Semi-Quantum Copy-Protection and More

collaboration with Huy Vu and Céline Chevalier

Copy-Protection of Point Functions

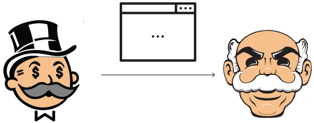
collaboration with Huy Vu and Céline Chevalier

What is Copy-Protection ?

Produce unclonable programs

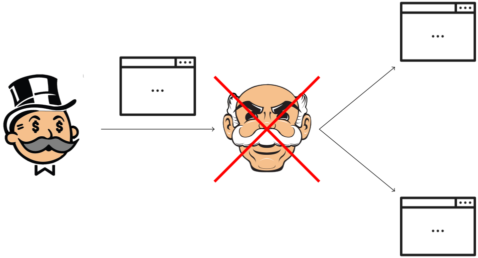
What is Copy-Protection ?

Produce unclonable programs



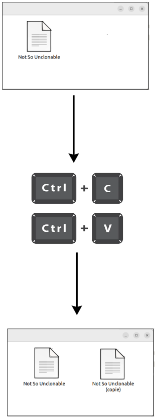
What is Copy-Protection ?

Produce unclonable programs



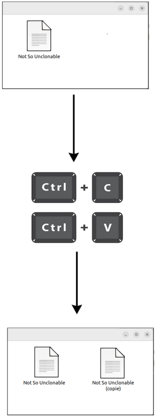
Classical Impossibility

Classically

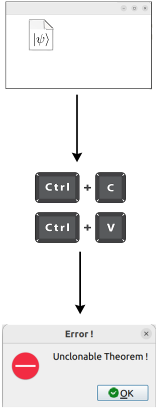


Classical Impossibility

Classically



Quantumly



Overview

1. Unclonability
2. Copy-Protection of Point Functions
3. Copy-Protection of Point Functions in the Plain Model

Unclonability

Quantum States

- A quantum state is a *superposition* of vectors
- To read it, one must *measure* the state:
  - the outcome is one of these vectors
  - the other ones are destroyed

Example

$$|00\rangle + |01\rangle \longrightarrow \boxed{\text{Measurement } +} \longrightarrow 01$$

Quantum States

- A quantum state is a *superposition* of vectors
- To read it, one must *measure* the state:
  - the outcome is one of these vectors
  - the other ones are destroyed

Example

$$\begin{tikzcd} \boxed{|00\rangle + |01\rangle} \arrow[r] \arrow[d, bend right] & \boxed{\text{Measurement } +} \arrow[r] & 01 \\ \boxed{|01\rangle} & & \end{tikzcd}$$

No-Cloning Theorem

There is no quantum algorithm that clones arbitrary quantum states.

Copy-Protection of Point Functions

Definitions

Point function: $\mathsf{PF}_y(x) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$

Copy-Protection of $\{\mathsf{PF}_y\}_{y \in \{0,1\}^n}$

Definitions

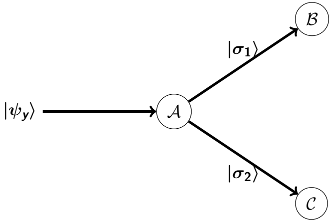
Point function: $\mathsf{PF}_y(x) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$

Copy-Protection of $\{\mathsf{PF}_y\}_{y \in \{0,1\}^n}$

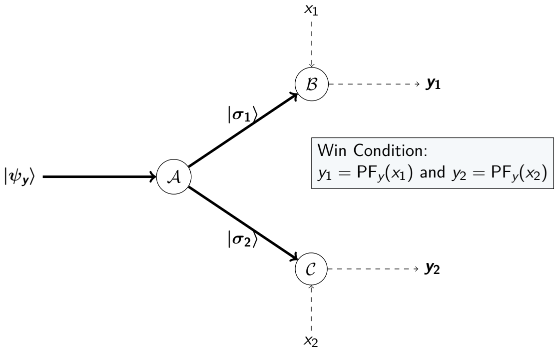
$$\boldsymbol{y} \longrightarrow \boxed{\textbf{Protect}} \longrightarrow |\psi_{\boldsymbol{y}}\rangle$$

$$\begin{array}{l} |\psi_{\boldsymbol{y}}\rangle \longrightarrow \\ \boldsymbol{x} \longrightarrow \end{array} \boxed{\textbf{Eval}} \longrightarrow \mathbf{PF}_{\boldsymbol{y}}(\boldsymbol{x})$$

