Recent Developments in Quantum Copy Protection

Mark Zhandry (Princeton & NTT Research)

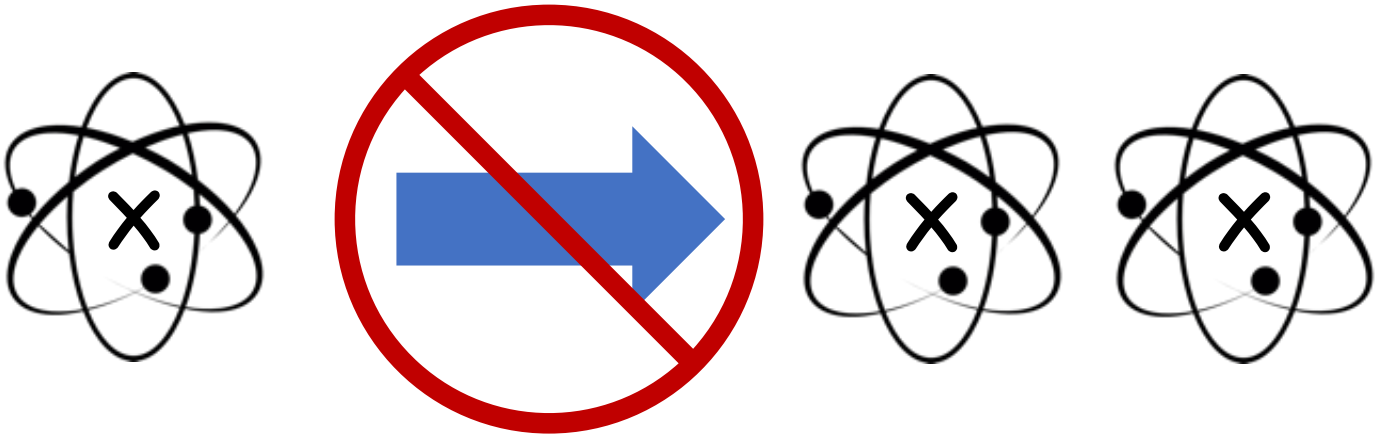
Based on joint works with Scott Aaronson, Andrea Coladangelo,
Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang


Microsoft Office Activation Wizard
Microsoft Office Professional Plus 2016
Activation Wizard
Office
Follow these steps to activate your software over the telephone.
Step 1: Select the country/region you are calling from and call the Product Activation Center using any of the telephone numbers provided.
United Kingdom
Mobile or Toll: (44) (203) 147 4930
Toll-Free: (0) (800) 018 8354
Step 2: When prompted, provide this Installation ID:
4196076 2037705 9336500 3309242 1012711 3669762 4644166 1495676 4262483
Step 3: Enter your Confirmation ID here:
A B C D E F G H
Copy Protection
Privacy Statement
Help
Back
Next
Cancel

= 1110111010010001010000110001101O...

