A Novel RFID Distance Bounding Protocol Based on Physically Unclonable Functions

Süleyman Kardaş[1,2], Mehmet Sabir Kiraz[1]
Muhammed Ali Bingöl[1,3], and Hüseyin Demirci[1]

[1] TUBITAK UEKAE, Gebze, Kocaeli, Turkey
[2] Sabanci University, Istanbul, TR-34956, Turkey
[3] Istanbul Technical University,
Institute of Science and Technology, Istanbul,Turkey

Abstract. Radio Frequency Identification (RFID) systems are vulnerable to relay attacks (i.e., mafia, terrorist and distance frauds) when they are used for authentication purposes. Distance bounding protocols are particularly designed as a countermeasure against these attacks. These protocols aim to ensure that the tags are in a distant area by measuring the round-trip delays during a rapid challenge-response exchange of short authenticated messages. Terrorist fraud is the most challenging attack to avoid, because a legitimate user (a tag owner) collaborates with an attacker to defeat the authentication system. Many RFID distance bounding protocols have been proposed recently, with encouraging results. However, none of them provides the ideal security against the terrorist fraud.

Motivated by this need, we first introduce a strong adversary model for Physically Unclonable Functions (PUFs) based authentication protocol in which the adversary has access to volatile memory of the tag. We show that the security of Sadeghi *et al.*'s PUF based authentication protocol is not secure in this model. We provide a new technique to improve the security of their protocol. Namely, in our scheme, even if an adversary has access to volatile memory she cannot obtain all long term keys to clone the tag. Next, we propose a novel RFID distance bounding protocol based on PUFs which satisfies the expected security requirements. Comparing to the previous protocols, the use of PUFs in our protocol enhances the system in terms of security, privacy and tag computational overhead. We also prove that our extended protocol with a final signature provides the ideal security against all those frauds, remarkably the terrorist fraud. Besides that, our protocols enjoy the attractive properties of PUFs, which provide the most cost efficient and reliable means to fingerprint chips based on their physical properties.

Key words: RFID, Distance Bounding Protocol, PUF, Security, Terrorist fraud.

1 Introduction

Radio **F**requency **ID**entification (RFID) is a technology that has been widely used in daily life, such as in access control, in electronic passports, public transportation, payment and ticketing. The reader communicates with the RFID tags using a wireless channel where the security and privacy requirements are satisfied via cryptographic building blocks (e.g, hash functions, symmetric encryptions and secure authentication protocols). However, such cryptographic mechanisms are not sufficient to enforce strong authentication in RFID systems. The seminal works of Desmedt *et al.* [7] and Beth *et al.* [2] on *mafia* and *terrorist frauds* demonstrated how an adversary can defeat such protocols by simply relaying the messages without dealing with cryptography. The *chess grandmaster attack*, which is introduced by Conway [6] in 1976, can be given as an illustration of the problem. In this problem, an unskilled player challenges two different chess grandmasters simultaneously. By only relaying the moves of the grandmasters the player finally either defeats one of the grandmasters or draws against both. Those kinds of attacks have been practically demonstrated in many different contexts and especially in RFID systems [12, 14–16, 21]. Nowadays, RFID and contactless smart card producers take relay attacks into account in the design of secure commercial products [25].

Mafia fraud is a kind of relay attack where an adversary is willing to be authenticated as if she is a legitimate prover. In order to perform this attack, the adversary relays the messages between a prover (e.g., a tag) and a verifier (e.g., a reader). Terrorist fraud is similar to mafia fraud except that the legitimate tag collaborates with an adversary to be able to authenticate her. However, the prover does not reveal his long-term private key to the adversary [5]. Finally, distance fraud is also similar to relay attacks where a fraudulent prover tries to persuade the verifier that she is within a certain authentication area whereas she is not.

In order to mitigate these frauds, two main countermeasures have been adopted. The first one is based on measuring the radio signal strength (RSS) so that the verifier can learn whether the prover is close to it. This method has a drawback that a capable adversary can regulate its signal strength to convince the verifier that it is close to the verifier [13]. The second one is measuring the round trip time of exchanged messages between the reader and the tag [7]. At *Eurocrypt'93*, Brands and Chaum [4] proposed the first distance-bounding protocol to prevent mafia fraud and distance fraud while leaving the terrorist fraud attack as an open issue. Then, several such protocols, which use the round trip time method, have been proposed to improve security levels against distance, mafia and terrorist attacks [1, 13, 19, 22, 24, 27, 29, 31, 32, 35]. However, one of the main obstacles of the existing distance bounding protocols is achieving the ideal security level (i.e., $(1/2)^n$ where n is a security parameter) against terrorist fraud. Some attempts to thwart terrorist fraud [32] yield a more serious security problem namely, the key recovery attack. This attack occurs due to the misuse of long-term key in the protocol [19].

Our Contributions. In this paper, we first analyze the security of Sadeghi *et al.*'s PUF based RFID authentication protocol [28] by our stronger adversarial model in which an adversary has access to the volatile memory of the tag. We show that their protocol is not secure in this model and we propose a new technique to avoid this attack even if the adversary has the ability to access volatile memory.

Next, we apply this technique to propose a new PUF based RFID distance bounding protocol. To the best of our knowledge, this is the first paper that introduces a PUF based RFID distance bounding protocol. It is well-known that obtaining the long-term key of a tag is crucial in order to successfully perform the terrorist and the distance frauds. One of the main problems of existing distance bounding protocols is storing the long-term key into its memory which can be obtained by a fraudulent prover. Our protocol has the advantage that the long-term key will not be stored in the memory of the tag but will be reconstructed by using a PUF circuit.

