Oblivious Transfer from Zero-Knowledge Proofs

or How to Achieve Round-Optimal Quantum Oblivious Transfer and Zero-Knowledge Proofs on Quantum States

Léo Colisson, Garazi Muguruza, Florian Speelman

CWI · University of Amsterdam · QuSoft

ASIACRYPT 2023


?
<
Multi-Party Computing (MPC)


Oblivious
Transfer

Oblivious Transfer
m_0
m_1


b
Oblivious
Transfer
m_0
m_1


b
Oblivious Transfer
m_0
m_1
m_b

OT: state of the art

Oblivious Transfer (OT) : studied a lot ([Rab81], [EGL85], [PVW08], [BD18], [GLSV22], [BCKM21]. . .)

State of the art

Classical	Quantum
Requires trapdoors (= CryptoMania, asymmetric crypto)	No structure is necessary (= hash function)
2 messages	7 messages ([CK88]/[BBCS92]. . .) → 3 messages ([ABKK23])

With **pre-shared EPR pairs:**
[BKS23]: 1-message **random** receiver bit string OT & 2-message OT

[Agarwal, Bartusek, Khurana, Kumar 23] raises the question:

? Is there an OT protocol in 2-messages (optimal) without structure?

Our contributions

Yes !

Theorem 1 (informal)

There exists a 2-message (optimal) quantum OT protocol secure in the Random Oracle Model (i.e. no structure) assuming the existence of a hiding collision-resistant hash function.

Our approach

- No structure is necessary
  (= hash function)
- 2 messages

Methods

Remove cut-and-choose: classical Zero-Knowledge proofs + quantum protocol
= prove a statement on a quantum state non-destructively.


Proof


Proof


Proof


Proof


Either:
Qubits 1 & 2 collapsed
or qubits 2 & 3 collapsed
Proof


Either:
Qubits 1 & 2 collapsed
or qubits 2 & 3 collapsed
I trust you!
But which are the
collapsed ones?
Proof


Secret !
I trust you!
But which are the
collapsed ones?
Proof

Our contributions

We can prove that a received quantum state belongs to a fixed set of quantum state:

Theorem 2 (informal)

For any arbitrary predicate $\mathcal{P}$, there exists a protocol such that:

- *The prover chooses a secret subset S of qubits such that $\mathcal{P}(S) = \top$*
- *At the end of the protocol, the verifier ends up with a quantum state such that qubits in S are collapsed (measured in computational basis), even if the prover is malicious*
- *S stays unknown to the verifier*

($\mathcal{P}$ allows us to get string-OT, k-out-of-n OT...)

Complexity theory:
$\Rightarrow$ generalize ZK proofs to quantum languages (ZKstatesQMA)

(we do not characterize ZKstatesQMA/ZKstatesQIP completely, but we define them and show they are not trivial)


Zero
Knowledge
Our
Work


Our Work
Oblivious Transfer


NIZK
[Unr15]
Our
Work


Our Work
Oblivious Transfer (2-messages)


ZK plain-model
[HSS11]
Our
Work


Our Work
Oblivious Transfer (plain-model)

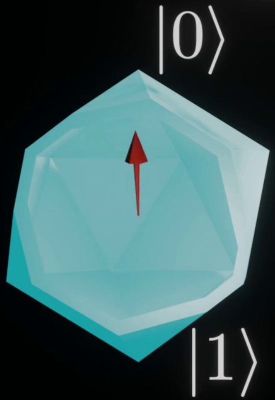
Theorem 3 (ZK $\Rightarrow$ quantum OT, informal)

Assuming the existence of a collision-resistant hidding function, there exists a protocol turning any n-message, post-quantum Zero-Knowledge (ZK) proof of knowledge into an $(n+1)$-message quantum OT protocol assuming a Common Random String model or $n+2$ without further setup assumptions.

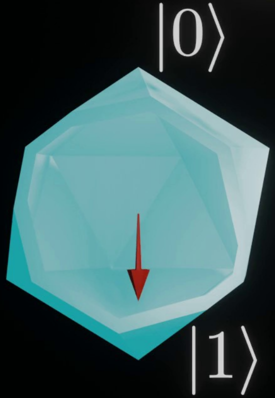
The security properties (statistical security, etc.) and assumptions (setup, computational assumptions, etc.) of the ZK protocol are mostly preserved.

