MITSUBISHI ELECTRIC
Changes for the Better

Computational self-testing for entangled magic states

Physical Review A **106**, L010601 (2022)

Akihiro Mizutani, Ryo Hiromasa, Yusuke Aikawa
(Mitsubishi Electric)
Yuki Takeuchi, Seiichiro Tani (NTT)

Beyondiid10 (2022)

Self-testing

Mayers, Yao, QIC (2004)
Review: Supic, Bowles, Quantum (2020)

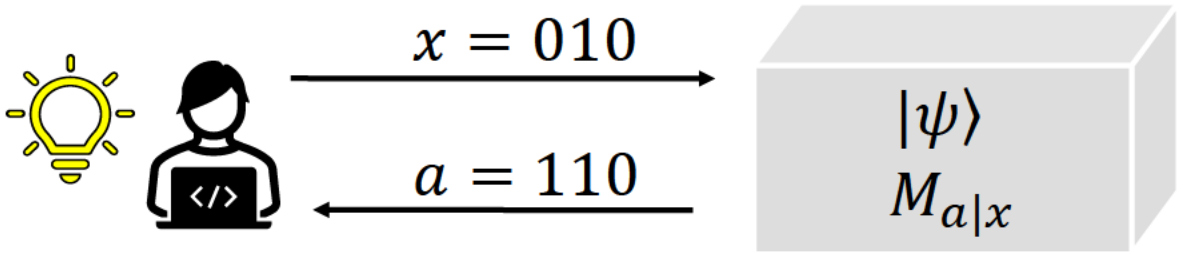
Classical verifier

Quantum device (prover)

Goal: To know inner workings of black-box by classical verifier

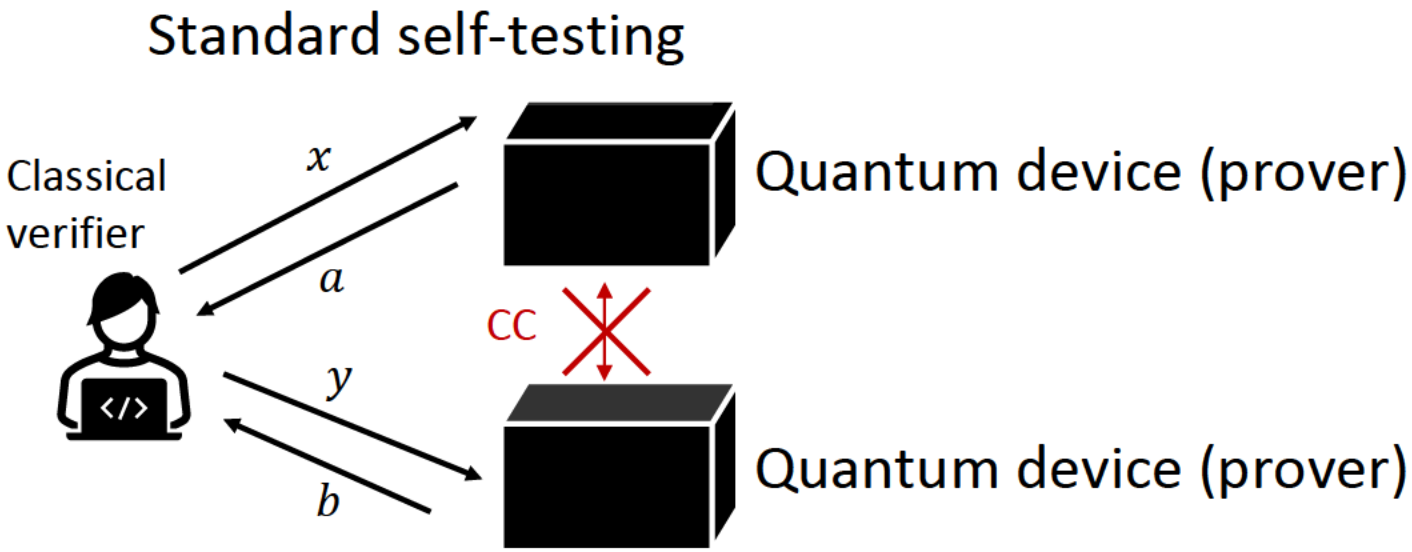
Classical verifier

Quantum device (prover)