Our first PUF based distance bounding protocol is based on the well-known Hancke and Kuhn's scheme [13] which is the starting point of this work. Although their original protocol is known to be simple and efficient, the adversary's probability of success is high (namely $(3/4)^n$ for both the distance and the mafia frauds, and 1 for the terrorist fraud). By the use of PUF, the adversarial capabilities of the terrorist fraud is reduced to that of the mafia fraud. In this way, we improve the security of Hancke-Kuhn's protocol against the terrorist fraud from 1 to $(3/4)^n$.

We also propose our second distance bounding protocol which is an extension of the first one involving a hash-based final signature. To the best of our knowledge, this is the first protocol that achieves the ideal security levels $(1/2)^n$ against all frauds.

Outline of the paper. The organization of the paper is as follows: In Section II, we briefly describe some existing distance bounding protocols. In Section III, we illustrate the notion of PUF functions and its characteristics. Section IV describes the adversary capabilities for both PUFs and distance bounding protocols. In Section V, we propose our first distance bounding protocol and analyze its security. In Section VI, we present our second protocol and analyze its security. Section VII concludes the paper.

2 Distance Bounding Protocols

Distance bounding approach was a breakthrough to thwart relay attacks by measuring the round trip time of short authenticated messages. Brands and Chaum introduced the first distance bounding protocol [4]. This protocol aims to bring a solution to mafia and distance frauds. It consists of three phases, a slow phase, followed by a fast phase and a final signature phase. The first slow phase is used to exchange the committed random bits. The proximity verification is achieved by a bitwise challenge-response during the second phase (i.e., fast phase), namely after series of n rounds where n is a security parameter. For each round of the fast phase, the verifier measures the round-trip time in order to extract the propagation time. Finally, the prover sends a final signature to the verifier and opens the commitments to complete the protocol. The success probability of mafia and distance frauds for this protocol are $(1/2)^n$, but it is not secure against terrorist fraud.

Čapkun *et al.* modified the Brands and Chaum's protocol to achieve mutual authentication with distance-bounding [35]. However, their protocol is also vulnerable to terrorist fraud and is not resilient to bit errors during the rapid bit exchange.

Hancke and Kuhn proposed the first use of distance bounding protocol for RFID systems [13]. The major difference from Brands and Chaum's protocol is that it does not involve a final signature phase. This protocol involves a common secret symmetric-key k between a prover and a verifier. This protocol can be briefly described as follows. The verifier first generates a nonce N_v and sends it to the prover. Similarly, the prover also generates a nonce N_p and sends it to the verifier. Two n-bit registers R^1, R^2 are computed such that $R^1 \| R^2 = f(k, N_v, N_p)$ where f is a public pseudorandom function. After that, n-round fast phase starts. For each i-th round, the verifier picks a random challenge-bit c_i and sends it to the prover. The prover replies with a response-bit r_i such that

$$r_i = \left\{ \begin{matrix} R_i^0 & if c_i = 0 \\ R_i^1 & if c_i = 1 \end{matrix} \right\}.$$

The success probabilities against the mafia fraud and distance fraud are both equal to $(3/4)^n$ [13,18].

Distance bounding protocols are classified into two classes depending on whether a final signature is involved (e.g., [1,18,19,22,24,31,32]). These papers mostly focused on improving the security against mafia and distance frauds, and in fact some of them achieved the ideal security level $(1/2)^n$ against only both frauds. Furthermore, some others achieve $(3/4)^n$ as the best security level for terrorist fraud. Unfortunately, none of these protocols achieve the ideal security against terrorist fraud.

Avoine *et al.* [**?**] introduced a unified framework for improving the analysis and the design of distance bounding protocols. The black-box and the white-box security models are introduced in the distance bounding domain, and the relation between the frauds are described with respect to these models. In the white-box model, the prover can provide more information to the adversary since the can access the internal key. We note that all the protocols in the literature are analyzed in the white-box model and therefore, the security level is worse than that can be achievable in the black-box model.

In the next section, PUFs will be described which will be later used in our protocols. We later show that the use of PUFs eliminates our protocols to be analyzed in the white-box model.

3 Physically Unclonable Functions (PUFs)

Physically **U**nclonable **F**unctions (PUFs) were invented by Naccache and Fremanteau in 1992 [23]. A PUF is defined as an unclonable function that maps challenges to responses. The response r is calculated as a result of physical properties such as delays of gates and wires in a circuit, variations in the temperature and supply voltage. The unclonability of the function is guaranteed as a result of these physical processes. An ordinary PUF circuit may produce slightly different outputs to the same inputs. Using mechanisms like Fuzzy Extractors [9, 36], one can guarantee that PUF circuit produces the same response to the same challenge. For further information about other types of PUFs we refer to [30].

Since PUFs behave as a random function, it is hard to predict the inputs as given the outputs. Therefore, they can also be considered as one-way functions. In addition, a PUF circuit can easily be implemented into a small area with less than 1000 gates [33]. Besides that, their intrinsic structure yields resistance against tampering. When the adversary tries to evaluate a PUF or an IC, for instance, by using the probes to measure the wire delays, the characteristics of that particular PUF will be changed. Thus, this physical attack will not give any advantage to the adversary [20]. These features make PUF an attractive tool for authentication mechanisms in RFID systems.

In [26] the use of PUFs in RFID systems is proposed. The idea is to use a set of predetermined set of challenge-response pairs with the help of a database. The readers use the database to identify the tag. In this protocol, the possible challenge-response pairs are restricted with the database. A challenge also cannot be used for the second time, since it results to replay attacks. The proposed scheme has been implemented and analyzed in [8].

In [33], PUF is used as a secure key derivation mechanism. Instead of putting the key in memory, it is derived from the circuit each time whenever it is required. This property of PUFs mitigates the hardware-based cloning attacks. A practical illustration is RFID tags, which can easily be cloned. When equipped with a PUF, creating a clone in a reasonable time is impractical. Furthermore, the concept of SRAM-PUFs is proposed in [17]. They propose that SRAM memory cells can be used as a PUF mechanism which are readily available in the existing RFID chips.

