Verifiable Quantum Advantage without Structure

Takashi Yamakawa (NTT Social Informatics Laboratories)
Mark Zhandry (NTT Research & Princeton University)

Can **quantum** computers offer a superpolynomial computational **advantage**?

Can such advantage
be efficiently **verified**?

Real-world impact $\Rightarrow$ verified

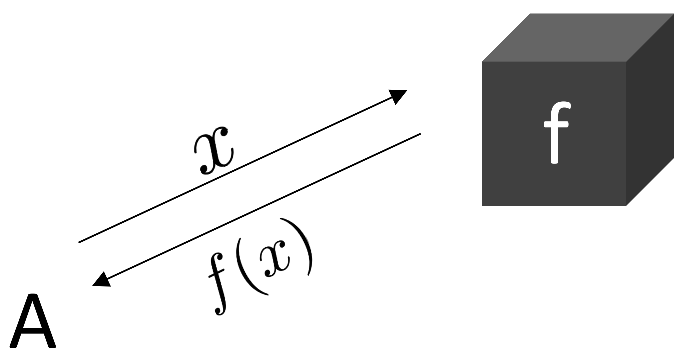
Is **structure** needed for quantum advantage?

Current state of complexity theory

$\Longrightarrow$ no unconditional results

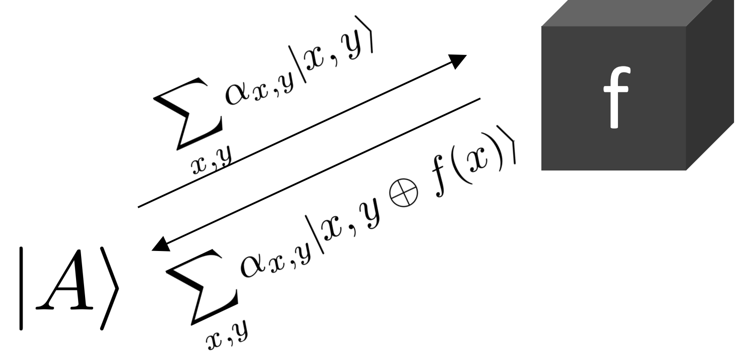
Option 1: Oracle Separations

Classical algorithms



vs

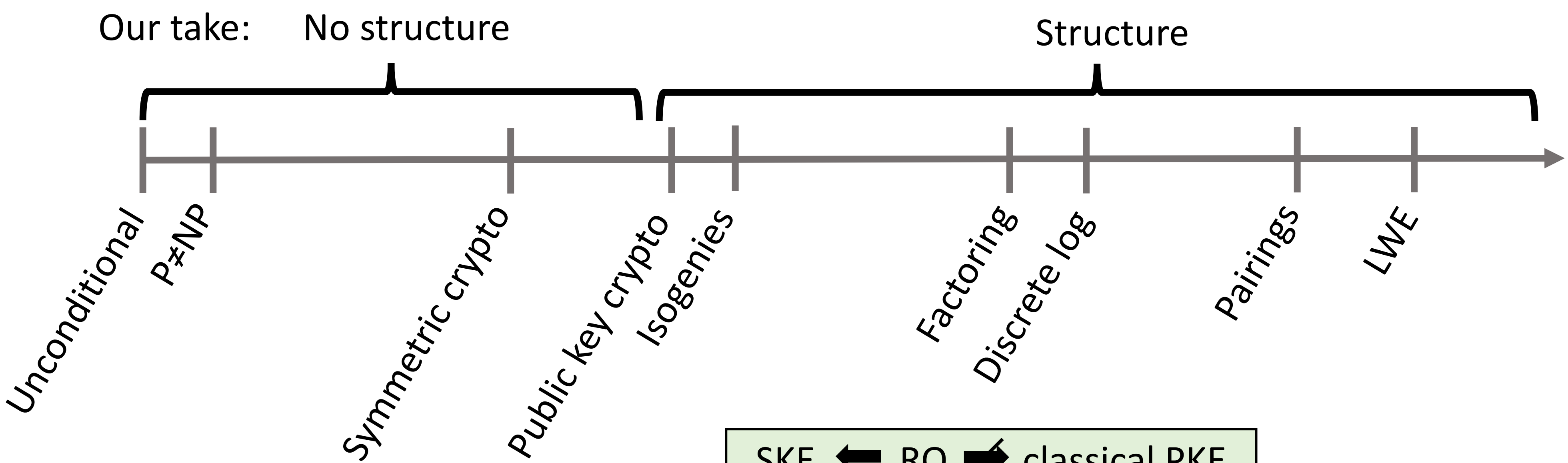
Quantum algorithms



no structure = random oracle

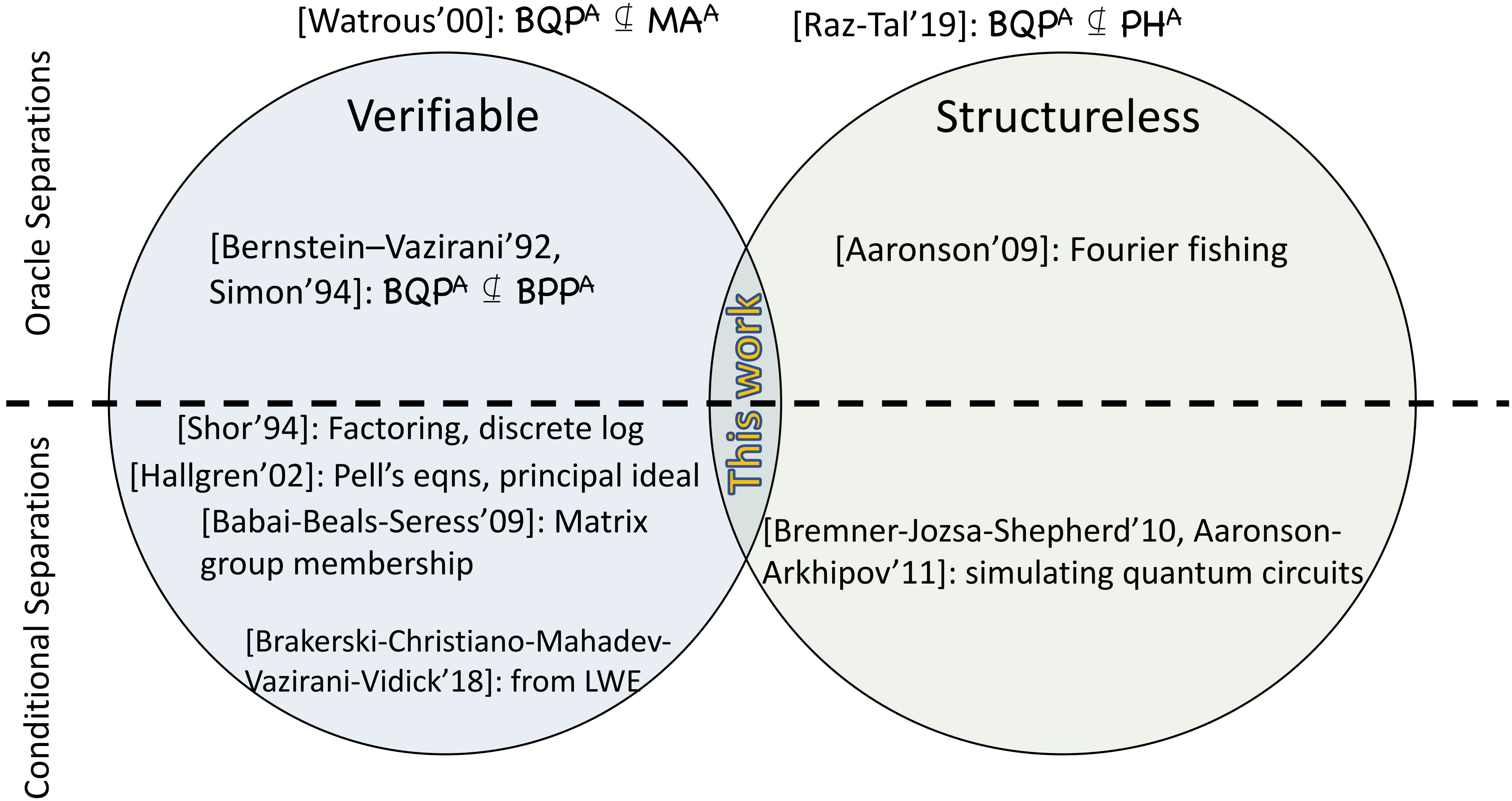
Option 2: Conditional Separations

Prove advantage under some computational assumption



SKE $\Leftarrow$ RO $\not\Rightarrow$ classical PKE

[Impagliazzo-Rudich'89]


[Watrous'00]: BQP^A ⊈ MA^A
[Raz-Tal'19]: BQP^A ⊈ PH^A
Verifiable
Structureless
Oracle Separations
[Bernstein–Vazirani'92, Simon'94]: BQP^A ⊈ BPP^A
[Aaronson'09]: Fourier fishing
This work
Conditional Separations
[Shor'94]: Factoring, discrete log
