A Formal Framework for Cryptanalyzing RFID Distance Bounding Protocols

(eprint version)

Gildas Avoine[1], Muhammed Ali Bingöl[2⋆], Süleyman Kardaş[2⋆], Cédric Lauradoux[3], and Benjamin Martin[1]

[1] UCL, Information Security Group, Louvain-la-Neuve, Belgium
[2] TUBITAK UEKAE, Gebze, Kocaeli, Turkey
[3] INRIA SWING, CITI Laboratory, Villeurbanne, France

Abstract. Many distance bounding protocols appropriate for RFID technology have been proposed recently. However, the design and the analysis of these protocols are not based on a formal perspective. Motivated by this need, a formal framework is presented that helps the future attempts to cryptanalyze and design new distance bounding protocols. We first formalize the adversary scenarios, the protocol means, and the adversary goals in general. Then, we focus on the formalism for RFID systems by describing and extending the adversary strategies and the prover model. Two recently published distance bounding protocols are cryptanalyzed using our formal framework to demonstrate its relevancy and efficiency. Our formalism thus allows to prove that the adversary success probabilities are higher than the originally claimed ones.

Key words: Authentication, Distance bounding, Proximity check, RFID.

1 Introduction

Impact of the mafia fraud. Desmedt, Goutier, and Bengio presented at Crypto'87 a new attack called the *mafia fraud* [12] that defeats any authentication protocol. In this attack, the adversary successfully passes the authentication by relaying the messages between the verifier and the legitimate prover. When it was introduced, the mafia fraud appeared somehow artificial because the legitimate prover is required to be involved in the execution of the protocol without being aware of the manoeuvre.

The mafia fraud recently resurrected with the deployment of ubiquitous computing systems, especially those based on radio-frequency identification (RFID), including contactless smartcards. Everyone employs RFID tags daily, for example for mass transportation, ticketing, access control, electronic passports, etc. Whatever the capabilities of the tags, from a simple memory to a powerful contactless smartcard, they all share the peculiarity that they answer to the reader's requests without any agreement or awareness of their holder. The mafia fraud is so a major issue of concern for contactless systems and we illustrate its impact in a real environment as follows.

Consider a payment system based on contactless credit cards, for example [10,42]. An adversary would like to "buy" an expensive good without paying it herself. An accomplice is located in the changing room of a swimming pool and scans all the lockers until finding one containing a contactless credit card. Once found, the attack can start: the adversary forwards to her accomplice all the requests from the payment terminal of the merchant. The accomplice sends them to the credit card, receives its responses, which are in turn forwarded to the payment terminal through the accomplice and the adversary. The communication between the adversary and her

⋆ This work is partially funded by FP7-Project ICE under the grant agreement number 206546.

accomplice can be set up using mobile phones. One may argue that the merchant will detect the attack. However, some payment systems are based on the NFC technology [15] (in brief, an NFC device is an RFID-friendly mobile phone), which still facilitates the masquerade because the merchant is not able to see that the mobile phone performs a mafia fraud.

Feasibility of the mafia fraud. The mafia fraud is clearly a practicable attack. The messages between the verifier and the prover are relayed at a very low level, definitely below the application layer where the cryptographic messages are sent. Consequently, the attack can be performed even if the adversary as no clue about what is exchanged in the application layer.

In 2005, Hancke [18] demonstrated that a mafia fraud can be performed while the two colluders are distant from 50 meters and connected through a radio-channel. This is long enough to perform the attack in a waiting line in front of a ticketing machine for example. This attack was applied to RFID but [21, 25, 29] point out that some other domains are targeted by the mafia fraud. Recently, Adam Laurie published on Internet material to carry out a mafia fraud with off-the-self RFID devices [28]. This work puts the mafia fraud accessible to everyone.

In 2007, Halváč and Rosa [17] noticed that the standard ISO 14443 [24] targeting proximity cards and widely deployed in secure applications, can easily be abused by a mafia fraud due to the untight timeouts in the communication. Indeed, the standard ISO 14443 specifies a *frame waiting time* (FWT) such that the reader is allowed to retransmit or give up the communication if the queried tag remains unresponsive while the FWT is over. However, when the tag needs more time to process the information it receives, it can impose the reader to increase the FWT up to 4.949 second. Such an untight timeout is long-enough to carry out a mafia fraud over thousands kilometers.

Distance bounding in the literature. The first countermeasure against mafia fraud was suggested by Desmedt *et al.* [2, 3, 12] by introducing the distance checking concept based on the measurement of the round trip time of exchanged messages. Brands and Chaum [5] then designed the first distance checking protocol based on the ideas of Desmedt *et al.*

Since then, many works about distance checking have been published, which include variants of the problem and improvements of the solutions. Unfortunately, all of them address the problem in a pedestrian way, which leads to confused or erroneous analysis. For example, the mafia fraud (e.g., [12]) is also known as a relay attack (e.g., [1, 17, 18, 20, 25, 26, 36, 38]), a chess grandmaster problem (e.g, [3]), or a wormhole problem (e.g., [22, 23]). The distance fraud (e.g., [26, 34, 37]) is also considered as a relay attack but there is actually no relay in such an attack. As a last example of the current situation, in some papers, the prover as a full access to its internal calculations (e.g., [2]) while she can only observe them in some other papers (e.g., [33]). This lack of formalism leads to underestimated adversary success probabilities.

Contributions. This paper aims to provide a formal framework for cryptanalyzing and consequently designing distance bounding protocols suited to RFID systems. To do so, it formalizes the adversary scenarios, the protocol aims, and the adversary goals. Our work then refines the formalism for RFID systems; in particular, it formalizes the adversary strategies and the prover model.

In order to illustrate the benefit of our formalism, we apply it to two recently published distance bounding protocols: Munilla and Peinado's protocol [34] and Singelée and Preneel's protocol [40]. Munilla and Peinado have used "void challenges" to extend the protocol of Hancke and Khun [19]. We exploit the use of the void challenges to increase the attacker success probability. Singelée and Preneel have proposed in [40] a variant of the Mutual Authenticated Distance

Bounding protocol (MAD) [8] resilient to noise. Their solutions is based upon error correcting codes. We show a new attack strategy that improves the previous result for some parameters considered in [40].

Road map. Section 2 introduces a general threat model formalism, including attack scenarios, protocol aims, and adversary goals. Section 3 describes the relevancy of the formalism with respect to the adversary goals. Section 4 refines the formalism to suit it to RFID systems, taking into account their specificities, and supplies new tools to analyze these systems in a more efficient way. We then illustrate in Section 5 and Section 6 the power of our formalism by stressing new weaknesses on two existing protocols. We finally conclude in Section 7.

2 Formalism of the Threat Model

In what follows, we consider a two-party communication protocol, performed between Alice and Bob. As commonly admitted, we assume that no two competing attacks can occur during a same instance of the protocol. The adversary can be a third party, called Eve, or a dishonest party among the two communicating ones. Without loss of generality, we assume in the latter case that the party that does not follow the protocol properly is Alice. Note that Alice and Eve can potentially collude.

