

# 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

QCRYPT 2023













# Multi-Party Computing (MPC)



Oblivious  
Transfer



# Oblivious Transfer

$m_0$

$m_1$





# Oblivious Transfer

$b$

$m_0$

$m_1$



# Oblivious Transfer

$b$

$m_0$

$m_1$

$m_b$

# OT: state of the art

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

## State of the art

### Classical



Requires trapdoors

(= CryptoMania, asymmetric crypto)



2 messages

### Quantum



No structure is necessary

(= hash function)



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:

⇒ **generalize ZK proofs to quantum languages (ZKstatesQMA)**

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

The background features a stylized, low-poly landscape in shades of red, orange, and white, resembling a desert or volcanic terrain. Several small, purple, tree-like plants are scattered across the ground. In the foreground, there are two large, rectangular blocks. The block on the left is purple and contains the text "Zero Knowledge". The block on the right is blue and contains the text "Our Work".

Zero  
Knowledge

Our  
Work

The background features a stylized, low-poly landscape in shades of red and orange. It includes several large, jagged mountain peaks with white caps and smaller, rounded hills. Sparse vegetation consists of small, purple, bushy trees scattered across the terrain.

Our  
Work

Oblivious  
Transfer



NIZK  
[Unr15]

Our  
Work



# Our Work

Oblivious  
Transfer  
(2-messages)

The background features a stylized, low-poly landscape in shades of red, orange, and white. It includes several mountain peaks with white caps and small purple trees scattered across the terrain. In the foreground, there are two large, semi-transparent cubes. The cube on the left is purple and contains the text "ZK plain-model [HSS11]". The cube on the right is blue and contains the text "Our Work".

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 hiding 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

