A Framework for Analyzing RFID Distance Bounding Protocols

Gildas Avoine[1] Muhammed Ali Bingöl[2,3] Süleyman Kardaş[2,4]
Cédric Lauradoux[5] Benjamin Martin[1]

[1]Université catholique de Louvain, Louvain-la-Neuve, Belgium
[2]TUBITAK UEKAE, Gebze, Kocaeli, Turkey
[3] Istanbul Technical University, Institute of Science and Technology, Istanbul, Turkey
[4] Sabanci University, Istanbul, TR-34956, Turkey
[5]Université de Lyon, INRIA, INSA-Lyon, CITI, F-69621, France

Abstract

Many distance bounding protocols appropriate for the RFID technology have been proposed recently. Unfortunately, they are commonly designed without any formal approach, which leads to inaccurate analyzes and unfair comparisons. Motivated by this need, we introduce a unified framework that aims to improve analysis and design of distance bounding protocols. Our framework includes a thorough terminology about the frauds, adversary, and prover, thus disambiguating many misleading terms. It also explores the adversary's capabilities and strategies, and addresses the impact of the prover's ability to tamper with his device. It thus introduces some new concepts in the distance bounding domain as the black-box and white-box models, and the relation between the frauds with respect to these models. The relevancy and impact of the framework is finally demonstrated on a study case: Munilla-Peinado distance bounding protocol.

1 Introduction

Desmedt *et al.* presented at Crypto'87 a new attack called the *mafia fraud* [19] that defeats any authentication protocol. Based on the *chess grandmaster problem* [17], this attack allows the adversary to successfully pass the authentication by relaying the messages between a verifier and a legitimate prover. When it was introduced, the mafia fraud appeared somehow unrealistic because the legitimate prover is required to be involved in the execution of the protocol without being aware of the manoeuvre.

Mafia fraud in RFID. The mafia fraud has been recently resurrected with the deployment of ubiquitous computing systems, especially those based on passive RFID. Whatever the capabilities of RFID tags, from a simple memory to a powerful contactless smartcard, they all share the particularity that they answer to the reader's requests without any agreement or awareness of their holder. This clearly opens the door to mafia frauds.

To illustrate this concern, consider a payment system based on contactless credit cards [15, 59]. 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 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 accomplice can be set up, for example, using mobile phones. One may argue that the merchant will detect the attack. However, some payment systems are based on the NFC-friendly cell-phones and this still facilitates the masquerade because the merchant is not able to see that the cell-phone performs a mafia fraud.

Feasibility of the mafia fraud. 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. Therefore, the attack can be performed even if the adversary has no clue about what is exchanged in the application layer. In 2005, Hancke [28] demonstrated a mafia fraud which can be performed while the two colluders are 50 meters apart and connected through a radio-channel. This is long enough to perform the attack in a waiting line in front of a ticket machine. This attack was applied to RFID but the authors in [24,25,29,37,42] point out that some other domains are targeted by the mafia fraud. Recently, Adam Laurie published on Internet some tool to carry out a mafia fraud with off-the-self RFID devices [41]. This work puts the mafia fraud accessible to everyone.

In 2007, Halváč and Rosa [27] noticed that the standard ISO 14443 [34] widely deployed in secure applications can easily be abused by a mafia fraud due to the lax timeouts in the communication. Indeed, the standard ISO 14443 specifies a *frame waiting time* (FWT) in which 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 a timeout is long-enough to carry out a mafia fraud over thousands kilometers.

Distance bounding protocols. The first countermeasure against mafia fraud, called *distance bounding protocol*, was suggested by Desmedt *et al.* [7, 8] by introducing the distance bounding concept based on the measurement of the round trip time of exchanged messages. Brands and Chaum [10] then designed the first *distance bounding protocol* based on the ideas of Desmedt *et al.* in order to mitigate or thwart the relay attacks.

