Secure Random Number Generation from Parity Symmetric Radiations

(arXiv:1912.09124 [quant-ph])

Toyohiro Tsurumaru[1], Toshihiko Sasaki[2], Izumi Tsutsui[3]

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 radiations 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 (^{241}Am)) emit parity invariant radiation.
  - By detecting it with detectors in a parity covariant configuration, one can obtain a random number.

Random Number Generator (RNG)

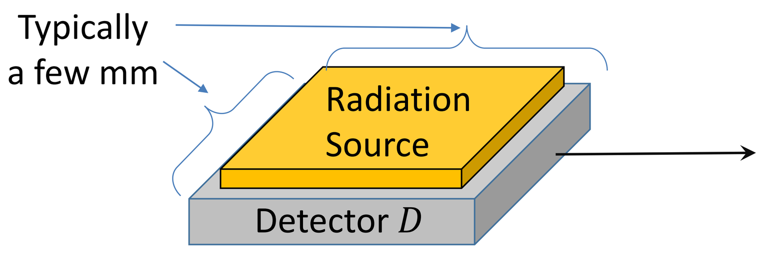
A device which repeatedly outputs number r in a certain range.

- **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:**

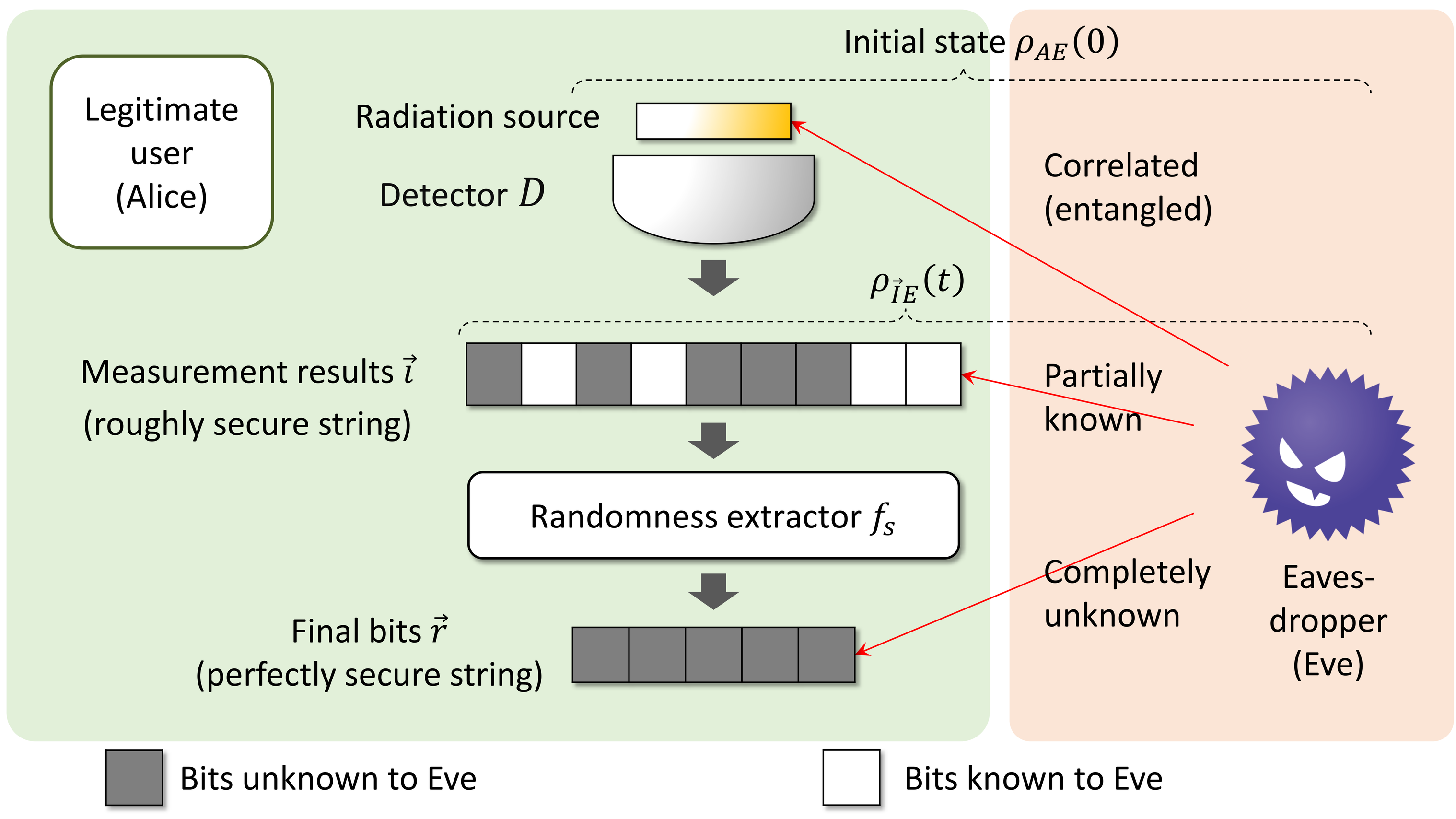
Step 1: Measure radiations emitted from the source in time bins $i = 1, \ldots, N$.
Then record the timings of detections $\vec{\imath} = (i_1, \ldots, i_{n_{\det}})$



