

# Lighten Encryption Schemes for Secure and Private RFID Systems<sup>\*</sup>

Sébastien Canard<sup>1</sup>, Iwen Coisel<sup>2</sup>, and Jonathan Etrog<sup>3</sup>

<sup>1</sup> Orange Labs, 42 rue des Coutures, BP6234, F-14066 Caen Cedex, France

<sup>2</sup> UCL, Place du Levant, 3, B-1348 Louvain-la-Neuve, Belgium

<sup>3</sup> Orange Labs, 38-40 rue du Général Leclerc, F-92794 Issy les Moulineaux, France

**Abstract.** We provide several concrete implementations of a generic method given by Vaudenay to construct secure privacy-preserving RFID authentication and identification systems. More precisely, we give the first instantiation of the Vaudenay's result by using the IND-CCA secure DHAES cryptosystem. Next we argue that weaker cryptosystems can also be used by recalling the WIPR RFID system and giving a new protocol based on the El Gamal encryption scheme. After that, we introduce a new generic construction based on the use of any IND-CPA secure public key cryptosystem together with a MAC scheme and describe a possibility using the Hash El Gamal cryptosystem. We finally compare all these schemes, both in terms of implementation and security, proving that, nowadays the DHAES and our Hash El Gamal based solutions appear as the most promising schemes.

## 1 Introduction

RFID (Radio-Frequency Identification) technology appeared a while ago but it only spread into a very large number of applications recently, because of both technical improvements and dramatic cost decrease. RFID tags usually broadcast a unique identifier over the air whenever they are powered on, as for Electronic Product Code (EPC) tags with long range used in supply chains, but also for most short range (ISO 14443/15693) tags regardless of theoretically broader abilities. This behavior raises many concerns on privacy and active research has recently been done on this subject.

Many use cases for tags thus require authentication, identification and privacy. For instance, if the tag is embedded into a passport, it is desirable that the latter be authenticated and identified by immigration officials while counterfeited passports should be detected. Moreover, other entities should not be able to trace all RFID tag's movements.

---

<sup>\*</sup> This work has been financially supported by the French Agence Nationale de la Recherche under the RFID-AP project while 2nd author was working at Orange Labs.

## 1.1 Related Work

Many privacy-friendly RFID authentication constructions already exist in the literature. Some of them are symmetric-based constructions [19,17,10] and some others [24,20,15,18,4] are designed using asymmetric cryptography, on which we will focus in this paper.

As an example, Batina *et al.* [4] prove that it is possible to embed elliptic curve cryptography, but their scheme does not include the privacy properties. The GPS authentication family, based on the initial work of Girault and Poupard-Stern, also fits the RFID setting, as stated by Girault and Lefranc [15]. A practical implementation is moreover given in [18]. But, again, the proposed scheme does not provide the privacy properties we need. An attempt has been made in [9]. However the efficiency of this scheme is bad as the reader has to perform an exhaustive search in the database and computes lots of modular exponentiations in order to identify a tag.

Recently, Vaudenay proposes in [24] a generic privacy-preserving authentication and identification scheme based on any encryption scheme with undistinguishability property against adaptive chosen-cipher attack (IND-CCA). He proves that if the cryptosystem is IND-CCA, the scheme is secure and private. However, no practical instantiation is given by Vaudenay and thus, it only remains a theoretical scheme.

One such concrete instantiation, named WIPR, has afterward been proposed in [20] using the Rabin encryption scheme. Oren and Feldhofer consequently provide a concrete hardware implementation of the Vaudenay’s proposal. However, as the Rabin cryptosystem is only IND-CPA and since there is no security proof in [20], it remains some work to do on privacy-preserving RFID identification schemes based on public key cryptosystems.

## 1.2 Our Contributions

In this paper, we focus on the generic construction from Vaudenay [24] based on the use of a public key cryptosystem and we go further by making the following contributions.

1. We give in Section 2 the first concrete instantiation of the Vaudenay’s result by using the IND-CCA secure cryptosystem DHAES.
2. We next notice in Section 3 that the IND-CCA property is only reached by a few public key cryptosystems that can be embedded into an RFID tag and consequently, we argue that a weaker cryptosystem can also be used. More precisely, we introduce the “constant fixed non malleability”.
3. Next, in Section 5, we give a new generic construction based on the use of an IND-CPA secure public key cryptosystem (undistinguishability against chosen plaintext attack) together with a MAC scheme. We next give an example of a concrete implementation of this construction.
4. Finally, we make an implementation comparison between all the above instantiations in Section 6.

## 2 RFID Systems

In the following, we study protocols where the reader interacts with a tag in order to authenticate and identify it by retrieving the corresponding identifier  $ID$ , while protecting the privacy of the tag owner against all other readers.