A simple privacy preserving identification system is proposed in [3]. This protocol uses a PUF P for frequently updating the identity of tags where the reader stores the vector $(ID, P(ID), P^2(ID), \ldots, P^k(ID))$. To authenticate to a reader, a tag first sends its current ID and updates it using the PUF $P(ID)$. The reader searches the current identifier of the tag from the database. If the reader finds a tuple, it authenticates the tag and removes all the elements which have been used before in the authentication mechanism. Note that this protocol suffers from the Denial of Service Attacks since the tag must be re-initialized after at most k sessions.

Sadeghi *et al.* [28] suggested to deploy PUF (in a similar way as described by Tuyls and Batina in [33]) in order to develop a privacy-preserving tag authentication protocol for RFID systems. This protocol provides destructive privacy in the Vaudenay's formal framework [34].

In this paper, we will focus on an ideal PUF P such that $P : \{0,1\}^\ell \rightarrow \{0,1\}^m$ where the challenge c_i is mapped to the response r_i. P is said to be an *ideal PUF* if the following properties are satisfied.

1. If $c_i = c_j$, then we have $r_i = r_j$ for a PUF on a particular device. Presenting the same challenge to the PUF on a different device will produce a different response.
2. The mapping between c_i and r_i is unpredictable and random. For instance, if r_i and r_j differ in only a single bit, knowledge of c_i does not reveal usable information to predict c_j.
3. Any attempt to physically tamper with the device implementing P causes to change its physical characteristics. Namely, P is then destructed and can no longer be evaluated correctly.

We note that the third property of the idealized PUF can be achieved by integrating PUF circuit with the chip on the tag. To do so, Tuyls *et al.* in [33] propose *Integrated PUFs* (I-PUFs). For further information we recommend reading [28, 33]. In this work, we use the ideal PUF for distance bounding protocols and show how the security is enhanced to ideal levels.

4 Adversary Capabilities

In this section, we first present a stronger adversarial model for analysis of PUF based RFID authentication protocols which considers the accessibility to the internal state of tags. We next discuss the notion of white and black box models for distance bounding protocols. We aim to unify and express the adversarial capabilities of PUFs and distance bounding protocols.

4.1 Adversary capabilities for PUFs

In a PUF based authentication protocol, the shared secrets are stored in its physical characteristics instead of storing them in a non-volatile memory. These keys are reconstructed whenever needed during the execution of the protocol. As soon as the keys are reconstructed, they are stored in a volatile memory of the RFID chip. In some previous articles (e.g., [28, 33]), it is assumed that the communication between a PUF circuit and a chip is not tractable by any side-channel attack.

Unlike the previous works, in this paper, we propose a more stronger adversary model where an attacker has the ability to compromise the tag and reaches the state in the volatile memory. Since the structure of the PUF circuit has been destroyed, the attacker is no longer able to re-evaluate the PUF again. Thus, a malicious tag owner can perform only one side-channel attack on the tag and access the volatile memory only once. For instance, Halderman *et al.* recently demonstrated a side-channel attack for DRAM, called *cold boot attack* [11]. In this attack, they first powered off the system and later showed how to extend the main memory persistence by 'freezing' the DRAM chips in order to maintain the memory cell state. In this way, an adversary will be able to retrieve any password or cryptographic key that was not disappeared before the system is switched off.

The protocol of Sadeghi *et al.* [28] is facing a similar attack described above. Their protocol is briefly described as follows (Figure 1). Let $l \in \mathbb{N}$ be a security parameter, and F:$\{0,1\}^k \times \{0,1\}^{2\alpha} \rightarrow \{0,1\}^\beta$ be a public pseudorandom (PRF) function. Each tag $\mathcal{T}$ is equipped with a PUF function P:$\{0,1\}^\gamma \rightarrow \{0,1\}^k$ and is initialized with a random state $S_1 \in_R \{0,1\}^\gamma$. The credential of each tag (ID, K), where $K \leftarrow P(S)$ and is stored in the database DB of the reader. The reader $\mathcal{R}$ first picks a random nonce a to the tag $\mathcal{T}_{ID}$. Then, $\mathcal{T}_{ID}$ picks a random nonce b and evaluates the PUF function $K = P(S)$. $\mathcal{T}_{ID}$ computes $c = F_K(a, b)$ and sends the message c along with the random nonce b and immediately erases K, a, b and c from its volatile memory. Upon receiving of b and c, $\mathcal{R}$ evaluates $c' = F_K(a, b)$ for each tuple (ID,K) in DB until there is a match. If a matching (ID,K) is found, then it accepts $\mathcal{T}_{ID}$ and returns ID; otherwise, it rejects by sending $\perp$ back.

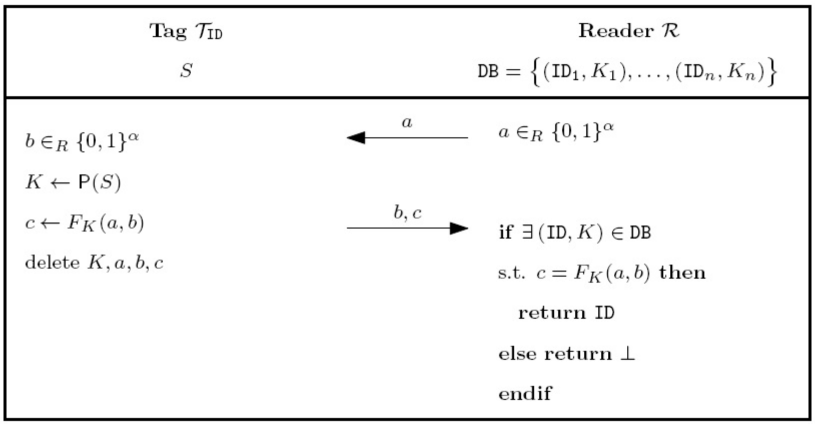
Tag $\mathcal{T}_{\mathtt{ID}}$
S
Reader $\mathcal{R}$
$\mathtt{DB} = \{(\mathtt{ID}_1, K_1), \ldots, (\mathtt{ID}_n, K_n)\}$
a
$a \in_R \{0,1\}^\alpha$
$b \in_R \{0,1\}^\alpha$
$K \leftarrow \mathsf{P}(S)$
$c \leftarrow F_K(a, b)$
b, c
delete K, a, b, c
if $\exists\,(\mathtt{ID}, K) \in \mathtt{DB}$
s.t. $c = F_K(a, b)$ **then**
return ID
else return $\perp$
endif

