Pseudorandomness in EPC Gen2 Commercial Tags: A Preliminary Analysis

Joan Melià-Seguí[1], Joaquin Garcia-Alfaro[2], Jordi Herrera-Joancomartí[3]

Keywords

- RFID
- EPC Gen2
- PRNG
- Security
- Demo Tag
- Implementation
- Frequency Analysis

Context and Goal

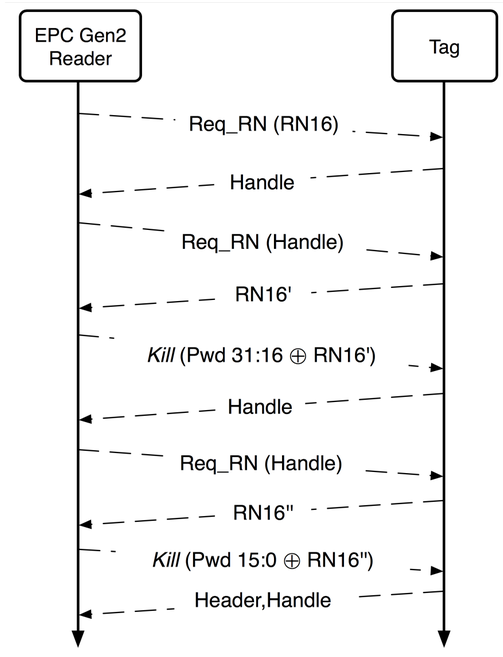
- Context: 16-bit pseudorandom sequences are used to encrypt the communication between readers and tags, and to acknowledge the proper execution of password-protected operations.
- Current EPC Gen2 integrated circuit (IC) manufacturers do not provide information about their Pseudorandom Number Generator (PRNG) designs. The EPC Gen2 standard provides statistical requirements for PRNG.

EPC 1st PRNG requirement:

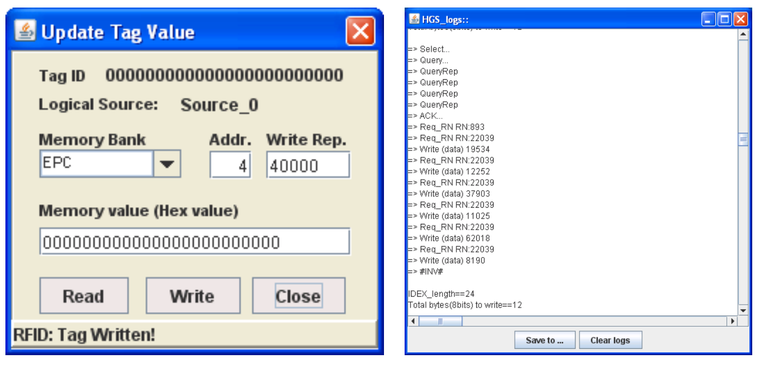
$$P_{min} = \frac{0.8}{2^{16}} < RN16 < P_{max} = \frac{1.25}{2^{16}}$$

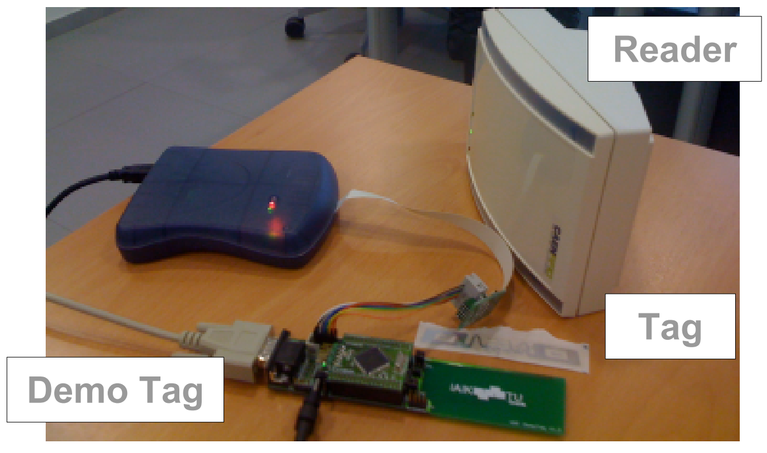
- Goal: Evaluate the security of current EPC Gen2 systems by analyzing the randomness of the 16-bit pseudorandom sequences generated by resource-constrained EPC Gen2 tags.