An RFID authentication scheme, denoted  $\mathcal{S}$  is composed of the following procedures, where  $\lambda$  is a security parameter.

- $\text{SETUP}(1^\lambda)$  is a probabilistic algorithm which outputs the parameters  $\text{param}$  of the system, generates a private/public key pair  $(\text{rsk}, \text{rpk})$  for the reader and initialized the database  $\text{DB}_{\mathcal{R}}$  to the empty set.
- $\text{TKEYGEN}(1^\lambda, \text{param}, ID, \text{rpk})$  is a probabilistic algorithm which returns a tag-dependent key set  $\text{tk}[ID]$ .  $(ID, \text{tk}[ID])$  is added in  $\text{DB}_{\mathcal{R}}$  containing the whole set of legitimate tags.
- $\text{IDENT}$  is an interactive protocol between the reader  $\mathcal{R}$  taking as inputs  $1^\lambda$ ,  $\text{param}$ ,  $\text{rsk}$ ,  $\text{rpk}$  and  $\text{DB}_{\mathcal{R}}$ , and a tag  $\mathcal{T}$  with identifier  $ID$  taking as inputs  $1^\lambda$ ,  $\text{param}$ ,  $\text{tk}[ID]$ ,  $\text{rpk}$  and eventually  $ID$ . At the end of the protocol, the reader either accepts the tag and outputs its identifier  $ID$  or rejects it and outputs  $\perp$ .

### 2.1 Usual Security Properties

Before introducing the security properties required for an RFID identification system, it is necessary to first define the adversary by giving him access to some oracles. Next, we will show that an RFID identification system should provide two main security properties.

**Oracles.** We consider that there is only one valid reader  $\mathcal{R}$  in the system. However, as we will see below, the adversary will play the role of dishonest readers to interact with a tag and we assume that the tag does not know *a priori* if it is interacting with  $\mathcal{R}$  or the adversary  $\mathcal{A}$ . We assume that  $\mathcal{A}$  is always given  $1^\lambda$ ,  $\text{param}$  and  $\text{rpk}$  that are initially generated.

- We first assume that there are no tag at the beginning of one experiment and we give to  $\mathcal{A}$  an oracle to introduce new tags.
- Vaudenay has been the first to introduce the concept of “future correlations”, that is the possibility for an adversary against privacy to recognize a tag she has previously corrupted. For this purpose, he introduces the concept of free and drawn tags. More precisely, the adversary can only interact with tags that are sufficiently close to her without having access to other existing ones. Thus, drawn tags are the ones within “visual contact” to the adversary so that she can communicate with them using a temporary pseudonym while free tags are all the other tags. At the creation of a new tag, this tag has the status free and, at any time, the adversary is able to draw some tags or to free specific tags.

- As a consequence, the adversary is only able to interact with tags by using the pseudonyms. To simplify notation, we denote by  $\text{tk}[t]$  the secret key of the tag with pseudonym  $t$ , which is equal to the secret key  $\text{tk}[ID]$  of the underlying identifier  $ID$  of this tag. At the creation of a new tag, this tag has the status *legitimate*. Next,  $\mathcal{A}$  is able to corrupt tags by using a specific oracle.
- Finally, the adversary can be *passive* by running the whole protocol IDENT between a valid tag and the valid reader, or *active* by participating in an IDENT protocol, stopping at any step the identification protocol, deleting or modifying some requests or responses.

Finally, Vaudenay gives the following classification for an adversary which is said *weak* if she has no access to the corruption oracle; *forward* if, after a corruption query, she can next only make corruption queries; *destructive* if she cannot use anymore a corrupted pseudonym  $t$ ; *strong* if she has no limit on the oracles. An adversary is moreover said *narrow* if she is not able to obtain the result of an identification.

**Correctness.** The first security property, the correctness (also known as the completeness property) says that a legitimate tag is always accepted in the IDENT protocol. A formal definition can be found in [12]. Note that in some cases, it is necessary to define a strong correctness, where the aim of the active adversary is to make rejected a legitimate tag [10], but this is not our case in this paper.

**Soundness.** The second property is the soundness one. It states that a fake tag cannot be accepted by the system. One formal definition, called the strong soundness, is described in [12] where the adversary can corrupt tags.

**Privacy.** The scheme has to preserve the privacy of a tag in its previous authentications, even if an adversary compromises it and outputs its internal data: this is what is called forward-privacy.

In fact, several attempts have been done concerning the design of a privacy model for RFID systems. Le *et al.* adopt in [17] a specific approach to the formalization of protocol security based on the Universal Composability (UC) framework. Some other proposals are based on a different concept, introduced by Avoine [2] in the RFID setting, where privacy is formalized by the ability for the adversary to distinguish two known tags. This model was refined by Juels and Weis [16]. However, none of these models permit the adversary against privacy to make future correlations (that is the target tags cannot have been corrupted by the adversary). This case is taken into account in Vaudenay’s model [24], which is very elegant and complete. However, this model is very hard to handle and only few papers have used it so far.

