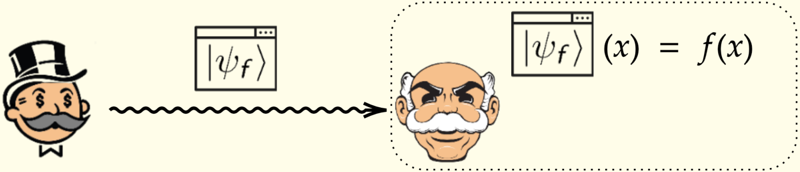
Semi-Quantum Copy-Protection and More

Céline Chevalier, Paul Hermouet and Quoc-Huy Vu

Copy-Protection

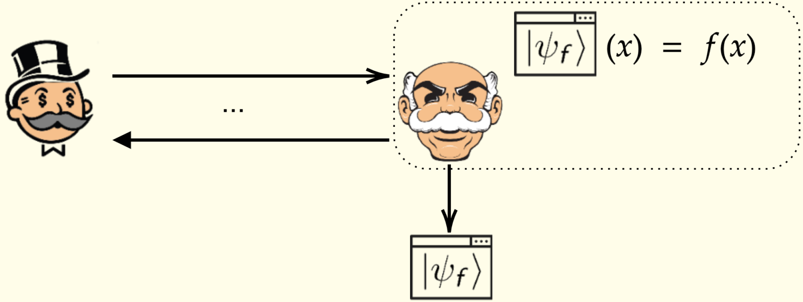
Copy-protection: Vendor and Client are quantum; quantum communications

Copy-Protection



Copy-protection: Vendor and Client are quantum; quantum communications

Semi-Quantum Copy-Protection



Copy-protection: Vendor and Client are quantum; quantum communications

Semi-quantum Copy-protection: Vendor is classical; classical communications

Coset States

For $A \subset \mathbb{F}_2^n$, $s, s' \in \mathbb{F}_2^n$

$$|A_{ss'}\rangle = \frac{1}{\sqrt{|A|}} \sum_{a \in A} (-1)^{a \cdot s'} |a + s\rangle$$

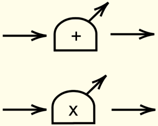
Holds information on both $A + s$ and $A^{\perp} + s'$

[1] [CLLZ21]

Coset States

For $A \subset \mathbb{F}_2^n,\ s, s' \in \mathbb{F}_2^n$

$$|A_{ss'}\rangle = \frac{1}{\sqrt{|A|}} \sum_{a \in A} (-1)^{a \cdot s'} |a + s\rangle$$



$u \in A + s$

$v \in A^{\perp} + s'$

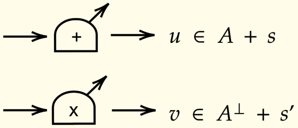
Holds information on both $A + s$ and $A^{\perp} + s'$

[1] [CLLZ21]

Coset States

For $A \subset \mathbb{F}_2^n$, $s, s' \in \mathbb{F}_2^n$

$$|A_{ss'}\rangle = \frac{1}{\sqrt{|A|}} \sum_{a \in A} (-1)^{a \cdot s'} |a + s\rangle$$



Holds information on both $A + s$ and $A^\perp + s'$

Direct product hardness:
No adversary can, given $|A_{s,s'}\rangle$ return $u \in A + s$ and $v \in A^\perp + s'$.

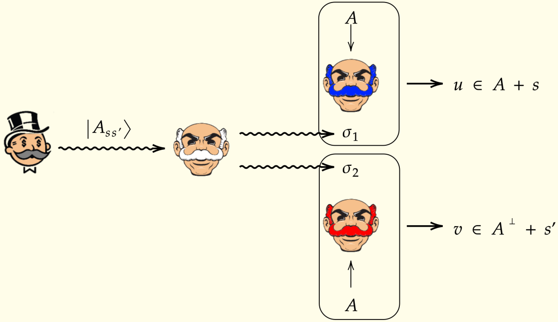
[1][CLLZ21]

