \in \{+,\times\}^\lambda$



$\tilde{S}$

$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle...|x^\lambda_{\theta^\lambda}\rangle$

$c_i = comm(\hat{\theta}_i, \hat{x}_i)$

T

Equivocation of c_i for $i \in T$

$\vec{\theta}$

I_0, I_1

a_0, a_1

Sim

Measure qubits in T

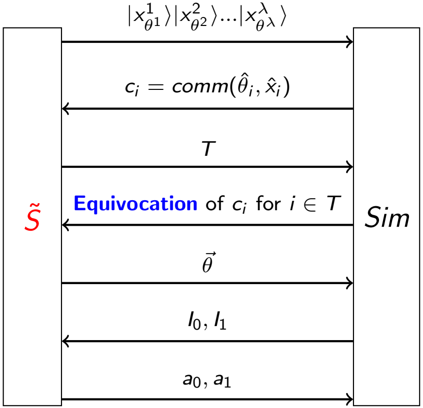
$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

Security of BBCS against malicious sender

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

$\vec{\theta} \in \{+,\times\}^\lambda$



$\tilde{S}$

Sim

$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle\ldots|x^\lambda_{\theta^\lambda}\rangle$

$c_i = comm(\hat{\theta}_i, \hat{x}_i)$

T

Equivocation of c_i for $i \in T$

$\vec{\theta}$

I_0, I_1

a_0, a_1

Measure qubits in T

Measure remaining qubits using $\vec{\theta}$ (get $\vec{x}$)

Partition I_0 and I_1 at random

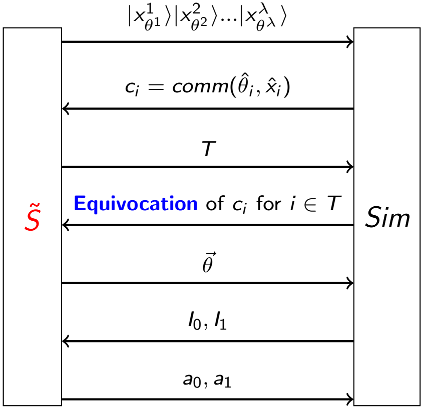
$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

Security of BBCS against malicious sender

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

$\vec{\theta} \in \{+,\times\}^{\lambda}$



$\tilde{S}$

Sim

$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle...|x^{\lambda}_{\theta^{\lambda}}\rangle$

$c_i = comm(\hat{\theta}_i, \hat{x}_i)$

T

Equivocation of c_i for $i \in T$

$\vec{\theta}$

I_0, I_1

a_0, a_1

Measure qubits in T

Measure remaining qubits using $\vec{\theta}$ (get $\vec{x}$)

Partition I_0 and I_1 at random

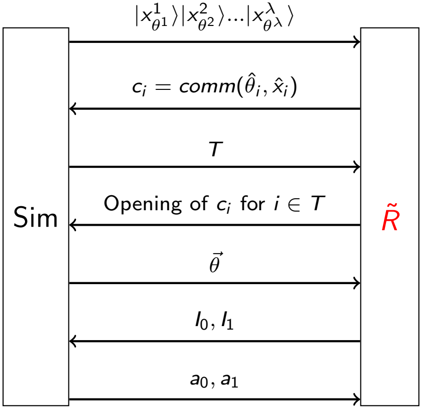
$$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$$
$$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$$

$$m_0 = Dec_{\hat{\vec{x}}_{I_0}}(a_0)$$
$$m_1 = Dec_{\hat{\vec{x}}_{I_1}}(a_1)$$

Security of BBCS against malicious receiver

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

$\vec{\theta} \in \{+,\times\}^\lambda$



Sim

$\tilde{R}$

$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle...|x^\lambda_{\theta^\lambda}\rangle$

$c_i = comm(\hat{\theta}_i, \hat{x}_i)$

T

Opening of c_i for $i \in T$

$\vec{\theta}$

I_0, I_1

a_0, a_1

$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

↓Measurement

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

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

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

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

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

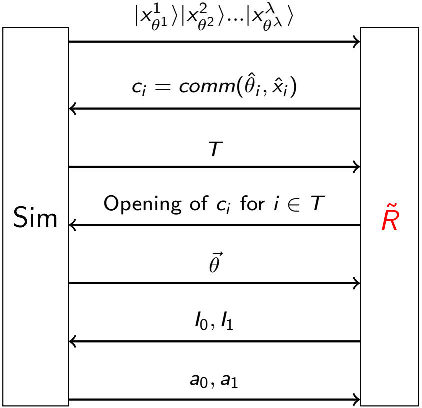
$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

Security of BBCS against malicious receiver

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

$\vec{\theta} \in \{+,\times\}^\lambda$

Extract $\vec{\hat{\theta}}$



$|x^1_{\theta^1}\rangle|x^2_{\theta^2}\rangle\dots|x^\lambda_{\theta^\lambda}\rangle$

