RESEARCH LETTER

On the Similarity of Commercial EPC Gen2 Pseudorandom Number Generators

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

[1] Department of Communications and Information Technologies, Universitat Pompeu Fabra,Tànger 122-140, 08018 Barcelona - Spain [2] Telecom Sudparis, CNRS Samovar UMR 5157, 9 Rue Charles Fourier, 91000 Evry - France [3] Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, Edifici Q, Campus de Bellaterra, 08193 Bellaterra - Spain

ABSTRACT

Pseudorandom generators are the main security tool in EPC Gen2 systems. Besides its statistical compliance with the standard, no further information is provided on its design, performance or generation scheme. We empirically analyzed EPC Gen2 pseudorandom sequences using a novel experimental setup. From our analysis, we obtained evidences that pseudorandom number generators used in different commercial IC use the same algorithm. This paper presents the results of this analysis.

Keywords: RFID; EPC Gen2; PRNG; Security; Demo Tag; Implementation; Frequency Analysis.

*__Correspondence__
Department of Communications and Information Technologies, Universitat Pompeu Fabra,Tànger 122-140, 08018 Barcelona - Spain
Email: joan.melia@upf.edu

1. INTRODUCTION

EPC Gen2 [1] is de-facto standard for supply chain Ultra High Frequency Radio Frequency Identification. EPC Gen2 tags are designed to balance cost and functionality, and its manufacture faces several challenging constraints such as cost, compatibility regulations, power consumption, performance requirements and energy harvesting [2]. As a consequence, computational capabilities of EPC Gen2 tags are very simple, usually provided by CMOS Integrated Circuits (IC), which can lead to vulnerabilities in their implemented algorithms [3].

Besides the compliance of the EPC Gen2 [1], ICs are also adjusted to the complementary ISO 18,000-6C [4] standard. One of the parameters implicitly related to the accomplishment of these standards is the on-board Pseudorandom Number Generation (PRNG), which is the basic security tool for the EPC Gen2 tags. Since the manufacturers declare the compliance of their products with the standard, their PRNG method satisfies the three statistical requirements specified in the standard for that issue [1]. However, manufacturers are reluctant to provide further information regarding the underlying algorithm generating the pseudorandom sequences. To address the lack of information regarding this issue in this letter we analyze the PRNG behavior of three different IC models used in EPC Gen2 compliant commercial tags. PRNG analysis can also be applied to other resource-constrained communication technologies like cognitive radio networks [5].

2. COMMERCIAL ANALYZED ICS

EPC Gen2 IC manufacturers commercialize their ICs and inlay together (that is, the tag ready to work), or as single product to add to other inlay manufacturers. Hence, there are several different tags (even from different manufacturers) sharing the same IC.

We have analyzed the PRNG behavior of three different IC models (NXP Ucode *G2XL*, Alien *Higgs3* and Impinj *Monza3*) used in EPC Gen2 compliant commercial tags.

The UCODE G2XL and G2XM ICs is currently available product line for the NXP UHF RFID [6]. The analyzed IC is the Ucode G2XL [7] (hereinafter represented as *G2XL*) which is compliant to EPC Gen2 1.1.0. The Alien Technology supplies the Higgs family for UHF RFID. The analyzed model in this letter is the Higgs 3 IC (hereinafter represented as *Higgs3*), which is compatible with the EPC Gen2 specifications (1.2.0)

[†]Joan Melià-Seguí was with the Universitat Oberta de Catalunya, during the development of this work.

and ISO 18,000-6C standard. Finally, the EPC Gen2 and ISO 18,000-6C Monza 3 is analyzed for the Impinj ICs (hereinafter represented as *Monza3*). Newer versions of the Monza series have been released, adding user memory and custom commands capabilities.

3. EXPERIMENTAL SETUP

We propose to analyze the aformentioned PRNGs through the ICs' binary pseudorandom sequence generation, included in the communication protocol commands.

In the identification stage, the tag uses the PRNG to inform the reader that it can be identified. If the reader acknowledges the sequence, the tag sends its full EPC identification. If later the reader requests access to the reserved memory contents, or if it wants to modify the memory content, the tag generates new sequences to cipher the specific passwords and new memory content, following a one-time-pad scheme [1]. Note that the pseudorandom sequences are not a parameter to be set up by the user or the middleware. They are used in the lower layers of the communication. Therefore, there is no possibility to access the sequence values from the reader software or middleware.

The security in EPC Gen2 systems relies on the low-power tag to reader channel, used to transmit the tag generated pseudorandom sequences to reader, which in turn, will use them as specified above in the more powerful reader-to-tag channel.

