PRIVACY ISSUES IN RFID BANKNOTE PROTECTION SCHEMES

Gildas Avoine
Swiss Federal Institute of Technology (EPFL)
Security and Cryptography Laboratory (LASEC)
CH-1015 Lausanne Switzerland
gildas.avoine@epfl.ch

Abstract Radio Frequency Identification systems are in the limelight for a few years and become pervasive in our daily lives. These smart devices are nowadays embedded in the consumer items and may come soon into our banknotes. At *Financial Cryptography 2003,* Juels and Pappu proposed a practical cryptographic banknote protection scheme based on both Optical and Radio Frequency Identification systems. We demonstrate however that it severely compromises the privacy of the banknotes' bearers. We describe some threats and show that, due to the misuse of the secure integration method of Fujisaki and Okamoto, an attacker can access and modify the data stored in the smart device without optical access to the banknote. We prove also that despite what the authors claimed, an attacker can track the banknotes by using the access-key as a marker, circumventing the randomized encryption scheme that aims at thwarting such attacks.

Keywords: RFID, Privacy, Banknote Protection.

1 Introduction

The main goal of Radio Frequency Identification (RFID) systems is to identify objects in an environment by embedding tags onto these objects. A tag is a tiny device capable of transmitting, over a short distance, a unique serial number and other additional data. For instance, goods in stores can be tagged in order to prevent shoplifting, or to speed up the goods registration process by using wireless scanning instead of human or optical scanning. The security issues of such systems are therefore two-fold. On one hand, it must be impossible to thwart the system by modifying the tag's data or even creating fake tags; on the other hand, tags should not compromise the bearers' privacy.
It is vital to ensure the security of RFID systems, since many organiza-

tions have already turned to use such devices for many large-scale applications. In particular, the European Central Bank (ECB) decided to use some RFIDs to protect Euro banknotes [13]. Although Euro banknotes already include physical security features, ECB believes that RFIDs will add further protection: electronic tags will give governments and law enforcement agency the means to track banknotes in illegal transactions. We do not know yet if such chips will be embedded into all Euro banknotes, or just those of a high denomination. Japanese government also plans to embed RFIDs into new 10'000 Yen notes [9]. Though these examples may be just rumors until now, we can consider that such devices will be used for such applications soon. Up to now, RFIDs are already used in less sensitive applications. For instance, the tire manufacturer Michelin decided to implant RFID tags inside the rubber sidewall of its tires. These tags contain the tire's unique ID and maybe some other data such as origin, maximum inflation pressure, size, etc. The data stored in these tags are readable by a receiver positioned up to 30 inches away from the tire. These tags could pinpoint, for example, tires belonging to a defective batch. The purpose currently is to identify and track tires, but it could be adapted to allow tags to communicate directly with the vehicle's dashboard to indicate if the tires are properly inflated, overheated, overloaded, or if the tire tread is seriously worn [7]. Michelin Tires' RFID system is currently being tested in some taxis and rental cars, but it could be extended to all Michelin Tires after 2005.

When technology advances, research on the privacy and security aspects of such devices lags far behind. Security flaws could however result in large-scale consequences from a sociological and economic point of view, by flooding the market with fake-tagged items. By proposing the first cryptanalysis of a scheme specially designed for RFID systems, we show that, up to now, such systems can not be used in practical applications without endangering the users' privacy.

In this paper, we first describe the main characteristics of the RFIDs and present in Section 3 the Juels – Pappu banknote protection scheme [8], which uses RFIDs. We then describe in Section 4 some potential threats to this scheme and show that, due to the misuse of the secure integration method of Fujisaki and Okamoto, an attacker can access and modify the data stored in the smart device without optical access to the banknote. We also prove that despite the claims of the authors, an attacker can track the banknotes by using the access-key as a marker, circumventing the randomized encryption scheme that aims to thwart such attacks.

2 Radio Frequency Identification Systems

In this section, we describe the technical aspects of RFID systems, which consist of three elements:

- The RFID tag *(transponder)* that carries the identifying data;
- The RFID readers *(transceivers)* that read and write the tags' data.
- The back-end database, connected to the readers, that records information related to the tags data.