Article	Classical	Setup	Messages	MiniQCrypt	Composable	Statistical
This work + [Unr15]	No	RO	2	Yes	Yes	No
This work + [HSS11]	No	Plain M.	> 2	No (LWE)	Yes	No
This work + S-NIZK	No	Like ZK	2	Like ZK	Yes	Sender
This work + NIZK proof	No	Like ZK	2	Like ZK	Yes	Receiver
This work + ZK	No	Like ZK	ZK + 1 or 2	Like ZK	Yes	Like ZK

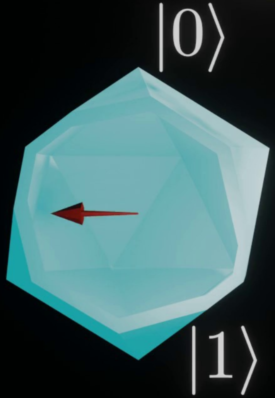
Qubits



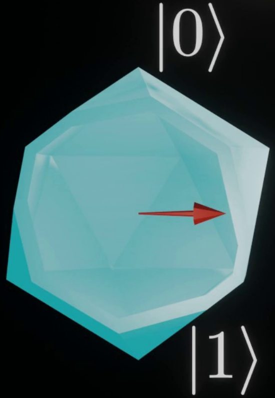
Qubits



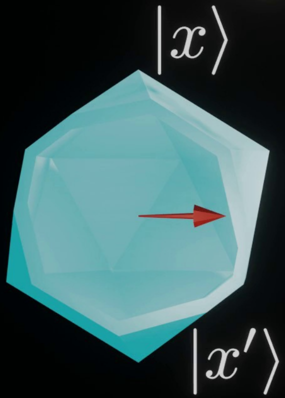
Qubits



Qubits



Qubits



Superposition

$$a_x |x\rangle + a_{x'} |x'\rangle$$

Qubits

Superposition

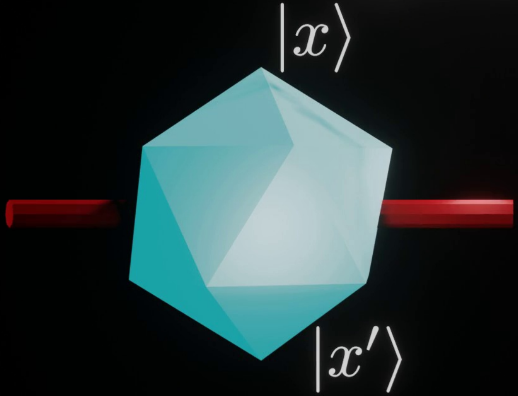
$$a_x\,|x\rangle + a_{x'}\,|x'\rangle$$

Qubits

Superposition

$$a_x \, |x\rangle + a_{x'} \, |x'\rangle$$

Qubits



Superposition

$$a_x \left|x\right\rangle + a_{x'} \left|x'\right\rangle$$

Qubits

$|x\rangle$

d

$|x'\rangle$

Superposition

