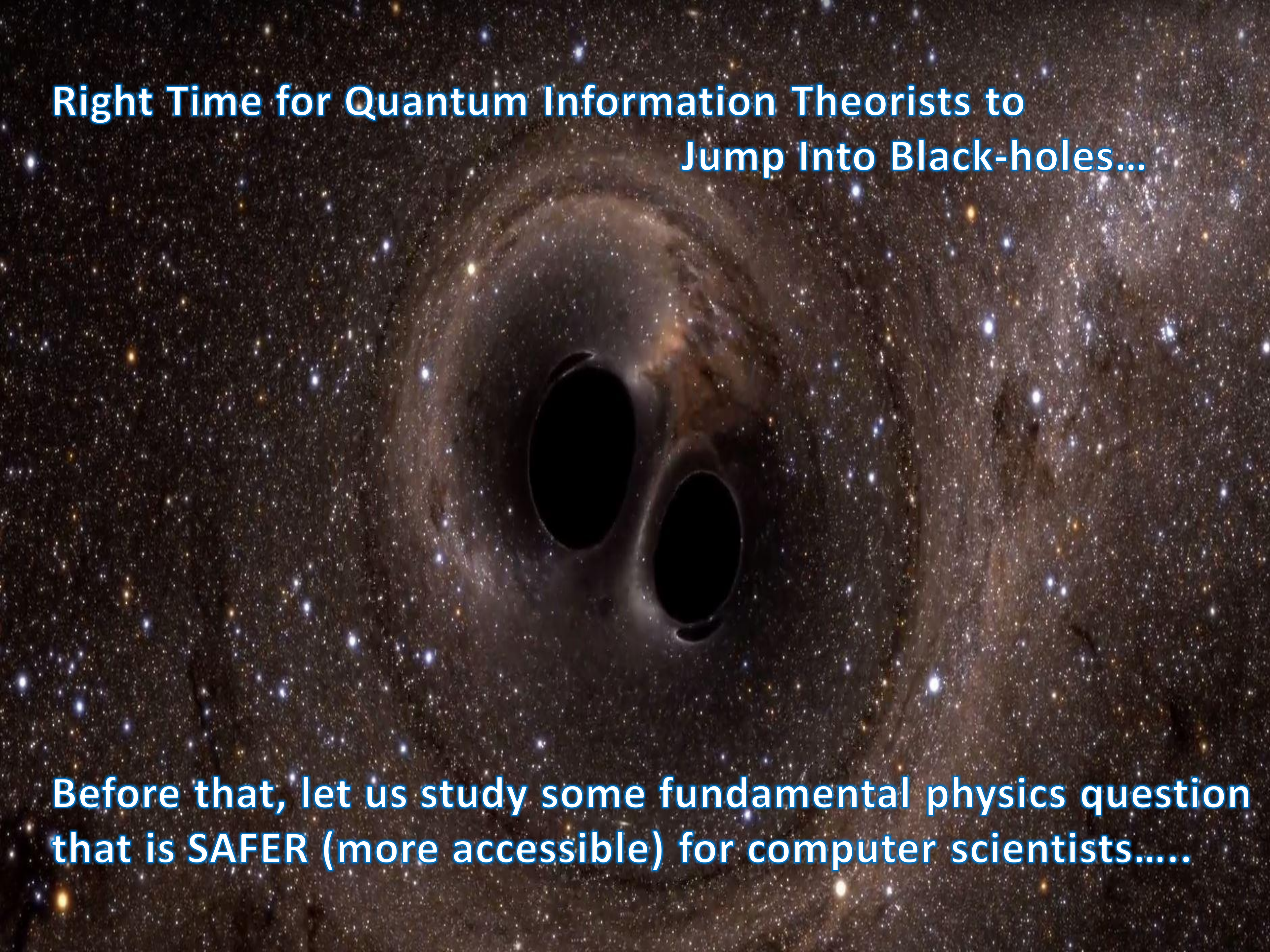
# General Randomness Amplification with non-signaling security

Xiaodi Wu
University of Oregon

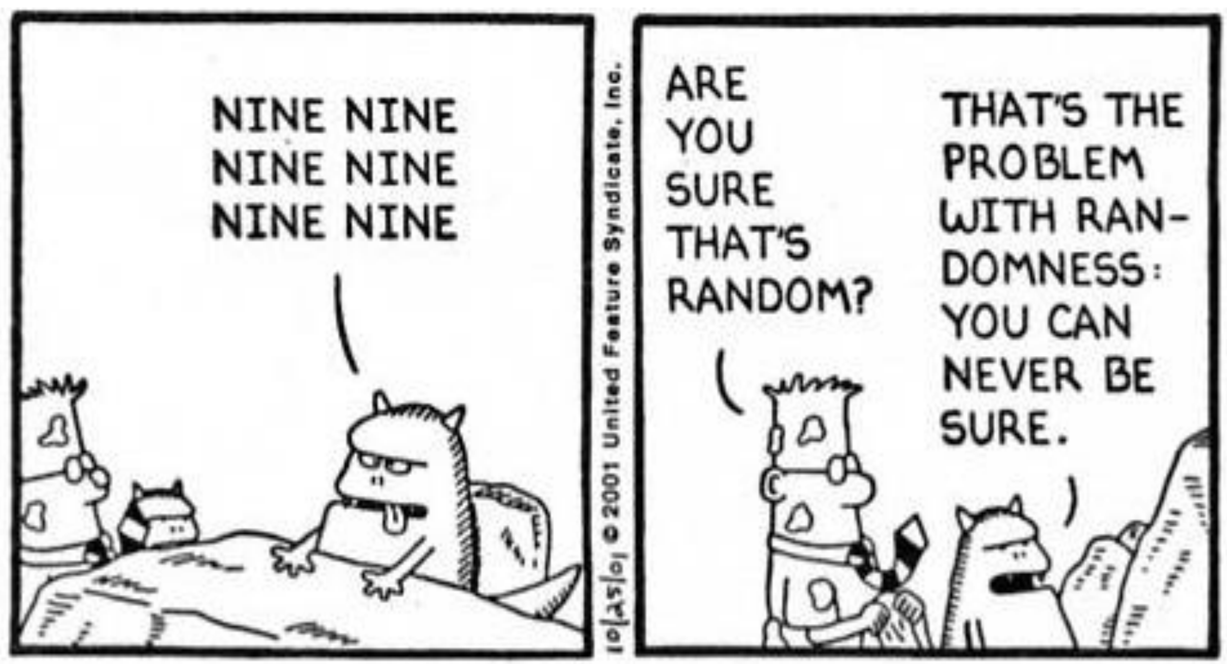
Yaoyun Shi
University of Michigan

Kai-Min Chung
Academia Sinica


Right Time for Quantum Information Theorists to
Jump Into Black-holes…
Before that, let us study some fundamental physics question
that is SAFER (more accessible) for computer scientists…..

Is our world deterministic?

How could fundamentally unpredictable events be possible and certifiable?



# We can't be sure … without believing first of all its existence

One POSSIBILITY:

a deterministic "matrix" world!