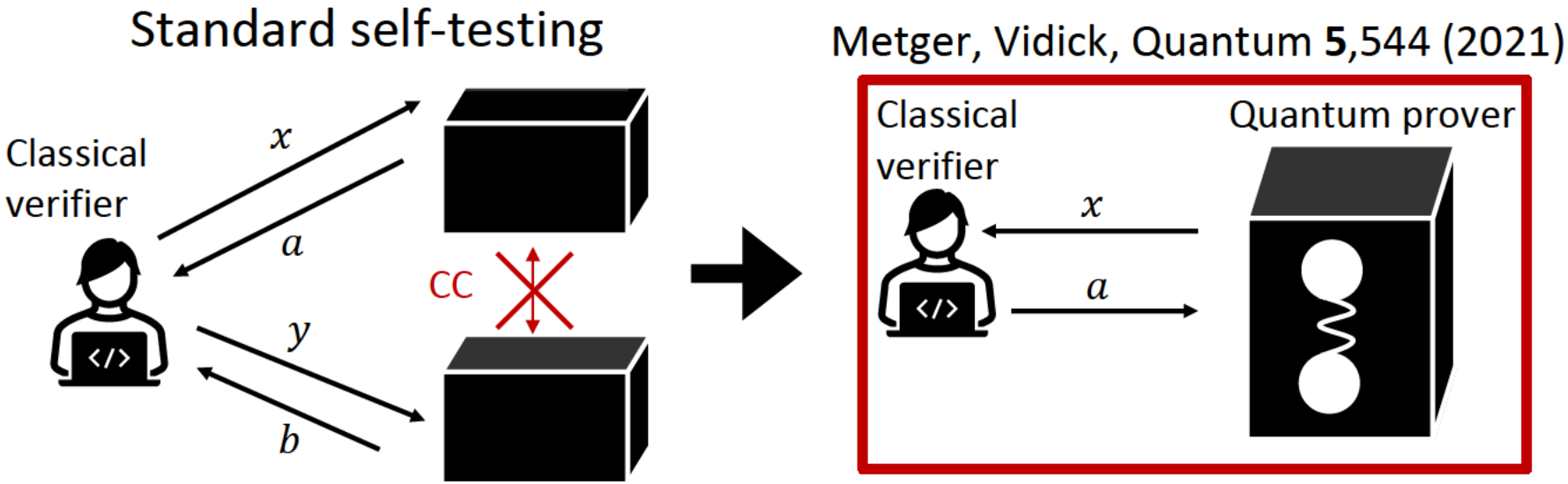
Standard self-testing

Mayers, Yao, QIC (2004)
Review: Supic, Bowles, Quantum (2020)



- Spatially-separated multiple-provers
- Assumption: Provers cannot communicate during the test
- ∵ To certify entanglement, execute test based on Bell inequality
- If devices **can** communicate, any classical devices can pass such self-testing protocol
- Multi-prover assumption is crucial

Self-testing with a single device

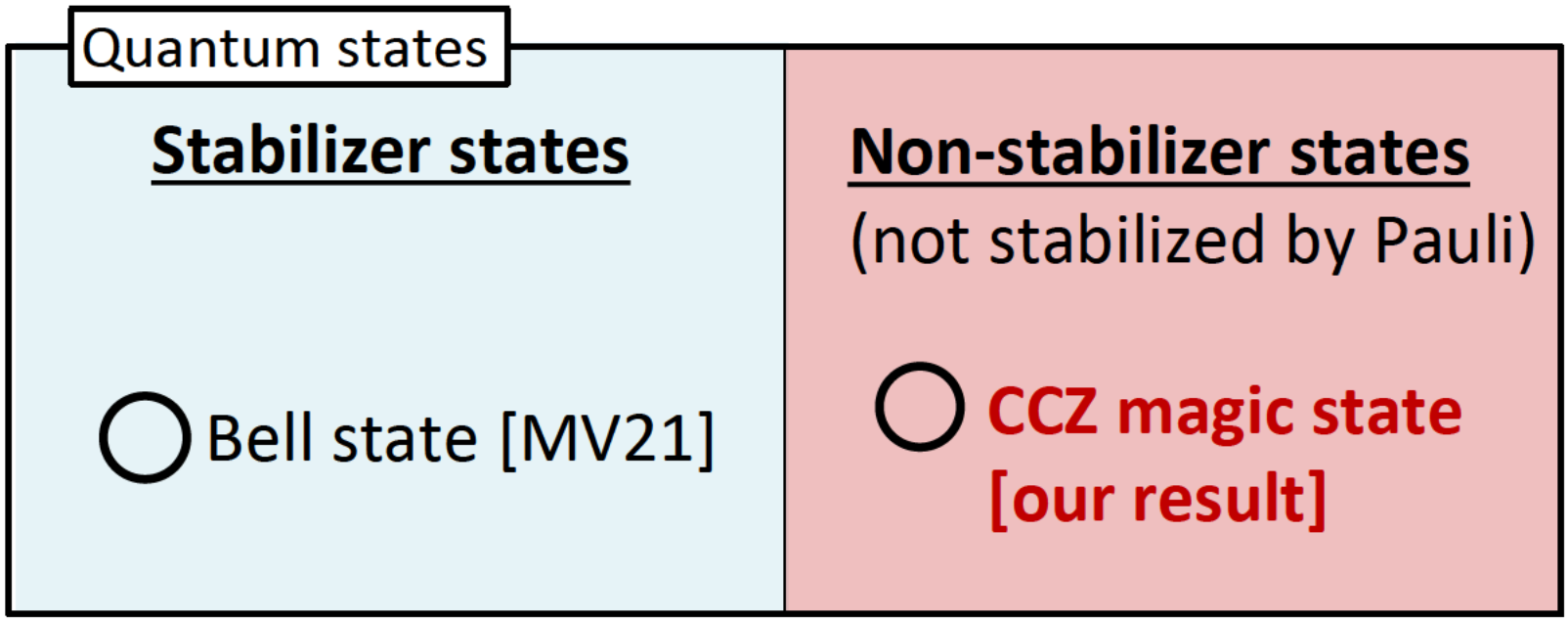


- We can no longer rely on Bell inequality because any classical prover achieves the maximum violation
- [MV21] assumes a quantum-poly-time prover and cannot solve the Learning with errors (LWE) used in Post-Quantum cryptography
- Self-test Bell state (stabilizer state) relying on stabilizer test