$$a_x |x\rangle + a_{x'} |x'\rangle$$

Oblivious Transfer
b
m_0
m_1
m_b


b
m_0
m_1


If $b = 0$
m_0
m_1

If $b = 0$
r
m_0
m_1

If $b = 1$
m_0
m_1
r

If $b = 1$
m_0
m_1
r
Proof
One qubit comp. basis


If $b = 1$
m_0
m_1
r
Proof

If $b = 1$
m_0
m_1
r
$R_z^{m_0}$
$R_z^{m_1}$
Proof


If $b = 1$
r
m_0
m_1
$R_z^{m_0}$
$R_z^{m_1}$
Proof

If $b = 1$
m_0
m_1
r
Proof

If $b = 1$
m_0
m_1
s_0
r
Proof

If $b = 1$
m_0
m_1
s_0
s_1
r
Proof


If $b = 1$
m_0
m_1
s_0
s_1
r
$= m_1 \oplus r$
Proof

If $b = 1$
m_0
m_1
s_0
s_1
r
Proof


If $b = 1$
m_0
m_1
r s_0 s_1
Proof


If $b = 1$
m_0
m_1
$r \quad s_0 \quad s_1$
$m_b = s_b \oplus r$
Proof

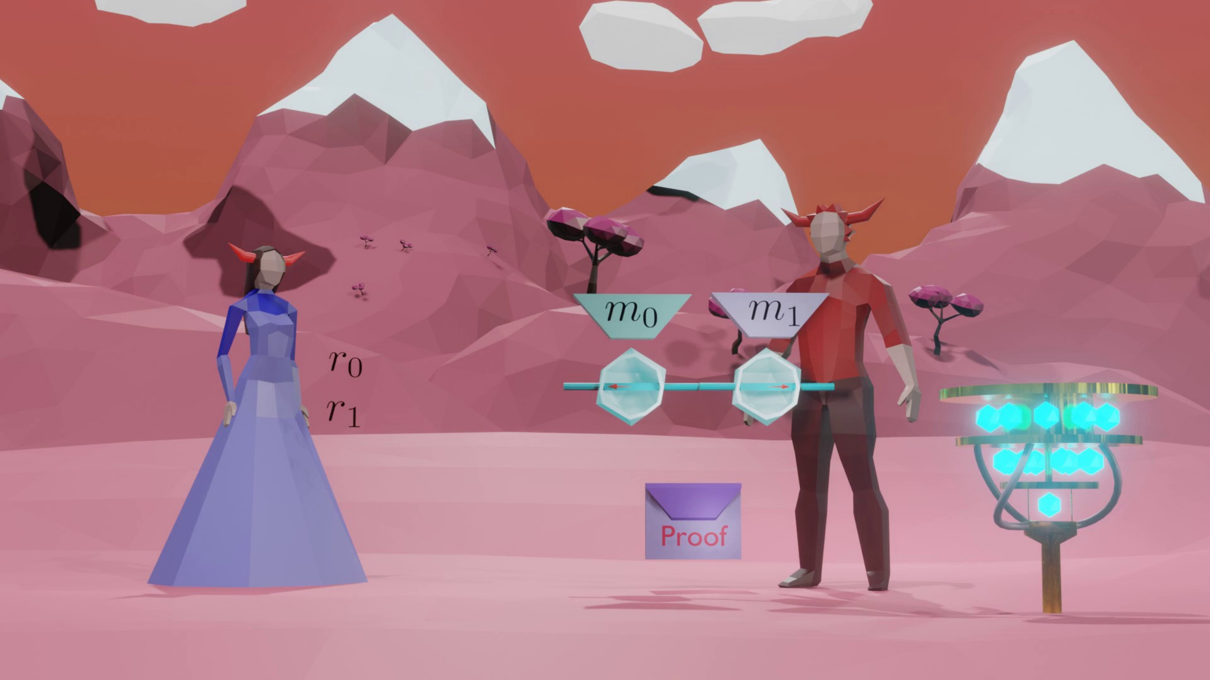
This is not secure!

Problem of naive construction

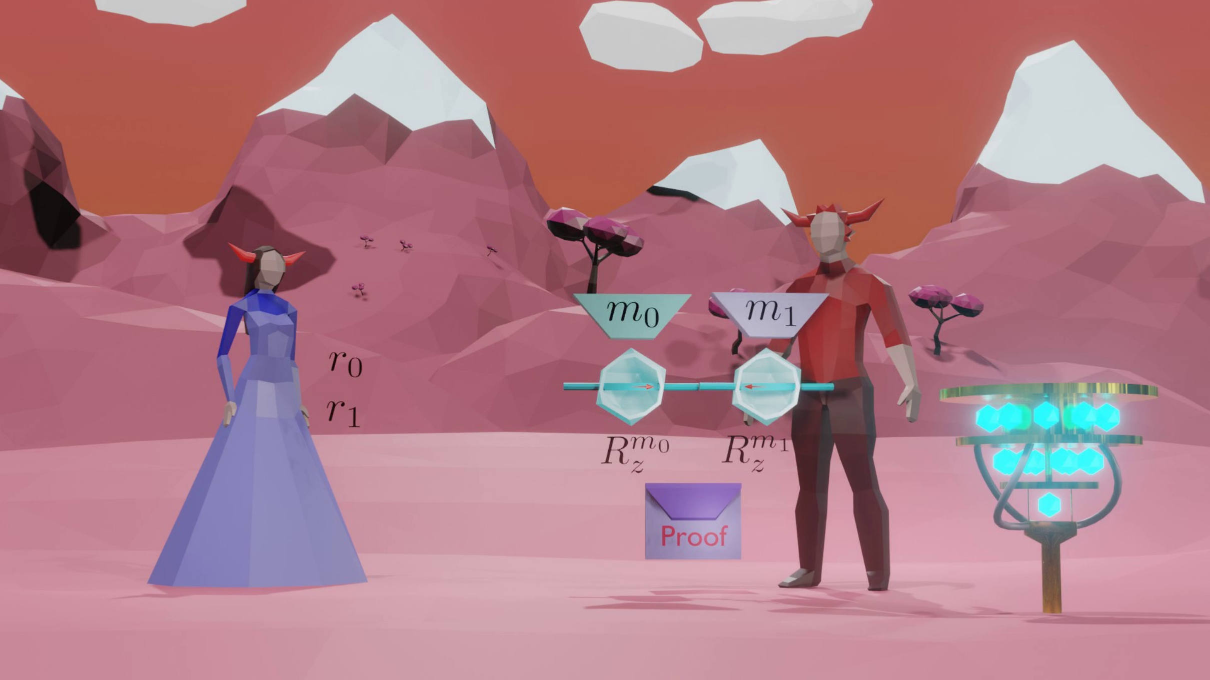
Problem: Alice can cheat by sending two $|+\rangle$ states instead of one $|0/1\rangle$ and one $|\pm\rangle$.