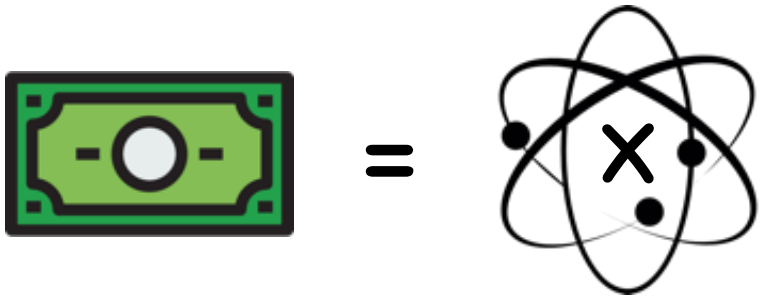
Enter quantum…

Quantum No-Cloning



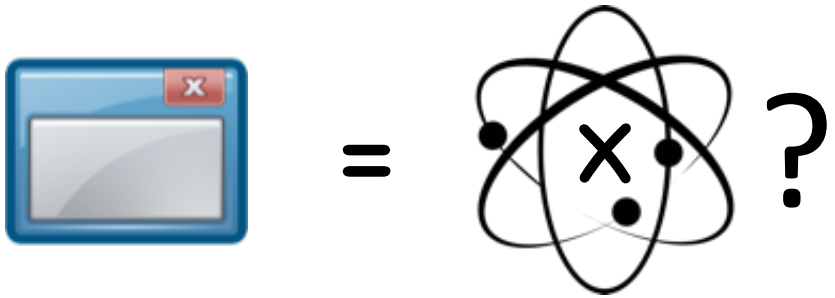
Quantum Money

[Wiesner'70]



Quantum Copy Protection

[Aaronson'09]

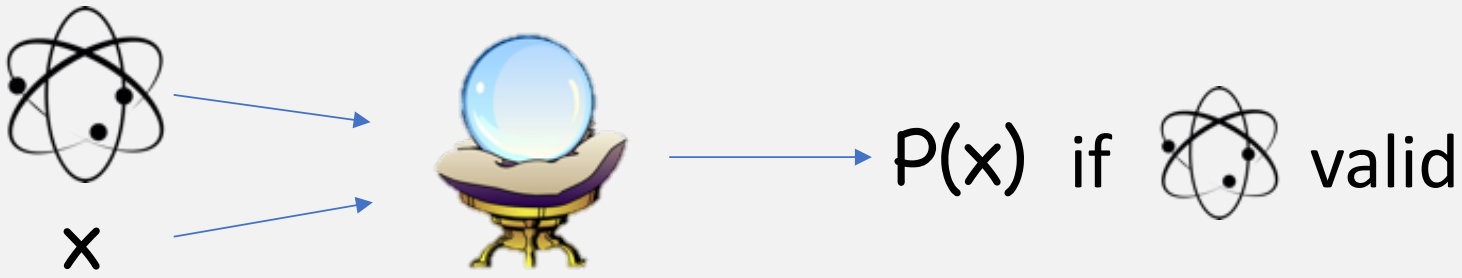


Problem: No-cloning theorem gives non-functional states

Thm [Aaronson'09]: Relative to a quantum oracle, $\exists$ quantum copy protection $\forall$ non-learnable classical programs

Inherent

Idea



Q: Can oracle be implemented in real world?

Detour:
Some other classical DRM objectives…

Software Obfuscation

```
                                    for(v A((u A((e A((r-2?0:(V A(1[U])),"C")
),system("stty raw -echo min 0"),fread(l,78114,1,e),B(e),"B")),"A")); 118-(x
=*c++); (y=x/8%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 2 S 182 S 4)?D(0)D(1)D(2)D(3)D(4)D(5)D(6)D(7)(z=x-2 C C C C
C C C C+129 S 6 S 4 S 6 S 8 S 8 S 6 S 2 S 2 S 12)?x/64-1?((0 O a(y)=a(x) O 9
[o]=a(5),8[o]=a(4) O 237==*c++?((int (*)())(2-*c++?fwrite:fread))(l+*k+1[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=l+d(5) O y=l[x=d(9)],z=l[++x]