MITSUBISHI ELECTRIC
Changes for the Better

Self-testing with a single device

- It should be straightforward to extend [MV21] to other stabilizer states
- We show that we can self-test **CCZ magic state (non-stabilizer state)**



1. Cryptographic primitive underlying the protocol
2. Our self-testing protocol for CCZ magic state

Trapdoor claw-free function families

Brakerski, et al, FOCS (2018), Mahadev, FOCS (2018)

From LWE assumption, function families F and G can be constructed

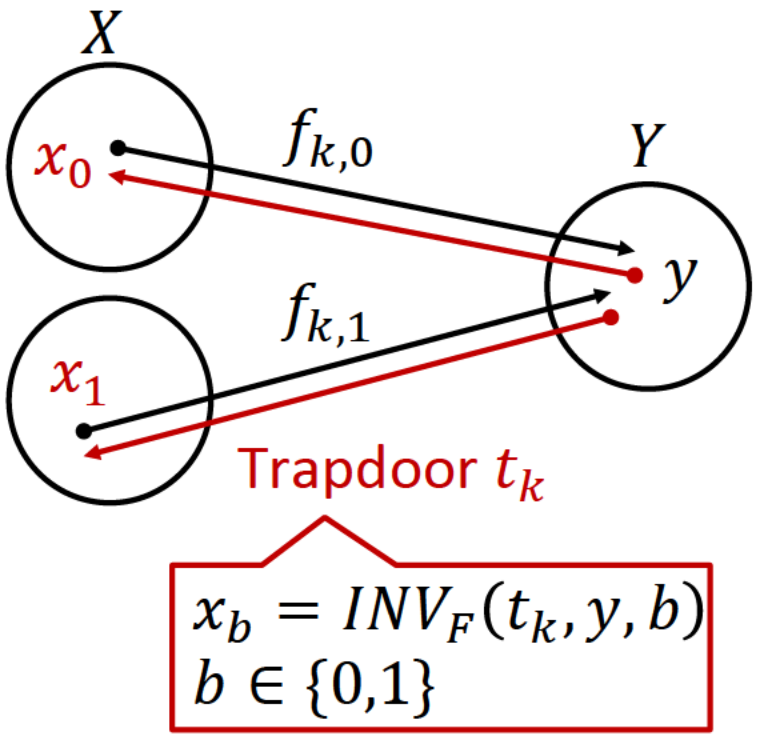
Function family $F = \{f_{k,0}, f_{k,1}\}_k$

1. **2 to 1**:
   $f: X \to Y$

   $\exists$ preimages (x_0, x_1) of y s.t.
   $y = f_{k,0}(x_0) = f_{k,1}(x_1)$

2. **Claw-free property:**

   Quantum poly-time prover cannot calculate preimages (x_0, x_1) from y



Trapdoor claw-free function families

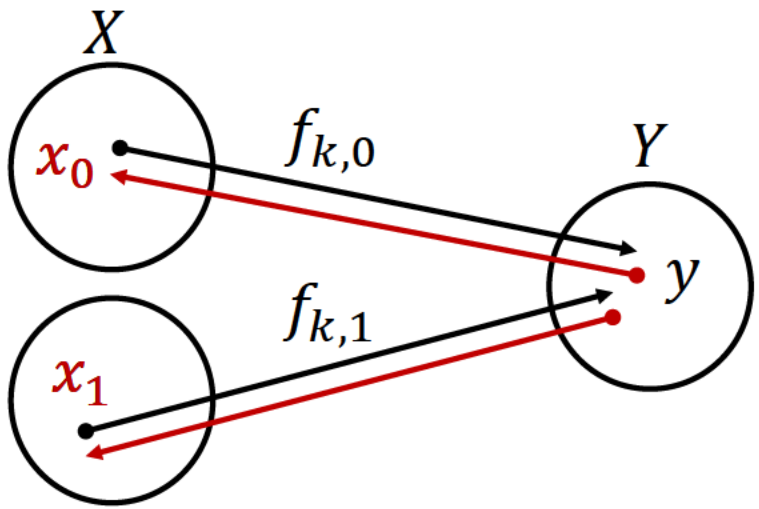
Brakerski, et al, FOCS (2018), Mahadev, FOCS (2018)

From LWE assumption, function families F and G can be constructed

Function family $F = \{f_{k,0}, f_{k,1}\}_k$

3. Adaptive hardcore bit property:

QPT prover is hard to output
$(y, b, x_b, r, d \neq 0)$
from k s.t.
$y = f_{k,b}(x_b)$, $r = d \cdot (x_0 \oplus x_1) \in \{0,1\}$