$c_i = comm(\hat{\theta}_i, \hat{x}_i)$

T

Opening of c_i for $i \in T$

$\vec{\theta}$

I_0, I_1

a_0, a_1

$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

↓Measurement

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

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

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

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

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

Compute b

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

Implemententing commitment scheme with simulation security from OWF

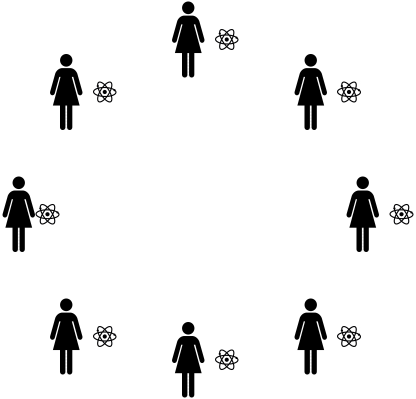
Implemententing commitment scheme with simulation security from OWF

[BCKM21]	[GLSV21]
1. (Black-box) equivocality compiler 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
- **Black-Box** use of one-way functions - **Statistical** security against malicious receiver	- **Constant-Round** OT in the CRS model - **Statistically binding** extractable commitment

Features:

Multi-party quantum computation

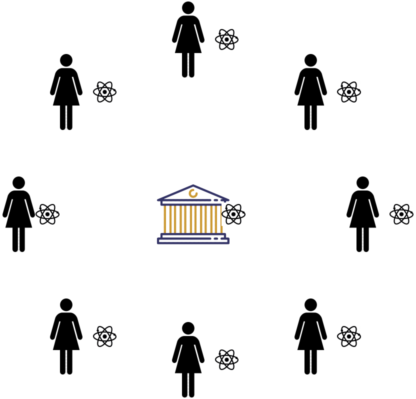
Parties share some input state $\rho_{A_1,\ldots,A_8}$



Goal: Compute U on joint share state ρ without revealing their share

Multi-party quantum computation

Parties share some input state $\rho_{A_1,\dots,A_8}$

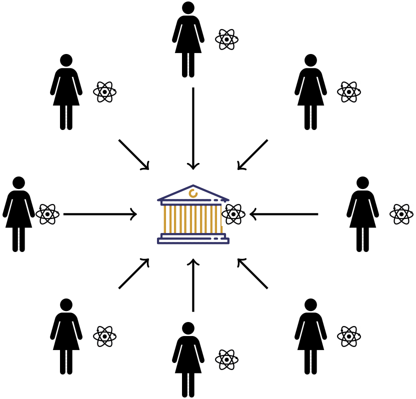


Goal: Compute U on joint share state ρ without revealing their share

Ideal world

Multi-party quantum computation

Parties share some input state $\rho_{A_1,\dots,A_8}$

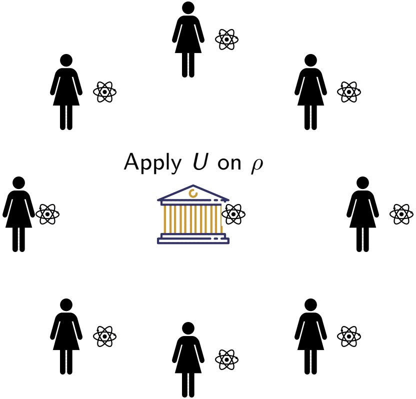


Goal: Compute U on joint share state ρ without revealing their share

Ideal world

Multi-party quantum computation

Parties share some input state $\rho_{A_1,...,A_8}$



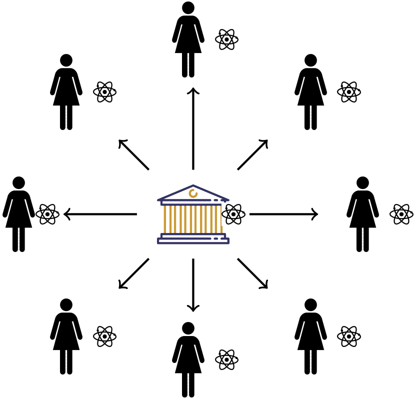
Apply U on ρ

Goal: Compute U on joint share state ρ without revealing their share

Ideal world

Multi-party quantum computation

Parties share some input state $\rho_{A_1,\dots,A_8}$



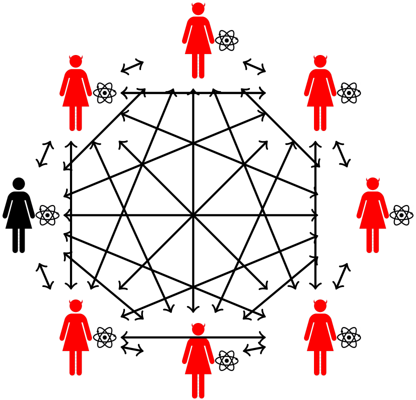
Goal: Compute U on joint share state ρ without revealing their share

