NS-secure Physical Randomness Extractors, or Randomness Amplification for Weak Source

Kai-Min Chung

Academia Sinica & NCTU, Taiwan

Joint work with Yaoyun Shi, and Xiaodi Wu

Original Motivation from 90's

- Randomness is extremely useful resource
  - Randomized algorithm, Distributed algorithm, Cryptography,…
- Typically assume perfect uniform sources
  - Unbiased, independent random bits
  - Unrealistic strong assumption
- Can we weaken the assumption?
  - Use unstructured weak sources with min-entropy

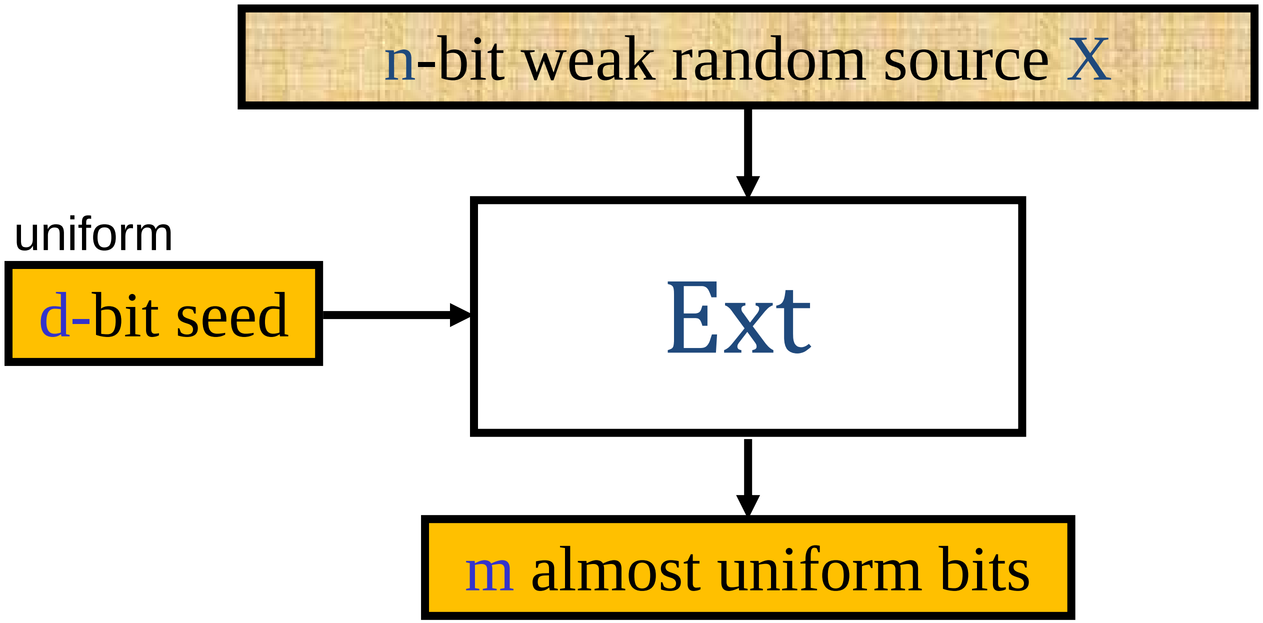
Randomness Extraction Paradigm

- Extract uniform randomness from weak random sources
  - Source = classical distribution over $\{0,1\}^n$
  - Correlated and biased (unstructured), guarantee min-entropy

- Impossible given a single such source
  - Even with $n-1$ bits of entropy

Classical Seeded Extractors [NZ96]

- Add *short* uniform seed as catalyst for extraction



(k,ε)-extractor*:*

X has $\geq k$-bits min-entropy

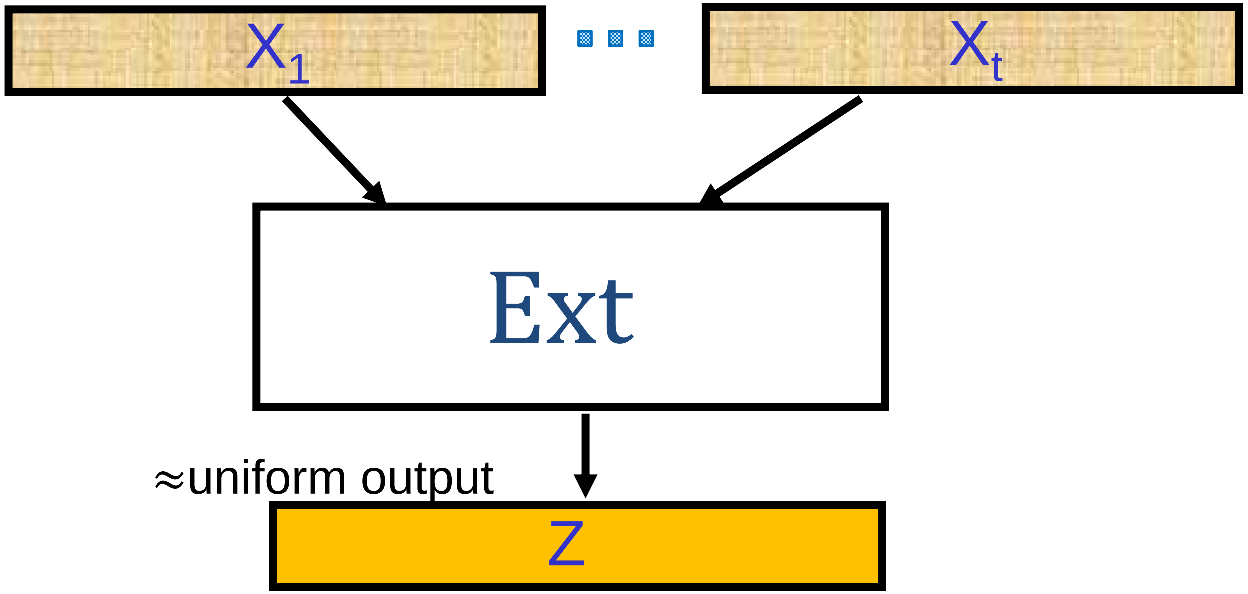
$\Longrightarrow$ $\text{Ext}(X,U_d)$ ε-close to uniform

Pervasive Applications

- Diverse topics in Theoretical Computer Science
  - Cryptography, Derandomization [Sis88, NZ93,…], Distributed algorithms [WZ95], Data structures [Ta02], Hardness of Approximation [Zuc93,…]
- Many applications in Cryptography
  - Bounded-storage model [Lu02,V03], PRG [HILL89], Biometrics [DRS04], Leakage-resilient crypto [DP09]…
- Also in Quantum Cryptography
  - Privacy amplification [BBR88], Randomness expansion, Physical randomness extractors,…

Avoiding Uniform Seed

- Multi-source extractor: use multiple *indep.* sources

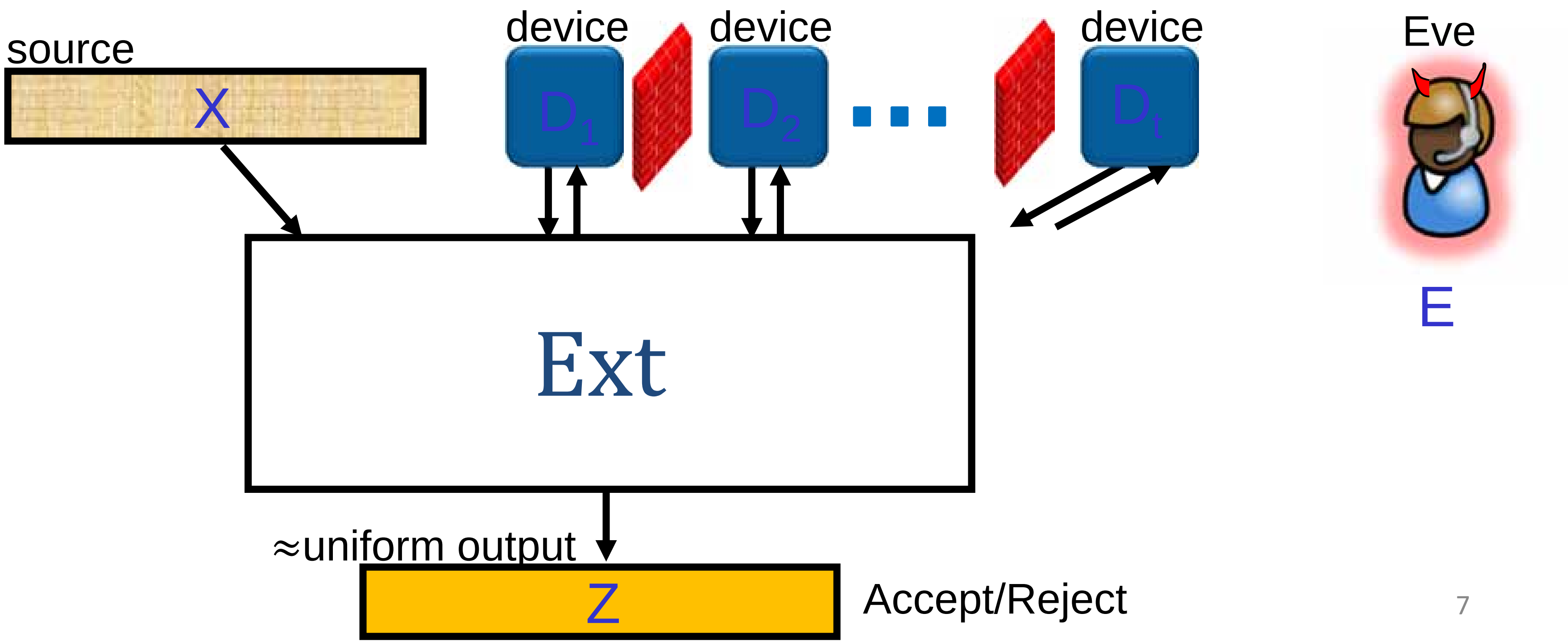


(t,k,ε)-multi-source extractor*:*

X_i has $\geq k$-bit entropy $\Longrightarrow$ $Ext(X_1,\ldots,X_t)$ ε-close to uniform

Can We Remove *Independence*?