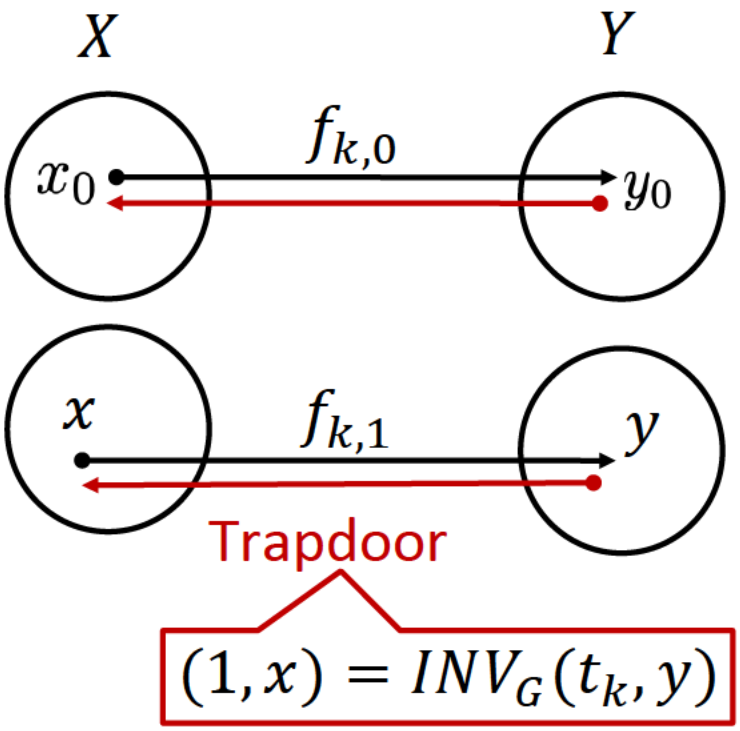
Hard to compute one preimage and any-one bit information about the other preimage

Trapdoor claw-free function families

Brakerski, et al, FOCS (2018), Mahadev, FOCS (2018)

From LWE assumption, function families F and G can be constructed

Function family $G = \{f_{k,0}, f_{k,1}\}_k$



1. 1 to 1:

$f: X \to Y$

∃ preimage x of y s.t.

$y = f_{k,b}(x)$

2. Injective invariance:

Quantum poly-time prover is hard to distinguish between F and G from public key k

Using F and G, we construct our self-testing protocol

Self-testing of CCZ magic state

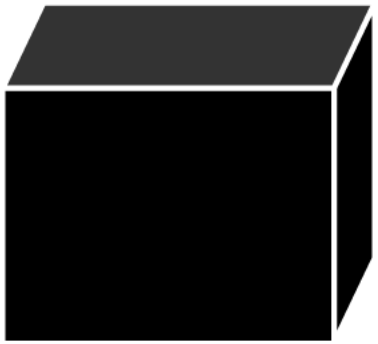
Mizutani et al PRA (2022)

Choose $\theta_1\theta_2\,\theta_3 \in \{000,001,010,100,111\}$
$\theta = 1 \rightarrow$generate (k, t_k) of F
$\theta = 0 \rightarrow$generate (k, t_k) of G

Public keys k_1, k_2, k_3

From k, I cannot find θ

Quantum prover



$$\sum_{b=0}^{1}\sum_{x\in X}|b\rangle|x\rangle|f_{k,b}(x)\rangle$$

Classical verifier

Self-testing of CCZ magic state

Mizutani et al PRA (2022)

Choose $\theta_1\theta_2\,\theta_3 \in \{000,001,010,100,111\}$
$\theta = 1$ →generate (k, t_k) of F
$\theta = 0$ →generate (k, t_k) of G

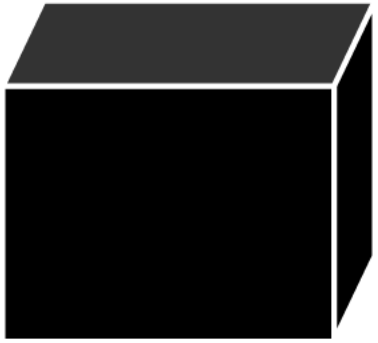
From k, I cannot find θ

Quantum prover

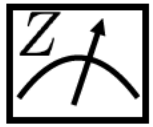
Public keys k_1, k_2, k_3

y_1, y_2, y_3

Classical verifier



$$\sum_{b=0}^{1}\sum_{x\in X}|b\rangle|x\rangle|f_{k,b}(x)\rangle$$



Self-testing of CCZ magic state

Mizutani et al PRA (2022)

Choose $\theta_1\theta_2\,\theta_3 \in \{000,001,010,100,111\}$
$\theta = 1$ →generate (k, t_k) of F
$\theta = 0$ →generate (k, t_k) of G

