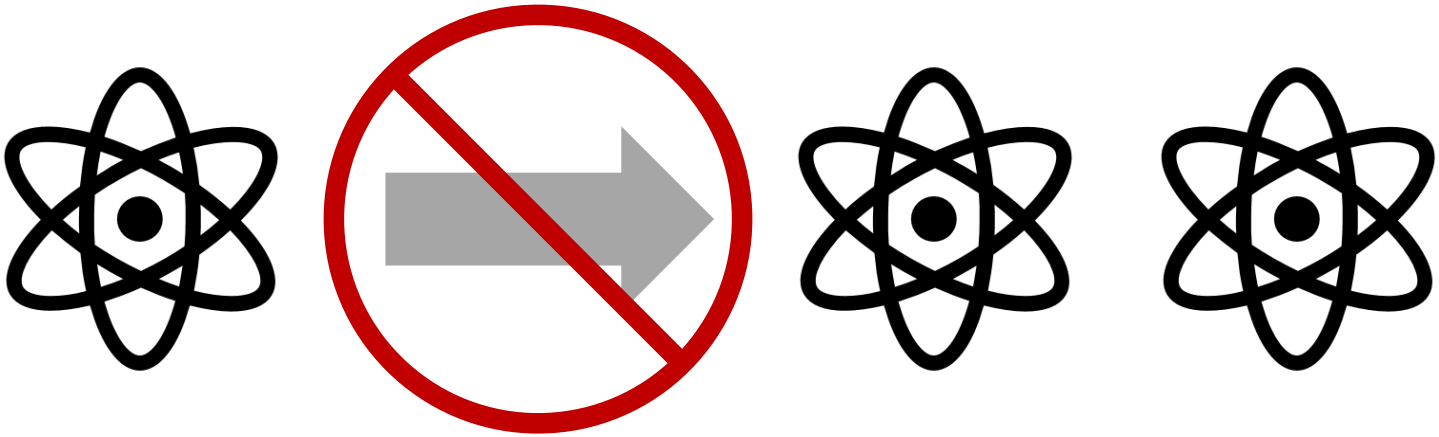
Unclonable Quantum Cryptography

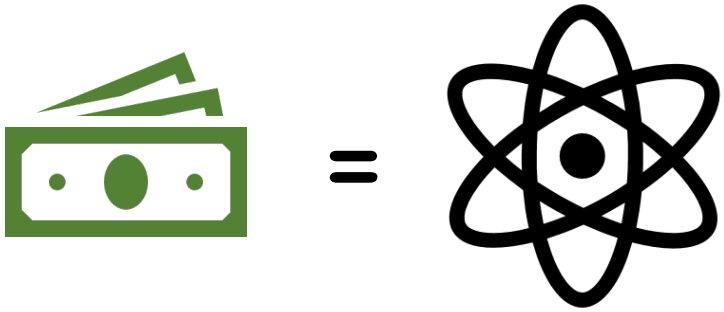
Mark Zhandry (NTT Research & Princeton University)

Quantum No-Cloning



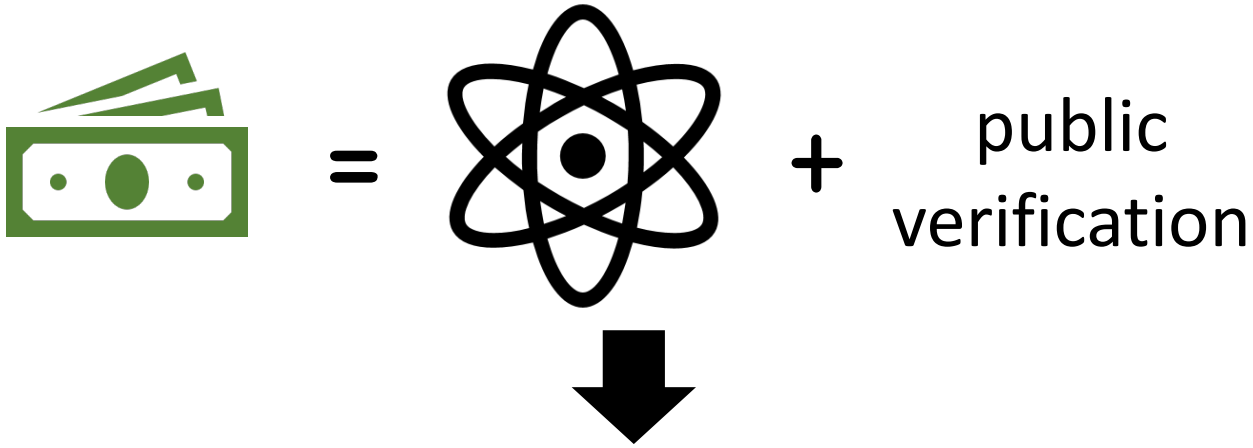
Quantum Money

[Wiesner'70]



Public Key Quantum Money

[Aaronson'09]



Need no-cloning + computational security

This Talk

Survey landscape of computational no-cloning

Other impacts of quantum not discussed

Improved assumptions for crypto
[Bartusek-Coladangelo-Khurana-Ma'21, Grilo-Lin-Song-Vaikuntanathan'21]

Proof challenges
Rewinding: [Graaf'97, Watrous'08, Unruh'12, Chiesa-Ma-Spooner-Z'21]
Random oracle model: [Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Z'11]

Superposition attacks
[Kuwakado-Morii'10, Damgård-Funder-Nielsen-Salvail'11, Z'12]

(Public key) quantum money

Copy protection

Revocable cryptography

Public Key Quantum Money

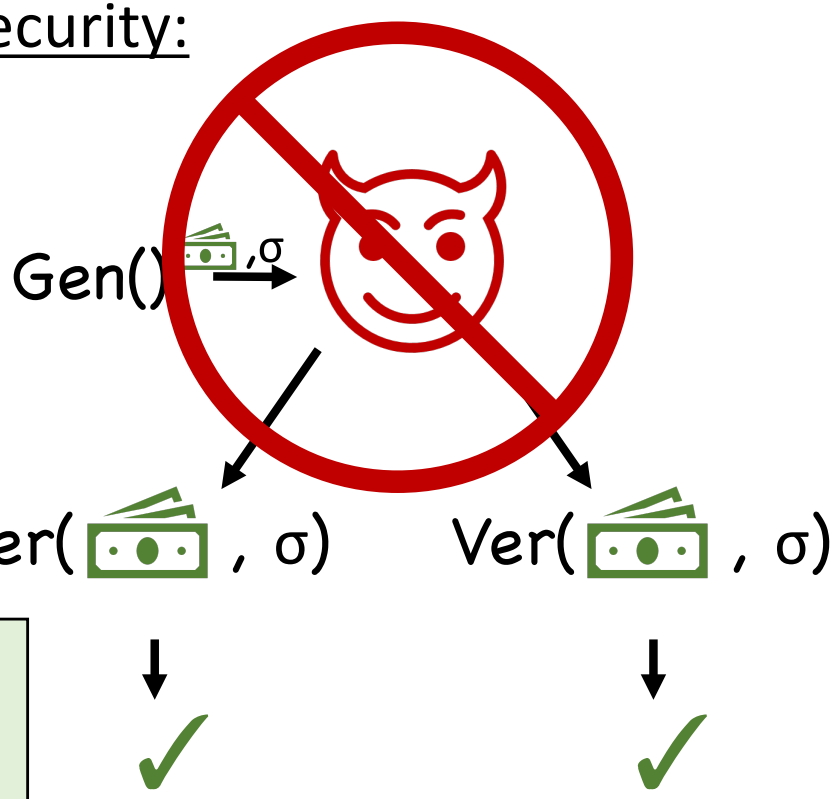
Our Focus: "Mini-schemes"

