Constant-round Blind Classical Verification of Quantum Sampling

Kai-Min Chung[1] Yi Lee[2,4] Han-Hsuan Lin[3] Xiaodi Wu[2]

[1] Academia Sinica, Taiwan
[2] University of Maryland, USA
[3] National Tsing Hua University, Taiwan
[4] (Visiting) Max Planck Institute for Security and Privacy, Germany

Motivations

Motivations

$$(f, x)$$

Motivations

(f, x)

$y \leftarrow f(x)$

Motivations

(f, x)

$y \leftarrow f(x)$

y

Motivations

(f, x)

Private input?
(Blindness)

$y \leftarrow f(x)$

y

Motivations

(f, x)

Private input?
(Blindness)

y

$\boxed{y \leftarrow f(x)}$

Verifiability?

Motivations

(f, x)

Private input?
(Blindness)

$\boxed{y \leftarrow f(x)}$

Verifiability?

y

Can a classical computer verify the result of a quantum computation through interaction (Gottesman, 2004)?

Motivations

(f, x)

Private input?
(Blindness)

$\boxed{y \leftarrow f(x)}$

y

Verifiability?

Can a classical computer verify the result of a quantum computation through interaction (Gottesman, 2004)?

[Mah18]: Yes, for *decision* problems.

Motivations

(f, x)

Private input?
(Blindness)

$$\boxed{y \leftarrow f(x)}$$

y

Verifiability?

Can a classical computer verify the result of a quantum computation through interaction (Gottesman, 2004)?

[Mah18]: Yes, for *decision* problems.

$$L \in \mathsf{BQP}, x \overset{?}{\in} L$$

What about randomized outputs?

What about randomized outputs?

- Many natural applications

What about randomized outputs?

- Many natural applications
    - Quantum mechanical simulations

What about randomized outputs?

- Many natural applications
  - Quantum mechanical simulations
  - Quantum supremacy experiments

What about randomized outputs?

- Many natural applications
  - Quantum mechanical simulations
  - Quantum supremacy experiments
  - Quantum machine learning & optimization

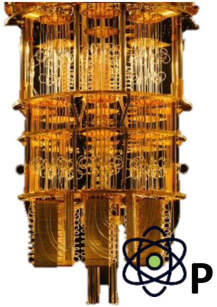
What about randomized outputs?

- Many natural applications
  - Quantum mechanical simulations
  - Quantum supremacy experiments
  - Quantum machine learning & optimization
- Decision problems $\Longrightarrow$ *sampling* problems

Model: Classical Verification of Quantum Sampling

Verifier

$$(C, x)$$



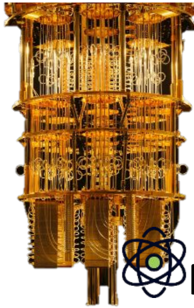
Prover

Model: Classical Verification of Quantum Sampling

Verifier

(C, x)

Randomized output!



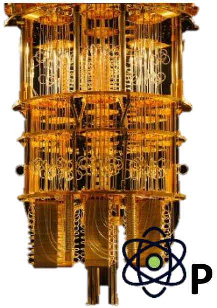
Prover

Model: Classical Verification of Quantum Sampling

Randomized output!

Verifier

(C, x)



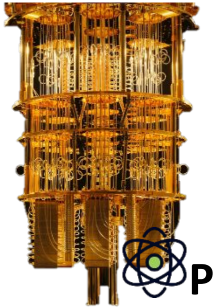
Prover

Model: Classical Verification of Quantum Sampling

Verifier

(C, x)

Randomized output!



Prover

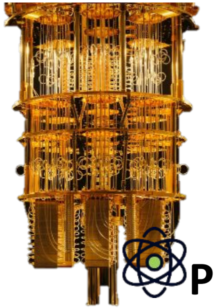
Accept/Reject

Model: Classical Verification of Quantum Sampling

Verifier

(C, x)

Randomized output!



Prover

$\mathrm{Accept}/\mathrm{Reject}$

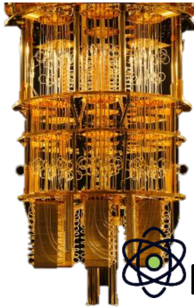
If accept, output y

Model: Classical Verification of Quantum Sampling

Verifier

(C, x)

Randomized output!



Prover

Goal (completeness): Honest prover $\implies [y \leftarrow C(x)]$

$\mathsf{Accept}/\mathsf{Reject}$

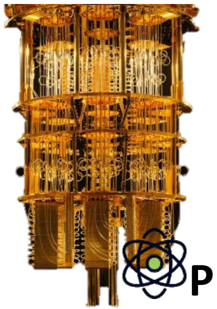
If accept, output y

Model: Classical Verification of Quantum Sampling

Verifier

(C, x)

Randomized output!



Prover

Goal (completeness): Honest prover $\Longrightarrow [y \leftarrow C(x)]$

(soundness): $\varepsilon = 1/\mathsf{poly}(n),$

$\mathsf{Accept}/\mathsf{Reject}$

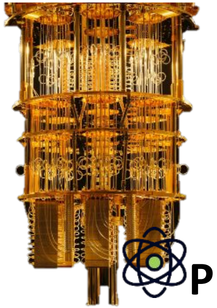
If accept, output y

Model: Classical Verification of Quantum Sampling

Verifier

(C, x)

Randomized output!



Prover

Goal (completeness): Honest prover $\Longrightarrow [y \leftarrow C(x)]$

(soundness): $\varepsilon = 1/\mathsf{poly}(n)$,

$\Pr[\mathsf{Accept}] > \varepsilon \Longrightarrow y|_{\mathsf{Accept}} \approx_\varepsilon C(x)$

$\mathsf{Accept}/\mathsf{Reject}$

If accept, output y

Challenges with Sampling Problems

Challenges with Sampling Problems

- Classical derandomization doesn’t work

Challenges with Sampling Problems

- Classical derandomization doesn't work

$$f(x) = f(x; r)$$

Challenges with Sampling Problems

- Classical derandomization doesn't work

$$\underbrace{f}_{\text{Deterministic}}(x) = f(x; r)$$

Challenges with Sampling Problems

- Classical derandomization doesn't work

$$f(x) = f(x; r)$$

Fix randomness and rerun for all output bits

Deterministic

Challenges with Sampling Problems

- Classical derandomization doesn't work

$$\underbrace{f}_{\text{Deterministic}}(x;\underbrace{r}_{\text{Fix randomness and rerun for all output bits}}) \quad f(x) = f(x;r)$$

- Amplification doesn't work

Challenges with Sampling Problems

- Classical derandomization doesn't work

$$\underbrace{f}_{\text{Deterministic}}(x) = f(x; \underbrace{r}_{\text{Fix randomness and rerun for all output bits}})$$

- Amplification doesn't work

Decision problems:

$x \in L$

$x \notin L$

Challenges with Sampling Problems

- Classical derandomization doesn't work

$$f(x) = \underbrace{f}_{\text{Deterministic}}(x; \underbrace{r}_{\text{Fix randomness and rerun for all output bits}})$$

- Amplification doesn't work

Decision problems:

$$x \in L \Rightarrow \Pr[\text{Accept} \leftarrow \Pi(x)] > \frac{2}{3}$$

$$x \notin L \Rightarrow \Pr[\text{Accept} \leftarrow \Pi(x)] < \frac{1}{3}$$

Challenges with Sampling Problems

- Classical derandomization doesn't work

$$\underbrace{f}_{\text{Deterministic}}(x) = f(x; \underbrace{r}_{\text{Fix randomness and rerun for all output bits}})$$

- Amplification doesn't work

Decision problems:

$$x \in L \Rightarrow \Pr[\mathsf{Accept} \leftarrow \Pi(x)] > \boxed{\frac{2}{3}}$$

$$x \notin L \Rightarrow \Pr[\mathsf{Accept} \leftarrow \Pi(x)] < \boxed{\frac{1}{3}}$$

Arbitrary!

Challenges with Sampling Problems

- Classical derandomization doesn't work

$$f(x) = \underbrace{f}_{\text{Deterministic}}(x; \underbrace{r}_{\text{Fix randomness and rerun for all output bits}})$$

- Amplification doesn't work

Decision problems:

Arbitrary!

$$x \in L \Rightarrow \Pr[\text{Accept} \leftarrow \Pi(x)] > \boxed{\frac{2}{3}} \xrightarrow{\text{Repeat}} \boxed{1-\varepsilon}$$

$$x \notin L \Rightarrow \Pr[\text{Accept} \leftarrow \Pi(x)] < \boxed{\frac{1}{3}} \xrightarrow{\text{Repeat}} \boxed{\varepsilon}$$

Challenges with Sampling Problems

- Classical derandomization doesn't work

$$f(x) = \underbrace{f}_{\text{Deterministic}}(x; \underbrace{r}_{\text{Fix randomness and rerun for all output bits}})$$

- Amplification doesn't work

Decision problems:

$$x \in L \Rightarrow \Pr[\text{Accept} \leftarrow \Pi(x)] > \boxed{\tfrac{2}{3}}$$

$$x \notin L \Rightarrow \Pr[\text{Accept} \leftarrow \Pi(x)] < \boxed{\tfrac{1}{3}}$$

Arbitrary!

$\xrightarrow{\text{Repeat}}$ $\boxed{1 - \varepsilon \quad \varepsilon}$

Sampling problems:

$$||C(x) - \Pi(x)|_{\text{Accept}}|| < \frac{1}{3}$$

Challenges with Sampling Problems

- Classical derandomization doesn't work

$$f(x) = \underbrace{f}_{\text{Deterministic}}(x; \underbrace{r}_{\text{Fix randomness and rerun for all output bits}})$$

- Amplification doesn't work

Decision problems:

$$x \in L \Rightarrow \Pr[\text{Accept} \leftarrow \Pi(x)] > \frac{2}{3}$$

$$x \notin L \Rightarrow \Pr[\text{Accept} \leftarrow \Pi(x)] < \frac{1}{3}$$

Arbitrary!

$$\boxed{\begin{matrix} \frac{2}{3} \\ \frac{1}{3} \end{matrix}} \xrightarrow{\text{Repeat}} \boxed{\begin{matrix} 1-\varepsilon \\ \varepsilon \end{matrix}}$$

Sampling problems:

$$||C(x) - \Pi(x)|_{\text{Accept}}|| < \frac{1}{3} \xrightarrow{?} \varepsilon$$

Our contributions

Under the QLWE assumption, we construct a *Classical Verification of Quantum Sampling* protocol that is:

- Blind
- Four-message
- Negligible completeness errors
- *Computationally* sound

Classical Verification of Quantum Computing

	Constant-round	Errors	Problem type	Blindness
[Mah18]	✓	≈ 3/4	Decision	

Classical Verification of Quantum Computing

	Constant-round	Errors	Problem type	Blindness
[Mah18]	✓	≈ 3/4	Decision	
[GV19]		negl.	Decision	✓
[CCY20, ACGH20]	✓	negl.	Decision	

Classical Verification of Quantum Computing

	Constant-round	Errors	Problem type	Blindness
[Mah18]	✓	$\approx 3/4$	Decision	
[GV19]		negl.	Decision	✓
[CCY20, ACGH20]	✓	negl.	Decision	
This work	✓	1/poly(n)	Sampling	✓

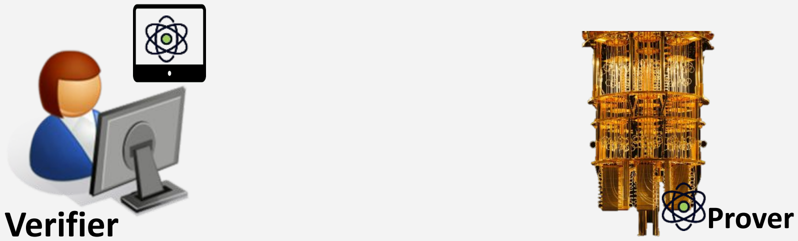
Classical Verification of Quantum Computing

	Constant-round	Errors	Problem type	Blindness
[Mah18]	✓	≈ 3/4	Decision	
[GV19]		negl.	Decision	✓
[CCY20, ACGH20]	✓	negl.	Decision	
This work	✓	1/poly(n)	Sampling	✓
[Bar21]	✓	negl.	Pseudo-deterministic	✓

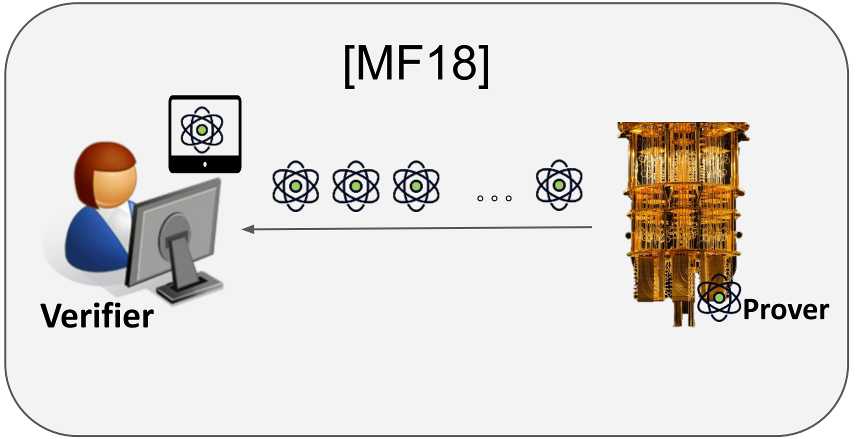
Overview of [Mah18]

Overview of [Mah18]