$|0\rangle$



$|1\rangle$

# Qubits

$|0\rangle$



$|1\rangle$

# Qubits

$|0\rangle$



$|1\rangle$

# Qubits

$|0\rangle$



$|1\rangle$

# Qubits

$|x\rangle$



$|x'\rangle$

Superposition

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

# Qubits

$|x\rangle$



$|x'\rangle$

Superposition

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

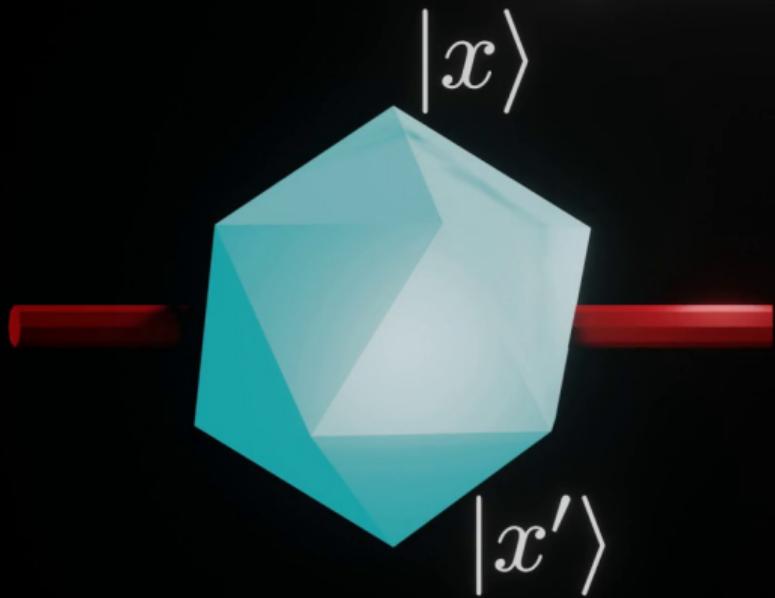
# Qubits



Superposition

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

# Qubits



Superposition

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

# Qubits

$|x\rangle$

Superposition

$d$

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

$|x'\rangle$



# Oblivious Transfer

$b$

$m_0$

$m_1$

$m_b$



*b*

*m*<sub>0</sub>

*m*<sub>1</sub>



If  $b = 0$



$m_0$

$m_1$



If  $b = 0$



$m_0$

$m_1$



If  $b = 1$



$m_0$

$m_1$



$r$



If  $b = 1$



$m_0$

$m_1$

$r$

Proof

One qubit comp. basis



If  $b = 1$



$r$



If  $b = 1$



$m_0$

$R_z^{m_0}$

$m_1$

$R_z^{m_1}$

Proof



If  $b = 1$



$r$

$m_0$

$R_z^{m_0}$

$m_1$

$R_z^{m_1}$

Proof



If  $b = 1$



$r$



If  $b = 1$



$r$

$m_0$

$m_1$

$s_0$

Proof



If  $b = 1$



$r$

$m_0$

$s_0$

$m_1$

$s_1$

Proof



If  $b = 1$



$r$



$m_0$

$s_0$

$$= m_1 \oplus r$$



$m_1$

$s_1$



If  $b = 1$



$r$

$m_0$

$s_0$

$m_1$

$s_1$



If  $b = 1$



$r \ s_0 \ s_1$



$m_0$

$m_1$



If  $b = 1$

$r \cdot s_0 \cdot s_1$

$$m_b = s_b \oplus r$$

Proof

$m_0$

$m_1$



# 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  $b = 1$



$m_0$

$m_1$

One qubit comp. basis

Proof







$r_0$   
 $r_1$





$r_0$   
 $r_1$

$m_0$

$m_1$

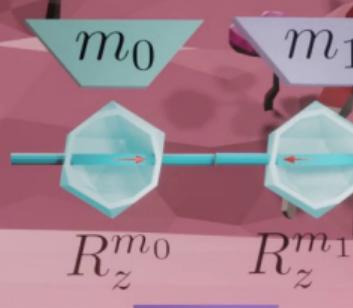
$R_z^{m_0}$

$R_z^{m_1}$





$r_0$   
 $r_1$



 $r_0$   
 $r_1$ 

 $r_0$   
 $r_1$  $m_0$   
 $s_0$  $m_1$ 



$r_0$   
 $r_1$

$$\begin{array}{c} m_0 \quad m_1 \\ s_0 \quad s_1 \\ = m_0 \oplus r' = m_1 \oplus r \end{array}$$



 $r_0$  $r_1$  $s_0 \ s_1$  $m_0$  $m_1$ 

$$m_0 = s_0 \oplus r_0$$

$$m_1 = s_1 \oplus r_1$$

 $m_0$  $m_1$ 



# Classical Zero-Knowledge



# Classical Zero-Knowledge

Solution exists?

1			
			4
		3	
	2		



# Classical Zero-Knowledge



Yes!  
I won't reveal it.

Solution exists?

1			
			4
		3	
	2		



# Classical Zero-Knowledge



A low-poly 3D scene set in a red-toned landscape with jagged mountains. In the foreground, a female character with long dark hair and a blue dress stands on the left, facing right. A male character with red skin and horns stands on the right, facing left. Between them is a 4x4 grid of cards. The top-left card has '1' on it. The top-right card has '4' on it. The bottom-left card has '3' on it. The bottom-right card has '2' on it. Two speech bubbles are present: one from the female character saying 'Yes! I won't reveal it.' and one from the male character saying 'I don't trust you.'

Yes!  
I won't reveal it.

I don't trust you.