While tags are low-capability devices, as explained below, readers and back-end database have powerful capability of storage, computation and communication. Therefore readers and back-end database can communicate through a secure channel.

2.1 Tags

In order to use RFID tags in large-scale applications, the per-unit cost of such devices should be very low. Currently, the cost of such devices is a few tens US cents [12] and would further drop to 5 US cents [10]. On the other hand, practical applications require that the tag size be as tiny as a few millimeters square. Cost and size requirements mean that power consumption, processing time, storage and logical gates are extremely limited. From a technical point of view, a tag consists of an antenna and a microchip capable of storing data and performing logical operations such as bit-string comparisons of keys. One can distinguish *active* tags which have a battery to run the microchip's circuit and to broadcast a signal to the reader, from *passive* tags which have no battery. Active tags are suitable to track high cost items over long ranges but they are too expensive to be embedded into banknotes. Only passive tags are suitable for this application. Tags memory is small and can store only a few hundreds bits in the best case [4]. Tags contain a few thousands gates, which is below the threshold of embeding cryptographic algorithms. For instance AES typically requires about 20,000 gates and SHA-1 requires about 15,000 gates. From a security point of view, tags can not be considered as tamper-resistant: all physical threats, such as laser etching, ion-probes, clock glitching, etc. [12] are applicable to recover the data stored in the tag. Therefore the tag cannot securely store secret keys in the long term, for instance.

2.2 Communication

As will be explained in Section 2.3, the reader can transmit various commands to the tag. In order to do this, the reader broadcasts Radio

Frequency radiation as long as necessary to bring sufficient power to the tag. The tag modulates the incoming radiation with its stored data. We actually consider two channels: the *forward channel* from the reader to the tag which can operate over long distance and the *backward channel* from the tag to the reader which can operate over a shorter distance. Both channels can be eavesdropped by an attacker since it is obviously impossible to use cryptographic features.

2.3 Interface

We give below the common commands that are available on a tag:

- `read`: allows every reader to obtain the data stored in the tag memory.
- `write`: allows every reader to write data in the tag memory.

Some other commands can be available on a tag:

- `sleep`: this command is keyed so that the reader has to send a key in order to put the tag into the sleep state. Then the tag does not respond to the reader's queries until it receives the `wake` command with the legitimate key.
- `wake`: after this command, the tag starts afresh to respond to the reader. It is a keyed command associated with the `sleep` command.
- `kill`: this command destroys the tag definitively.

Moreover, Juels and Pappu [8] suppose that the following commands are available:

- `keyed-read`
- `keyed-write`

These commands are similar to the `read/write` commands except that they are keyed.

3 Juels – Pappu banknote protection scheme

3.1 Interested parties

Juels and Pappu proposed a banknote protection scheme whose goal is to resist banknotes counterfeiting and track traffic flows by some law enforcement agency, nevertheless guaranteeing the privacy of the banknote

handlers. First we describe all the interested parties who are involved in the scheme.

- *Central bank.* The central bank aims at creating banknotes and at avoiding banknote forgery. It is therefore in its interest to have unique banknote serial numbers and to protect the secret key, which is used to sign the banknotes.
- *Law enforcement agency.* The goal of this agency is to arrest forgers. In order to achieve this, it needs to track banknotes and detect fake ones easily, even in areas of dense traffic, such as airports.
- *Merchants.* Merchants handle large quantities of banknotes. It is conceivable that they will try to compromise their clients' privacy. Merchants may comply with the law enforcement agency by reporting irregularities in banknote data.
- *Consumers.* Banknotes bearers want to protect their privacy. They want therefore to limit banknotes tracking even if it means not respecting existing laws.

3.2 Concept and requirements

Up to now, banknote security solely relies on optical features, which can be checked either by human-scanning or machine-scanning. In [8] security relies on both optical and electronic features. Banknotes thus have two data sources:

- *Optical:* data can be encoded in a human-readable form and/or in a machine-readable form such as a two-dimensional bar code. It contains banknote serial number as well as denomination, origin, etc.
- *Electronic:* data can be read by wireless communication. Data are signed by the central bank and encrypted with the law enforcement agency public key and a random number.