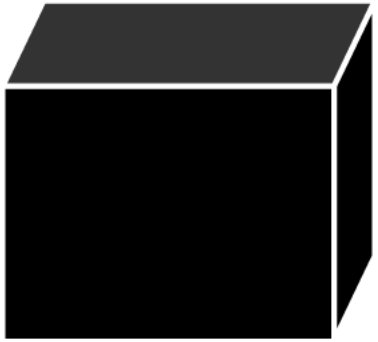
From k, I cannot find θ

Quantum prover

Public keys k_1, k_2, k_3

y_1, y_2, y_3

Classical verifier



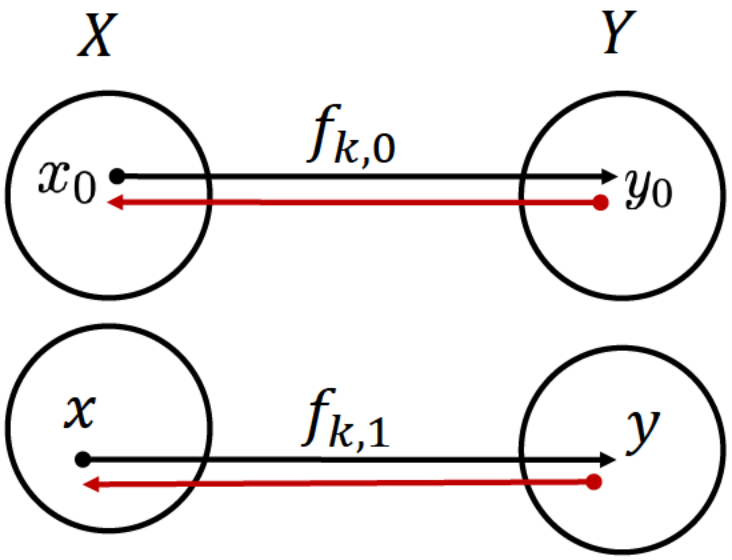
$\theta = 0 \rightarrow |b\rangle|x_b\rangle$
$\theta = 1 \rightarrow |0\rangle|x_0\rangle + |1\rangle|x_1\rangle$

Trapdoor claw-free function families

Brakerski, et al, FOCS (2018), Mahadev, FOCS (2018)

From LWE assumption, function families F and G can be constructed

Function family $G = \{f_{k,0}, f_{k,1}\}_k$



1. **1 to 1**:
   $f: X \to Y$

   ∃ preimage x of y s.t.
   $y = f_{k,b}(x)$

Self-testing of CCZ magic state

Mizutani et al PRA (2022)

Choose $\theta_1\theta_2\,\theta_3 \in \{000,001,010,100,111\}$
$\theta = 1$ →generate (k, t_k) of F
$\theta = 0$ →generate (k, t_k) of G

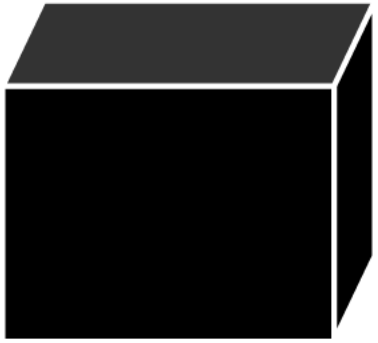
From k, I cannot find θ

Quantum prover

Public keys k_1, k_2, k_3

y_1, y_2, y_3

Classical verifier



$\theta = 0 \rightarrow |b\rangle|x_b\rangle$
$\theta = 1 \rightarrow |0\rangle|x_0\rangle + |1\rangle|x_1\rangle$

Trapdoor claw-free function families

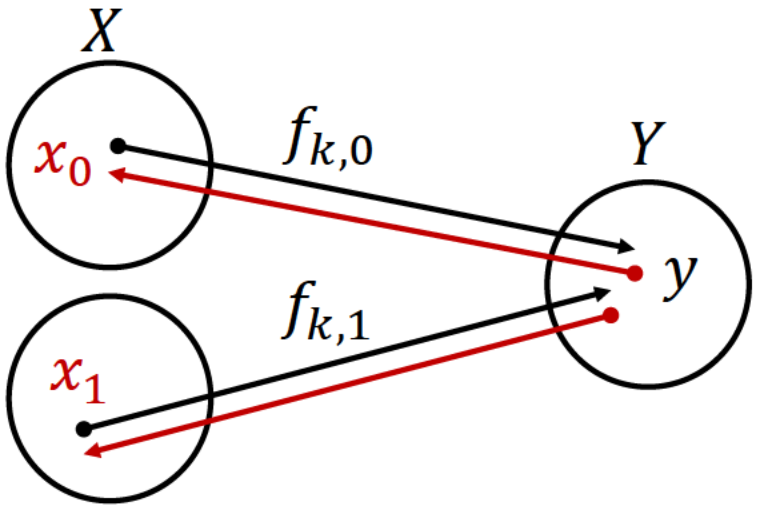
Brakerski, et al, FOCS (2018), Mahadev, FOCS (2018)

From LWE assumption, function families F and G can be constructed

Function family $F = \{f_{k,0}, f_{k,1}\}_k$

1. **2 to 1**:
   $f: X \to Y$

   $\exists$ preimages (x_0, x_1) of y s.t.
   $y = f_{k,0}(x_0) = f_{k,1}(x_1)$



Self-testing of CCZ magic state

Mizutani et al PRA (2022)

Choose $\theta_1\theta_2\,\theta_3 \in \{000,001,010,100,111\}$
$\theta = 1$ →generate (k, t_k) of F
$\theta = 0$ →generate (k, t_k) of G