Syntax/correctness:

Gen() →  , σ

Ver( , σ) → ✓

Security:

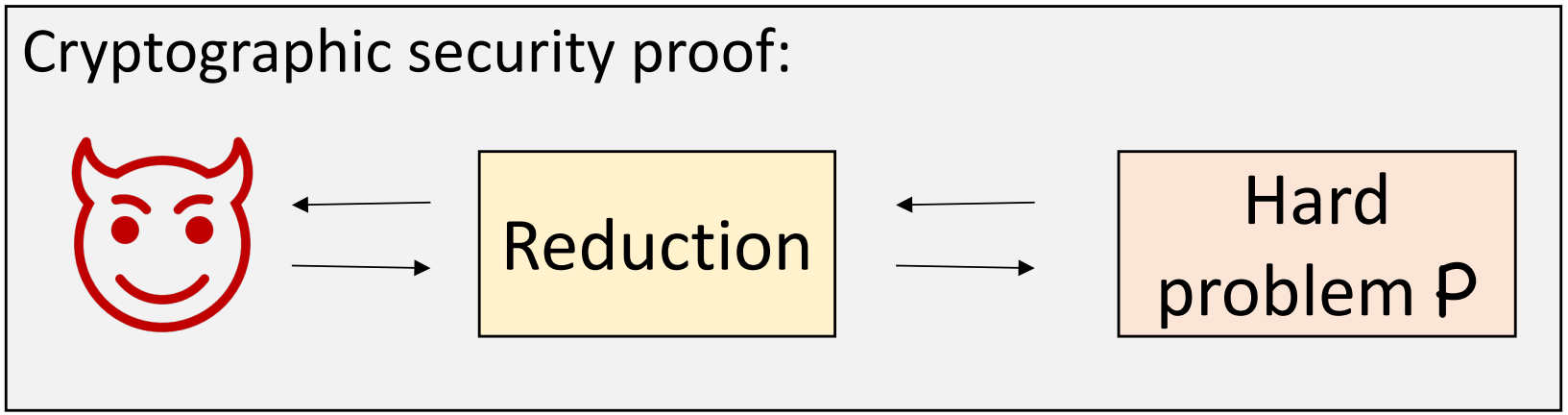


Thm [Aaronson-Christiano'12]:
Mini-scheme + Signatures = Full scheme

Most schemes = candidates

[Aaronson'09]: random stabilizer states	✘	[Lutomirski-Aaronson-Farhi-Gosset-Hassidim-Kelner-Shor'10]
[Farhi-Gosset-Hassidim-Lutomirski-Shor'10]: knots	?	little published cryptanalysis effort
[Aaronson-Christiano'12]: polynomials hiding subspaces	✘	[Pena-Faugère-Perret'14, Christiano-Sattath'16]
[Kane'18]: Modular forms	?	[Bilyk-Doliskani-Gong'22] analysis
[Z'19]: quadradic systems of equations	✘	[Roberts'21]
[Kane-Sharif-Silverberg'21]: Quaternion Algebras	?	No published cryptanalysis effort

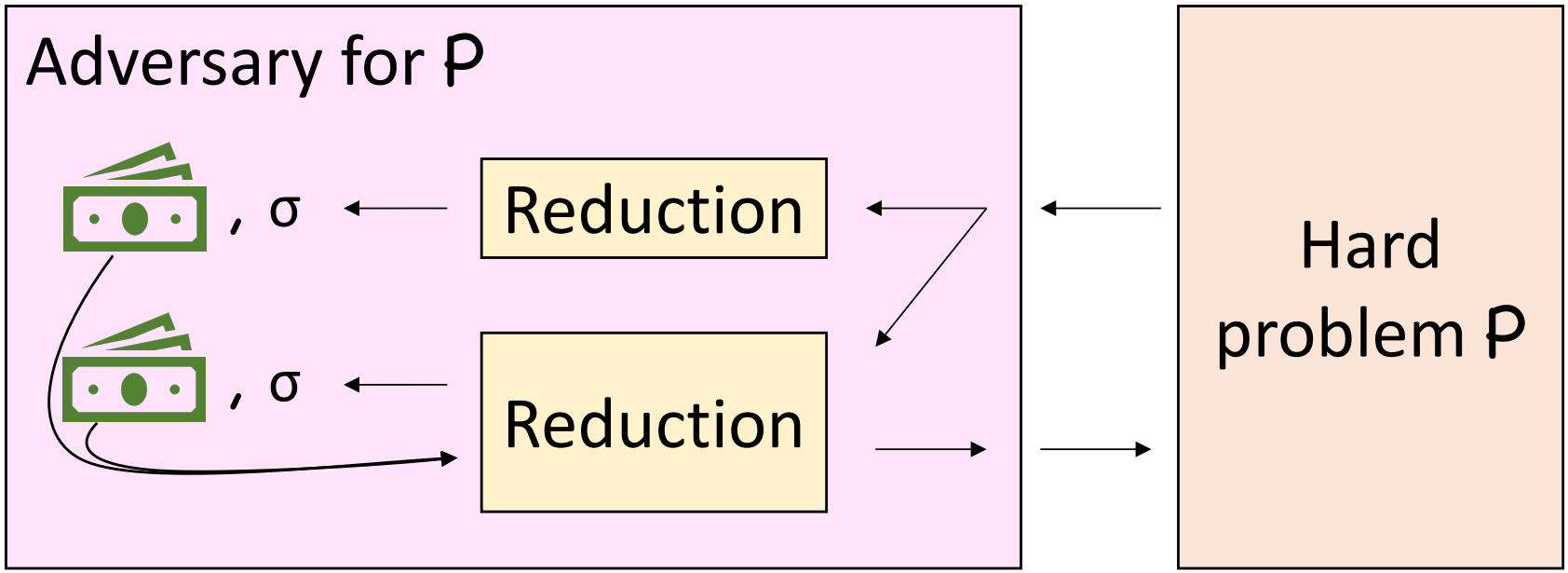
Central Challenge 1:



Ꝑ should be widely believed, studied, easy to think about, etc

Ꝑ should be **classical** problem with post-quantum hardness

Central Challenge 1:



Central Challenge 2:

No-cloning comes from information-theory

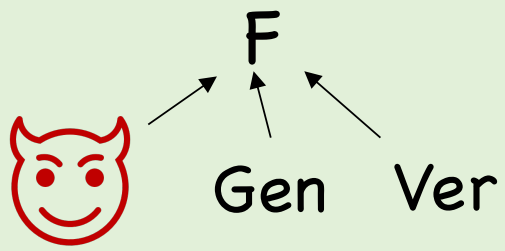
But  is information-theoretically clonable

How to combine?

Three known strategies to justify security

Oracles

[Aaronson'09, Aaronson-Christiano'12]



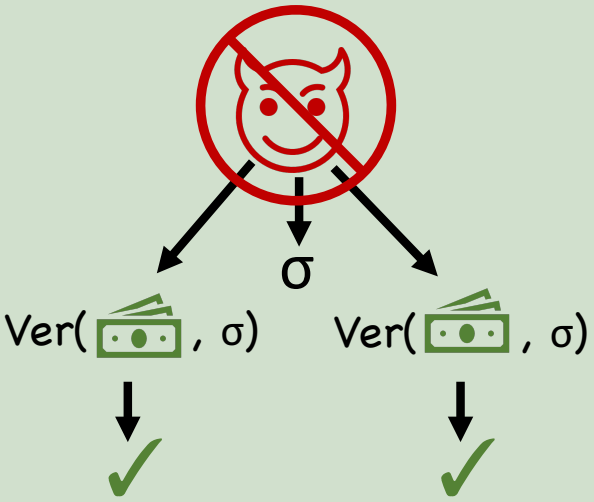
Pro: Unconditional security!