[Hallgren'02]: Pell's eqns, principal ideal
[Babai-Beals-Seress'09]: Matrix group membership
[Brakerski-Christiano-Mahadev-Vazirani-Vidick'18]: from LWE
[Bremner-Jozsa-Shepherd'10, Aaronson-Arkhipov'11]: simulating quantum circuits

All existing oracle-free advantage in NP relies on period-finding

All existing structure-less sources of advantage are sampling problems

[Aaronson-Ambanis'09]: under a plausible conjecture

$$0/1 \leftarrow |A\rangle \overset{q\text{ queries}}{\rightleftarrows} \text{RO} \quad \Rightarrow \quad \approx 0/1 \leftarrow \text{S} \overset{\text{poly}(q)}{\rightleftarrows} \text{RO}$$

S potentially computationally unbounded

Basically, random oracles shouldn't help separating BQP from BPP

This work: verifiable quantum advantage without structure

Results: relative to random oracle with probability 1:

$\exists$ NP search problem in BQP \ BPP

$\exists$ OWF, CRHFs, signatures that are classically hard but quantumly easy

Assuming classically hard PKE, $\exists$ PKE that is classically hard but quantumly easy

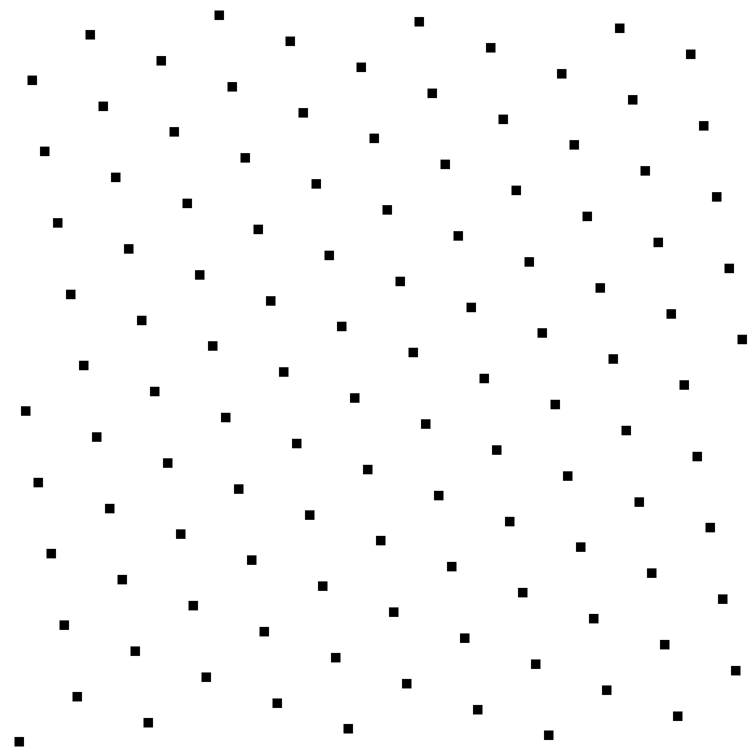
$\exists$ publicly verifiable proof of quantumness with minimal rounds