Fig. 1. Sadeghi *et al.*'s authentication protocol [28]

The authors claim that their protocol achieves destructive-privacy under the assumption that K is inaccessible. However, we show that their protocol suffers from the same above-mentioned cold-boot attack. Assume that an adversary sends a random nonce a to the tag $\mathcal{T}_{ID}$. $\mathcal{T}_{ID}$ then generates another random nonce b and reconstructs a secret K by evaluating the PUF with input S. The secret K is stored in the volatile memory during the computation of $c = F_K(a, b)$. The adversary compromises $\mathcal{T}_{ID}$ while $c = F_K(a, b)$ is computed and can capture the secret K. Hence, the tag can be successfully cloned although the structure of the PUF circuit has been destroyed.

In order to thwart this attack, instead of using only one key we propose to use two different keys K, L which are consecutively generated as outputs of the PUF function. Note that K and L never appear in the volatile memory at the same time. First, K is used as an input of one-way PRF function, and then completely deleted from the memory. Next, in a similar way, L is generated and used in the PRF function. Hence, whenever an adversary applies the above-mentioned attack he will be able to obtain only one of the keys, and hence will not have sufficient information to defeat the privacy. Also, since the PUF circuit has been destroyed he will not be able to perform the same attack again. Thus, applying our technique avoids the tag cloning.

4.2 Adversary capabilities for distance bounding protocols

In the analysis of our protocols, Dolev-Yao adversary model are considered [10]. In this model, the adversary can perform polynomial number of computations and cannot obtain the secret keys from the honest parties. This assumption is then relaxed with the terrorist and distance frauds, where the prover has access to the keys [?]. However, he disagrees to share these keys with any third party. The adversary may use one of the three strategies to query a prover such as pre-ask strategy, post-ask strategy and early-reply strategy. The detailed explanations of these strategies are addressed in [?].

As in the conventional distance bounding protocols, we also assume that the verifier is an honest party where it faithfully follows the protocol specifications without cheating. Mafia fraud is a kind of man-in-the-middle attack where an adversary defeats both honest parties i.e., verifier and prover. Unlike mafia fraud, in distance and terrorist frauds, the prover himself is dishonest. The previous distance bounding protocols consider that the prover has a full control on the execution of the algorithm in the device. As it is discussed in Section 3, PUFs can be used to provide resistance against side-channel attacks. Therefore, an adversary can be limited to the execution of the algorithm inside the device. In order to analyze distance bounding protocols, the generic capabilities of the adversary are addressed in [?]. The capabilities are categorized in two models, white-box model and black-box model. The following definitions of these two models are excerpted from [?].

Definition 1. ***(Black-box model)*** *In this model, the prover cannot observe or tamper with the execution of the algorithm.*

Definition 2. ***(White-box model)*** *In this model, the prover has full access to the implementation of the algorithm and has a complete control over the execution environment.*

Regarding to the white-box and the black-box models Figure 2 presents the relation between the distance, mafia and terrorist frauds. An arrow from X to Y means that, for any fraud in X that succeeds with probability p_X, then there exists an attack in Y that succeeds with probability p_Y such that $p_Y \geq p_X$. Two

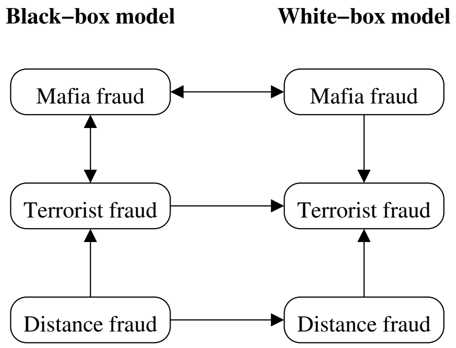

Fig. 2. Relations between the frauds in the white-box and the black-box models [**?**].

side arrow means that the success probabilities of two corresponding frauds are equal [**?**].

It is interesting to note that in the black-box model, the success probabilities of the mafia and the terrorist frauds are equal (Figure 2).

5 Our First Protocol

We now propose the first PUF based distance bounding protocol which is efficient for implementation in low cost devices. In the next section, we extend this protocol by adding a final signature to enhance the security against terrorist fraud. The former achieves the security level of $(3/4)^n$ against mafia, terrorist and distance frauds, where n is the number challenge/response bits during the fast phase. We show in the next section that the latter achieves the ideal security level against all the frauds (i.e., $(1/2)^n$).

5.1 Protocol descriptions

Our first distance bounding protocol is based on Hancke and Kuhn's scheme [13], which is the starting point of this work. Although their protocol is simple and efficient the adversary's probability of success is high. The steps of our protocol are summarized below and depicted in Figure 3.

Initialization Let $P_i : \{0,1\}^k \rightarrow \{0,1\}^\ell$ be a (unique) ideal PUF of the i-th legitimate prover $\mathcal{P}_i$. The credentials database DB of the verifier $\mathcal{V}$ stores a tuple (K_i, L_i) where $K_i = P_i(G_i^1)$ and $L_i = P_i(G_i^2)$ for random states G_i^1, $G_i^2 \in_R \{0,1\}^k$. Let also $F : \{0,1\}^\ell \times \{0,1\}^{2\ell} \rightarrow \{0,1\}^{2\ell}$ be a one-way pseudorandom function. We denote n as the main security parameter of the fast phase where $3n = 2\ell$. $|S|$ denotes the bit-length of a bit-string S.