- Cannot be verified & don't know how to guarantee
- Device-independent Extractors
  - Extract randomness from physical sources without trust

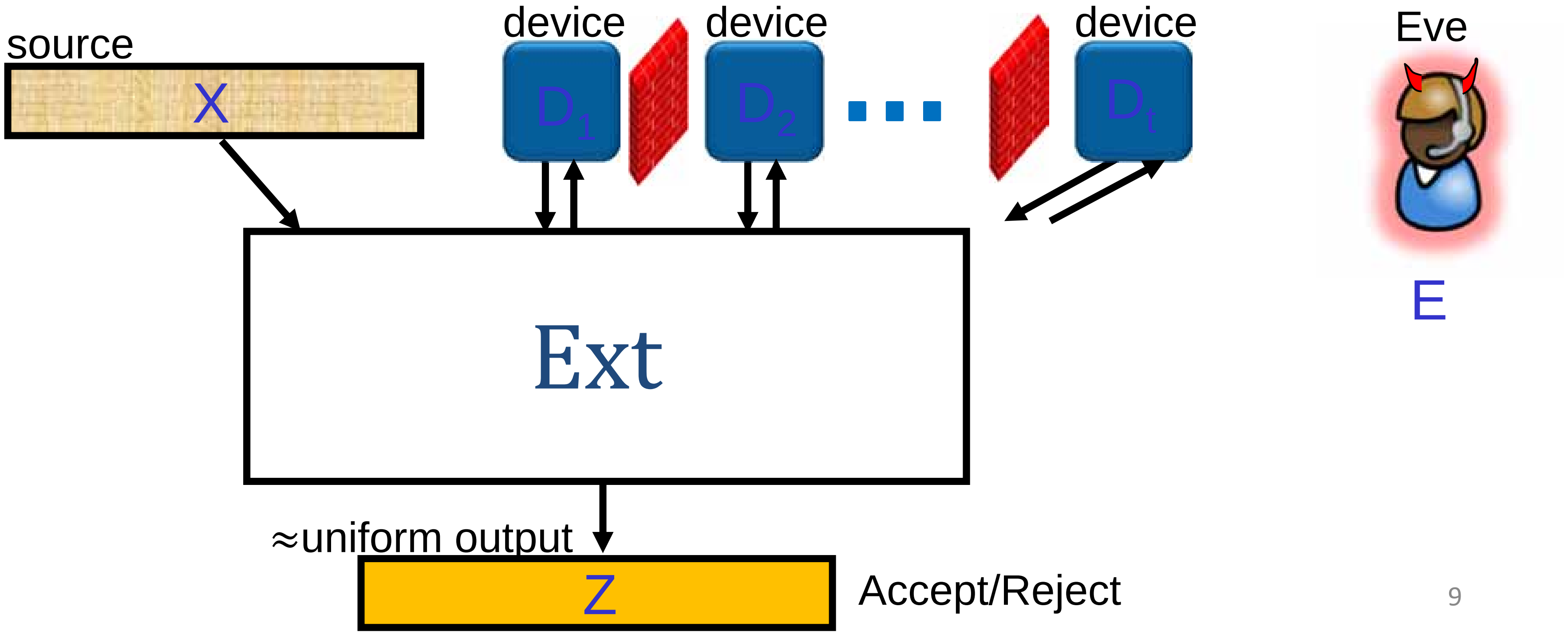


Can We Remove *Independence*?

- Cannot be verified & don’t know how to guarantee
- Device-independent Extractors
  - Extract randomness from physical sources without trust
  - Randomness expansion: seeded setting
    - Still require uniform seed and independence
  - Randomness amplification: Santha-Vazirani (SV) source
    - Structured source with high min-entropy
    - Require source-device conditional independence
- Does randomness extraction remain feasible without any *independence* or *structural* assumptions?

Physical Randomness Extractor (PRE)

- DI extraction for *general* weak source
- *Quantum-secure* PRE [CSW14]
  - Only require O(1) bits min-entropy; minimal assumptions!
- *No-signaling*-secure PRE [CSW15]
  - Physics motivation [CR12,GMT+13]: a dichotomy theorem



Dichotomy Theorem [CR12,GMT+13]

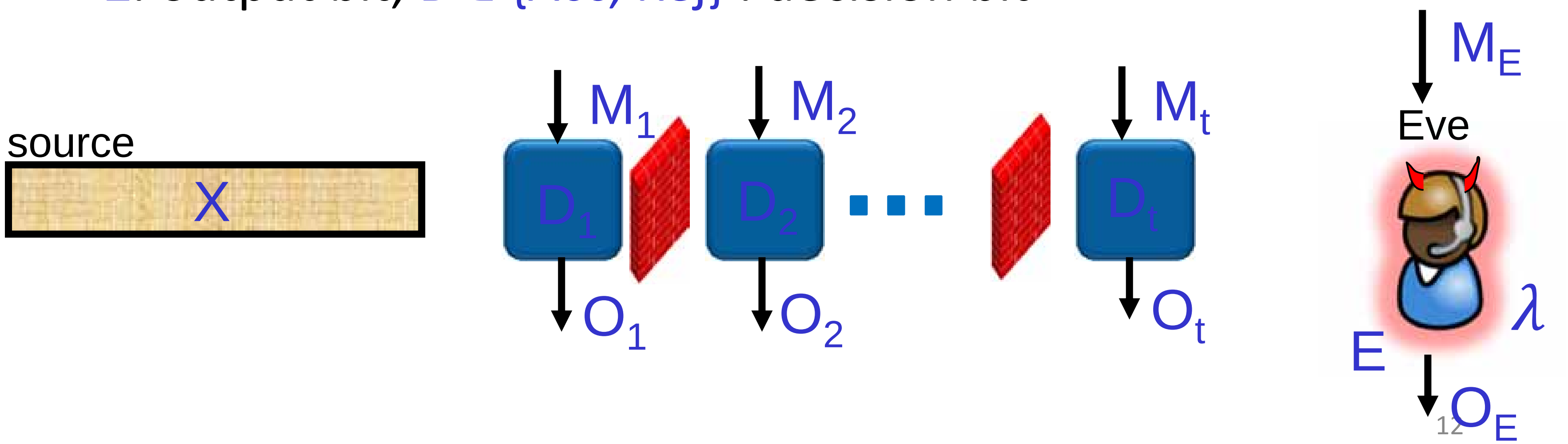
- Can we certify our physical world is random?
  - NO if the world is fully deterministic
- Dichotomy: either deterministic, or certifiably random
  - "Not fully deterministic"

    $\Longrightarrow$ $\exists$ certification procedure for truly random events
  - Do not want to assume quantum mechanics
  - Do not want to assume independence
- NS-secure PRE = cert. procedure assuming NS condition
  - "Not fully deterministic" = $\exists$ unstructured min-entropy source
- Randomness amplification (SV source) [CR12,GMT+13,BRG+13,RBH+15]
  - "Not fully deterministic" = structured, per-bit uncertainty with conditional independence

NS-secure PRE: The Model

The Model

- Source-Device-Eve system: $P_{XO_1\ldots O_tO_E|\perp M_1\ldots M_tM_E}$
  – Only model one-time use of the devices
- Assumptions:
  – $P_{XO_1\ldots O_tO_E|\perp M_1\ldots M_tM_E}$ is no-signaling.
  – (X|Device) has k-bit min-entropy: $P_{guess}(X|Device) \leq 2^{-k}$
- Output-Source-Eve system: $P_{ZBXO_E|\perp\perp\perp M_E}$
  – Z: output bit, B ∈ {Acc, Rej} : decision bit