Ideal world

- Each party gets their share of the output $U\rho U$

Multi-party quantum computation

Parties share some input state $\rho_{A_1 \dots A_8}$



Goal: Compute U on joint share state ρ without revealing their share

Ideal world

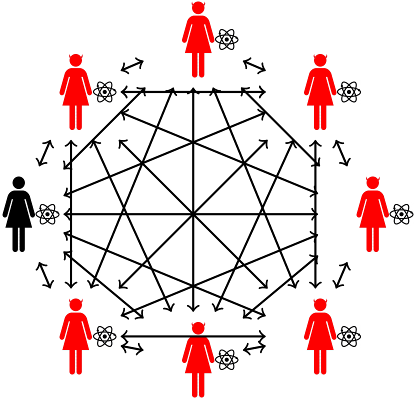
- Each party gets their share of the output $U\rho U$

Real world

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

Multi-party quantum computation

Parties share some input state $\rho_{A_1,\ldots,A_8}$



Goal: Compute U on joint share state ρ without revealing their share

Ideal world

- Each party gets their share of the output $U\rho U$

Real world

- Goal: implement the ideal functionality
- Protocols where parties interact, but still they only learn their share even if they behave disonestly
- Security definition similar to the classical setting

MPQC

- Statistically secure MPQC with honest majority [Crépeau-GS'02,BenOr-CGHS'06]
- Computationally secure 2PQC [Dupuis-NS'10, Dupuis-NS'12, Kashefi-MW'17]
- MPQC with allowed dishonest subsets [Kashefi-P'17]
- Computationally secure MPQC with arbitrary dishonest majority [Dulek-**G**JMS'20]

MPQC

- Statistically secure MPQC with honest majority [Crépeau-GS'02,BenOr-CGHS'06]
- Computationally secure 2PQC [Dupuis-NS'10, Dupuis-NS'12, Kashefi-MW'17]
- MPQC with allowed dishonest subsets [Kashefi-P'17]
- **Computationally secure MPQC with arbitrary dishonest majority** [Dulek-**G**JMS'20]

MPQC

- Statistically secure MPQC with honest majority [Crépeau-GS'02,BenOr-CGHS'06]
- Computationally secure 2PQC [Dupuis-NS'10, Dupuis-NS'12, Kashefi-MW'17]
- MPQC with allowed dishonest subsets [Kashefi-P'17]
- **Computationally secure MPQC with arbitrary dishonest majority** [Dulek-**G**JMS'20]
    - Extends DNS'12 to the multi-party setting
    - Assumes ideal MPC functionality ($\mathcal{F}_{MPC}$)

Clifford encoding

Clifford encoding

Clifford operations:

Unitaries generated by $\{H, P, CNOT\}$

$\mathcal{C}_m = \{$Clifford circuits on m qubits $\}$

Clifford encoding

Clifford operations:
Unitaries generated by $\{H, P, CNOT\}$
$\mathcal{C}_m = \{\text{Clifford circuits on } m \text{ qubits }\}$

Clifford encoding for n-qubit state $|\psi\rangle$ and security parameter λ:

1. Pick a random $(\lambda + n)$-qubit Clifford C
2. $C(|\psi\rangle \otimes |0^\lambda\rangle)$

Clifford encoding

Clifford operations:
Unitaries generated by $\{H, P, CNOT\}$
$\mathcal{C}_m = \{$Clifford circuits on m qubits $\}$

Clifford encoding for n-qubit state $|\psi\rangle$ and security parameter λ:

1. Pick a random $(\lambda + n)$-qubit Clifford C
2. $C(|\psi\rangle \otimes |0^\lambda\rangle)$

Privacy:
$C|\psi\rangle$ is one-time padded

Clifford encoding

Clifford operations:
Unitaries generated by $\{H, P, CNOT\}$
$\mathcal{C}_m = \{$Clifford circuits on m qubits $\}$

Clifford encoding for n-qubit state $|\psi\rangle$ and security parameter λ:

1. Pick a random $(\lambda + n)$-qubit Clifford C
2. $C(|\psi\rangle \otimes |0^\lambda\rangle)$

Privacy:
$C|\psi\rangle$ is one-time padded

Authentication:
For any non-trivial $\mathcal{A}$, trap qubits of $C^\dagger \mathcal{A}(C|\psi\rangle|0^n\rangle)$ will be non-zero w.p. $1 - \text{negl}(\lambda)$

MPQC protocol - General idea

Focus on a single (pure) qubit

MPQC protocol - General idea

Focus on a single (pure) qubit

- P_{i^*} holds $C(|\psi\rangle|0^{2\lambda}\rangle)$
- All players (secret) share C
  - Players share random C_i's s.t. $C_k \dots C_1 = C$

MPQC protocol - General idea

Focus on a single (pure) qubit

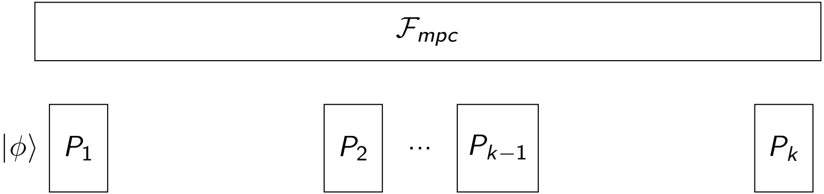
- P_{i^*} holds $C(|\psi\rangle|0^{2\lambda}\rangle)$
- All players (secret) share C
    - Players share random C_i's s.t. $C_k \ldots C_1 = C$
- Public authentication test
    - λ trap qubits used in the test
    - remaining λ to keep privacy/authentication even in the test