If $b = 1$
m_0
m_1
r_1
Proof
One qubit comp. basis

m_0
m_1
r_0
r_1
Proof
One qubit comp. basis


m_0
m_1
r_0
r_1
Proof


m_0
m_1
r_0
r_1
$R_z^{m_0}$
$R_z^{m_1}$
Proof

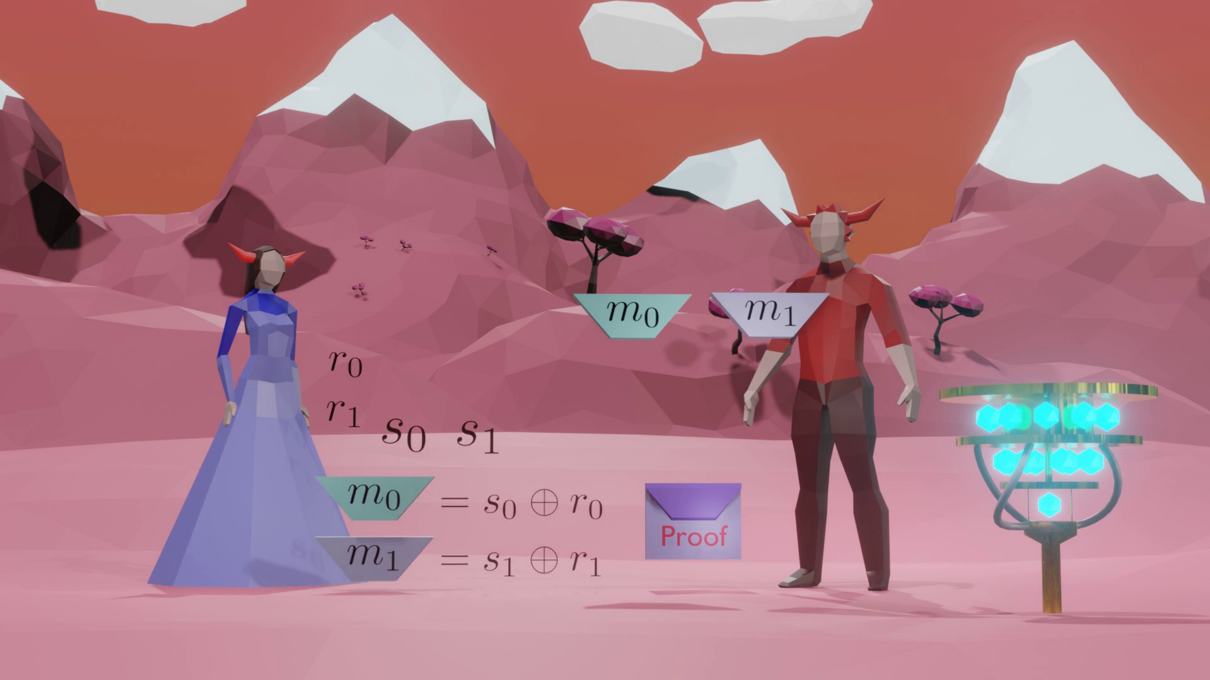


m_0
m_1
r_0
r_1
$R_z^{m_0}$
$R_z^{m_1}$
Proof


m_0
m_1
r_0
r_1
Proof


m_0
m_1
r_0
r_1
s_0
Proof


r_0
r_1
m_0
m_1
s_0
s_1
$= m_0 \oplus r'$
$= m_1 \oplus r$
Proof


m_0
m_1
r_0
r_1
s_0 s_1
$m_0 = s_0 \oplus r_0$
$m_1 = s_1 \oplus r_1$
Proof

Classical Zero-Knowledge

Classical Zero-Knowledge

Classical Zero-Knowledge

Classical Zero-Knowledge

Classical Zero-Knowledge

Classical Zero-Knowledge

Generalizable in a non-interactive way to NP problems.

?

How can Alice prove that one qubit is in the **computational** basis and the other is in the **Hadamard** basis?

?

How can Alice prove that one qubit is in the **computational** basis and the other is in the **Hadamard** basis?

$\Rightarrow$ Known to be possible using LWE (Colisson, Grosshans, Kashefi (2022))
Problem: need structure + not suitable for statistical security.
What about a weaker statement?

?

How can Alice prove that one qubit is in the **computational** basis ~~and the other is in the **Hadamard** basis~~?