# Deterministic World v.s. Truly Random World [CR]

Does *non-deterministic* world imply *truly random* world?

the world allows **uniformly random** events

**A Possible Dichotomy Theorem:**

Weak "uncertainty"
(e.g., guess probability < 1)
**Weak random Source**

deterministic
operation
→
no extra randomness

Full "uncertainty"
(**uniformly random**)
against environment

Thus, *either* the world is **deterministic**
*or* we can faithfully create **uniformly random** events

**Colbeck & Renner [CR'12]:**
**Can we certify existence of true randomness ?**
**(based on physical laws)**

**Can we generate uniform bits from weak sources with minimal assumptions?**

# Can we certify exist. of true randomness?


- System performs experiment to output a bit $b \in \{0,1\}$
- Eve models external observer
- **<u>Necessary Assumptions</u>**: (1) **weak source** (some uncertainty)
- (2) **No-signaling between System and Eve**. In particular, System cannot signal $b$ to Eve.

# Approaches w/ additional assumptions

System

Weak Source

**Classical system** : require **independent** weak sources.

**Quantum system**: seemingly intrinsic randomness

**Question:** QM could be incomplete. Devices are untrusted. Can we still generate uniform bits from weak sources?

A… …**on** by **"Classical"** Human being.

A more fundamental issue: **Randomness from Quantum Mechanics**?

**YES?** If Quantum mechanics explains the inner-working of Nature

**NO!** If QM is incomplete: e.g. existence of a deterministic alternative

# Device-Independent Cryptography

**No Trust** of the inner-working due to ***technical*** or ***fundamental*** issues

**GOAL:** only make *classical* operations, still leverage *quantum* devices

=> **Device-Independent Quantum Cryptography** !!!

How can "classical" human being leverage quantum power?

**Bell-tests** for detecting quantum behavior (*non-locality*)

Force to use the *"quantumness"* via non-locality!


Successful Examples: (this session and the incomplete list)

1) QKD [BHK05, MRC+06, MPA, VV13, BCK13, RUV13, MS13, AF et al..]
2) Randomness Expansion [Col06, PAM+10, PM11, FGS11, VV12, MS13, CY13]
3) Free-randomness Amplification [CR12, GMdlT+12, MP13, BR+13…]
4) Quantum Bit Commitment & Coin Flipping [SCA+11]
5) Quantum Computation Delegation [RUV13, MacK13]

# Randomness Amplification [CR12]

- Certify true randomness from weak randomness
  - via Bell violation, **device-independent** framework

- Weak source = Santha-Vazirani ($\varepsilon$-SV) sources

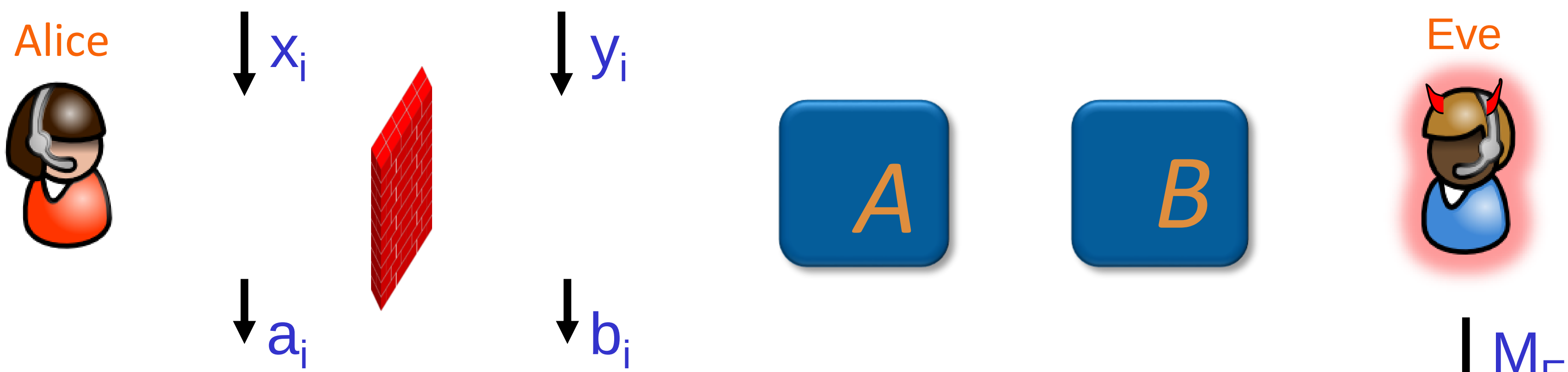
$$(1/2) - \varepsilon \leq \Pr[X_i = x_i \mid X_{<i} = x_{<i}] \leq (1/2) + \varepsilon$$

  - **physical principles** behind choosing this SV
  - Amplification from $\varepsilon$-SV for $\varepsilon < 0.058$

# Rand. Amp. Protocol of [CR12]

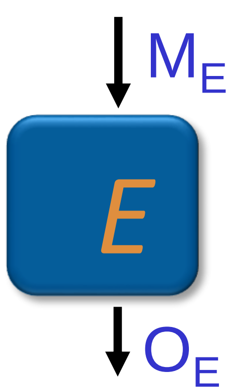
SV Source

01011010100100100




Accept if Device “play well” &
Output $z = a_r$ for $r \leftarrow$ SV Source

Guess z



# Dichotomy Theorem [CR12,GMT+13]

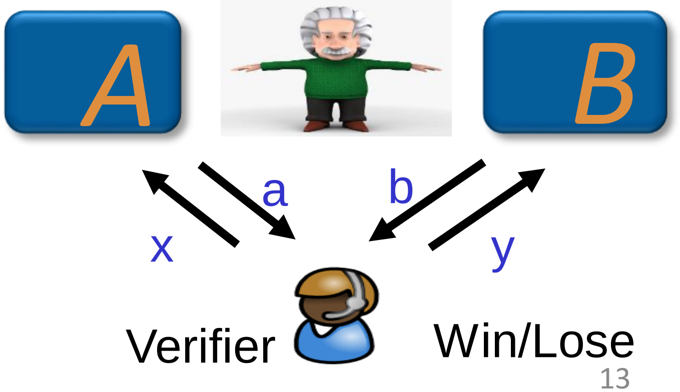
- Can we certify our physical world is inherently random?
  - NO if the world is fully deterministic ("super-determinism")
- Dichotomy: either deterministic, or certifiably random
- **RA**: weak randomness $\Longrightarrow$ certifiable true randomness
- **Weaker assumptions $\Longrightarrow$ Stronger Dichotomy Thm**
- Require Non-Signaling (NS) security [CR12]
  - Should *not* assume quantum completeness
  - Only assume NS condition (necessary)

# Non-Signaling (NS) Security

- Devices A, B, E may share "non-signaling correlation"
  - Arbitrary correlation not signaling the input
  - Marginal distribution of A depend only on value $X = x$
    - $p(a|xy) = p(a|xy')$ for any $x, y, y'$

- Powerful: can win CHSH w.p. 100%
  - Random $A \oplus B = x \wedge y$ & marginal of $A, B$ = uniform

