RFID Noisy Reader
How to Prevent from Eavesdropping on the Communication?

O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert, J. Reverdy

CEA-LETI, 17 avenue des Martyrs, 38054 Grenoble Cedex 9, France

Abstract. RFID applications do not always use encryption to ensure the security as public key cryptographic algorithms that are costly in term of computing resources. We proposed to secure the communication from an ISO 14443 RFID card to the reader against passive eavesdropping at the physical layer by adding noise. During the card reply, the reader generates an appropriate noise that is modulated by the load of the card. By knowing the noise it emitted, the reader is able to subtract it and to retrieve the card message when a spying probe in the field is inefficient.
Keywords: RFID, ISO 14443, smartcard, RNG, Tausworthe cell, eavesdropping.

1 Introduction

RFID techniques were born in the late 80's and early 90's and are nowadays widespread in a certain number of application fields: logistics, access control, cashless payment, transport ticketing, electronic passports, and health cards [1,2]. The main advantage of RFID devices is the absence of physical contact with the reader. Thus, operations are simplified and transactions are quicker. However, this contactless side makes privacy concerns come up. Indeed, RFID devices can easily be used to track people or items, to read data stored without the user's consent and even to eavesdrop on the communication during the reading. Many surveys can be consulted to have a comprehensive overview of RFID security and privacy issues [3,4,5]. Why not imagine a hacker listening to the communication when you present your electronic passport to the customs officer or when you fill your electronic purse. This possibility of eavesdropping is claimed by several papers [6] and relayed by press reports as the US National Institute of Science and Technology (NIST) that eavesdropped on the RFIDs to be used in US passports from as far as 9 meters [7,8].

The basic solution to overcome this threat is to encrypt the communication and to ensure the authentication of the user. This encryption is for example applied in the second level of security of the e-passports named BAC for Basic Access Control [1]. Nevertheless, only the first level of security is used in most countries and it does not involve any cryptography. Moreover, cryptographic algorithms are expensive in term of computing resources (this is particularly true

for public key algorithms) and are time consuming when RFID devices should be satisfied with a minimum energy supply because of the remote powering.

To prevent from passive eavesdropping on communication, it could be useful to ensure security at the physical layer. This aim can be achieved by applying noise at the air interface level. Thus, we propose according to a patent we deposited in 2004 [14] to add an analog noise to the magnetic field sent by the reader to power the card during the transmission in the way card to reader. The card will only apply a load modulation on this noisy magnetic field to communicate its data. As the reader knows the noise that it emitted, it is able to filter it and to retrieve the contactless card message. This solution prevents a spying probe in the field from understanding the noisy transmission. The message from the card to the reader becomes protected. Actually, this communication way is the most sensitive since it is often the user who sends confidential data whereas the reader merely sends commands. Moreover, the use of private key algorithms can be considered instead of costly public key algorithms since the card is then able to convey a secured message that can be a private key. The environment of this noisy reader will be described in detail in the first part of our article with standard and modulation considerations. Then, the generation of the noise will be discussed and finally we will show how we filter the noise from the tag message and what kind of protection we can expect with the help of simulations.

2 The noisy reader principle

2.1 The principle

To understand the principle of the noisy reader, we have to remind how contactless cards answer to a RFID reader. RFID uses a sequential two-way transmission since card and reader are not able to perform a full duplex communication. The reader modulates the carrier frequency it emits to convey a command. During the card reply, the reader still emits this carrier frequency but with a constant amplitude to power the RFID devices in its field. To transmit a message, the card that can not supply power, modulates a resistive or capacitive load at its antenna terminals. The load change creates a variation in the coupling of the two antennas. Thus, the reader sees a varying emitted magnetic field and can demodulate a card message.