Our aim in this paper is not to give a new privacy model for RFID systems but, in the following, we only give some arguments on what is behind the “privacy property” according to Vaudenay’s model. In a nutshell, the goal is to prove that for a given experiment, the success probability of an adversary, which interacts

with the system through oracles, is undistinguishable of a “blinded” adversary, which interacts with a simulated system controlled by a simulator, which does not know anything about secret values. If those success probabilities are undistinguishable, it means that there are no privacy loss through the communication channel. In other words, the adversary make no effective use of the messages as their simulation (without using the secret values) leads to the same probability of success.

Contrary to previous models, as for example the Juels-Weis model, this model is more complete as the success of the adversary is not limited to linking two conversations of a same tag. However, a too much powerful adversary will be able to win against every scheme. Consequently, it is not possible to prove the strong privacy property (for a non-narrow adversary) for any scheme, as it has been proven by Vaudenay in his article [24].

### 3 Privacy of RFID Systems and IND-CCA Cryptosystems

In this section, we recall the result of Vaudenay which says that the narrow-strong (which corresponds to the strong privacy for a narrow adversary) and the forward privacy can be obtained using any public key cryptosystem<sup>1</sup>.

#### 3.1 The Generic Construction from Vaudenay

We first recall the notion of public key cryptosystems and what does IND-CCA and IND-CPA say. We next give the generic construction of [24].

**Public Key Cryptosystem.** Let a public-key encryption scheme  $\mathcal{E} = (\text{KEYGEN}, \text{ENC}, \text{DEC})$  such that:

- KEYGEN is a probabilistic key generation algorithm which on input the security parameter  $1^\lambda$  outputs the encryption public key  $\text{epk}$  and the corresponding decryption secret key  $\text{esk}$ ,
- ENC is a probabilistic encryption algorithm which on input a message  $m$  and the public key  $\text{epk}$  outputs the corresponding ciphertext  $c$ ,
- DEC is a deterministic decryption algorithm which on input a ciphertext  $c$  and the decryption secret key  $\text{esk}$  outputs a plaintext  $m$ .

The correctness of the scheme is defined as  $\text{DEC}(\text{ENC}(m, \text{epk}), \text{esk}) = m$ . Moreover, an encryption scheme should also be secure in the sense that it should not be possible for an adversary to learn any information about the plaintext  $m$  underlying a challenge ciphertext  $c$ . Such scheme is said to have the indistinguishability (IND) property.

---

<sup>1</sup> Note that Vaudenay has proved in [24] that, in the model he has defined, the strong privacy cannot be reached by an RFID identification system, and thus do not consider that case.

We then consider three different attacks for the adversary.

- Under *chosen-plaintext attack* (CPA), the adversary can obtain ciphertexts of plaintexts of her choice, using the public key.
- Under *non-adaptive chosen-cipher attack* (CCA1), the adversary gets, in addition to the public key, access to an oracle for the decryption function. The adversary may use this decryption function only for a period of time before receiving the challenge ciphertext  $c$ .
- Under *adaptive chosen-cipher attack* (CCA2) the adversary again gets, in addition to the public key, access to an oracle for the decryption function, but this time she may use this decryption function even on ciphertexts chosen after obtaining the challenge ciphertext  $c$ , the only restriction being that the adversary may not ask for the decryption of  $c$  itself.

Note that the notion of IND-CCA usually refers to the IND-CCA2 property while the IND-CCA1 is rarely used in practice. We utilize this notation in the following.

**Proposed Construction.** Using a public key cryptosystem  $\mathcal{E}$  such as defined above, Vaudenay introduces the following RFID identification scheme, also depicted in Figure 1. In this scheme and in all the following ones in this paper, the reader key pair  $(rsk, rpk)$  corresponds to the public key cryptosystem key pair  $(esk, epk)$ . Moreover, let  $tk$  be the  $\lambda$ -bit key of a tag, which is known by both the tag and the reader. In [24], Vaudenay proves that if the cryptosystem is IND-CPA, then the identification scheme is narrow-strong private and if the cryptosystem is IND-CCA2, the scheme is further secure and forward private. We do not recall the security proof in this paper.