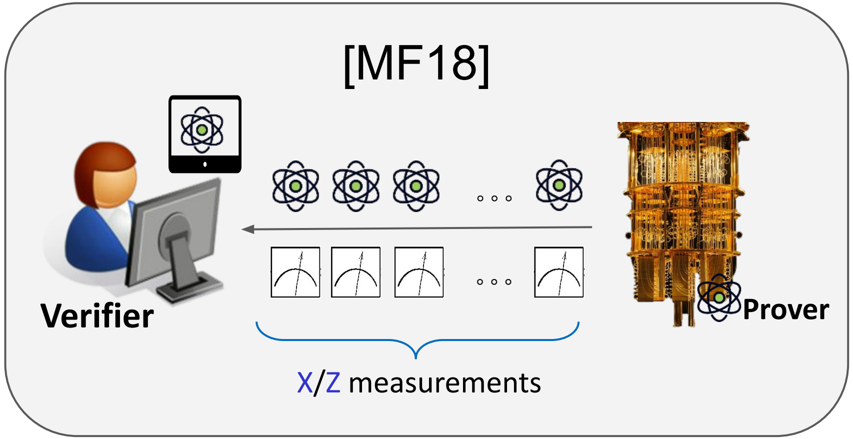
[MF18]



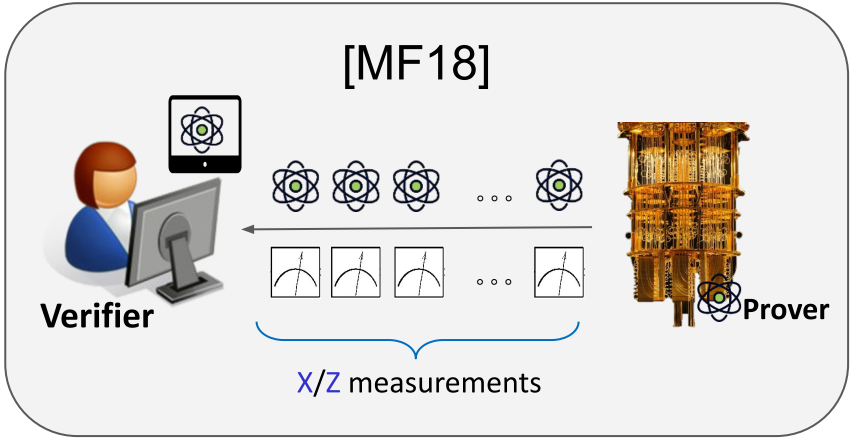
Overview of [Mah18]



Overview of [Mah18]

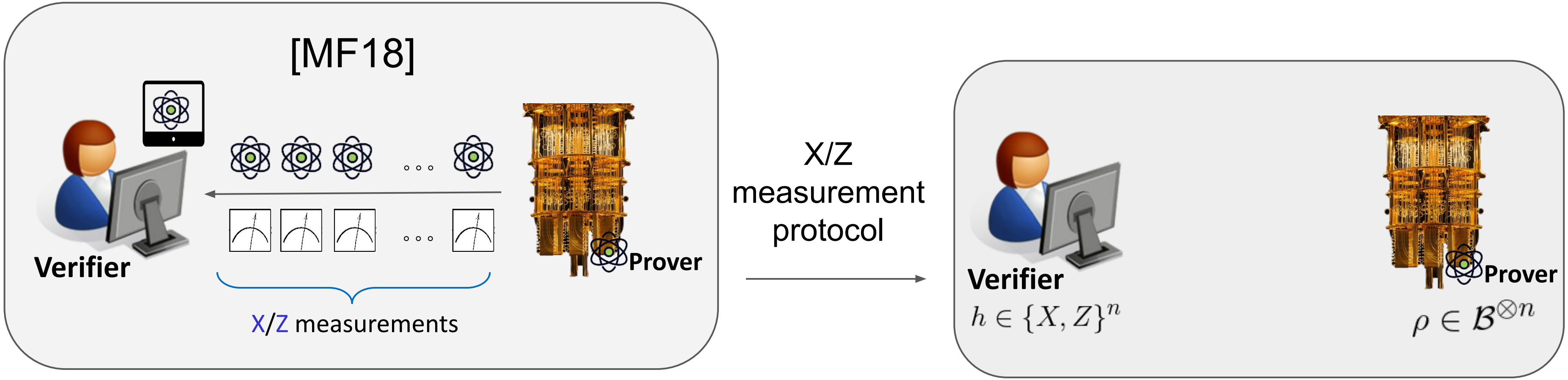


Overview of [Mah18]

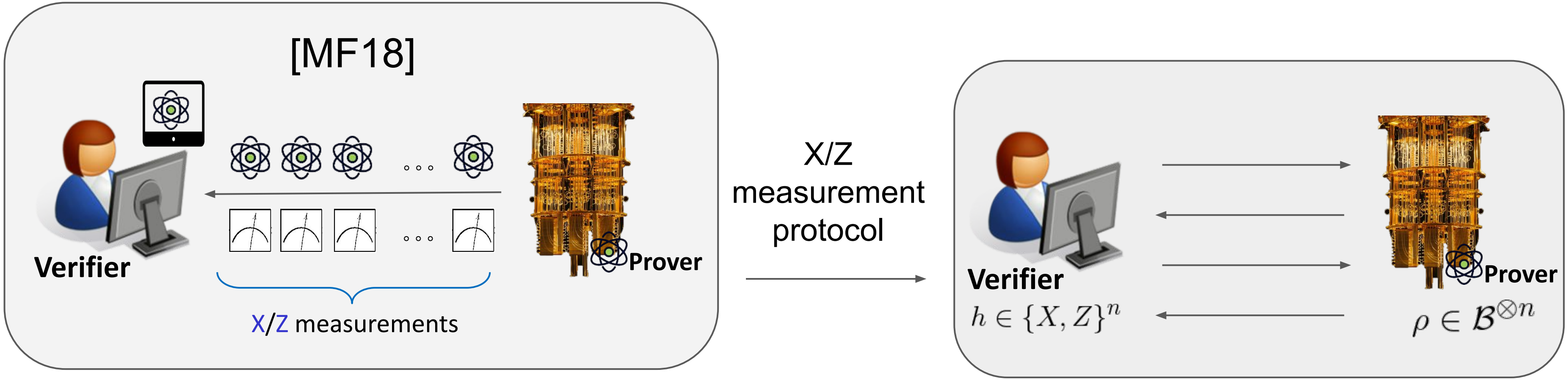


X/Z measurement protocol

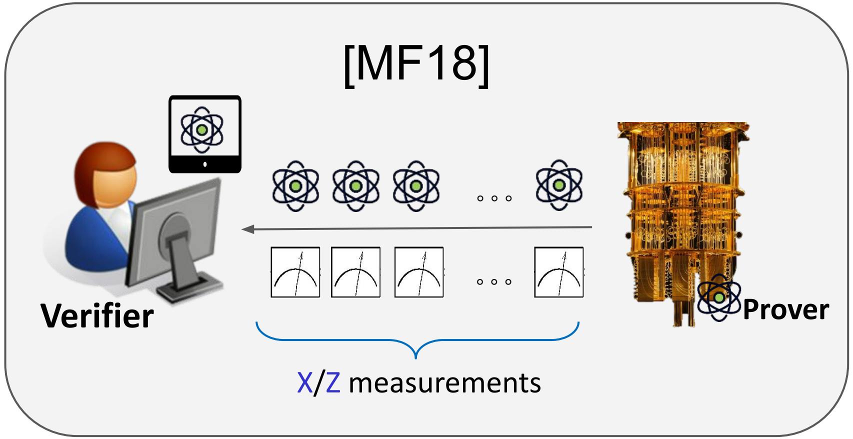
Overview of [Mah18]