Our protocol consists of two phases: a slow phase and a fast phase.

Slow phase:

- First of all, $\mathcal{V}$ generates a random nonce r_V and sends it to $\mathcal{P}_i$.
- Upon receiving r_V, $\mathcal{P}_i$ generates a random nonce r_P and reconstructs $K_i = P_i(G_i^1)$. $\mathcal{P}_i$ computes $T = F_{K_i}(r_P, r_V)$, then immediately deletes K_i from the memory. After that, $\mathcal{P}_i$ reconstructs the secret key $L_i = P_i(G_i^2)$ and computes the message $F_{L_i}(T)$. Similarly, $\mathcal{P}_i$ immediately deletes L_i from the memory. The value $F_{L_i}(T)$ is divided into three registers v_1, v_2 and v_3 where $|v_1| = |v_2| = |v_3| = n$. Finally, $\mathcal{P}_i$ sends r_T and v_1 to $\mathcal{V}$.
- Upon receiving r_T and v_1, for each tuple (K_i, L_i) in DB $\mathcal{V}$ searches $v_1', v_2', v_3' = F_L(F_K(r_P, r_V))$ such that $v_1' = v_1$. If not found, $\mathcal{V}$ aborts the protocol.

Fast phase:

- The fast phase consists of n bitwise challenge-response exchange. For each round $j \in \{1, \ldots, n\}$, $\mathcal{V}$ picks a random challenge bit c_j and sends it to $\mathcal{P}_i$.
- $\mathcal{P}_i$ immediately responds $r_j = v_2^j$ if $c_j = 0$, otherwise $r_j = v_3^j$.

Verification Whenever the fast phase is finished $\mathcal{V}$ verifies that the responses from $\mathcal{P}_i$ are correct and checks whether $\triangle t_j \leq \triangle t_{max}\ \forall\ j = 1, \ldots, n$ where $\triangle t_{max}$ is a timing bound.

5.2 Security analysis

Mafia, terrorist, and distance frauds are the three main security concerns when considering distance bounding protocols. The following Theorem 1 indicates that no adversary (e.g., a malicious tag owner) can access to both secrets K_i and L_i. Thus, the use of PUF in the protocol makes the RFID tags as tamper proof against any malicious adversary.

Theorem 1. *Let K_i, L_i be secrets of a tag $\mathcal{T}_i$ for some i in the above-mentioned protocol (see Figure 3). Assume that there is an adversary $\mathcal{A}$ with a full side-channel capability on the tag $\mathcal{T}_i$. If P_i is an ideal PUF, then $\mathcal{A}$ can only access either the secret K_i or the secret L_i, but not both in the same tag $\mathcal{T}_i$.*

Proof. (sketch) The pre-keys G_i^1 and G_i^2 are feeded into the P_i function to generate the real keys K_i and L_i. The real keys only appear during the execution of the protocol. Note that K_i and L_i never appear in the memory of $\mathcal{T}_i$ at the same time because K_i is first used as an input of a one-way PRF function, and then completely deleted from the memory. Next, in a similar way, L_i is generated and used in the PRF function. Whenever $\mathcal{A}$ applies a side channel attack to $\mathcal{T}_i$, the physical characteristics of the PUF P_i will be broken and will no longer be evaluated correctly. If $\mathcal{A}$ applies side-channel attack to extract K_i then the structure of P_i will be destroyed and L_i cannot be generated. Similarly, if $\mathcal{A}$ applies side-channel attack to extract L_i she cannot obtain K_i since it is already deleted. Therefore, $\mathcal{A}$ can access either K_i or L_i but not both. Hence, $\mathcal{A}$ will not be able to get the complete key of $\mathcal{T}_i$.

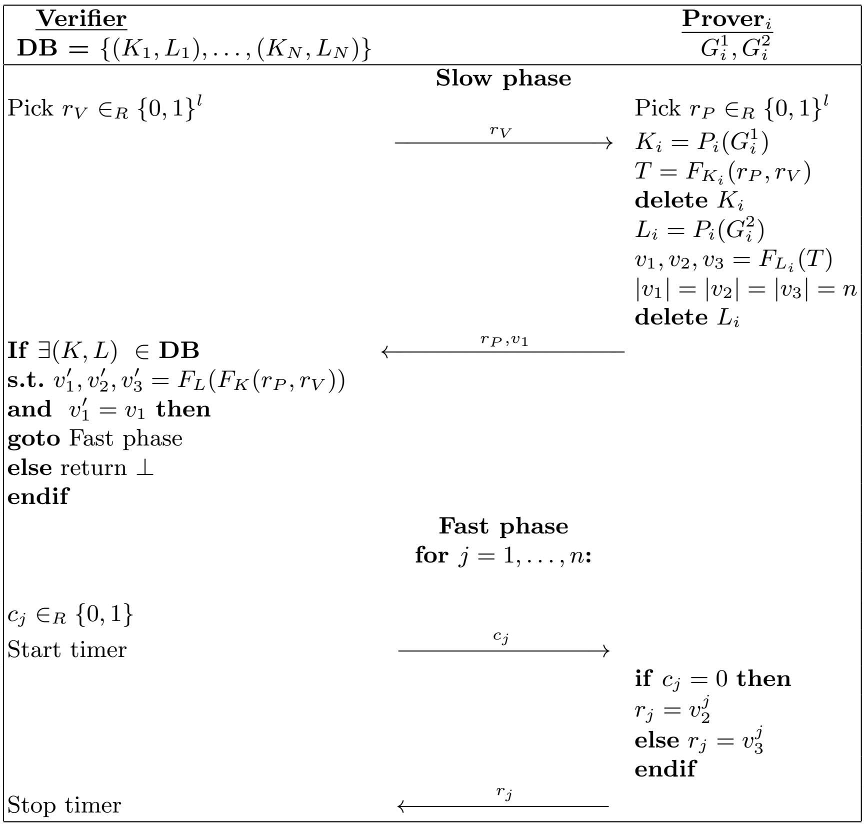
Verifier
$\mathbf{DB} = \{(K_1, L_1), \ldots, (K_N, L_N)\}$
Prover$_i$
G_i^1, G_i^2
Slow phase
Pick $r_V \in_R \{0,1\}^l$
Pick $r_P \in_R \{0,1\}^l$
r_V
$K_i = P_i(G_i^1)$
$T = F_{K_i}(r_P, r_V)$
delete K_i
$L_i = P_i(G_i^2)$
$v_1, v_2, v_3 = F_{L_i}(T)$
$|v_1| = |v_2| = |v_3| = n$
delete L_i
r_P, v_1
If $\exists (K, L) \in$ **DB**
s.t. $v_1', v_2', v_3' = F_L(F_K(r_P, r_V))$
and $v_1' = v_1$ **then**
goto Fast phase
else return $\perp$
endif
Fast phase
for $j = 1, \ldots, n$**:**
$c_j \in_R \{0,1\}$
Start timer
c_j
if $c_j = 0$ **then**
$r_j = v_2^j$
else $r_j = v_3^j$
endif
r_j
Stop timer