The noisy reader is a modified reader that sends an analog noisy signal added to the field that enables the tag powering. The RFID card during its reply modulates this noisy signal in order that any probe in the field could not eavesdrop on the answer. The reader, by knowing the noise that it sent, is able to subtract this noise and to retrieve the tag answer. Figure 1 explains how the device works. An eavesdropping probe in the field does not know the emitted noise so it cannot demodulate the answer. C. Castelluccia and G. Avoine [15] developped an apparently similar solution they named "noisy tag". A special tag shares a key with the reader to create a secure exchange channel. Thus, the noisy tag emits some bits generated with this key known only by the reader during the reply of the tag to be read. The noise created by the noisy tag should prevent from

the eavesdropping on the communication but the communication can still be understood by the reader since it is able to subtract it. This approach presents some important drawbacks. First of all, it requires a key agreement that implies to change the ISO standards. Secondly, the noise generated is digital (bits are sent) then it will be really unlikely that a spying probe in the field sees the signal from the noisy tag and from the tag with the same amplitude. It will be always possible to see a difference that is enough to retrieve the message from the tag. Later on, E. Haselsteiner and K. Breitfuss [16] proposed a variant where the role of the noisy tag is played by the reader with the same drawback that is shown in the second point.

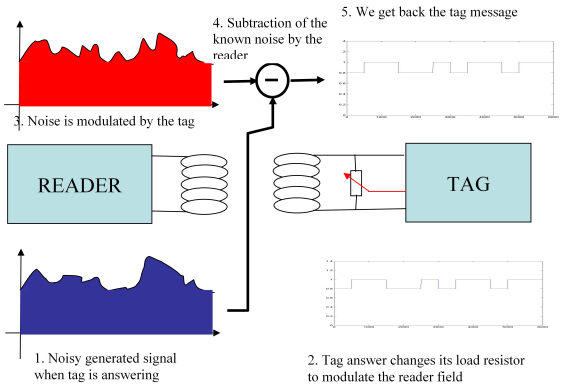

Fig. 1. The principle of the noisy reader. First, the reader generates a noisy signal and emits it through its antenna during the period of the tag answer. Secondly, the tag, in order to answer, modulates its load as any other tag. So the reader or a spying probe in the field will see a noisy signal where the tag message is hidden. But, as the reader knows the noise it emitted, it can subtract it from the signal it received to retrieve the tag message.

2.2 The standards

The "RFID" term encompasses a certain number of different devices in the near field communication domain. Since it is not possible to implement all the available standards, we had to make a choice to show the feasibility of our approach. The RFID cards can use LF, HF and UHF bands. Three standards require the HF band interfaces: ISO 14443 [9] for "proximity" devices with a reading distance around 10 cm, ISO 15693 [10] and ISO 18000 [11] for "vicinity" devices with an operating range up to 1 meter. The EPC class-1 standard [12] is also well known for UHF tags required for items identification and management.

The use of the noisy reader can be justified when the card has an important amount of confidential data to transmit or when those data require a high level

of security. Thus, the standards dealing with identification of items like EPC and ISO 18000 or with identification of people like ISO 15693 present a medium interest. So our effort was focused on the ISO 14443 standard that targets applications with a higher added value like electronic passport, transport ticketing, electronic purse, etc... Indeed, those applications manipulate an important number of data that should be highly protected.

2.3 Modulation

In the framework of the ISO 14443, two types coexist: type A and type B with different bit codings in the reply of the card. Concerning the modulation, both types use a carrier at 13.56 MHz and a sub-carrier at 847 kHz. The bit coding of the type A is a simple Manchester coding of the sub-carrier. The advantage of this coding is that each bit shows a transition in the signal and that it is simple to generate. Indeed, it is just necessary to carry out logic "XOR" between the data and the clock. Thus, as shown on Fig. 2. The logic "1" has always the same shape with a negative transition at the middle of the bit. The logic "0" has always the same shape with a positive transition at the middle of the bit.

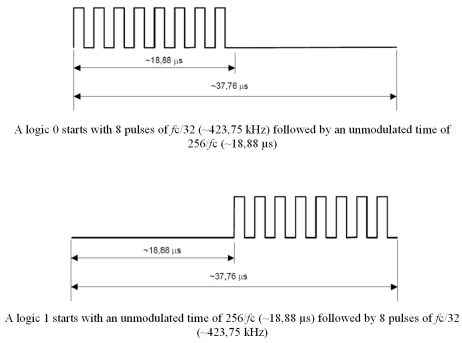

Fig. 2. Type A bit coding of the card reply

The type B uses the same sub-carrier as the type A, but it uses a BPSK modulation (Binary Phase Shift Keying) with phase shift that should occur at nominal positions of rising or falling edges of the sub-carrier as shown on the Fig.3 . Bit coding shall be NRZ-L where a change of logic level shall be denoted by a phase shift (180°) of the sub-carrier. This phase shift is really robust to noise and difficult to blur. As a consequence, the type B should be chosen to prove the feasibility of the noisy reader.