Section 2.1 defines scenarios independently of the considered protocols. Section 2.2 targets two specific protocol aims, which are authentication and distance checking. Section 2.3 defines the respective adversary goals.

2.1 Attack Scenarios

Definition 1 is a broad-sense definition where Alice is the only involved adversary. Definition 2 concerns the well-known concept of man-in-the-middle. Finally, Definition 3 and Definition 4 provide two variants of the man-in-the-middle attack – *mafia fraud* and *terrorist fraud* – that depend on the honesty of Alice.

Definition 1 (Cheat Fraud). *Given a two party protocol executed between Alice and Bob, a* cheat fraud *is an attack where Alice is dishonest without any help from Eve.*

Definition 2 (Man-In-The-Middle). *A* man-in-the-middle *(MITM) is a form of attack, where Eve provokes or manipulates the communication between Alice and Bob. Manipulating the communication means relay, withhold, or insert messages.*

Remark 1. Definition 2 does not assume anything about the honesty of Alice.

Definition 3 (Mafia Fraud). *Given a two party protocol executed between Alice and Bob, a mafia fraud is a MITM where Alice is honest.*

Definition 4 (Terrorist Fraud). *Given a two party protocol executed between Alice and Bob, a terrorist fraud is a MITM, where Alice actively helps Eve to maximize her attack success probability, without giving any advantage to Eve for future attacks.*

Remark 2. Cheat, mafia, and terrorist frauds can be characterized by the level of collusion between Alice and Eve. In the mafia fraud, Eve is not helped by anyone. In the terrorist fraud Eve colludes with Alice. Finally the cheat fraud is a degenerated case where Eve and Alice are combined in a single entity.

Remark 3. In the literature, the generic term *relay attack* is used to refer to any of the three above-mentioned attacks.

2.2 Protocol Aims

Our formalism addresses two protocols aims that are *authentication* and *distance checking*. Authentication is a well-known concept already defined in many classical textbooks. Below, we remind the definition given in [31].

Definition 5 (Authentication). *An authentication is a process whereby one party is assured (through acquisition of corroborative evidence) of the identity of a second party involved in a protocol, and that the second has actually participated (i.e. is active at, or immediately prior to, the time evidence is acquired).*

We similarly define the concept of distance checking.

Definition 6 (Distance Checking). *A distance checking is a process whereby one party is assured (through acquisition of corroborative evidence) that a given property on its distance to a second party involved in a protocol is satisfied at some point in the protocol. The area where the property is satisfied is called the neighborhood of the verifying party.*

Remark 4. The previous definition does not suggest any *distance*. In Section 4, we will focus on RFID-based systems, where the *Euclidean* distance is the most meaningful, and also the one used in most of the previous works [1, 5–7, 13, 19, 26, 27, 30, 33–35, 38, 40, 41]. Some other works consider different distances, for example distance checking protocols to counter wormholes in computer networks [8, 9, 22, 23].

Remark 5. There is no *property* on the distance suggested in Definition 6. Depending on the considered protocol, the property can be for example an upper-bound or a lower-bound on the distance between the two parties.

Definition 7 (Distance Bounding). *A distance bounding is a distance-checking where the process succeeds if the distance between the two parties is bounded by a given value.*

Remark 6. One may also suggest that the property relies on the exact measurement of the distance. This is not always practical, especially when considering low-capability devices, which justifies that many existing works consider distance bounding only, especially distance upper-bounding. This particular variant is also known in the literature as *proximity check* or simply *distance bounding* [1, 5–8, 13, 19, 26, 27, 30, 33–35, 38, 40, 41].

2.3 Adversary Goals

Following the definitions of authentication and distance checking, we provide below the related definitions for the adversary goals. Definition 8 reminds the *impersonation attack* as suggested in [31]. We then define in the same vein the concept of *distance attack*.

Definition 8 (Impersonation Attack). *An impersonation attack is a deception whereby one entity purports to be another.*

Definition 9 (Distance Attack). *A distance attack is a deception whereby one entity purports to be in the neighborhood of a second one.*

3 Relevancy of the Formalism w.r.t. the Adversary Goals

We now check the relevancy of the three attack scenarios defined in Section 2.1 with respect to the three protocol aims defined in Section 2.2. We use for that the impersonation and distance attacks defined in Section 2.3.

3.1 Authentication Protocols.

Cheat fraud. The cheat fraud in the context of authentication is an impersonation attack that does not involve the impersonated party. It matches the classical definition of impersonation attack described in textbooks.

Mafia and terrorist frauds. Performing a mafia fraud or a terrorist fraud is also clearly relevant with respect to authentication. Indeed, they have been both originally proposed in this framework by Desmedt, Goutier, and Bengio at Crypto 87 [12], then extended with Brassard and Quisquater in [2]. Their goal was to prove that the Fiat-Shamir zero-knowledge protocol [14] was weaker than what was claimed by Shamir when he said that his protocol is secure even being executed one million times in a Mafia-owned store [16].

3.2 Distance Checking Protocols.

Cheat fraud. The cheat fraud in the context of distance checking is a distance attack where Alice is not in the neighborhood of Bob. To illustrate this case, consider an example where Alice is bored to waste time each time she leaves her parking lot, just because Bob is used to park his car too close to Alice's one. To prevent Bob's car from being so close, Alice performs a distance cheat fraud against Bob's sensor-based car parking aid system: Alice's car cheats on the distance between the two cars in order to save some room for Alice's manoeuvres. Note that this example illustrates that distance checking does not necessarily requires authentication.

Mafia and terrorist frauds. On the other side, because there is no authentication, Bob cannot distinguish Eve from Alice when a mafia or a terrorist fraud is performed against a distance checking. Consequently, when Eve is within the neighborhood of Bob, as depicted in Figure 1(a), there is no attack since she already legitimately fulfills the requirement of the protocol. One could make the parallel with the authentication problem: there is no attack when someone tries to impersonate himself. Figure 1(b) shows the case where Eve is outside Bob's neighborhood. In this situation, the mafia or terrorist fraud is nothing more than a cheat fraud between Eve and Bob because the latter does not care about the identity of the other party. Consequently, we can state that analyzing the resistance of a distance checking (only) protocol

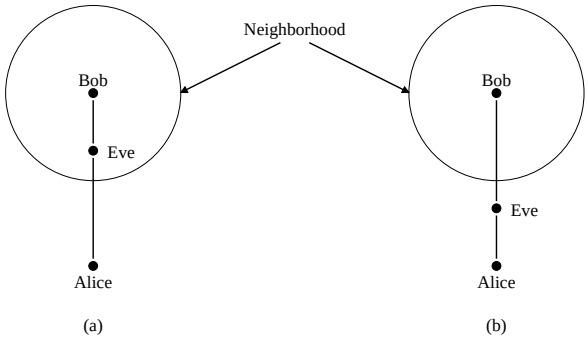

Fig. 1. Scenarios for distance mafia and terrorist frauds

against a mafia or terrorist fraud does not make sense.