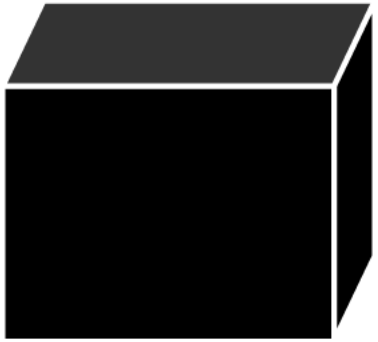
From k, I cannot find θ

Quantum prover

Public keys k_1, k_2, k_3

y_1, y_2, y_3

Classical verifier



$\theta = 0 \rightarrow |b\rangle|x_b\rangle$
$\theta = 1 \rightarrow |0\rangle|x_0\rangle + |1\rangle|x_1\rangle$

Self-testing of CCZ magic state

Mizutani et al PRA (2022)

Choose $\theta_1\theta_2\,\theta_3 \in \{000,001,010,100,111\}$
$\theta = 1$ →generate (k, t_k) of F
$\theta = 0$ →generate (k, t_k) of G

From k, I cannot find θ

Quantum prover

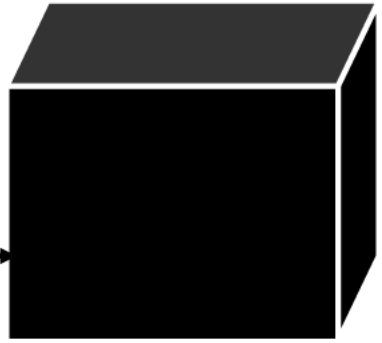
Public keys k_1, k_2, k_3

y_1, y_2, y_3

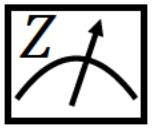
Z measurement

(b, x_b)

Classical verifier



$\theta = 0 \rightarrow |b\rangle|x_b\rangle$
$\theta = 1 \rightarrow |0\rangle|x_0\rangle + |1\rangle|x_1\rangle$



Check of Z-measurement:
Check if (b, x_b) is correct
($y = f_{k,b}(x_b)$ holds or not)
Failure prob. P_Z

Self-testing of CCZ magic state

Mizutani et al PRA (2022)

Choose $\theta_1\theta_2\,\theta_3 \in \{000,001,010,100,111\}$
$\theta = 1$ →generate (k, t_k) of F
$\theta = 0$ →generate (k, t_k) of G

From k, I cannot find θ

Quantum prover

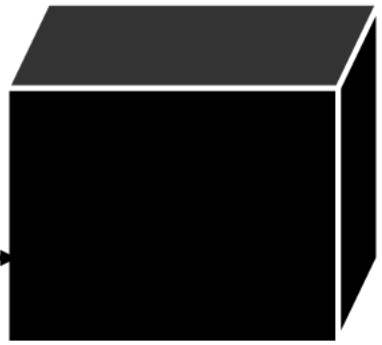
Public keys k_1, k_2, k_3

y_1, y_2, y_3

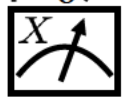
Classical verifier

X measurement

$(d, d \cdot (x_0 \oplus x_1))$



$\theta = 1 \rightarrow |0\rangle|x_0\rangle + |1\rangle|x_1\rangle$



d

$|0\rangle + (-1)^{d\cdot(x_0\oplus x_1)}|1\rangle$

$m = d \cdot (x_0 \oplus x_1)$

Check of X-measurement :
Using trapdoor, check if outcomes are equal to $(d, d \cdot (x_0 \oplus x_1))$
Failure prob. P_X

Trapdoor claw-free function families

Brakerski, et al, FOCS (2018), Mahadev, FOCS (2018)

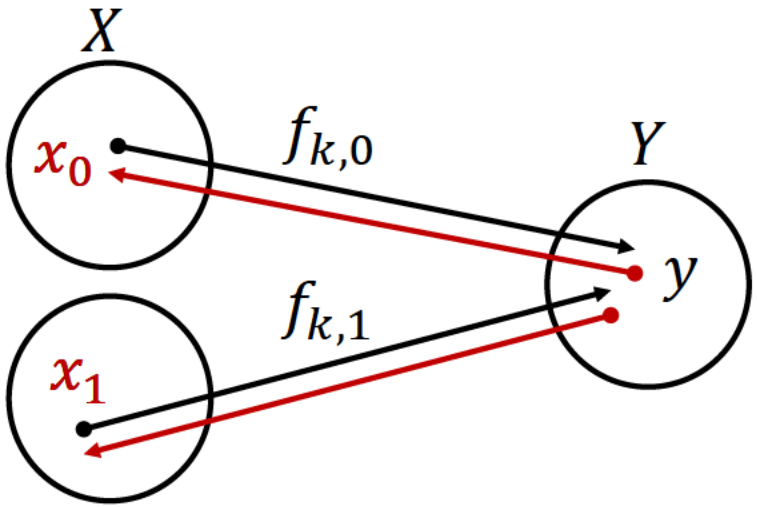
From LWE assumption, function families F and G can be constructed

Function family $F = \{f_{k,0}, f_{k,1}\}_k$

3. Adaptive hardcore bit property:

QPT prover is hard to output $(y, b, x_b, r, d \neq 0)$ from k s.t.