Time bin i	1	2	3	4	5	6
Detection	yes	no	yes	no	no	yes

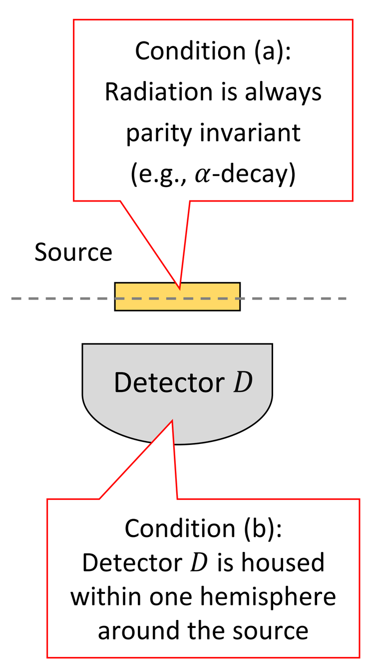
timing of detections $\vec{\imath} = (1,\ 3,\ 6)$

Step 2: Apply a randomness extraction (e.g. random matrix) on $\vec{\imath}$, and obtain random number 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 radiated particles is always parity invariant.
    $P_A \rho_{AE}(t) P_A = \rho_{AE}(t)$.
    where $\mathcal{H}_A$ =Deg. of freedom of radiated particles,
    P_A = Parity (space inversion) operator in $\mathcal{H}_A$,
    $\mathcal{H}_E$ = Deg. of freedom of Eavesdropper.
  - Condition (b): Detector D is housed within a hemisphere around the source.
  - Condition (c): For probability more than $1-\delta$, the following ineqs. hold:
    #detection events $\geq n_{\mathrm{thr}}$, #multi-particle emission events$\leq n_{\mathrm{multi}}$,
    #dark counts events $\leq n_{\mathrm{dark}}$ (Out of N time bins).



Main Result: Security of our Radiactive RNG

- Security of random number r is measured by the smooth min-entropy $H^{\delta}_{\min}\left(\vec{\imath}|E\right)$.
  - $H^{\delta}_{\min}\left(\vec{\imath}|E\right)$ = ambiguity of detection timing $\vec{\imath}$, seen from the eavesdropper E.
  - By applying the randomness extraction on $\vec{\imath}$, one can extract the secure random number r of $\cong H^{\delta}_{\min}\left(\vec{\imath}|E\right)$ bits.

> - Theorem Under condition of the previous page, we have
> $$H^{\delta}_{\min}\left(\vec{\imath}|E\right) \geq n_{\mathrm{thr}} - n_{\mathrm{multi}} - 2n_{\mathrm{dark}}.$$

- I.e., one can extract the secure random number r of roughly $n_{\mathrm{thr}} - n_{\mathrm{multi}} - 2n_{\mathrm{dark}}$ bits.

Proof Sketch

- Observation 1:

Time bin i	1	2	3	4	5	6
Detection	yes	no	yes	no	no	yes

Detection' $\vec{z}$ = (1, 0, 1, 0, 0, 1)