Monogamy-of-Entanglement

Monogamy-of-Entanglement

$$p_{win} = \mathsf{negl}(\lambda)$$

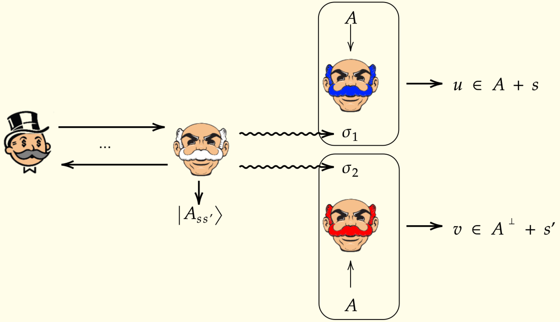
Monogamy-of-Entanglement



Monogamy-of-Entanglement

$$p_{win} = \text{negl}(\lambda)$$

Monogamy-of-Entanglement



Semi-Quantum Monogamy-of-Entanglement

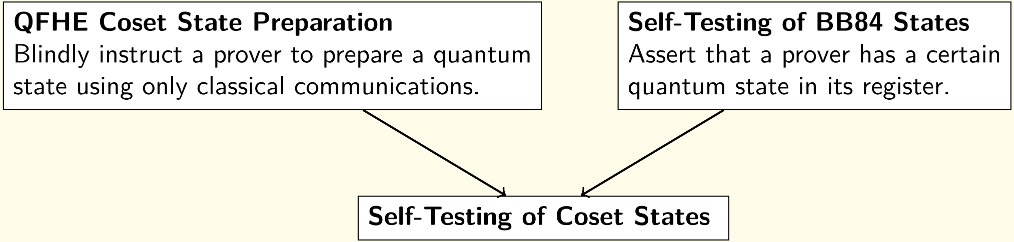
$$p_{win} = \mathsf{negl}(\lambda) \text{ ?}$$

Construction Overview

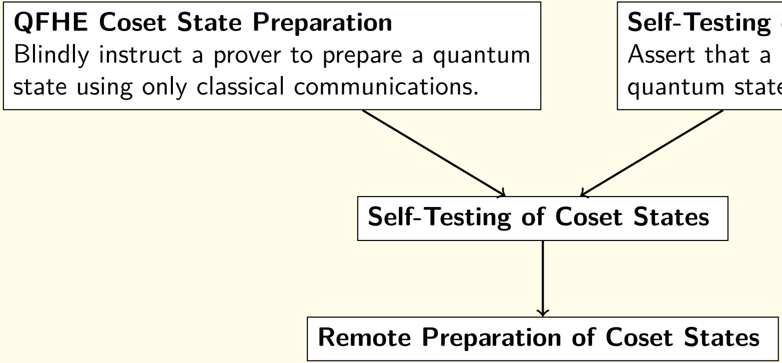
QFHE Coset State Preparation
Blindly instruct a prover to prepare a quantum state using only classical communications.

Self-Testing of BB84 States
Assert that a prover has a certain quantum state in its register.

Construction Overview



Construction Overview



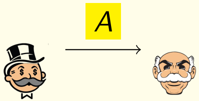
QFHE Coset State Preparation

Q(uantum)FHE: $\mathsf{Enc}(x) \rightarrow$ x $\mathsf{Eval}(C,$ x $) \rightarrow \mathsf{QOTP}_{s,s'} C(x),$ s, s'

[1] [Shm22]

QFHE Coset State Preparation

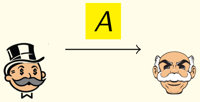
Q(uantum)FHE: $\mathsf{Enc}(x) \to$ x $\quad$ $\mathsf{Eval}(C,$ x $) \to \mathsf{QOTP}_{s,s'}\, C(x)$, s, s'



[1] [Shm22]

QFHE Coset State Preparation

Q(uantum)FHE: $\text{Enc}(x) \rightarrow$ x $\qquad \text{Eval}(C,$ x $) \rightarrow \text{QOTP}_{s,s'}\, C(x)$, s, s'



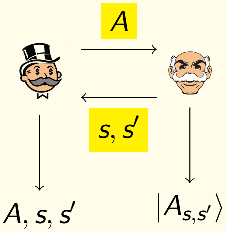
$$\text{Eval}(C, A)$$
$$\downarrow$$
$$|A_{s,s'}\rangle, s, s'$$

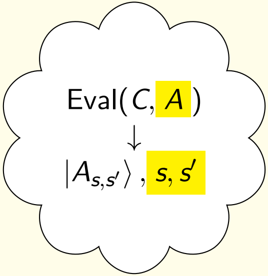
$C(A) \rightarrow |A\rangle = \sum_{a \in A} |a\rangle$