,x[l]=a(4),l[--x]=a(5),a(5)=y,a(4)=z O 2-*c?Z||read(0,&Z,1),1&*c++?Q=Z,Z=0:(
Q=!!Z):(c++,Q=r=V?fgetc(V):-1,s=s&~1|r<0) O++c,write(1,&7[o],1) O z=c+2-l,w,
c=l                                                                    x=q]
,a(                                                                    <8)
O l                                                                    /
128,Q=Q*2+s%2,s=s&~1|x O l[d(3)]=Q O s=s&~1|1&Q,Q=Q/2|Q<<7 O Q=l[d(1)]O s=~1
&s|Q>>7,Q=Q*2|Q>>7 O l[d(1)]=Q O m y n(0,-,7)y) O m z=0,y=Q|=x,h(y) O m z=0,
y=Q^=x,h(y) O m z=Q*2|2*x,y=Q&=x,h(y) O m Q n(s%2,-,7)y) O m Q n(0,-,7)y)  O
m Q n(s%2,+,7)y) O m Q n(0,+,7)y) O z=r-8?d(r+1):s|Q<<8,w O p,r-8?o[r+1]=z,r
[o]=z>>8:(s=~40&z|2,Q=z>>8) O r[o]--||--o[r-1]O a(5)=z=a(5)+r[o],a(4)=z=a(4)
+o[r-1]+z/256,s=~1&s|z>>8 O ++o[r+1]||r[o]++O o[r+1]=*c++,r[o]=*c++O z=c-l,w
,c=y*8+l O x=q,b z=c-l,w,c=l+x) O x=q,b c=l+x) O b p,c=l+z) O a(y)=*c++O r=y
,x=0,a(r)n(1,-,y)s<<8) O r=y,x=0,a(r)n(1,+,y)s<<8))));
system("stty cooked echo"); B((B((V?B(V):0,u)),v)); }
```