Cons:

- How to implement F?
- Justify implementation "as good as" black box?

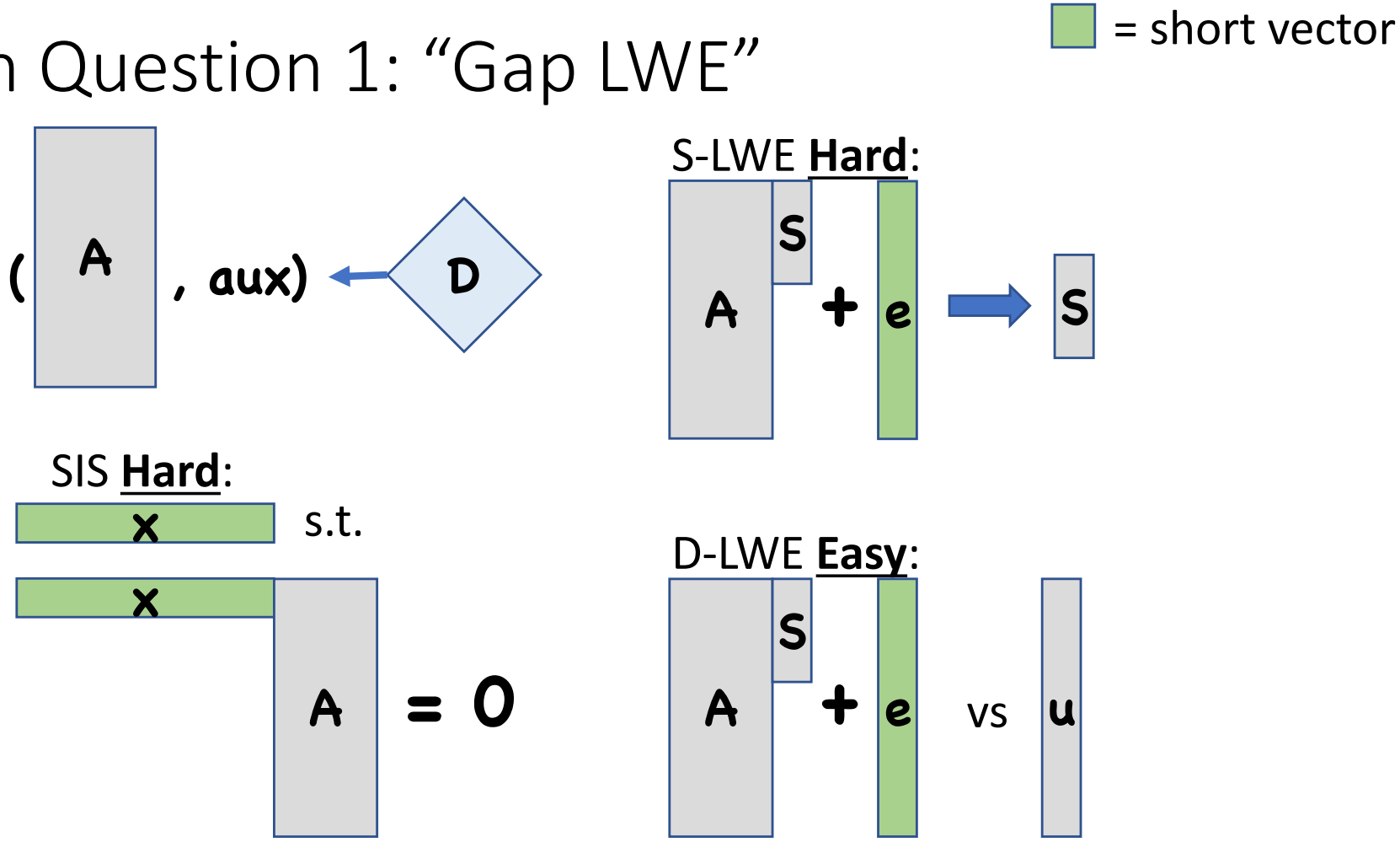
Quantum lightning

[Lutomirski-Aaronson-Farhi-Gosset-Hassidim-Kelner-Shor'10, Z'19]



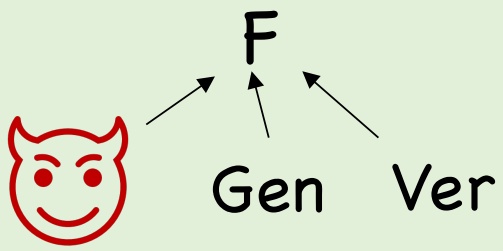
No known provably secure instantiation w/o oracles

Open Question 1: “Gap LWE”



Three known strategies to justify security

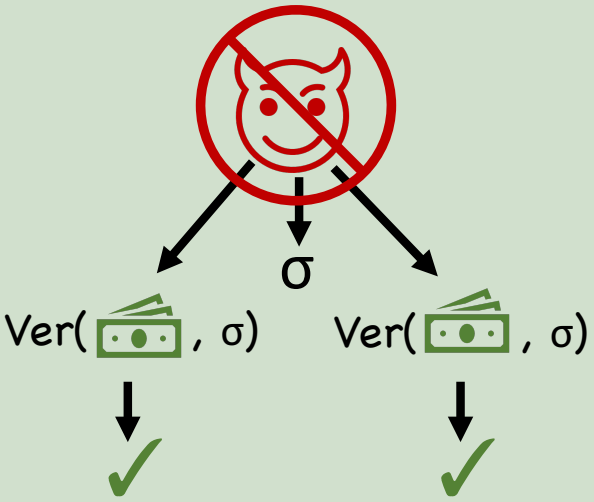
Oracles
[Aaronson'09, Aaronson-Christiano'12]



Pro: Unconditional security!

Cons:
- How to implement F?
- Justify implementation "as good as" black box?

Quantum lightning
[Lutomirski-Aaronson-Farhi-Gosset-Hassidim-Kelner-Shor'10, Z'19]



No known provably secure instantiation w/o oracles

Switch to information-theoretic unclonability
[Z'19]

Real world $\approx_c$ Fake world

Cloning information-theoretically impossible

Only one known instance, using very powerful tools

Aaronson-Christiano'12 Scheme

Linear subspace

$$= |A\rangle := \sum_{x \in A} |x\rangle \qquad \sigma = (A, A^{\perp})$$

Ver:

→ QFT → $|A^{\perp}\rangle$ → QFT^{-1} →

$\in A?$ $\in A^{\perp}?$

Aaronson-Christiano'12 Scheme

Linear subspace

Hope: somehow hides A

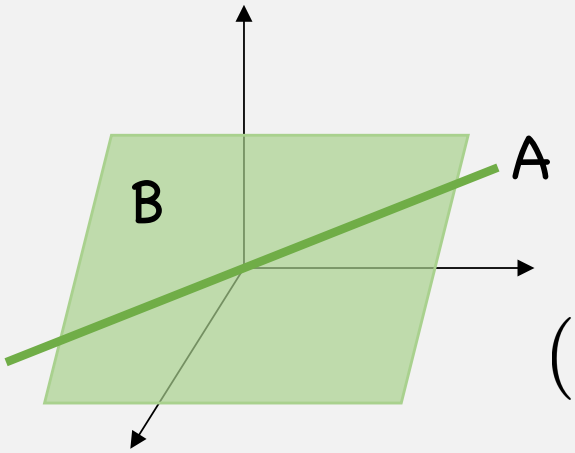
 $= |A\rangle := \sum_{x \in A} |x\rangle$ $\sigma = (\ \mathrm{Obf}(A)\ ,\ \mathrm{Obf}(A^{\perp})\ )$