In order to obtain the pseudorandom sequences from the communication between readers and tags, the IAIK UHF Demo Tag [8] is used. The Demo Tags produced by IAIK TU Graz are programmed for delivery with an *ISO 18,000-6C firmware*. The Demo Tag works with a customizable application using the functions included in the Demo Tag firmware to act like an EPC Gen2 tag, with some extended functionalities. Some of these functionalities are related to the UART module that enables the visualization of information through a serial terminal.

Two of the extended functions are used for the eavesdropping technique, the *Verbose Buffer* and the *Tag Normal / Silent Mode*. The *Verbose Buffer* is a first-input first-output stack that stores the EPC Gen2 protocol commands exchanged between reader and tag. The buffer stores both the commands received from the reader and the tag responses, and it can be visualized through the serial terminal. The *Tag Normal / Silent Mode* allows the deactivation of the Demo Tag responses but without turning it off. This command is activated through the serial terminal.

The combination of these two extended functionalities allows us to use the Demo Tag to obtain the *reader-to-tag* communication between the reader and the commercial tags. Readers interested in the experimental setup may refer to [9] and [10] for further details.

4. DATA RETRIEVAL

The *write* command [1], used to write information in the tag memory, uses the one-time-pad cover-coding to cipher the new information to be written with the pseudorandom sequences. Then, writing the full EPC identification memory area allows us to retrieve up to eight 16-bit pseudorandom sequences, which means 128 bits.

To determine the number of randomly generated bits that have to be eavesdrop from the commercial tags for the later analysis we use the fulfillment of the first EPC Gen2 requirement for random number generation [1]. Such requirement specifies that any single 16-bit pseudorandom sequence generated by an EPC Gen2 tag shall be bounded by $P_{min} = 0.8/2^{16}$ as the minimum probability; and $P_{max} = 1.25/2^{16}$ as the maximum probability, with respect to the mean of all the generated values.

If we use the *Random.org* service [11], which provides true random sequences, we obtain that about 10 million of 16-bit sequences (160 Mb) are necessary to reach a 99% of sequence values ensuring the EPC Gen2 first requirement for random number generation. Then, we consider this value as a proper size for the eavesdropped sequences of the commercial ICs analyzed.

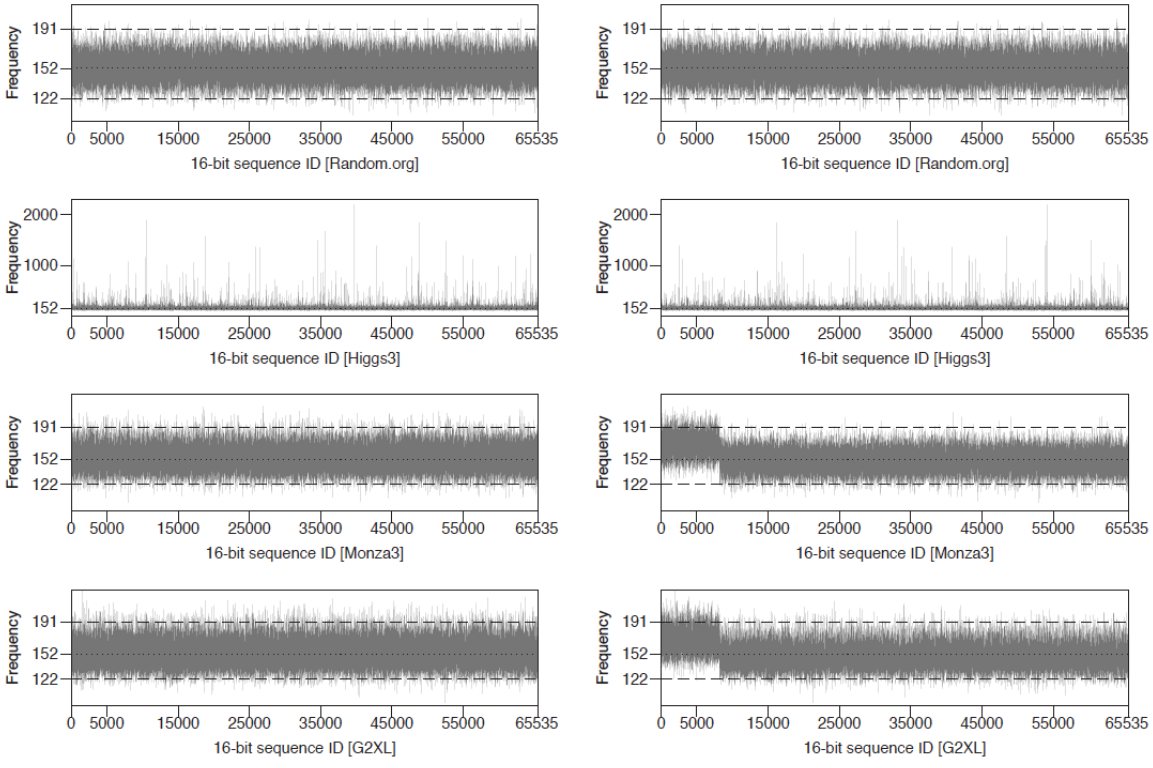
In order to evaluate the commercial ICs PRNG we shall choose a tag using the specified IC. We generate 10 million 16-bit sequences with the Confidex Cassey tag [12] for the *G2XL* IC, the Alien Squiggle tag [13] for the *Higgs3* IC, and the TRACE Inlay tag [14] for the *Monza3* IC.