MPQC protocol - General idea

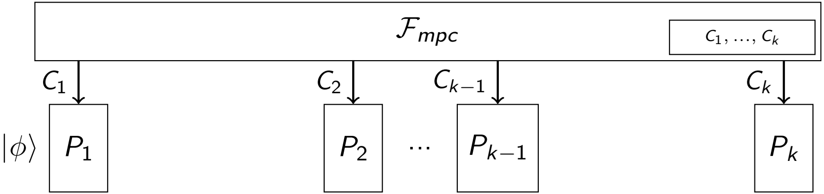
Focus on a single (pure) qubit

- P_{i^*} holds $C(|\psi\rangle|0^{2\lambda}\rangle)$
- All players (secret) share C
  - Players share random C_i's s.t. $C_k ... C_1 = C$
- Public authentication test
  - λ trap qubits used in the test
  - remaining λ to keep privacy/authentication even in the test
- Computation on encoded data

MPQC protocol - Encoding

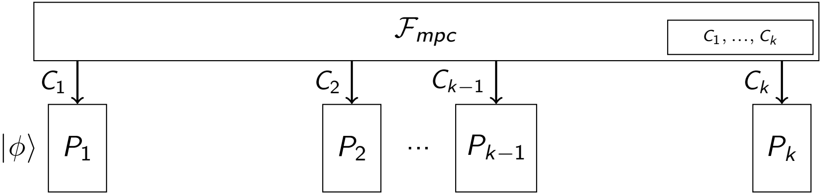


MPQC protocol - Encoding



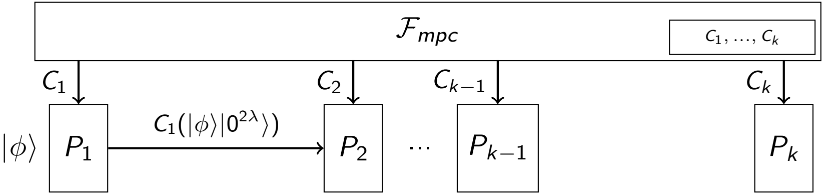
- $\mathcal{F}_{mpc}$ computes random $\{C_i\}_{2\lambda+1}$

MPQC protocol - Encoding



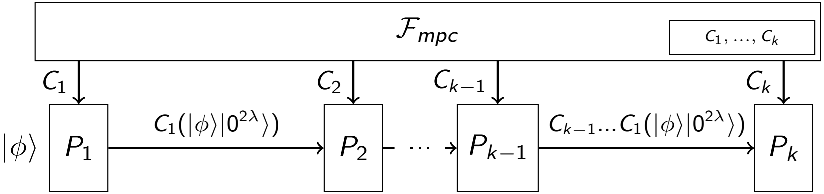
- $\mathcal{F}_{mpc}$ computes random $\{C_i\}_{2\lambda+1}$, parties apply C_i and send the state around the table

MPQC protocol - Encoding



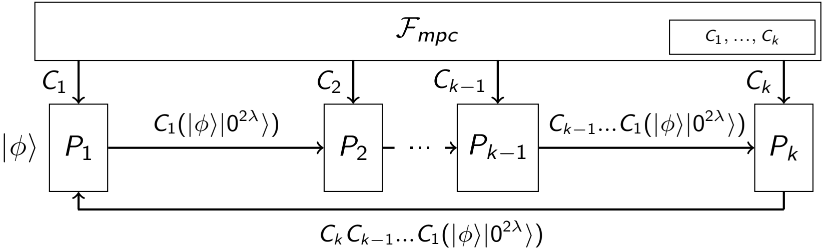
- $\mathcal{F}_{mpc}$ computes random $\{C_i\}_{2\lambda+1}$, parties apply C_i and send the state around the table

MPQC protocol - Encoding



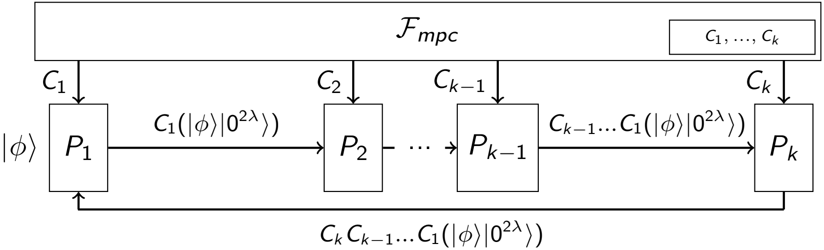
- $\mathcal{F}_{mpc}$ computes random $\{C_i\}_{2\lambda+1}$, parties apply C_i and send the state around the table