Ver:  → QFT → $|A^{\perp}\rangle$ → QFT^{-1} → 

$\in A?$ $\in A^{\perp}?$

Thm [AC'12]: Secure in black box model

Def [Z'19]: Subspace hiding obfuscation (shO):



B = random subspace of $\mathbb{F}^n$

A = random subspace of B

$$(A,\ \mathrm{Obf}(A)\ ) \approx_c (A,\ \mathrm{Obf}(B)\ )$$

Thm [Z'19]: Subspace hiding → Secure quantum money

Proof: $(\ \mathrm{Obf}(A)\ ,\ \mathrm{Obf}(A^{\perp})\ ) \to (\ \mathrm{Obf}(S)\ ,\ \mathrm{Obf}(T)\ ) \quad S \supseteq A, T \supseteq A^{\perp}$

Verification of adversary's state still wrt A,$\mathsf{A}^{\perp}$

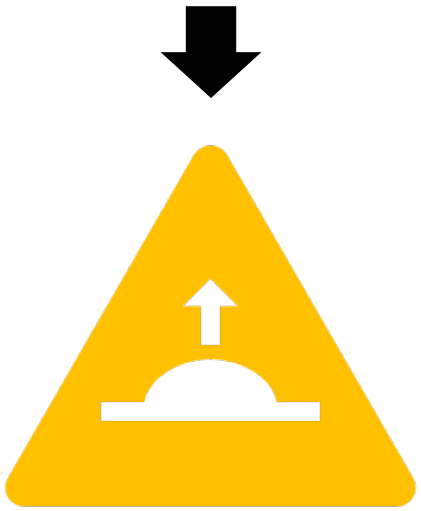
→ Now information-theoretic no-cloning

Open Question 2: Post-quantum ShO from standard assumptions

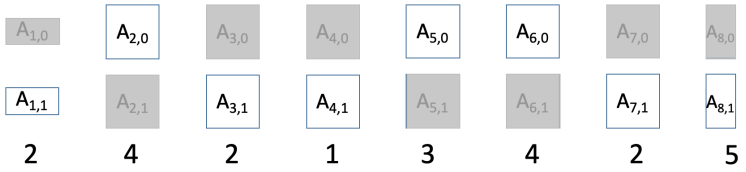
Detour: The Obfuscation Landscape

Ad Hoc 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+l[k]*
256,128,1,(fseek(y=5[k]-17u: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),l&*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+q O p,c=l+z O c=l+q O s^=1 O Q=q[l] O s|=1 O q[l]=Q O Q=~Q O a(5)=l[x=q]
,a(4)=l[++x] O s|=s&16|9<Q%16?Q+=6,16:0,z=s|=1&s|Q>159?Q+=96,1:0,y=Q,h(s<<8)
O l[x=q]=a(5),l[++x]=a(4) O x=Q%2,Q=Q/2+s%2*128,s=s&~1|x O Q=l[d(3)]O x=Q  /
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-1,w
,c=y*8+l O x=q,b z=c-1,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)); }
```



Mathematical Obfuscation

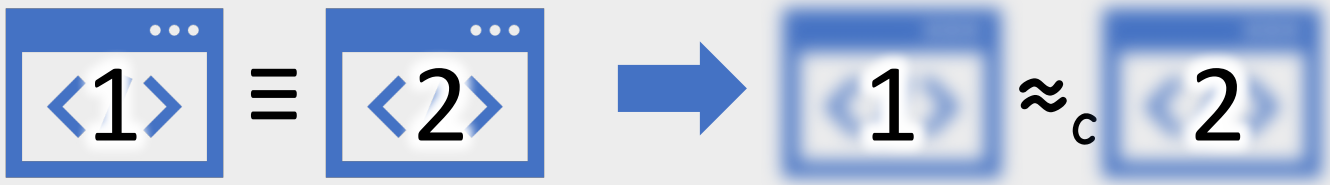


Central object in theoretical cryptography

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,…]

