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
= 1110111010010001010000110010...
Enter quantum...
Quantum No-Cloning
Quantum Money

[Wiesner’70]
Quantum Copy Protection [Aaronson’09]

Problem: No-cloning theorem gives non-functional states
Theorem [Aaronson’09]: Relative to a quantum oracle, there exists quantum copy protection for all non-learnable classical programs.
Q: Can oracle be implemented in real world?
Detour:
Some other classical DRM objectives...
Software Obfuscation

```c
for(v A((u A((e A((x=270:(V A(U[1])))"C")
}, system("stty raw -echo min 0",fread(1,78114,1,e),B(e),"B")),"A")); 118- (X
"++c++); (y=x/8%&z=(x&199)-4 & S 1 S 1 S 186 S 2 S 2 S 3 S 0,r=(y>5)?2+y,z=(x&
207)-1 S 2 S 6 S S 2 S 182 S 4)?D(0)?D(1)?D(2)?D(3)?D(4)?D(5)?D(6)?D(7)?(2=x-2 C C C
C C C+129 S 6 S 4 S 6 S 8 S S 8 S 2 S 2 S 12)?x/64-1!=(0 0 a(y)=a(x) O 9
[0]=a(5),8[0]=a(4) O 237==*c++?((int (*)())(2-*c+++fwrite;fread))1++k+l[k]=
256,128,1,[fseek(y=5[k]-1?u:v,((3[k]|4[k]<8)<7|2[k]<7,Q=0),y)):0 O y=a(5
),z=a(4),a(5)=a(3),a(4)=a(2),a(3)=y,a(2)=z O c=1+d(5) O y=1[x=d(9)],z=1++x
,x[1]=a(4),l[-x]=a(5),a(5)=y,a(4)=z O 2=c?Z|read(0,&Z,1),1&c+++Z=Z=0:
Q=1?e?)(c++,O=r=V?fgetc(V):-1,s=s-1|r<0) O w++,write(1,&7[o,1]) O z=c2-1,w,
c=] ];system("stty cooked echo"); B((B(V?B(V):0,u)),u));
```
Watermarking
What do we know?
Ad Hoc Obfuscation

Mathematical Obfuscation

Central object in theoretical cryptography
Thm [Barak-Goldreich-Impagliazzo-Rudich-Sahai-Vadhan-Yang’01]:
Some programs cannot be obfuscated
Indistinguishability obfuscation (iO):

\[
1 \equiv 2 \quad \Rightarrow \quad 1 \approx_c 2
\]

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 $\rightarrow$ obfuscation for specific programs $\rightarrow$ applications
Known unobfuscatable programs

Provably obfuscatable programs

All (Classical) Programs
Known unobfuscatable programs

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

Provably obfuscatable programs

Known unobfuscatable 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 ≈ 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*

\[ = \text{atom}, \text{can also be verified by anyone} \]

**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, ∃ quantum copy protection ∀ unlearnable programs

**Thm (informal):** Assuming *public key* quantum money,  
Public watermarking  →  copy *detection*

[Coladangelo-Liu-Liu-Z’21]:

**Thm (informal):** Under certain crypto assumptions,  
∃ 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]

Oracles: \( 1_S \), \( 1_{S\perp} \)

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

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

Verification:

\( |\phi\rangle \rightarrow 1_S \rightarrow \text{QFT} \rightarrow 1_{S\perp} \rightarrow \wedge \rightarrow \text{acc/rej} \)
Our Construction

\[ \psi_S \]

\[ O_1 \quad R(x) \times 1_S(v) \quad O_2 \quad (R(x) \oplus P(x)) \times 1_{S^\perp}(v) \]

Random function

Evaluation:

\[ \phi \]

\[ O_1 \quad \text{QFT} \quad O_2 \quad P(x) \]
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

= 🟢 + 💰 + ⓒ = serial #
Copy Protection in the Standard Model
Observation: Copy protection only possible against computationally bounded adversaries

Security “proof” = Computational Assumption + Reduction
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:

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

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

\[ y' \in S^\perp + y \]

Conjecture
Hidden Coset Game, with oracles:

$$\langle \psi_{S,x,y} \rangle \rightarrow I_{S+x} \quad I_{S \perp +y}$$

**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

[Gregoriou-Z’20]

Unclonable PRFs

“hidden sparse triggers”

[Sahai-Waters’13]
Future Directions?

Conjecture: Public watermarking $\rightarrow$ copy protection
Q’s?