1			
			4
		3	
	2		



# Classical Zero-Knowledge

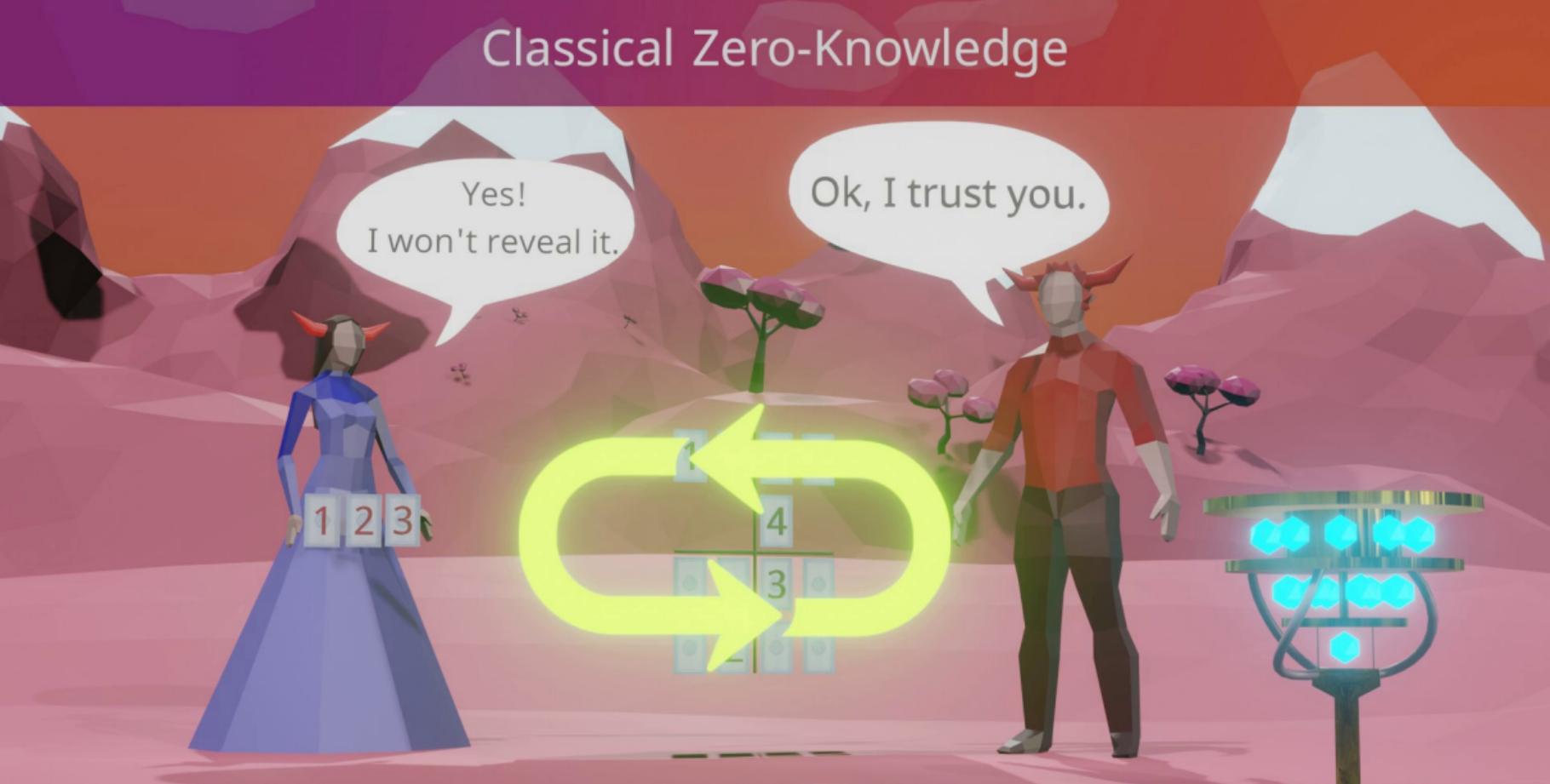
Yes!  
I won't reveal it.

I don't trust you.

1			
		4	
			3
	2		



# 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?

- ⇒ 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?

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

If  $b = 0$



Random string starting with 0

Random string starting with 1

If  $b = 1$

$$|l\rangle|w_l^{(1-b)}\rangle$$
  
  
 $|1-l\rangle|w_{1-l}^{(1-b)}\rangle$

$$|0\rangle|w_0^{(b)}\rangle$$
  
  
 $|1\rangle|w_1^{(b)}\rangle$

$m_0$

$m_1$

Random string starting with 0

Random string starting with 1



If  $b = 1$

$$\begin{array}{c} |l\rangle|w_l^{(1-b)}\rangle \\ \xrightarrow{r} \\ |1-l\rangle|w_{1-l}^{(1-b)}\rangle \end{array}$$

$$\begin{array}{c} |0\rangle|w_0^{(b)}\rangle \\ \xrightarrow{h} \\ |1\rangle|w_1^{(b)}\rangle \end{array}$$