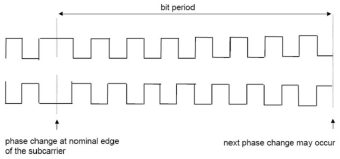

Fig. 3. Type B bit coding of the card reply

2.4 Noise description

Knowing the framework, the ISO 14443 standard Type B, two different considerations should be kept in mind to generate the convenient noise. First, to prevent from an easy filtering of the noise by a spying probe and to keep an energetic efficiency, the noise must be in the same bandwidth as the card message. Secondly, the modulated load of the card can be resistive or capacitive. So, the system should not only blur an amplitude modulation but also a phase modulation. To fulfill the first point, the noise should be bit synchronous with the card answer at a 106 kHz frequency with the same sub carrier at 847 kHz as shown in Fig.4 . Finally, we should be able to modulate the amplitude and the phase of this signal by a random value at 106 kHz. A temporal example of such a noise in Fig.5. Its PSD can be formulated by Eq.1 where 1/Tb is two times the frequency of the sub-carrier at 847 kHz and 1/T is the bit rate at 106 kHz.

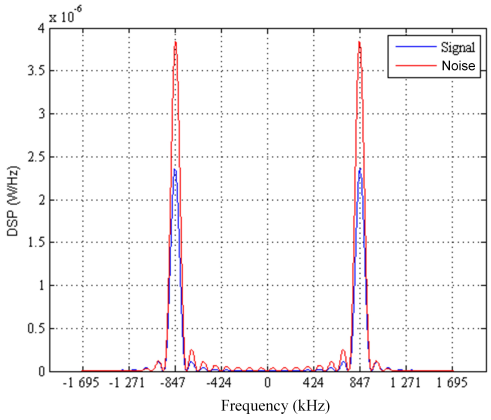

Fig. 4. The noise power spectral density compared to the card reply power spectral density around the carrier frequency represented by the 0 frequency.

$$\Gamma_b(f) = \frac{T_b^2}{T}\mathrm{sinc}^2(\pi f T_b)\left(\frac{\sin(16\pi f T_b)}{\cos(\pi f T_b)}\right)^2 \quad (1)$$

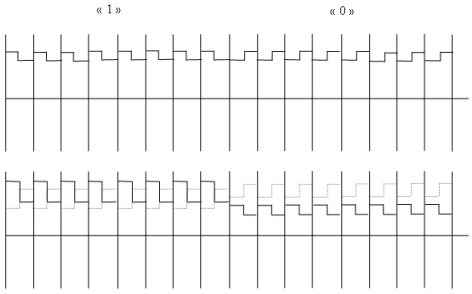

Fig. 5. Above: 2 bits of a tag answer (bit rate 106 kbits), Below: The noise added synchronized with the tag answer (bit synchronized) as it could be seen with a probe in the field. We can notice that the noise is not specific to a "1" or "0" and that its phase and amplitude are varying.

3 Noise generation

3.1 Random number sequence

Noise is generated by a random number generator (Fig. 6 and Fig.7) based on three Tausworthe cells, which are particularly efficient for a hardware implementation [13]. The random sequence follows a uniform distribution and has a 2^{88} period (much longer than a RFID 14443 frame); numbers are generated each 106 kHz clock rising edge. Generated numbers are 7 bit width.

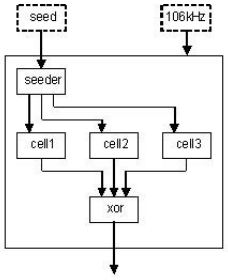

Fig. 6. Tausworthe random number generator

Each Tausworthe cell needs an initial seed, which should be different each time the generator starts (i.e. for each tag answer). For a given three seeds set the generator will always produce the same random sequence (2^{88} numbers long), that why it is important to have a pseudo-random seed. To obtain this we use a binary counter clocked with an uncorrelated 1.8432 MHz frequency. The counter value is read when the generator starts; a full-combinatorial mixer helps obtaining a different 32 bit number for each cell.

