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
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 existence of true randomness?

- System performs an experiment to output a bit $b \in \{0,1\}$
- Eve models an external observer
- **Necessary Assumptions:** (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 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, GMdT+12, MP13, BR+13...]
4) Quantum Bit Commitment & Coin Flipping [SCA+11]
5) Quantum Computation Delegation [RU13, 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 \(\varepsilon < 0.058\)

Alice

\[ x_i \]

\[ a_i \]

Accept if Device “play well” &

Output \( z = a_r \) for \( r \leftarrow \text{SV Source} \)

Eve

\[ y_i \]

\[ b_i \]

\[ M_E \]

\[ O_E \]

Guess \( z \)
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 $\implies$ certifiable true randomness

Weaker assumptions $\implies$ 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 \( X = x \)
    - \( p(a \mid xy) = p(a \mid xy') \) for any \( x, y, y' \)

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

- NS Security:
  - If \( \Pr[\text{Alice accepts}] \geq \epsilon \), then
  - \( \Pr[\text{Eve guess } z \text{ correctly}] \leq (1/2) + \epsilon \)
# Developments of RA Protocols

<table>
<thead>
<tr>
<th>Source</th>
<th>Eve</th>
<th>Conditional independence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Source-Device</td>
<td>Source-Eve</td>
</tr>
<tr>
<td>[CR12]</td>
<td>SV ( \varepsilon &lt; 0.058 )</td>
<td>Classical</td>
</tr>
<tr>
<td>[GMT+13]</td>
<td>SV ( \varepsilon &lt; 1/2 )</td>
<td>NS</td>
</tr>
<tr>
<td>[BRG+13]</td>
<td>SV ( \varepsilon &lt; 1/2 )</td>
<td>NS</td>
</tr>
<tr>
<td>[RBH+15]</td>
<td>SV ( \varepsilon &lt; 1/2 )</td>
<td>NS</td>
</tr>
<tr>
<td>[WBG+16]</td>
<td>SV ( \varepsilon &lt; 0.0144 )</td>
<td>NS</td>
</tr>
</tbody>
</table>
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 $X \in \{0,1\}^n$

$\minentropy = \log (\text{the maximum probability of guessing } x \text{ sampled from } X \text{ correctly})$.

$\NSentropy = \log (\text{the maximum probability of guessing } x \text{ sampled from } X \text{ correctly with the help of NS correlation})$.

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 $\rightarrow$ Non-Zero Min-entropy $\rightarrow$ Weak Min-entropy Sources
## Summary of RA Protocols

<table>
<thead>
<tr>
<th>Source</th>
<th>Eve</th>
<th>Conditional independence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Source-Device</td>
</tr>
<tr>
<td>[CR12]</td>
<td>SV $\varepsilon &lt; 0.058$</td>
<td>Classical</td>
</tr>
<tr>
<td>[GMT+13]</td>
<td>SV any $\varepsilon &lt; 1/2$</td>
<td>NS</td>
</tr>
<tr>
<td>[BRG+13]</td>
<td>SV any $\varepsilon &lt; 1/2$</td>
<td>NS</td>
</tr>
<tr>
<td>[RBH+15]</td>
<td>SV any $\varepsilon &lt; 1/2$</td>
<td>NS</td>
</tr>
<tr>
<td>[CSW14]</td>
<td>Any weak</td>
<td>Quantum</td>
</tr>
<tr>
<td>[WBG+16]</td>
<td>SV $\varepsilon &lt; 0.0144$</td>
<td>NS</td>
</tr>
<tr>
<td><strong>This Talk</strong></td>
<td>Any weak</td>
<td>NS</td>
</tr>
</tbody>
</table>
Our Result: Ideal Dichotomy Thm

• Randomness amplification assuming
  – \((\text{Source} | \text{Device})\) has sufficient \textbf{NS} min-entropy
  – \textbf{NS} condition among \textit{Eve} & \textit{Devices}

• Minimal assumption: both are necessary
  • \textit{No structural or independence} assumptions about the sources

• Ideal dichotomy theorem
  – Weak source = arbitrary source w/ sufficient uncertainty
  – \textbf{Local} uncertainty \(\implies\) certifiable \textbf{global} randomness
Our Construction
All Existing Protocols

SV source

00000000000010010

Alice

\[ x_i \]

\[ a_i \]

\[ y_i \]

\[ b_i \]

Eve

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

min-entropy sources

some → Decouple → Z₁

where → Decouple → Zᵢ

random → Decouple → Zₙ

Z = XOR all Xᵢs

Classical pre-processing:
transfer input to uniform “locally”
impose correlations among blocks

Decouple the correlations:
design special DI protocols

Some Zᵢ is global uniform

By establishing a new property
input seeds uniform to device only
arbitrarily correlated otherwise
e.g., Adv can know the inputs

Classical Post-Processing: XOR picks the right one
Our Solutions in the \textbf{NS} setting

- min-entropy sources
  - some
  - where
  - random

Decouple

$Z_1$

$Z_i$

$Z_N$

$Z = \text{XOR all } X_i \text{s}$

**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 \textit{local} to \textit{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: \( Y_i = \text{Ext}(X,i) \)
\[ \implies \text{somewhere almost-uniform-to-all-Device} \]
NS-proof strong extractors \textbf{DO NOT} exist!

\textit{a counter-example in the paper}

\textbf{IMPOSSIBLE} to achieve with the construction!
Obtain **NS** Somewhere Uniform Sources

NS-proof strong extractors *DO NOT* exist!

*a counter-example in the paper*

\[ X \in \text{any (n,k) source} \]

\[ \approx \text{uniform } \otimes \text{Device T} \]

**POSSIBLE** w/ classical extractors + \(2^m\) error loss!

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

To balance the error, \# devices \(\geq 2^{\text{poly}(1/\varepsilon)}\)
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 \( \Rightarrow \) efficiently generated!
Decoupler Construction

- Play BHK game $N \times K$ 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 $\leq C \cdot \langle P_{AB|XY}|BHK^K \rangle$
- 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
  \[ P_{ARBR|XYR,Acc}\mid BHK^K \] 
  – since only output when Acc

• Bound it by \( P_{ARBR|XYR} \mid BHK^K \).

• 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

Real World

≈ ϵ  
≈ √ϵ

Ideal World

**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:

\[
\Pr[\text{Acc} \land \langle P_{ABR|R|X_{RYR},\text{Acc}|BHK^K} \rangle \geq \gamma ] \leq \delta
\]

• If claim is false when \(X\) is \(\varepsilon\)-close to uniform-to-Device

\[
\Pr[\text{Acc} \land \langle P_{ABR|R|X_{RYR},\text{Acc}|BHK^K} \rangle \geq 2\gamma ] > 2\delta
\]

\(\Rightarrow \exists D\) distinguish \((X, \text{Device})\) from \(U \otimes \text{Device}\) w/ adv > \(\varepsilon\)

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

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

• Thus,

\[
\Pr[\text{Acc} \land \langle P_{ABR|R|X_{RYR},\text{Acc}|BHK^K} \rangle \geq 2\gamma ] \leq 2\delta
\]

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

- Randomness amplification under minimal assumptions
  - \((\text{Source} \mid \text{Device})\) has sufficient min-entropy
  - NS condition among Eve & Devices
  - No structural or independence assumptions about the source

- Ideal dichotomy theorem
  - Sufficient local uncertainty \(\implies\) certifiable global uniform rand.
  - \(\text{poly}(1/\varepsilon)\) min-entropy \(\implies\) certify \(\varepsilon\)-close to uniform bits
  - Use \(2^{\text{poly}(1/\varepsilon)}\) 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...