$m_0$

$m_1$

$h_0^{(0)}$

$h_1^{(0)}$

$h_0^{(1)}$

$h_1^{(1)}$



If  $b = 1$

$$|l\rangle|w_l^{(1-b)}\rangle \xrightarrow{r} |1-l\rangle|w_{1-l}^{(1-b)}\rangle$$

$$|0\rangle|w_0^{(b)}\rangle \xrightarrow{r} |1\rangle|w_1^{(b)}\rangle$$

$m_0$

$m_1$



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.  $w_d^{(c)}[1] = 1$

$h_0^{(0)}$

$h_1^{(0)}$

$h_0^{(1)}$

$h_1^{(1)}$

If  $b = 1$



$r$

$m_0$

$m_1$

$|l\rangle|w_l^{(1-\delta)}\rangle$

$|0\rangle|w_0^{(\delta)}\rangle$

$|1-l\rangle|w_{1-l}^{(1-\delta)}\rangle$

$|1\rangle|w_1^{(\delta)}\rangle$

$h_0^{(0)}$

$h_1^{(0)}$

$h_0^{(1)}$

$h_1^{(1)}$

Proof

If  $b = 1$

$r$



Proof

$m_0$

$|l\rangle|w_l^{(1-\delta)}\rangle$

$|1-l\rangle|w_{1-l}^{(1-\delta)}\rangle$

$m_1$

$|0\rangle|w_0^{(\delta)}\rangle$

$|1\rangle|w_1^{(\delta)}\rangle$

$h_0^{(0)}$

$h_1^{(0)}$

$h_0^{(1)}$

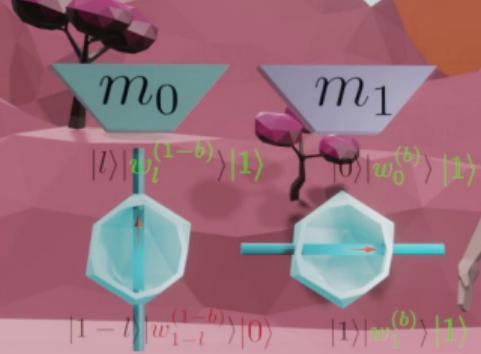
$h_1^{(1)}$



If  $b = 1$



$r$



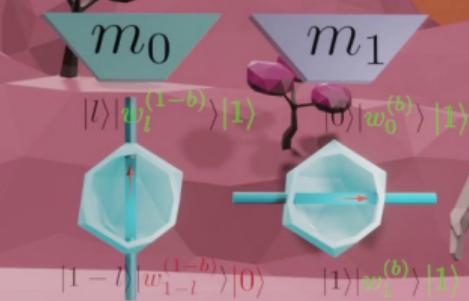
$\forall c$ , run on state  $c$  the unitary  $U_{f^{(c)}}$  with:

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

Proof

If  $b = 1$

$r$



$\forall c$ , 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



$h_0^{(0)}$

$h_1^{(0)}$

$h_0^{(1)}$

$h_1^{(1)}$

Proof

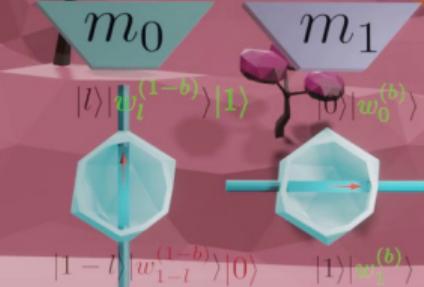
If  $b = 1$



$r$

$\forall c$ , 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



$h_0^{(0)}$

$h_1^{(0)}$

$h_0^{(1)}$

$h_1^{(1)}$

Proof

If  $b = 1$

$r$



$m_0$

$m_1$

$$|l\rangle |w_l^{(1-b)}\rangle |1\rangle \\ |1-l\rangle |w_{1-l}^{(1-b)}\rangle |0\rangle \quad |0\rangle |w_0^{(b)}\rangle \\ |1\rangle |w_1^{(b)}\rangle$$

$h_0^{(0)}$

$h_1^{(0)}$

$h_0^{(1)}$

$h_1^{(1)}$

$\forall c$ , run on state  $c$  the unitary  $U_{f^{(c)}}$  with:

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

Measure output, check = 1

Proof

If  $b = 1$

$r$



$$\begin{array}{c} m_0 \quad m_1 \\ |l\rangle|w_l^{(1-\delta)}\rangle|1\rangle \quad |0\rangle|w_0^{(\delta)}\rangle \\ |1-l\rangle|w_{1-l}^{(1-\delta)}\rangle|0\rangle \quad |1\rangle|w_1^{(\delta)}\rangle \end{array}$$

$\forall c$ , 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



$h_0^{(0)}$

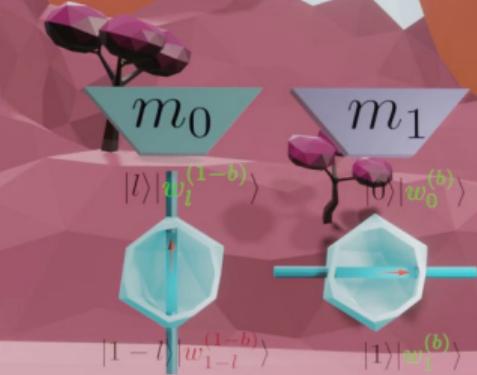
$h_1^{(0)}$

$h_0^{(1)}$

$h_1^{(1)}$

If  $b = 1$

$r$



$\forall c$ , 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



$h_0^{(0)}$

$h_1^{(0)}$

$h_0^{(1)}$

$h_1^{(1)}$

Proof

If  $b = 1$



$r$

$m_0$

$m_1$

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

$|0\rangle|w_0^{(b)}\rangle$

$|1-l\rangle|w_{1-l}^{(1-b)}\rangle$

$|1\rangle|w_1^{(b)}\rangle$

$h_0^{(0)}$

$h_1^{(0)}$

$h_0^{(1)}$

$h_1^{(1)}$

Measure the second register in  $H$  basis

Proof

If  $b = 1$

$r$



$m_0$

$|l\rangle$

$s^{(0)}$

$|1-l\rangle$

$m_1$

$|0\rangle$

$s^{(1)}$

$|1\rangle$



$h_0^{(0)}$

$h_1^{(0)}$

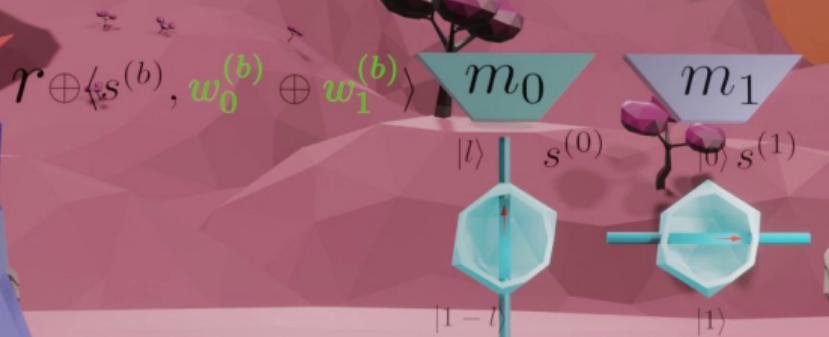
$h_0^{(1)}$

$h_1^{(1)}$

Measure the second register in  $H$  basis

If  $b = 1$

$$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$



Measure the second register in  $H$  basis

$$h_0^{(0)}$$

$$h_1^{(0)}$$

$$h_0^{(1)}$$

$$h_1^{(1)}$$

Proof

If  $b = 1$

$$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$m_0$

$m_1$

$|l\rangle$

$|1-l\rangle$

$|1\rangle$

$h_0^{(0)}$

$h_1^{(0)}$

$h_0^{(1)}$

$h_1^{(1)}$

Measure the second register in  $H$  basis

Proof

If  $b = 1$

$$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$m_0$

$m_1$

$|l\rangle$

$|1-l\rangle$

$|1\rangle$

$h_0^{(0)}$

$h_1^{(0)}$

$h_0^{(1)}$

$h_1^{(1)}$

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  $b = 1$

$$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$m_0$

$m_1$

$|l\rangle$

${}^1R_z^{m_0}$

$R_z^{m_1}$

$h_0^{(0)}$

$h_1^{(0)}$

$h_0^{(1)}$

$h_1^{(1)}$

Proof

If  $b = 1$

$$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$$m_0$$

$$m_1$$

$|l\rangle$

$$|^1R_z^{m_0}$$

$$R_z^{m_1}$$

$$h_0^{(0)}$$

$$h_1^{(0)}$$

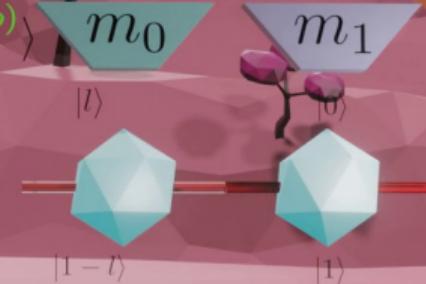
$$h_0^{(1)}$$

$$h_1^{(1)}$$



If  $b = 1$

$$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$



$$h_0^{(0)}$$

$$h_1^{(0)}$$

$$h_0^{(1)}$$

$$h_1^{(1)}$$

Proof



If  $b = 1$

$$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$m_0$

$m_1$



$s_0 - s_1$



$h_0^{(0)}$

$h_1^{(0)}$

$h_0^{(1)}$

$h_1^{(1)}$

Proof

If  $b = 1$

$$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$$m_1$$

$$m_b = s_b \oplus$$



$$h_0^{(0)}$$

$$h_1^{(0)}$$

$$h_0^{(1)}$$

$$h_1^{(1)}$$

Proof

If  $b = 1$

$$m_b = s_b \oplus r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$m_0$

$m_1$

$h_0^{(0)}$

$h_1^{(0)}$

$h_0^{(1)}$

$h_1^{(1)}$

Proof



If  $b = 1$

$$m_b = s_b \oplus r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$$m_0$$