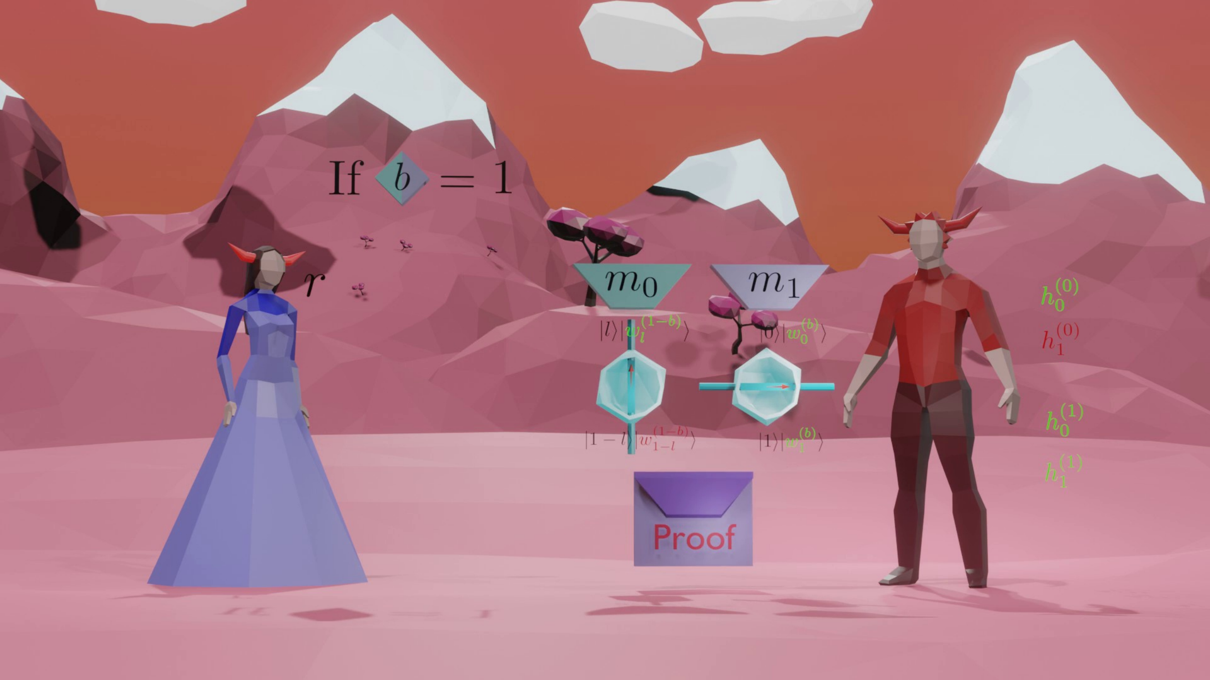
$\Rightarrow$ Known to be possible using LWE (Colisson, Grosshans, Kashefi (2022))
Problem: need structure + not suitable for statistical security.
What about a weaker statement?

If $b = 0$
r
$|0\rangle|w_0^{(b)}\rangle$
$|l\rangle|w_l^{(1-b)}\rangle$
$|1\rangle|w_1^{(b)}\rangle$
$|1-l\rangle|w_{1-l}^{(1-b)}\rangle$
m_0
m_1
Random string starting with 0
Random string starting with 1

If $b = 1$
r
$|l\rangle|w_l^{(1-b)}\rangle$
$|1-l\rangle|w_{1-l}^{(1-b)}\rangle$
$|0\rangle|w_0^{(b)}\rangle$
$|1\rangle|w_1^{(b)}\rangle$
m_0
m_1
Random string starting with 0
Random string starting with 1

If $b = 1$
r
$|l\rangle|w_l^{(1-b)}\rangle$
$|0\rangle|w_0^{(b)}\rangle$
$|1-l\rangle|w_{1-l}^{(1-b)}\rangle$
$|1\rangle|w_1^{(b)}\rangle$
m_0
m_1
h
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$


If $b = 1$
$|l\rangle|w_l^{(1-b)}\rangle$
$|0\rangle|w_0^{(b)}\rangle$
r
$|1-l\rangle|w_{1-l}^{(1-b)}\rangle$
$|1\rangle|w_1^{(b)}\rangle$
m_0
m_1
Proof
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Prove that $\exists (w_d^{(c)})_{c,d}$, s.t. $\forall c, d, h_d^{(c)} = h(d \| w_d^{(c)}))$
and $\exists c, d$ s.t. $w_d^{(c)}[1] = 1$



If $b = 1$
r
m_0
m_1
$|l\rangle|w_l^{(1-b)}\rangle$
$|0\rangle|w_0^{(b)}\rangle$
$|1-l\rangle|w_{1-l}^{(1-b)}\rangle$
$|1\rangle|w_1^{(b)}\rangle$
Proof
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$

If $b = 1$
r
m_0
m_1
$|l\rangle|w_l^{(1-b)}\rangle$
$|0\rangle|w_0^{(b)}\rangle$
$|1-l\rangle|w_{1-l}^{(1-b)}\rangle$
$|1\rangle|w_1^{(b)}\rangle$
Proof
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$