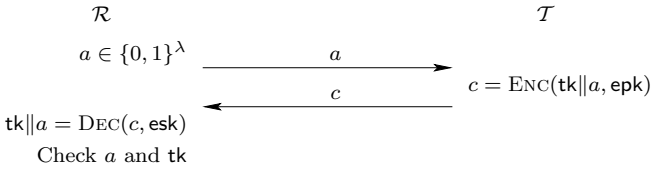


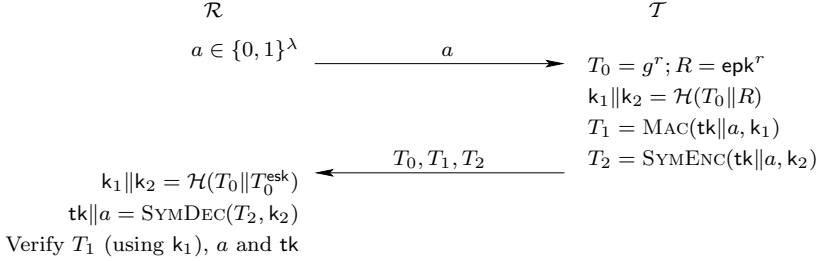
Fig. 1. Vaudenay’s protocol

### 3.2 A Very Practical Instantiation: The DHAES Case

The DHAES has been introduced in [1] by Abdalla, Bellare and Rogaway and has been submitted to the IEEE P1363a standard. Its aim is to propose a method to encrypt strings using the Diffie-Hellman assumption, since the standard El Gamal encryption scheme has some flaws when regarding the message as a string. It is as efficient as the standard El Gamal encryption but has more and better security properties since it has been proved to have the indistinguishability property against adaptive chosen ciphertext attacks with unlimited access to the decryption oracle (IND-CCA2). It is thus possible to directly use it in the above

generic construction to obtain the security of the underlying privacy-preserving RFID identification scheme (see 3.1 and [24]).

Let  $G$  be a cyclic group of prime order  $q$ . The private key to decrypt a message is  $\text{esk} \in \mathbb{Z}_q$  and the corresponding public key is  $\text{epk} = g^{\text{esk}}$ . The DHAES encryption scheme can be used to obtain and RFID identification scheme as described in Figure 2, where  $\mathcal{H}$  is a cryptographically secure hash function.



**Fig. 2.** DHAES based protocol

### 3.3 The “Constant Fixed Non Malleability” Property

In [5], Bellare *et al.* have shown that the IND-CCA property is equivalent to the NM-CCA one. The Non-Malleability (NM) property formalizes an adversary’s inability, given a challenge ciphertext  $y$ , to output a different ciphertext  $y'$  such that the plaintexts  $x, x'$  underlying these two ciphertexts are “meaningfully related” (for example,  $x' = x + 1$ ).

Intuitively, the soundness property of the Vaudenay’s generic scheme comes from the non-malleability of the public key cryptosystem while the privacy property comes from the indistinguishability property. But the non-malleability property may be too strong for our purpose and, as we need lightweight computation, this may be not a good choice. In fact, most of existing IND-CCA secure cryptosystems are not relevant in the RFID setting and thus, cannot be used in practice.

However, we can notice that in the Vaudenay’s generic construction, the RFID tag does not simply encrypt a message but the concatenation of some secret values  $\text{tk}$  that are always the same for a particular tag together with some randomness  $a$  that are “publicly” known, since they are sent in clear by the reader. We thus introduce the following security definition for encryption schemes.

**Definition 1 (Constant Fixed Non Malleability).** *A public key encryption scheme verifies the constant fixed non malleability if given the encryption public key and having access to an oracle which on input a value  $a$ , outputs the encryption of  $\text{tk} \| a$ , where  $\text{tk}$  is secret, an adversary is unable to output the encryption of  $\text{tk} \| \tilde{a}$  on input  $\tilde{a}$  with non-negligible probability.*

As a conclusion, if we are able to find a public key cryptosystem not necessarily IND-CCA but having the constant fixed non malleability property, then we have the following result on privacy-preserving RFID systems.

**Theorem 1.** *The Vaudenay’s generic construction given in Figure 1 using a constant fixed non malleable encryption scheme is secure and forward private.*

The following sections discuss about the potential existence of a secure and private scheme based on the constant fixed non-malleability of the used public-key cryptosystem.

## 4 Privacy of RFID Systems and IND-CPA Cryptosystems

The scheme presented in Figure 1 can be instantiated with a public-key cryptosystems which is only IND-CPA. In Vaudenay’s article [24], the author claims that such a scheme is narrow-strong private but not necessarily sound (see section 2.1). In this section, we study the case of several existing IND-CPA public-key cryptosystems.

We first show that a construction based on the Hash El Gamal is insecure. We next recall the WIPR construction which is due to Oren and Feldhofer [20] and which falls in the above case. Finally, we introduce our new construction based on the El Gamal encryption scheme.