5. TEST RESULTS

A frequency test has been applied to the reference *Random.org* sequences and to the sequences generated by the analyzed ICs PRNGs (*G2XL*, *Monza3* and *Higgs3*). For each analyzed IC, and the reference data, we have analyzed 10 million 16-bit sequences, generated from the same tag. A perfectly uniform PRNG is supposed to generate uniform binary sequences, that is, the same number of 0's and 1's, or the same frequency for each n-bit value. As defined in the Standard [1] the desired uniformity for EPC Gen2 PRNGs is $P_{min} = 0.8/2^{16}$ and $P_{max} = 1.25/2^{16}$. Hence, a PRNG with all values' frequency within the boundaries would be 100% uniform.

If sequences are arranged as 16-bit numbers using the big endian notation (right to left decreasing powers of 2) the resulting plots for the four obtained sequences are depicted in Figure 1 (a). Using this representation, and taking as a reference data the *Random.org* plot, we can observe that both IC, *Monza3* and *G2XL* approximately provide the uniformity that one should expect from pseudorandom data. However, *Higgs3* does not meet the desired uniformity (notice the different scale in Figure 1 for *Higgs3* plots).

But, if we now compute the 16-bit values following the little endian notation (left to right decreasing powers



(a) Big endian notation

(b) Little endian notation

Figure 1. Frequency analysis results of EPC Gen2 commercial IC's PRNG.

of 2) the resulting plots, depicted in Figure 1 (b), provide interesting results. Plots for the *Random.org* and *Higgs3* sequences present a similar shape than the ones obtained for the big endian representation. Surprisingly, *Monza3* and *G2XL* show an artifact that suggests that both sequences, although generated with IC coming from different vendors, apparently are generated by the same pseudorandom number generator. We repeated the analysis using 8-bit pseudorandom sequences, obtaining the same artifact, proportionally to 20 million sequences for the same number of analyzed bits.

PRNGs are used as a security tool in the EPC Gen2 technologies, i.e. enabling one-time-pad ciphering sequences. Hence, the possibility of different manufacturer ICs using the same algorithms for PRNG presents implications regarding the security of the RFID communications. On one hand, predicting the pseudorandom sequence generation for one specific IC (e.g. using an eavesdropping technique like the one presented in this paper, and analyzing the sequences) would also apply to other ICs implementing the same algorithm. On the other hand, the strengths associated these PRNG algorithms would also apply to each IC implementing them.

Moreover, Table I shows a summary of the ICs frequency analysis. As can be observed in Figure 1 some sequences in the analyzed generators surpass $P_{min} = 0.8/2^{16}$ and $P_{max} = 1.25/2^{16}$, that is, showing within 122 and 191 appearances for 10 million 16-bit sequences. This is the case of *Alien Higgs3* and the first values of *Impinj Monza3* and *NXP G2XL* in the little endian formation. Table I shows the fraction of pseudorandom sequences being generated within the specified boundaries for each IC generating 10 million 16-bit sequences.

An adversary (e.g. an entity trying to obtain the sequences transferred from reader-to-tag) could take advantage of such deviations to understand details of the PRNG using reverse engineering. Also, the EPC Gen2 model supposes that an adversary eavesdropping the reader-to-tag channel cannot capture sensitive data (such as passwords or the contents of password-protected operations) since the information is blinded (via exclusive-OR operations) with the random sequences generated at the tag side. However, it is straightforward that an adversary capable of predicting the output of the random bit generator of a tag (e.g., based on a flawed uniformity property of the generator), can easily obtain the sensitive data by simply applying Exclusive-OR operations [10].