Watermarking

What do we know?

Ad Hoc Obfuscation

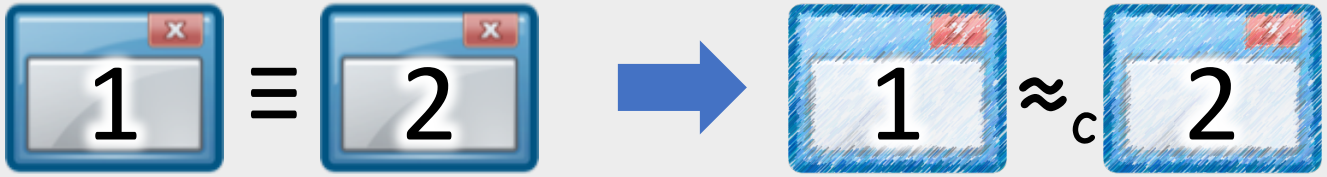
Mathematical Obfuscation

Central object in theoretical cryptography

Thm [Barak-Goldreich-Impagliazzo-Rudich-Sahai-Vadhan-Yang'01]:

Some programs cannot be obfuscated

Indistinguishability obfuscation (iO):



No meaningful obfuscation guarantee on its own

Thm [Goldwasser-Rothblum'07]: If Ƥ *can* be obfuscated, iO obfuscates Ƥ

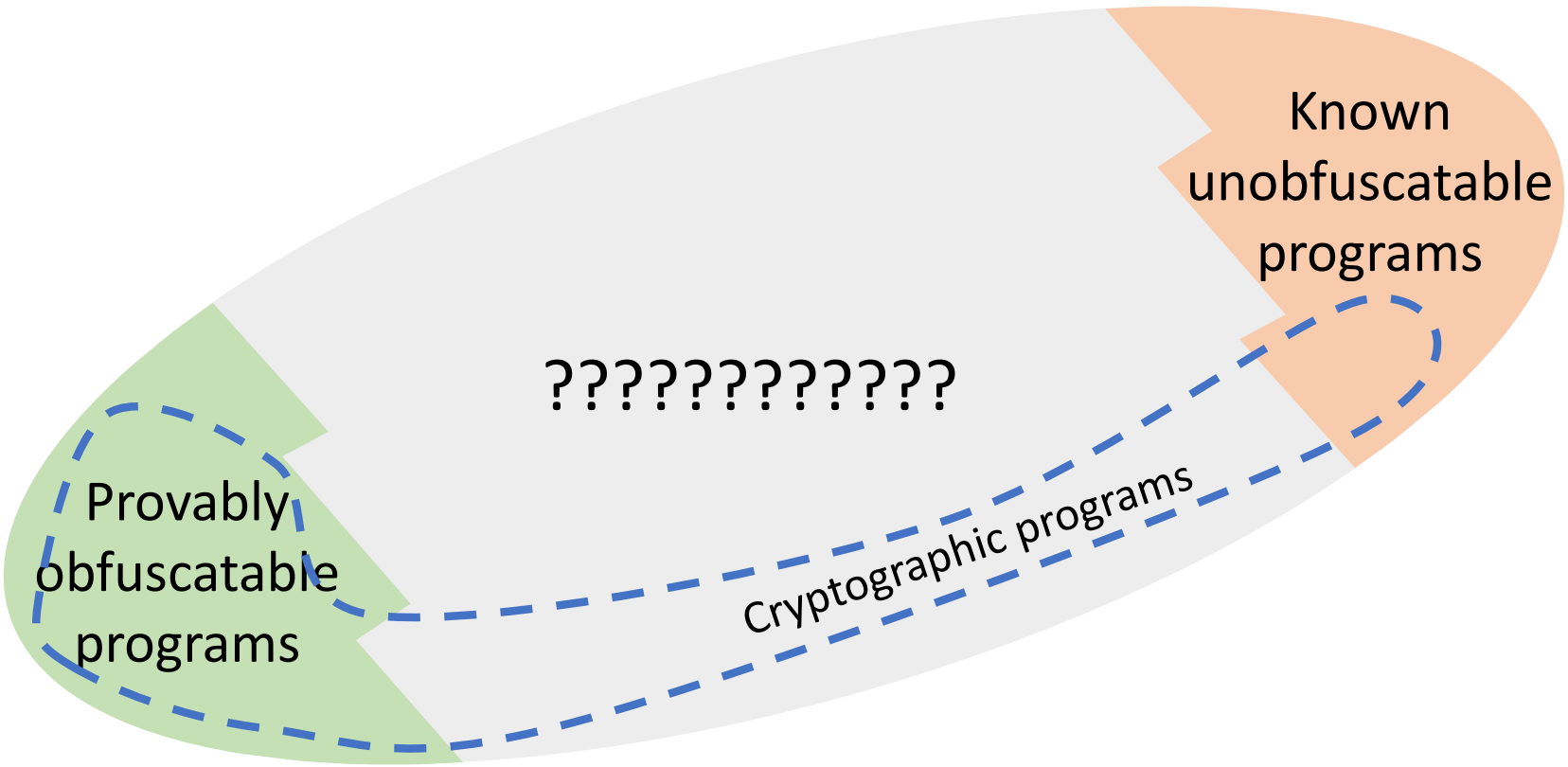
[Garg-Gentry-Halevi-Raykova-Sahai-Waters'13,…]