Under the AA conjecture, $\exists$ certifiable randomness with minimal rounds

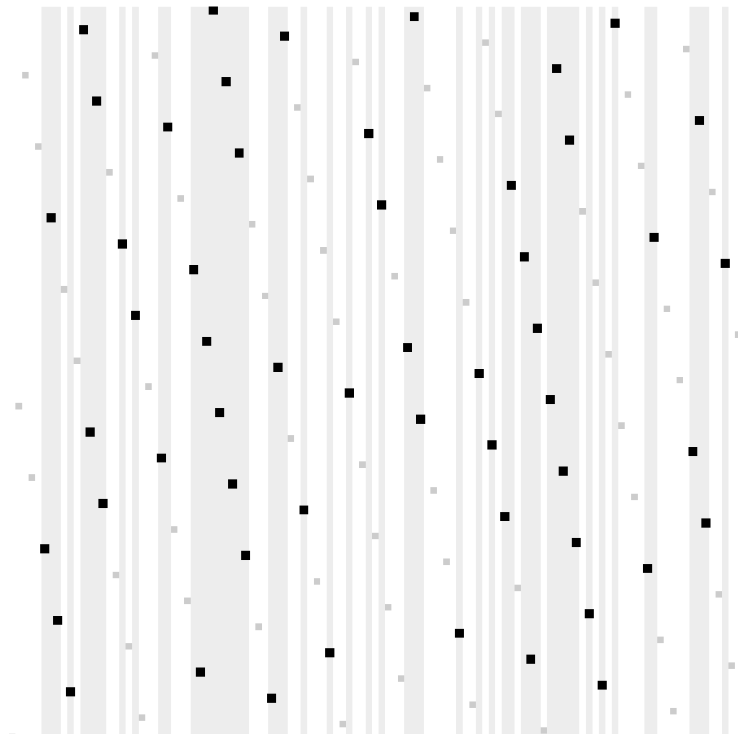
Can replace RO with SHA256 to obtain conjectured non-relativized versions

Our Construction

High-dimensional, Large-alphabet, Linear Code C

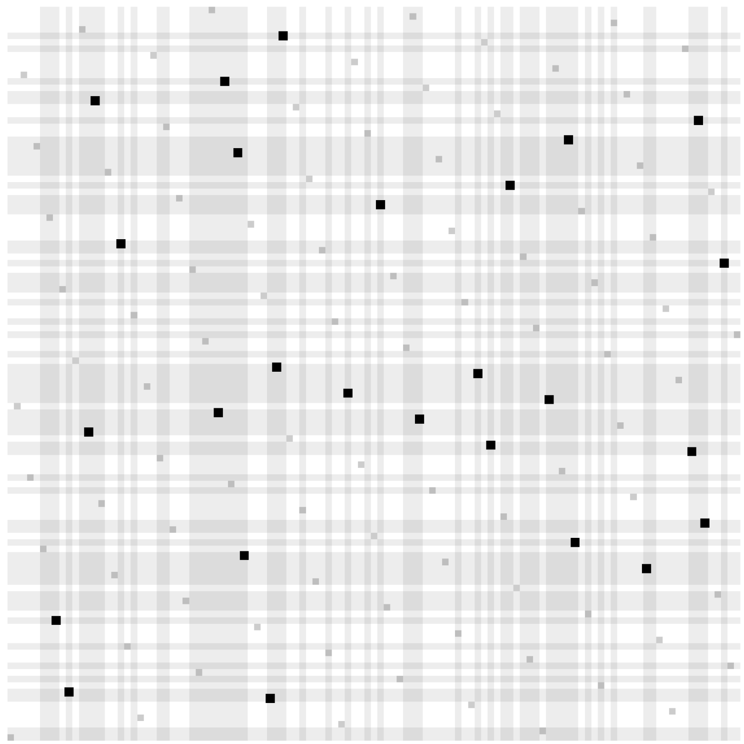


Random Subset of x-coordinates



Determined by querying random oracle

Random Subset of y-coordinates



Repeat for all coordinates

Questions:

- Why classically hard?
- Why quantumly easy?
- What code to use?

Why/when should it
be classically hard?

Domain-constrained Linear Equations

[Ajtai'96]: Random linear code + low L_2 norm (SIS)

[Applebaum-Haramaty-Ishai-Kushilevitz-Vaikuntanathan'17]
[Yu-Zhang-Weng-Guo-Li'17]:
[Brakerski-Lyubashevsky-Vaikuntanathan-Wichs'18]

Random binary linear code
+ low Hamming weight

These seem likely to be (quantum) hard

Def: $\mathrm{Dist}(c, S_1 \times S_2 \times \ldots \times S_n) := \#\{ i : c_i \notin S_i \} / n$

Def: C is *list recoverable* if $\exists\, \delta, \varepsilon, \varepsilon'$ such that, if $|S_1|, |S_2|, \ldots, |S_n| \leq 2^{n^{\varepsilon}}$, then

$$\#\{ c \in C : \mathrm{Dist}(c, S_1 \times S_2 \times \ldots \times S_n) \leq \delta \} \leq 2^{n^{\varepsilon'}}$$

