Studying the Pseudo Random Number Generator of a low-cost RFID tag

Mohamad Merhi
Faculty of Technology, School of Computing
University of Portsmouth
Portsmouth, UK
Email: mohamad.merhi@port.ac.uk

Julio Cesar Hernandez-Castro
Faculty of Technology, School of Computing
University of Portsmouth
Portsmouth, UK
Email: Julio.Hernandez-Castro@port.ac.uk

Pedro Peris-Lopez
Security and Privacy Lab
Delft University of Technology
The Netherlands
Email: P.PerisLopez@tudelft.nl

***Abstract*—Due to severe limitations in their computational and storage capabilities, many low-cost RFID tags have been shown to implement quite weak authentication protocols, largely due to weakness in their pseudorandom number generators (PRNG). This aim of this is to examine the PRNG in use within the authentication protocol of the new NXP MIFARE Ultralight C RFID low-cost card. The article investigates the nonces generated by the card during the authentication protocol to assess their randomness, and to test any possible attacks down this path. We confirm the validity of the methodology by applying similar techniques to the Mifare 1K Classic, confirming previously discovered weaknesses. We conclude that in the light of our analysis, the PRNG of the Ultralight C is a major improvement over that of the Mifare 1K, and that the nonces generated by the former can't be easily distinguished from truly random ones.**

I. RFID Overview

Radio Frequency Identification (RFID) is an emerging and promising technology for automated object identification. RFID is based on the use of the radio frequency signal and transmission characteristics [5]. RFID has been demonstrated to have a large number of advantages over barcodes [4]. Although extremely cheap, barcodes have limited storage capacity and cannot be reprogrammed, which is increasingly triggering the use of RFID in many industries and activities. Uses include Point of Sale (POS), access control to buildings or rooms within buildings, livestock identification, asset and product tracking in a supply chain, and product security & counterfeit. In addition, RFID's major benefit could be its ability of communication from a distance, without the need of being in direct contact. On the other hand, this makes it far more vulnerable to security and privacy threats, namely location tracking and user privacy. Security and privacy threats are specially acute in Ultralightweight low-cost RFID tags, as they have very limited computing functions and storage capabilities to implement countermeasures [1].

II. Authentication Protocols

Most authentication protocol proposals involve a challenge-response mechanism between the reader and the tag, as this scheme is well-known, efficient, easy to implement and provides with adequate security for most applications. This means that the reader sends a question, known as a challenge, to the tag, and the tag must reply with a valid answer to the reader, known as a response, in order to be authenticated [9]. Authentication protocols, even minimalistic ones, should be resilient against attacks based on eavesdropping multiple challenge-response pairs [4]. This is the reason why cryptographic solutions propose mutual authentication protocols where both reader and tag must convince each other that they both know a shared secret. One way for this to be done is by including nonces (random numbers only used once) in the challenge-response exchanges. Cao and Shen [13] affirm that authentication plays a crucial role in RFID applications for addressing the many security and privacy challenges that rise in these scenarios.

III. MIFARE cards

There are currently a vast variety of RFID cards on the market, that come in quite different shapes and sizes, equipped with different memory and computing capabilities, and a range of security features. Well known cards are those of the MIFARE family, produced by NXP (sponsored by Philips). NXP is considered one of the World leading companies in the semi-conductor field [2]. NXP produced MIFARE cards which are widely used around the world in different markets such as transportation, access control and event ticketing. According to NXP, they have sold more than 3.5 billion cards [6] so far, covering a large percentage of the world market. NXP has produced so far a range of cards: MIFARE ProX; SmartMX; MIFARE DESFire; MIFARE DESFire EV1; MIFARE Plus; MIFARE Classic and MIFARE Ultralight. All these cards, however, have shown various security weaknesses that in most cases also affected their pseudorandom number generators. Accordingly, NXP carefully designed the new MIFARE Ultralight C with the clear aim of eliminating previous security weaknesses, and particularly focusing on developing a more robust PRNG. This is a challenging task, due to the inherent limitations of these low-cost RFID tags. In this paper, two smart cards are discussed, the MIFARE 1K Classic and the recent MIFARE Ultralight C. The reason for applying the same analysis to both of them is to confirm the validity of the approach by verifying the weaknesses previously found by other researchers on the MIFARE Classic. An additional reason for testing both cards is because the Classic has sold around one billion tags worldwide, to cover more than 70% of