If $b = 1$
r
m_0
m_1
$|l\rangle|w_l^{(1-b)}\rangle|1\rangle$
$|0\rangle|w_0^{(b)}\rangle|1\rangle$
$|1-l\rangle|w_{1-l}^{(1-b)}\rangle|0\rangle$
$|1\rangle|w_1^{(b)}\rangle|1\rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
$\forall c$, run on state c the unitary $U_{f^{(c)}}$ with:
$f^{(c)}(x, w) = w[1] \neq 1 \wedge \exists d, h(x\|w) = h_d^{(c)}$
Proof

If $b = 1$
r
m_0
m_1
$|l\rangle|w_l^{(1-b)}\rangle|1\rangle$
$|0\rangle|w_0^{(b)}\rangle|1\rangle$
$|1-l\rangle|w_{1-l}^{(1-b)}\rangle|0\rangle$
$|1\rangle|w_1^{(b)}\rangle|1\rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
$\forall c$, run on state c the unitary $U_{f^{(c)}}$ with:
$f^{(c)}(x, w) = w[1] \neq 1 \wedge \exists d, h(x \| w) = h_d^{(c)}$
Measure output, check $= 1$
Proof

If $b = 1$
r
m_0
m_1
$|l\rangle|w_l^{(1-b)}\rangle|1\rangle$
$|0\rangle|w_0^{(b)}\rangle$
$|1-l\rangle|w_{1-l}^{(1-b)}\rangle|0\rangle$
$|1\rangle|w_1^{(b)}\rangle$
$|1\rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
$\forall c$, run on state c the unitary $U_{f^{(c)}}$ with:
$f^{(c)}(x, w) = w[1] \neq 1 \wedge \exists d, h(x\|w) = h_d^{(c)}$
Measure output, check $= 1$
Proof


If $b = 1$
r
m_0
m_1
$|l\rangle|w_l^{(1-b)}\rangle|1\rangle$
$|0\rangle|w_0^{(b)}\rangle$
$|1-l\rangle|w_{1-l}^{(1-b)}\rangle|0\rangle$
$|1\rangle|w_1^{(b)}\rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
$\forall c$, run on state c the unitary $U_{f^{(c)}}$ with:
$f^{(c)}(x, w) = w[1] \neq 1 \wedge \exists d, h(x \| w) = h_d^{(c)}$
Measure output, check $= 1$
Proof

If $b = 1$
r
m_0
m_1
$|l\rangle|w_l^{(1-b)}\rangle|1\rangle$
$|0\rangle|w_0^{(b)}\rangle$
$|1-l\rangle|w_{1-l}^{(1-b)}\rangle|0\rangle$
$|1\rangle|w_1^{(b)}\rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Proof
$\forall c$, run on state c the unitary $U_{f^{(c)}}$ with:
$f^{(c)}(x, w) = w[1] \neq 1 \land \exists d, h(x \| w) = h_d^{(c)}$
Measure output, check $= 1$


If $b = 1$
r
m_0
m_1
$|l\rangle|w_l^{(1-b)}\rangle$
$|1-l\rangle|w_{1-l}^{(1-b)}\rangle$
$|0\rangle|w_0^{(b)}\rangle$
$|1\rangle|w_1^{(b)}\rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
$\forall c$, run on state c the unitary $U_{f^{(c)}}$ with:
$f^{(c)}(x, w) = w[1] \neq 1 \land \exists d, h(x \| w) = h_d^{(c)}$
Measure output, check $= 1$
Proof


If $b = 1$
r
m_0
m_1
$|l\rangle|w_l^{(1-b)}\rangle$
$|0\rangle|w_0^{(b)}\rangle$
$|1-l\rangle|w_{1-l}^{(1-b)}\rangle$
$|1\rangle|w_1^{(b)}\rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Mesure the second register in H basis
Proof

If $b = 1$
r
m_0
m_1
$|l\rangle$
$s^{(0)}$
$|0\rangle$
$s^{(1)}$
$|1-l\rangle$
$|1\rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Proof
Mesure the second register in H basis


If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1
$|l\rangle$
$s^{(0)}$
$|0\rangle$ $s^{(1)}$
$|1-l\rangle$
$|1\rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Mesure the second register in H basis
Proof

If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1
$|l\rangle$
$|1-l\rangle$
$|0\rangle$
$|1\rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Mesure the second register in H basis
Proof

If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1
$|l\rangle$
$|1-l\rangle$
$|0\rangle$
$|1\rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
We got (NI)ZKoQS !
(one state is collapsed, Bob does not know which one)
(NI)ZKoQS = Non-Interactive Zero-Knowledge Proof on Quantum State
Proof

If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1
$R_z^{m_0}$
$R_z^{m_1}$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Proof


If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1
$R_z^{m_0}$
$R_z^{m_1}$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Proof