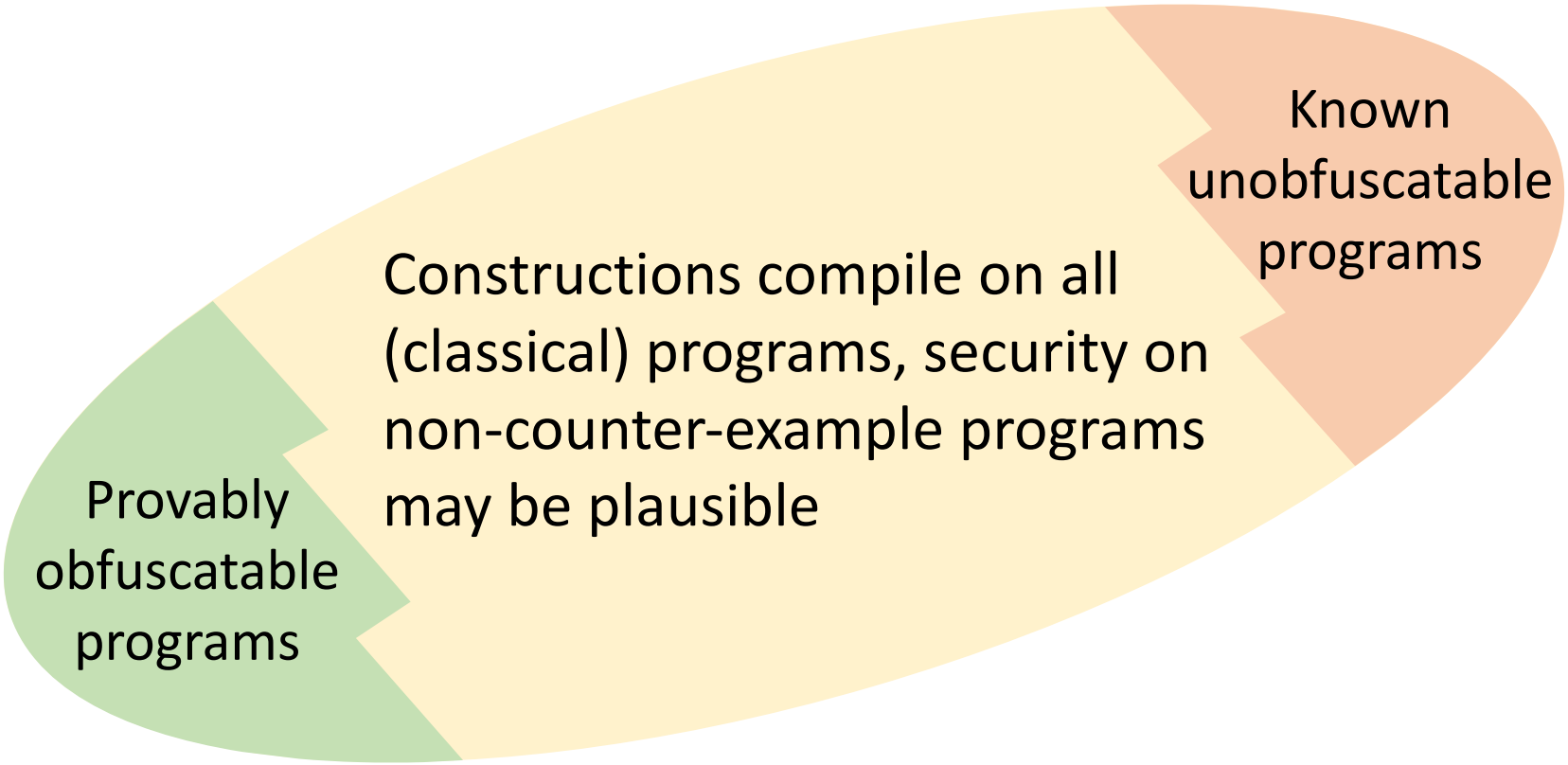
[Jain-Lin-Sahai'20]:
Pre-quantum iO from standardish tools

[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

↓

$\exists$ 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?

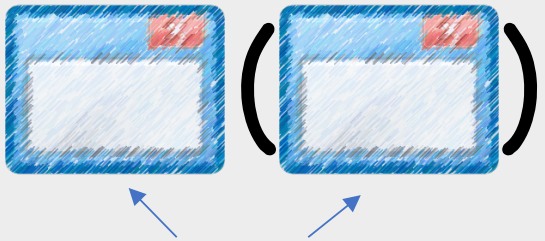
Despite some ideas (e.g. [Alagic-Jeffery-Jordan'12]), little progress on obfuscating quantum programs

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

 =  , 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

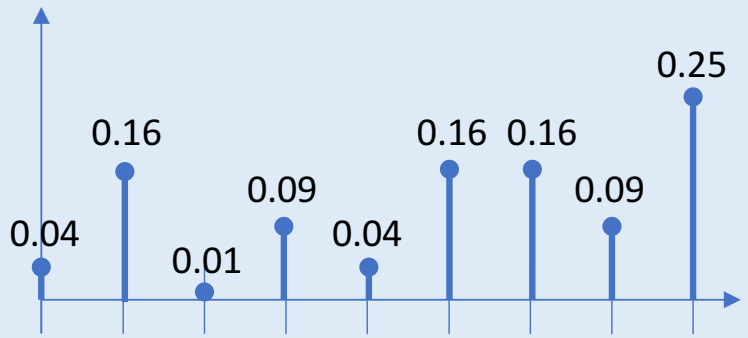
Thm (informal): Assuming *public key* quantum money,