MPQC protocol - Encoding



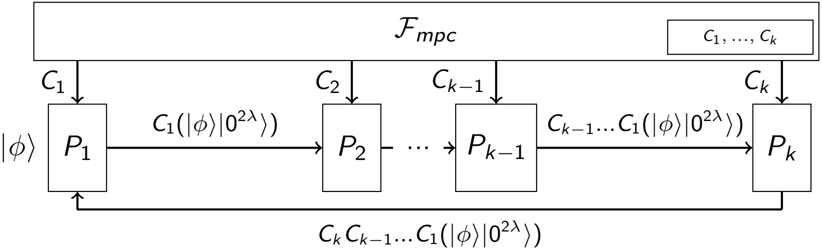
- $\mathcal{F}_{mpc}$ computes random $\{C_i\}_{2\lambda+1}$, parties apply C_i and send the state around the table

MPQC protocol - Encoding



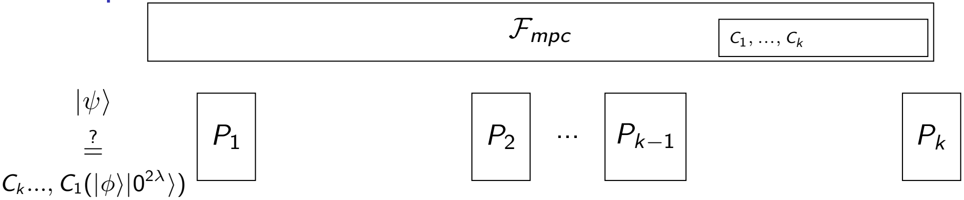
- $\mathcal{F}_{mpc}$ computes random $\{C_i\}_{2\lambda+1}$, parties apply C_i and send the state around the table
- How to prevent that any of the parties replaces the quantum state (or cheat arbitrarily)?

MPQC protocol - Encoding



- $\mathcal{F}_{mpc}$ computes random $\{C_i\}_{2\lambda+1}$, parties apply C_i and send the state around the table
- How to prevent that any of the parties replaces the quantum state (or cheat arbitrarily)?
  - Public authentication test

MPQC protocol - Public authentication test



$\mathcal{F}_{mpc}$

$C_1, \ldots, C_k$

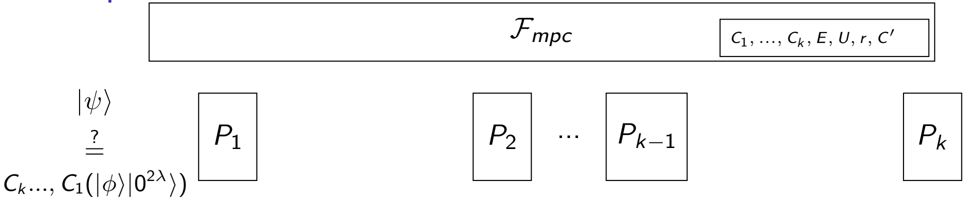
$$|\psi\rangle \overset{?}{=} C_k \ldots, C_1(|\phi\rangle|0^{2\lambda}\rangle)$$

P_1

P_2 $\cdots$ P_{k-1}

P_k

MPQC protocol - Public authentication test



$\mathcal{F}_{mpc}$

$C_1, \ldots, C_k, E, U, r, C'$

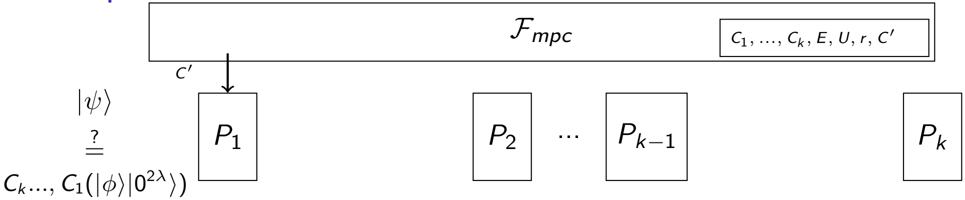
$|\psi\rangle \overset{?}{=} C_k \ldots, C_1(|\phi\rangle|0^{2\lambda}\rangle)$

P_1 P_2 $\cdots$ P_{k-1} P_k

- $\mathcal{F}_{mpc}$ computes random $C' \in \mathcal{C}_{2\lambda+1}$, $E \in \mathcal{C}_{\lambda+1}$, linear function U and $r \in \{0,1\}^{\lambda}$ s.t.

$$C' = (E \otimes X^r)(I_2 \otimes U)C_1^{\dagger} \ldots C_{k-1}^{\dagger} C_k^{\dagger}$$

MPQC protocol - Public authentication test



$\mathcal{F}_{mpc}$

$C_1, \ldots, C_k, E, U, r, C'$

C'