- NS Security:
  - If Pr[ Alice accepts ] $\geq \varepsilon$, then
  - Pr[ Eve guess z correctly ] $\leq (1/2) + \varepsilon$



# Developments of RA Protocols

| | Source | Eve | Conditional independence | |
|---|---|---|---|---|
| | | | Source-Device | Source-Eve |
| [CR12] | SV $\varepsilon < 0.058$ | Classical | Indep. | --- |
| [GMT+13] | SV any $\varepsilon < 1/2$ | NS | Indep. | Arbitrary |
| [BRG+13] | SV any $\varepsilon < 1/2$ | NS | Indep. | Indep. |
| [RBH+15] | SV any $\varepsilon < 1/2$ | NS | Indep. | Indep. |
| | | | | |
| [WBG+16] | SV $\varepsilon < 0.0144$ | NS | Somewhat | Somewhat |
| | | | | |

# Assumptions on the Source

- SV source is highly structured
  - Guarantee entropy for every bit of the Source
  - SV bit vs. SV block? Physics principle at the bit level (too strong?)

**Question:** can we reduce all these assumptions on the source to minimal?

# Minimal Weak Sources: in non-deterministic world

**Min-entropy** Sources: a random variable $X \in \{0,1\}^n$

(=) - log (the *maximum probability* of guessing x sampled from X correctly).

**NS** (=) - log (the *maximum probability* of guessing x sampled from X correctly w/ the help of NS correlation).

- A general measure of the randomness. Capture ***arbitrarily weak*** sources.
- Capture ***the amount of uniform bits*** that can be extracted via classical means.

**Non-deterministic World** → Non-Zero Min-entropy

→ **Weak Min-entropy Sources**

# Summary of RA Protocols

| | Source | Eve | Conditional independence | |
|---|---|---|---|---|
| | | | Source-Device | Source-Eve |
| [CR12] | SV<br>$\varepsilon < 0.058$ | Classical | Indep. | --- |
| [GMT+13] | SV<br>any $\varepsilon < 1/2$ | NS | Indep. | Arbitrary |
| [BRG+13] | SV<br>any $\varepsilon < 1/2$ | NS | Indep. | Indep. |
| [RBH+15] | SV<br>any $\varepsilon < 1/2$ | NS | Indep. | Indep. |
| **[CSW14]** | **Any weak** | **Quantum** | **Arbitrary** | **Arbitrary** |
| [WBG+16] | SV<br>$\varepsilon < 0.0144$ | NS | Somewhat | Somewhat |
| **This Talk** | Any weak | NS | Arbitrary | Arbitrary |

# Our Result: Ideal Dichotomy Thm

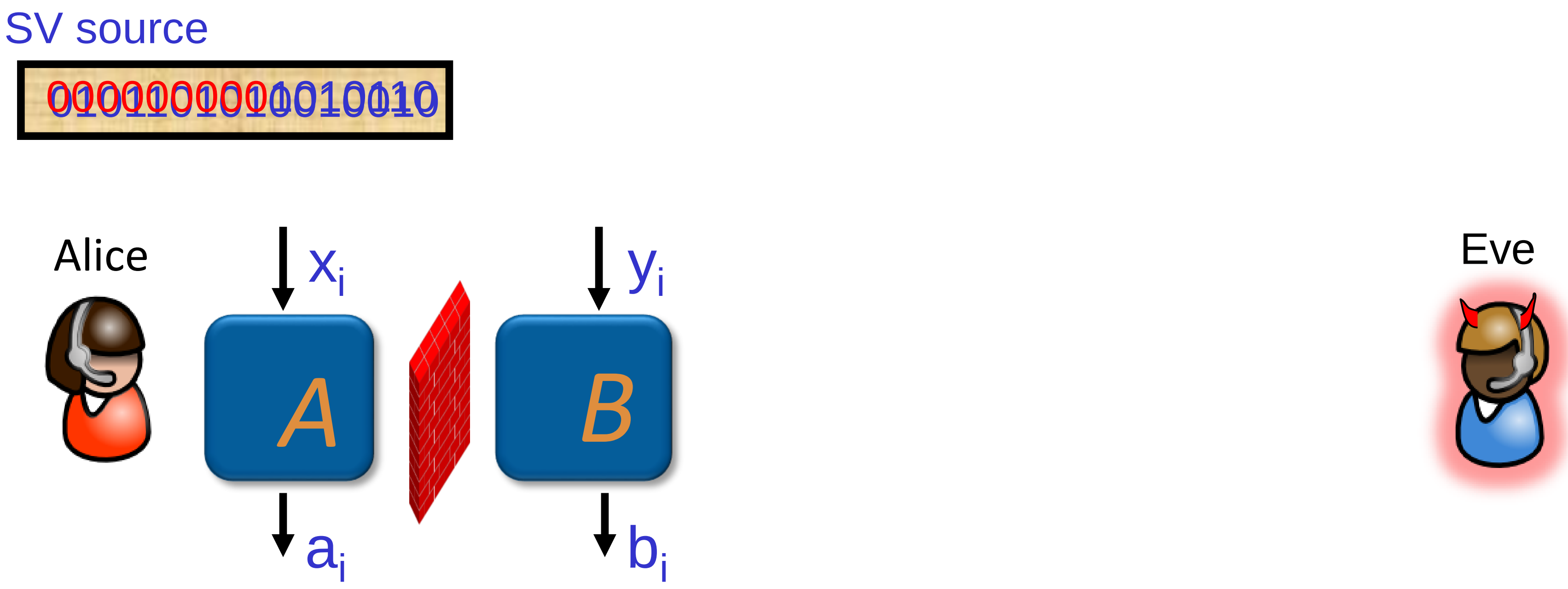
- Randomness amplification assuming
  - (Source|Device) has sufficient **NS** min-entropy
  - **NS** condition among Eve & Devices

- Minimal assumption: both are necessary
  - *No* structural or independence assumptions about the sources

- Ideal dichotomy theorem
  - Weak source = arbitrary source w/ sufficient uncertainty
  - **Local** uncertainty $\Longrightarrow$ certifiable **global** randomness