Electronic data are stored in a RFID tag, which consists here of two cells whose access is key-protected. The access-key can be (re-)generated from the banknote optical data. One of the two cells, denoted γ, is universally readable but keyed-writable. The other cell, denoted δ, is both keyed-readable and keyed-writable. In [8], the proposed scheme consists in writing in γ the serial number of the banknote signed by the central bank and encrypted with the law enforcement agency public key. If this encrypted value was static, then an attacker could still track the banknote using this value as a marker. To overcome this weakness, the

signature on the serial number is re-encrypted by merchants as often as possible, using obviously a probabilistic encryption scheme. Since the signature is available from the optical data, encryption is performed from scratch and does not need to be homomorphic. After the re-encryption is performed, the new encrypted value is put into γ and the used random value r is put into δ. Since γ and δ are keyed-writable, one must have optical contact with the banknote to obtain the access-key and thereby to re-encrypt the banknote. We will detail this procedure in Section 3.3.

We give below the requirements that [8] should guarantee.

- *Consumer privacy.* Only the law enforcement agency is able to track the banknotes using the RFID interface. Even the central bank is not allowed to track banknotes.
- *Strong tracking.* Law enforcement agency are able to identify a banknote (by its serial number) even without optical contact.
- *Minimal infrastructure.* In order to be user-friendly, the system should not require that banknote bearers possess special equipment. For their part, retail banks and shops should only buy devices at reasonable cost. Furthermore, they should not be required to set up a permanent network connection.
- *Forgery resistance.* A forger has to have optical contact with a banknote in order to create a fake one with the same serial number. A forger should not be able to create a fake banknote with a new serial number and moreover he should not be able to change the banknote denomination.
- *Privilege separation.* The data stored in the tag should only be alterable given optical contact with banknotes.
- *Fraud detection.* If the data stored by the tag are wrong, then a merchant who has optical access to the banknote should be able to detect the forgery.

In order to illustrate these requirements, Juels and Pappu give two examples of privacy attacks that a banknote protection system should withstand. We give these two examples here because we will show, in Section 4, that their scheme is actually not resistant to these attacks.

EXAMPLE 1 *"Bar X wishes to sell information about its patrons to local Merchant Y. The bar requires patrons to have their drivers' licenses scanned before they are admitted (ostensibly to verify that they are of legal drinking age). At this time, their names, addresses, and dates of birth are recorded. At the same time. Bar X scans the serial numbers of the*

RFID tags of banknotes carried by its patrons, thereby establishing a link between identities and serial numbers. Merchant Y similarly records banknote serial numbers of customers from RFID tags. Bar X sells to Merchant Y the address and birth-date data it has collected over the past few days (over which period of time banknotes are likely not yet to have changed hands). In cases where Bar X and Merchant Y hold common serial numbers, Merchant Y can send mailings directly to customers indeed, even to those customers who merely enter or pass by Merchant Y's shops without buying anything. Merchant Y can even tailor mailings according to the ages of targeted customers. Patrons of Bar X and Merchant Y might be entirely unaware of the information harvesting described in this example."

EXAMPLE 2 *"A private detective wishes to know whether Bob is conducting large-value cash transactions at Carl's store. She surreptitiously intercepts the serial numbers on banknotes withdrawn by Bob and also records the serial numbers of those brought by Carl out of his store. If there is any overlap between sets of numbers, she concludes that Bob has given money to Carl. The private detective might reach the same conclusion if Bob leaves without banknotes that he carried into Carl's store. The private detective might also try to reduce her risk of detection by reading the banknotes of Bob and Carl at separate times, e.g., en route to or from the bank."*

3.3 Description of the method

We explain in this section the operations that should be performed on the banknote. Let $\mathsf{Sign}(k, m)$ be the signature on a message m with a key k and $\mathsf{Enc}(k, m, r)$ the encryption of m under the key k with the random number r. We note $||$ the concatenation of two bit-strings.

Setup. Central bank $\mathcal{B}$ and law enforcement agency $\mathcal{L}$ respectively own a pair of public/private keys $(PK_{\mathcal{B}}, SK_{\mathcal{B}})$ and $(PK_{\mathcal{L}}, SK_{\mathcal{L}})$. $PK_{\mathcal{B}}$ and $PK_{\mathcal{L}}$ are published as well as a collision-resistant hash function h.