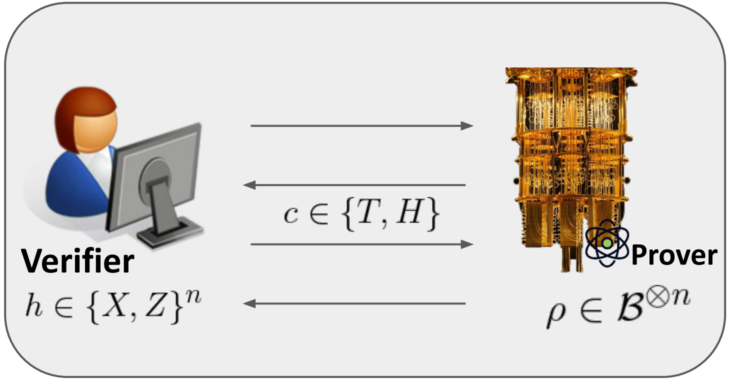
Overview of [Mah18]



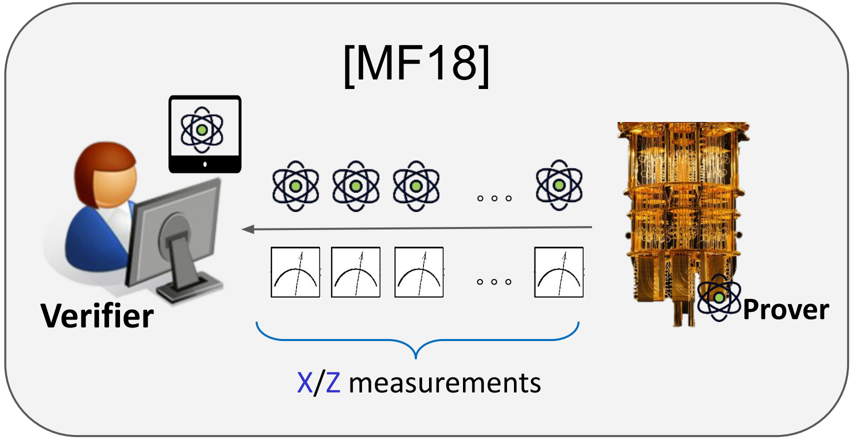
Overview of [Mah18]



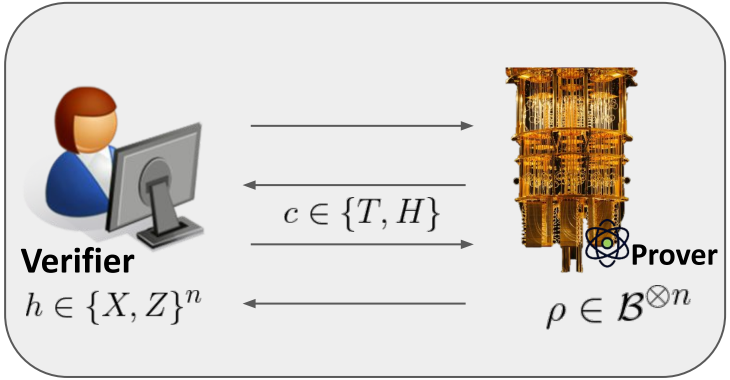
X/Z measurement protocol



Overview of [Mah18]

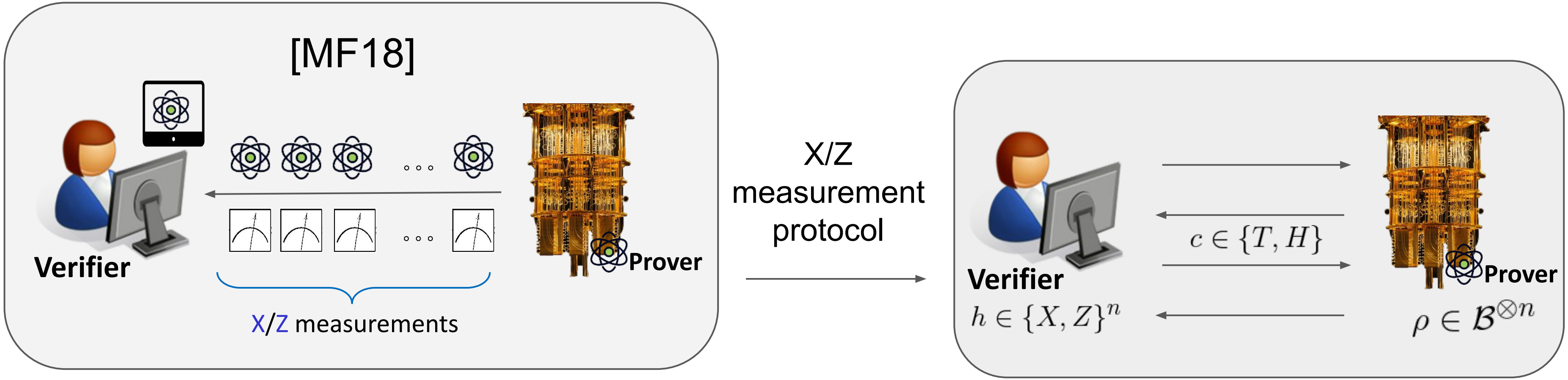


X/Z measurement protocol



$$(\mathsf{flag}, m) \leftarrow \mathcal{V}(c = H, \ldots)$$

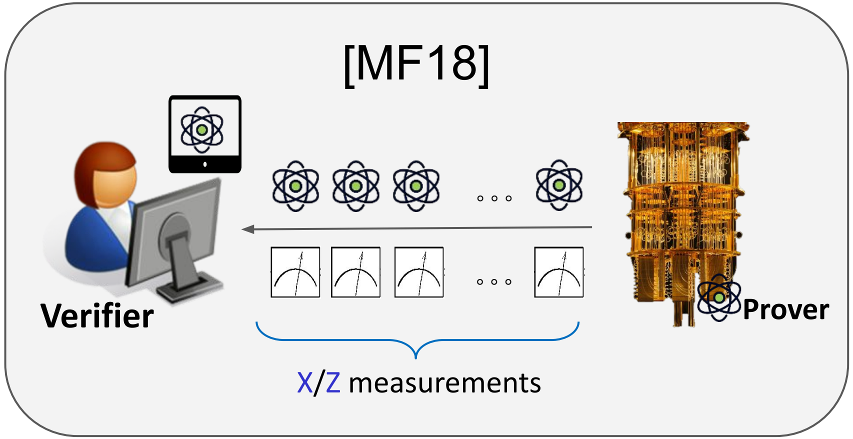
Overview of [Mah18]