3.3 Distance Checking with Authentication Protocols.

As already mentioned, Desmedt *et al.* [2, 12] suggested the mafia and terrorist frauds in the framework of authentication. They introduced the distance checking [3] as a countermeasure to these frauds, not as a primary goal. Brands and Chaum [5] then designed the first distance checking protocol based on the ideas of Desmedt *et al.* Since then, all the works about distance checking [1, 6, 8, 9, 19, 26, 27, 33–35, 38, 40] were related to physical devices and considered both authentication and distance checking as primary goals.

It is so legitimate to consider that an execution of distance checking with authentication succeeds if the distance and the authentication requirements are both fulfilled. Consequently, an attack succeeds if and only if the distance checking with authentication succeeds while at least one of the two requirements was not legitimately satisfied by the adversary.

Cheat fraud. In this case, the cheat fraud can be used to defeat (a) the distance checking, (b) the authentication, or (c) both of them. These three cases must be considered when analyzing a distance checking with authentication protocol.

As an illustration, consider the following example. A burglar would like to steal a famous painting in a picture gallery, protected with a radio anti-theft system: RF-reader on the wall and RF-transponder on the painting. To give him enough time to go away, the burglar desires to defeat the anti-theft system; three cases must be considered. (a) The burglar takes away the painting and defeats the anti-theft system remotely using a communication channel between the reader and the transponder on the painting (distance attack). (b) The burglar takes away the painting and places a poor one instead (impersonation attack). (c) The burglar uses a communication channel between the reader and a poor painting, so that the deception still continues once she sold the famous painting (impersonation and distance attacks).

Mafia and terrorist frauds. If Alice is inside Bob's neighborhood, the distance checking with authentication legitimately succeeds and speaking about attack does not make sense. Consequently, we assume that Alice is outside Bob's neighborhood. The security analysis must so consider only two cases, whether or not Eve is inside Bob's neighborhood as depicted in Figure 1.

4 Refinement of the Formalism for RFID Environments

In Section 2 and Section 3, we provided a general framework for analyzing distance checking with authentication protocols. In Section 4, we refine this framework to suit it to RFID systems. This refinement allows us to better and finer analyze RFID-friendly distance checking with authentication protocols, commonly and simpler known as distance bounding protocols. Hence, for the sake of simplicity and in accordance with the literature, we will use the remaining parts of this paper the term *distance bounding protocol* as a shorter denomination than *distance upper-bounding with authentication protocol*.

In the previous sections, unilateral or multilateral distance checking and authentication were both considered. In RFID applications, although reader and tag can be both verifier and prover with respect to authentication, the tag is always the prover when considering distance checking. In what follows, we will so call Bob the verifier (an RFID reader) and Alice the prover (an RFID tag).

4.1 Distance Measurement

There exist several methods to evaluate the distance between two parties. The most common ones are summarized below.

Received Signal Strength (RSS) is the core of radar systems. However, in modern wireless communications, signal amplifiers put the security of such solutions into question. As an illustration, readers will find details on how to build an ISO 14443-A compliant RFID amplifier in [32].

Global Positioning System (GPS) is very common nowadays to localize goods and persons. When the two parties have access to this technology, the verifier can evaluate an upper bound on its distance to the prover. However, this technology requires dedicated hardware and significant power supply that are not available in low-cost RFID devices.

Round Trip Time (RTT) can be used to evaluate the distance between two parties. By measuring the RTT of a message, the sender of the message can estimate an upper bound on its distance to the recipient, given that it cannot propagate faster than the light. This solution requires a single trusted clock owned by the sender and is the common way to design distance bounding protocols for low-cost devices. That is the approach we consider in the sequel.

4.2 Distance-bounding Authentication Protocols Based on RTT

Among the existing distance checking with authentication protocols based on RTT, one may distinguish two large families: either the authentication and the distance checking are done separately, or they are done jointly. The earliest protocol of the first family has been proposed by Brands and Chaum [5]. Later on, Hancke and Kuhn [19] proposed a protocol in which authentication and distance checking are combined. Both protocols can be implemented using symmetric-key cryptography. We briefly describe these two protocols.

Brands and Chaum's protocol. The protocol consists of three phases: the first and the final ones are denoted "slow phases", and the second one is called "fast phase". RTT are measured during the fast phase only. The slow phases include all the time-consuming operations; in particular the final slow phase is used to complete the authentication.

Slow Phase 1 – The prover and the verifier randomly generate n bits, respectively $m = (m_1, \ldots, m_n)$ and $c = (c_1, \ldots, c_n)$. The prover then commits on m to the verifier. At the end of this phase, the prover obtained the n-bit value $r := (r_1, \ldots, r_n)$.

Fast Phase – Verifier and prover perform n rounds where, for each of them, the verifier sends a 1-bit challenge c_i and the prover replies $r_i := c_i \oplus m_i$.

Slow Phase 2 – The prover computes and sends to the verifier the value $s = \mathrm{sign}_k(c \parallel r)$ where sign is a signature algorithm, k the prover's key, and $\parallel$ the interleaving operator, i.e., $c \parallel r = (c_1, r_1, \ldots, c_n, r_n)$. The prover finally opens the commitment on m. The verifier checks that the received r matches the expected one, the signature is correct, and the RTTs are valid.

Hancke and Kuhn's protocol. The protocol consists of a single slow phase followed by a fast one. The fast phase allows the verifier to check both the authentication and the distance.

Slow phase – The prover and the verifier exchange nonces, respectively N_P and N_V. From these values, a pseudo random function f and a shared secret k, they both compute a $2n$-bit value $H = f(k, N_V, N_P)$. Then, the value H is split in two n-bit registers H^0 and H^1. These registers are used in the fast phase to authenticate the prover and to verify the distance.

Fast phase – Verifier and prover perform n rounds where, for each of them, the verifier sends a 1-bit challenge c_i and the prover replies $r_i = H_i^{c_i}$, which denotes the ith bit of the register H^{c_i}.

Upon reception of the last answer, the verifier checks whether the received responses match the expected ones, and whether the RTTs are valid. Some other schemes [26, 34], use the same approach with additional registers.

General sketch. Existing works are based on either Hancke and Kuhn's approach [1, 19, 26, 35, 38] or on Brands and Chaum's approach [5, 27, 33, 34, 40, 41]. A general sketch for all these schemes is the following one: the protocol begins with a slow phase, followed by a fast phase, and finally followed by an optional second slow phase. The critical part in this model is the fast phase, which detects suspicious RTTs. The different strategies for the attacker are discussed in the next section with respect to this model.

4.3 Adversary Strategies for Mafia and Terrorist Frauds

In order to deceived the verifier, an adversary, who wants to mount a mafia or a terrorist fraud has to exploit the characteristics of the considered protocol. Our formalism provides three strategies that unify all the existing attacks on distance bounding protocols.