Fig. 3. Our first PUF based distance bounding protocol without a final signature.

Theorem 1 indicates that a malicious prover cannot obtain the secret keys, and thus cannot evaluate the registers v_1, v_2, v_3. Unlike existing distance bounding protocols, it is not possible to apply the white-box analysis to our protocol. Therefore, we analyze our protocol according to the black-box model. In the black-box model, note that it is already proven that the capability of terrorist fraud is equivalent to the mafia fraud [**?**] (see also Figure 2). Hence, we combine the security analysis of both mafia and terrorist frauds.

Note that a malicious prover can access the registers v_1, v_2, v_3 by applying side-channel attack only once. Furthermore, he can complete only the current session successfully because of the destruction of PUF. However, since the registers v_1, v_2, v_3 are randomized this does not give any future advantage to the adversary.

For a distance bounding protocol, an adversary is able to use three different strategies to conduct her attack such that early-reply, pre-ask, and post-ask [**?**]. We denote by $\mathcal{A}$ a malicious adversary. Let also denote by MF, TF and DF the mafia fraud, the terrorist fraud and the distance fraud, respectively. Let F be a fraud and S be the strategy used by the adversary $\mathcal{A}$. Let $Pr_{F|S}$ be the success probability in the black-box model of the fraud F ($MF/DF/TF$) using the strategy S (*early/pre/post*). Note that the strategies can also be combined and this is denoted by an &. Next, we describe the success probability of each fraud as follows.

Mafia and terrorist fraud analysis The adversary uses pre-ask or post-ask strategies in order to achieve mafia or terrorist fraud.

Pre-ask strategy [?] In this strategy, $\mathcal{A}$ first relays the slow phase between $\mathcal{V}$ and $\mathcal{P}$. Then $\mathcal{A}$ executes the fast phase with $\mathcal{P}$. $\mathcal{A}$ sends predicted challenges c'_j to $\mathcal{P}$ and get the responses r'_j corresponding to her challenges. With this a strategy, $\mathcal{A}$ obtains only one of the register. Afterward, $\mathcal{A}$ executes the fast phase with $\mathcal{V}$ and receives the challenges c_js. There are two equal likely cases, (i) if $c_j = c'_j$ $\mathcal{A}$ sends the correct response with probability of 1; otherwise, (ii) $\mathcal{A}$ guess the response with probability of 1/2. Hence, the success probability of mafia fraud and terrorist fraud for n-round fast phase is computed as follows.

$$Pr_{MF|pre} = Pr_{TF|pre} = \left(\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2}\right)^n = \left(\frac{3}{4}\right)^n .$$

Post-ask strategy [?] In pre-ask strategy, $\mathcal{A}$ first relays the slow phase, then executes the fast phase with $\mathcal{V}$. The probability of sending a correct response for a challenge is 1/2. Then, $\mathcal{A}$ queries $\mathcal{P}$ with the correct challenges received during the fast phase to check whether she is succeed on cheating. The success probability of mafia fraud for this strategy is:

$$Pr_{MF|post} = Pr_{TF|post} = \left(\frac{1}{2}\right)^n .$$

To maximize the success probability the attacker chooses the best strategy. Hence, the success probability of both mafia and terrorist frauds are $(3/4)^n$.

Distance fraud analysis In distance fraud, the tag owner herself is fraudulent who tries to cheat on her proximity from $\mathcal{V}$. It is important to highlight that unlike the existing protocols, the tag owner cannot control the internal executions of the tag in our protocol. The fraudulent prover can query its tag to get the responses. In distance fraud, since the prover is outside of the legal authentication region she should send the responses earlier in order to pass the proximity check (i.e., round trip time measurement). This is called *early-reply strategy* [**?**]. To ease our analysis, we denote the fraudulent tag owner by $\mathcal{A}$, and the tag by $\mathcal{T}$.