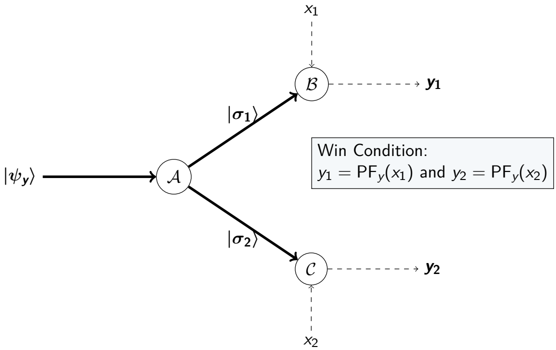
Anti-Piracy Security



Anti-Piracy Security



Anti-Piracy Security



Challenge Distributions

Product distribution: $(y, y), (y, \$), (\$, y), (\$, \$) \to p_{win} \leq 1/2$
Non-colliding distribution: $(y, \$), (\$, y), (\$, \$) \to p_{win} \leq 2/3$

History

	Security	**Model**	**Distribution**
CMP20	constant	QROM	non-colliding
AKL+22	negligible	QROM	product
CHV23	negligible	Plain Model	non-colliding
This work	negligible	Plain Model	product

In the Plain Model

Coset States

$A \subset \mathbb{F}_2^n$, $dim(A) = n/2$, $s, s' \in \mathbb{F}_2^n$

$|A, s, s'\rangle$: superposition of all vectors in $A + s$ (*regular coset*) and $A^{\perp} + s'$ (*dual coset*)

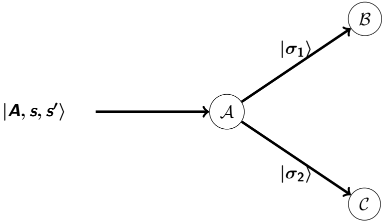
It is only possible to get information on either the regular coset of the dual one: $p_{win}(\text{MoE}) \leq \text{negl}(n)$

Coset States

$A \subset \mathbb{F}_2^n$, $dim(A) = n/2$, $s, s' \in \mathbb{F}_2^n$

$|A, s, s'\rangle$: superposition of all vectors in $A + s$ (*regular coset*) and $A^{\perp} + s'$ (*dual coset*)

It is only possible to get information on either the regular coset of the dual one: $p_{win}(\text{MoE}) \leq \text{negl}(n)$

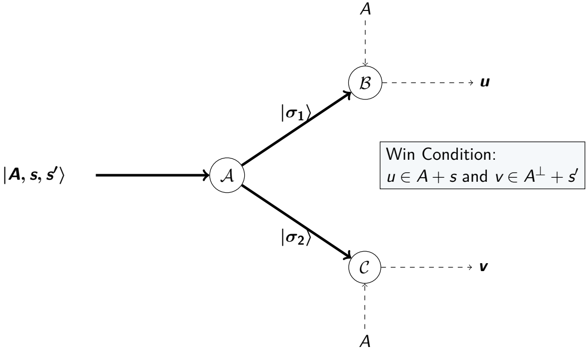


Coset States

$A \subset \mathbb{F}_2^n$, $dim(A) = n/2$, $s, s' \in \mathbb{F}_2^n$

$|A, s, s'\rangle$: superposition of all vectors in $A + s$ (*regular coset*) and $A^\perp + s'$ (*dual coset*)

It is only possible to get information on either the regular coset of the dual one: $p_{win}(\mathrm{MoE}) \leq \mathrm{negl}(n)$