Public watermarking ➡ copy *detection*

[Coladangelo-Liu-Liu-Z'21]:

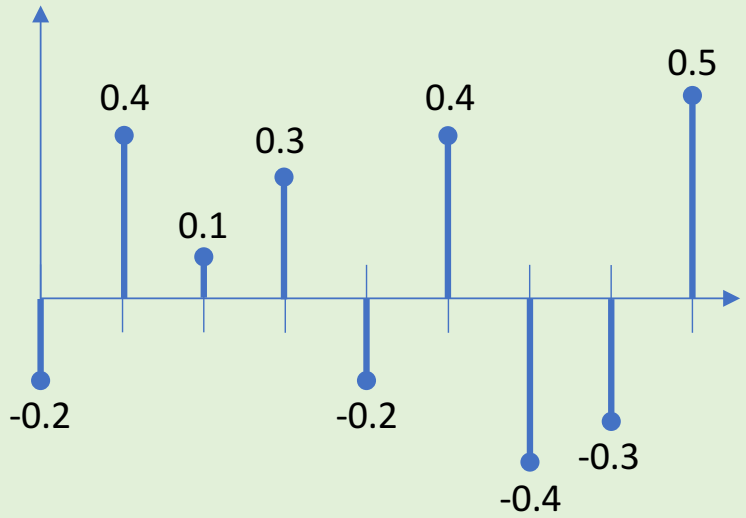
Thm (informal): Under certain crypto assumptions, $\exists$ copy protection for particular crypto functions

Probability distribution



$\Sigma_i p_i = 1$

Quantum state



$\Sigma_i |w_i|^2 = 1$

Measurement

Denoted $\Sigma_i\ w_i|i\rangle$

$p_i \leftarrow |w_i|^2$

Copy Protection with Classical Oracles

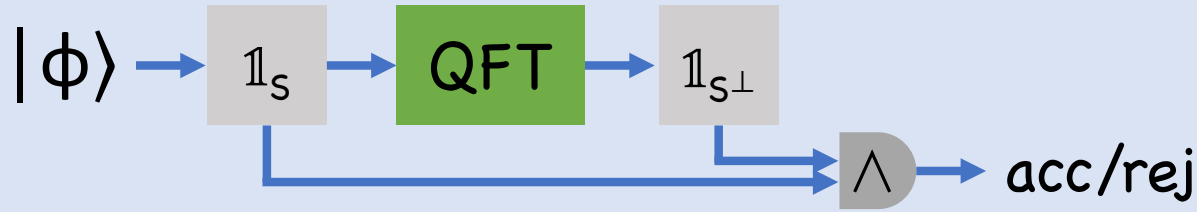
A Closer Look at [AC'12]

Oracles: $\mathbb{1}_S$ $\mathbb{1}_{S^\perp}$

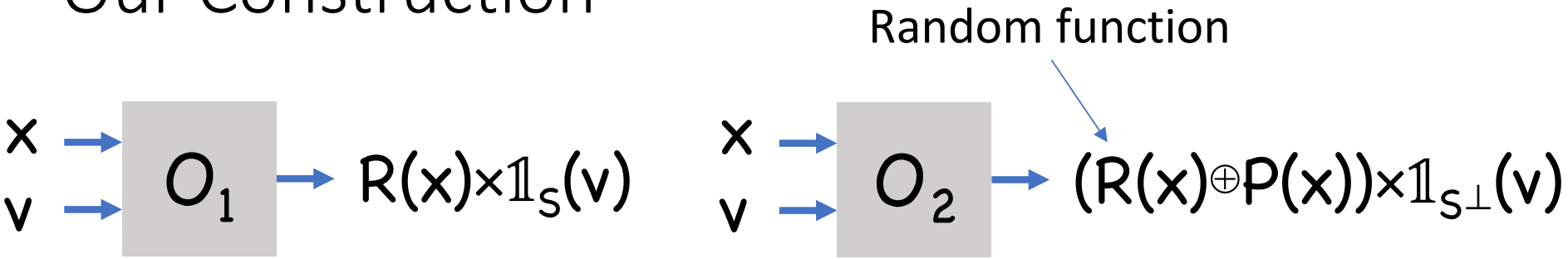
 $= |\psi_S\rangle := \sum_{v \in S} |v\rangle$