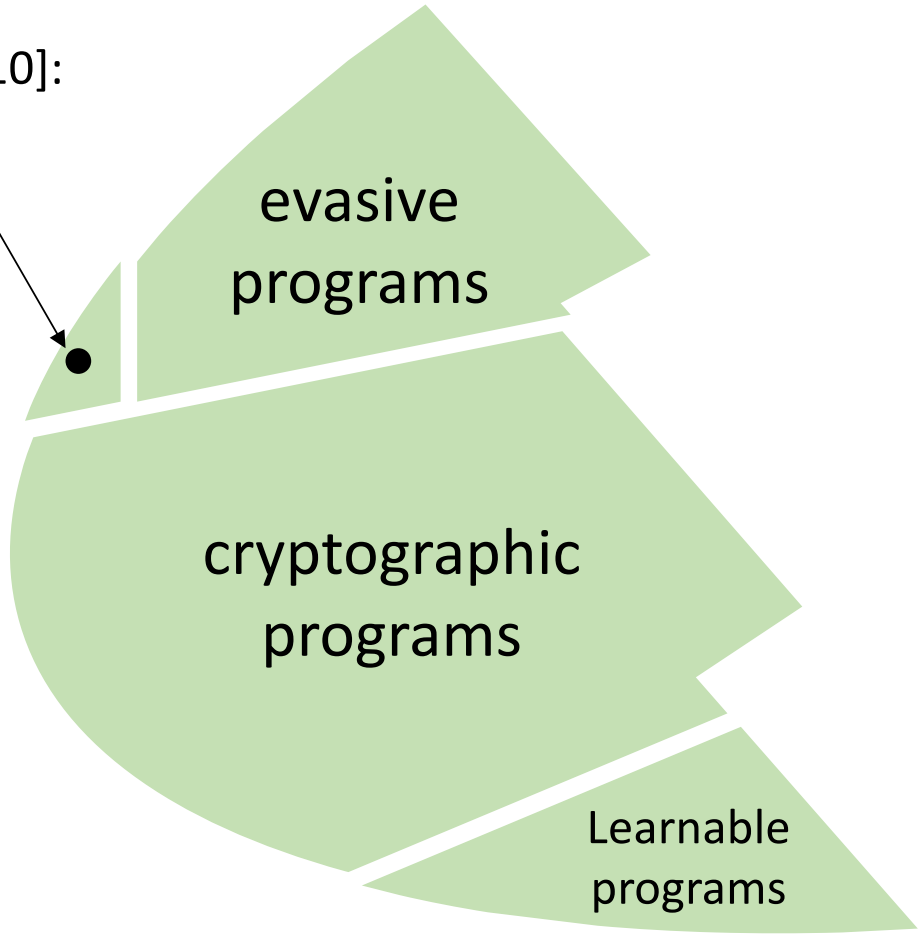
[Jain-Lin-Sahai'20]:
Pre-quantum iO from standardish tools

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

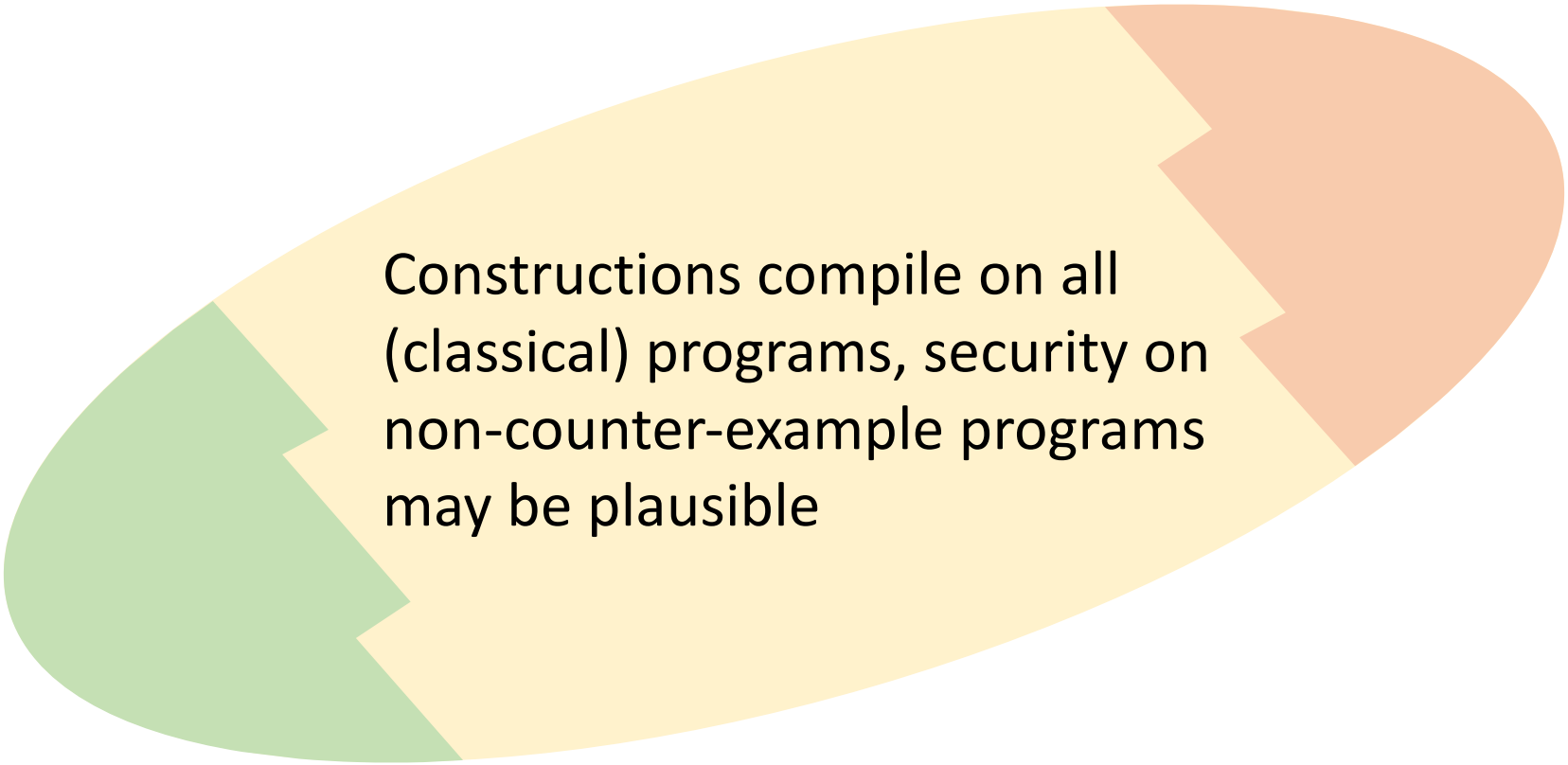
[Garg-Gentry-Halevi-Raykova-Sahai-Waters'13,…]:
iO ➡ obfuscation for specific programs ➡ applications


Known unobfuscatable programs
All (Classical) Programs
Provably obfuscatable programs

[Canetti-Rothblum-Varia'10]:
Groups → ShO
[Z'19]: iO → shO



Open Question 3: Find More Non-evasive, non-cryptographic programs that can be obfuscated


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

Main takeaways regarding iO:

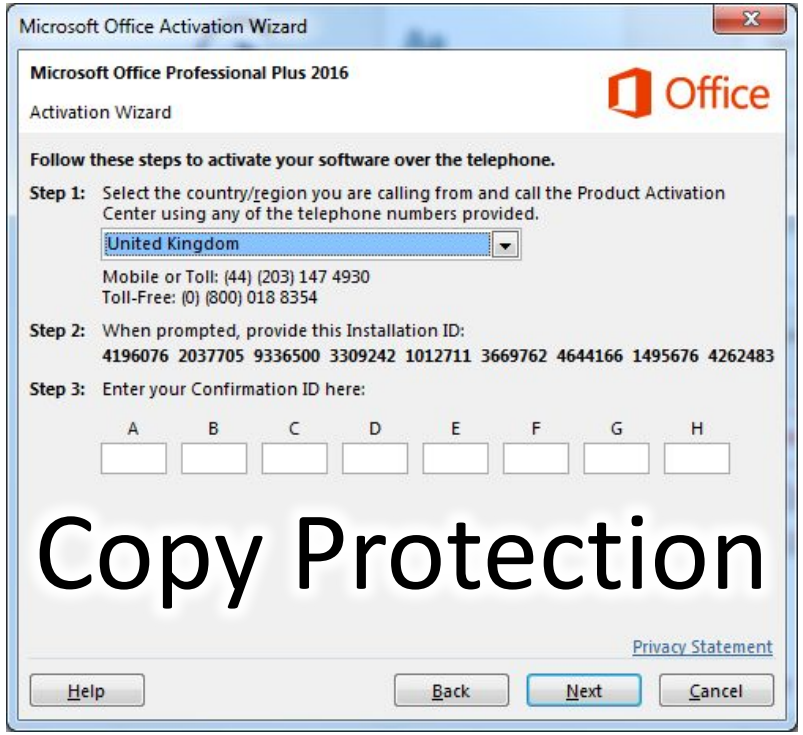
- Somewhat compelling pre-quantum iO
- Good candidates for post-quantum iO, but uncertain
- Good understanding about guarantees of iO for some cryptographic or evasive programs
- Minimal understanding for non-crypto/evasive programs

Back to Quantum…

(Public key) quantum money ✓

Copy protection

Revocable cryptography


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

= 1110111010010001010000110001101 0...

A classical possibility: Watermarking Software

Note: impossible for learnable functions, frequently also for evasive functions

Positive results for cryptographic functionalities

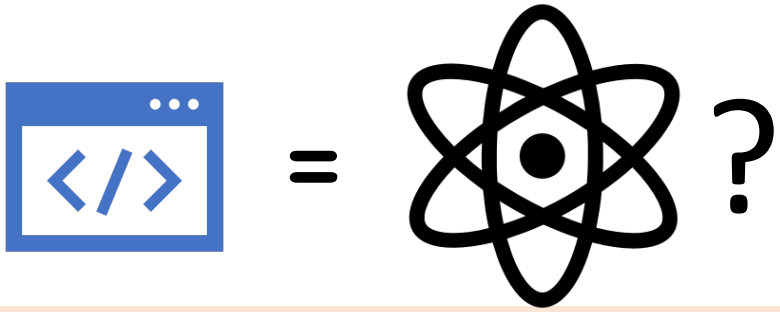
[Cohen-Holmgren-Nishimaki-Vaikuntanathan-Wichs'15,…]

Traitor tracing ≈ watermarking for decryption functions

Quantum Copy Protection

[Aaronson'09]

Note: impossible for learnable functions



Problem: often implies quantum money

Problem: implies obfuscation