$$m_1$$

$$h_0^{(0)}$$

$$h_1^{(0)}$$

$$h_0^{(1)}$$

$$h_1^{(1)}$$

Proof

If  $b = 1$

$$m_b$$

$$= s_b \oplus r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$$m_0$$

$$m_1$$

$$h_0^{(0)}$$

$$h_1^{(0)}$$

$$h_0^{(1)}$$

$$h_1^{(1)}$$

Proof

If  $b = 1$

$$m_b$$

$$= s_b \oplus r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$$m_0$$

$$m_1$$

$$h_0^{(0)}$$

$$h_1^{(0)}$$

$$h_0^{(1)}$$

$$h_1^{(1)}$$

Proof

If  $b = 1$

$$m_b = s_b \oplus r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$$m_0$$

$$m_1$$

$$h_0^{(0)}$$

$$h_1^{(0)}$$

$$h_0^{(1)}$$

$$h_1^{(1)}$$

Proof

**Alice**( $b \in \{0, 1\}$ )

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

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

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

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

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

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

$\pi := (\text{NI})\text{ZK proof that: }$  ←

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

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

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

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

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

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).

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

Check (or run if interactive proof)  $\pi$ .

$\forall c$ , 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 .....

$\forall c, s^{(c)}, z^{(c)}$

←  
 $\forall c, s^{(c)}, z^{(c)}$

$\forall c, \text{apply } Z^{m_c} \text{ on } |\psi^{(c)}\rangle \text{ and measure it}$   
in the Hadamard basis (with outcome  $z^{(c)}$ ).

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

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

OT from ZK | 8

# 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**<sup>1</sup> (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).

<sup>1</sup> 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  $b = 1$

$$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$$m_0$$

$$m_1$$

$$h_0^{(0)}$$

$$h_1^{(0)}$$

$$h_0^{(1)}$$

$$h_1^{(1)}$$

Proof

If  $b = 1$

$$\mathcal{R} \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$$m_0$$

$$m_1$$

$$h_0^{(0)}$$

$$h_1^{(0)}$$

$$h_0^{(1)}$$

$$h_1^{(1)}$$

Proof



If  $b = 1$

$$\mathcal{R} \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$$m_0$$

$$m_1$$

$$h_0^{(0)}$$

$$h_1^{(0)}$$

$$h_0^{(1)})$$

$$h_1^{(1)}$$



If  $b = 1$

$$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$m_0$

$m_1$



If  $b = 1$

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



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  $b = 1$

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

$h_0^{(b)}$

$h_1^{(b)}$

$h_2^{(b)}$

$h_3^{(b)}$



If  $b = 1$

$$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$m_0$

$m_1$

$h_0$ )