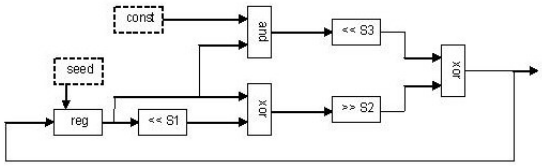

Fig. 7. Tausworthe cell

3.2 Random number modulation

A composite modulation is used to transform the 13.56 MHz carrier: a two state phase shift keying and an envelope modulation. More precisely its phase is changed every 847 kHz rising or falling edge from 0° to 180° and its envelope is multiplied every 106 kHz by a 7 bit random number. An example of such a signal is given in Fig.8.

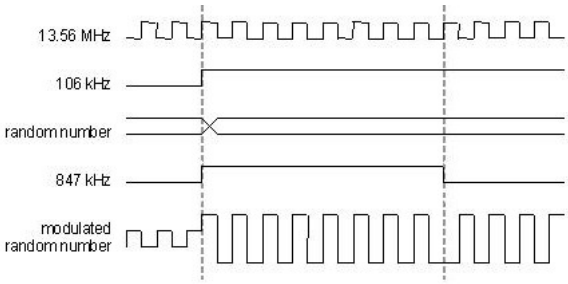

Fig. 8. noisy modulation of the sub-carrier

3.3 Noise generation

The noise generator is composed of two Tausworthe modulated generators in 13.56 MHz quadrature (for each phase I and Q). Two desynchronised counters are used to make the initial pseudo-random seed for each generator. A numerical registered adder takes care of the 7 bits noisy voices mix; note that the generator and the output signal is 8 bits width and have a 54.24 MHz clock domain (Fig.9).

In order to blur only the tag answer, the noise generator needs a signal from the reader which detects a frame emitted by the tag in the field. Then to ensure that the noise 106 kHz is well synchronized with the tag answer one, the noise generator should be aware of the answer "start-of-frame" which is detected by the reader.

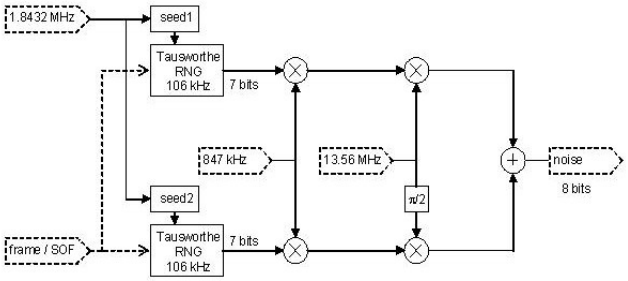

Fig. 9. Noise generator schematic

3.4 Noise amplification to magnetic field

Thanks to an 8 bit digital-to-analog converter working at a 54.24 MHz sampling frequency, the generated numeric noise is transposed to an analog signal. DAC output, which has a 50Ω resistive load, is wired to a 0-40 dB attenuator followed by a 1W power amplificator (see Fig.10).

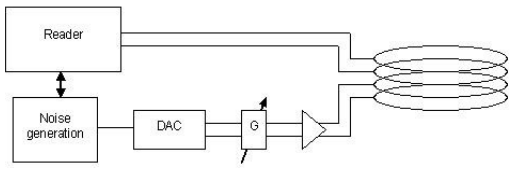

Fig. 10. Noise in magnetic field introduction

4 Noise subtraction

4.1 Modelling

Before developing the noisy reader, we design a model of the system described by Fig.11 and Eq.2 (q_1 is the charge of the C_1 capacitor).

$$\begin{cases} E(t) = r_1 i_1(t) + \frac{q_1}{C_1} + L_1 \frac{di_1}{dt} + M_{1b} \frac{di_b}{dt} + M_{12} \frac{di_2}{dt} + M_{1E} \frac{di_E}{dt} \\ e_b(t) = r_b i_b(t) + \frac{q_b}{C_b} + L_b \frac{di_b}{dt} + M_{1b} \frac{di_1}{dt} + M_{2b} \frac{di_2}{dt} + M_{Eb} \frac{di_E}{dt} \\ 0 = r_E i_E(t) + \frac{q_E}{C_E} + L_E \frac{di_E}{dt} + M_{1E} \frac{di_1}{dt} + M_{Eb} \frac{di_b}{dt} + M_{2E} \frac{di_2}{dt} \\ v_2(t) = L_2 \frac{di_2}{dt} + M_{12} \frac{di_1}{dt} + M_{2b} \frac{di_b}{dt} + M_{2E} \frac{di_E}{dt} \\ v_2(t) + R_2 C_2 \frac{dv_2}{dt} = -R_2 i_2 \end{cases} \quad (2)$$

