Secure Random Number Generation from Parity Symmetric Radiations
(arXiv:1912.09124 [quant-ph])
Toyohiro Tsurumaru¹, Toshihiko Sasaki², Izumi Tsutsui³
1: Mitsubishi Electric Corporation, Information Technology R&D Center
2: Photon Science Center, Graduate School of Engineering, The University of Tokyo
3: Theory Center, Institute of Particle and Nuclear Studies, High Energy Accelerator Research Organization (KEK)

Outline
- The random number generators (RNGs) are an indispensable tool in cryptography, and various methods are known.
- RNGs using raditions from nuclear decays (radioactive RNG) has a relatively long history, but their security has never been discussed rigorously in literature.
- We here propose a new method of the radioactive RNG that admits a rigorous proof of security.
- The security proof is made possible here by exploiting the parity (space inversion) symmetry arising in the device, the property previously unfocused.
- α-decaying nuclides (e.g., americium[²⁴¹Am]) emit parity invariant radiation.
- By detecting it with detectors in a parity covariant configuration, one can obtain a random number.

Random Number Generator (RNG)
A device which repeatedly outputs number \( r \) in a certain range.
- The goal of the RNG:
  * Uniformity: the output \( r \) occurs with a uniform distribution.
  * Security: The value \( r \) is unpredictable and unknown to anyone other than the legitimate user.
- Threats to the security:
  Components of an RNG may have been tampered with by the Eavesdropper, and the eavesdropper can tamper with the RNG to make \( r \) predictable.

Radioactive RNG
- Procedure:
  Step 1: Measure raditions emitted from the source in time bins \( i = 1, \ldots, N \).
  Then record the timings of detections \( z = (z_i) \in \{1, 0\}^N \).

Main Result: Security of our Radiactive RNG
- Security of random number \( r \) is measured by the smooth min-entropy \( H_{\text{min}}^{\text{se}}(\mathbf{z}|\mathbf{r}) \).
- \( H_{\text{min}}^{\text{se}}(\mathbf{z}|\mathbf{r}) \) = ambiguity of detection timing \( \mathbf{z} \) seen from the eavesdropper \( \mathcal{E} \).
- By applying the randomness extraction on \( \mathbf{z} \), one can extract the secure random number \( r \) of a \( H_{\text{min}}^{\text{se}}(\mathbf{z}|\mathbf{r}) \) bits.
- Theorem: Under condition of the previous page, we have
  \[ H_{\text{min}}^{\text{se}}(\mathbf{z}|\mathbf{r}) \leq H_{\text{min}}(\mathbf{z}|\mathbf{r}) - 2H_{\text{amb}}(\mathbf{z}|\mathbf{r}) \]
- i.e., one can extract the secure random number \( r \) of roughly \( H_{\text{min}}(\mathbf{z}|\mathbf{r}) - 2H_{\text{amb}}(\mathbf{z}|\mathbf{r}) \) bits.

Proof Sketch
- Observation 1: \( H_{\text{min}}^{\text{se}}(\mathbf{z}|\mathbf{r}) \) is the min-entropy of \( \mathbf{z} \).
- It suffices to lower bound \( H_{\text{min}}(\mathbf{z}|\mathbf{r}) \).

Assumption: Parity (Space Inversion) Symmetry
- The security is guaranteed by using the parity symmetry of the device.
- The parity symmetry can be realized by the following conditions.
  * Condition (a): The state of raditation is always parity invariant.
  * Condition (b): For probability more than 1/4, the following events hold:
    1. \( H_{\text{amb}}(\mathbf{z}|\mathbf{r}) \)
    2. \( z_i \) is uniformly distributed, and unknown to Eve; hence a secure random number.

The general (non-ideal) case can also be proved similarly.
- Differences from the ideal situation:
  * The vacuum and multi-particle emission events.
  * Detector D may not be perfect.

Observation 2: “Space inversion (parity transt) of the device” = “bit flip of \( z_i \)”
- For the sake of simplicity, we temporarily consider the following ideal case:

Random Source
Detectors D₁, D₂

Random Number Generator (RNG)

Random Sources
Detector D₁
Detector D₂

Radioactive RNG

Measurement results \( \mathbf{i} \)
(roughly secure string)

Final bits \( \mathbf{i} \)
(perfectly secure string)

Partially known
Carefully unknown
Eavesdropper (Eve)

Initial state \( \rho_{\text{ini}}(0) \)

Correlated (entangled) state

Assumption: Parity (Space Inversion) Symmetry
- The security is guaranteed by using the parity symmetry of the device.
- The parity symmetry can be realized by the following conditions.
  * Condition (a): The state of raditation is always parity invariant.
  * Condition (b): For probability more than 1/4, the following events hold:
    1. \( H_{\text{amb}}(\mathbf{z}|\mathbf{r}) \)
    2. \( z_i \) is uniformly distributed, and unknown to Eve; hence a secure random number.

The general (non-ideal) case can also be proved similarly.
- Differences from the ideal situation:
  * The vacuum and multi-particle emission events.
  * Detector D may not be perfect.