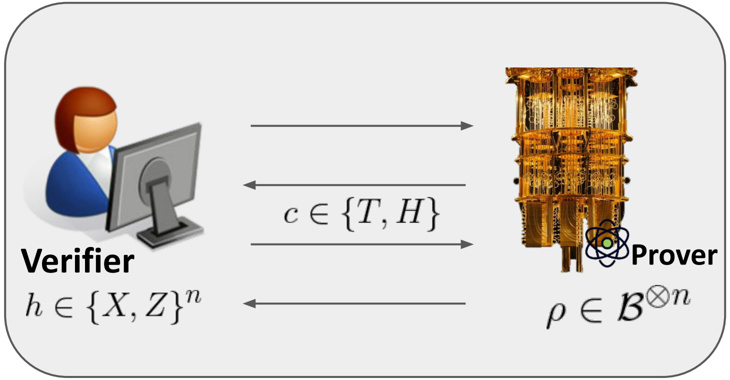
$$(\text{flag}, m) \leftarrow \mathcal{V}(c = H, \ldots)$$

$$\text{flag} = \text{Accept} \Rightarrow [m \xleftarrow[h]{\nearrow} \rho]$$

Overview of [Mah18]



X/Z measurement protocol

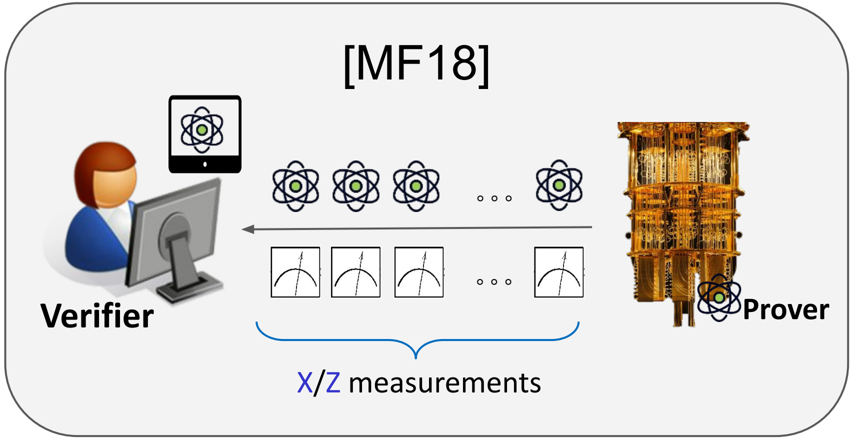


$$(\mathsf{flag}, m) \leftarrow \mathcal{V}(c = H, \ldots)$$

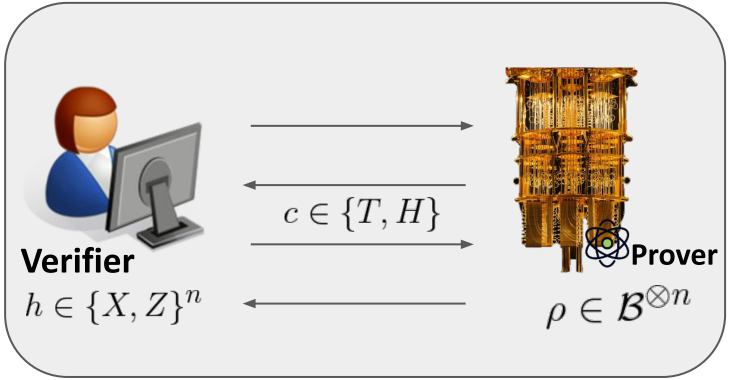
$$\mathsf{flag} = \mathsf{Accept} \Rightarrow [m \xleftarrow[h]{} \rho]$$

$$\mathsf{flag} \leftarrow \mathcal{V}(c = T, \ldots)$$

Overview of [Mah18]



X/Z measurement protocol



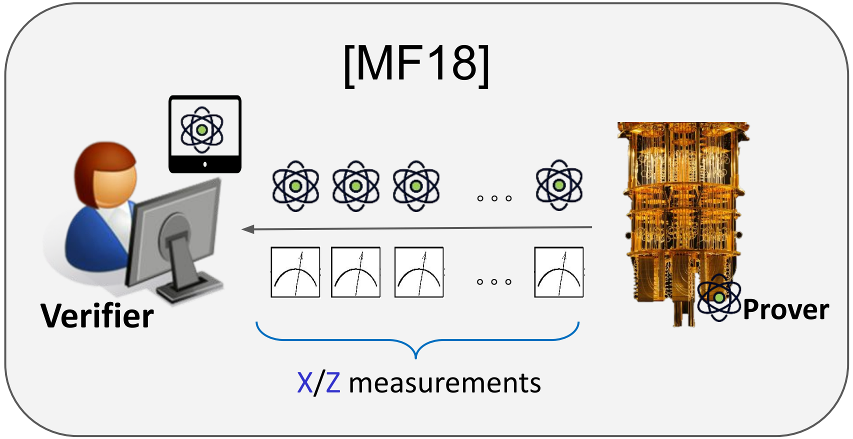
$$(\mathsf{flag}, m) \leftarrow \mathcal{V}(c = H, \ldots)$$

$$\mathsf{flag} = \mathsf{Accept} \Rightarrow [m \xleftarrow[h]{} \rho]$$

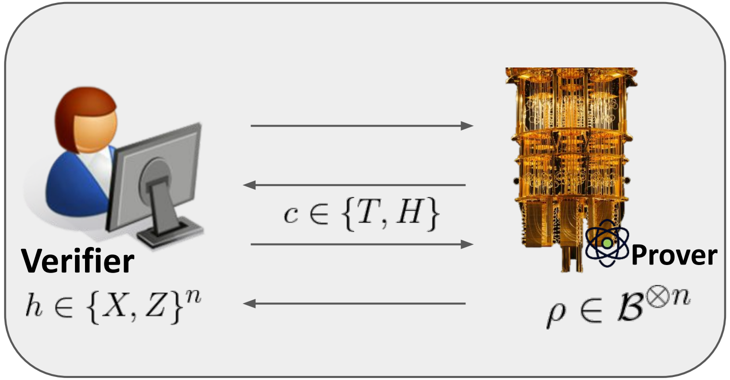
$$\mathsf{flag} \leftarrow \mathcal{V}(c = T, \ldots)$$

No measurement outcomes!