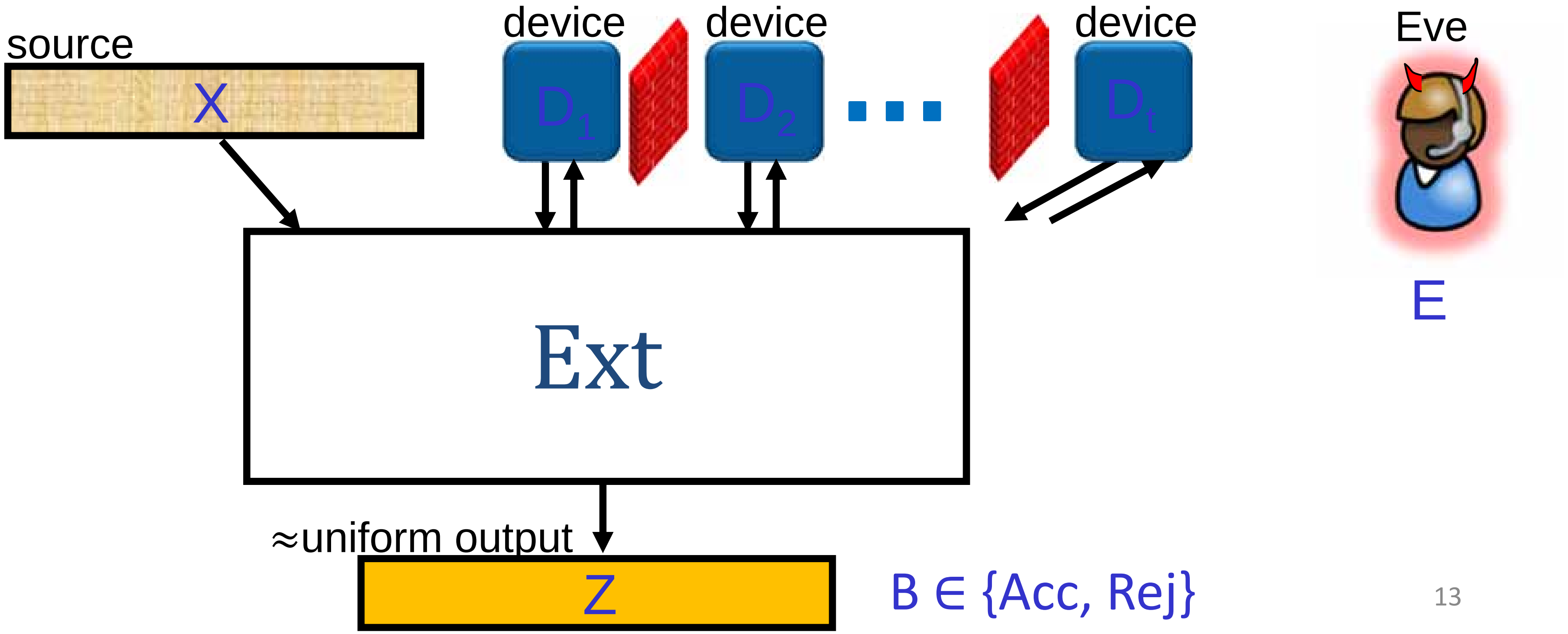


(k,ε)-NS-secure PRE

- Completeness: accept honest devices with high prob.
- Soundness: For any $P_{XO_1\ldots O_tO_E|\perp M_1\ldots M_tM_E}$
  - (X|Device) has $\geq$ k-bits min-entropy

    $\Longrightarrow$ Z is ε-close to uniform-to-(X,Eve):

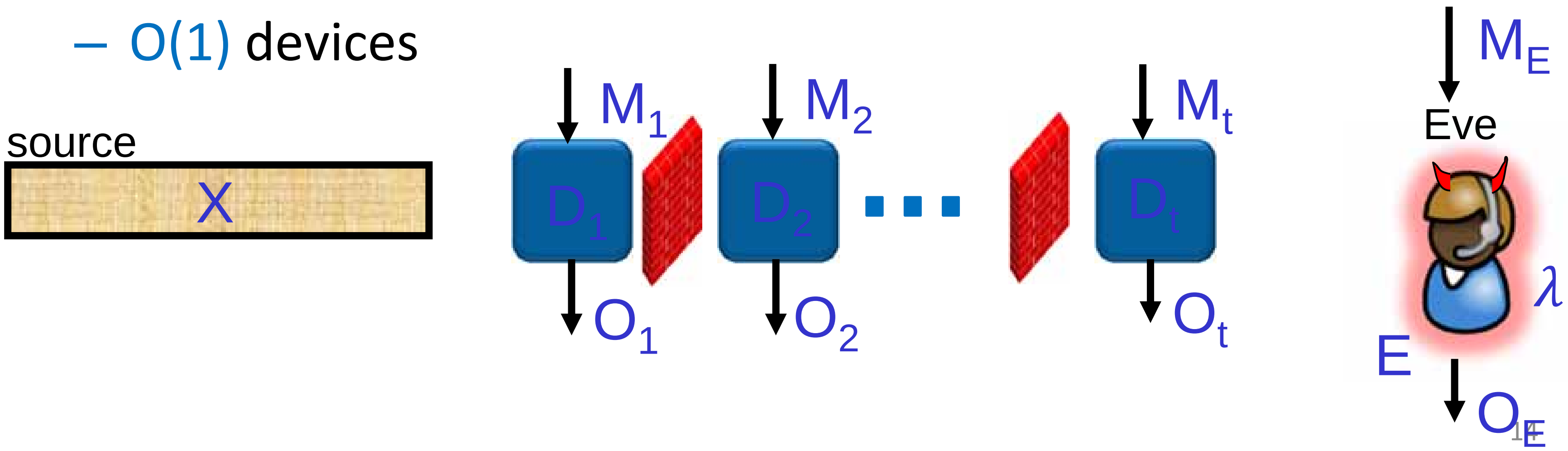
i.e., $P_{ZBXO_E|\perp\perp\perp M_E}$ and $\mathrm{P}^{\mathrm{Ideal}}_{Z'BXO_E|\perp\perp\perp M_E}$ are ε-close



Comparison of the Models

- Colbeck, Renner [CR12]
  - high quality SV; no independence requirement, i.e.,

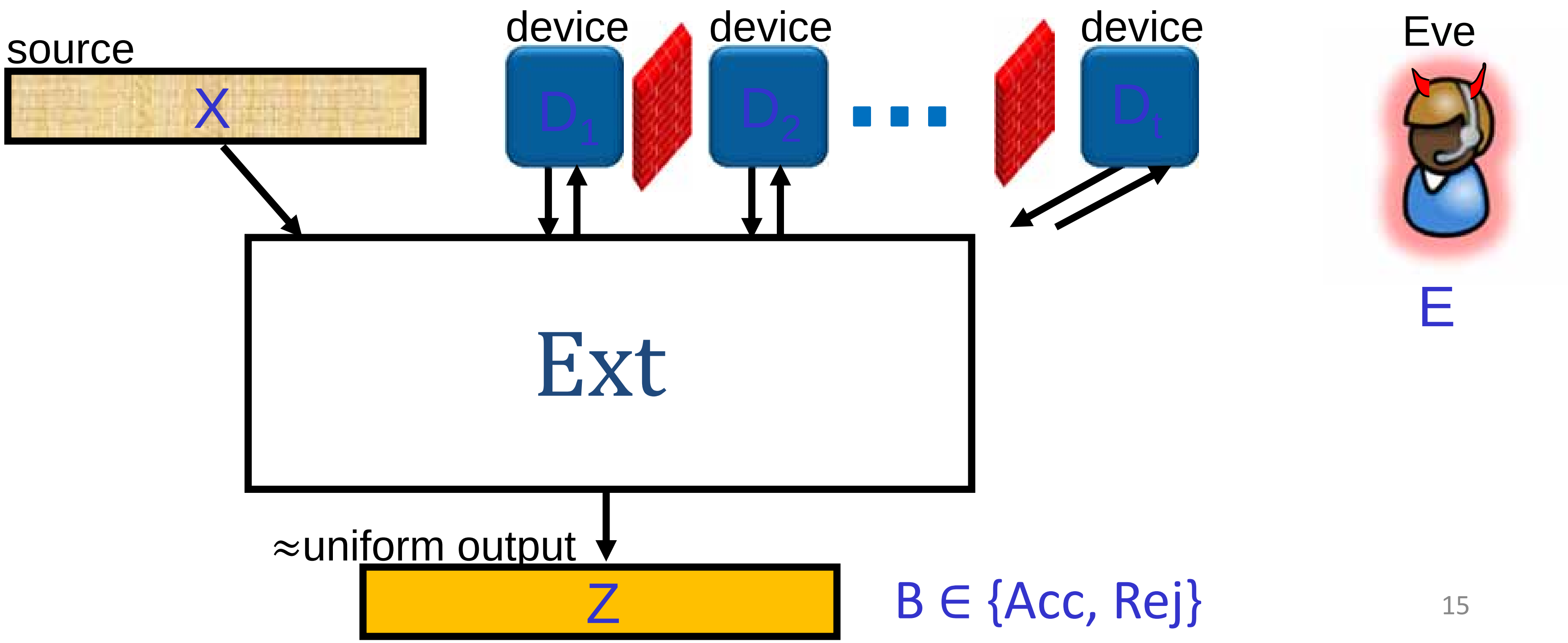
    $P_{guess}(X_i | \text{Device}, X_1{=}x_1,\ldots,X_{i-1}{=}x_{i-1}) < 0.558 \qquad \forall\, x_1,\ldots,x_{i-1}$
- Gallego *et. al.* [GMT+13]
  - need *cond. independence* between Source & Device
  - handle any SV
- Brandão *et. al.*, Ramanathan *et. al.* [BRG+13,RBH+15]
  - need *cond. independence* between Source & (Device + Eve)
  - O(1) devices