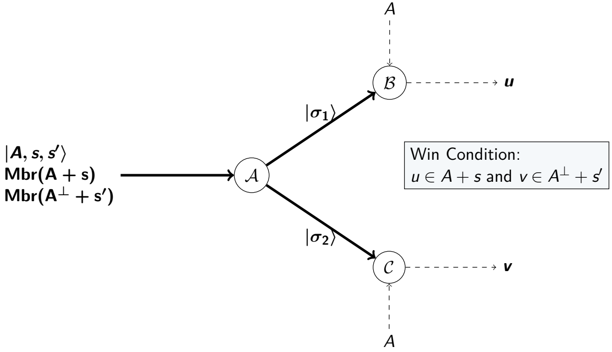


Coset States

$A \subset \mathbb{F}_2^n$, $dim(A) = n/2$, $s, s' \in \mathbb{F}_2^n$

$|A, s, s'\rangle$: superposition of all vectors in $A + s$ (*regular coset*) and $A^\perp + s'$ (*dual coset*)

It is only possible to get information on either the regular coset of the dual one: $p_{win}(\mathrm{MoE}) \leq \mathrm{negl}(n)$



Construction

We use a pseudorandom functions family PRF and indistinguishable obfuscation iO.

Protect(y)

Return $\mathsf{PRF}(\mathsf{k}, y), \mathsf{iO}(\mathsf{P_k}), |A, s, s'\rangle$

$\mathsf{P_k}(u, x)$:

- Checks whether $u \in \begin{cases} A + s & \text{if } x_0 = 0 \\ A^{\perp} + s' & \text{if } x_0 = 1 \end{cases}$
- Return $\mathsf{PRF}(\mathsf{k}, x)$

Eval($z, \widehat{\mathsf{P_k}}, |A, s, s'\rangle, x$)

- Compute $z' = \widehat{\mathsf{P_k}}(|A, s, s'\rangle, x)$
- Return 1 if $z' = z$ and 0 otherwise

Security: Main Argument

$\rightarrow$ relies on Compute-and-Compare Obfuscation

$$\mathcal{B}(\sigma_1) \text{ distinguishes between } y \text{ and } \$$$

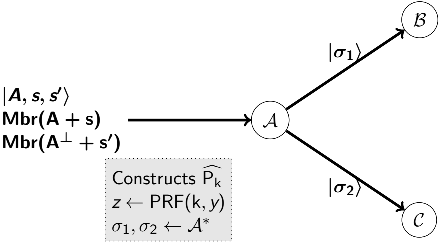
$$\Downarrow$$

$$\mathcal{B}(\sigma_1, x_1, A) \rightarrow u \in \begin{cases} A + s \\ \text{or} \\ A^{\perp} + s' \end{cases} \quad \text{(depends on } x_1\text{)}$$

Also works for $\mathcal{C}$ with (σ_2, x_2)

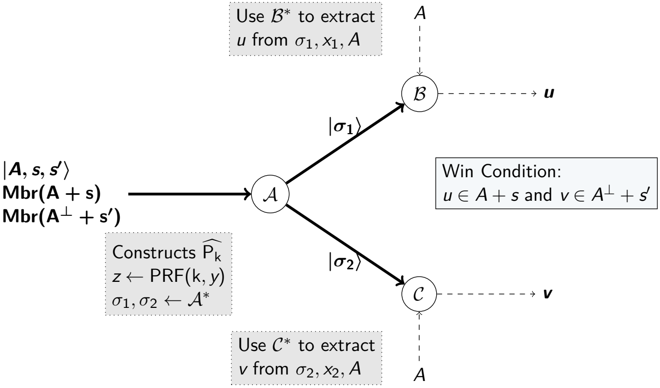
Reduction

$\mathcal{A}^*, \mathcal{B}^*, \mathcal{C}^*$ break anti-piracy security of our construction.