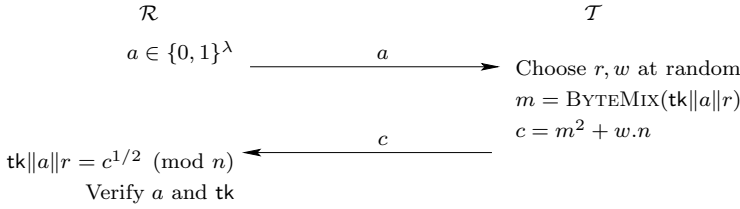
### 4.1 The Hash El Gamal Case

The Hash El Gamal encryption scheme [11] consists in computing  $T_0 = m \oplus \mathcal{H}(\text{epk}^r)$  and  $T_1 = g^r$  for the encryption of the message  $m$ .

Using the hash El Gamal encryption scheme in the Vaudenay’s construction, it is trivially possible to break the soundness of the resulting scheme. Concretely, from one successful authentication  $T_0 = (\text{tk}||a) \oplus \mathcal{H}(\text{epk}^r)$  and  $T_1 = g^r$ , one can fake the valid tag by simply computing, on reception of the new random  $\tilde{a}$ ,  $\tilde{T}_0 = T_0 \oplus (0 \cdots 0 || (a \oplus \tilde{a}))$  which is obviously equal to  $(\text{tk}||\tilde{a}) \oplus \mathcal{H}(\text{epk}^r)$ . Thus,  $(\tilde{T}_0, T_1)$  is a valid authentication of  $ID$  under the request  $\tilde{a}$ . One possibility to avoid this attack is to keep all received successful authentications and checks that the received  $T_1$  has not previously been used. But we do not want the reader to perform so many comparisons and store so much data in its database.

### 4.2 The Rabin Case

The Rabin cryptosystem [21] is a public key cryptosystem introduced by Rabin whose security is related to the factorization problem. In the RFID setting, this cryptosystem has been used by Shamir to describe a MAC scheme [22]. In [20], Oren and Feldhofer also use this cryptosystem in the design of their privacy-preserving RFID identification scheme named WIPR. Let  $p$  and  $q$  be two large prime numbers and let  $n = pq$ . The private key  $\text{esk}$  is the factorization  $(p, q)$  of  $n$  and the corresponding public key  $\text{epk}$  is  $n$ . The scheme is described in Figure 3, where BYTEMIX is a publicly known byte-interleaving operation used to ensure that neither the tag nor the reader fully dominates a large element of the plaintext. Moreover, reduction modulo  $n$  is replaced by an addition of a multiple of the divisor  $n$ .



**Fig. 3.** The WIPR protocol

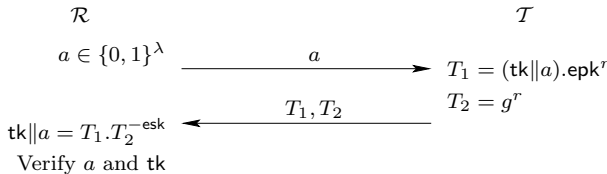
**Security Considerations.** As said above, it is well-known that the Rabin cryptosystem is not IND-CCA. The preprocessing step which consists in adding some redundancy permits to overcome some known chosen ciphertext attacks but no security proof can be done. However, it is not possible to prove that the resulting encryption scheme is IND-CCA secure.

Nevertheless, we only need that the scheme verifies the *constant fixed non malleability* property. In [25], the authors show that without a good preprocessing step (e.g. a weak BYTEMIX), the scheme is unsecure. They use the preprocessing step SAEP (Simple OAEP) so as to prove the security in a simple model where, unfortunately, strong privacy is not taken into account.

### 4.3 The El Gamal Case

The El Gamal encryption scheme has been introduced in [14] and is now largely used in many cryptographic papers. The El Gamal encryption scheme can be used either in groups of prime order or in groups of unknown order. In the following, we use a group of prime order.

**Description of the System.** Let  $G$  be a cyclic group of prime order  $q$ . The private key to decrypt a message is  $\text{esk} \in \mathbb{Z}_q$  and the corresponding public key is  $\text{epk} = g^{\text{esk}}$ . We next obtain the RFID identification scheme described in Figure 4.



**Fig. 4.** El Gamal based protocol

**Security Considerations.** As for the Rabin case, we are unable to provide a proof that the construction based on El Gamal is secure but again, it would seem that this is the case.

In addition to what has been said for the Rabin case, the El Gamal opens a new problem. In fact, we should be careful here that the message  $tk||a$  truly belongs to the right working group. This should be done by using a good preprocessing step. Note however that this may imply some additional computations for the RFID tag. This is for example the case if the implementation is done using elliptic curves [8].

## 5 Privacy and IND-CPA Cryptosystems + MAC

In this section, we first provide a generic construction of a privacy-preserving RFID identification system which make use of any IND-CPA public key cryptosystem and a MAC function. Next, we provide a practical implementation using the Hash El Gamal encryption scheme.

### 5.1 Our New Generic Construction

Our generic construction needs a public key cryptosystem and a MAC scheme as defined below.