Banknote creation. For every banknote i, $\mathcal{B}$ selects (according to its own rules – which can be assumed to be public) a unique serial number S_i and computes its signature $\Sigma_i = \mathsf{Sign}(SK_{\mathcal{B}}, S_i||den_i)$ where den_i is the banknote denomination. $\mathcal{B}$ then computes an access-key D_i such that $D_i = h(\Sigma_i)$[1], prints S_i and Σ_i on the banknote, and computes

$$C_i = \mathsf{Enc}(PK_{\mathcal{L}}, \Sigma_i||S_i, r_i)$$

where r_i is a random number. C_i is written into γ and r_i is written into δ. Note that the access-keys D_i is not stored in the databases of $\mathcal{B}$. In order to keep in mind the values stored on/in the banknote, we give in Tab. 1, established from [8], the content of the optical information as well as those of cells γ and δ.

[1]Juels and Pappu point out that it is important that the hash function be applied on Σ_i rather than on S_i because an attacker who knows a serial number would be able to compute the corresponding access-key without any optical contact with the banknote.

RFID	
Cell γ *universally-readable / keyed-writable*	Cell δ *keyed-readable / keyed-writable*
$C = \mathsf{Enc}(PK_{\mathcal{L}}, \Sigma \| \| S, r)$	r

Optical	
S	$\Sigma = \mathsf{Sign}(SK_{\mathcal{B}}, S \| \| den)$

Table 1. Optical and RFID data

Banknote verification and anonymization. When a merchant $\mathcal{M}$ receives a banknote, he verifies it then re-encrypts it according to the following steps:

1 $\mathcal{M}$ reads the optical data S_i and Σ_i and computes $D_i = h(\Sigma_i)$.

2 $\mathcal{M}$ reads C_i, stored in γ, and keyed-reads r_i which is stored in δ.

3 $\mathcal{M}$ checks that $C_i = \mathsf{Enc}(PK_{\mathcal{L}}, \Sigma_i \| \| S_i, r_i)$.

4 $\mathcal{M}$ chooses randomly r'_i and keyed-writes it into δ.

5 $\mathcal{M}$ computes $C'_i = \mathsf{Enc}(PK_{\mathcal{L}}, \Sigma_i \| \| S_i, r'_i)$ and keyed-writes it into γ.

If one of these steps fails then the merchant should warn the law enforcement agency.

Banknote tracking. Let us consider a target banknote that the law enforcement agency $\mathcal{L}$ wants to check or track. $\mathcal{L}$ is able to easily obtain the cipher C reading the cell γ and then to compute the plaintext $\Sigma \| \| S = \mathsf{Dec}(SK_{\mathcal{L}}, C)$. $\mathcal{L}$ can then check whether or not Σ is a valid signature. If Σ is valid then $\mathcal{L}$ obtains the banknote serial number S.

3.4 Cryptographic algorithms

Encryption and signature schemes can be chosen among the existing secure schemes. However they should bring security without involving high overhead. Juels and Pappu suggest to use an El Gamal-based encryption scheme [5] and the Boneh–Shacham–Lynn signature scheme [3], both using elliptic curves. Let $\mathcal{G}$ denote an elliptic-curve-based group with prime order q and let P be a generator of $\mathcal{G}$. Let $SK_{\mathcal{L}} = x \in_R Z_q$ be the law enforcement agency private key and $PK_{\mathcal{L}} = Y = xP$ the corresponding public key. A message $m \in \{0,1\}^n$ where n is reasonable

sized, is encrypted with the El Gamal scheme under the random number r as follows:

$$\mathsf{Enc}(PK_{\mathcal{L}}, m, r) = (m + rY, rP).$$

Since El Gamal encryption scheme is not secure against adaptive chosen-ciphertext attacks, Juels and Pappu suggest to use the secure integration method due to Fujisaki and Okamoto [6]; the message m is then encrypted as follows:

$$\mathsf{Enc}^*(PK_{\mathcal{L}}, m, r) = (\mathsf{Enc}(PK_{\mathcal{L}}, r, h_1(r||m)), h_2(r) \oplus m)$$