The reader, the noise generator, the card and the spying probe are modeled by RLC circuits. The coupling between the noise generator and the reader is

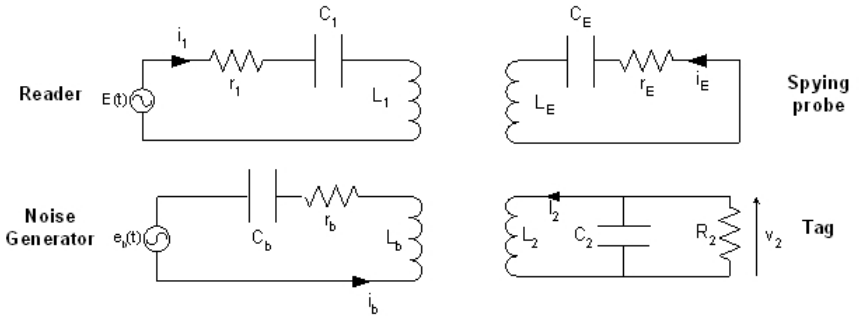

Fig. 11. The model of the system

null. Thus, the reader does not see (at a first-order) the noise generator. During the card emission, we have:

$$E(t) = E_0 \cos(\omega_0 t) \tag{3}$$

And when the noise is emitted, we define:

$$E_b(t) = G \cdot E_0 \left[b_I(t) \cos(\omega_0 t) - b_Q \sin(\omega_0 t) \right] \tag{4}$$

where b_I and b_Q are random variable with an uniform distribution between -1 and 1. Moreover, we described the different components with realistic values:

$$\begin{cases} r_1 = r_E = r_b = 7.3\Omega \\ L_1 = L_b = L_E = 1.5\mu H \text{ and } L_2 = 1.7\mu H \\ k_{1b} = 0 \text{ except if it is specified where } M_{ij} = k_{ij}\sqrt{L_i L_j} \end{cases} \tag{5}$$

During the load modulation, the card resistor R_2 varies from 220Ω to 440Ω. The system of equations is solved using Simulink. This software also helps us to demodulate the signal. First this signal is filtered by a bandpass that only keeps one sideband around the carrier frequency at 13.56 MHz. A sampling at the same frequency is then applied. A last filter and a correlator are used to define the emitted bit.

The model was tested with different configurations of the card, of the noise generator, of the reader and of the spying probe that are specified through the coupling factors k_{ij}. Those values reflect the distance between the devices. We calculated the Bit Error Rate (BER) after the demodulation according to the gain G applied on the noise. A BER near 0.5 discloses a good jamming of the signal whereas a weak BER ($< 10^{-3}$) is the sign that the message remains intelligible. In this system, it is important to obviously emit a high noise to jam the spying probe. But, the noise should be also low for the reader to understand the tag message. The first results of simulations quickly show that a null coupling is a good approach but not sufficient. Indeed, the reader still sees an image of the noise that is sent back by the card or even by the spying probe.

4.2 Noise filtering

To be able to increase the amount of noise, its subtraction was implemented in the reader. First, the noisy signal is filtered by a band pass to keep only one sideband. Secondly, it is sampled at the carrier frequency to work in the base band. Then a correlation is made with this signal and the sub-carrier retrieved by the reader (847 kHz pulses). The result of this correlation that is emphasized by a sub-sampling will show the phase shift of the BPSK coding (Cf Fig.12).