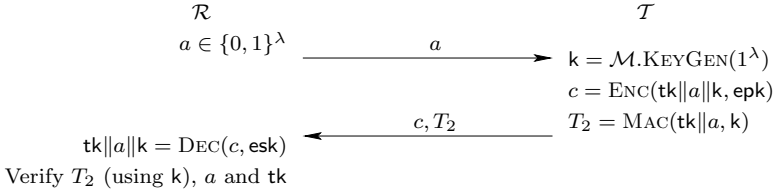
**MAC Function.** A cryptographic message authentication code (MAC) is a cryptographic tool used to authenticate a message and belongs to the family of symmetric cryptography. A *MAC scheme* denoted  $\mathcal{M}$  is composed of the following procedures: **KEYGEN** is the key generation algorithm which permits to generate the MAC key denoted  $k$ ; **MAC** is the code generation algorithm which accepts as input an arbitrary-length message  $m$  and the secret key  $k$  and outputs the MAC  $\sigma$  for message  $m$ , under the secret key  $k$ ; **VERMAC** is the code verification algorithm which takes as input a message  $m$ , the secret key  $k$  and a message authentication code  $\sigma$  and outputs 1 if  $\sigma = \text{MAC}(m, k)$  and 0 otherwise.

To be considered as secure, a MAC scheme should resist to existential forgery under chosen-plaintext attacks (EF-CPA). This means that even if an adversary  $\mathcal{A}$  has access to an oracle which possesses the secret key and generates MACs for messages chosen by the adversary,  $\mathcal{A}$  is unable to guess the MAC for a message it did not query to the oracle.

**Proposed Construction.** Let  $\mathcal{E}$  be a public-key encryption scheme with the IND-CPA property and a MAC scheme  $\mathcal{M}$  such as defined above, we next introduce our new RFID identification scheme in Figure 5, where each tag shares with the reader a unique key denoted  $tk$ .

**Security Considerations.** Assume an adversary able to impersonate an uncorrupted tag. As she has no control over the nonce  $a$  chosen by the reader, the returned values will correspond, with a significant probability, to a new message  $tk||a$ , which contradict the EF-CPA property of the MAC. Consequently, under the EF-CPA property, our new generic construction is sound.

Regarding the untraceability property, we have to prove that for every adversary  $\mathcal{A}$  of this protocol, there exists a blinded adversary  $\mathcal{A}^B$  such that whatever



**Fig. 5.** Our generic protocol

$\mathcal{A}$  do,  $\mathcal{A}^{\mathcal{B}}$  can obtain the same result by interacting with the simulator. The game technique, presented by Shoup is perfectly adapted to obtain this result. The purpose is to replace every interactions with oracles of  $\mathcal{A}$  by an answer of the simulator. The success of each game is the experiment that perform the adversary, for example : find a non-trivial link between two pseudonyms. If the difference between the success probabilities of two successive games is negligible, then it follows that the difference between the success probability of the adversary and the one of the blinded adversary is negligible.

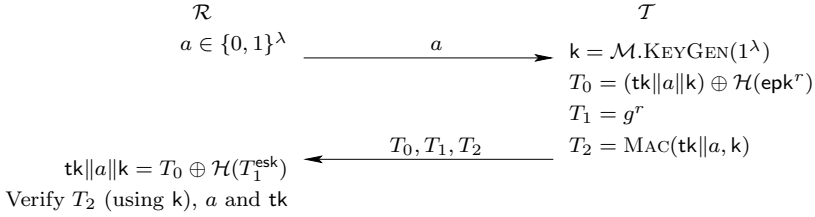
We give here some details about this proof. It is possible to replace one by one every plaintexts of the public key cryptography by random messages. As detailed in [23], these operations cannot influenced the success probability of the adversary, otherwise it is possible to exhibit a distinguisher for the IND-CPA experiment. In order to obtain a perfect simulation of all messages exchanged during the experiment, it is also necessary to modify inputs of the MAC function. For this purpose, the MAC scheme must be a pseudo random function, which is also required to avoid attacks as those presented in [6]. This is not restrictive in practice as most of MAC schemes verifies this property. In conclusion, as we use the game technique, the difference between the success probabilities of  $\mathcal{A}$  and  $\mathcal{A}^{\mathcal{B}}$  is increased by the advantage of an adversary against the IND-CPA property of the encryption scheme plus the advantage of an adversary against the pseudo-random property. As both of these advantages are negligible by definition, the success probability of  $\mathcal{A}$  must be negligible which demonstrates the unreachability property of our scheme.

## 5.2 The Hash El Gamal Case

The Hash El Gamal encryption scheme [11] is a variant of the classical El Gamal encryption scheme which uses a hash function. It allows a compact ciphertext and avoids problems with messages whose orders are not the one of the group.