# Our Construction

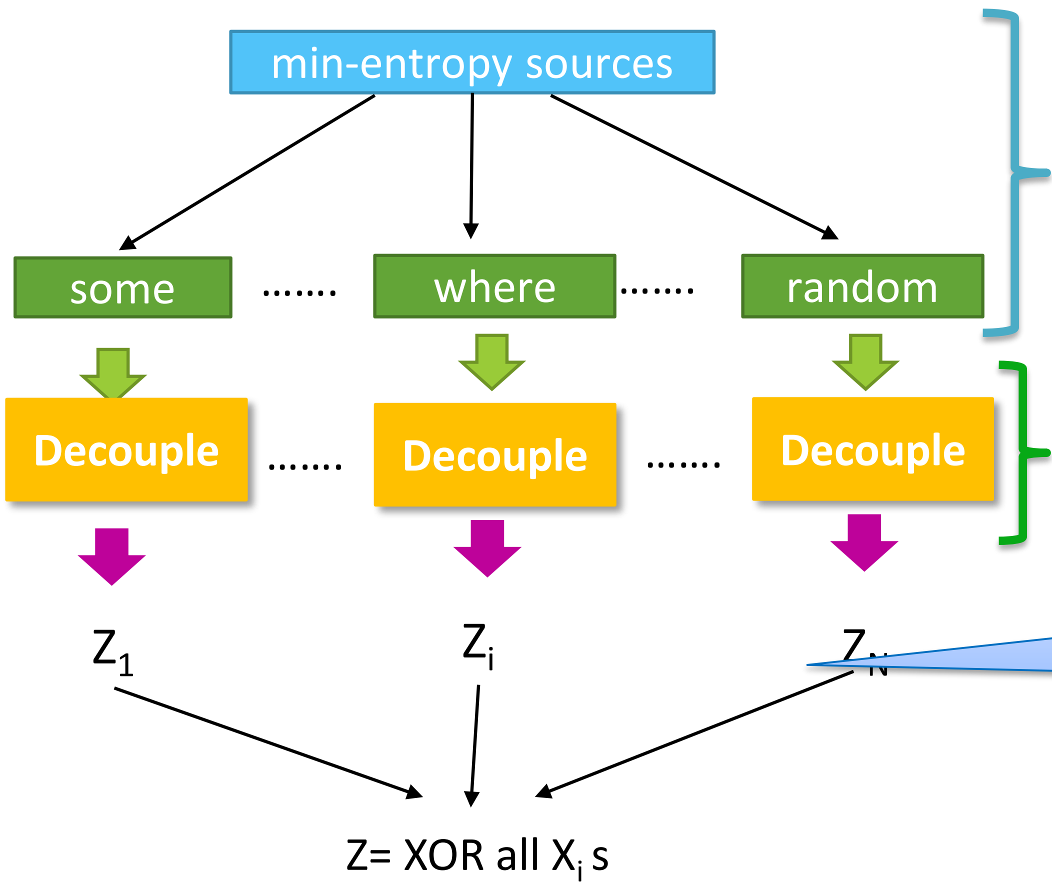
# All Existing Protocols




Directly use Source bits as inputs to Device

- Require SV structure & sophisticated games
- Unknown to handle unstructured weak sources