Problem: how to combine?

What's known?

Thm [Aaronson'09]: Exists relative to **quantum** oracle

Thm [Aaronson-Liu-Liu-Z-Zhang'20]: Exists relative to **classical** oracle

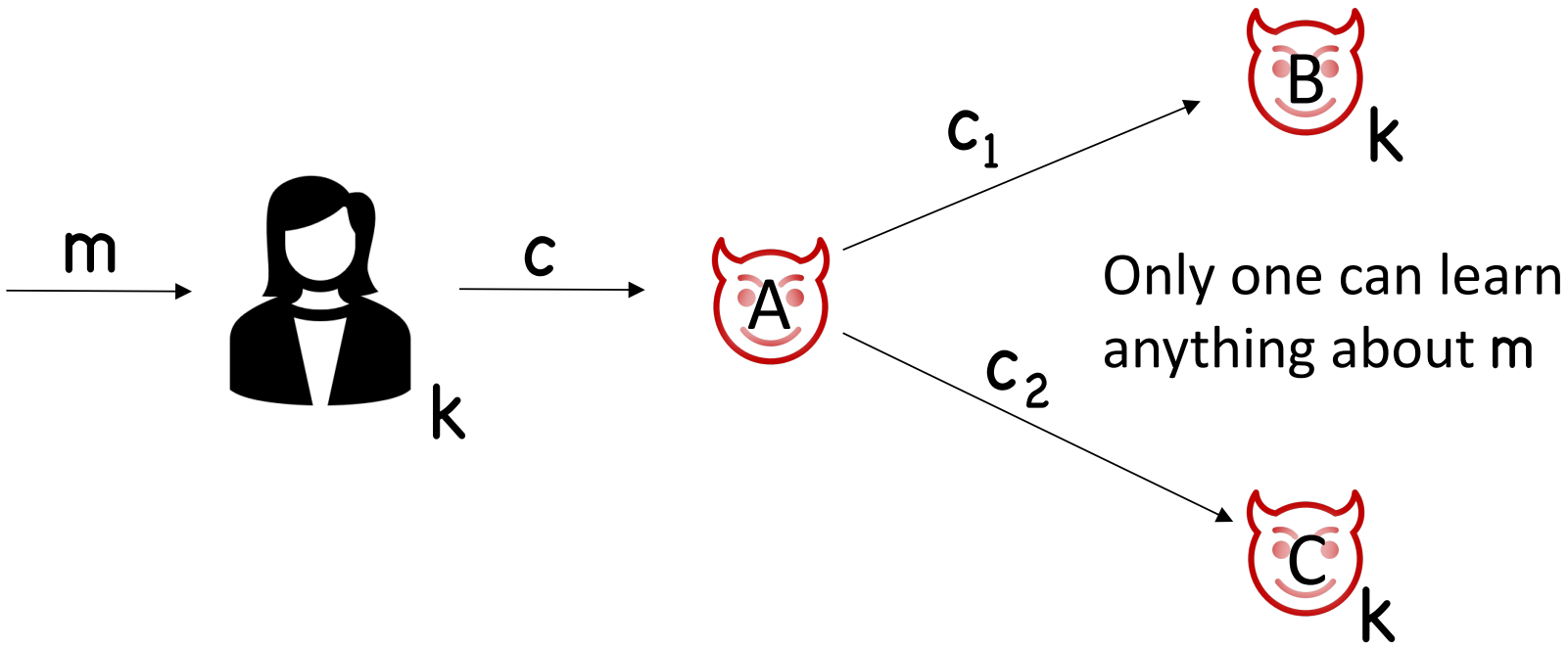
Thm [Ananth-La Placa'20]: Impossible for some non-learnable functions

Thm [Coladangelo-Majenz-Poremba'20]: Random oracles → CP for some evasive functions with *some* security

Thm [Coladangelo-Liu-Liu-Z'21, Culf-Vidick'21]: iO → CP for PRFs, decryption, signature tokens

Special Case: Unclonable Encryption

[Gottesman'03, Broadbent-Lord'19]



Observation: 1-time, symmetric key ≈ CP for point functions

$$c = CP(\ x \rightarrow \text{if}(x==k)\ \text{output}\ m\ )$$

Thm [Broadbent-Lord'19]:

- Statistical **weak "unpredictability"** security in the one-time, symmetric key setting
- Improved, but still weak, security using random oracles

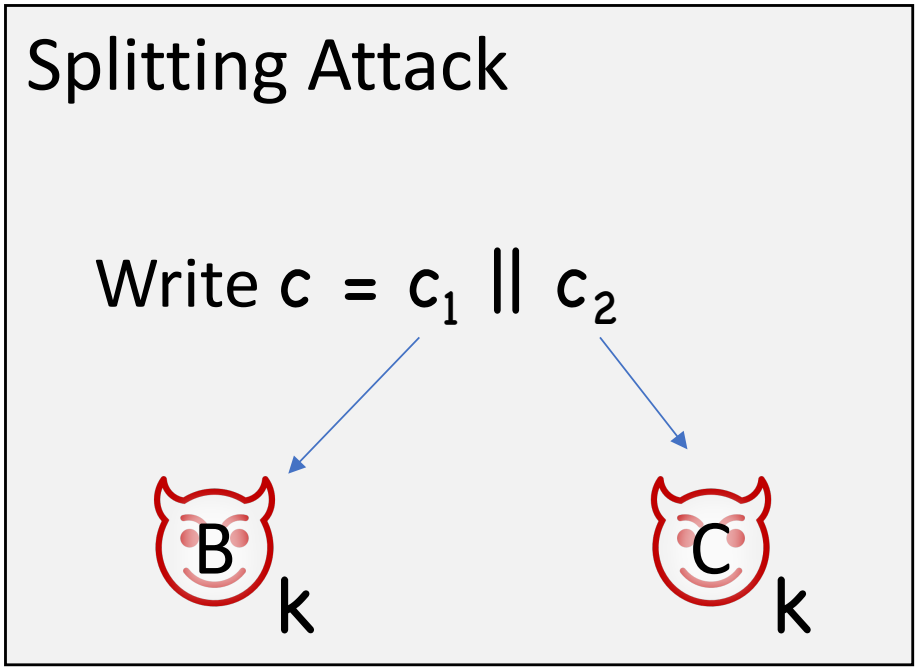
Conjugate Coding

[Weisner'70]

$$k = (k_1, k_2) \in \{0,1\}^{2n}$$

$$c = \mathsf{H}^{k_2}\mathsf{NOT}^{k_1}|m\rangle$$

Thm [Broadbent-Lord'19]: No split adversaries can simultaneously predict random m with probability > 0.85356^n



Easy for each adversary to learn different parts of message

1-Bit Attack

Guess k'_2

Measure $H^{k'_2}|c\rangle = H^{k_2 \oplus k'_2} NOT^{k_1} |m\rangle \mapsto d$

Send (d, k'_2) to both B,C

For each i, let $m_i := \begin{cases} d_i \oplus (k_1)_i & \text{if } (k_2 \oplus k'_2)_i = 0 \\ \perp & \text{otherwise} \end{cases}$

For each i, both parties learn m_i unambiguously with probability ½