978-1-4577-0027-9/11/$26.00 ©2011 IEEE

Fig. 1. MIFARE 1K classic

Fig. 2. MIFARE Ultralight C card

contactless cards in the market as claimed by Garcia, Rossum, Verdult and Schreur [14], and the Ultralight C seems destined to be its natural replacement.

A. Mifare Classic 1K

The Mifare Classic 1K was designed to contain an enhanced integrated circuit (IC), better than those present on classical RFID chips that had a very modest computational power, in ordet to be suitable for many applications beyond identification, including access control, ticketing systems and public transportation such as the Oyster card in London [14]. The Mifare Classic 1k card complies with the first three of four parts of the ISO 14443 standard [2]. This first three parts specify the physical characteristics, the radio frequency interface, and the anti-collision protocol. The fourth component of ISO 14443 is not implemented in Mifare Classic, and describes the transmission protocol. Instead, the Mifare Classic has built-in security personalised features to secure the communication layer using a proprietary stream cipher called CRYPTO1 to provide data confidentiality and mutual authentication between card and reader [14].

Several researchers have revealed crucial weaknesses in the MIFARE Classic 1K chip. Nohl, Evans, and Plotz [8] were the first to partially recover the CRYPTO1 algorithm and to reverse engineer the hardware structure of the chip. Notably, their analysis used traditional techniques using extremely expensive hardware when conducting their experiment which proved security weaknesses mainly in the pseudorandom generator and the authentication protocol. Similar results were found later by Gans, Hoepman, and Garcia [2], [14] and [15], who extended the results of Nohl, Evans, and Plotz using a different methodology. For instance, in [15] Gans, Muijrers, Rossum, Verdult, Schreur and Jacobs were able to eavesdrop on the transaction through reading the first 6 bytes of every block. In summary, researchers quickly detected critical weaknesses in the pseudorandom number generator used for nonces, and in the authentication protocol and nonlinear filter generator, together with some minor issues in the generation, communication and encryption of parity bits.
The example below shows an instance of the Mifare 1K authentication protocol. In Line 6, we can see the eavesdropped pseudorandom number generated by the tag.

```
1. R -> T: 93 20
2. T -> R: 1E B1 61 A8 66
3. R -> T: 93 70 1E B1 61 A8 66 DD 49
4. T -> R: 08 B6 DD
5. R -> T: 60 00 F5 7B
6. T -> R: 43 48 19 F9
```

B. NXP Ultralight C RFID tag

NXP designed the MIFARE Ultra-light C in an attempt to improve security and to overcome previous cards limitations, with a strong focus on trying to cover most if not all of the security and privacy problems that plagued previous cards. The MIFARE Ultralight C core tried to improve all security related features by integrating 3DES authentication. The implemented encryption algorithm $e_k()$ is a classical 2 key 3DES encryption in EDE (Encryption, Decryption, Encryption) mode. Moreover, the MIFARE Ultralight C card also come with some anti-cloning capabilities, supported by an unique 7-byte serial number for each card [7].

The following example illustrates the NXP Ultralight C authentication protocol algorithm, which closely follows the standard, as follows.

```
1.   PCD  -> PICC:1A
2.   PICC -> PCD : e_k(RndB)
3.   PCD  -> PICC :AF e_k(RndA||RndB')
4.   PICC -> PCD: e(RndA')
```

Where: PCD stands for Proximity Coupling Device (the Reader) PICC is the Proximity Integrated Circuit Card (MIFARE Ultra-light C card) 1A this is a fixed value, first number and first letter to check connectivity $e_k()$ is encryption under key k, in the case of the ultraligth C card it is 3DES RndA, RndB are random numbers generated by the pseudonumber generator.