If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1
$|l\rangle$
$|0\rangle$
$|1-l\rangle$
$|1\rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Proof


If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1
s_0 s_1
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Proof

If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1
$m_b = s_b \oplus$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Proof


If $b = 1$
m_0
m_1
$m_b = s_b \oplus r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Proof


If $b = 1$
m_0
m_1
$m_b = s_b \oplus r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Proof

If $b = 1$
m_0
m_1
$m_b = s_b \oplus r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Proof


If $b = 1$
m_0
m_1
$m_b = s_b \oplus r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Proof


If $b = 1$
m_0
m_1
$m_b = s_b \oplus r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
$h_0^{(0)}$
$h_1^{(0)}$
$h_0^{(1)}$
$h_1^{(1)}$
Proof

Alice($b \in \{0,1\}$) — **Bob**($(m_0, m_1) \in \{0,1\}^2$)

$\forall d \in \{0,1\}, w_d^{(b)} \xleftarrow{\$} \{0\} \times \{0,1\}^n$

$l \xleftarrow{\$} \{0,1\}$

$w_l^{(1-b)} \xleftarrow{\$} \{0\} \times \{0,1\}^n$

$w_{1-l}^{(1-b)} \xleftarrow{\$} \{1\} \times \{0,1\}^n$

$\forall (c,d) \in \{0,1\}^2, h_d^{(c)} := h(d \| w_d^{(c)})$

$\pi :=$ (NI)ZK proof that:

$\exists (w_d^{(c)})_{c,d}, \forall c,d, h_d^{(c)} = h(d \| w_d^{(c)}))$

and $\exists c, d$ s.t. $w_d^{(c)}[1] = 1$.

If the ZK proof is interactive, then we actually run the ZK protocol (before sending the quantum state) instead of sending the proof (of course this adds additional rounds of communication).

$r^{(b)} \xleftarrow{\$} \{0,1\}$

$|\psi^{(b)}\rangle := |0\rangle |w_0^{(b)}\rangle + (-1)^{r^{(b)}} |1\rangle |w_1^{(b)}\rangle$

$|\psi^{(1-b)}\rangle := |l\rangle |w_l^{(1-b)}\rangle$

Alice → Bob: $\forall (c,d) : h_d^{(c)}, \pi, |\psi^{(0)}\rangle, |\psi^{(1)}\rangle$

Check (or run if interactive proof) π.

$\forall c$, apply on $|\psi^{(c)}\rangle |0\rangle$ the unitary:

$x, w \mapsto w[1] \neq 1 \wedge \exists d, h(x \| w) = h_d^{(c)}$,

measure the last (output) register

and check that the outcome is 1.

$\forall c$, measure the second register of $|\psi^{(c)}\rangle$

in the Hadamard basis (with outcome $s^{(c)}$).

At that step, $|\psi^{(b)}\rangle = |0\rangle \pm |1\rangle$ and $|\psi^{(1-b)}\rangle = |l\rangle$, but Bob does not know b (NIZKoQS).

.... End of NIZKoQS ....

$\forall c$, apply Z^{m_c} on $|\psi^{(c)}\rangle$ and measure it

in the Hadamard basis (with outcome $z^{(c)}$).

Bob → Alice: $\forall c, s^{(c)}, z^{(c)}$

Compute $\alpha := r^{(b)} \oplus \bigoplus_i s^{(b)}[i](w_0^{(b)} \oplus w_1^{(b)})[i]$

return $\alpha \oplus z^{(b)}$ / Should be m_b

Security Proof

Composable security (informal)

The protocol quantum-standalone realizes the OT functionality, assuming that:

- h is **collision resistant** (security against malicious Alice),
- h is **hiding**[1] (i.e. no information leaks on x given $h(x\|r)$, security against malicious Bob).
- There exists a ZK **proof of knowledge**

Moreover, it is secure against **statistically unbounded parties** if the ZK protocol is secure in that setting and if the corresponding assumptions statistically hold (e.g. injective h for unbounded Alice, lossy h for unbounded Bob).

[1] Note that we can get an even weaker assumption (h is one-way) by using hardcore bits and the Goldreich-Levin construction, but we leave the formalization of this proof for future work.