where h_1 and h_2 are two hash functions from $\{0,1\}^*$ to $\{0,1\}^n$. As explained in [8], signature size could be 154 bits. Assuming than a serial number can be encoded over 40 bits, the plaintext $\Sigma||S$ requires 194 bits. Let us consider a 195 bits order elliptic curve group, the size of $\mathsf{Enc}^*(PK_{\mathcal{L}}, \Sigma||S, r)$ will be 585 bits. The total required size will then be 780 bits (585 bits in γ and 195 bits in δ). As pointed out in [8], current RFID tags can provide such resources. For instance the Atmel TK5552 [4] offers a 1056 bits memory (only 992 bits are usable by the user). [11] suggests that only RFID costing about 50 US cents could supply such a capacity but less expensive tags with a few hundreds bits memory could appear in a few years. RFID tags currently costing 5 US cents supply less capacity, usually 64 or 96 bits of user memory [10].

4 Attacks on the banknote protection system

We introduce in this section several attacks that can be performed on the Juels – Pappu banknote protection scheme. While some of these attacks are proper to that scheme (Sections 4.2, 4.3, and 4.7), some other are more general and could be applied to other RFID-based privacy protection schemes (Sections 4.1, 4.4, 4.5, and 4.6).

4.1 Pickpocketing attack

This attack that Juels and Pappu already mentioned is significant enough to be recalled here. It requires an attacker to test a passer-by in order to detect if he carries some banknotes. Even if the attacker is not able to discover neither the serial number nor the denomination, he is able to establish how many banknotes the passer-by is bearing.
The attacker has less information if banknotes of all denominations are tagged than if only the largest ones are tagged. However, tagging banknotes of all denominations may be dangerous with the Juels – Pappu scheme due to the fact that scanning banknotes takes some time. Merchants would not agree to re-encrypt notes of small denominations; privacy could consequently be threatened.

EXAMPLE 3 *Some criminals want to steal some cars in a car park. During daylight hours, they only break into a few cars so as not to attract attention. Their problem is therefore to determine which cars could be the "best" ones, that is the cars that contain currency. Thanks to the banknote protection system, they can radio-scan numerous cars in order to pinpoint their targets.*

These "pickpocketing" attacks show that the attack described in the second example of Juels and Pappu (See page 39) still occurs even using their banknote protection scheme.

4.2 Data recovery attack

The *data recovery* attack consists of two steps: the first one aims at obtaining the access-key D and then the random number r which is stored in the δ-cell; the second step exploits a misuse of the secure integration method of Fujisaki and Okamoto, in order to recover S and Σ. So, the attacker can obtain the serial number of the banknote without optical access to it. Note that even well-behaving merchants are not supposed to obtain this information from the electronic data.

Step 1: One of the goals of the scheme is to avoid γ-write-access without optical reading of the banknote. This implies that an attacker must have physically access to the banknote to modify the γ-cell. However a merchant who is willing to re-encrypt the banknote sends the access-key $D = h(\Sigma)$ (obtained by optical reading) to the tag in order to receive the value stored in the δ-cell, i.e. the random number r. The attacker can just eavesdrop the communication in order to steal D and then he is able to communicate with the tag and finally obtain the δ-cell value r. To buttress our argumentation, remind that it is usually easier to eavesdrop the forward channel, that is from the reader to the tag, than the backward channel. Note also that the communication range should not be too short since one of the goals of the Juels – Pappu scheme is to enforce banknotes tracking be the law enforcement agency, even in areas of dense traffic, such as airports.

Step 2: The attacker first obtains the value stored in the γ-cell (universally readable). γ-cell contains:

$$\begin{aligned} \mathsf{Enc}^*(PK_{\mathcal{L}}, m, r) &= (\mathsf{Enc}(PK_{\mathcal{L}}, r, h_1(r||m)), h_2(r) \oplus m) \\ &= (r + h_1(r||m)PK_{\mathcal{L}},\ h_1(r||m)P,\ h_2(r) \oplus m) \end{aligned}$$

Notation is defined in Section 3.4. Let us consider $(\epsilon_1, \epsilon_2, \epsilon_3)$ such that

$$(\epsilon_1, \epsilon_2, \epsilon_3) = \mathsf{Enc}^*(PK_{\mathcal{L}}, m, r).$$