Our Results

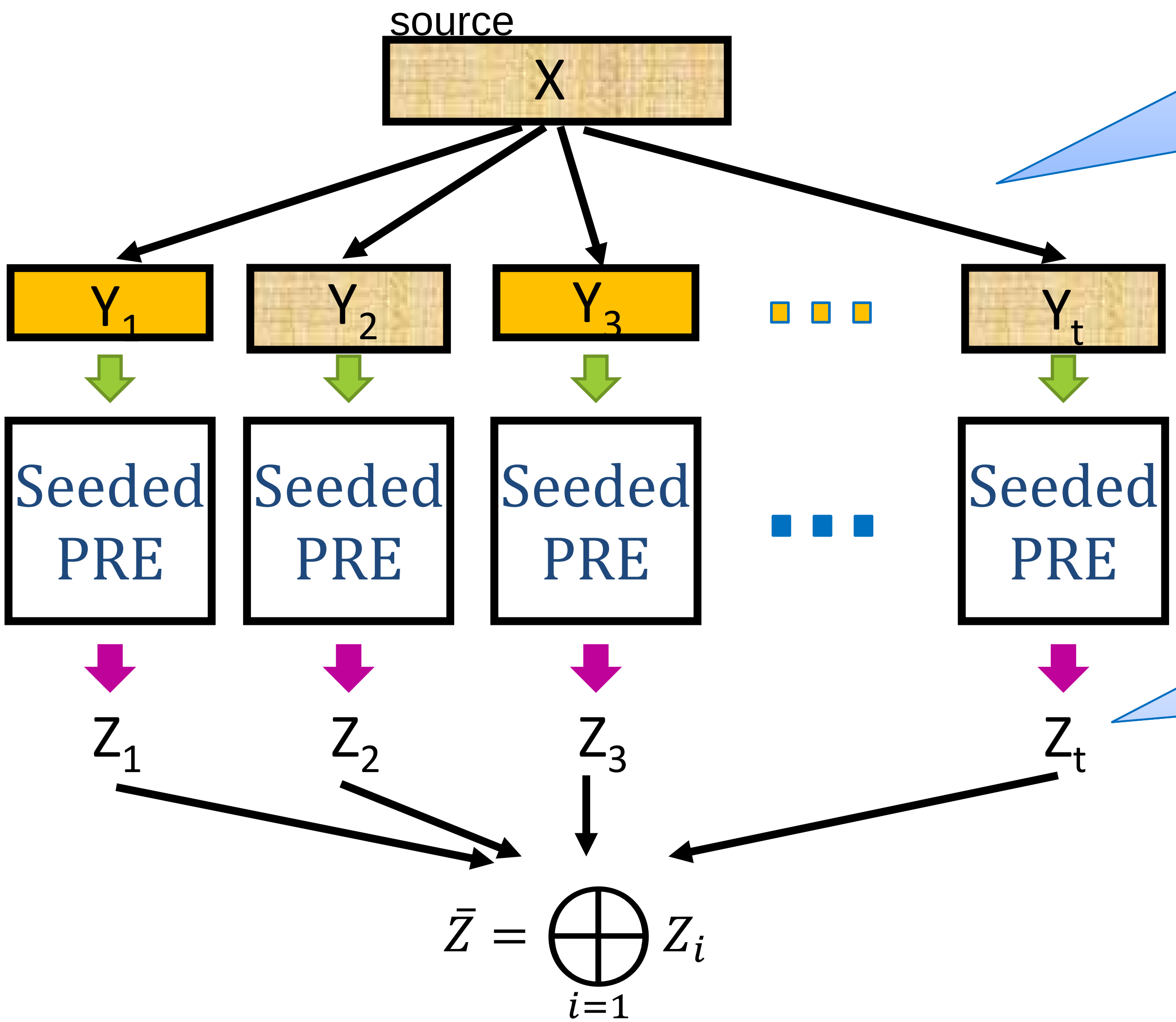
- We construct (k,ε)-NS-secure PRE for any $\varepsilon > 0$ with
  - min-entropy $k = \mathrm{poly}(1/\varepsilon)$
  - # devices = $2^{\mathrm{poly}(1/\varepsilon)}$
  - Robust: accept w.h.p. even

World record high!
OK for Dichotomy Thm



Our Construction

Our Approach: Make Source *Uniform* First!