No-ask strategy. The adversary does not interact with the prover during the attack.

Pre-ask strategy. The adversary queries the prover before he starts the fast phase with the legitimate verifier. With such a strategy, the adversary can for example obtain one register among two in Hancke and Kuhn's protocol, or she can she retrieve the random value m in Brands and Chaum's protocol.

Post-ask strategy. The adversary queries the prover after the verifier stops the fast phase. This strategy only makes sense if a second slow phase exists. For example, an adversary can randomly answer to the verifier in the Brands and Chaum's protocol, and finally apply a post-ask strategy by querying the prover with the right challenges in order to get the valid signature.

Remark 7. The no-ask and pre-ask strategies have been introduced in [26]. The post-ask strategy is usually forgotten in the published security analysis and was never clearly defined before.

4.4 Prover Model

After defining the adversary strategies, it is important to refine the adversary means according to the prover model. Indeed the relation between the prover and the algorithm executed at the prover side during the protocol becomes a major concern in the choice of the best strategy, especially for the cheat and terrorist frauds. Two situations are considered in our formalism, the black box model [4, 43] and the white box model [11, 39], as defined below.

Definition 10 (Black-box model). *In a black-box model, the prover cannot observe or tamper with the execution of the algorithm.*

Definition 11 (White-box model). *In the white-box model, the prover has full access to the implementation of the protocol and a complete control over the execution environment.*

Remark 8. We emphasize that the two models only concern the prover, Alice. The external adversary, Eve, is neither able to directly observe not to tamper with the execution of the protocol.

Figure 2 presents the relations between the attack scenarios and the models. An arrow from A to B, both corresponding to a pair (attack scenario, model) means that: if there exists an attack in A that succeeds with probability p_A, then there exists an attack in B that succeeds with probability p_B such that $p_B \geq p_A$. A crossed out arrow means that the implication is false. Note that finding relations between cheat frauds and mafia/terrorist frauds is out of the scope of this paper, because cheat frauds involve two parties while mafia and terrorist frauds involve three parties.

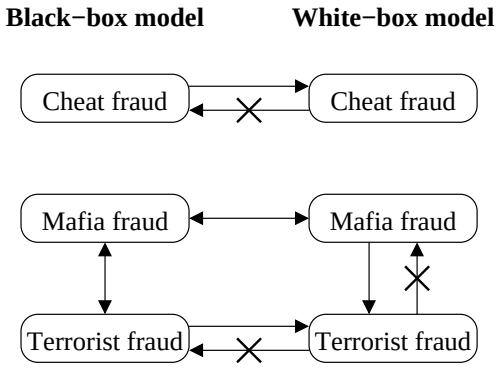

Fig. 2. Relations between the attack scenarios in the white-box and black-box models.

Cheat fraud. The adversary is the prover in a cheat fraud. Because she has access to more information in the white box model, her success probability is obviously higher than in the black box model. The reverse implication is clearly false. For example, the best attack in the black box model against Hancke and Kuhn's protocol has a success probability equal to $\left(\frac{1}{2}\right)^n$: the dishonest prover must answer randomly in each rounds without waiting for the challenge from the verifier. In the white box model, the adversary definitely knows in advance the right answer in round i when $H_i^0 = H_i^1$, which leads to a success probability equal to $\left(\frac{3}{4}\right)^n$. This proves that the reverse implication is false.

Mafia fraud. The prover does not collude with the adversary in the mafia fraud. Because the output of an honest prover is independent of the considered model, black-box or white-box, the success probability of the adversary is not influence by the model. This proves the equivalence stated in Figure 2.

Terrorist fraud. The prover colludes with the adversary in the terrorist fraud. Similarly to the cheat fraud, the prover has access to more information in the white box model than in the black model, and so the adversary. This proves the implication from the black-box model to the white-box model. The reverse implication is false. Indeed, best adversary success probability is $\left(\frac{3}{4}\right)^n$ in the black-box model, while she succeeds with probability 1 in the white-box model [27].

Mafia fraud vs terrorist fraud. In the black-box model, the prover cannot observe or tamper with the execution of the algorithm. Consequently, even if he colludes with the adversary, he has no way to provide her information that she would not be able to obtain herself. This clearly proves that mafia fraud and terrorist fraud are equivalent in the black box model. In the white-box model, the prover has access to more information than in the black-box model; because the prover colludes with the adversary, the success probability of the adversary is at least as high in the white-box model than in the black-box one. This prove the implication. The reverse

implication is false. For example, the best mafia fraud attack in the Hancke and Kuhn's protocol has a success probability equal to $\left(\frac{3}{4}\right)^n$ [19] while there exist a terrorist fraud attack against Kuhn's protocol that has a success probability equal to 1 [27].

Consequently, we state that analyzing the security of a distance bounding protocol requires to consider exactly 4 cases: cheat fraud in the black-box model, cheat fraud in the white-box model, terrorist fraud in the white-box model, and mafia fraud in the black-box model (or equivalently mafia fraud in the white-box model, or terrorist fraud in the black-box model).

Remark 9. Clearly defining the prover model is quite important in the cryptanalysis of the distance bounding protocols. This statement has never been done before, which led to incorrect security proof. Indeed, some articles implicitly consider the white-box model, but the prover is only offered to look at the execution of the algorithm, without being able to intervene in its execution. In such a case, the adversary is not optimal and the so-called best success probability is underestimated.

5 Munilla and Peinado's protocol

We study here a protocol with respect to our model. First, we present the protocol, then we apply our model and show that Munilla and Peinado do not consider the best adversary strategy in their success probability computations.

5.1 Protocol description

In order to decrease the adversary success probability in Hancke and Kuhn's protocol, Munilla and Peinado introduce the concept of void challenges in [33,34]. The basic idea is that challenges can be 0, 1, or *void* meaning in such a case that no challenge is sent. Prover and verifier agree on which challenges should be void. Upon reception of 0 or 1 while a void challenge was expected, the prover detects the attack and gives up the protocol. The prover (P) and the verifier (V) share a secret k and agree on (a) a security parameter n, (b) a public pseudo random function f whose output size is $4n$ bits, and (c) a given timing bound $\Delta t_{\max}$.

Slow phase 1– V and P exchange nonces N_V and N_P. From these values, they compute $H = f(k, N_P, N_V)$. $2n$ bits are used to generate a n-bit register T as follows: if $H_{2i-1}H_{2i} =$ 00, 01, or 10 then $T_i = 1$, otherwise $T_i = 0$. The $2n$ remaining bits are used to generate the two registers $H^0 = H_{2n+1} \dots H_{3n}$ and $H^1 = H_{3n+1} \dots H_{4n}$ as done by Hancke and Kuhn.