Different attack can learn each m_i ambiguously with prob 0.85355

Idea [Broadbent-Lord'19]: Extract with random oracle

$$x \leftarrow \{0,1\}^{\ell}$$

$$c = (\mathsf{H}^{k_2}\mathsf{NOT}^{k_1}|x\rangle, O(x) \oplus m)$$

Thm [Broadbent-Lord'19]: Better security

Thm [Majenz-Schaffner-Tahmasbi'21]: cannot be proven optimally secure under usual techniques

Thm [Ananth-Kaleoglu-Li-Liu-Z'22]: no statistical security for deterministic (unitary) schemes

Contrast with ordinary encryption, where statistical deterministic encryption is trivial

Thm [Ananth-Kaleoglu-Li-Liu-Z'22]: RO + random coins → secure scheme

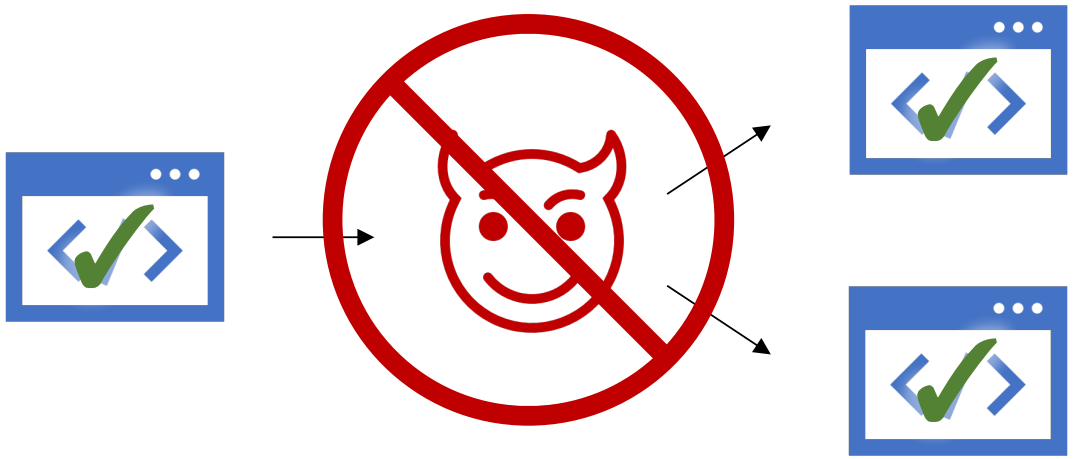
$$k = A$$

$$c = (|A_{s,s'}\rangle, H(s,s') \oplus m), s, s' \leftarrow \$$$

$$|A_{s,s'}\rangle = \sum_{x \in A} \omega^{x \cdot s'} |x + s\rangle$$

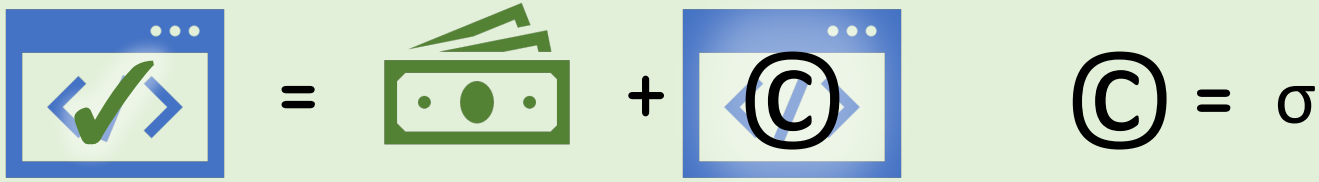
Open Question 4: Unclonable encryption/ CP for point functions without oracles

Relaxation: Copy detection



Adversary may copy, but copies will be detectable

Thm [Aaronson-Liu-Liu-Z-Zhang'20]: quantum money + classical public watermarking → copy detection for same programs



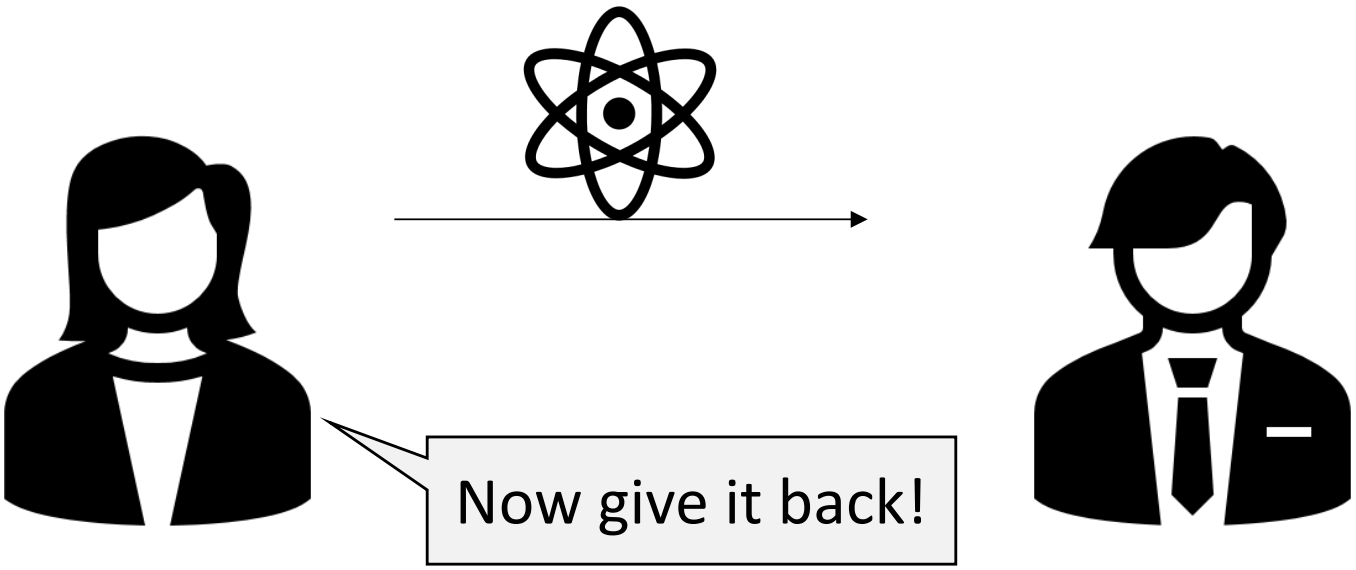
Thm [Ananth-La Placa'20]: quantum money + other tools
→ copy detection for certain evasive functions

(Public key) quantum money ✓

Copy protection ✓

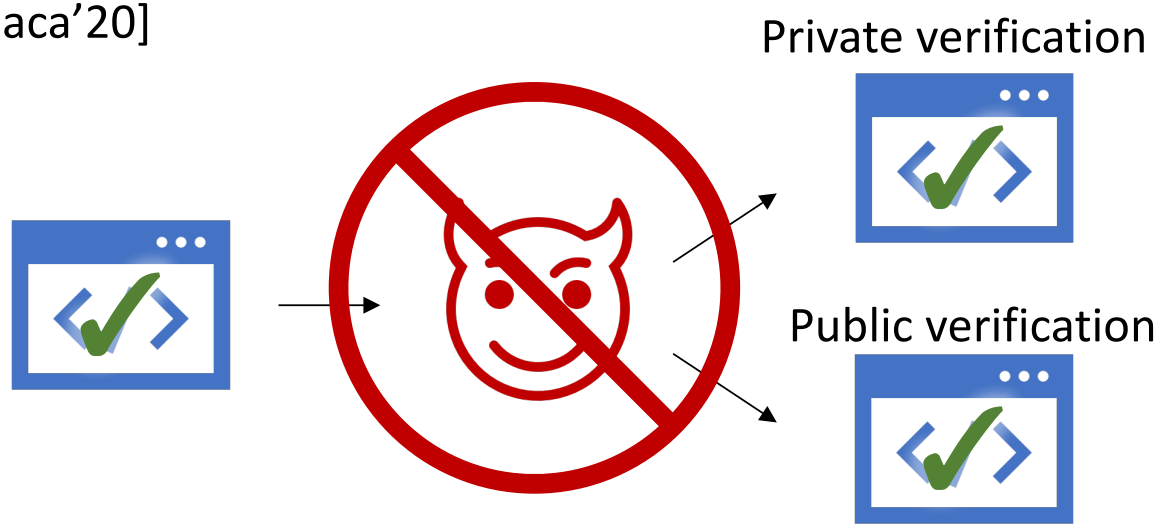
Revocable cryptography

Revocable Cryptography



Secure Software Leasing

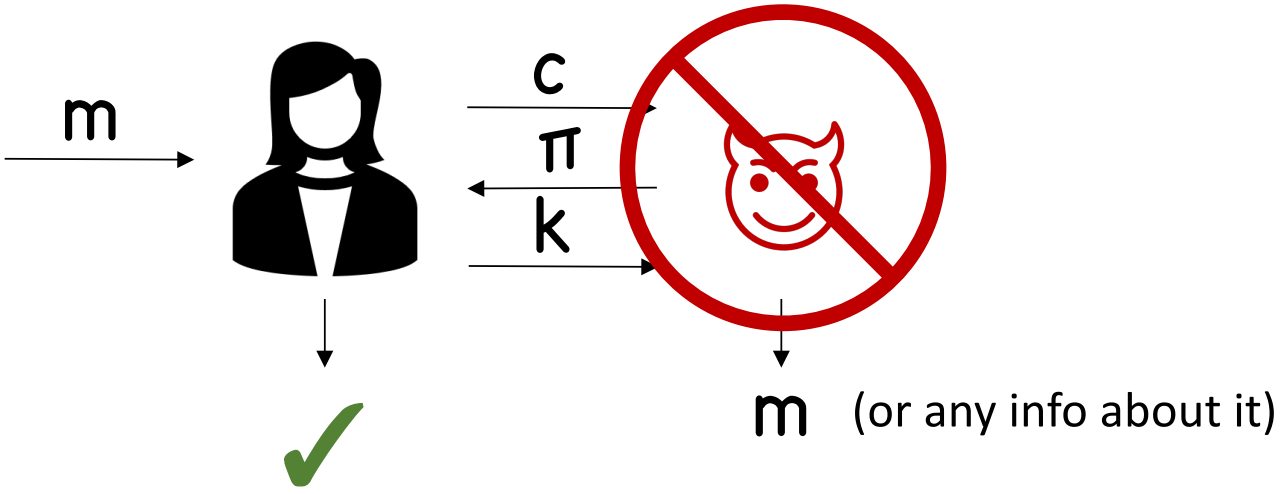
[Ananth-La Placa'20]



Thm [Ananth-La Placa'20]: Standard tools → SSL for certain evasive functions