Pre-ask combined with early-reply strategy In this strategy, $\mathcal{A}$ first relays the slow phase between $\mathcal{V}$ and $\mathcal{T}$, then executes the fast phase with $\mathcal{T}$. $\mathcal{A}$ can only obtain n-bit responses corresponding to her predicted challenges. Since $\mathcal{A}$ is not inside the neighborhood of $\mathcal{V}$, she sends her responses in advance. Two cases occurs for each round of the fast phase. (i) $\mathcal{A}$ predicts $\mathcal{V}$'s challenge correctly, then she sends a correct corresponding response in advance. (ii) $\mathcal{A}$ cannot not predict $\mathcal{V}$'s challenge correctly, but she sends a correct answer with probability of 1/2. Thus, the distance fraud success probability is:

$$Pr_{DF|pre\&early} = \left(\frac{1}{2}\cdot 1 + \frac{1}{2}\cdot\frac{1}{2}\right)^n = \left(\frac{3}{4}\right)^n .$$

Post-ask combined with early-reply strategy Similar to the mafia fraud analysis, it is clear that using the post-ask strategy is equivalent to randomly guessing the responses,

$$Pr_{DF|post\&early} = \left(\frac{1}{2}\right)^n .$$

The distance fraud attacker chooses the strategy with the maximum success probability. Consequently, the success probability of distance fraud is $(3/4)^n$.

6 Our Extended Protocol

We are now ready to propose our extended protocol which is resistant to all the frauds.

6.1 Protocol descriptions

In what follows, we present our second protocol which is an extension of the first one by adding a final signature. This protocol consists of three phases. The first two phases are exactly the same with the previous protocol. In the third phase, the prover computes the following final signature

$$f_{sign} = h(c_1, \ldots, c_n, T, L_i).$$

where h denotes a collusion resistant and one-way hash function. To evaluate f_{sign}, first prover regenerate L_i once more and delete it from the memory as soon as f_{sign} is computed. The prover sends f_{sign} to the verifier, then the verifier checks the correctness of this message.

6.2 Security analysis

In the first protocol, mafia and distance frauds can successfully pass the fast phase with probability of $(3/4)^n$ by predicting the challenges. However, this attack does not work in the extended protocol because the challenges received by the tag are digested in f_{sign}. In order to pass the authentication, the adversary must send a valid final signature to the verifier. Similar to the first protocol, there are two strategies for both mafia and terrorist frauds:

(i) In the pre-ask strategy, the adversary first executes the fast phase with the prover by sending $c'_1, \ldots, c'_n$ challenges, then prover replies with the corresponding responses $r'_1, \ldots, r'_n$. In the final phase, the adversary gets $f'_{sign} = h(c'_1, \ldots, c'_n, T, L_i)$. The final signature is valid if and only if all the challenges $c_1, \ldots, c_n$ sent by the verifier are equal to the ones predicted by the adversary. Thus, it is clear that the probability of $f_{sign} = f'_{sign}$ is equal to $(1/2)^n$.

(ii) In the post-ask strategy, the adversary first plays with the verifier and guesses all the responses during the fast phase. If she passes the fast phase then it is easy to get the valid final signature from the prover by forwarding the challenges of the verifier. However, the probability of guessing all the correct responses during the fast phase is equal to $(1/2)^n$. Thus,

$$Pr_{MF} = Pr_{TF} = \left(\frac{1}{2}\right)^n .$$

Similarly, the security of the extended protocol for distance fraud is also bounded by $(1/2)^n$ due to the same reasons described-above. Namely, in order to receive a valid final signature from the tag the fraudulent prover should have queried the tag with all correct challenges in advance. Hence, the use of final signature enhances the security level of our extended protocol against the distance fraud to the ideal level $(1/2)^n$.

7 Conclusion

Relay attacks are indeed practical threats for RFID systems since using only cryptographic primitives it is not easy to thwart mafia, distance and terrorist frauds. Distance bounding protocols are used to mitigate these threats. However, the existing distance bounding protocols cannot achieve ideal security level against all frauds.

In this paper, we present the first PUF based distance bounding authentication protocol. Note that the protocols based on PUFs are known to be powerful since attacks can be easily prevented and the use of expensive cryptographic primitives can be minimized. In our protocol, we use the idea of key storage mechanism based on PUFs for public-key cryptosystems presented by Tuyls and Batina [33] (which is also later used for symmetric key storage by Sadeghi *et al.* [28]). We modified their protocol in such a way that all the keys are not constructed at the same time. This enables us to achieve a stronger assumption and there is no way to extract the whole secret key from the tag. We show that our first protocol achieves the security level of $(3/4)^n$ against mafia, terrorist and distance frauds. We also extend our protocol by adding a final signature to enhance the security levels. Namely, we achieve the security level $(1/2)^n$ against for all mafia, terrorist and distance frauds. To the best our knowledge, this is the first paper that achieves the ideal security level $(1/2)^n$ against all frauds.

An interesting further question is whether it is possible to find an efficient protocol without a final signature having the ideal security level against all frauds.

8 Acknowledgment

We thank anonymous referees for valuable comments on a previous version of this paper. This work has been partially funded by FP7-Project ICE under the grant agreement number 206546.

References

1. G. Avoine, C. Floerkemeier, and B. Martin. RFID Distance Bounding Multistate Enhancement. In *Proceedings of the 10th International Conference on Cryptology in India – Indocrypt 2009*, volume 5922 of *Lecture Notes in Computer Science*, pages 290–307, New Delhi, India, December 2009. Springer-Verlag.
2. T. Beth and Y. Desmedt. Identification tokens - or: Solving the chess grandmaster problem. In *CRYPTO*, volume 537 of *Lecture Notes in Computer Science*, pages 169–177, Santa Barbara, California, USA, August 1990. Springer-Verlag.
3. L. Bolotnyy and G. Robins. Physically unclonable function-based security and privacy in rfid systems. In *Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications*, pages 211–220, Washington, DC, USA, 2007. IEEE Computer Society.
4. S. Brands and D. Chaum. Distance-Bounding Protocols. In *Advances in Cryptology – EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 344–359, Lofthus, Norway, May 1993. Springer-Verlag.
5. L. Bussard and W. Bagga. Distance-bounding proof of knowledge to avoid real-time attacks. In S. Ryoichi, Q. Sihan, and O. Eiji, editors, *Security and Privacy in the Age of Ubiquitous Computing*, volume 181 of *IFIP International Federation for Information Processing*, pages 223–238, Chiba, Japan, May-June 2005. Springer-Verlag.
6. J. H. Conway. *On Numbers and Games.* Number 6 in London Mathematical Society Monographs. Academic Press, London-New-San Francisco, 1976.
7. Y. Desmedt, C. Goutier, and S. Bengio. Special Uses and Abuses of the Fiat-Shamir Passport Protocol. In C. Pomerance, editor, *Advances in Cryptology – CRYPTO'87*, volume 293 of *Lecture Notes in Computer Science*, pages 21–39, Santa Barbara, California, USA, August 1988. IACR, Springer-Verlag.