# Our Solutions: a bird's-eye view




**Classical pre-processing**:

transfer input to **uniform "locally"**

impose *correlations* among blocks

**Decouple the correlations:**

design special DI protocols

Some $Z_i$ is *global uniform*

**Classical Post-Processing: XOR picks the right one**

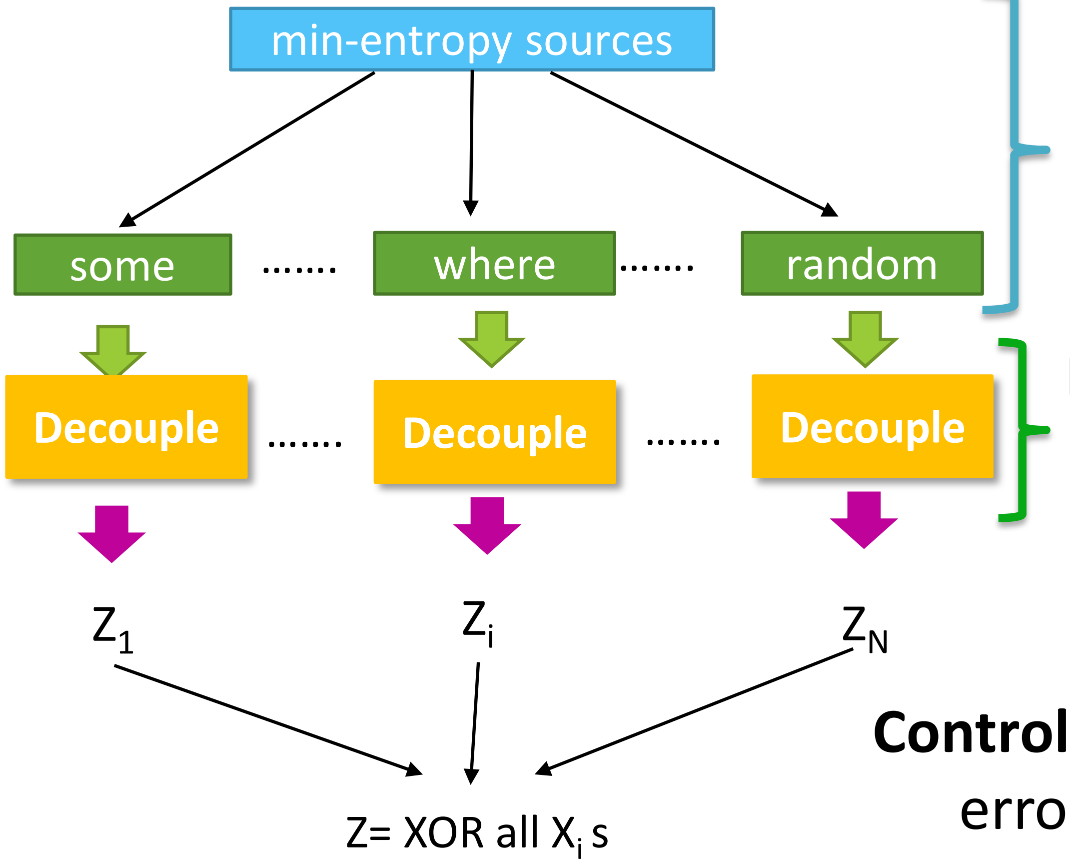
**By establishing a new property**

input seeds uniform to device only

*arbitrarily correlated* otherwise

e.g., Adv can know the inputs

# Our Solutions in the NS setting




**Classical pre-processing**:
somewhere random NS source

**Decouple the correlations:**
Equivalence Lemma [CSW14]
**unknown to hold in the NS**

**Control errors in compositions:**
errors from **local** to **global** systems.

**Classical Post-Processing: XOR picks the right one**

# Obtain Somewhere Uniform Source

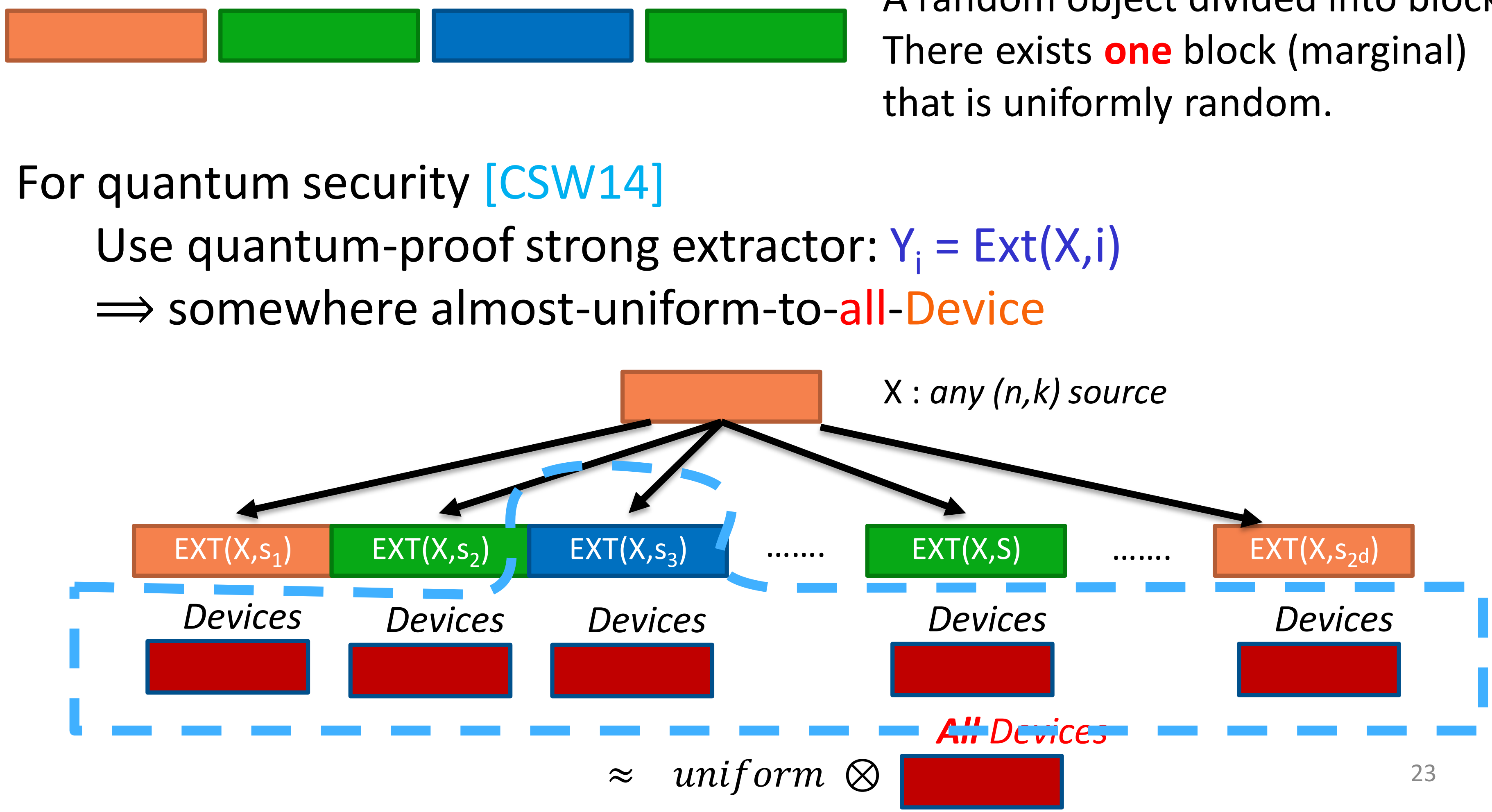
Somewhere Random Source (SR source):

A random object divided into blocks. There exists **one** block (marginal) that is uniformly random.

For quantum security [CSW14]