**Description of the System.** Let  $G$  be a cyclic group of prime order  $q$ . The private key to decrypt a message is  $\text{esk} \in \mathbb{Z}_q$  and the corresponding public key is  $\text{epk} = g^{\text{esk}}$ . We thus obtain the RFID identification scheme described in Figure 6.

In a nutshell, we have described an efficient authentication scheme based on an IND-CPA public-key cryptosystem and a MAC scheme. It is sound and private as the DHAES scheme and seems to be efficient. In the next section we



**Fig. 6.** Hash El Gamal based protocol

give some implementation estimation for all presented schemes. We will then be able to conclude about the relevancy of an authentication scheme based on an IND-CPA public-key cryptosystem.

## 6 Comparison

It is notoriously difficult to make implementation estimates without going through the implementation process and so, by necessity, our estimates offer a rough guide only. In particular, since there are so many implementation variables (space, power, speed...) and so we have concentrated our efforts on getting an estimate for the space required, using as our data-points established reference points in the literature. Of course power consumption and timing are vital considerations, however our goal has been to give a first-order comparison between the schemes described in this paper. Throughout, we will use *gate equivalents* (GEs) as the unit of comparison. We're aiming for a 80-bit security level which is typically of interest and we will use approximately 160-bit elliptic curves.

**The Case of DHAES.** To reach our security model we choose the parameters  $\text{tk}$ ,  $a$ ,  $k_1$  and  $k_2$  to all be 80-bits in length. We might consider using coupons and pre-computing a set of 320-bit valid coupons of the form  $(T_0, k_1||k_2)$  where  $T_0 = g^r$  and  $k_1||k_2 = \mathcal{H}(T_0||\text{epk}^r)$ . These would be stored on the tag.

In terms of computational operations, the tag computes SYMENC over a 160-bit input as well as a MAC with a 160-bit input.

An efficient option would probably be to build the symmetric primitives out of a block cipher. One could use AES for SYMENC and a corresponding MAC-construction which could all be done for around 3600 GE [13], though some significant overheads to deal with different modes should be anticipated. A more lightweight possibility would be to use PRESENT [7] to construct both SYMENC and the corresponding MAC. A range of implementations suggests that 1500 GE would be a good estimate for the basic core, with a range of overheads suggesting that 2000-3000 GE could be enough. Finally the last possibility is to store the 160-bit key  $k_3$  generated by a pseudo random generator and  $k_2$  and to don't store  $k_2$  in the tag as a coupon. This means using 400-bit coupons  $(T_0, k_1||k_3)$ . As the exclusive-or on the tag of two 160-bit numbers requires around

400 GE, this increases slightly the number of gates but requires half less PRESENT computations so it appears as the most efficient in term of implementation.

**The Case of WIPR.** In [20], Oren and Feldhofer propose a hardware implementation of WIPR and obtain a total chip area of 5705 GEs. Note that this implementation does not use elliptic curves and coupons, and so this offers some additional storage and usage advantages over the schemes that do.

**The Case of El Gamal.** As in the case of DHAES, it is interesting to consider the use of coupons. In this scheme the 320-bit coupons are of the form  $(\text{epk}^r, T_2 = g^r)$ . However even though we use coupons, the computation that remains on the tag is an elliptic curve addition. Depending on the elliptic curve and the underlying field arithmetic, there are a vast range of different elliptic curve implementations available. The most striking are those of Batina *et al* [3] where we might expect an elliptic curve addition to take a few thousand GEs.

**The Case of Hash El Gamal.** Again, coupons are likely to make the most efficient implementations. In this scheme, the 480-bit coupons are of the form  $(k, \mathcal{H}(\text{epk}^r), T_1 = g^r)$ . It is possible to generalize the scheme by replacing the computation of  $T_0$  via the exclusive-or to encryption using any symmetric scheme. However, the use of the exclusive-or would perhaps offer the best implementation opportunities. In this case in term of implementation the situation is like the last possibility for DHAES with the difference than the tag has to store bigger coupons and to perform an exclusive-or between two 240-bit numbers instead of two 160-bit numbers so it requires approximatively 200 GE more.

**Summary.** While coupons carry a storage and usage cost, they are often the best technique available to make a serious reduction in the cost of an on-tag RFID computation. With these in place, most of the rest of the functionality can be provided using lightweight primitives such as PRESENT. This tend to all lead to roughly the same space cost for the cryptographic operations (except for the case of El Gamal) with a slightly edge for DHAES.

Table 1 sum up the previous comparison of this paper. It is obvious that in terms of security, the DHAES scheme is most promising than the Hash El Gamal scheme as for the same estimation of gate equivalent, security is proven in a better model, the standard one. But in terms of time execution, the the Hash El Gamal scheme seems better since the generation of the key  $k$  can be pre-computed while the execution of the hash function cannot.