8. S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal. Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications. In *RFID, 2008 IEEE International Conference on*, pages 58–64, 2008.
9. Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, 38(1):97–139, 2008.
10. D. Dolev and A. C.-C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–207, 1983.
11. J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten. Lest we remember: cold-boot attacks on encryption keys. *Commun. ACM*, 52:91–98, May 2009.
12. G. Hancke. A Practical Relay Attack on ISO 14443 Proximity Cards. Manuscript, February 2005.
13. G. Hancke and M. Kuhn. An RFID Distance Bounding Protocol. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, Athens, Greece, September 2005. IEEE.
14. G. Hancke, K. Mayes, and K. Markantonakis. Confidence in smart token proximity: Relay attacks revisited. *Computers & Security*, 28(7):615 – 627, June 2009.
15. G. P. Hancke. Practical Attacks on Proximity Identification Systems (Short Paper). In *IEEE Symposium on Security and Privacy – S&P '06*, Oakland, California, USA, May 2006. IEEE, IEEE Computer Society.
16. M. Hlaváč and T. Rosa. A Note on the Relay Attacks on e-Passports: The Case of Czech e-Passports. Cryptology ePrint Archive, Report 2007/244, 2007.
17. D. E. Holcomb, W. P. Burleson, and K. Fu. Initial SRAM state as a fingerprint and source of true random numbers for RFID tags. In *In Proceedings of the Conference on RFID Security*, 2007.
18. O. Kara, S. Kardaş, M. A. Bingöl, and G. Avoine. Optimal Security Limits of RFID Distance Bounding Protocols. In S. O. Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 220–238, Istanbul, Turkey, June 2010. Springer.
19. C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira. The Swiss-Knife RFID Distance Bounding Protocol. In *International Conference on Information Security and Cryptology – ICISC'08*, volume 5461 of *Lecture Notes in Computer Science*, pages 98–115, Seoul, Korea, December 2008. Springer-Verlag.
20. L. Kulseng. Lightweight mutual authentication, ownership transfer, and secure search protocols for rfid systems. Master's thesis, Electrical & Computer Engineering Department, Iowa State University, 2009.
21. K. Markantonakis, M. Tunstall, G. Hancke, I. Askoxylakis, and K. Mayes. Attacking smart card systems: Theory and practice. *Information Security Technical Report*, 14(2):46 – 56, 2009. Smart Card Applications and Security.
22. J. Munilla and A. Peinado. Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels. *Wireless Communications and Mobile Computing*, 8(9):1227–1232, 2008.
23. D. Naccache and P. Fremanteau. Unforgeable identification device, identification device reader and method of identification. Patent-EP0583709, 1994.
24. V. Nikov and M. Vauclair. Yet Another Secure Distance-Bounding Protocol. Cryptology ePrint Archive, Report 2008/319, 2008.
25. NXP. NXP mifare plus – benchmark security for mainstream applications. http://mifare.net/downloads/NXP_Mifare_Plus_leaflet.pdf, 2009.

26. D. C. Ranasinghe, D. W. Engels, and P. H. Cole. Security and Privacy: Modest Proposals for Low-Cost RFID Systems. In *Systems, Proc. Auto-ID Labs Research Workshop*, 2004.
27. J. Reid, J. Gonzalez Neito, T. Tang, and B. Senadji. Detecting relay attacks with timing based protocols. In F. Bao and S. Miller, editors, *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security – ASIACCS '07*, pages 204–213, Singapore, Republic of Singapore, March 2007. ACM.
28. A.-R. Sadeghi, I. Visconti, and C. Wachsmann. PUF-Enhanced RFID Security and Privacy. In *Secure Component and System Identification – SECSI'10*, Cologne, Germany, April 2010.
29. D. Singelée and B. Preneel. Key Establishment Using Secure Distance Bounding Protocols. In *MOBIQUITOUS '07: Proceedings of the 2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking&Services (MobiQuitous)*, pages 1–6, Philadelphia, Pennsylvania, USA, August 2007. IEEE Computer Society.
30. G. E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. In *DAC '07: Proceedings of the 44th annual Design Automation Conference*, pages 9–14, New York, NY, USA, 2007. ACM.
31. R. Trujillo Rasua, B. Martin, and G. Avoine. The Poulidor Distance-Bounding Protocol. In S. O. Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 239–257, Istanbul, Turkey, June 2010. Springer.
32. Y.-J. Tu and S. Piramuthu. RFID Distance Bounding Protocols. In *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.
33. P. Tuyls and L. Batina. RFID-Tags for Anti-counterfeiting. In *Topics in Cryptology – CT-RSA 2006*, volume 3860 of *LNCS*, pages 115–131, 2006.
34. S. Vaudenay. On privacy models for rfid. In *Proceedings of the Advances in Crypotology 13th international conference on Theory and application of cryptology and information security*, ASIACRYPT'07, pages 68–87, Berlin, Heidelberg, 2007. Springer-Verlag.
35. S. Čapkun, L. Buttyán, and J.-P. Hubaux. SECTOR: secure tracking of node encounters in multi-hop wireless networks. In *SASN'03 : Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 21–32, New York, NY, USA, 2003. ACM.
36. L. R. Yevgeniy Dodis and A. Smith. *Security with Noisy Data, chapter Fuzzy Extractors.* Springer-Verlag, 2007.