Fast phase – Each T_i decides whether c_i is a void challenge ($T_i = 0$) or not ($T_i = 1$). In the latter case, c_i will be either 0 or 1, and will be called a *full* challenge. If a full challenge is received and $T_i = 1$, the prover answers $r_i = H_i^{c_i}$ as in Hancke and Kuhn. If a void challenge is received and $T_i = 0$, the prover stays silent. Otherwise, the prover detects an attack and aborts the protocol.

Slow phase 2– Upon termination of the fast phase, the prover sends $f(k, H^0, H^1)$ to the verifier, if he did not detect any attack during the fast phase execution. The verifier checks that the received value is correct, meaning that the prover did not detect any attack. The verifier finally checks the RTTs and the r_is as it is done in Hancke and Kuhn's protocol.

5.2 Computation of the Adversary Mafia Fraud Success Probability

According to [34], the adversary mafia fraud probability is $\left(\frac{9}{16}\right)^n$. We analyze below Munilla and Peinado's protocol according to our formalism and prove that the adversary success probability is actually higher. We remind that the choice of the black-box or white-box model is not relevant when considering the mafia fraud, as stated in Section 4.4.

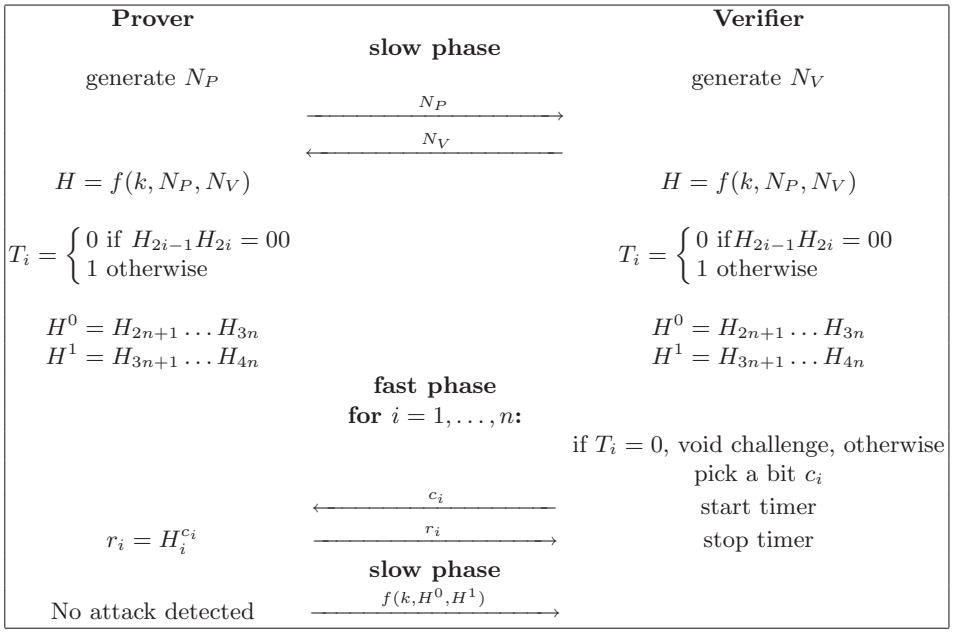

Fig. 3. Munilla and Peinado's protocol

No-ask strategy – The adversary has to successfully answer to the challenges during the fast phase and to guess the final signature. Two cases should be considered for analyzing the fast phase: (a) When a challenge is void, the adversary definitely knows that the right answer is also void. (b) When a challenge is full, the adversary replies with an arbitrary answer. Denoting $p(i)$ the probability that exactly i challenges are full during the fast phase, we compute the success probability of the adversary w.r.t. the fast phase:

$$\sum_{i=0}^{i=n} p(i) \cdot \left(\frac{1}{2}\right)^i. \tag{1}$$

In what follows we denote p_f the probability that a full challenge is expected by the prover and the verifier, then we have:

$$p(i) = \binom{n}{i} \cdot p_f^i \cdot (1 - p_f)^{n-i}. \tag{2}$$

Let p_{sign} be the probability that the adversary successfully forges the signature. Equations 1 and 2 yield:

$$P_{\text{no-ask}} = \left(1 - \frac{p_f}{2}\right)^n \cdot p_{\text{sign}}.$$

Note that depending on the function f, obtaining the optimal p_{sign} can be reached by randomly guessing the signature or by randomly picking k, H^0, H^1 and computing the right signature from them.

Post-ask strategy – The adversary does not intervene during the first slow phase between the verifier and the prover. Then she executes the fast phase herself with the verifier, trying to guess the right answers and learning the registers T. Afterward, she executes the fast phase with the prover, transmitting the verifier received challenges. As she sends to the prover the void and full challenge at correct moment, she is not detected by the prover. Hence she receives the signature from the prover and sends it to the verifier during the final slow phase. The adversary succeeds

with the same probability as in the no-ask strategy except that she does not have to deceive on the signature. Her success probability is therefore:

$$P_{\text{post-ask}} = \left(1 - \frac{p_f}{2}\right)^n.$$

Pre-ask strategy – In the original paper [34], the authors consider a pre-ask strategy in which the attacker can not send void challenges to the prover. With this assumption, they obtain the following success probability:

$$P_{\text{pre-ask}} = \left(\frac{3}{4} \cdot p_f\right)^n.$$

We prove below that in [34], Munilla and Peinado do not compute the adversary success probability for the pre-ask strategy with the best attack. We state that an attacker with the capability of sending void challenge can increase its success probability.

First, we remark that the adversary succeeds if at each rounds (a) she is not detected by the prover, i.e she sends a void challenge when a void challenge is expected (probability $p_{\text{not detected}}$), and (b) she gives the correct answer to the verifier (probability $p_{\text{good answer}}$).

The attacker is not detected by the prover if she sends a void challenge when $T_i = 0$, and she sends a full challenge when $T_i = 1$. So this probability is equal to:

$$p_{\text{not detected}} = p_c \cdot p_f + (1 - p_c) \cdot (1 - p_f),$$

where p_c is the probability that the attacker sends a full challenge.

When the prover is queried by the attacker, the latter can obtain the value H_i^0 corresponding to the ith full challenge. When the verifier sends a challenge to the attacker the following situations occurs:

- the challenge is a void challenge, and the attacker knows the answer,
- the response expected is from register H^0, she knows the answer,
- the response expected is from register H^1, she guesses randomly the answer.