Examples:

- Folded Reed-Solomon [Guruswami-Rudra'05]
- Random Linear codes [Rudra-Wootters'17]

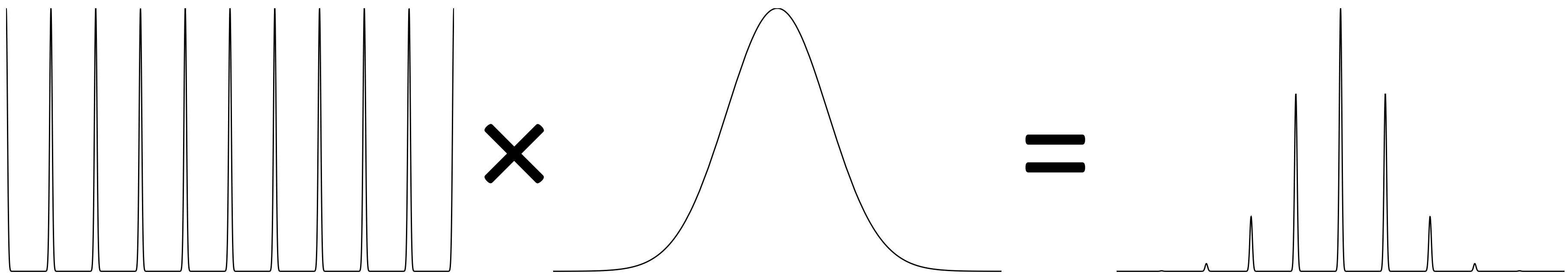
Thm: list recoverable $\Rightarrow$ classically intractable

Concretely, Pr[poly(n) queries give solution] $\leq 2^{n^{\varepsilon'}} \times 2^{-\delta n}$

[Haitner-Ishai-Omri-Shaltiel'15]:
List recovery $\rightarrow$ parallel hashing

Why/when should it
be quantumly easy?

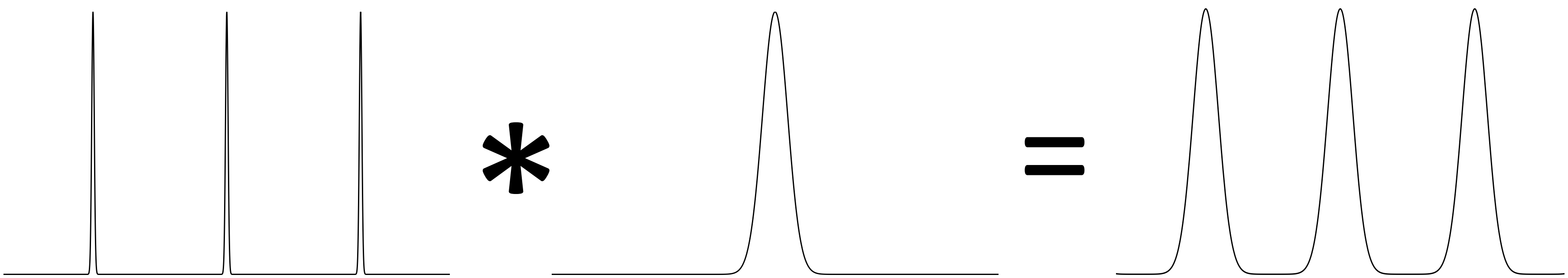
“Multiplying” quantum states
[Regev’05]



$$\sum_x \alpha_x |x\rangle \qquad \sum_x \beta_x |x\rangle \qquad \sum_x \alpha_x \beta_x |x\rangle$$

Ignoring normalization

Switch to Fourier Domain: Convolution



$$\sum_x \hat{\alpha}_x |x\rangle$$

$$\sum_y \hat{\beta}_y |y\rangle$$

$$\sum_{x,y} \hat{\alpha}_x \hat{\beta}_y |x+y\rangle$$

1. Construct separately:

$$\left(\sum_x \hat{\alpha}_x |x\rangle\right) \otimes \left(\sum_y \hat{\beta}_y |y\rangle\right) = \sum_{x,y} \hat{\alpha}_x \hat{\beta}_y |x, y\rangle$$

Given

2. Add “in superposition”:

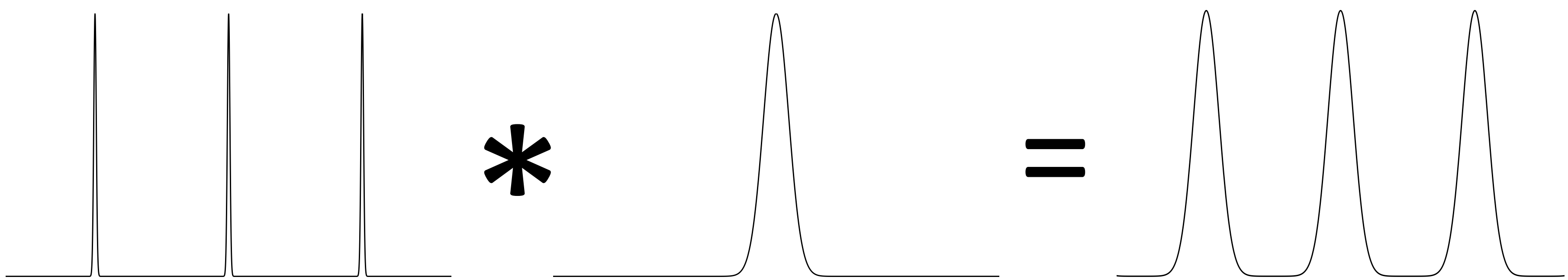
$$\sum_{x,y} \hat{\alpha}_x \hat{\beta}_y |x, y\rangle \to \sum_{x,y} \hat{\alpha}_x \hat{\beta}_y |x, y, x+y\rangle$$