**Table 1.** Comparison of schemes in gate equivalents and security proofs

Scheme	DHAES	WIPR	El Gamal	Our scheme
Security proof	standard model	don't exist	don't exist	ROM
GE	$\approx 3000$	5705	$> 5000$	$\approx 3000$

Nevertheless, we have prove in this paper that it is possible to reach the higher security level for an RFID authentication scheme from an IND-CPA encryption scheme. Then, it is may be possible to develop a really performant scheme by using such a scheme.

## References

1. Abdalla, M., Bellare, M., Rogaway, P.: DHAES: An Encryption Scheme Based on the Diffie-Hellman Problem. Technical report, UC Davis Computer Science (1998)
2. Avoine, G.: Adversarial Model for Radio Frequency Identification. Cryptology ePrint Archive, Report 2005/049 (2005)
3. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., Verbauwhede, I.: An Elliptic Curve Processor Suitable for RFID-Tags. In: IACR eprint (2006), <http://eprint.iacr.org/2006/227>
4. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., Verbauwhede, I.: Public-Key Cryptography for RFID-Tags. In: PerCom Workshops 2007, pp. 217–222. IEEE Computer Society, Los Alamitos (2007)
5. Bellare, M., Desai, A., Pointcheval, D., Rogaway, P.: Relations Among Notions of Security for Public-Key Encryption Schemes. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 26–45. Springer, Heidelberg (1998)
6. Bellare, M., Namprempre, C.: Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 531–545. Springer, Heidelberg (2000)
7. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
8. Boyen, X., Martin, L.: Identity-Based Cryptography Standard (IBCS) #1. In: Request for Comments: 5091. IETF (2007)
9. Bringer, J., Chabanne, H., Icart, T.: Efficient Zero-Knowledge Identification Schemes which respect Privacy. In: ACM Symposium on Information, Computer and Communication Security – ASIACCS 2009, Sydney, Australia (March 2009)
10. Canard, S., Coisel, I.: Data Synchronization in Privacy-Preserving RFID Authentication Schemes. In: Proceedings of RFIDSec 2008 (2008)
11. Chevallier-Mames, B., Paillier, P., Pointcheval, D.: Encoding-Free ElGamal Encryption Without Random Oracles. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T.G. (eds.) PKC 2006. LNCS, vol. 3958, pp. 91–104. Springer, Heidelberg (2006)
12. Damgård, I., Pedersen, M.Ø.: RFID Security: Tradeoffs between Security and Efficiency. In: Malkin, T.G. (ed.) CT-RSA 2008. LNCS, vol. 4964, pp. 318–332. Springer, Heidelberg (2008)
13. Feldhofer, M., Dominikus, S., Wölkerstorfer, J.: Strong Authentication for RFID Systems Using the AES Algorithm. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 357–370. Springer, Heidelberg (2004)
14. Gamal, T.E.: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory 31(4), 469–472 (1985)
15. Girault, M., Lefranc, D.: Public Key Authentication with One (Online) Single Addition. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 413–427. Springer, Heidelberg (2004)

16. Juels, A., Weis, S.A.: Defining Strong Privacy for RFID. In: PERCOMW 2007, Washington, DC, USA, pp. 342–347. IEEE Computer Society, Los Alamitos (2007)
17. Van Le, T., Burmester, M., de Medeiros, B.: Universally composable and forward-secure RFID authentication and authenticated key exchange. In: ASIACCS 2007, pp. 242–252. ACM, New York (2007)
18. McLoone, M., Robshaw, M.J.B.: Public Key Cryptography and RFID Tags. In: Abe, M. (ed.) CT-RSA 2007. LNCS, vol. 4377, pp. 372–384. Springer, Heidelberg (2006)
19. Ohkubo, M., Suzuki, K., Kinoshita, S.: Cryptographic Approach to “Privacy-Friendly” Tags. In: RFID Privacy Workshop 2003 (2003)
20. Oren, Y., Feldhofer, M.: WIPR - Public Key Identification on Two Grains of Sand. In: Proceedings of RFIDSec 2008 (2008)
21. Rabin, M.O.: Digitalized Signatures and Public-Key Functions as Intractable as Factorization. In: MIT Laboratory for Computer Science. MIT, Cambridge (1979)
22. Shamir, A.: SQUASH - A New MAC with Provable Security Properties for Highly Constrained Devices Such as RFID Tags. In: Nyberg, K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 144–157. Springer, Heidelberg (2008)
23. Shoup, V.: Sequences of Games: a Tool for Taming Complexity in Security Proofs (2004)
24. Vaudenay, S.: On Privacy Models for RFID. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 68–87. Springer, Heidelberg (2007)
25. Wu, J., Stinson, D.: How to Improve Security and Reduce Hardware Demands of the WIPR RFID Protocol. In: IEEE International Conference on RFID – RFID 2009, Orlando, Florida, USA (April 2009)