use strong seeded extractor $Y_i = \mathrm{Ext}(X,i)$

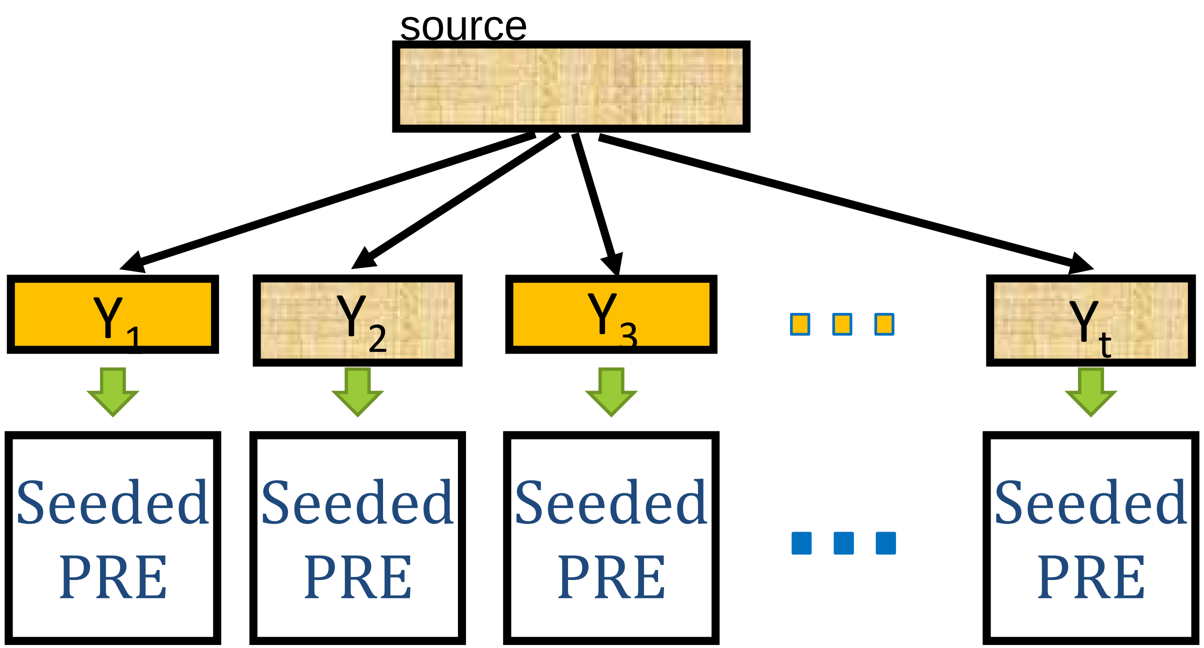
somewhere uniform but *correlated*

acts as *decoupler*

Some Z_i is uniform-to-*all*

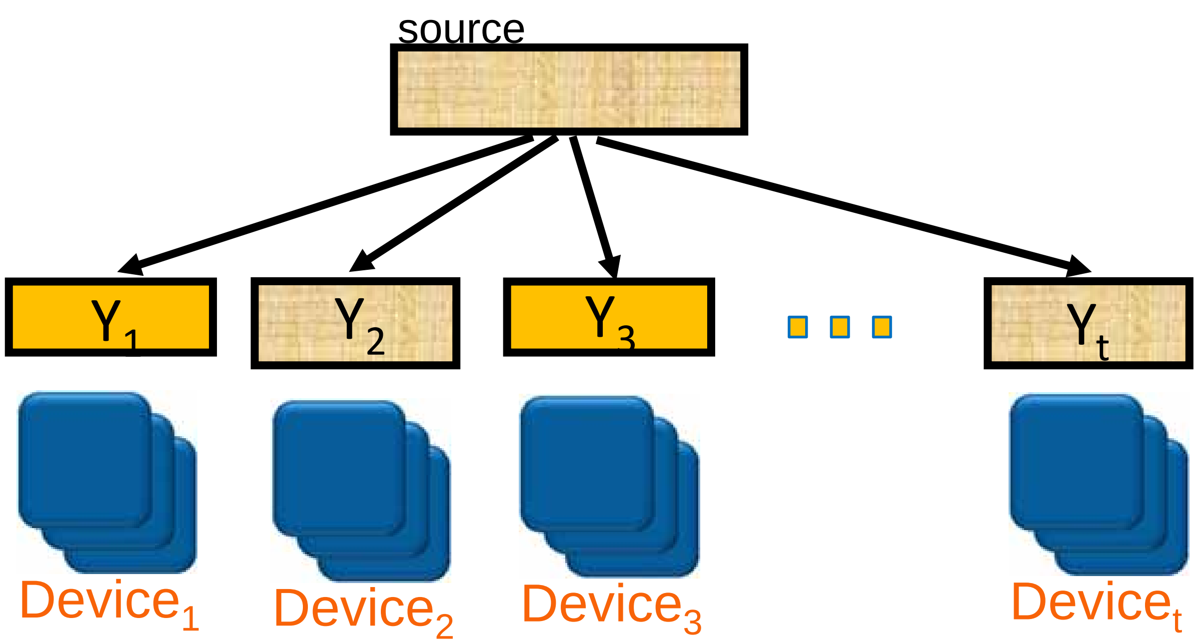
XOR $\Longrightarrow$ uniform output

Challenge 1: Somewhere Uniform Source



Challenge 1: Somewhere Uniform Source

- Need: some Y_i is close to uniform-to-*$Device_i$*
- Quantum security:
  - Use quantum-proof strong seeded extractor: $Y_i = Ext(X,i)$
  - $\exists$ i s.t. Y_i is ε-close to uniform-to-*all-Device*



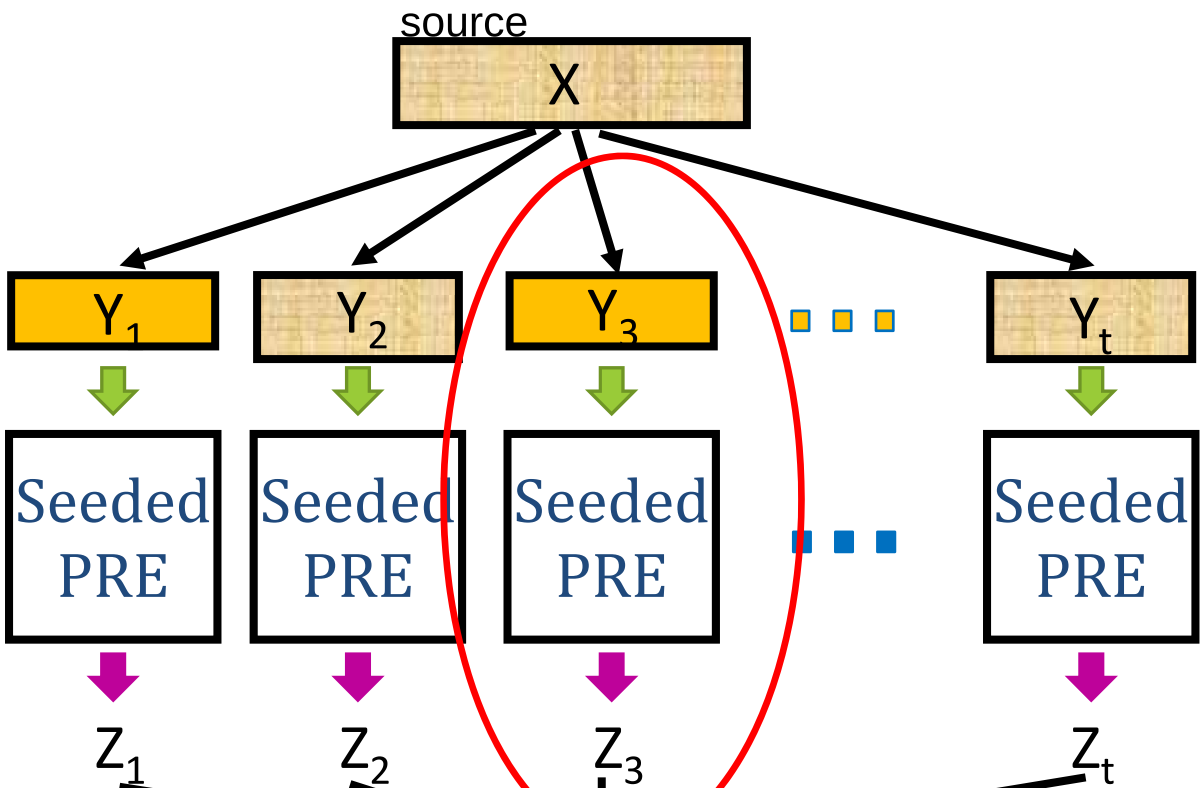
Challenge 1: Somewhere Uniform Source

- Need: some Y_i is close to uniform-to-*$Device_i$*
- Quantum security:
  - Use quantum-proof strong seeded extractor: Y_i = Ext(X,i)
  - ∃ i s.t. Y_i is ε-close to uniform-to-*all-Device*
- NS security:
  - "NS-proof" strong seeded extractor does **NOT** exist!
    - ∃ source $P_{X\mathrm{O_E}|\perp\mathrm{M_E}}$ with (n-1)-bit min-entropy s.t. all extractors fails
  - Still, *classical* strong extractor $\longrightarrow$ NS somewhere uniform source!
  - ∃ i s.t. Y_i is $(2^m \cdot \varepsilon)$-close to uniform-to-*$Device_i$*

Challenge 2: Seeded PRE as Decoupler

- Need: If Source is uniform-to-Device,

  then Output is uniform-to-all-but-Device



$$\bar{Z} = \bigoplus_{i=1} Z_i$$

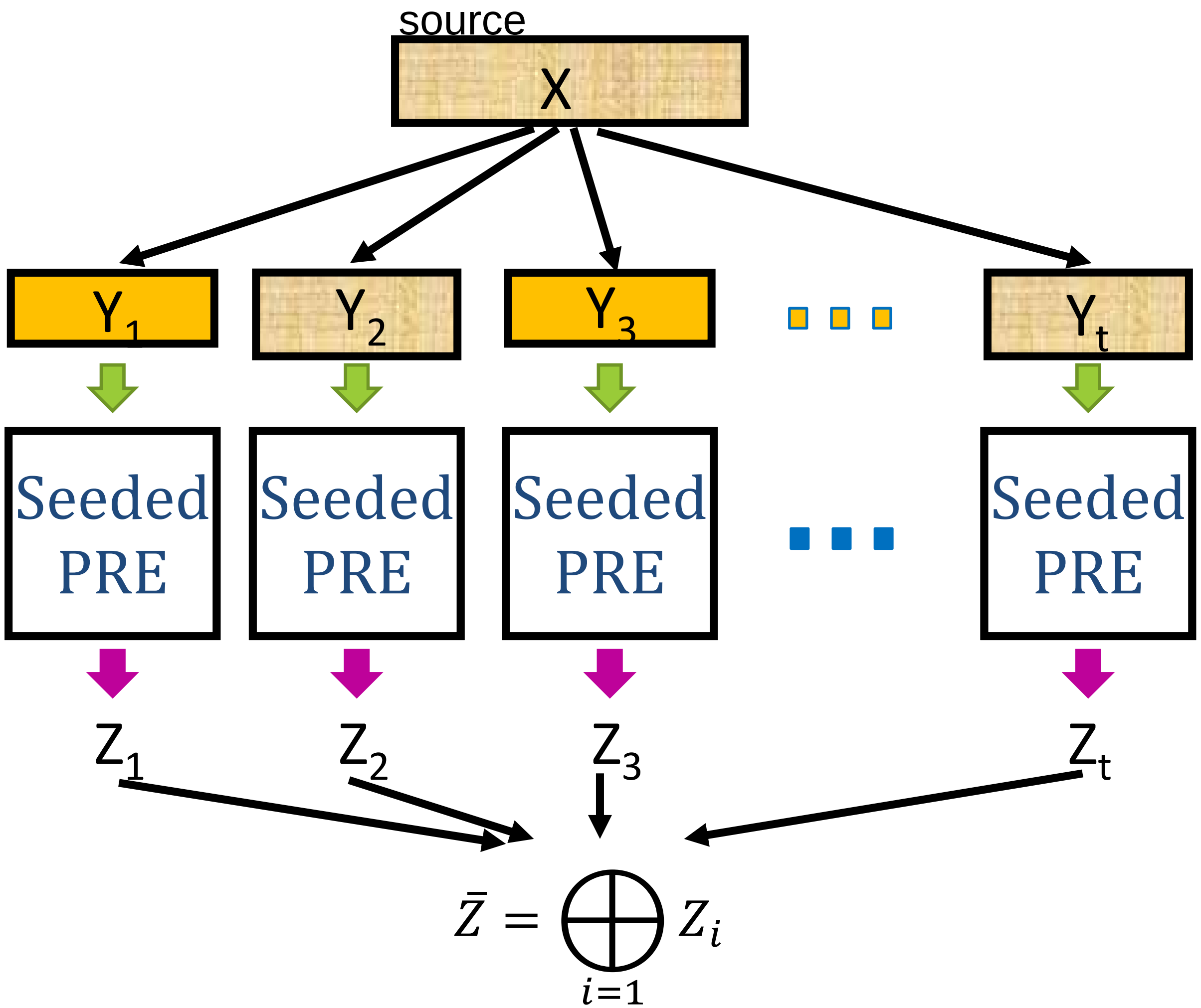
Challenge 2: Seeded PRE as Decoupler

- Need: If Source is uniform-to-Device,

  then Output is uniform-to-all-but-Device
- Quantum security:
  - Equivalence lemma: *any* randomness expansion protocol is a good decoupler
- NS security:
  - No equivalence lemma
  - Use randomness amplification protocol of [GMT+13]
    - But not robust and not explicit
  - We make it robust and explicit in seeded setting
    - Simplify and modularize the proof