Keys are generated by the least resource-constrained devices



Eavesdropping Technique

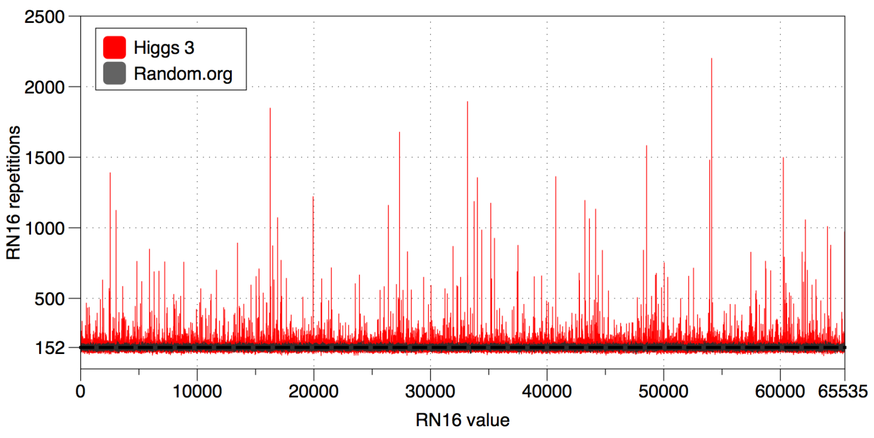


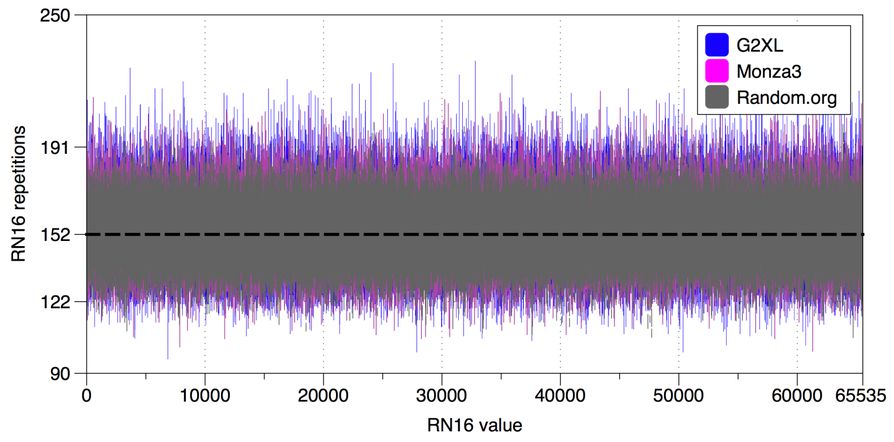


- Accessing the *Verbose Buffer* of a UHF Demo Tag, we can recover the reader to tag communication between EPC Gen2 commercial readers and tags.
- Writing a new 96-bit Identification to an EPC Gen2 tag generates up to 8 pseudorandom sequences (128 bits) with a single *write* command, which can be obtained through the Demo Tag's UART module.
- 10 million sequences (160 Mb) generated from each analyzed tag.

Alien Higgs 3 | NXP Ucode G2XL | Impinj Monza 3

Statistical Evaluation





Expected repetitions: mean = 152, P_{min} = 122, P_{max} = 191.

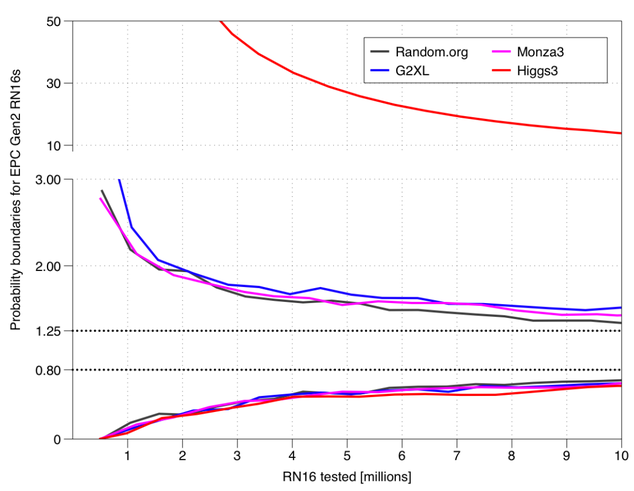
Reference data: True random sequences are obtained from Random.org service.

National Institute of Standards and Technology (NIST) test suite to evaluate randomness deviations:

Higgs3	G2XL	Monza3	
✓	✗	✗	Frequency
✗	✓	✓	Block Frequency
✓	✗	✗	Runs
✓	✓	✓	Longest Run of 1's
✓	✓	✓	Binary Matrix Rank
✓	✓	✓	Non-overlap. Temp.
✗	✓	✓	Overlap. Template
✓	✓	✓	Linear Complexity
✗	✓	✓	Serial Test
✗	✓	✓	Approx. Entropy
✓	✗	✗	Cumulative Sums
✓	✓	✓	Rand. Excursions

Result and Discussion

- The main goal of a PRNG is to ensure the forward unpredictability of its generated sequences.
- Evidences of non-randomness in pseudorandom sequences generated from commercial EPC Gen2 PRNGs.
- Discussion: Weaknesses in EPC Gen2 security?



This work has been supported by the Spanish Ministry of Science and Innovation, the FEDER funds under the grants TSI2007-65406-C03-03 E-AEGIS, CONSOLIDER CSD2007-00004 ARES and the Institut TELECOM through its Futur et Ruptures program.

1 Universitat Oberta de Catalunya,
Roc Boronat 117, 08018 Barcelona - Spain,
melia@uoc.edu

2 Institut Telecom, Telecom Bretagne,
02, rue de la Chatagneraie, Cesson-Sevigne 35576 - France,
joaquin.garcia-alfaro@acm.org

3 Universitat Autònoma de Barcelona,
Edifici Q, Campus de Bellaterra, 08193, Bellaterra - Spain,
jordi.herrera@uab.cat