$h_1$ )

$h_0$ )

$h_1$ )



If  $b = 1$

$$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$$m_0$$

$$m_1$$

$$h_0)$$

$$h_1)$$

$$h_2)$$

$$h_3)$$

At most 4 elements in the superpositon  
(or collision with the extracted values)



If  $b = 1$

$$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$$m_0$$

$$m_1$$

$$h_0)$$

$$h_1)$$

$$h_e)$$

$$h)$$



No element map to the dummy hash  
(or collision with the extracted values)



If  $b = 1$

$$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$



No element map to the dummy hash  
(or collision with the extracted values)



$h_0^{(b)}$

$h_1^{(b)}$

$h_0^{(c)}$

$h_1^{(c)}$

If  $b = 1$

$$r \oplus \langle s^{(b)}, w_0^{(b)} \oplus w_1^{(b)} \rangle$$

$m_1$

$h_0^{(1)}$

$h_1^{(1)}$

$h_0^{(2)}$

$h_1^{(2)}$



No element map to the dummy hash  
(or collision with the extracted values)



# Quantum language and ZK on quantum state

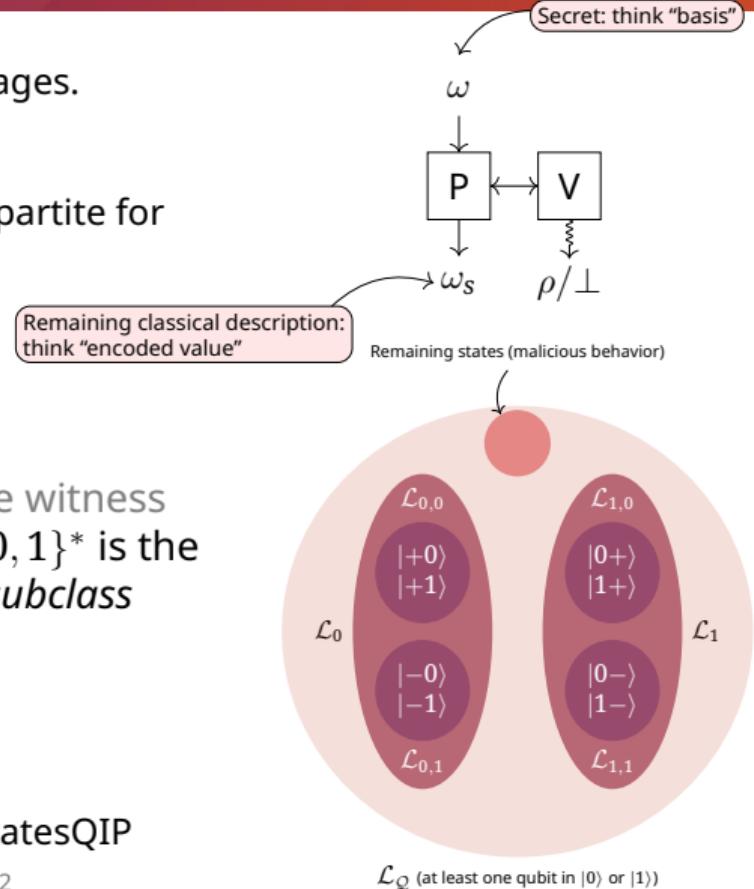
# Quantum language and ZKoQS

Quantum language = generalization of classical languages.