Challenge 3: Composition

- Somewhere uniform Y_i only ε-close to uniform-to-*Device*$_i$



Challenge 3: Composition

- Somewhere uniform Y_i only ε-close to uniform-to-*Device*$_i$
- Quantum security:
  - Handled by a standard fidelity trick
- NS security:
  - No fidelity trick
  - Look into our seeded PRE construction and analysis
  - Show: if *analysis fails*, then ∃ distinguisher w/ advantage $> \varepsilon$

Somewhere Uniform Source

Somewhere Uniform from Classical Ext

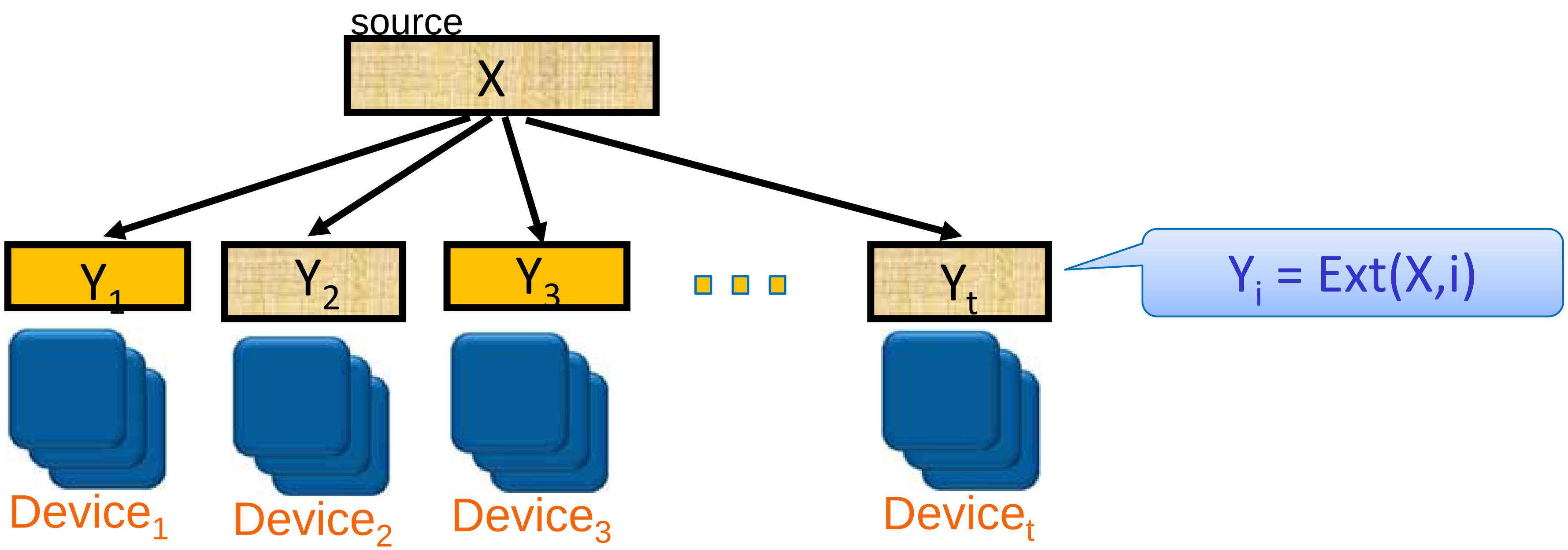
Thm: If Ext is classical (k,ε)-strong seeded extractor, and

(X|Device) has k-bits min-entropy,

Then ∃ i s.t. Y_i is $(2^m \cdot \varepsilon)$-close to uniform-to-*Device*$_i$`

Proof: Let $P_{XO_1\ldots O_t|\perp M_1\ldots M_t}$ denote the Source-Device system.

– Suppose Thm is false, then ∀ i, ∃ distinguisher D_i s.t.
  - D_i distinguishes $P_{Y_iO_i|M_i}$ from $P_U \otimes P_{O_i|M_i}$ with advantage $> 2^m \cdot \varepsilon$



Somewhere Uniform from Classical Ext

Thm: If Ext is classical (k,ε)-strong seeded extractor, and

(X|Device) has k-bits min-entropy,

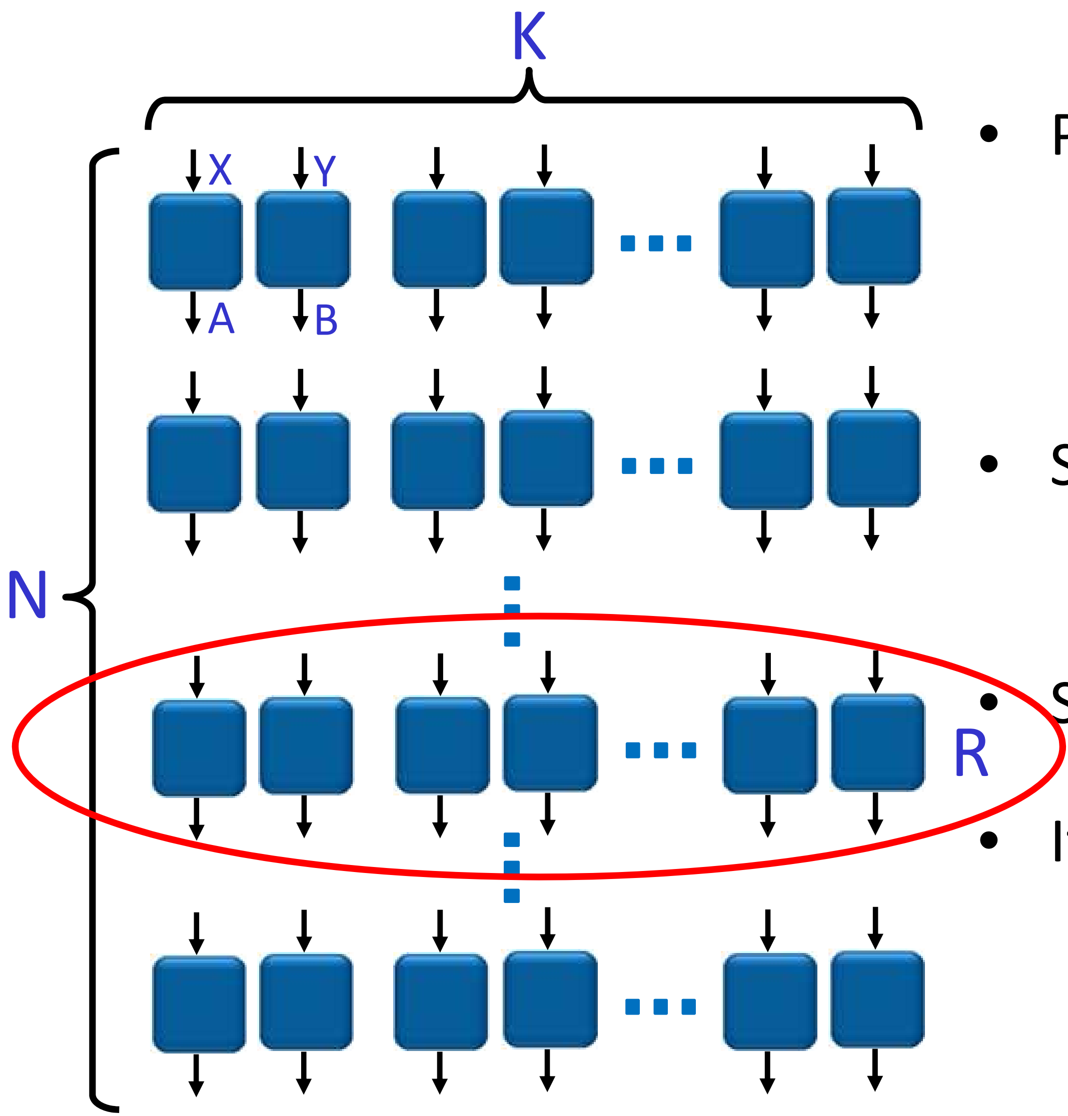
Then ∃ i s.t. Y_i is $(2^m \cdot \varepsilon)$-close to uniform-to-*Device*$_i$.

Proof: Let $P_{XO_1 \ldots O_t | \perp M_1 \ldots M_t}$ denote the Source-Device system.