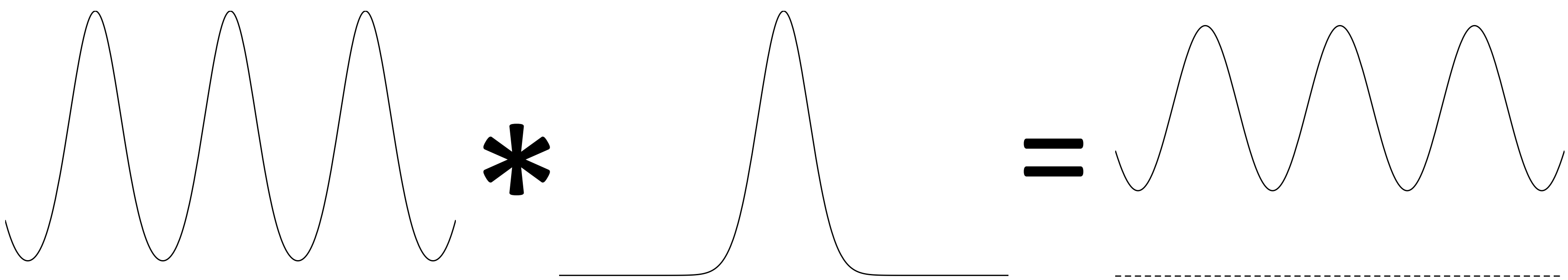
Easy

3. Decode $x + y \to (x, y)$ in reverse:

$$\sum_{x,y} \hat{\alpha}_x \hat{\beta}_y |x, y, x+y\rangle \to \sum_{x,y} \hat{\alpha}_x \hat{\beta}_y |x+y\rangle$$

Not always possible





Example [Regev'05]:

<u>Primal domain:</u>

α_x = indicator for linear code C

$\beta_x \propto e^{-|x|^2/\sigma^2}$

Product ≈ short vectors in C

aka SIS

<u>Fourier domain:</u>

$\hat{\alpha}_x$ = indicator for $C^\perp$

$\hat{\beta}_x \propto e^{-|x|^2/(\sigma')^2}$

Step 3 ≈ bounded dist. decoding

aka LWE

quantum hardness of SIS ➡ quantum hardness of LWE

Applying to our construction

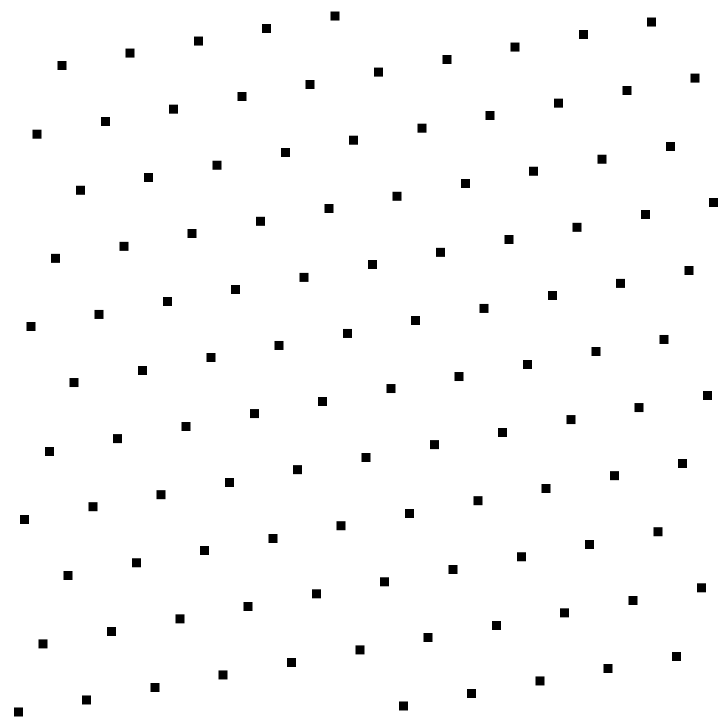
α_x = indicator for C

β_x = indicator for valid coordinates

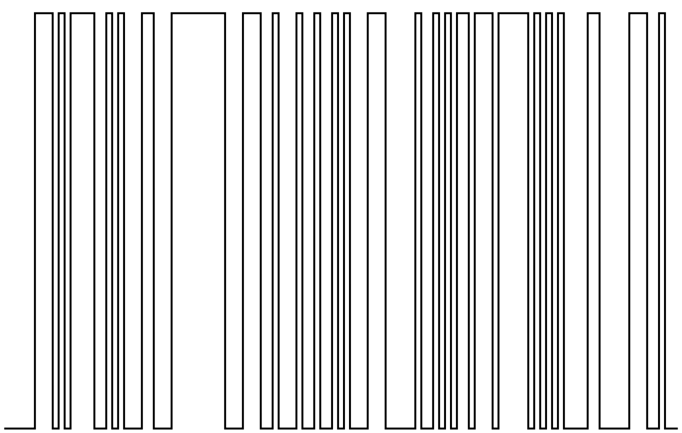
Product = solutions to our problem

What is the decoding problem?