Overview of [Mah18]



X/Z measurement protocol



$$(\text{flag}, m) \leftarrow \mathcal{V}(c = H, \ldots)$$

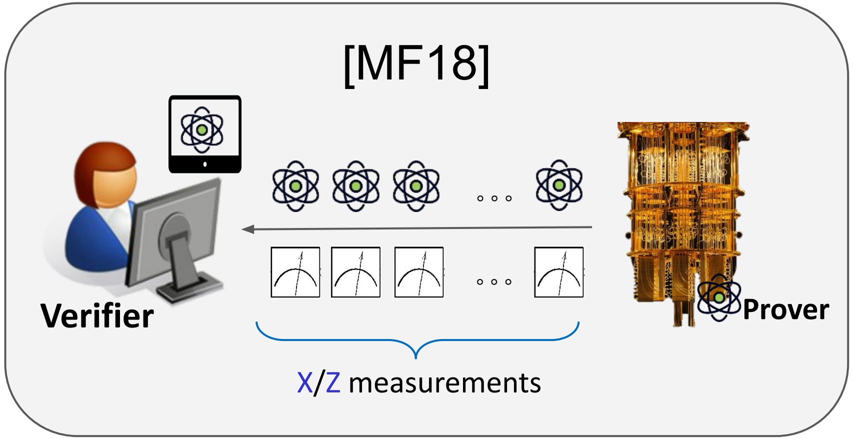
$$\text{flag} = \text{Accept} \Rightarrow [m \xleftarrow[h]{\nearrow} \rho]$$

$$\text{flag} \leftarrow \mathcal{V}(c = T, \ldots)$$

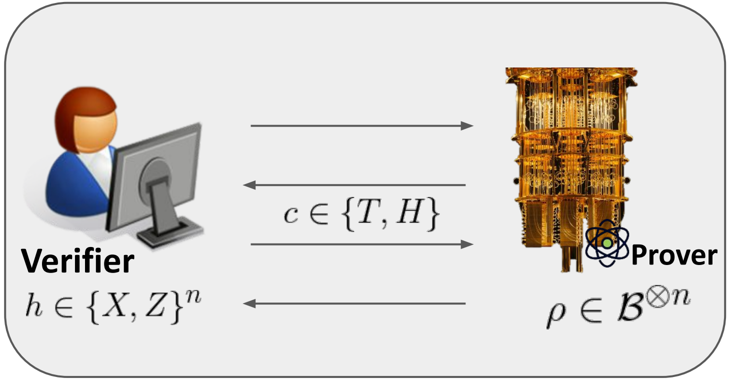
No measurement outcomes!

OK for BQP; ½ soundness loss…

Overview of [Mah18]



X/Z
measurement
protocol



$$(\mathsf{flag}, m) \leftarrow \mathcal{V}(c = H, \ldots)$$

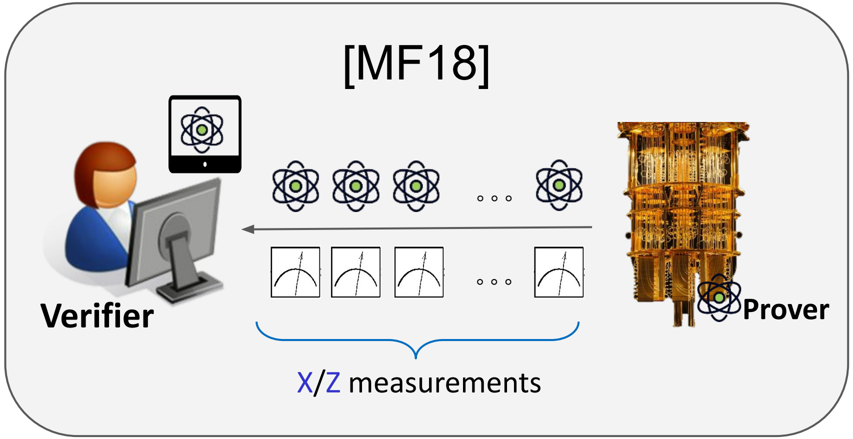
$$\mathsf{flag} = \mathsf{Accept} \Rightarrow [m \xleftarrow[h]{} \rho]$$

$$\mathsf{flag} \leftarrow \mathcal{V}(c = T, \ldots)$$

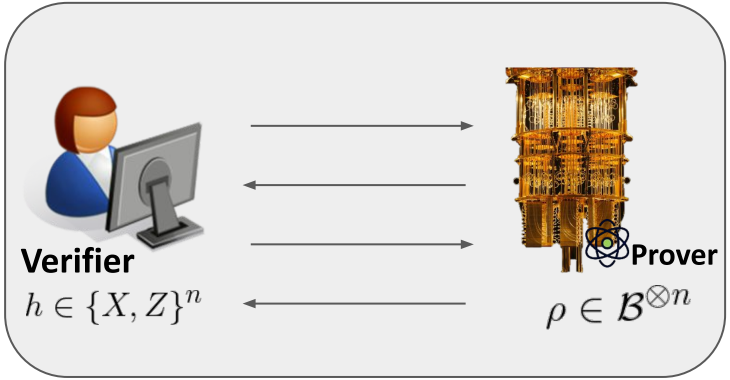
No measurement outcomes!

OK for BQP; ½ soundness loss… What about sampling?