So:

$$\epsilon_1 = r + h_1(r||m)PK_{\mathcal{L}},\ \epsilon_2 = h_1(r||m)P, \text{ and } \epsilon_3 = h_2(r) \oplus m.$$

She obtains therefore

$$m = \epsilon_3 \oplus h_2(r) \text{ where } \epsilon_3, r, \text{ and } h_2 \text{ are known.}$$

Since $m := \Sigma||S$, this proves that an attacker can discover the serial number and the signature of a banknote without having optical access to it, contrary to what Juels and Pappu claim.
The problem arises from the fact that the integration method of Fujisaki and Okamoto is not secure anymore when the random value r is revealed. Indeed, the purpose of the asymmetric encryption $\mathsf{Enc}(PK_{\mathcal{L}}, r, h_1(r||m))$ is to "hide" the random value that is used to generate the key of the symmetric encryption. If this random value is public or can be determine easily by an attacker, the integration method becomes null and void.

4.3 Ciphertext tracking

The protection method that we are discussing in this paper uses re-encryptions to prevent tracking attacks. However, re-encryptions can only be performed in practice by merchants or retail banks[2]. Therefore the time period between two re-encryptions could last long enough to track banknotes.

EXAMPLE 4 *Many supermarkets use massive computing power to analyze the buying patterns of their clients. Identifying these patterns enables merchants to reorganize their store layouts to increase their sales. Data mining consists of using computer-based search techniques to sort through the mounds of transaction data captured through goods bar-coding. The frequently cited example is the "beer and diapers" example: a large discount chain discovered by data mining its sales data that there was a correlation between beer and diaper purchases during the evening hours. The discount chain therefore moved the beer next to the diapers and increased sales. Let us now consider a merchant who installs RFID readers in his store departments: now he is able to analyze precisely his client's path and thereby to reorganize his store layout. Since some existing payment systems contain names and addresses, a client who stays during a long time in the bicycle department without buying anything will receive directly advertising literature to his door.*

[2] We could imagine a scenario where citizens are able to re-encrypt their own banknotes, but it is an unrealistic assumption.

Ciphertext tracking attacks show that the threat described in the first example of Juels and Pappu (See page 38) still occurs within their banknote protection scheme. Let us first consider a milder version of the attack: bar X cannot read the optical data on the banknotes of his customers (We consider that a *customer* is a person who comes in the shop; he does not necessarily need to buy anything). So, he stores in a database all the γ-values that he is able to collect matched with the name and address of their handlers. Merchant Y also reads the γ-values of his clients and stores them. Bar X and merchant Y can combine their databases: if a γ-value appears in both databases, they are almost sure that it is the same client. Let us now consider a stronger attack: when bar X returns change to a client, he re-encrypts banknotes with a fixed number, denoted r_0 also known by merchant Y. When a customer arrives in Merchant Y's store, the merchant reads the γ-value of the customer's banknotes (universally readable) and computes Σ_0 using r_0 (applying the method described in Section 4.2). He then computes $D_0 = h(\Sigma_0)$ and tries to read δ with D_0; if the tag agrees this means that r_0 was the appropriate random number and that merchant Y can be almost sure that this client comes from Bar X. Note that Merchant does not "touch" the banknote here: he has just to scan the people when they pass through the store door for instance.

This issue is inherent in re-encryption-based privacy protection schemes: since re-encryptions cannot be performed very frequently, it is possible to track tags with their universally readable values (even if these values seem to be some garbage for a person who is not authorized to decrypt them). Note that even with a higher re-encryption frequency, the attack still works if the re-encryptions are performed by the merchants, and not by the users themselves.