[1] [Shm22]

QFHE Coset State Preparation

Q(uantum)FHE: $\text{Enc}(x) \to$ x $\quad \text{Eval}(C,$ x $) \to \text{QOTP}_{s,s'}\, C(x),$ s, s'





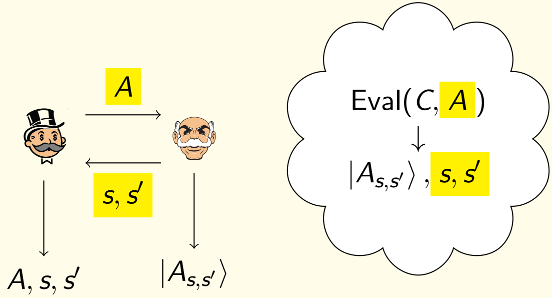
$C(A) \to |A\rangle = \sum_{a \in A} |a\rangle$

[1] [Shm22]

QFHE Coset State Preparation

Q(uantum)FHE: $\mathsf{Enc}(x) \to$ x $\quad$ $\mathsf{Eval}(C,$ x $) \to \mathsf{QOTP}_{s,s'}\, C(x)$, s, s'

$C(A) \to |A\rangle = \sum_{a \in A} |a\rangle$

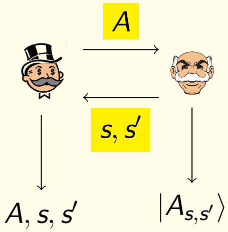


- **Problem:** there is a simple "cloning" attack in our case...

[1] [Shm22]

QFHE Coset State Preparation

Q(uantum)FHE: $\text{Enc}(x) \rightarrow$ x $\qquad \text{Eval}(C,$ x $) \rightarrow \text{QOTP}_{s,s'}\, C(x),$ s, s'



$\text{Eval}(C, A)$

$\downarrow$

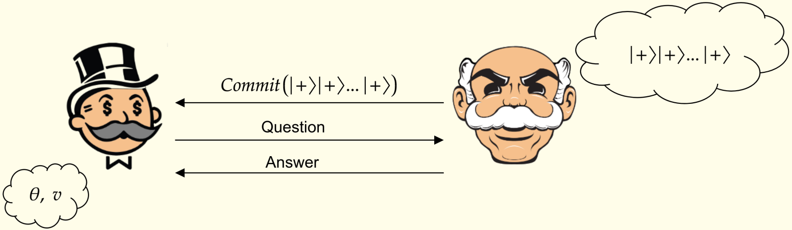
$|A_{s,s'}\rangle\,, s, s'$

$C(A) \rightarrow |A\rangle = \sum_{a \in A} |a\rangle$

- **Problem:** there is a simple "cloning" attack in our case...
- **Solution:** use self-testing !

[1] [Shm22]

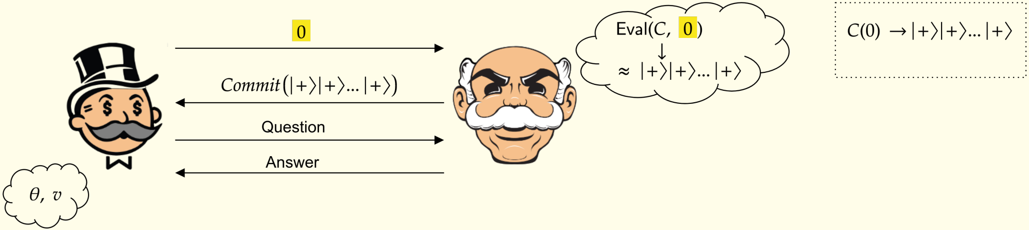
Self-Testing of BB84 States



Soundness: If the Verifier accepts, then the state in the Prover's register before the last message is $H^{\theta}|v\rangle$.