Finally, we also used the NIST Statistical Test Suite for pseudorandom number generation [15] to evaluate the randomness deviations of the EPC Gen2 PRNGs binary sequences using the same datasets. *Monza3* and *G2XL* PRNGs show again similar results in the analysis, with evidences of non-randomness in the *Frequency* and *Runs* tests. Evidences of non-randomness are also found in the

Table I. EPC Gen2 ICs PRNGs uniformity for 10 million 16-bit sequences

PRNG Generator	Random.org	Alien Higgs 3	Impinj Monza 3	NXP G2XL
Rate (%)	99.45	89.40	98.67	97.35

Higgs3 through its performance in the BlockFrequency, ApproximateEntropy and Serial tests. Readers interested in further details of this analysis can refer to [16].

6. CONCLUSION

Thanks to a novel bit-extraction method using the Demo Tag we have been able to obtain information from the reader-to-tag communication using the EPC Gen2 protocol. The obtained data are the 16-bit sequences generated from the PRNGs which EPC Gen2 tags implement onboard. 10 million 16-bit sequences (160 Mb), are obtained from each commercial IC.

We have focused our analysis on the *NXP G2XL*, *Alien Higgs 3* and *Impinj Monza 3* ICs, using truly random data sequences from *Random.org* as a reference data.

From our evaluation, we conclude that pseudorandom number generators used in different manufacturer ICs use the same algorithm. Furthermore, some results regarding the pseudorandom sequence probability boundaries indicate that the uniformity of the pseudorandom generator is lower than it should be.

ACKNOWLEDGEMENT

This work was partly funded by the Spanish Government through projects TSI2007-65406-C03-03 E-AEGIS, TIN2011-27076-C03-02 CO-PRIVACY, TIN2010-15764 N-KHRONOUS, and CONSOLIDER INGENIO 2010 CSD2007-0004 ARES.

REFERENCES

1. EPCglobal. EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860-960 MHz. Available at `http://gs1.org/gsmp/kc/epcglobal/`.
2. Alvarado U, Juanicorena A, Adin I, Sedano B, Gutiérrez I, de Nó J. Energy harvesting technologies for low-power electronics. *Transactions on Emerging Telecommunications Technologies* 2012; DOI: 10.1002/ett.2529.
3. Lv C, Li H, Ma J, Zhang Y. Vulnerability analysis of elliptic curve cryptography-based RFID authentication protocols. *Transactions on Emerging Telecommunications Technologies* 2012; DOI: 10.1002/ett.2514.
4. ISO/IEC 18000-6: Radio frequency identification for item management - parameters for air interface communications at 860 MHz to 960 MHz. *Technical Report*, International Organization for Standardization (ISO), [Online] Available at `http://www.iso.org/` 2006.
5. Sodagari S, Bilén SG. On cost-sharing mechanisms in cognitive radio networks. *European Transactions on Telecommunications* 2011; **22**(8):515–521. DOI: 10.1002/ett.1501.
6. NXP UHF UCODE Website. [Online]. Last access Oct. 2012 Available at `http://www.nxp.com/`.
7. NXP. UCODE G2XL Leaflet. [On-line] 2010. Available at `http://www.nxp.com/`.
8. IAIK - Graz University of Technology. UHF RFID Demo Tag. Available at `http://jce.iaik.tugraz.at/sic/Products/`.
9. Garcia-Alfaro J, Herrera-Joancomartí J, Melià-Seguí J. Practical Eavesdropping of Control Data from EPC Gen2 Queries with a Programmable RFID Toolkit. *Hakin9* 2011; [Online].
10. Melià-Seguí J, Garcia-Alfaro J, Herrera-Joancomartí J. A Practical Implementation Attack on Weak Pseudorandom Number Generator Designs for EPC Gen2 Tags. *Wireless Personal Communications,* 2011; **59**(1):27 – 42. DOI: 10.1007/s11277-010-0187-1.
11. Haahr M. True random number service. [Online, last access Oct. 2012] Available at `http://random.org`.
12. Confidex. Casey inlay 2010. Available at `http://www.confidex.fi/`.
13. Alien technology - squiggle inlay 2010. Available at `http://www.alientechnology.com/tags/`.
14. Trace tecnologías - trace inlay 2010. Available at `http://www.tracetecnologias.com/`.
15. National Institute of Standards and Technology. Random number generation. Available at `http://csrc.nist.gov/groups/ST/toolkit/rng/`.
16. Melià-Seguí J. Lightweight PRNG for low-cost passive RFID security improvement. PhD Thesis, Universitat Oberta de Catalunya 2011.