Recent Developments in Quantum Copy Protection

**Mark Zhandry** (Princeton & NTT Research)

Based on joint works with Scott Aaronson, Andrea Coladangelo, Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang
Copy Protection
= 1101110100100010100001100011010...
Enter quantum...
Quantum No-Cloning
Quantum Money

[Wiesner’70]
Quantum Copy Protection

[Aaronson’09]

Problem: No-cloning theorem gives non-functional states
Thm [Aaronson’09]: Relative to a quantum oracle, \( \exists \) quantum copy protection \( \forall \) non-learnable classical programs

Inherent
Q: Can oracle be implemented in real world?
Detour:
Some other classical DRM objectives...
Software Obfuscation
Watermarking
What do we know?
Ad Hoc Obfuscation

Central object in theoretical cryptography

Mathematical Obfuscation
Thm [Barak-Goldreich-Impagliazzo-Rudich-Sahai-Vadhan-Yang’01]: Some programs cannot be obfuscated.
Indistinguishability obfuscation (iO):

$\equiv$  

No meaningful obfuscation guarantee on its own

**Thm [Goldwasser-Rothblum’07]:** If $P$ can be obfuscated, iO obfuscates $P$
[Garg-Gentry-Halevi-Raykova-Sahai-Waters’13,...]

[Jain-Lin-Sahai’20]: Pre-quantum iO from standardish tools

[Bartusek-Guan-Ma-Z’18, Brakerski-Döttling-Garg-Malavolta’20,Wee-Wichs’20]: “Candidate” (post-quantum) iO

[Garg-Gentry-Halevi-Raykova-Sahai-Waters’13,...]: iO → obfuscation for specific programs → applications
Known unobfuscatable programs

All (Classical) Programs

Provably obfuscatable programs
Known unobfuscatable programs

Provably obfuscatable programs

Cryptographic programs
Known unobfuscatable programs

Constructions compile on all (classical) programs, security on non-counter-example programs may be plausible

Provably obfuscatable programs
Watermarking Software?

**Easy Fact:** if program is learnable, cannot watermark

VBB impossibility

∃ Non-learnable and non-watermark-able programs

Positive results for cryptographic functionalities

[Cohen-Holmgren-Nishimaki-Vaikuntanathan-Wichs’15,...]

Traitor tracing \(\approx\) watermarking for decryption functions
For cryptographic functionalities, have a reasonable idea of how to obfuscate/watermark

Constructions plausibly secure for non-crypto functions (except where impossibility applies). Just can’t prove it!
Back to Quantum...
Q: Can we obfuscate Aaronson’s oracle to achieve copy protection?
Issue 1: Obfuscating quantum programs?

Despite some ideas (e.g. [Alagic-Jeffery-Jordan’12]), little progress on obfuscating quantum programs.

Objective 1: Get result using *classical* oracles

Then, maybe can use classical post-quantum obfuscation.
Issue 2: What about VBB impossibility?

[Aaronson’05]: Maybe not an issue?

Need two copies!

Thm [Alagic-Brakerski-Dulek-Schaffner’20]: Still holds 😞

Thm [Ananth-La Placa’20]: Applies to copy protection, too

Objective 2: Use obfuscation techniques to copy protect specific functionalities
Motivating Example: *Public Key Quantum Money*

\[ \text{\$} = \begin{array}{c} \text{\$} \\ \text{\$} \end{array} = \begin{array}{c} \text{\$} \\ \text{\$} \end{array}, \text{ can also be verified by anyone} \]

**Thm [Aaronson’09]:** Publicly verifiable quantum money relative to a quantum oracle

**Thm [Aaronson-Christiano’12]:** Publicly verifiable quantum money relative to a classical oracle

**Thm [Z’19]:** Provably obfuscate \([AC’12]\) oracle using iO
Our Results

[Aaronson- Liu-Liu-Z-Zhang’21]:

**Thm**: Relative to a *classical* oracle, \( \exists \) quantum copy protection \( \forall \) unlearnable programs

[Coladangelo-Liu-Liu-Z’21]:

**Thm (informal)**: Under certain crypto assumptions, \( \exists \) copy protection for particular crypto functions
Probability distribution

\[ \sum_i p_i = 1 \]

Quantum state

\[ \sum_i |w_i|^2 = 1 \]

Denoted \( \sum_i w_i| i \rangle \)

Measurement

\[ p_i \leftarrow |w_i|^2 \]
Copy Protection with Classical Oracles
A Closer Look at [AC’12]

\[ |\psi_S\rangle := \sum_{v \in S} |v\rangle \]

Linear subspace of \( \mathbb{Z}_2^n \)

Verification:

\[ |\phi\rangle \xrightarrow{1_S} \text{QFT} \xrightarrow{1_{S\perp}} \wedge \xrightarrow{\text{acc/rej}} \]
Our Construction

\[ O_1 \xrightarrow{X, v} R(x) \times 1_S(v) \]

\[ O_2 \xrightarrow{X, v} (R(x) \oplus P(x)) \times 1_{S^\perp}(v) \]

Random function

\[ = |\psi_S\rangle \]

Evaluation:

\[ |\phi\rangle \xrightarrow{X} O_1 \xrightarrow{QFT} O_2 \xrightarrow{\oplus} P(x) \]
Copy *Detection* from Quantum Money
Copy Detection/Secure Software Leasing

Still classically impossible

[Ananth-La Placa’20] Impossibility still applies quantumly
Concurrent work [Ananth-La Placa’20]:
Copy Detection for certain *evasive* functions, under certain assumptions
Our work: *public* watermarking $\rightarrow$ copy detection

\[\checkmark + \copyright = \text{serial \#}\]
Copy Protection in the Standard Model
Observation: Copy protection only possible against computationally bounded adversaries
No cloning (with oracles) = Information theoretic

**Challenge:** combine quantum information theory with reductions

Some techniques (e.g. [Brakerski-Christiano-Mahadev-Vazirani-Vidick’18,...,Z’19]) but very limited so far
Our Work: Hidden Coset States

\[ |\psi_{S,x,y}\rangle := \sum_{v \in S+x} (-1)^{y \cdot v} |v\rangle \]

Note: \( \text{QFT} |\psi_{S,x,y}\rangle = |\psi_{S^\perp,y,x}\rangle \)
Hidden Coset Game:

\[ |\psi_{S,x} \rangle \]

\[ x', y' \in S \perp + y \]

Conjecture
Hidden Coset Game, with oracles:

$|\psi_{S,x,y}\rangle \rightarrow 1_{S+x} \quad 1_{S\perp+y}$

$S$ \hspace{1cm} $S$

**Thm:** Under hidden coset assumption, Hidden Coset Game with oracles remains hard, even if oracles iO’d
Applications

Quantum Signature Tokens:
(proposed by [Ben-David,Sattath’16])

\[ \text{Sign}(0) \in S+x \]
\[ \text{Sign}(1) \in S^\perp+y \]

Unclonable decryption:
(proposed by [Gregoriou-Z’20])

decryption key = signing key
ctxt = witness encryption
[Garg-Gentry-Sahai-Waters’13]

Unclonable PRFs

“hidden sparse triggers”
[Sahai-Waters’13]
Future Directions?

Conjecture: Public watermarking → copy protection
Q’s?