Hence:

$$p_{\text{good answer}} = (1 - p_f) \cdot 1 + \frac{3}{4} \cdot p_f \cdot p_c.$$

Finally, the adversary success probability of the pre-ask strategy is equal to

$$\begin{aligned} P_{\text{pre-ask}} &= \left((p_c \cdot p_f + (1 - p_c) \cdot (1 - p_f)) \cdot \left((1 - p_f) + \frac{3}{4} \cdot p_f \cdot p_c\right)\right)^n \\ &= \left(1 - 2p_f - p_c + p_f^2 + \frac{15}{4} p_c p_f - \frac{11}{4} p_c p_f^2 - \frac{3}{4} p_c^2 p_f + \frac{6}{4} p_c^2 p_f^2\right)^n. \end{aligned}$$

The authors proposed to take $p_f = \frac{3}{4}$. With this value, we have:

$$P_{\text{pre-ask}} = \left(\frac{1}{16} + \frac{17}{64} p_c + \frac{9}{32} p_c^2\right)^n.$$

At last, with $p_c = 1$, we find that

$$P_{\text{pre-ask}} = \left(\frac{39}{64}\right)^n.$$

Munilla and Peinado claimed that the pre-ask strategy succeeds with probability $\left(\frac{9}{16}\right)^n$ which lower than our attack probability.

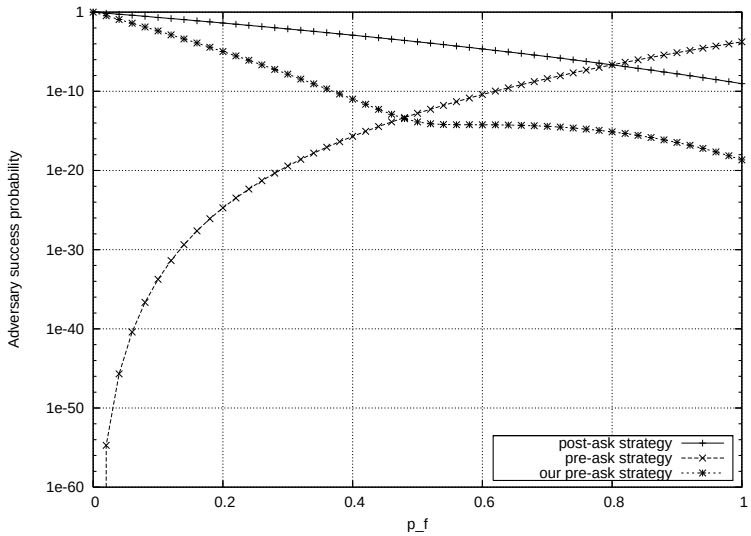

Fig. 4. $p_{\text{pre-ask}} - p_{\text{post-ask}}$ depending on p_c for given p_c

Comparison between the strategies – We now compare the different adversary strategies. Clearly, the adversary does not take any advantage to use the no-ask strategy. The Figure 4 depicts the behavior of $p_{\text{pre-ask}} - p_{\text{post-ask}}$ depending on p_c for a given p_f

We can observe that the adversary increases her success probability by using the pre-ask strategy if $p_f \geq 0,77$. Otherwise, the adversary uses the post-ask strategy. Hence, we summarize these observations:

$$P_{\text{adv}} = \begin{cases} p_{\text{post-ask}} \text{ if } p_f < 0,77 \\ p_{\text{pre-ask}} \text{ if } p_f \geq 0,77 \end{cases}$$

6 Singelée and Preneel's protocol

Capkun *et al.* have modified in [8] the Brands and Chaum's protocol to obtain a mutual authenticated distance bounding protocol (MAD). In their seminal works, Hancke and Khun [19] have emphasized the issue of noise during the fast phase. Singelée and Preneel suggest in [40] to use linear codes to obtain a noise resilient MAD. The verifier and the prover share a secret k, and agree on (a) a (n, p) error correcting code (ECC) with minimal Hamming distance d_{min} such that $x = \frac{d_{min}-1}{2}$ and x is the error correction capability of the code, (b) a commitment scheme. The authors have proposed to use random linear codes or non-linear codes for the ECC.

6.1 Protocol description

Slow phase 1– The prover and the verifier both generate p bits at random, respectively $s = (s_1, \cdots, s_p)$ and $r = (r_1, \cdots, r_p)$. Then, they both apply a coding algorithm to obtain respectively $(s_1, \cdots, s_n)$ and $(r_1, \cdots, r_n)$. Afterwards they commit to each other the n bits obtained.

Fast phase – The fast phase begins, and the verifier sends $\alpha_1 = r_1$, the prover answers $\beta_1 = r_1 \oplus s_1$. For $i = 2, \ldots, n-1$, the verifier sends $\alpha_i = \beta_{i-1} \oplus r_i$, the prover answers $\beta_i = \alpha_i \oplus s_i$. At the final rounds, the verifier sends $\alpha_n = \beta_{n-1} \oplus r_n$, and prover's response is $\beta_n = \alpha_n \oplus s_n$.

Slow phase 2– Then, the verifier computes $s'_i = \alpha_i \oplus \beta_i$, the prover computes $r'_1 = \alpha_1$, and $r'_i = \beta_i \oplus \alpha_i$. Both of them use the ECC on the n bits computed before. They obtained the p first bits generated by the other. The verifier computes $m_V = \text{sign}_k(s' \parallel r)$. The prover computes $m_P = \text{sign}_k(r' \parallel s)$. Then, they open the commit to each other, and exchange the signed messages. The signatures m_P and m_V are correct if and only if $s' = s$ and $r' = r$. This protocol is depicted in figure 5.

Verification. The verification phase is done as in Brands and Chaum, except that, to provide mutual authentication, both of the prover and the verifier realize this stage.