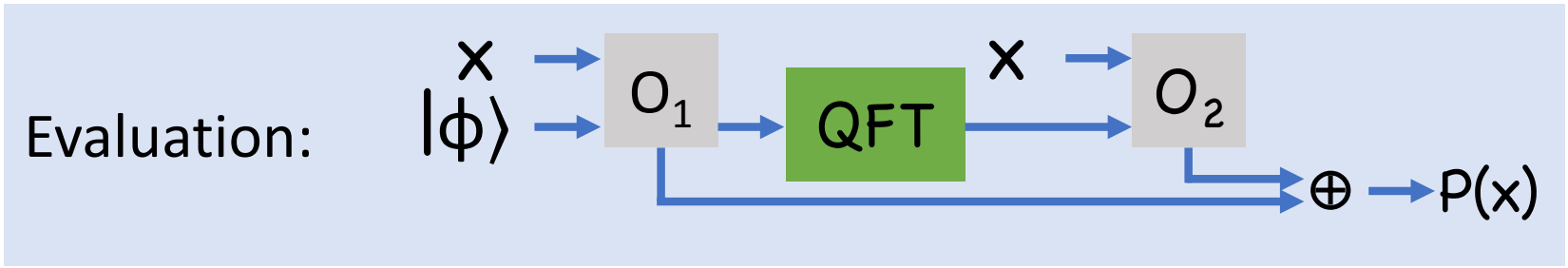
Linear subspace of $\mathbb{Z}_2^n$

Verification:



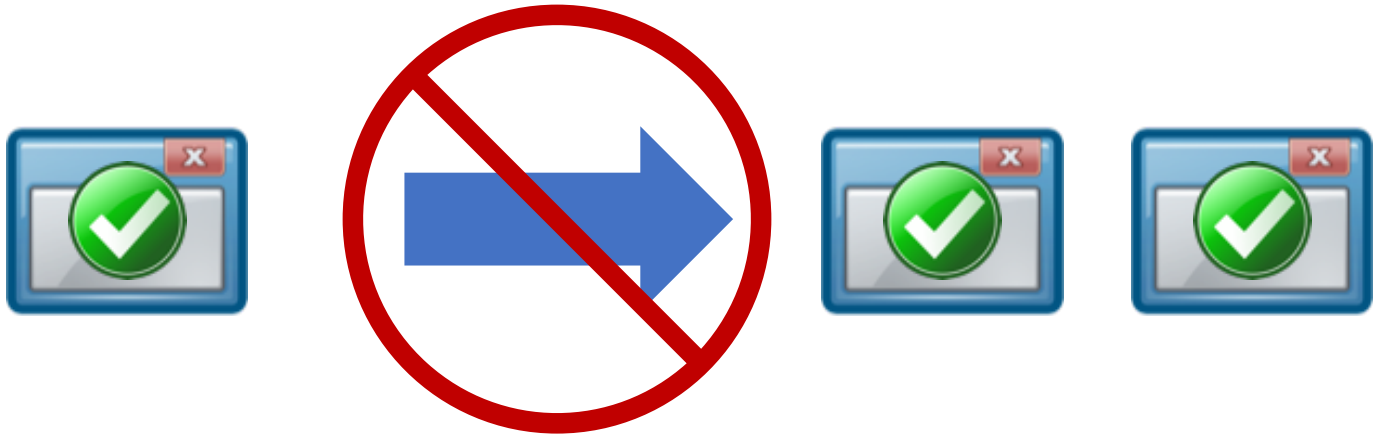
Our Construction





Copy *Detection* from Quantum Money

Copy Detection/Secure Software Leasing

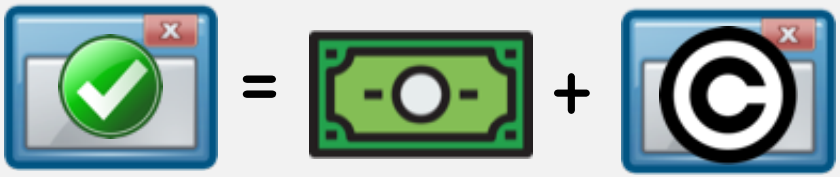


Still classically impossible

[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 ➡ 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

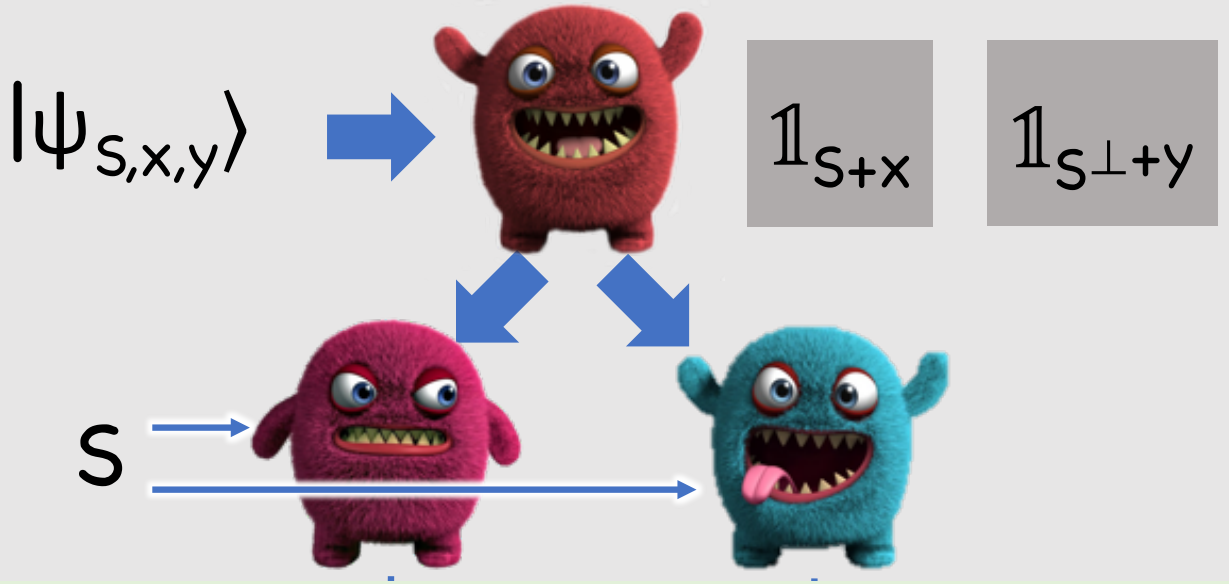
Our Work: Hidden Coset States

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

Note: $QFT|\psi_{S,x,y}\rangle = |\psi_{S^\perp,y,x}\rangle$


Hidden Coset Game:
$|\psi_{S,x}\rangle$
Conjecture
S
$x' \in S+x$
$y' \in S^{\perp}+y$

Hidden Coset Game, with oracles:



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])

$\text{Sign}(0) \in S+x$

$\text{Sign}(1) \in S^{\perp}+y$

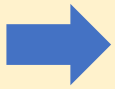
Unclonable decryption:
(proposed by [Gregoriou-Z'20])

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?