Encryption with Certified Deletion

[Broadbent-Islam'19]



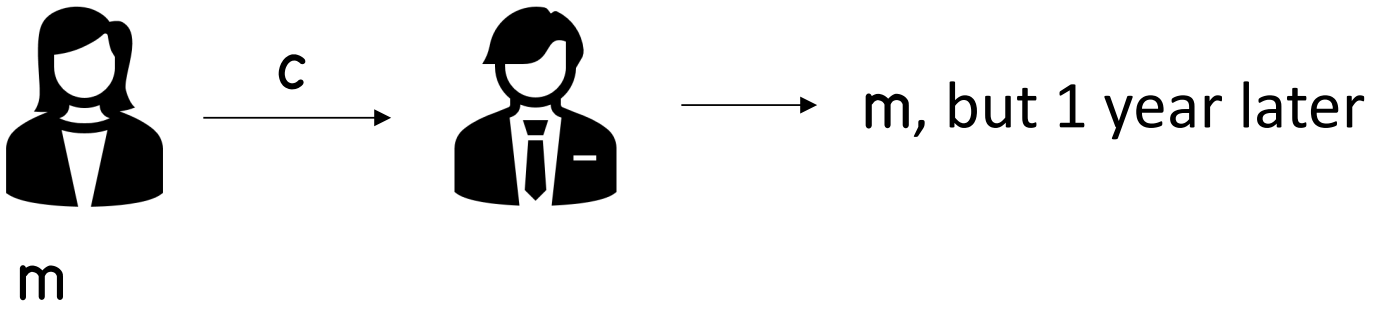
Not hard observation: Unclonable Enc can be used to construct Enc w/ Certified Deletion

Thm [Broadbent-Islam'19]: Statistical, one-time, secret key

Thm [Hiroka-Morimae-Nishimaki-Yamakawa'21]: classical PKE → public key, many time

Revocable Time-Released Crypto

Classical time-released crypto:
[Rivest-Shamir-Wagner'96]



Thm [Unruh'13]: Classical TRE → Revocable TRE

Construction idea:

$$c = (\ \mathsf{TRE}(k)\ ,\ \mathsf{Enc}(\mathsf{k},\mathsf{m})\ )$$

Classical TRE

Enc w/ certified deletion

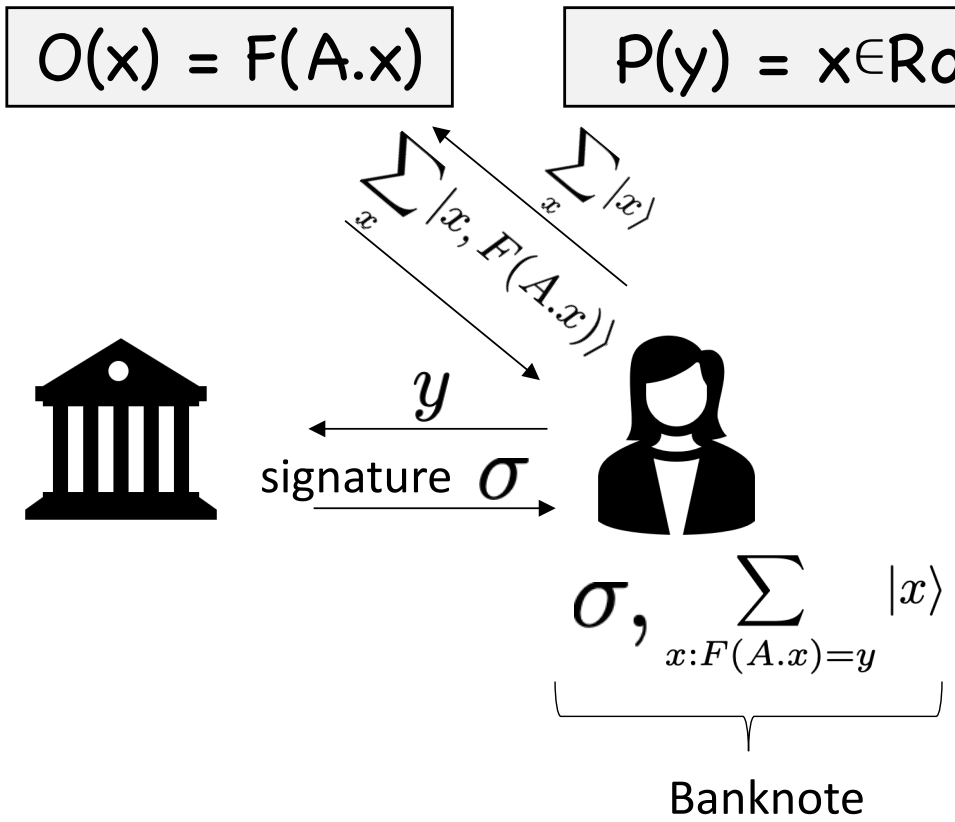
Security proof not generic and non-trivial

(Public key) quantum money ✓

Copy protection ✓

Revocable cryptography ✓

Unclonable Crypto with Classical Communication



Suppose O is post-quantum collision-resistant*

* Its not! O is periodic

Correctness: Just need pre-image sets of O to be subspaces
Collision-resistance: Need (at minimum) subspaces not all the same
(Need P to check different subspace for each y)

[Brakerski-Christiano-Mahadev-Vazirani-Vidick'18]: Use trapdoor 2-to-1 function (aka Trapdoor Claw-Free func) from LWE

Any pair of points is a subspace!

Limitation: P needs secret trapdoor, so no public verification

Nevertheless, ideas used for many results

Open Question 5: Publicly verifiable money with classical communication from iO + LWE + Isogenies + LPN + …

[Radian-Sattath'19]: private key case
[Shmueli'21]: public key classical bank