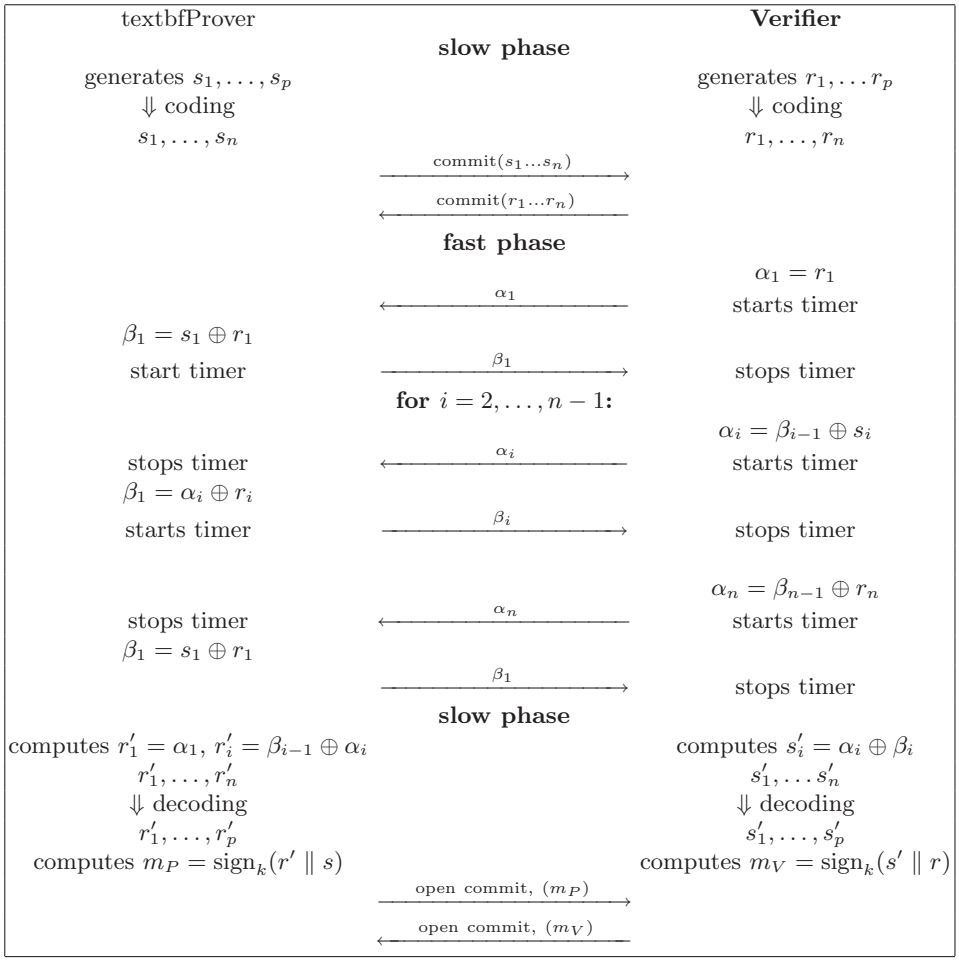

Fig. 5. Singelée and Preneel's protocol

6.2 Computation of the adversary success probability

In the following, it assumed that the adversary has a complete control on the environment between the prover and her and between the reader and her. Indeed, the attacker can afford to use dedicated hardware and antenna to set up communication channels without noise.

No-ask strategy – The adversary has only to forge a valid signature. The success probability for this attack is simply:

$$P_{\text{no-ask}} = p_{sign}.$$

Post-ask strategy – The attacker does not know the value generated by the prover in the first slow phase. She has to guess the answers to the challenges. First, it can be considered that the last $(n-p)$ bits of the message do not offer extra security. The attacker need only to guess the first p bits. This case was described in [40]. Its success probability is:

$$P_{\text{post-ask}} = \left(\frac{1}{2}\right)^p \text{ as in [40].}$$

It is also possible for the attacker to answer s'_i to the challenge r_i such that $d_{\mathcal{H}}(s, s') \leq x$ where $s = (s_1, s_2, \cdots, s_n)$ is the prover responses, $s' = (s'_1, s'_2, \cdots, s'_n)$ is the attacker responses and $d_{\mathcal{H}}$ is the Hamming distance. In this case, the success probability is:

$$P_{\text{post-ask}} = \frac{\sum_{i=0}^{x} \binom{n}{i}}{2^n}.$$

This mode of operation improves the post-ask strategy of Singelée and Preneel if and only if $\frac{\sum_{i=0}^{x} \binom{n}{i}}{2^{n-k}} > 1$.

Table 1. Comparison of the different pre-ask strategies with the parameters given in [40]. The minimal distance of the code considered in this table is the best maximum possible minimum distance of a linear code (computed with MAGMA and based on Brouwer's tables).

# allowed errors (x)	(n,p) ECC	$\left(\frac{1}{2}\right)^p$ [40]	$\frac{\sum_{i=0}^{x} \binom{n}{i}}{2^n}$	$\frac{\sum_{i=0}^{x} \binom{2n}{i}}{2^{2n}}$
4	(37,21)	$4,76 \cdot 10^{-7}$	$5,42 \cdot 10^{-7}$	$6,45 \cdot 10^{-17}$
3	(37,25)	$2,98 \cdot 10^{-8}$	$6,16 \cdot 10^{-8}$	$3,58 \cdot 10^{-18}$
2	(37,30)	$9,31 \cdot 10^{-10}$	$5,12 \cdot 10^{-9}$	$1,47 \cdot 10^{-19}$
1	(37,36)	$1,45 \cdot 10^{-11}$	$2,76 \cdot 10^{-10}$	$3,97 \cdot 10^{-21}$
13	(63,12)	$0,000244$	$3,73 \cdot 10^{-7}$	$2,55 \cdot 10^{-22}$
10	(63,18)	$3,81 \cdot 10^{-6}$	$1,69 \cdot 10^{-8}$	$2.47 \cdot 10^{-23}$
3	(63,50)	$8,88 \cdot 10^{-16}$	$4,52 \cdot 10^{-15}$	$3,92 \cdot 10^{-33}$
2	(63,56)	$1,38 \cdot 10^{-17}$	$2,19 \cdot 10^{-16}$	$9,41 \cdot 10^{-35}$
1	(63,61)	$4,33 \cdot 10^{-19}$	$6,94 \cdot 10^{-18}$	$1,49 \cdot 10^{-36}$

Pre-ask strategy – In the pre-ask strategy, the adversary can make x errors on $2n$ bits (challenge + response). The success probability is given by:

$$P_{\text{pre-ask}} = \frac{\sum_{i=0}^{x} \binom{2n}{i}}{2^{2n}}.$$

The adversary can still attempt to make only x errors on the n bits of challenges sent to the prover. In this case, she has the same success probability than in the post-ask strategy. The comparison of those different probabilities is given in Table 1.

7 Conclusion

Since there has been no formal method for previously proposed distance bounding protocols, they were usually designed and analyzed with a pedestrian approach. In addition, there was no agreement on most of the definitions for attack scenarios and entity models. To fulfill this need, we come up with a formal framework for the analysis of distance bounding protocols. The fair evaluations provided by our formalism can be used while designing or cryptanalyzing distance bounding protocols.

In this paper, we first formalized a general threat model in which the attack scenarios, protocol aims and the adversary goals are clearly described. By doing this, some ambiguity in the previous works was clarified. After that, the relevance of the attack scenarios and the protocol aims with respect to adversary goals is explored. As a practical illustration, we refined our formalism for the RFID environments. In the refinement, the methods for evaluating the distance checking and general sketch of distance-bounding authentication protocols based on RTT are explained. In addition, we also defined an additional adversary strategy (post-ask) for mafia and terrorist frauds. By help of this strategy, we found that the success probability of mafia fraud in [33, 34] is actually higher than the computed probability.