4.4 Access-key tracking

The goal of the re-encryptions is to prevent banknotes tracking, as we mentionned. If an attacker does not have optical contact with a given banknote, then he should not be able to track it in the long-term. Unfortunately, we demonstrate here that a side channel can be used to track the banknotes. Indeed, if the attacker can see the banknote once (or even, more simply, if he effects the first step of the attack described in Section 4.2) then thanks to the static access-key D, he will be able to track the banknote by just trying to read the δ-cell: the tag responds if and only if the key D is the good one;

This attack is particularly devastating because it dashes the purpose of the scheme. Actually, when a tag owns a unique access-key and responds

if and only if the key sent by the reader is the valid one, this key can be used to track the tag. On may think that the tag could thwart such an attack by replying with some garbage when the access-key is wrong, instead of remaining silent. Unfortunately, sending *static* garbage opens a new way to perform tracking attacks, and requiring the tag to be able to generate *random* garbage is not yet realistic due to the low capability of such devices.

EXAMPLE 5 *Mrs Johnson suspects that her husband is having an affair with his secretary. It seems that he has been giving her money. Mrs Johnson decides to read the optical data on her husband's banknotes - in order to generate the access-key - and to surreptitiously follow his secretary after work. She will soon know whether her suspicions are true or not.*

4.5 Cookies threat

According to [8], the sizes of the δ-cell and γ-cell are 195 bits and 585 bits respectively. Since these values can be modified for everyone having access to the banknote (or using the attack described in Section 4.2), the δ-cell and the γ-cell can be used to hide a certain amount of information. This hidden information channel looks like an HTTP cookie. This cookie will however be detected during the next re-encryption of the tag data (since merchants have to check the current value before performing the re-encryption) because δ and γ are not consistent anymore.
A clever way to abuse the tag is to put the cookie only in the δ-cell: since the value r stored in this cell is a random number, it can be used to store some information. Obviously, the γ-cell value will have to be re-encrypted with the new random number. This kind of cookie will be untraceable and will stay available until the next re-encryption.

4.6 Denial of service attack

We saw that when a merchant finds a discrepancy on a banknote, he cannot accept the payment and should warn the law enforcement agency. This could however be used to harm banknote bearers: all that is required is to input incorrect data into either δ or γ. This could be done not only by a merchant who has access to the optical data but also anyone who is able to perform the first step of the attack described in Section 4.2. Due to its simplicity, this malicious attack may bring about many problems as the law enforcement agency as well as the Central Bank – that has to restore the banknotes – would be flooded.

EXAMPLE 6 *In a store, some hackers are waiting in line for the cash register. The customer in front of them pays for his purchases. The hackers eavesdrop the communication between the reader and the tag, thus obtaining the access-key D; they then replace the data stored in the cell γ with a false value, just for fun. The banknote becomes out of service until it is restored by the Central Bank. They can block all cashiers this way and take advantage of panic scenes between cashiers and complaining customers in order to steal goods.*

4.7 Sleeping and dead banknotes

We present here two attacks that are possible using the native commands of the RFIDs. The first one exploits the `sleep` function of the device, and the second uses the `kill` function.

Juels and Pappu point out that banknotes issued from dirty money could pass, for instance, airport checking, by replacing Σ and S by values issued from clean money. Another solution would be to put banknotes into the sleep mode with the `sleep` function. After having passed through bank policy checking, money launderers are able to "wake up" the banknotes. It is therefore important that this function is not universally available. However, if forgers create fake banknotes (by cloning) they will be able to embed a `sleep` function in their tags: law enforcement agents consequently cannot detect the counterfeit banknotes during checking.

We propose now a stronger denial of service attack than those proposed in Section 4.6, involving the `kill` function of the tags. Obviously, this function is a keyed command but the key may be too short to ensure real security. According to the Auto-ID center's standards, the kill-key should be 24 bits [2] or even 8 bits [1]! This means that it would be so simple to perform an exhaustive search to destroy tags. Tag makers should therefore embed longer kill-keys, but the longer the key, the more expensive the tag.

5 Conclusion

We have outlined in this paper the main aspects of banknote protection and described the Juels - Pappu scheme, which is based on both Optical and Radio Frequency Identification systems. We show that two parties can benefit directly from the use of tags in the banknotes: the central bank and the law enforcement agency, both profiting from this system by enforcing banknote tracking and anti-counterfeiting. What about the other interested parties such as merchants and citizens? The role of merchants here is crucial since privacy relies only on their collaboration. Even if most of the merchants are compliant, one can notice

that re-encrypting banknotes implies a loss of time for merchants. Another issue is the attitude of a merchant when faced with a problematic banknote; according to [8], he should warn the law enforcement agency. However he is able to repair the problematic data as he has optical access to the banknote. Will he risk losing a customer by warning the law enforcement agency? From the citizens point of view, it would be difficult to tolerate such a system for three reasons. The first one is that citizens have to travel to the central bank (or perhaps to a retail bank) every time they have a faulty banknote. The second reason is that they will lose confidence in their banknotes: they can no longer be sure that they will be able to use their currency at the cash register! Last but not least, they will be suspicious about the fact that their privacy and their anonymity remain intact.