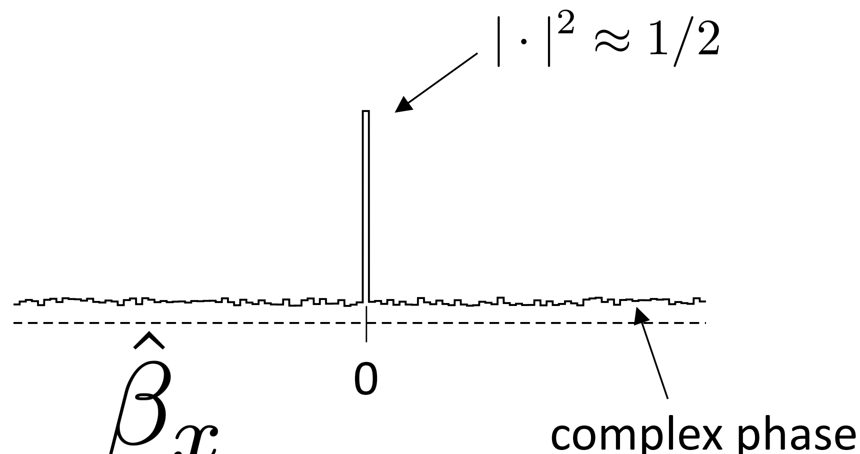
The dual code $C^\perp$



$$\hat{\alpha}_x$$



β_x for 1 dimension



$\hat{\beta}_x$

$x + y =$ (dual codeword)
+ (random errors in ≈ ½ coordinates)

Thm: Can decode efficiently **whp** if $C^{\perp}$ is **list-decodable** for ½+ε fraction of errors

Good news: Dual of Folded RS is another Folded RS, has essentially optimal list-decoding

Challenge: In general, "whp" decoding not good enough

Exponential!

Actual convolution theorem:

$$\sum_{x,y} \hat{\alpha}_x \hat{\beta}_y |x + y\rangle \longleftrightarrow \sqrt{N} \sum_x \alpha_x \beta_x |x\rangle$$

Error terms in decoding naively get multiplied by exponential

[Regev'05]: error prob $\ll N^{-1}$ ➡ still small after multiplying

Our work: error prob $\gg N^{-1}$ ➡ delicate analysis needed

Applications

1. NP search problem in BQP \ BPP

$$R^O : \{0,1\}^n \times \Sigma^n \to \{0,1\}$$

$$R^O(x,w) := \begin{cases} 1 & \text{if } w \in C \wedge O(i||w_i) = x_i \forall i \\ 0 & \text{otherwise} \end{cases}$$

2. Classical/Quantum Separations for Crypto

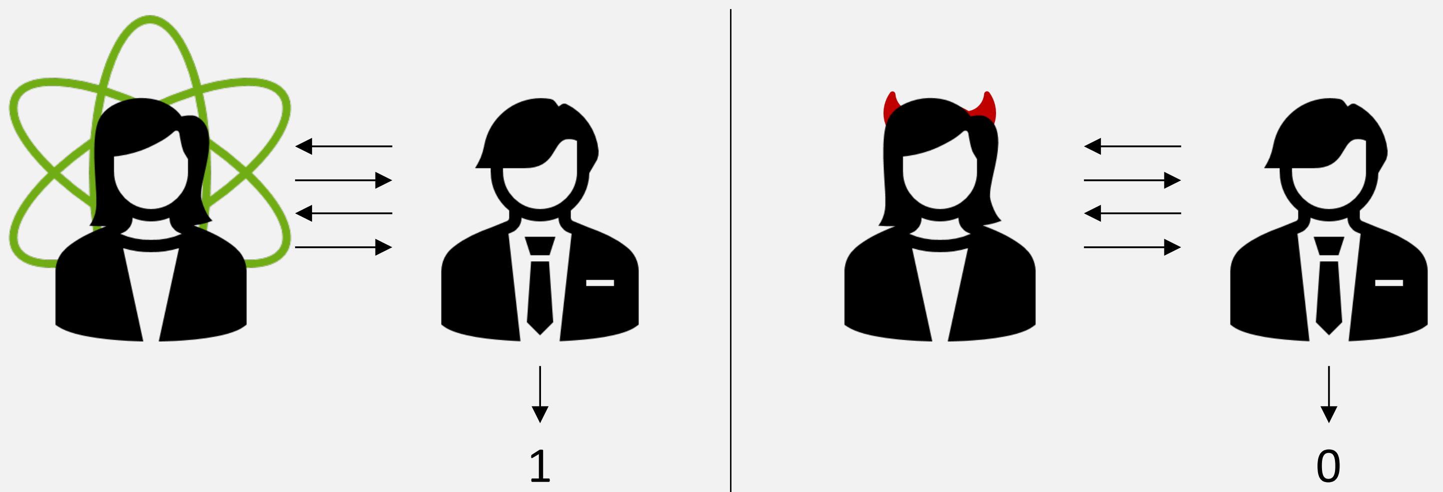
$$OWF^O : C \to \{0,1\}^n$$

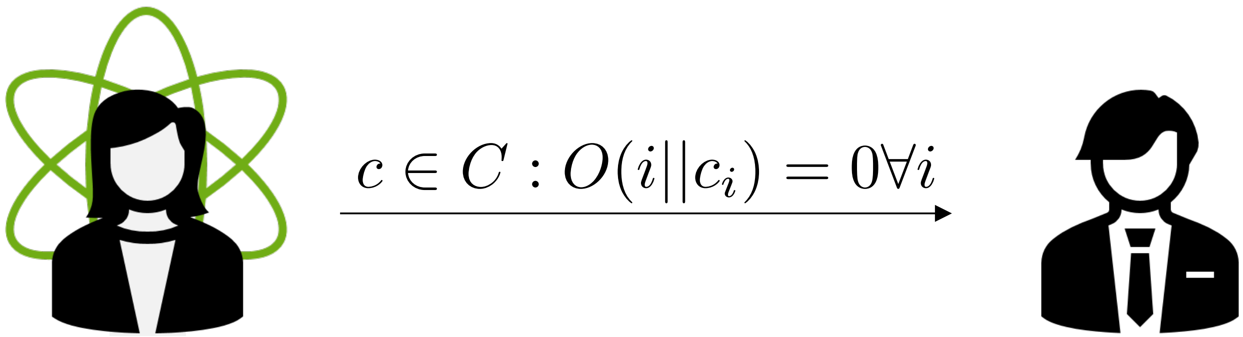
$$OWF^O(c) := O(1||c_1) \,||\, O(2||c_2) \,||\, \cdots \,||\, O(n||c_n)$$