References

1. Gildas Avoine and Aslan Tchamkerten. An Efficient Distance Bounding RFID Authentication Protocol: Balancing False-acceptance Rate and Memory Requirement. In *Information Security Conference – ISC'09*, volume 5735 of *Lecture Notes in Computer Science*, Pisa, Italy, September 2009.
2. Samy Bengio, Gilles Brassard, Yvo Desmedt, Claude Goutier, and Jean-Jacques Quisquater. Secure implementation of identification systems. *Journal of Cryptology*, 4(3):175–183, 1991.
3. Thomas Beth and Yvo Desmedt. Identification tokens - or: Solving the chess grandmaster problem. In *CRYPTO*, pages 169–177. Springer Verlag, 1990.
4. Matt Blaze. Looking on the Bright Side of Black-Box Cryptography (Transcript of Discussion). In *Security Protocols Workshop*, Lecture Notes in Computer Science 2133, pages 54–61. Springer Verlag, 2000.
5. Stefan Brands and David 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.
6. Laurent Bussard and Walid Bagga. Distance-bounding proof of knowledge to avoid real-time attacks. In Sasaki Ryoichi, Qing Sihan, and Okamoto 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.
7. Laurent Bussard and Yves Roudier. Embedding distance-bounding protocols within intuitive interactions. In Dieter Hutter, Günter Müller, Werner Stephan, and Markus Ullmann, editors, *Security in Pervasive Computing – SPC*, volume 2802 of *Lecture Notes in Computer Science*, pages 119–142, Boppard, Germany, March 2003. Springer-Verlag.
8. Srdjan Capkun, Levente Butty'an, and Jean-Pierre Hubaux. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In *ACM Workshop on Security of Ad Hoc and Sensor Networks – SASN'03*, pages 21–32. ACM, 2003.
9. Srdjan Capkun and Jean-Pierre Hubaux. Secure positioning of wireless devices with application to sensor networks. In *INFOCOM 2005*, pages 1917–1928. IEEE, 2005.
10. Master Card. Mastercard paypass. http://www.mastercard.com/, 2009.
11. Stanley Chow, Philip A. Eisen, Harold Johnson, and Paul C. van Oorschot. White-Box Cryptography and an AES Implementation. In *Selected Areas in Cryptography - SAC 2002*, Lecture Notes in Computer Science 2595, pages 250–270. Springer Verlag, 2002.
12. Yvo Desmedt, Claude Goutier, and Samy Bengio. Special uses and abuses of the fiat-shamir passport protocol. In Carl 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.
13. Saar Drimer and Steven J. Murdoch. Keep your enemies close: distance bounding against smartcard relay attacks. In *16th USENIX Security Symposium on USENIX Security Symposium*, pages 1–16. USENIX Association, 2007.
14. Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew Odlyzko, editor, *Advances in Cryptology – CRYPTO'86*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194, Santa Barbara, California, USA, August 1986. IACR, Springer-Verlag.
15. Near Field Communication Forum. Website. http://www.nfc-forum.org/, 2009.
16. James Gleick. A new approach to protecting secrets is discovered. *The New York Times*, February, 17th 1987.
17. Martin Halváč and Tomáč Rosa. A Note on the Relay Attacks on e-Passports: The Case of Czech e-Passports. Cryptology ePrint Archive, Report 2007/244, 2007.
18. Gerhard Hancke. A Practical Relay Attack on ISO 14443 Proximity Cards. Manuscript, February 2005.
19. Gerhard Hancke and Markus Kuhn. An RFID Distance Bounding Protocol. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, Athens, Greece, September 2005.

20. Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Confidence in Smart Token Proximity: Relay Attacks Revisited. In *Elsevier Computers & Security*, June 2009.
21. Gerhard P. Hancke. Practical Attacks on Proximity Identification Systems. In *IEEE Symposium on Security and Privacy - S&P 2006*, pages 328–333. IEEE Computer Society, 2006.
22. Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. In *INFOCOM*, 2003.
23. Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):370–380, 2006.
24. ISO/IEC 14443. Identification cards – contactless integrated circuit(s) cards – proximity cards.
25. Ziv Kfir and Avishai Wool. Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard Systems. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, Athens, Greece, September 2005. IEEE.
26. Chong Hee Kim and Gildas Avoine. RFID distance bounding protocol with mixed challenges to prevent relay attacks. In *International Conference on Cryptology and Network Security – CANS*, Lecture Notes in Computer Science, Kanazawa, Ishikawa, Japan, December 2009. Springer-Verlag.
27. Chong Hee Kim, Gildas Avoine, François Koeune, François-Xavier Standaert, and Olivier 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.
28. Adam Laurie. Website. http://www.rfidiot.org/, 2009.
29. Albert Levi, Erhan Çetintas, Murat Aydos, and Çetin Kaya Koçand M. Ufuk Çaglayan. Relay Attacks on Bluetooth Authentication and Solutions. In *International Symposium Computer and Information Sciences - ISCIS 2004*, Lecture Notes in Computer Science 3280, pages 278–288. Springer Verlag, 2004.
30. Catherine Meadows, Radha Poovendran, Dusko Pavlovic, LiWu Chang, and Paul Syverson. *Distance Bounding Protocols: Authentication Logic Analysis and Collusion Attacks*, volume 30 of *Advances in Information Security series, Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks*, chapter 2, pages 279–298. Springer-Verlag, 2007.
31. Alfred Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
32. Elke De Mulder, Wim Aerts, Bart Preneel, Guy Vandenbosch, and Ingrid Verbauwhede. A class E Power Amplifier for ISO-14443A. In *12th IEEE Workshop on Design and Diagnostics of Electronic Circuits & Systems (DDECS 2009)*, pages 20–23. IEEE, 2009.
33. Jorge Munilla, Andres Ortiz, and Alberto Peinado. Distance Bounding Protocols with Void-Challenges for RFID. In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006.
34. Jorge Munilla and Alberto 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.
35. Ventzislav Nikov and Marc Vauclair. Yet Another Secure Distance-Bounding Protocol. Cryptology ePrint Archive, Report 2008/319, 2008.
36. Yossef Oren and Avishai Wool. Relay Attacks on RFID-Based Electronic Voting Systems. Cryptology ePrint Archive, Report 2009/442, 2009. http://eprint.iacr.org/.
37. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, and Jan C. A. van der Lubbe. Shedding Some Light on RFID Distance Bounding Protocols and Terrorist Attacks. arXiv.org, Computer Science, Cryptography and Security, 2009.
38. Jason Reid, Juan Gonzalez Neito, Tee Tang, and Bouchra Senadji. Detecting relay attacks with timing based protocols. In Feng Bao and Steven 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.
39. Amitabh Saxena, Brecht Wyseur, and Bart Preneel. Towards Security Notions for White-Box Cryptography. In *Information Security Conference- ISC 2009*, Lecture Notes in Computer Science 5735, pages 49–58. Springer Verlag, 2009.
40. Dave Singelée and Bart Preneel. Distance Bounding in Noisy Environments. In *European Workshop on Security in Ad-hoc and Sensor Networks – ESAS'07*, volume 4572 of *Lecture Notes in Computer Science*, pages 101–115, Cambridge, UK, 2007.
41. Yu-Ju Tu and Selwyn Piramuthu. RFID Distance Bounding Protocols. In *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.
42. Visa. Visa conctless credit card. http://usa.visa.com/personal/cards/paywave/index.html, 2009.
43. Adam Young and Moti Yung. The Dark Side of "Black-Box" Cryptography, or: Should We Trust Capstone? In *Advances in Cryptology - CRYPTO '96*, Lecture Notes in Computer Science 1109, pages 89–103. Springer Verlag, 1996.