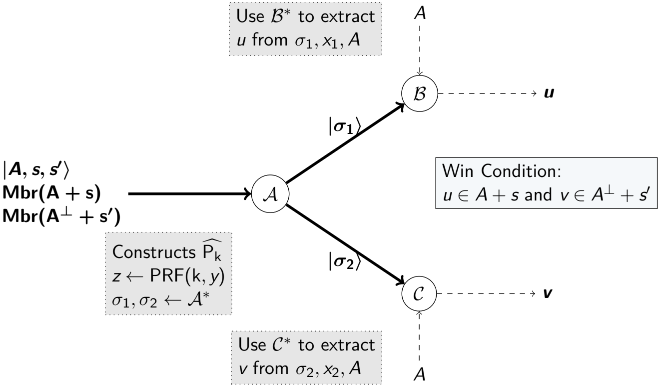
Reduction

$\mathcal{A}^*, \mathcal{B}^*, \mathcal{C}^*$ break anti-piracy security of our construction.



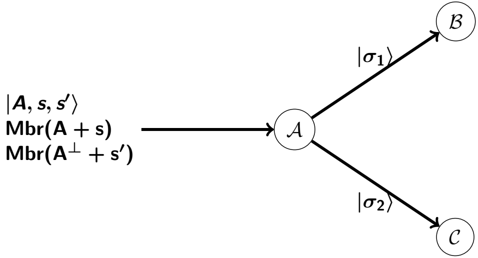
Reduction

$\mathcal{A}^*, \mathcal{B}^*, \mathcal{C}^*$ break anti-piracy security of our construction.

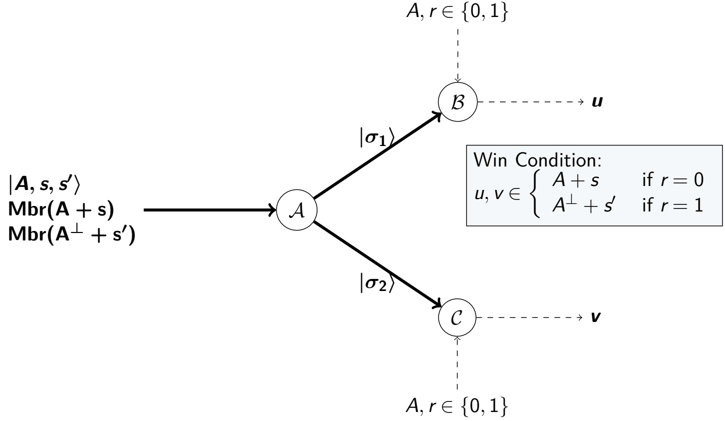


Problem when using product distribution !

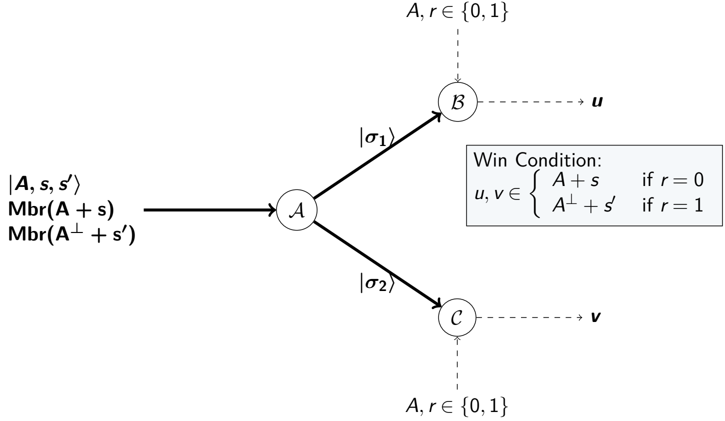
A New Monogamy-of-Entanglement Game



A New Monogamy-of-Entanglement Game



A New Monogamy-of-Entanglement Game



We prove $p_{win}(\text{MoE}) \leq 1/2$ and $p_{win}(\text{MoE}^n) \leq \text{negl}(n)$

Thank you !