3. Proof of Quantumness

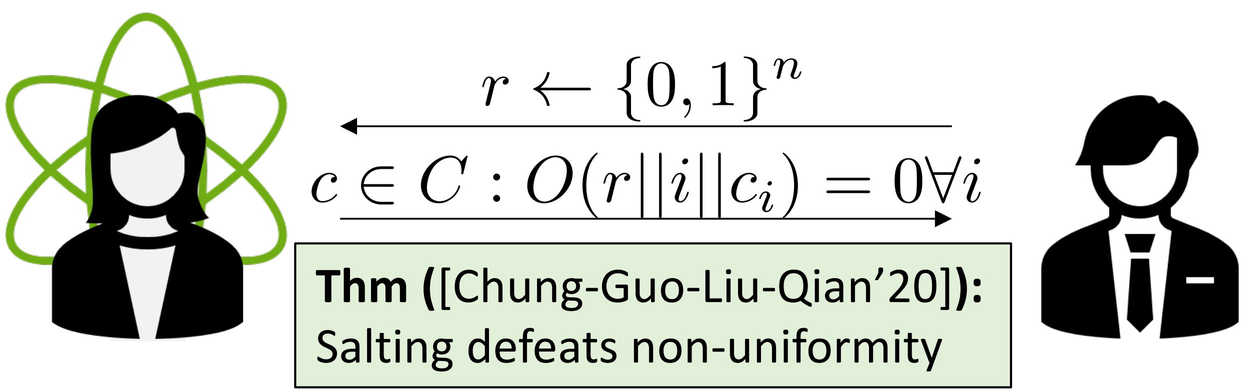
Def: Proof of Quantumness

[Brakerski-Christiano-Mahadev-Vazirani-Vidick’18]