Below is an example of a trace of the authentication protocol generated between the reader and the Ultralight C tag. The number from line 4 is the one which is analysed in this paper.

```
1. Auth1_apdu:
    FF:00:00:00:04:D4:42:1A:00
2. Auth1_resp:
    D5:43:00:AF:63:FC:19:
    90:6A:77:D1:3F:90:00
```

```
3. RndA: 74bd85757bd28b77
4. RndB: c00c24ed61ea0f3e
5. RndA||RndB':
    74bd85757bd28b770c24ed61ea0f3ec0
6. Auth2_apdu: FF:00:00:00:13:D4:42:AF:
  89:81:7f:e2:a8:d7:18:08:
     f7:03:d9:1b:dc:40:01:6f
7. Auth2_apdu: D5:43:00:00:C6:
FE:6C:74:2B:68:CE:E8:90:00
8. E(RndA'): C6FE6C742B68CEE8
9. RndA': bd85757bd28b7774
```

IV. Experimental Setting

This paper intestigates the quality of the pseudorandom number generator in the MIFARE Ultralight C, and hypothesises its output can be distinguished from truly random data. Our aim is to appraise the credibility of this assumption, by observing multiple runs of its authentication protocol. This is relevant since, as contended by [5], developing a comprehensive and robust authentication protocol is essential to tackle more complex security and privacy needs in data communication. To check whether the nonces generated by the PRNG are (or seem to be) random, the National Institute of Standards and Technology (NIST) ramdoness test suite was used. This comprises a set of statistical tests for detecting deviations of a binary sequence from randomness [10]. In addition, two more batteries of randomness test (ENT and Diehard) were employed. ENT is a simple randomness test battery used to evaluate PRNG and includes six tests to the stream of bytes stored in a file; these include an Entropy, Chi-square and Serial correlation coefficient (SCC) test [11], [3]. Yalcin, Suykens, and Vandewalle [12] recommend the Diehard tests as a well-known statistical test suite used in cryptographic testing, so we also used it.

In principle, to capture the numbers generated by the card, hardware alone can be used to eavesdrop and record the exchange between the reader and the card. However, in our case, we had full control over the reader application, and we modified the reader code to fully monitor and capture all authentication steps. For this, a PERL script from Jean-Pierre Szikora was adapted to control the authentication exchange between the card and the reader. This code is an implementation of the authentication protocol method. The algorithm used to generate random numbers in Ultralight C cards has not been published by NXP so the most convenient methodology is the analysis (by means of a battery of randomness test) of a long sequence of outputs generated by the on-chip PRNG. We treat the algorithm, then, like a black-box that outputs nonces which are later tasted by us. Below is an example of the code used to capture those nonces:

```
$RndB = $cipher->decrypt($Resp1);
$fN=$RndB;
$fN=~ s/../pack("H2",$&)/ges ;
print "Random number Hex: $RndB";
$myFile="uc.dat";
```

Fig. 3. Picture of the laptop, card and reader during number generation

(a) Ultralight C (b) Mifare 1K

Fig. 4. Retrieved data in Hexadecimal format

```
open(PLOT,">>$myFile")
|| die("file not opening");
print PLOT $fN;
close(PLOT);
```

An additional shellscript was developed in order to reinitiate the authentication procedure once the nonces we were interested in were captured, without removing the card. Having tested the MIFARE Ultralight C, the same method was then applied to MIFARE 1K, which had already proven to have a quite weak PRNG (shown by the findings of Gans, Hoepman, and Garcia [2] for instance). Therefore, we tested the outcome of Gans, Hoepman, and Garcia [2], and verified the validity of the methodology used for MIFARE Ultralight C.