$|\psi\rangle \overset{?}{=} C_k \ldots, C_1(|\phi\rangle|0^{2\lambda}\rangle)$

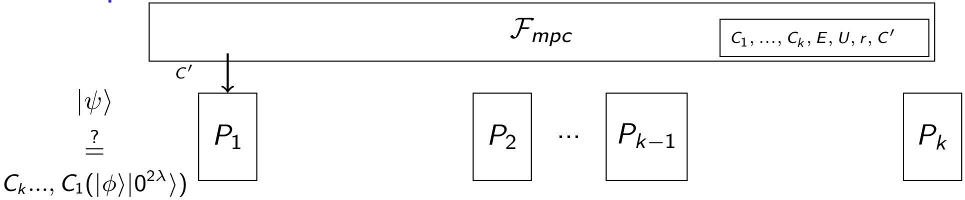
P_1 P_2 $\cdots$ P_{k-1} P_k

- $\mathcal{F}_{mpc}$ computes random $C' \in \mathcal{C}_{2\lambda+1}$, $E \in \mathcal{C}_{\lambda+1}$, linear function U and $r \in \{0,1\}^{\lambda}$ s.t.

$$C' = (E \otimes X^r)(I_2 \otimes U)C_1^{\dagger} \ldots C_{k-1}^{\dagger} C_k^{\dagger}$$

- $\mathcal{F}_{MPC}$ sends only C' to P_1 and P_1 applies C' on $|\psi\rangle$

MPQC protocol - Public authentication test



$\mathcal{F}_{mpc}$

$C_1, \ldots, C_k, E, U, r, C'$

C'

$|\psi\rangle \stackrel{?}{=} C_k \ldots, C_1(|\phi\rangle|0^{2\lambda}\rangle)$

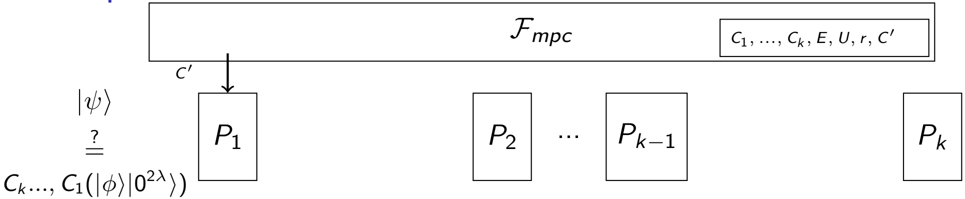
P_1 P_2 $\cdots$ P_{k-1} P_k

- $\mathcal{F}_{mpc}$ computes random $C' \in \mathcal{C}_{2\lambda+1}$, $E \in \mathcal{C}_{\lambda+1}$, linear function U and $r \in \{0,1\}^\lambda$ s.t.

$$C' = (E \otimes X^r)(I_2 \otimes U)C_1^\dagger \ldots C_{k-1}^\dagger C_k^\dagger$$

- $\mathcal{F}_{MPC}$ sends only C' to P_1 and P_1 applies C' on $|\psi\rangle$
  - Honest case: $E(|\phi\rangle|0^\lambda\rangle)|r\rangle$

MPQC protocol - Public authentication test



$\mathcal{F}_{mpc}$

$C_1, \dots, C_k, E, U, r, C'$

C'

$|\psi\rangle \overset{?}{=} C_k \dots, C_1(|\phi\rangle|0^{2\lambda}\rangle)$

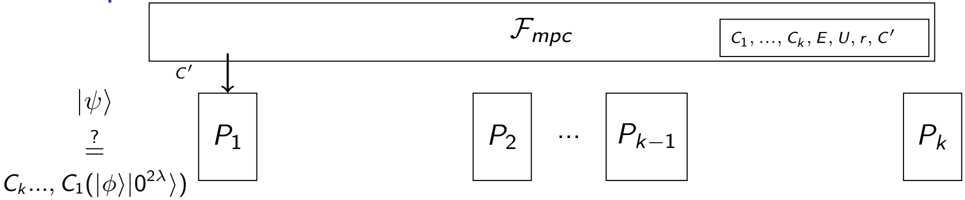
P_1 P_2 $\cdots$ P_{k-1} P_k

- $\mathcal{F}_{mpc}$ computes random $C' \in \mathcal{C}_{2\lambda+1}$, $E \in \mathcal{C}_{\lambda+1}$, linear function U and $r \in \{0,1\}^\lambda$ s.t.

$$C' = (E \otimes X^r)(I_2 \otimes U)C_1^\dagger \dots C_{k-1}^\dagger C_k^\dagger$$

- $\mathcal{F}_{MPC}$ sends only C' to P_1 and P_1 applies C' on $|\psi\rangle$
  - Honest case: $E(|\phi\rangle|0^\lambda\rangle)|r\rangle$
  - Dishonest case: last λ qubits are different of r with overwhelming probability

MPQC protocol - Public authentication test



$\mathcal{F}_{mpc}$

$C_1, \dots, C_k, E, U, r, C'$

C'

$|\psi\rangle$

$\overset{?}{=}$

$C_k \dots, C_1(|\phi\rangle|0^{2\lambda}\rangle)$

P_1

P_2 $\cdots$ P_{k-1}

P_k

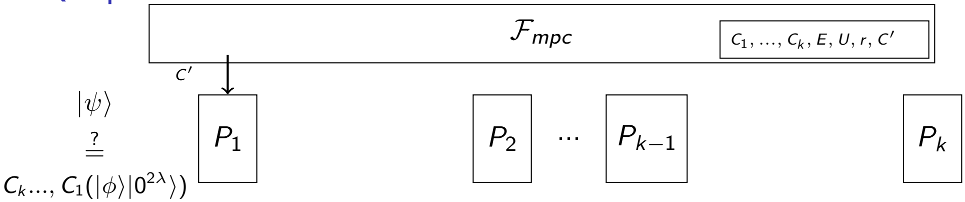
- $\mathcal{F}_{mpc}$ computes random $C' \in \mathcal{C}_{2\lambda+1}$, $E \in \mathcal{C}_{\lambda+1}$, linear function U and $r \in \{0,1\}^{\lambda}$ s.t.