Use quantum-proof strong extractor: $Y_i = Ext(X,i)$

$\Longrightarrow$ somewhere almost-uniform-to-all-Device

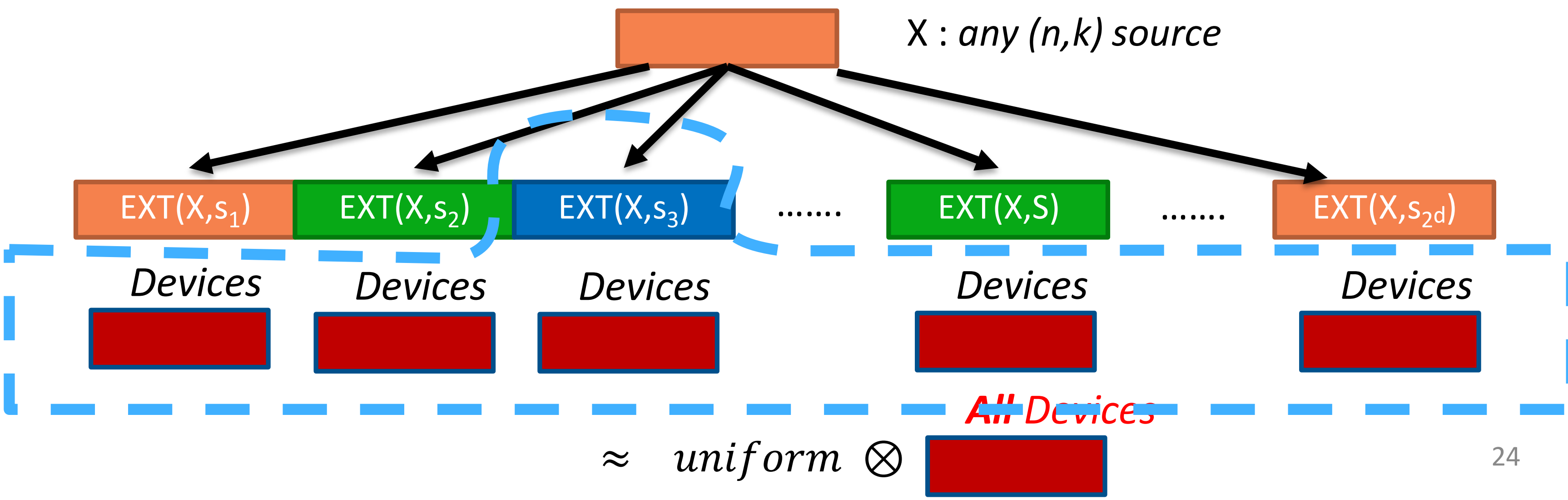



$\approx \ uniform \otimes$

# Obtain NS Somewhere Uniform Sources

**NS-proof strong extractors DO NOT exist!**

*a counter-example in the paper*

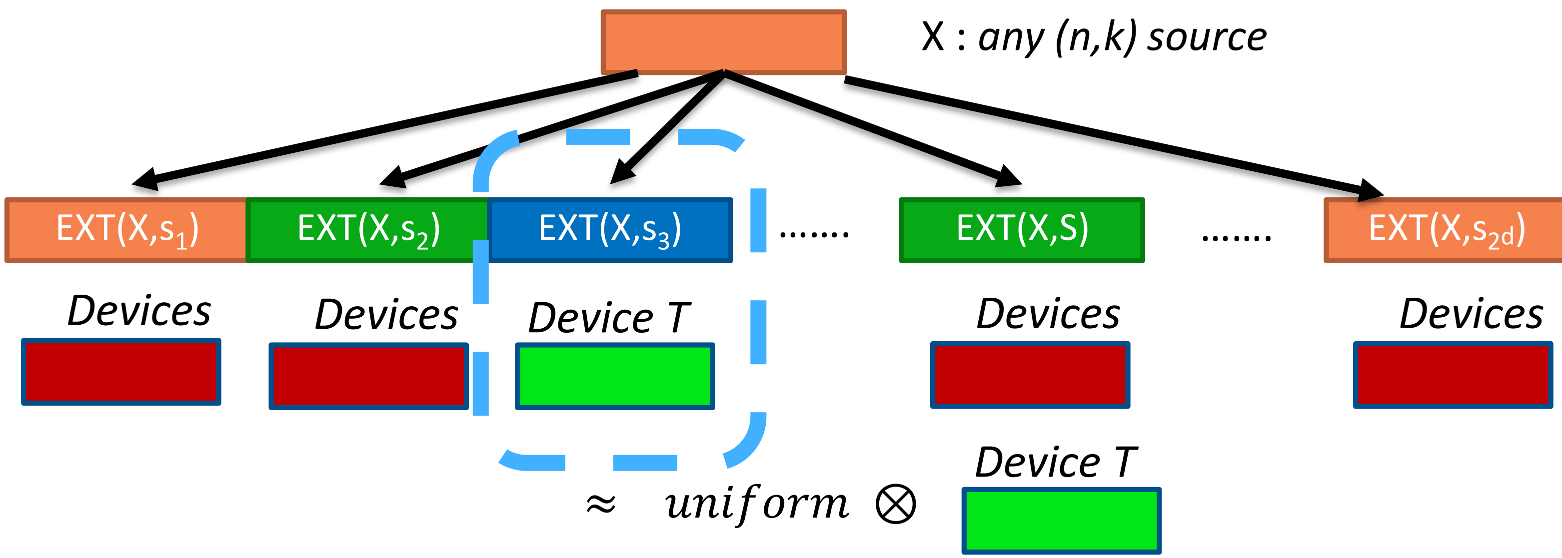



**IMPOSSIBLE to achieve with the construction!**

# Obtain NS Somewhere Uniform Sources

**NS-proof strong extractors DO NOT exist!**

*a counter-example in the paper*






**POSSIBLE** w/ classical extractors + $2^m$ error loss!

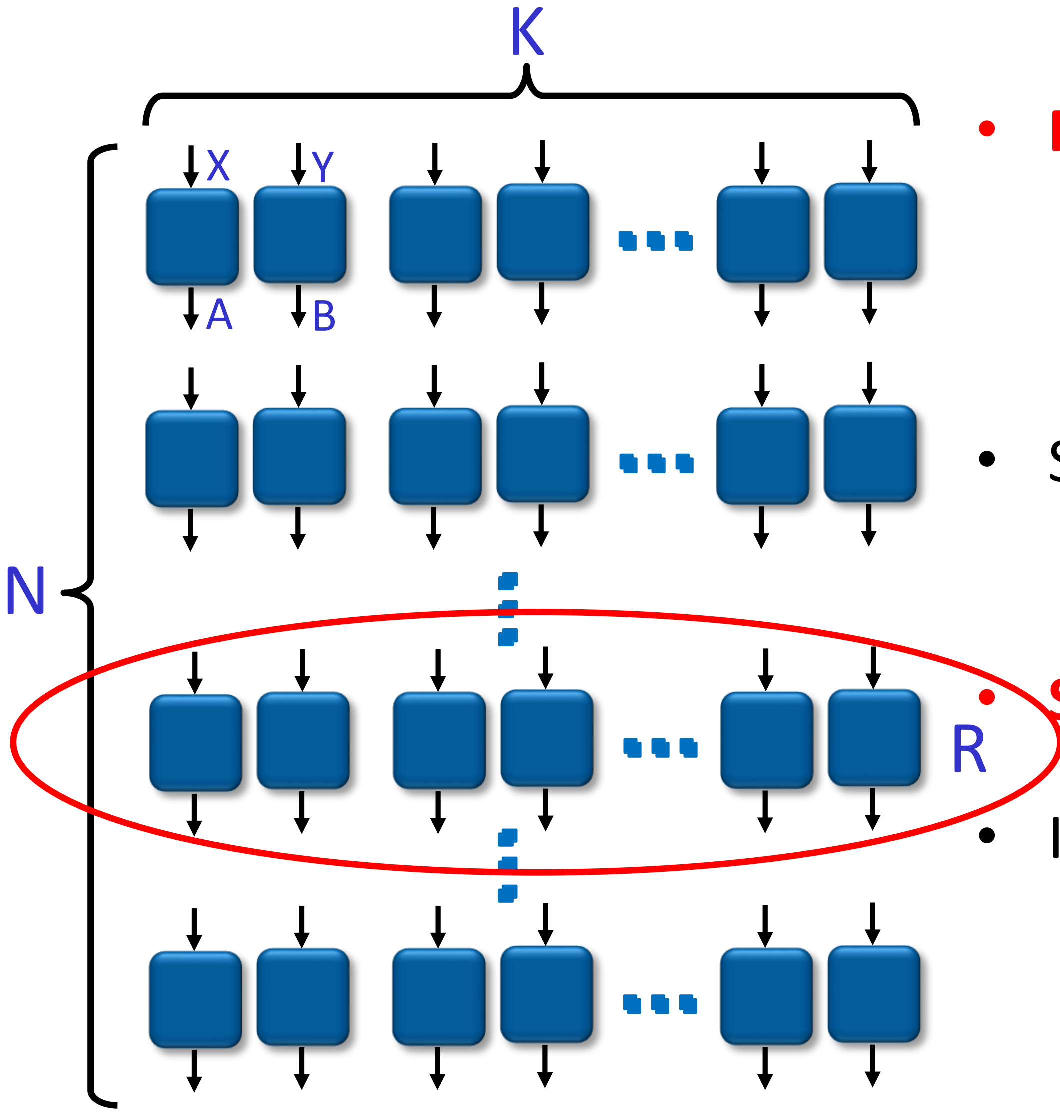
Achieved through an **imaginary post-selection** reduction!