Uniform (oracle-independent) adversaries

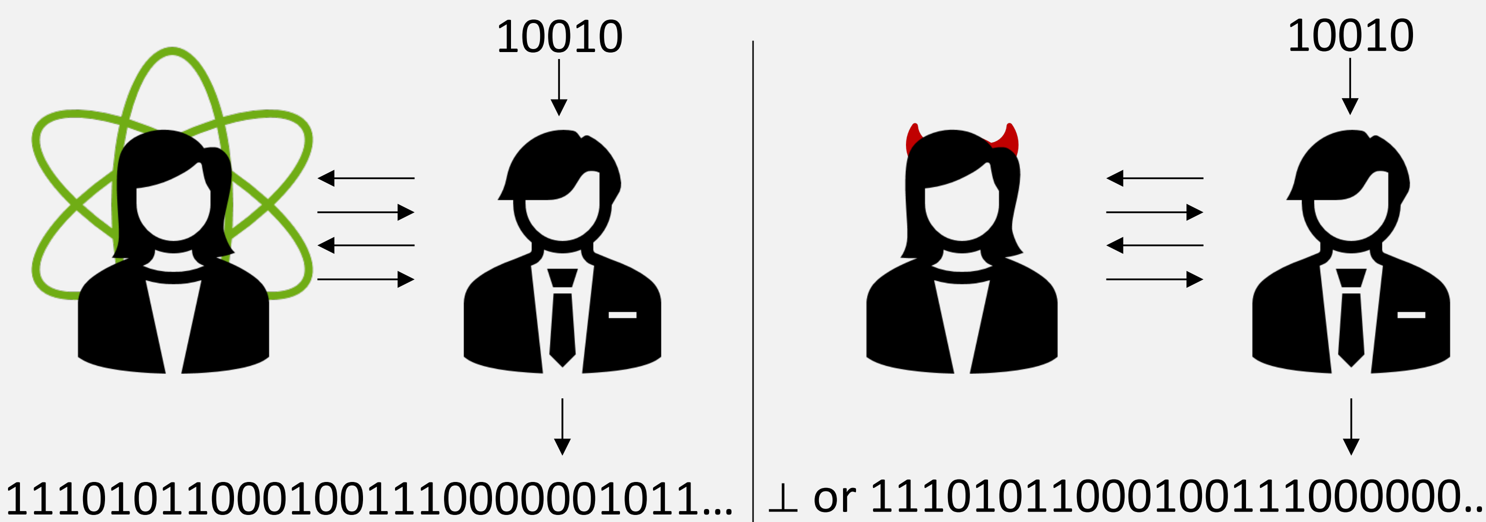


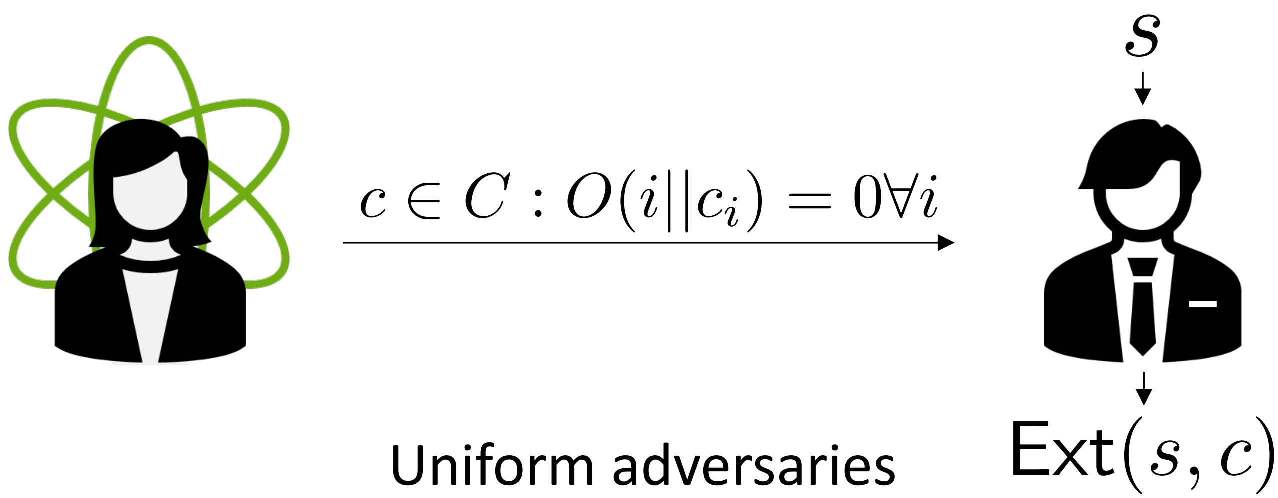
Oracle-dependent non-uniform adversaries

4. Certifiable Randomness

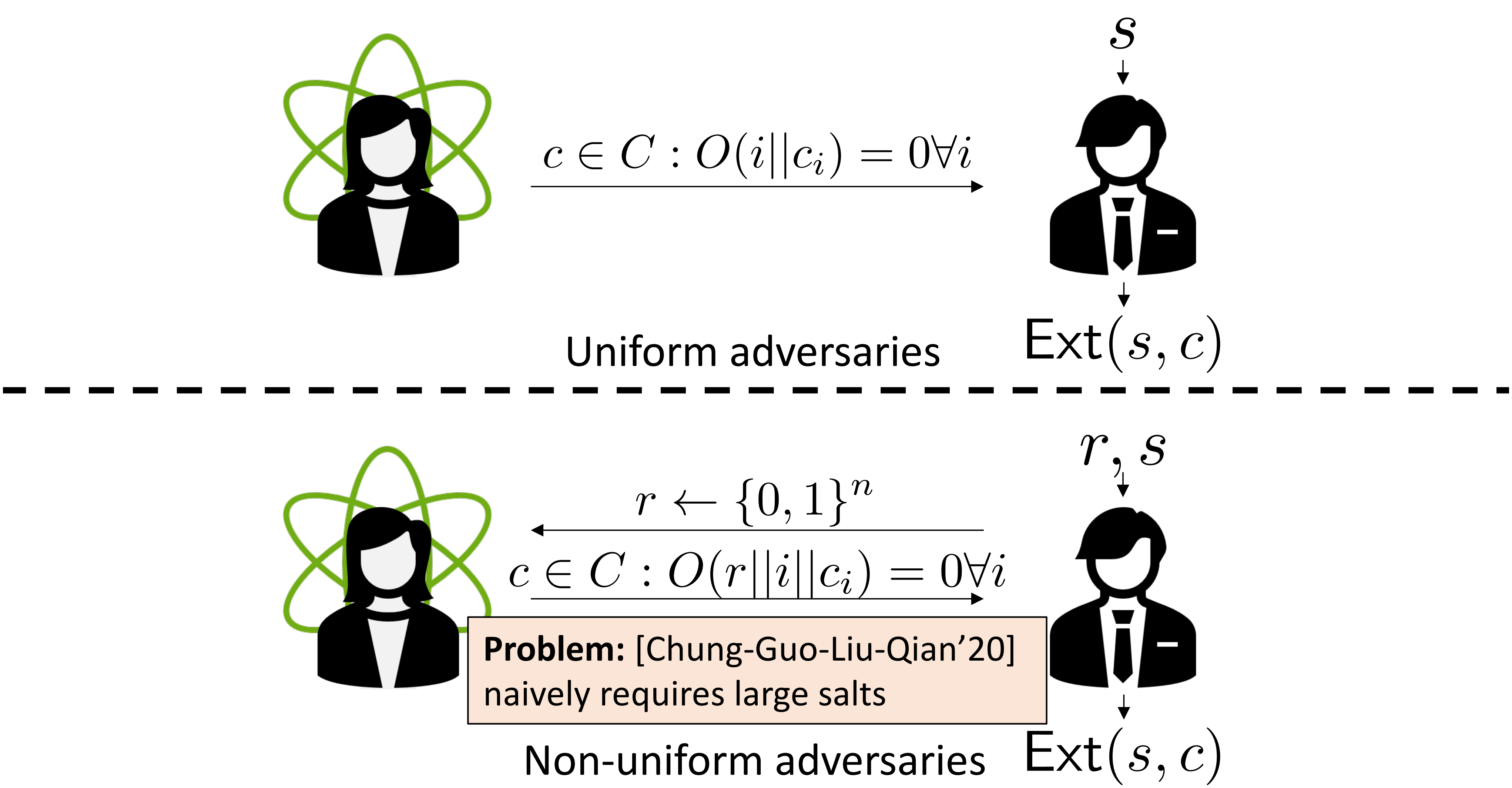
Def: Certifiable Randomness

[Brakerski-Christiano-Mahadev-Vazirani-Vidick’18]





Thm: AA conjecture ➡ c has min-entropy



s
$c \in C : O(i||c_i) = 0 \forall i$
Uniform adversaries
$\mathsf{Ext}(s, c)$
r, s
$r \leftarrow \{0,1\}^n$
$c \in C : O(r||i||c_i) = 0 \forall i$
Problem: [Chung-Guo-Liu-Qian'20] naively requires large salts
Non-uniform adversaries
$\mathsf{Ext}(s, c)$

Is it practical?

Thanks!