If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1
$h_0^{(0)}$
$h_1^{(0)}$
$h_1^{(1)}$
Proof


If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1
$h_0^{(0)}$
$h_1^{(0)}$
$h_1^{(1)}$
Proof


If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1
$h_0^{(0)}$
$h_1^{(0)}$
$h_1^{(1)}$


If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1


If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1


If $= 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1


If = 1
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1

If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1
Proof

If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1
Proof

If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1
At most 4 elements in the superpositon
(or collision with the extracted values)
Proof


If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_0
m_1
No element map to the dummy hash
(or collision with the extracted values)
Proof


If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_1
No element map to the dummy hash
(or collision with the extracted values)
Proof


If $b = 1$
$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$
m_1
No element map to the dummy hash
(or collision with the extracted values)
Proof

Quantum language and ZK on quantum state

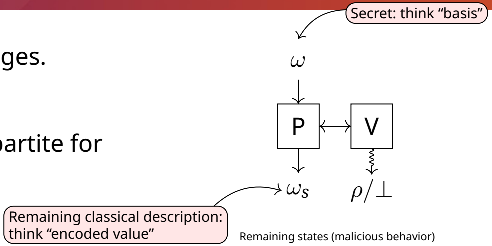
Quantum language and ZKoQS

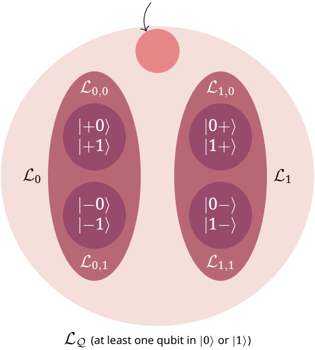
Quantum language = generalization of classical languages.

Properties of ZK on Quantum States (informal):

- **Soundness**: $\mathcal{L}_Q =$ **subset of quantum states** (bipartite for the adversary).
  - Classically $x \in \mathcal{L}$ if V accepts
  - Quantumly $\rho \in \mathcal{L}_Q$ if V accepts
- **Correctness**:
  - Classically: $x \in \mathcal{L}_w \subset \mathcal{L}$, $w \in \{0,1\}^*$ is the witness
  - Quantumly: $\rho \in \mathcal{L}_{\omega,\omega_s} \subseteq \mathcal{L}_\omega \subseteq \mathcal{L}_Q$, $\omega \in \{0,1\}^*$ is the witness or *class*, and $\omega_s \in \{0,1\}^*$ is the *subclass*
- **Zero-Knowledge**:
  - Classically: Bob can't learn info on w
  - Quantumly: Bob can't learn info on ω

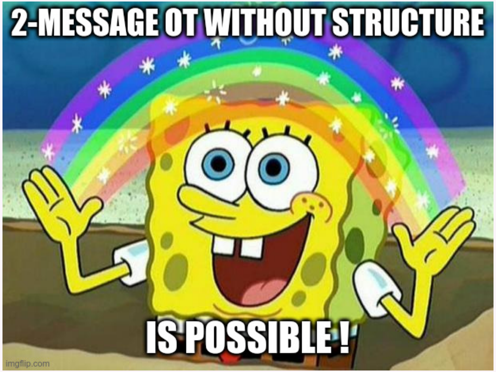
$\Rightarrow$ We introduce complexity classes ZKstatesQMA/ZKstatesQIP





Conclusion

Take-home message



(and Zero-Knowledge proofs on quantum states)

Open questions and ongoing works

- **Characterize ZKstatesQMA**
  What are the other ZKoQS properties that can(not) be verified? Under which assumption?
- **Role of entanglement**
  Prove (im)possibility of similar ZKoQS with only **single-qubit** operations? (entanglement seems important)
- Other **applications**?
  Quantum money, reducing communication complexity in other protocol...
- ...


Thank you!


Thank you!

Supplementary materials

Comparison with existing works

Article	Classical	Setup	Messages	MiniQCrypt	Composable	Statistical
[PVW08]	Yes	CRS	2	No (LWE)	Yes	Either
[BD18]	Yes	Plain M.	2	No (LWE)	Sender	Receiver
[CK88] + later works	No	Depends	7	Yes	Yes [DFL+09],[Unr10]	Either
[GLSV21]	No	Plain M./ CRS	poly/ cte ≥ 7	Yes	Yes	No
[BCKM21]	No	Plain M./ CRS	poly/ cte ≥ 7	Yes	Yes	Sender
[ABKK23]	No	RO	3	Yes	Yes	No
This work + [Unr15]	No	RO	2	Yes	Yes	No
This work + [HSS11]	No	Plain M.	> 2	No (LWE)	Yes	No
This work + S-NIZK	No	Like ZK	2	Like ZK	Yes	Sender
This work + NIZK proof	No	Like ZK	2	Like ZK	Yes	Receiver
This work + ZK	No	Like ZK	ZK $+1$ or 2[1]	Like ZK	Yes	Like ZK

Classical Zero-Knowledge

Classical Zero-Knowledge

Classical Zero-Knowledge

Classical Zero-Knowledge

Classical Zero-Knowledge

Classical Zero-Knowledge

Classical Zero-Knowledge

Classical Zero-Knowledge

Classical Zero-Knowledge

Classical Zero-Knowledge

Classical Zero-Knowledge

Classical Zero-Knowledge

Classical Zero-Knowledge

Generalizable in a non-interactive way to NP problems.