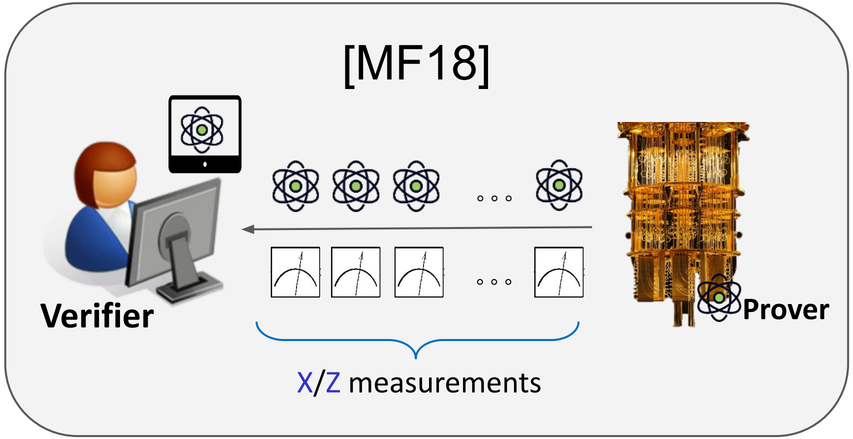
Our strategy



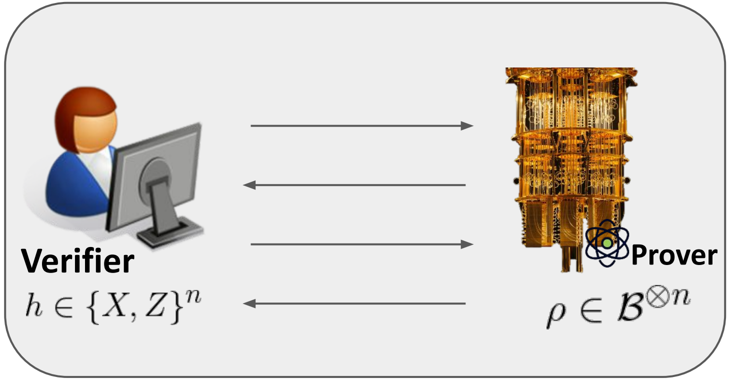
X/Z
measurement
protocol



Our strategy

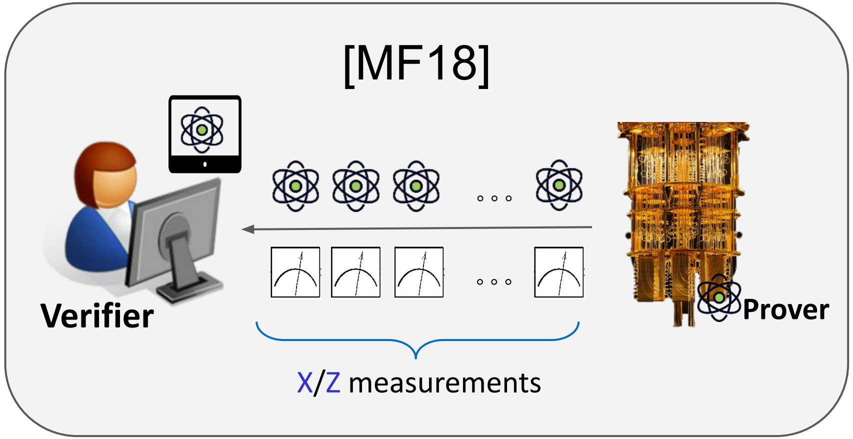


X/Z
measurement
protocol

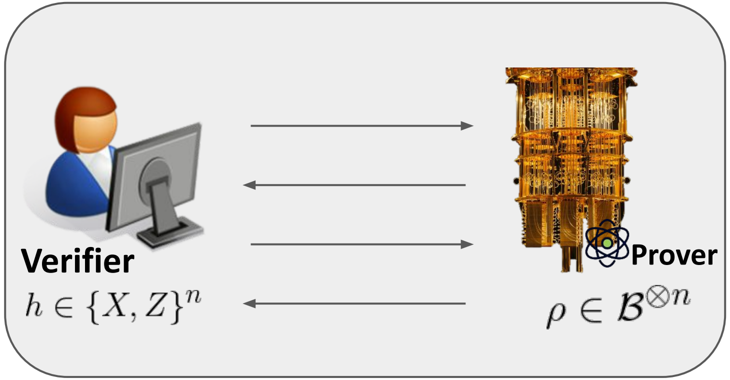


Generalize to handle
sampling problems

Our strategy



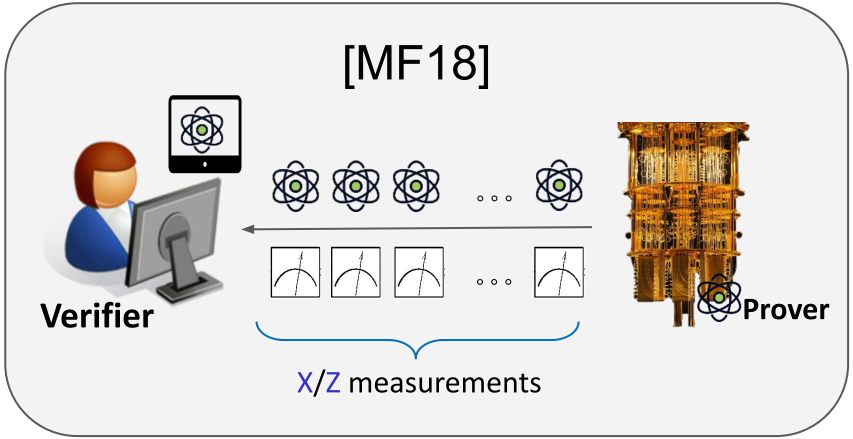
X/Z measurement protocol



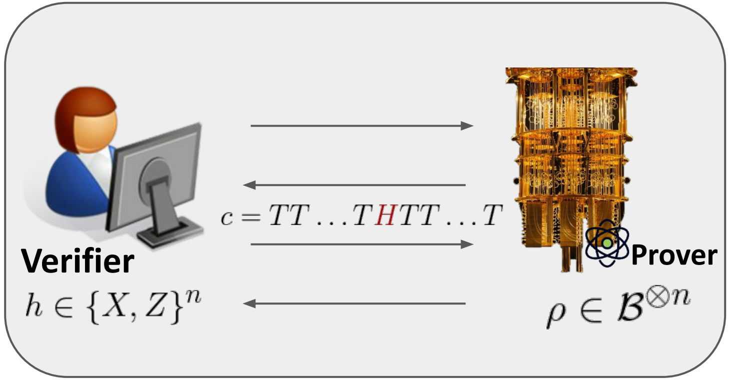
Generalize to handle sampling problems

Parallel repetition

Our strategy



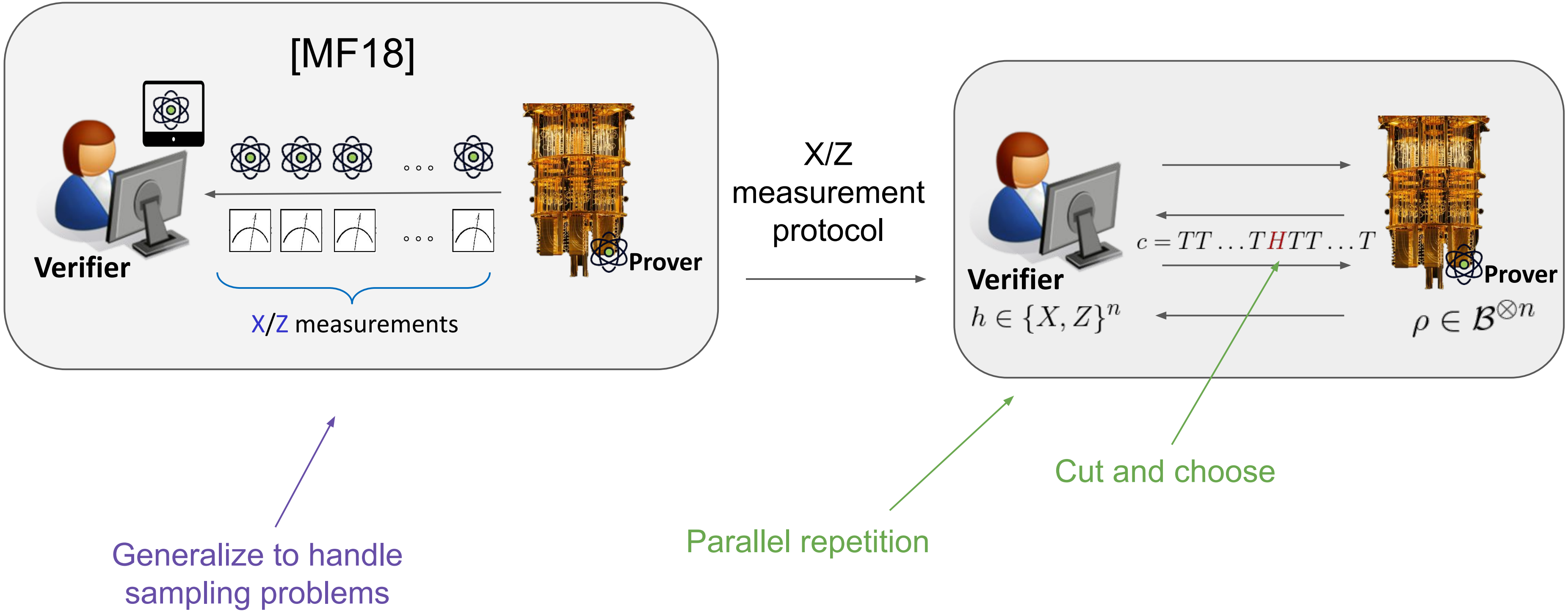
X/Z measurement protocol



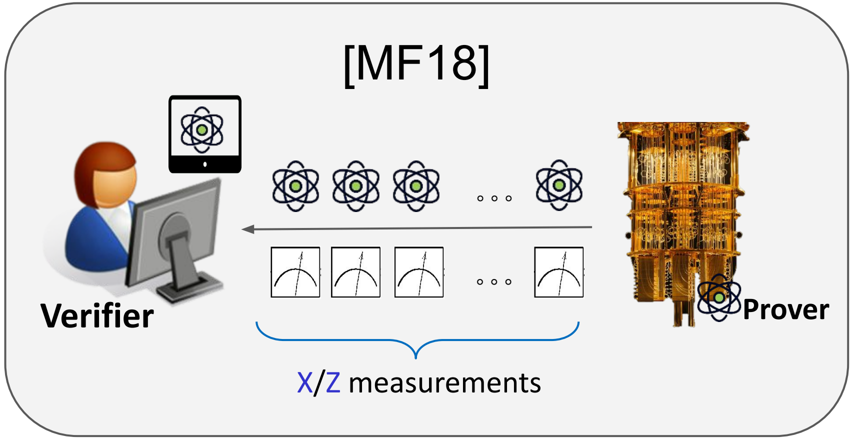
Generalize to handle sampling problems

Parallel repetition

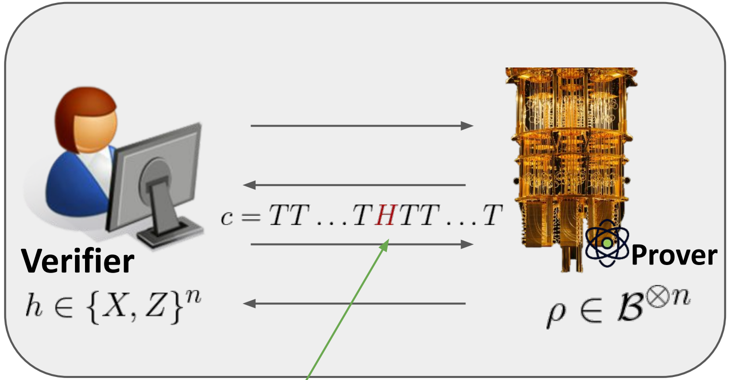
Our strategy



Our strategy



X/Z measurement protocol



Cut and choose

Parallel repetition

Generalize to handle sampling problems

[CCY20]: decompose prover's internal state

$$|\psi\rangle = |\psi_0\rangle + |\psi_{10}\rangle + |\psi_{110}\rangle + \ldots$$

Achieving Blindness

Achieving Blindness

- *Generic* Blindness Protocol Compiler

Achieving Blindness

- *Generic* Blindness Protocol Compiler
- Use *quantum fully homomorphic encryption*

Achieving Blindness

- *Generic* Blindness Protocol Compiler
- Use *quantum fully homomorphic encryption*
- Requires *classical-friendly* scheme [Bra18, Mah18]

Future Directions

Future Directions

- Is negligible errors achievable?

Future Directions

- Is negligible errors achievable?
  - Achieved in related settings

Future Directions

- Is negligible errors achievable?
  - Achieved in related settings
    - Verifiable quantum FHE [ADSS17]

Future Directions

- Is negligible errors achievable?
    - Achieved in related settings
        - Verifiable quantum FHE [ADSS17]
        - Multiparty quantum computations [CGS02, DNS12]

Future Directions

- Is negligible errors achievable?
  - Achieved in related settings
    - Verifiable quantum FHE [ADSS17]
    - Multiparty quantum computations [CGS02, DNS12]