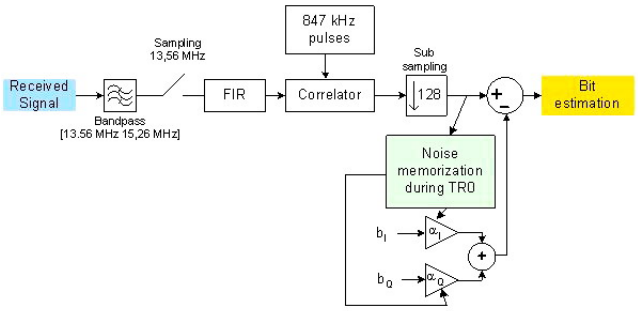

Fig. 12. Schematic of the noise subtraction

Finally, we took advantage of the time TR0 just after a reader command and just before the card answers and emits the sub-carrier. The time TR0 enables to assess the channel response to the emitted noise. During TR0:

1. Emission of noise during 9.44µs with b_I=1 and b_Q=0 then signal recording after the sampling of only one sample α_I
2. No emission of noise during at least 1.18µs
3. Emission of noise during 9.44µs with b_I=0 and b_Q=1 (the same signal in quadrature) then signal recording after the sampling of only one sample α_Q

Thus during the emission of the card:

1. The noise generator emits two random numbers at the instant n (b_{In},b_{Qn})
2. The noise to be subtracted at the instant n after the sub-sampling is :

$$bs_n = \alpha_I \cdot b_{In} + \alpha_Q \cdot b_{Qn} \tag{6}$$

4.3 Performances

The worst case for the security of the system is when the spying probe is close to the card. Indeed, this is the place where the amplitude of card signal is the most important whereas the noise is relatively weak because the spying probe is far

from the noise generator. This configuration was modelled by taking a really good coupling factor between the card and the spying probe $k_{2E} = 0.5$ that can be obtained when the probe is put on the card. The other coupling factors are taken to model a card at 3 cm from the reader ($k_{1b} = 0$; $k_{12} = k_{b2} = k_{1E} = k_{bE} = 0.1$). Figure 13 shows that when G is equal to 0.6, the BER is 10^{-3} for the reader (enough for the reader to read correctly the message) whereas the BER is 0.3 for the spying probe showing that the message will remain unintelligible for the hacker.

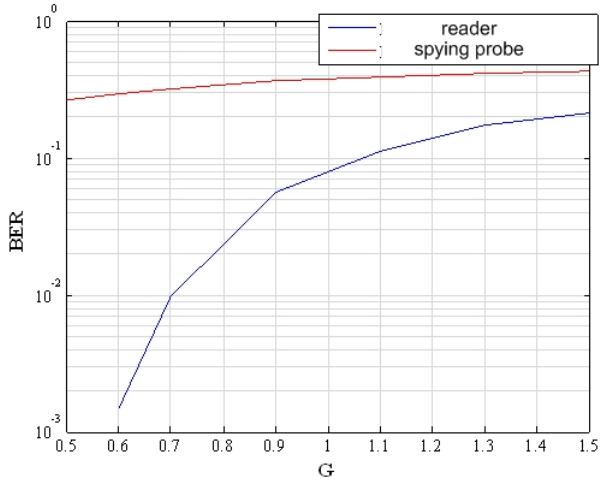

Fig. 13. BER depending on G. From the point of view of the reader and of the spying probe. In this case $k_{1b} = 0$; $k_{12} = k_{b2} = k_{1E} = k_{bE} = 0.1$ (the card is at 3 cm from the reader) and $k_{2E} = 0.5$ (the spying probe is put on the card)

The security of the system will be reduced if we take away the card from the reader. Figure 14 shows the result of this case where the card is at 10 cm from the reader ($k_{1b} = 0$; $k_{12} = k_{b2} = k_{1E} = k_{bE} = 0.01$). Obviously, G should be increase and be equal to 1.5 to find back the previous situation.

Unfortunately, Figure 13 points out that such a G value does not enable the reader to understand the message since the BER is 0.1. This problem can be overcome by using the Automatic Gain Control (ACG) implemented in the reader to detect the reply from the card. The ACG gives an information about the coupling factor between the card and the reader and can fruitfully be used to adapt the noise gain G. After a calibration of this gain, the channel will become totally secure.