$y = f_{k,b}(x_b)$, $r = d \cdot (x_0 \oplus x_1) \in \{0,1\}$



Honest quantum prover satisfies only one of the two relations, but cannot by **any** quantum prover due to the hardness of LWE

Self-testing of CCZ magic state

Mizutani et al PRA (2022)

Choose $\theta_1\theta_2\,\theta_3 = 111$

Quantum prover

Public keys k_1, k_2, k_3

$y_1, y_2, y_3, d_1, d_2, d_3$

Classical verifier

Generalized stabilizer test

(v_1, v_2, v_3)

$|CCZ\rangle$

Using trapdoor, check if (v_1, v_2, v_3) is correct

Failure prob. P_{STAB}

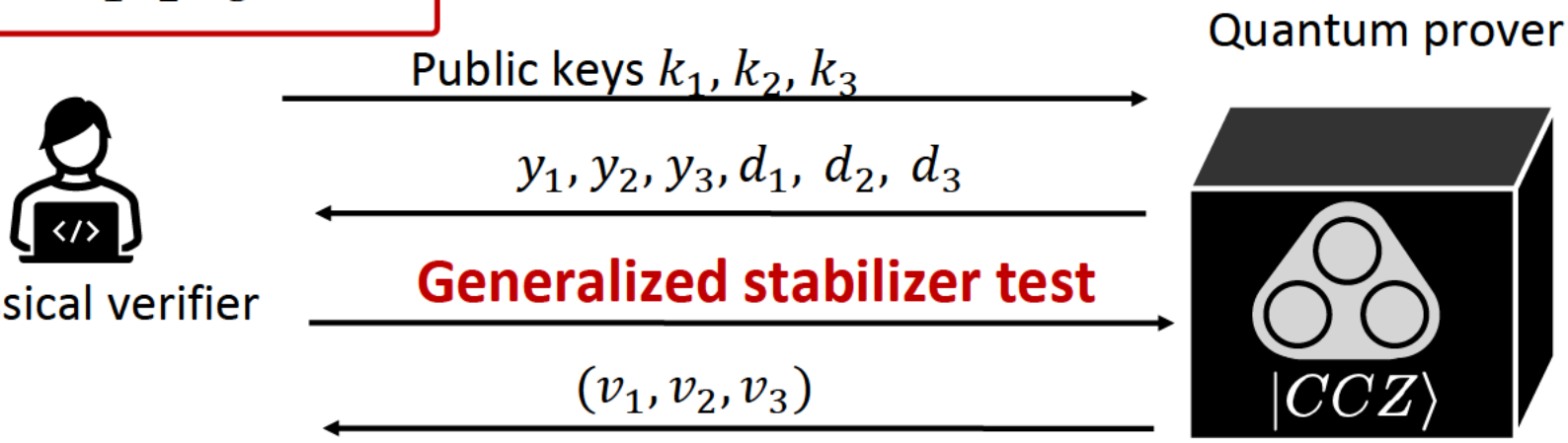
$$|\boldsymbol{CCZ}\rangle = CCZ\left[\bigotimes_{i=1}^{3}(|0\rangle + (-1)^{m_i}|1\rangle)\right]$$

$$m = d \cdot (x_0 \oplus x_1)$$

Self-testing of CCZ magic state

Mizutani et al PRA (2022)

Choose $\theta_1\theta_2\,\theta_3 = 111$



Any pure state $|\psi\rangle = U|0^n\rangle$ is stabilized by Hermitian operators:

Generalized stabilizers $\{g_i\}_{i=1}^n = \{UZ_iU^\dagger\}_{i=1}^n$

$$\boldsymbol{g_1|CCZ\rangle = (X \otimes CZ)|CCZ\rangle = |CCZ\rangle}$$

Generalized stabilizer test: Check measurement outcomes of $\{g_i\}_{i=1}^n$

Is a 2-qubit gate needed to measure the outcome of $\boldsymbol{X \otimes CZ}$?

Self-testing of CCZ magic state

Mizutani et al PRA (2022)

Choose $\theta_1\theta_2\,\theta_3 = 111$

Quantum prover

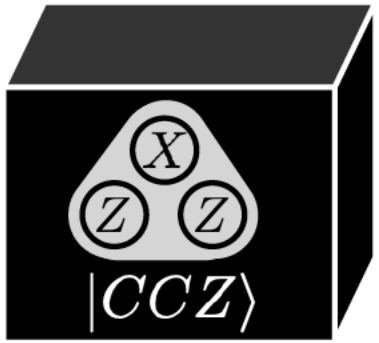
Public keys k_1, k_2, k_3

$y_1, y_2, y_3, d_1,\ d_2,\ d_3$

Classical verifier

Generalized stabilizer test

(v_1, v_2, v_3)