[0] [GMP22, GV19, Mah18]

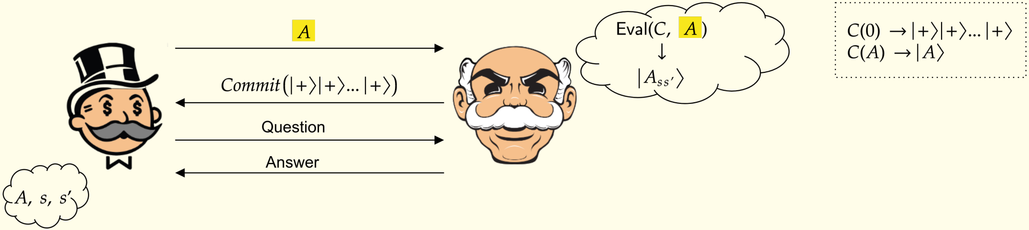
Self-Testing of BB84 States



QFHE preparation: Using QFHE for $|+\rangle$ preparation does not change the correctness and soundness.

[0] [GMP22, GV19, Mah18]

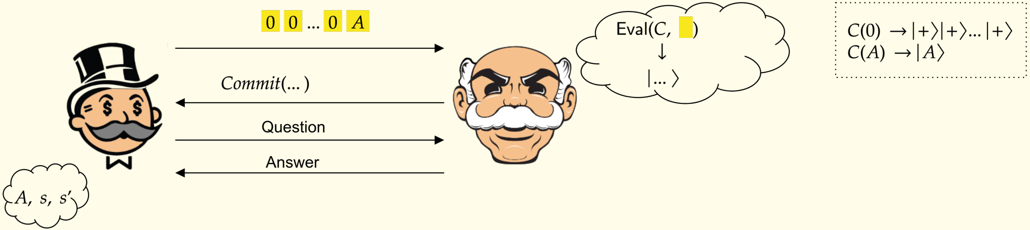
Self-Testing of Coset States



Using A: Replacing 0 by A is indistinguishable from the Prover's point of view.

[0] [GMP22, GV19, Mah18]

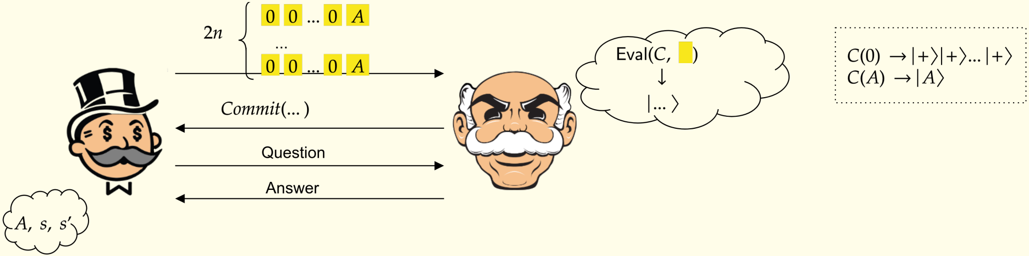
Self-Testing of Coset States



Self-testing: Run BB84 instances until we are sure the Prover is honest, then run a coset instance.

[0] [GMP22, GV19, Mah18]

Remote Preparation of Coset States



From self-testing to remote preparation: Self-testing destroys the state. Solution: run the protocol in a n-among-$2n$ cut-and-choose way.

[0] [GMP22, GV19, Mah18]

Semi-Quantum Monogamy-of-Entanglement

Soundness is not perfect: If the Verifier accepts, then the state in the Prover's register before the last message is $|A_{s,s'}\rangle$ (with probability $1 - 1/\text{poly}(\lambda)$).

Solution: We actually do not need negligible error: only that the prover cannot win the semi-quantum monogamy-of-entanglement $\rightarrow$ we reduce this semi-quantum monogamy-of-entanglement to the original monogamy-of-entanglement.

Conclusion

Contributions:

- Remote coset state preparation $\rightarrow$ semi-quantum copy-protection.
- Copy-protection for point functions in the plain model (for a specific distribution).
- Tokenized signature scheme with strong unforgeability property.

Thank You !

Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry.
Hidden cosets and applications to unclonable cryptography.
2021.

Alexandru Gheorghiu, Tony Metger, and Alexander Poremba.
Quantum cryptography with classical communication: parallel remote state preparation for copy-protection, verification, and more.
arXiv preprint arXiv:2201.13445, 2022.

Alexandru Gheorghiu and Thomas Vidick.
Computationally-secure and composable remote state preparation.
11 2019.

Urmila Mahadev.
Classical verification of quantum computations.
In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 259–267. IEEE, 2018.

Omri Shmueli.
Public-key quantum money with a classical bank.

In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 790–803, 2022.