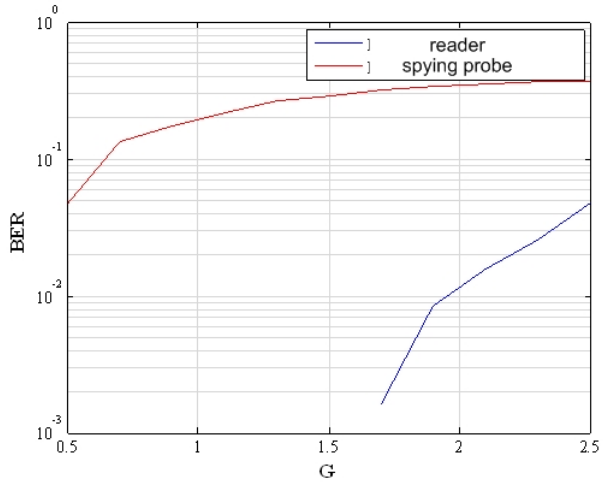

Fig. 14. BER depending on G. From the point of view of the reader and of the spying probe. In this case $k_{1b} = 0$; $k_{12} = k_{b2} = k_{1E} = k_{bE} = 0.01$ (the card is at 10 cm from the reader) and $k_{2E} = 0.5$ (the spying probe is put on the card)

5 Conclusion

RFID smartcards are vulnerable to communication eavesdropping when no encryption is applied. We proposed a third object that could be added to a ISO 14443 RFID reader that secures the physical layer by emitting analog noise during the smartcard reply and that without changing anything in the ISO standard. A specific noise in the exact bandwidth of the card and with the same power spectral density shape is transmitted via its own antenna designed to be in a null coupling configuration with the reader one. Two random numbers generators based on three Tausworthe cells compute a sequence of numbers at 106 kHz that modulates the sub-carrier and the carrier provided by the reader. Simulations of a model of the system show that this null coupling is not enough to ensure a safe transmission since a card in the reader magnetic field will send it back an image of the noise. We took advantage of the guard time TR0 between the end of the reader command and the start of the card sub-carrier generation to assess a channel response to the emitted noise. As a consequence, the reader is able to subtract with a correlation the known noise to retrieve the card message. Then a noise with the same maximum amplitude as the reader is able to blur efficiently the card transmission. The simulations disclose that a noise gain between 0.6 to 1.5 is sufficient to ensure a secure channel. However, the noise gain should be adapted with the distance from the card to the reader. The use of the reader ACG enables to adjust the noise gain and to overcome this problem .

6 Acknoledgement

This project was partly financed by the European Commission in the frame of the Discreet project.

References

1. International Civil Aviation Organization (ICAO). Document 9303 Machine readable Travel Documents (MRTD). Part I: Machine readable Passports, 2005.
2. Mastercard Paypass. Htpp:\\www.paypass.com
3. A. Juels, R.L. Rivest, M. Szydlo : Selective blocking of RFID tags for consumer privacy. In 10th Annual ACM CCS 2003, May 2003
4. K. Finkenzeller. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. John Wiley & Sons, Ltd, 2003.
5. S. Garfinkel, B. Rosenberg, RFID Applications, security, and privacy, Ed. Addison Wesley, 2005
6. Z. Kfir, A. Wool. Picking virtual pockets using relay attacks on contactless smartcard systems. Proceedings IEE/CreateNet SecureComm, pp47-58, 2005.
7. J. Yoshida. Tests reaveal e-passport security flaw. http://www.eetimes/showArticle.jhtml?articleID=45400010
8. G.P. Hancke, Practical Attacks on Proximity Identification Systems (Short Paper), http://www.cl.cam.ac.uk/~gh275/SPPractical.pdf
9. ISO 14443 Identification cards - Contactless integrated circuit cards - Proximity cards
10. ISO 15693 Identification cards - Contactless integrated circuit cards - Vicinity cards
11. ISO 18000 RFID for item management
12. EPC Class-1 Generation 2 UHF RFID Conformance Requirements Specification
13. G. Zang, D. Lee, R. Cheung, The Chinese University of Hong Kong, University of California, Imperial College London, Ziggurat-based hardware Gaussian random number generator, 2004.
14. Patent WO 2006/035178 A1, F. Dehmas, E. Crochon, F. Vacherand , 2004.
15. C. Castelluccia, G. Avoine, Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags, Proceedings of CARDIS 2006, 289-299, 2006
16. E. Haselsteiner, K. Breitfuss, Security in near field communication, Workshop on RFID security, July 2006