$$C' = (E \otimes X^r)(I_2 \otimes U)C_1^{\dagger} \dots C_{k-1}^{\dagger} C_k^{\dagger}$$

- $\mathcal{F}_{MPC}$ sends only C' to P_1 and P_1 applies C' on $|\psi\rangle$
  - Honest case: $E(|\phi\rangle|0^{\lambda}\rangle)|r\rangle$
  - Dishonest case: last λ qubits are different of r with overwhelming probability

Unknown to all parties!

MPQC protocol - Public authentication test



$\mathcal{F}_{mpc}$

$C_1, \ldots, C_k, E, U, r, C'$

C'

$$|\psi\rangle \overset{?}{=} C_k \ldots, C_1(|\phi\rangle|0^{2\lambda}\rangle)$$

P_1 P_2 $\cdots$ P_{k-1} P_k

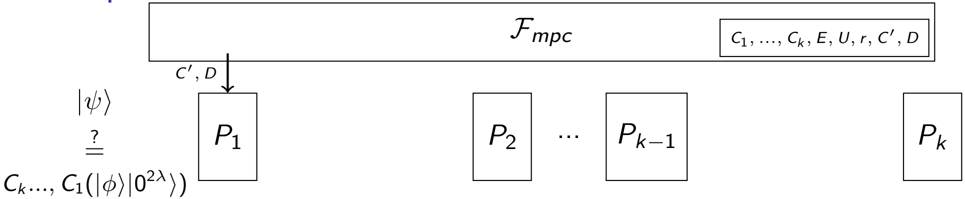
- $\mathcal{F}_{mpc}$ computes random $C' \in \mathcal{C}_{2\lambda+1}$, $E \in \mathcal{C}_{\lambda+1}$, linear function U and $r \in \{0,1\}^{\lambda}$ s.t.

$$C' = (E \otimes X^r)(I_2 \otimes U)C_1^{\dagger} \ldots C_{k-1}^{\dagger} C_k^{\dagger}$$

- $\mathcal{F}_{MPC}$ sends only C' to P_1 and P_1 applies C' on $|\psi\rangle$
  - Honest case: $E(|\phi\rangle|0^{\lambda}\rangle)|r\rangle$
  - Dishonest case: last λ qubits are different of r with overwhelming probability

    Unknown to all parties!
- Parties interact with $\mathcal{F}_{MPC}$ to check if the value of the traps is correct

MPQC protocol - Public authentication test



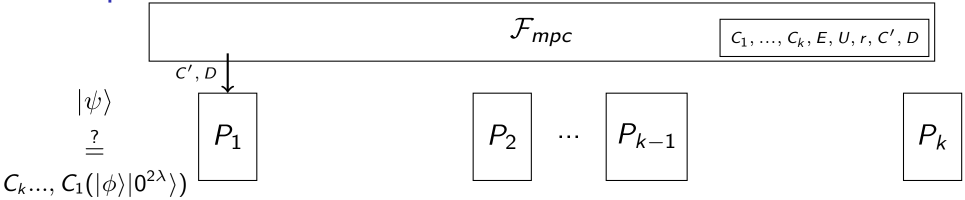
- $\mathcal{F}_{mpc}$ computes random $C' \in \mathcal{C}_{2\lambda+1}$, $E \in \mathcal{C}_{\lambda+1}$, linear function U and $r \in \{0,1\}^\lambda$ s.t.

$$C' = (E \otimes X^r)(I_2 \otimes U)C_1^\dagger \dots C_{k-1}^\dagger C_k^\dagger$$

- $\mathcal{F}_{MPC}$ sends only C' to P_1 and P_1 applies C' on $|\psi\rangle$
    - Honest case: $E(|\phi\rangle|0^\lambda\rangle)|r\rangle$
    - Dishonest case: last λ qubits are different of r with overwhelming probability

      Unknown to all parties!
- Parties interact with $\mathcal{F}_{MPC}$ to check if the value of the traps is correct
- $\mathcal{F}_{MPC}$ sends new $D \in \mathcal{C}_{2\lambda+1}$ to P_1

MPQC protocol - Public authentication test



$\mathcal{F}_{mpc}$

$C_1, \dots, C_k, E, U, r, C', D$

C', D

$|\psi\rangle \overset{?}{=} C_k \dots, C_1(|\phi\rangle|0^{2\lambda}\rangle)$

P_1 P_2 $\cdots$ P_{k-1} P_k

- $\mathcal{F}_{mpc}$ computes random $C' \in \mathcal{C}_{2\lambda+1}$, $E \in \mathcal{C}_{\lambda+1}$, linear function U and $r \in \{0,1\}^\lambda$ s.t.