V. Analysis

Each time an authentication session was successful, the random numbers generated by the card were decrypted using the known encryption key and the nonces captured on hexadecimal format, as in Fig. 4.

Comparing these two sources of randomness, it was noticeable that the data generated by the Mifare 1K classic is much worse and even contains a number of duplications of the same values. Fig. 5 and Fig. 6 are an example of the final format of the data:

A file of 20 MB was created in the aforementioned way,

Fig. 5. Sample of the generated data for Mifare Ultralight C

Fig. 6. Sample of the generated data for Mifare 1K Classic

and analyzed using three different set of tools (NIST, ENT, Diehard).

Using such a vast amount of data was required by some tests in order to generate significant results. A sample of the results is shown in the following:

A. NIST Randomness Evaluation

More details on the figure can be found at http://www.lightweightcryptography.com/research/ultralightC.html

In Fig. 7 we show a extract of the results obtained after the NIST tests. The minimum pass rate for each statistical test, with the exception of the random excursion (variant) test is approximately = 0.960150 for a sample size = 100 binary sequences. The screenshot was taken in the beginning of the file, showing the first few tests. And as it shows, the p-values are not significant as they are greater than one per cent. All the other 188 different tests were successfully passed with a value higher than one per cent.

B. ENT Randomness Evaluation

The results obtained by the ENT test program are summarized below:

```
Entropy = 7.999991 bits per byte.

Optimum compression would reduce the size
of this 20480000 byte file by 0 percent.

Chi square distribution for 20480000
samples is 259.47,
and randomly would exceed this value
41.05 percent of the times.
```

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
17	16	8	7	5	10	7	11	9	10	0.145326	0.9700	frequency
12	11	6	13	5	11	15	5	13	9	0.236810	0.9900	block-frequency
19	7	16	10	10	3	9	10	8	8	0.030806	0.9800	cumulative-sums
19	10	9	6	9	12	13	6	7	9	0.129620	0.9700	cumulative-sums
8	16	12	15	9	9	10	8	6	7	0.350485	0.9900	runs
6	13	13	13	13	8	6	9	6	13	0.366918	0.9700	longest-run
6	9	10	14	10	9	13	13	8	8	0.739918	1.0000	rank
16	21	8	10	6	8	7	10	8	6	0.012650	0.9700	fft
5	9	8	8	7	18	10	13	13	9	0.181557	0.9900	nonperiodic-templates
11	6	14	12	15	8	6	8	6	14	0.224821	1.0000	nonperiodic-templates
8	6	9	10	6	12	10	12	13	14	0.637119	0.9900	nonperiodic-templates
12	8	12	13	9	12	5	13	8	8	0.657933	0.9900	nonperiodic-templates
6	9	10	8	11	11	13	12	13	7	0.798139	0.9900	nonperiodic-templates
10	8	8	16	12	5	6	14	9	12	0.275709	1.0000	nonperiodic-templates
9	5	11	20	9	11	8	6	10	11	0.090936	0.9900	nonperiodic-templates
11	13	10	12	7	5	14	10	13	5	0.366918	0.9900	nonperiodic-templates
14	9	11	11	8	11	8	9	11	8	0.946308	0.9600	nonperiodic-templates
9	13	8	11	13	10	12	10	5	9	0.798139	1.0000	nonperiodic-templates