To balance the error, # devices >= $2^{poly(1/\varepsilon)}$

# Handle almost uniform-to-Device sources

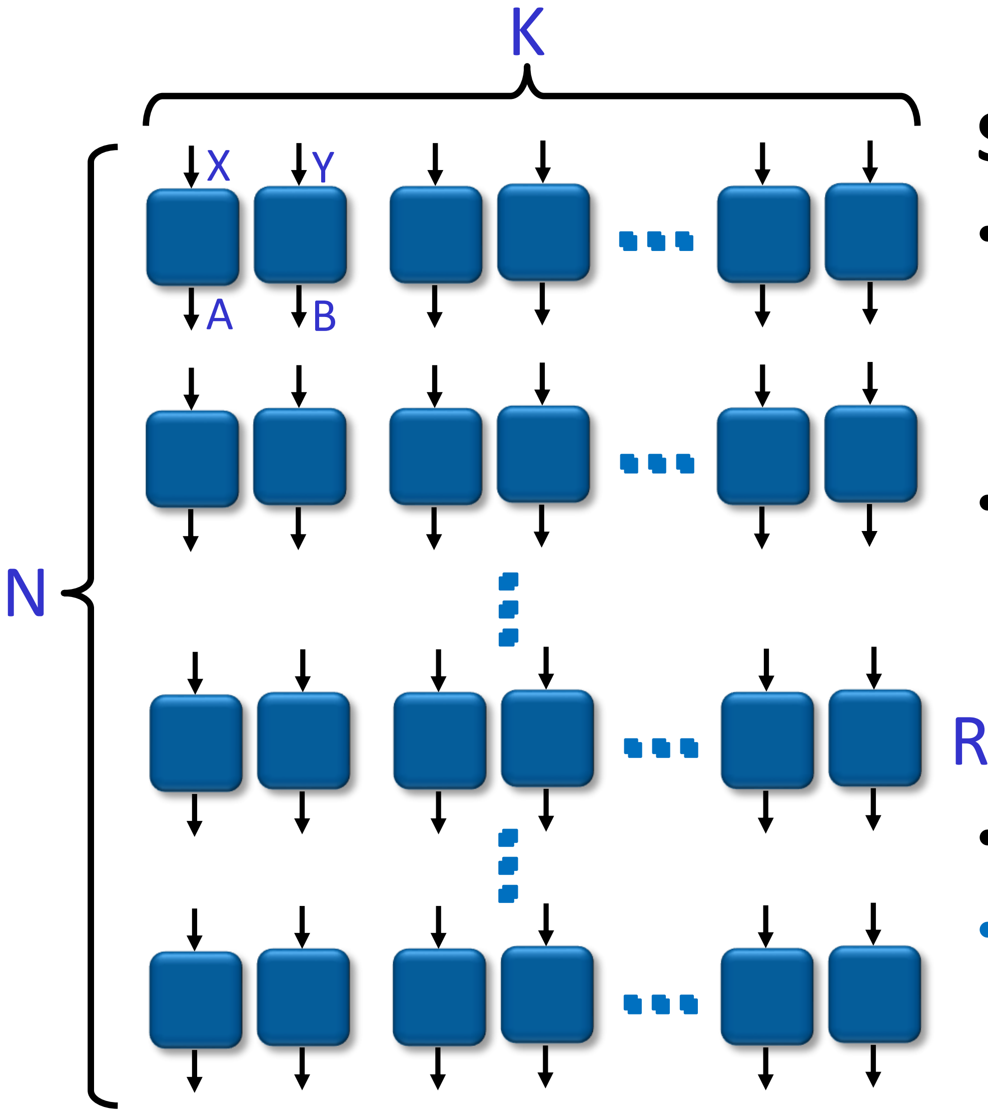
- Main challenge: local uniform & no independence
  - [CSW14] solved by the **Equivalence Lemma**
  - Unknown to hold in the NS setting.
- Previous NS-secure protocols
  - [BRG+13,RBH+15]: SV Source indep. of Device & Eve
  - [GMT+13]: SV Source indep. of Device
- Need to take [GMT+13] approach
  - Simplify and Modularize proof for **uniform sources**
    - Identify a key technical property for the analysis to go through
  - **Make it robust to a constant level of noises**
  - **Hash function: existential => efficiently generated**!

# Decoupler Construction




- Play BHK game N*K times
  - N rounds of $BHK^K$
  - Input alphabet size O(1)
- Select random **output** round R
  - Others are **testing** rounds
- Sample T-wise indep. hash H
- If **testing** rounds play "well"
  - Output $H(A_R)$

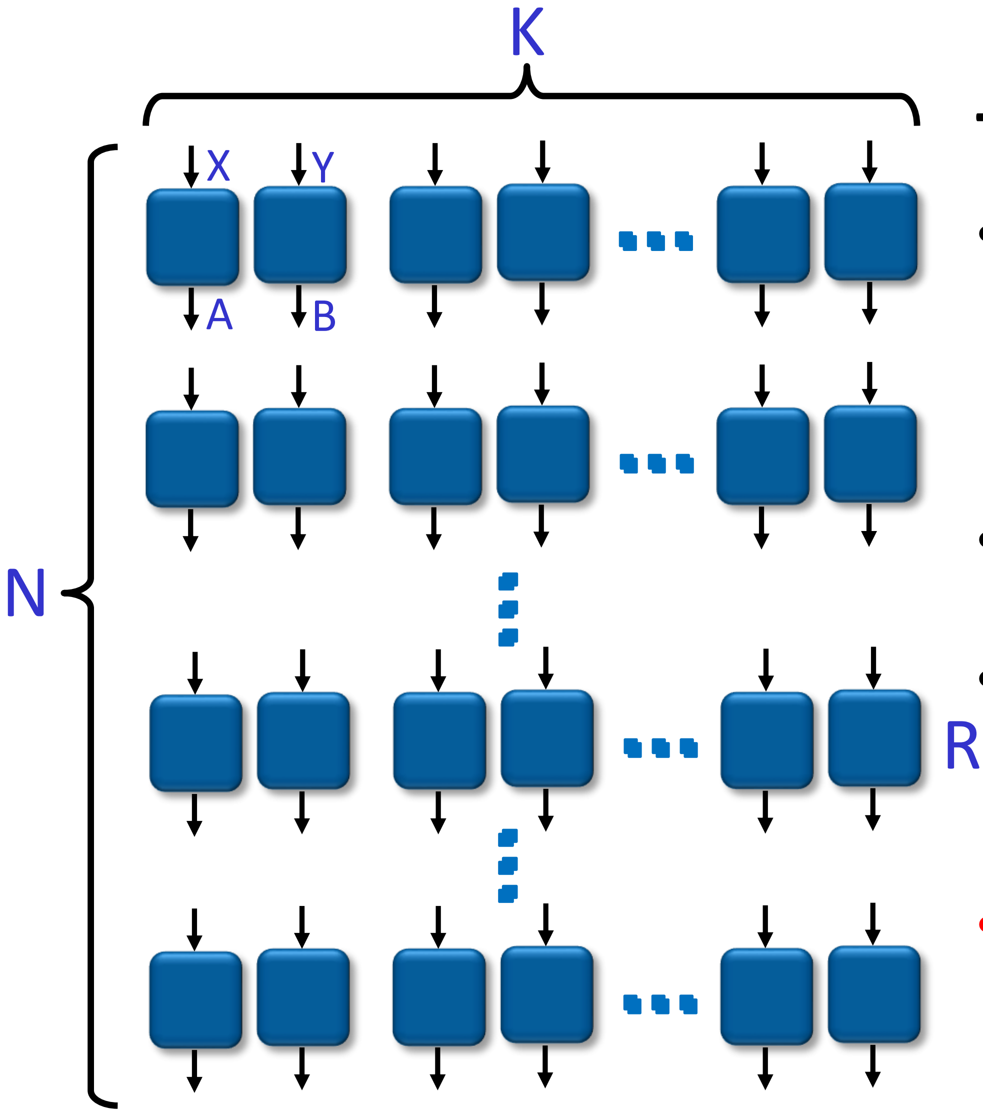
# Why Does It Work? (1)




**Strong monogamy**

- If Device play $\text{BHK}^{\text{K}}$ "well", then A must random-to-Eve (**monogamy**)
- Furthermore, for most H, H(A) close to uniform-to-Eve (**deterministic extraction**)
  - distance $\leq$ C$\cdot$ $\langle P_{AB|XY} | \text{BHK}^{\text{K}} \rangle$
- First done in [M09]
- **We make it explicit by T-wise independent hashing from uniform inputs**