    - Current constructions require weak quantum client

Future Directions

- Is negligible errors achievable?
  - Achieved in related settings
    - Verifiable quantum FHE [ADSS17]
    - Multiparty quantum computations [CGS02, DNS12]
    - Current constructions require weak quantum client
- Can we construct a general *remote state preparation* ([GV19]) protocol?

References

- [Mah18]: Classical verification of quantum computations. 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), 2018.
- [GV19]: Alexandru Gheorghiu and Thomas Vidick. Computationally-secure and composable remote state preparation. In FOCS, pages 1024–1033, 2019
- [CCY20]: Nai-Hui Chia, Kai-Min Chung, and Takashi Yamakawa. Classical verification of quantum computations with efficient verifier. In Theory of Cryptography Conference, pages 181–206. Springer, 2020.
- [ACGH20]: Gorjan Alagic, Andrew M Childs, Alex B Grilo, and Shih-Han Hung. Non-interactive classical verification of quantum computation. In Theory of Cryptography Conference, pages 153–180. Springer, 2020.
- [Bar21]: James Bartusek. Secure Quantum Computation with Classical Communication. In Theory of Cryptography Conference, pages 1–30. Springer, 2021.
- [MF18]: Joseph F. Fitzsimons, Michal Hajdušek, and Tomoyuki Morimae. Post hoc verification of quantum computation. Phys. Rev. Lett., 120:040501, Jan 2018.
- [ADSS17]: Gorjan Alagic, Yfke Dulek, Christian Schaffner, and Florian Speelman. Quantum fully homomorphic encryption with verification. In International Conference on the Theory and Application of Cryptology and Information Security, pages 438-467. Springer, 2017.
- [CGS02]: Claude Crépeau, Daniel Gottesman, and Adam Smith. Secure multi-party quantum computation. In Proceedings of the thirty-fourth annual ACM symposium on Theory of computing, pages 643-652. 2002.
- [DNS12]: Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Actively secure two-party evaluation of any quantum operation. In Annual Cryptology Conference, pages 794-811. Springer, 2012.