Fig. 7. NIST Results

```
BIRTHDAY SPACINGS TEST, M= 512 N=2**24 LAMBDA=  2.0000
           Results for ulc.dat
                   For a sample of size 500:       mean
         ulc.dat            using bits  1 to 24    1.882
  duplicate       number       number
  spacings       observed     expected
       0            70.        67.668
       1           148.       135.335
       2           149.       135.335
       3            73.        90.224
       4            37.        45.112
       5            14.        18.045
  6 to INF           9.         8.282
Chisquare with  6 d.o.f. =       8.36 p-value=  .787152
 :::::::::::::::::::::::::::::::::::::::::::
                   For a sample of size 500:       mean
         ulc.dat            using bits  2 to 25    1.928
  duplicate       number       number
  spacings       observed     expected
       0            61.        67.668
       1           141.       135.335
       2           153.       135.335
       3            89.        90.224
       4            36.        45.112
       5            15.        18.045
  6 to INF           5.         8.282
Chisquare with  6 d.o.f. =       6.87 p-value=  .667059
```

```
Arithmetic mean value of data bytes is
127.5017 (127.5 = random).
Monte Carlo value for Pi is 3.143253823
(error 0.05 percent).
Serial correlation coefficient is
-0.000451 (totally uncorrelated = 0.0).
```

The results above show that the Mifare Ultralight C passed all the tests on ENT.

C. Diehard Randomness Evaluation

In Fig. V-C we show an extract of the results obtained by Diehard suite. The KSTEST for 10 p-values is: .656282. in accordance with the ENT and NIST, the test file passed all tests in Diehard.

D. Comparison of Ultralight C and 1K Classic

Similar methodology was then applied on both Mifare Ultralight C and Mifare 1K Classic generating 5Mb of data. The results are compared in Table I and Table II.

The results of the Ent test reveals that the output obtained from the Mifare Ultralight C are much closer, if not identical, to the required values, so indistinguishable from random. This is not the case of the Mifare 1K Classic, that shows extremely

TABLE I
ENT RESULTS

ENT	Ultralight C	Mifare 1K	Optimal
Entropy	7.999961	6.732108	8.0
Opt. Compres.	0%	15%	0%
Chi Square	273.49 (20,35%)	15546510.63 (0.01%)	
A. mean	127.5431	129.6220	127.5
Monte Carlo	0.04%	2.74%	0.0
S. Correlation	-0.000243	-0.189910	0.0

TABLE II
NIST AND DIEHARD RESULTS

NIST	Ultralight C	Mifare 1K
Pass	158/162	7/162

Diehard	Ultralight C	Mifare 1K
Overall p-value	.743979	N/A

poor results in comparison. Just as an example, the optimum compression ratio of the Mifare Ultralight C output is 0%, which is the optimum value, and much better to the 15% of the Mifare 1K Classic. This happens with all the other tests.

The NIST battery of tests shows seemingly random results for Mifare Ultralight C, which passed 158 tests from 162 (normal at a value of p=0.05) while the Mifare 1K obtained an awful results passing only 7 out of 162 tests. The conclusion is clear: The PRNG of the Ultralight C is extremely good, in absolute terms but especially when compared with the very poor of its predecessor 1K.

Despite the old adagio that states that speed and security are in many cases mutually exclusive, the performance of Mifare Ultralight C is clearly much better than that of the Mifare Classic 1K, as can be easily seen in Table III). This is particularly significant because the size of the nonces in the ultralight C is larger than that of the 1K. Generating 1,000 nonces took 1:03 minutes in the case of the Ultralight C, with 8 byte nonces, whilst the a similar nonce generation proccess spent a considerable larger 7:04 minutes in the 1K, with 4 byte nonces.

VI. CONCLUSION

This paper was designed to analyse the security of the PRNG which is used in the authentication protocol of the new NXP MIFARE Ultralight C. The aim was to investigate the nonces generated by the card, and assess its randomness and any possible attacks. Any bad properties found in that PRNG could have compromised the security of the whole authentication protocol. However, no weaknesses were found after three complementary methods were applied to examine large quantities of nonces. The NIST, ENT and Diehard batteries were applied to 20 MB of data generated by the MIFARE Ultralight C. The file successfully passed all test batteries and we can conclude that the generated data looks as coming from a random source. Furthermore, we can state that the PRNG seems not vulnerable to easy cryptanalysis, and that exploiting the nonce used in the authentication protocol is not advantageous to an adversary. Having tested the MIFARE Ultralight C, a similar methodology was then undertook for 5 MB data generated by MIFARE Ultralight C and MIFARE Classic 1k. This comparison was applied to confirm the validity and credibility of the methodology applied on MIFARE Ultralight C, since MIFARE 1K has already shown security weaknesses. The comparison between findings on both cards proved the security strength of the PRNG in MIFARE Ultralight C taking into account not only the methodologies results but also the performance and improvements achieved. In conclusion, MIFARE Ultralight C proved to overcome security aspects created by the previous weak PRNG. Although random numbers used in authentication protocol in MIFARE Ultralight C provided with enough randomness, the MIFARE Ultralight C could still be open to other security attacks, something that we continue to investigate and will explore in future works.