$$C' = (E \otimes X^r)(I_2 \otimes U)C_1^\dagger \dots C_{k-1}^\dagger C_k^\dagger$$

- $\mathcal{F}_{MPC}$ sends only C' to P_1 and P_1 applies C' on $|\psi\rangle$
  - Honest case: $E(|\phi\rangle|0^\lambda\rangle)|r\rangle$
  - Dishonest case: last λ qubits are different of r with overwhelming probability

    Unknown to all parties!
- Parties interact with $\mathcal{F}_{MPC}$ to check if the value of the traps is correct
- $\mathcal{F}_{MPC}$ sends new $D \in \mathcal{C}_{2\lambda+1}$ to P_1
- Similar procedure enables (secure) public measurement in the computational basis

MPQC protocol - Applying gates

1. One-qubit Clifford D: can be perfomed by "changing the key"

$$C_k ... C_1(|\phi\rangle|0^{2\lambda}\rangle) = C_k ... C_1'(D|\phi\rangle|0^{2\lambda}\rangle), \text{ for } C_1' = C_1 D^\dagger$$

MPQC protocol - Applying gates

1. One-qubit Clifford D: can be perfomed by "changing the key"

$$C_k \dots C_1(|\phi\rangle|0^{2\lambda}\rangle) = C_k \dots C_1'(D|\phi\rangle|0^{2\lambda}\rangle), \text{ for } C_1' = C_1 D^\dagger$$

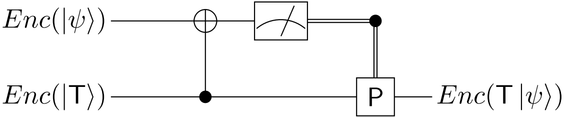
2. CNOT:
    1. Send two qubits to a single party (+ public authentication test)
    2. Re-encode the two qubits altogether (+ public authentication test)
    3. Apply CNOT "changing the key"
    4. Split the encoding of the two qubits (+ public authentication test)
    5. Send each qubit to the corresponding party (+ public authentication test)

MPQC protocol - Applying gates

1. One-qubit Clifford D: can be perfomed by "changing the key"

$$C_k \ldots C_1(|\phi\rangle|0^{2\lambda}\rangle) = C_k \ldots C_1'(D|\phi\rangle|0^{2\lambda}\rangle), \text{ for } C_1' = C_1 D^\dagger$$

2. CNOT:
   1. Send two qubits to a single party (+ public authentication test)
   2. Re-encode the two qubits altogether (+ public authentication test)
   3. Apply CNOT "changing the key"
   4. Split the encoding of the two qubits (+ public authentication test)
   5. Send each qubit to the corresponding party (+ public authentication test)
3. T-gate:



MPQC protocol - creating T magic states

MPQC protocol - creating T magic states

1. P_1 create $poly(\lambda, k)$ T-magic states
2. Parties run sub-protocol to encode the (supposed) magic states
3. Each party tests a random subset
    - Locally decode (with the help of $\mathcal{F}_{mpc}$)
    - Check if the “raw” qubit is indeed $|T\rangle$
4. Use magic state destillation procedure to transform somewhat-good T-magic states into almost-perfect ones
    - Only need Clifford circuit + measurement

MPQC protocol - overall protocol

MPQC protocol - overall protocol

Protocol

1. Parties run sub-protocol to create $Enc(|T\rangle^{\otimes t})$
2. Parties run sub-protocol to encode each qubit
3. For each gate/measurement, parties run the corresponding sub-protocol
4. Each party decodes her own output (with the help of $\mathcal{F}_{MPC}$)

Summary

Zero-knowledge proofs

Central tool in crypto toolbox

1. ZK for NP in MiniCrypt
2. ZK against quantum adversaries
3. ZK for QMA ("quantum NP")

Multi-party computation

Most-general functionality (modulo #rounds)

1. MPC from Oblivious transfer
2. OT is in Mini**Q**Crypt
3. Multi-party quantum computation

Some open questions

1. (Im)possitiblity of constant-round quantum ZK protocol in the plain model
2. Applications of zero-knowledge for quantum proofs
3. (Q)NIZK for QMA with RO/CRS
4. Zero-knowledge with multiple non-signaling provers
5. (Im)possibility of MPQC in constant rounds
6. (Black-box) separations of cryptographic primitives in the quantum setting
7. Further quantum protocols from weaker assumptions
8. Practical quantum cryptographic protocols
9. ...

Some open questions

1. (Im)possitiblity of constant-round quantum ZK protocol in the plain model
2. Applications of zero-knowledge for quantum proofs
3. (Q)NIZK for QMA with RO/CRS
4. Zero-knowledge with multiple non-signaling provers
5. (Im)possibility of MPQC in constant rounds
6. (Black-box) separations of cryptographic primitives in the quantum setting
7. Further quantum protocols from weaker assumptions
8. Practical quantum cryptographic protocols
9. ...

Thank you for your attention!