Rewrite "no" → 0, "yes"→ 1

Detection timings $\vec{\imath} = (1,\ 3,\ 6)$

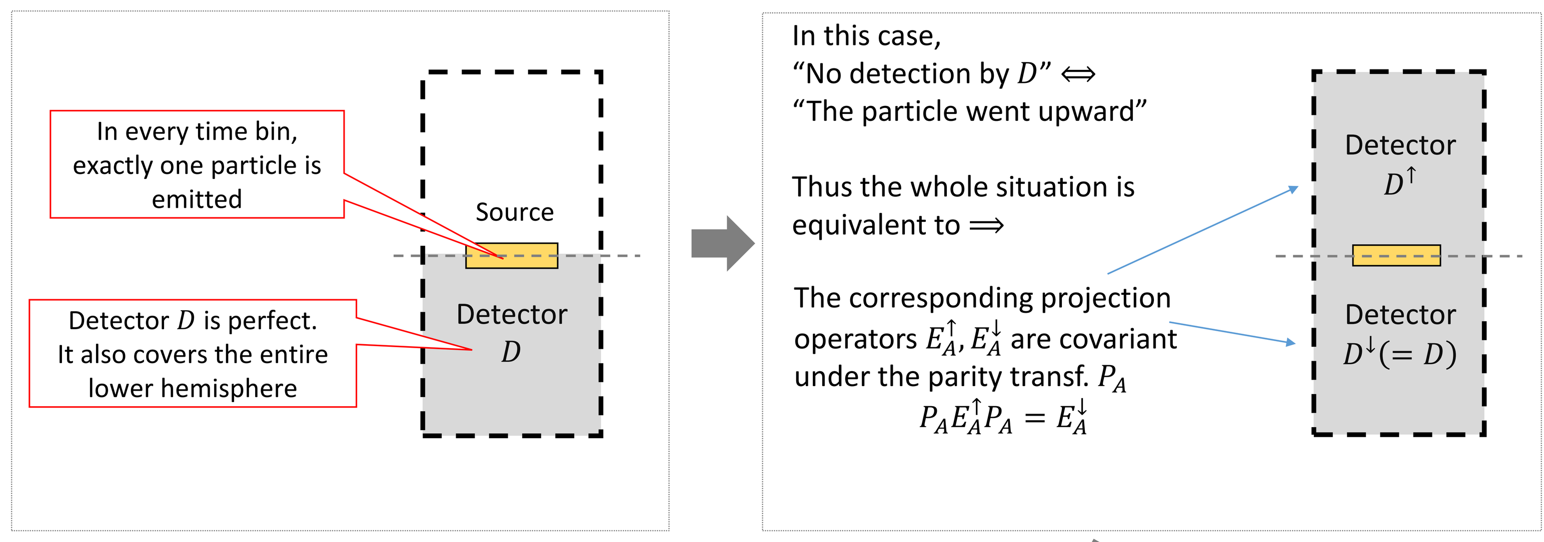
There is a one-to-one correspondence between detections $\vec{z}$ and detection timings $\vec{\imath}$

$\Rightarrow H_{\min}\left(\vec{\imath}|E\right) = H_{\min}\left(\vec{Z}|E\right)$ = the min-entropy of $\vec{z}$

$\Rightarrow$ It suffices to lower bound $H_{\min}\left(\vec{Z}|E\right)$

- Observation 2: "Space inversion (parity transf.) of the device" = "bit flip of z_i"

For the sake of simplicity, we temporarily consider the following ideal case



- State ρ_{AE} before measurement is parity invariant; $P_A \rho_{AE} P_A = \rho_{AE}$. (Condition (a))
- Eve's state after Alice's measurement is independent of the measurement result (↑,↓).
  $$\rho_E^{\uparrow} = \mathrm{tr}_A\left(E_A^{\uparrow}\rho_{AE}\right) = \mathrm{tr}_A\left(P_A E_A^{\uparrow} P_A P_A \rho_{AE} P_A\right) = \mathrm{tr}_A\left(E_A^{\downarrow}\rho_{AE}\right) = \rho_E^{\downarrow}$$
- The joint state of Alice's measurement result z_i and of Eve takes the form
  $$\rho_{Z_i E} = \frac{1}{2}\left(|\uparrow\rangle\langle\uparrow| + |\downarrow\rangle\langle\downarrow|\right)_{Z_i} \otimes \rho_E = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right)_{Z_i} \otimes \rho_E$$

z_i is uniformly distributed, and unknown to Eve; hence a secure random number.

- As the same reasoning applies to all bits $\vec{z} = (z_1, \ldots, z_N)$, we have
  $$H_{\min}\left(\vec{\imath}|E\right) = H_{\min}\left(\vec{Z}|E\right) = N$$

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.
    ⇒ None or both (instead of single one) of detectors $D^{\downarrow}, D^{\uparrow}$ can go off.
  - Still, if one focuses on single detection events only, the argument can be reduced to the ideal case.
    $\Rightarrow H_{\min}\left(\vec{Z}|E\right) \geq$ # single detection events
    ⇒The theorem follows from condition(c)