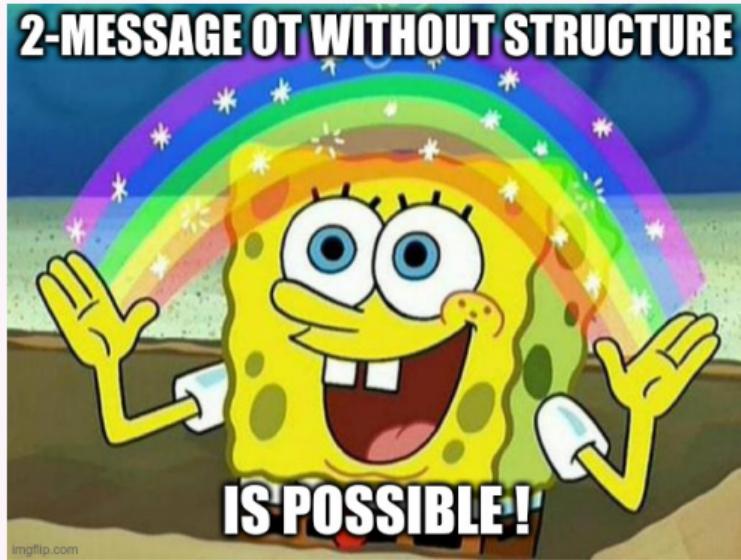
Properties of ZK on Quantum States (informal):

- **Soundness:**  $\mathcal{L}_Q = \text{subset of quantum states}$  (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:  $\rho \in \mathcal{L}_{\omega, \omega_s} \subseteq \mathcal{L}_\omega \subseteq \mathcal{L}_Q$ ,  $w \in \{0, 1\}^*$  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  $\omega$

⇒ We introduce complexity classes ZKstatesQMA/ZKstatesQIP



## 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...

- ...



Thankyou!



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 $\geq 7$	Yes	Yes	No
[BCKM21]	No	Plain M./ CRS	poly/ cte $\geq 7$	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 <sup>1</sup>	Like ZK	Yes	Like ZK

# Classical Zero-Knowledge



# Classical Zero-Knowledge

Solution exists?

1			
		4	
		3	
2			



# Classical Zero-Knowledge



Yes!  
I won't reveal it.

Solution exists?

1			
			4
		3	
	2		



# Classical Zero-Knowledge



A low-poly 3D scene set in a red-toned landscape with jagged mountains. In the foreground, a female character with long dark hair and a blue dress stands on the left, facing right. A male character with red skin and horns stands on the right, facing left. Between them is a 4x4 grid of 16 smaller squares. The squares are arranged in four rows and four columns. The numbers 1 through 4 are placed in specific squares: 1 is in the top-left, 4 is in the middle-right, 3 is in the bottom-middle, and 2 is in the bottom-left. The remaining squares are empty. Two speech bubbles are present: one from the female character saying "Yes! I won't reveal it." and one from the male character saying "I don't trust you." To the right of the male character is a glowing green circular device with a grid of glowing blue spheres.

Yes!  
I won't reveal it.

I don't trust you.

# Classical Zero-Knowledge

Yes!  
I won't reveal it.

I don't trust you.

1			
		4	
			3
	2		



# Classical Zero-Knowledge

Yes!  
I won't reveal it.

I don't trust you.

1	4	2	3
2	3	4	1
4	1	3	2
3	2	1	4



# Classical Zero-Knowledge



# Classical Zero-Knowledge



A low-poly 3D scene set in a red-hued landscape with jagged mountains. In the foreground, a character in a blue dress with red horns stands facing away from the camera. Another character in a red shirt and black pants with red horns stands facing the first character. Between them is a 4x4 grid of light blue rectangles. The top-left rectangle contains the number '1', the top-right '4', the middle-left '3', and the bottom-left '2'. The character in red is pointing towards the grid. Two speech bubbles are present: one from the character in blue saying 'Yes! I won't reveal it.' and one from the character in red saying 'I don't trust you.'

Yes!  
I won't reveal it.

I don't trust you.

# Classical Zero-Knowledge



A low-poly 3D scene set in a desert-like landscape with red mountains. In the center is a 4x4 grid of blue rectangular blocks. The blocks are labeled with numbers: 1 (top-left), 2 (bottom-left), 3 (bottom-middle), 4 (middle-right). A character in a blue dress and red horns stands on the left, holding a small device. Another character in a red shirt and red horns stands on the right. Two speech bubbles are present: one from the blue character saying "Yes! I won't reveal it." and one from the red character saying "I don't trust you." To the right is a glowing green circular structure.

Yes!  
I won't reveal it.

I don't trust you.

# Classical Zero-Knowledge



# Classical Zero-Knowledge



# Classical Zero-Knowledge



# Classical Zero-Knowledge



Generalizable in a non-interactive way to NP problems.