Beyond the sociological issues brought by this scheme, we proved that, despite what the authors claimed, the proposed banknote protection scheme suffers from some privacy issues and thus compromises the privacy of the banknotes' bearers. We have described many attacks that can be performed on the scheme and so, proved that the only RFID banknote protection scheme published until now is null and void and should not be used in practice. Even if this solution could be partially fixed, some attacks are inherent in re-encryption-based privacy protection schemes, as explained in Section 4.3, what strengthens our feeling in the fact that such an approach is not suitable to privacy protection schemes. Furthermore, some described attacks are beyond the scope of the banknote protection, as the access-key tracking attack, and we think that our contribution should be taken into account in future designs of RFID privacy protection schemes.

Acknowledgments

The work presented in this paper was supported (in part) by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center supported by the Swiss National Science Foundation under grant number 5005-67322. I would like to thank Serge Vaudenay and Lu Yi for their helpful comments on this work.

References

[1] Auto-ID Center. 860MHz-960MHz class I radio frequency identification tag radio frequency & logical communication interface specification: Recommended standard, version 1.0.0. Technical report `http://www.autoidcenter.org`, Massachusetts Institute of Technology, MA, USA, November 2002.

[2] Auto-ID Center. 13.56MHz ISM band class 1 radio frequency identification tag interface specification: Recommended standard, version 1.0.0. Technical report `http://www.autoidcenter.org`, Massachusetts Institute of Technology, MA, USA, February 2003.

[3] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In Colin Boyd, editor, *Advances in Cryptology – ASIACRYPT'01,* volume 2248 of *Lecture Notes in Computer Science,* pages 514–532, Gold Coast, Australia, December 2001. IACR, Springer-Verlag.

[4] Atmel Corporation. `http://www.atmel.com`.

[5] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory,* 31(4):469–472, July 1985.

[6] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Michael Wiener, editor, *Advances in Cryptology – CRYPTO'99,* volume 1666 of *Lecture Notes in Computer Science,* pages 537–554, Santa Barbara, California, USA, August 1999. IACR, Springer-Verlag.

[7] RFID Journal. Michelin embeds RFID tags in tires. `http://www.rfidjournal.com/article/view/269`, January 2003.

[8] Ari Juels and Ravikanth Pappu. Squealing euros: Privacy protection in RFID-enabled banknotes. In Rebecca N. Wright, editor, *Financial Cryptography – FC'03,* volume 2742 of *Lecture Notes in Computer Science,* pages 103–121, Le Gosier, Guadeloupe, French West Indies, January 2003. IFCA, Springer-Verlag.

[9] Mark Roberti. The money trail – RFID journal. `http://www.rfidjournal.com`, August 2003.

[10] Sanjay Sarma. Towards the five-cent tag. Technical Report MIT-AUTOID-WD-006, MIT auto ID center, Cambridge, MA, USA, November 2001.

[11] Sanjay Sarma, Stephen Weis, and Daniel Engels. Radio-frequency identification: security risks and challenges. *Cryptobytes, RSA Laboratories,* 6(1):2–9, spring 2003.

[12] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels. Security and privacy aspects of low-cost radio frequency identification systems. In Dieter Hutter, Günter Müller, Werner Stephan, and Markus Ullmann, editors, *First International Conference on Security in Pervasive Computing – SPC 2003,* volume 2802 of *Lecture Notes in Computer Science,* pages 454–469, Boppard, Germany, March 2003. Springer-Verlag.

[13] Junko Yoshida. Euro bank notes to embed RFID chips by 2005. `http://www.eetimes.com/story/OEG20011219S0016`, December 2001.