TABLE III
PERFORMANCE ANALYSIS

1000 nonces	Ultralight C	Mifare 1K
Time	1:03 minutes	7:04 minutes
Size	8000 bytes	4000 bytes

REFERENCES

[1] Finkenzeller, K. (2010). *RFID Handbook Fundamentals and Applications in Contactless Smart Cards, Radio Frequency (3rd Ed.).* Chicester: John Wiley and Sons Ltd

[2] Gans, G. K., Hoepman, J., and Garcia, F. D. (2008). A Practical Attack on the MIFARE Classic [Electronic version]. *Lecture Notes in Computer Science;* 5189, 267-282

[3] Gu, Q. (2010). *Security in Emerging Wireless Communication and Networking Systems*. Berlin : Springer-Verlag Berlin and Heidelberg GmbH & Co. KG.

[4] Juels, A. (2006). RFID Security and Privacy: A Research Survey [Electronic version]. *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS,* 24 (2), 381-394

[5] Luo, Q. (2010). *Advances in Wireless Networks and Information Systems.* Berlin: Springer-Verlag Berlin and Heidelberg GmbH & Co. KG

[6] Mifare.net (n.d.). *The success of MIFARE.* Retrieved March 2011, from http://www.mifare.net/

[7] MF0ICU2 (2009). *MIFARE Ultralight C* MIFARE Ultralight C. retrieved December 2010 from http://www.nxp.com/documents/short_data_sheet/MF0ICU2_SDS.pdf

[8] Nohl, K., Evans, D., and Plotz, H. (2008). *Reverse-Engineering a Cryptographic RFID Tag.* Retrieved December 2010 from: http://www.usenix.org/event/sec08/tech/full_papers/nohl/nohl_html/

[9] Piramuthu, S. (2007). Protocols for RFID tag/reader authentication. *Decision Support Systems,* 43 (3), 897-914

[10] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J. & Vo, S. (2001). *A statistical test suite for random and pseudorandom number generators for cryptographic applications.* Retrieved December 2010 from, http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22b.pdf

[11] Sobh, T, Elleithy, K. & Mahmood, A. (2008). *Novel algorithms and techniques in telecommunications, automation and industrial electronics.* New York : Springer-Verlag New York Inc.

[12] Yalcin, M.E., Suykens, J.A. & Vandewalle, J. (2004). True Random Bit Generation From a Double-Scroll Attractor [Electronic version]. *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS;* 51 (7), 1395 - 1404

[13] Tianjie Cao, Peng Shen, Elisa Bertino: Cryptanalysis of Some RFID Authentication Protocols. JCM 3(7): 20-27 (2008)

[14] Garcia, Flavio D.; Peter van Rossum; Roel Verdult; Ronny Wichers Schreur. Wirelessly Pickpocketing a Mifare Classic Card. 30th IEEE Symposium on Security and Privacy (S&P 2009), IEEE.

[15] Garcia, Flavio D.; Gerhard de Koning Gans; Ruben Muijrers; Peter van Rossum, Roel Verdult; Ronny Wichers Schreur; Bart Jacobs. Dismantling the MIFARE Classic. 13th European Symposium on Research in Computer Security (ESORICS 2008), LNCS, Springer.