# Why Does It Work? (2)



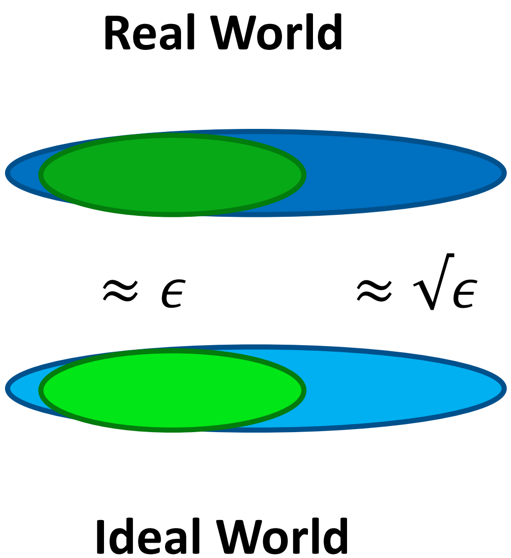

**Testing devices**

- Challenge: need to analyze $\langle P_{A_R B_R | X_R Y_R, \mathbf{Acc}} | \mathrm{BHK}^K \rangle$
  - since only output when Acc
- Bound it by $\langle P_{A_R B_R | X_R Y_R} | \mathrm{BHK}^K \rangle$.
- First done in [GMT+13] with complicated games for SV sources.
- **We make it robust to noise, and make proof simpler & modular.**

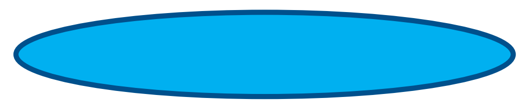
# Handle Close-to-Uniform Seeds

We over-simplify the condition:

we only have **locally** **close-to-uniform** seed




**Local** closeness -> **globally** close imaginary system

Does  always exist ?

**Quantum** Solution:

use fidelity and Ullman's theorem

**NS** Solution:

unknown, we believe **no black-box** solution (work in progress)

alternatively, we **repeat the analysis** with close-to-uniform seeds.

# Control error growth from local to global

- **Key Claim** in the analysis:

$$\Pr[\ \mathrm{Acc} \wedge \langle P_{A_R B_R | X_R Y_R, \mathbf{Acc}} | \mathrm{BHK}^{\mathrm{K}} \rangle \geq \gamma\ \ ] \leq \delta$$

- If claim is false when X is $\varepsilon$-close to uniform-to-Device

$$\Pr[\ \mathrm{Acc} \wedge \langle P_{A_R B_R | X_R Y_R, \mathbf{Acc}} | \mathrm{BHK}^{\mathrm{K}} \rangle \geq 2\gamma\ \ ] > 2\delta$$

=> **∃ D distinguish (X, Device) from U ⊗ Device w/ adv > $\varepsilon$**

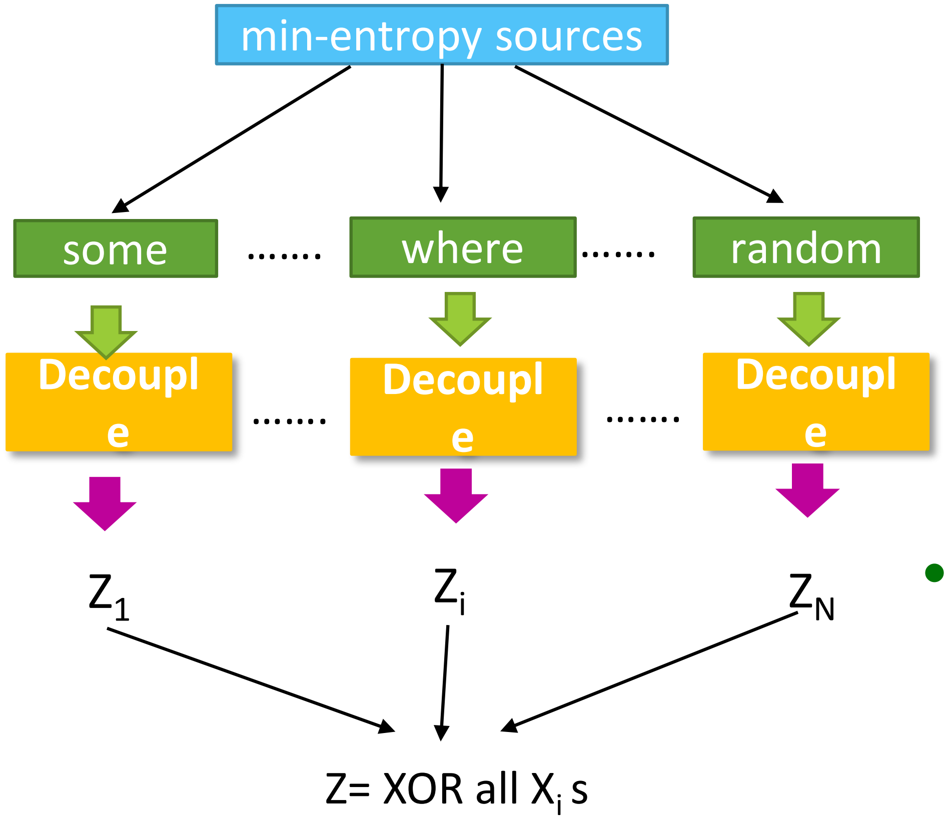
**(CS, Crypto) idea to construct an imaginary task (reduction)**

**Difficulty: probability of a property of the distribution itself**

- Thus, $\Pr[\ \mathrm{Acc} \wedge \langle P_{A_R B_R | X_R Y_R, \mathbf{Acc}} | \mathrm{BHK}^{\mathrm{K}} \rangle \geq 2\gamma\ \ ] \leq 2\delta$

and the rest of analysis goes through w/o much difficulty.

# Summary




- **Randomness amplification under minimal assumptions**
  - (Source|Device) has sufficient min-entropy
  - NS condition among Eve & Devices
  - *No* structural or independence assumptions about the source
- **Ideal dichotomy theorem**
  - Sufficient **local** uncertainty $\Longrightarrow$ certifiable global uniform rand.
  - poly($1/\varepsilon$) min-entropy $\Longrightarrow$ certify $\varepsilon$-close to uniform bits
  - Use $2^{\mathrm{poly}(1/\varepsilon)}$ devices

# Summary & Perspective

- Several (maybe generic) techniques for NS systems
  - Inspired by crypto techniques (composition & reduction)
  - e.g., somewhere random sources, error control in compositions
- **Open Questions**:
  - Improve or find tight examples for our analysis.
  - Improve the efficiency of our DI protocol, e.g. reduce the number of boxes
  - Find applications of these NS tools.
- **NS Information/Cryptography Theory**
  - NS security for DI-QKD, DI-randomness expansion
  - NS information theory.


Thank You...
Questions before jumping into the black holes…