- Suppose Thm is false, then ∀ i, ∃ distinguisher D_i s.t.
  - D_i distinguishes $P_{Y_i O_i | M_i}$ from $P_U \otimes P_{O_i|M_i}$ with advantage $> 2^m \cdot \varepsilon$
  - Here, D_i can choose measurement M_i *depending* on Y_i / U
- By a post-selection argument, ∀ i, ∃ distinguisher D'_i s.t.
  - D'_i distinguishes $P_{Y_i O_i | M_i}$ from $P_U \otimes P_{O_i|M_i}$ with advantage $> \varepsilon$
  - D'_i chooses measurement M_i *independent* of Y_i / U
- $\{D'_i\}$ as guessing strategy G(Device) ⟶ classical distribution O
  - (X|O) has k-bits min-entropy, so $E_i[\ |P_{Y_i O} - P_U \otimes P_O|] \leq \varepsilon$
- This is a contradiction!

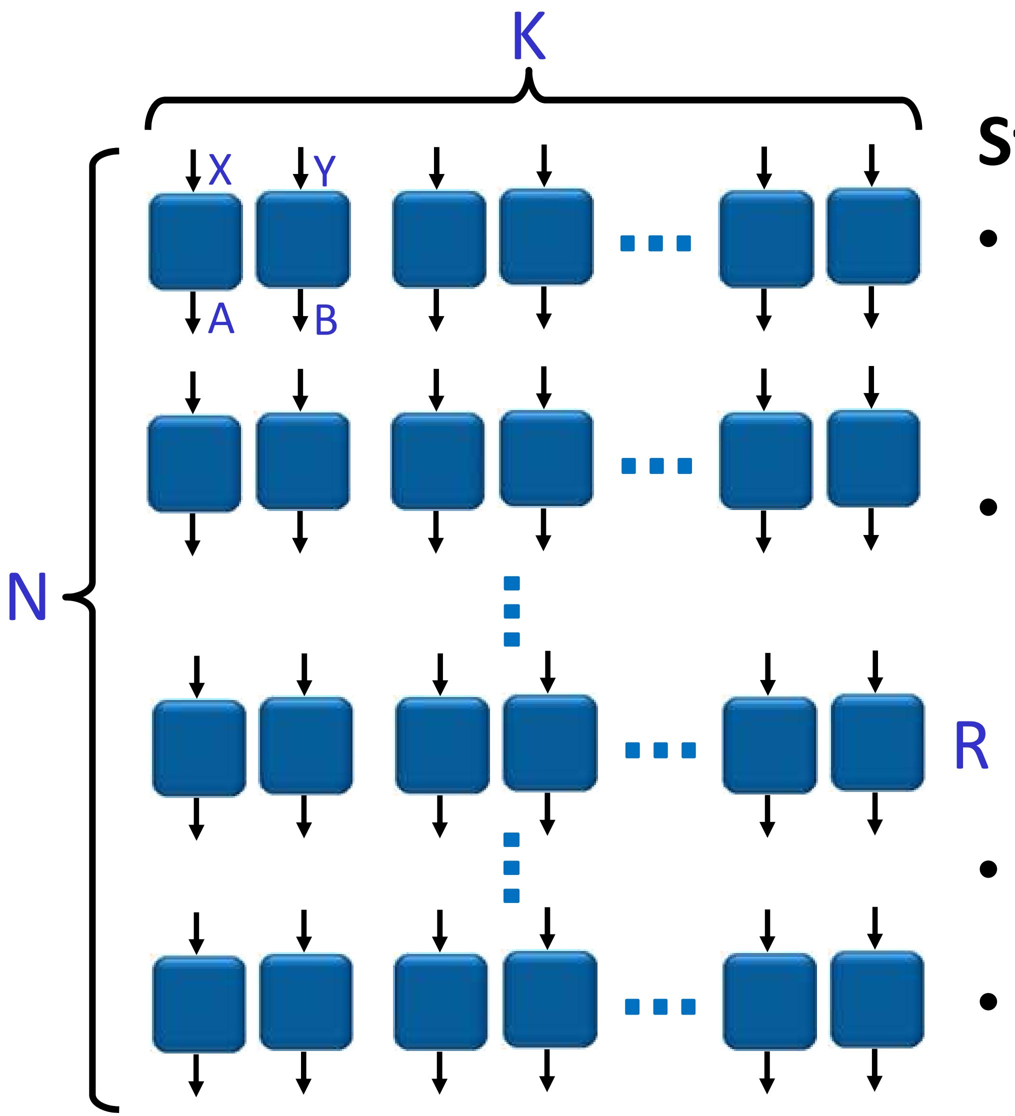
Seeded PRE as Decoupler

Construction Overview



- 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 $H(A_R)$

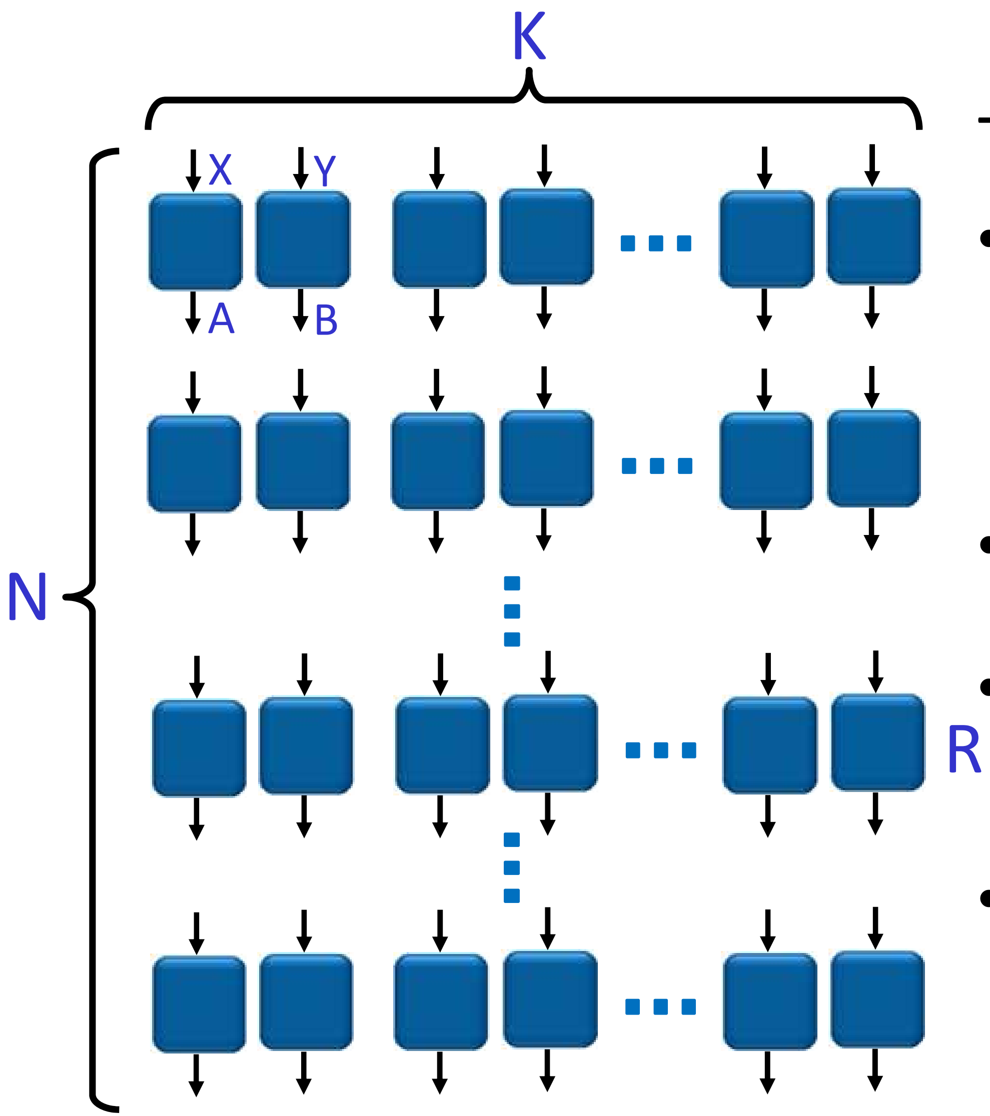
Why Does It Work? (1)



Strong monogamy

- If Device play BHK^{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$\cdot$ $\langle P_{AB|XY} | \mathrm{BHK}^{K} \rangle$
- Need to use different devices!
- First done in [M09], we make it explicit by T-wise indep hash

Why Does It Work? (2)



Testing devices

- Challenge: need to analyze $\langle P_{A_R B_R | X_R Y_R, \mathbf{Acc}} | \mathrm{BHK}^{\mathrm{K}} \rangle$
  - since only output when Acc
- Bound it by $\langle P_{A_R B_R | X_R Y_R} | \mathrm{BHK}^{\mathrm{K}} \rangle$
- Need to use different devices!
  - Use NS condition among rounds.
- First done in [GMT+13] we make it robust, and make proof simpler & modular

Composition:
Handle Close to Uniform Seed

Handle Close to Uniform Seed

- Key claim in the analysis of seeded PRE:

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

- If claim is false when X is ε-close to uniform-to-Device

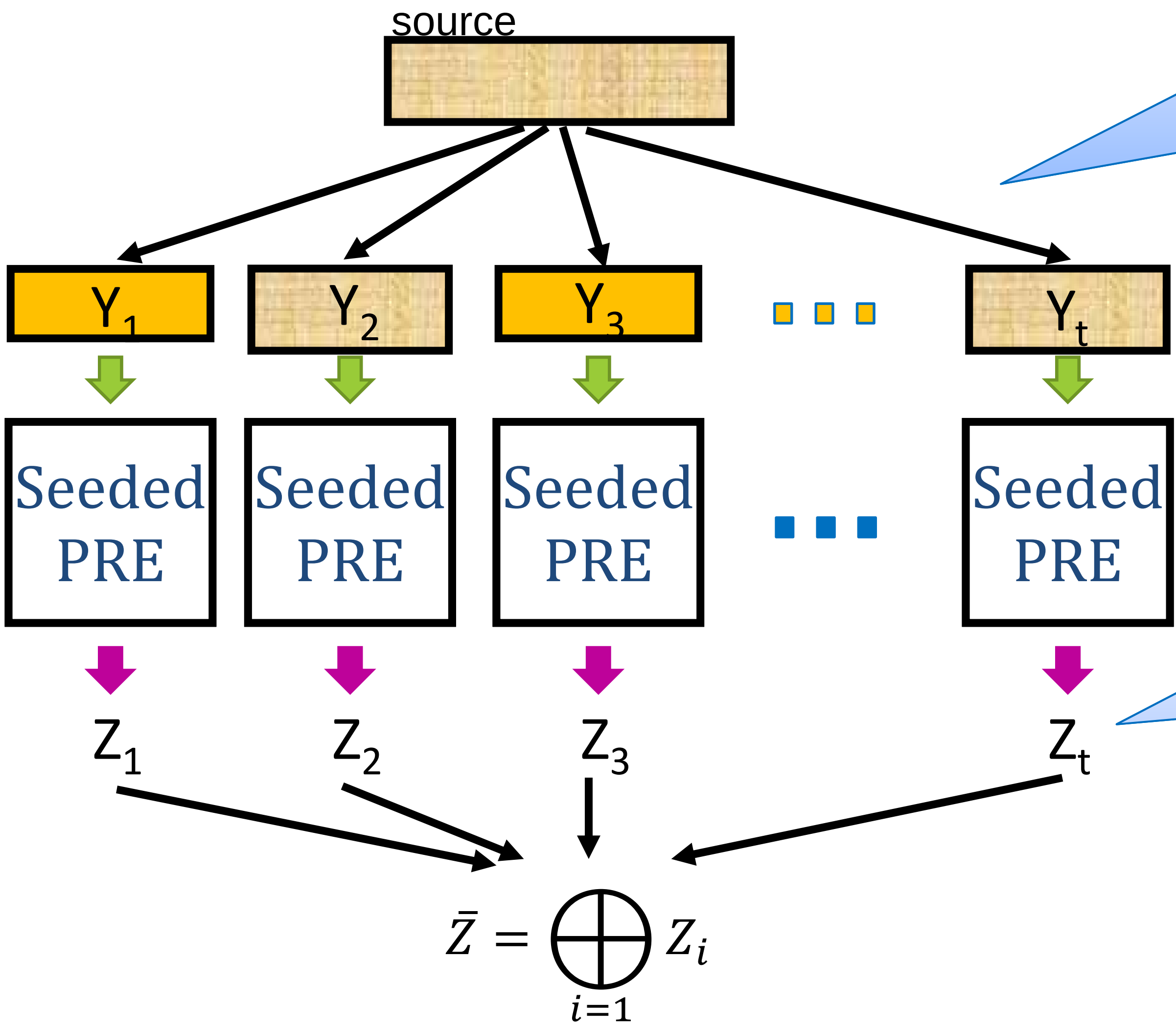
$$\Pr[\ \mathrm{Acc} \wedge \langle P_{A_R B_R | X_R Y_R, \mathbf{Acc}} | \mathrm{BHK^K} \rangle \geq 2\gamma \quad] > 2\varepsilon$$

then ∃ D distinguish (X, Device) from U ⊗ Device w/ adv > ε

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

and the rest of analysis go through.

Put Things Together



use strong seeded extractor $Y_i = \mathrm{Ext}(X,i)$

somewhere uniform but *correlated*

acts as *decoupler*

Some Z_i is uniform-to-*all*

XOR $\Longrightarrow$ uniform output

On the Number of Devices

- Need exponential number of devices
  - In seeded PRE, need seed length $m = 1/\text{poly}(\varepsilon)$
  - # somewhere uniform blocks $\geq 2^m$
    - since we need classical seeded extractor with error $\varepsilon/2^m$

  $\Longrightarrow$ need $2^{1/\text{poly}(\varepsilon)}$ devices

- Can we do better?
  - $1/\text{poly}(\varepsilon)$ devices assume Source-Device independence
  - $\omega(1)$ devices needed for "non-adaptive" protocols (on going work)

Open Problems

- Better NS-secure PRE / randomness amplification
  - General source, no independence, 1/poly(ε) devices?
  - SV source, no independence, O(1) devices?
  - NS-secure randomness expansion?
- PRE with negligible error
  - Important for crypto applications
  - Only known for randomness expansion [MS14]
  - Open even for SV source with quantum security

- Can we certify independence w/o cert. uniform?

Crypto against Quantum Side-Info: Randomness Extraction in Malicious Setting

- Many crypto tasks can be viewed as randomness extraction in malicious settings
  - Seeded and multi-source extractors
  - Privacy amplification, non-malleable extractors
  - Network extractors
  - Leakage-resilient cryptography, etc

- Can we achieve security against quantum side info

We welcome visitors!

AQIS 2016 in Taiwan

16th Asian Quantum Information Science Conference

Academia Sinica, Taipei, Taiwan

Aug 29 - Sep 2, 2016

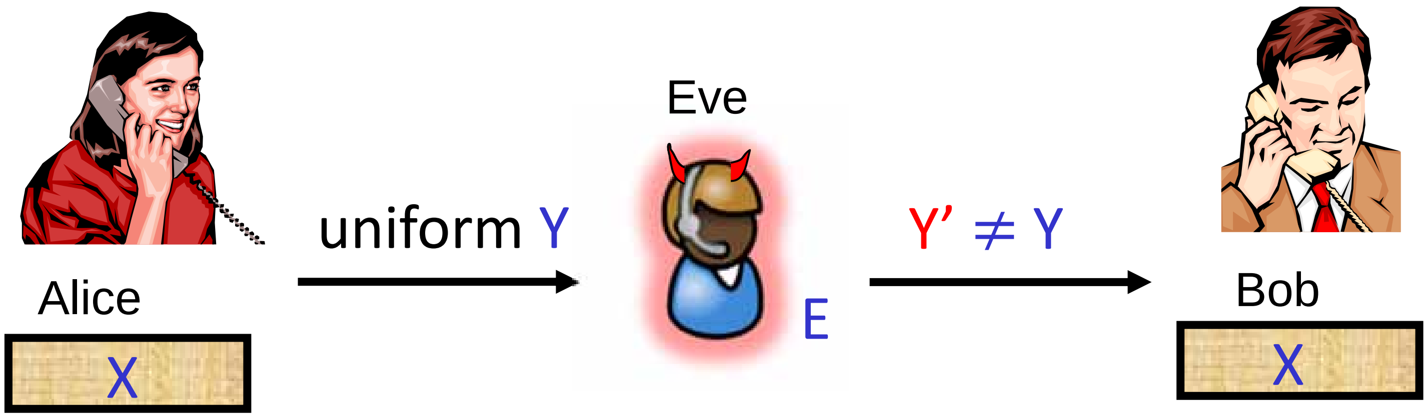
(Tutorials: Aug 28)

(Main Conference: Month Day-Day)

AMO Summer School: Aug 23 - 28

Privacy Amplification with Man-in-the-Middle (MIM) Adversary

- Eve holds side info E about X & launch MIM attack
  - Can arbitrarily modify, insert, delete, and reorder message
- Well-studied problem classically [MW97,DW09,RW03, KR09,CKOR10,DLWZ11,CRS12,Li12,Li15]
- Motivate quantum-proof non-malleable Ext



Z=Ext(X,Y)

Open! for quantum E

Z’=Ext(X,Y’)

Cryptography w/ Imperfect Randomness

- Strong impossibility [DOPS04]
  - Encryption, commitment, two-party computation, etc.
- If ≥ 2 indep sources available $\Rightarrow$ multi-source Ext
- Multi-party computation
  - Each party has *single* privacy weak source
  - Classically, solved by network extractor protocols
    - Weak feasibility in I.T setting [KLRZ08]
    - Strong feasibility in comp. setting [KLRZ08,KLR09]
  - Quantum-proof network extractors
    - We made some progress, but widely open

Thank you! Questions?