Takeuchi, Morimae, PRX (2018)

$$(\boldsymbol{X \otimes CZ})|\boldsymbol{CCZ}\rangle = \left(X \otimes \sum_i |i\rangle\langle i| \otimes Z^i\right)|CCZ\rangle = |\boldsymbol{CCZ}\rangle$$

v_1 v_2 v_3

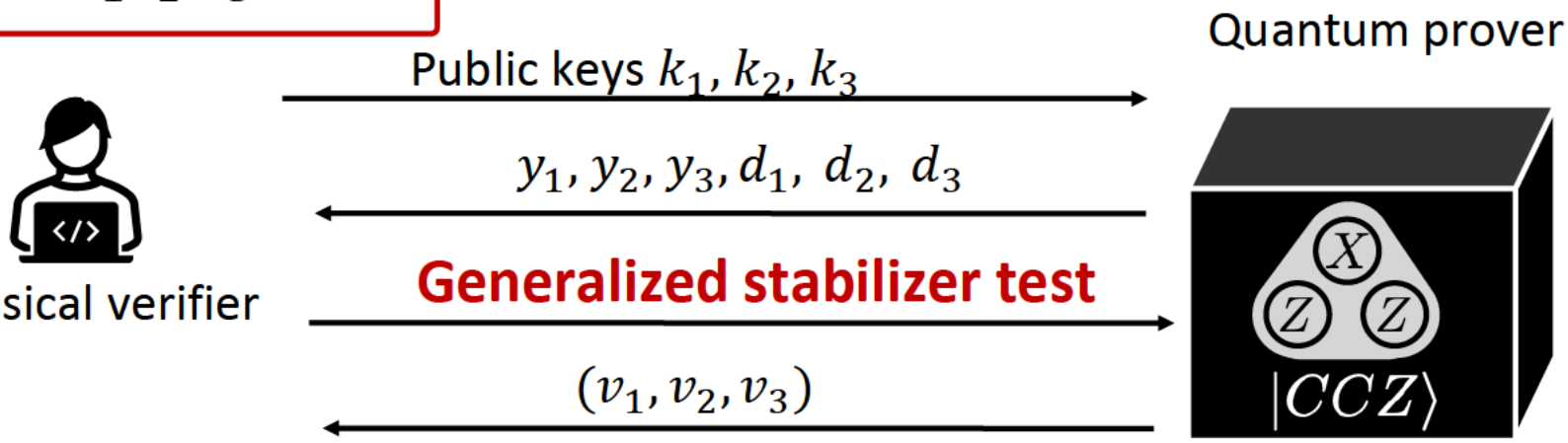
+1 eigenspace of $X \otimes CZ \Leftrightarrow v_1 \oplus v_2 v_3 = m$

Only the verifier knows

Self-testing of CCZ magic state

Mizutani et al PRA (2022)

Choose $\theta_1\theta_2\,\theta_3 = 111$



Takeuchi, Morimae, PRX (2018)

$$(\boldsymbol{X \otimes CZ})|\boldsymbol{CCZ}\rangle = \left(X \otimes \sum_i |i\rangle\langle i| \otimes Z^i\right)|CCZ\rangle = |\boldsymbol{CCZ}\rangle$$

v_1 v_2 v_3

- Using Z and X measurement checks, verifier knows how accurately prover performs generalized stabilizer measurements
- By checking $\{v_i\}_i$, verifier finds the distance of ρ and $|CCZ\rangle$

Main result

Mizutani et al PRA (2022)

Theorem

- Prover's failure probabilities of Z, X basis measurements and generalized stabilizer measurements: $(P_Z, P_X, P_{\mathrm{STAB}})$
- Prover's Hilbert space H

There exists an isometry $V: H \to C^8 \otimes H$, ζ_H and constant $r > 0$ such that for general prover's state ρ when $\theta = 111$, the following holds:

- Self-testing of state

$$||V\rho V^\dagger - |CCZ\rangle\langle CCZ| \otimes \zeta_H||^2 \leq O(P_Z^r + P_X^r + P_{\mathrm{STAB}}^r)$$

- Self-testing of state and measurement

$$|\mathrm{tr}[\rho P_{\vec{q}}^{(\vec{v})}] - |\langle \vec{v}_{\vec{q}}|CCZ\rangle|^2| \leq O(P_Z^r + P_X^r + P_{\mathrm{STAB}}^r)$$

Projector of outputting $\vec{v} = v_1 v_2 v_3$ given request $\vec{q} = q_1 q_2 q_3 \in \{Z, X\}^3$

$|000\rangle$ if $\vec{q} = ZZZ,\ \vec{v} = 000$
$|{+}{+}{+}\rangle$ if $\vec{q} = XXX, \vec{v} = 000$

Summary

Our contribution

Using Trapdoor claw-free function families, we reveal that the non-stabilizer state $|CCZ\rangle$ can also be self-tested with a single-quantum device

Future work

1. Self-test states where X, Y and Z appear in generalized stabilizers
   - If only X and Z appear, its single-device self-testing seems possible
   - It seems difficult as we have Trapdoor claw-free function families composed of only **2** function families F and G
2. Self-test in non-iid scenario
   - We assume prover's behavior is the same for each repetition
   - Is it possible by using de Finetti's theorem or by one-shot self-testing?