Since then, many works about distance bounding have been published [6, 10–14, 21, 30, 35, 38,39,43,45–47,52,54,55,57,58,60], 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., [19]) is also known as a relay attack (e.g., [6, 27, 28, 31, 37, 38, 49, 52]), a chess grandmaster problem (e.g, [8, 17]), or a wormhole problem (e.g., [32, 33]). The distance fraud (e.g., [38, 46, 50]) is also considered as a relay attack while there is here no relay. Also, some papers consider the prover has a full access to its internal state (e.g., [7]) while he can only observe it in some other papers (e.g., [45]).

Contribution. Given the current state of the art, comparing the existing protocols is an unfair and challenging task, due to the lack of formalism. While distance bounding protocols are on our doorstep [48, 51], the goal of this paper is to fill this gap.

Section 2 provides a thorough analysis of the terminology that is used or should be used in the distance bounding domain. This work does not simply consist in collecting definitions from the literature. Indeed, it distinguishes the historical terminology used in the distance bounding domain from the one used nowadays in most of the publications. This allows to provide new and – hopefully – unambiguous definitions, and to classify the three generic frauds considered in recent works: mafia, terrorist, and distance frauds.

Section 3 defines a generic model for the adversary. This model is fundamental to assess the security of distance bounding protocols. We particularly explore the adversary capabilities and strategies. We emphasize that our aim is to supply a generic model but, nevertheless precise enough to be useful in the protocol analysis. For example, we derive from our model several adversary strategies that should be considered when analyzing a distance bounding protocol, but we do not claim that these strategies are the only possible ones. They somehow define the minimum requirements one may expect from a distance bounding protocol.

Section 4 introduces a new view on the prover compared to previous works. We consider the black-box and white-box models and show the relations between the mafia, terrorist, and distance frauds with respect to these models. We show that some equivalences exist between these frauds. This reduces the number of cases to deal with when analyzing a distance bounding protocol. This new approach also points out that some previous works underestimate the success probability of the adversary, and emphasizes the need of a clear definition of the adversary capabilities when designing a new protocol.

Finally, Section 5 is a study case of an interesting protocol proposed by Munilla and Peinado [46]. We underline that our aim is not to exhibit weaknesses in this protocol, but to illustrate how our framework allows to refine the security analysis.

2 Towards some Unified Concepts for RFID

In what follows, we consider a two-party communication protocol. First, we define the man-in-the-middle attack and the relay attack. Then, the concept of distance bounding is introduced.

2.1 Man-in-the-Middle Attacks

Definition 1 (Man-In-The-Middle Attack)**.** *A man-in-the-middle (MITM) is a form of attack, where the adversary provokes or manipulates the communication between two parties. Manipulating the communication means relay, withhold, or insert messages.*

Remark 1. In RFID, a MITM practically consists in a rogue reader and a rogue tag each located close to a party and connected through a communication link.

Some early papers also consider a weaker form of adversary who is not able to withhold or insert a message. We then speak about *relay attacks.*

Definition 2 (Relay Attack)**.** *A relay attack is a form of man-in-the-middle where the adversary manipulates the communication by only relaying the verbatim messages between two parties.*

Remark 2. Typically, a relay attack can be mounted by an adversary who does not know the protocol used by the parties. This case is realistic in practice and appears in RFID when the communication protocols do not follow any open standard.

2.2 From Authentication to Distance Bounding

As a prelude to distance bounding, we consider two classes of protocols that are *authentication* and *distance checking*, both strongly related to our problem. Authentication is a well-known concept already defined in many classical textbooks, and Definition 3 is excerpted from [44].

Definition 3 (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).*

In the same vein, we define *distance checking.*

Definition 4 (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 3*.* Definition 4 does not suggest any *distance property.* Given that we target RFID, the *Euclidean* distance[1] is the most meaningful and used in the literature [6, 10–12, 21, 30, 38, 39, 43, 45–47, 52, 54, 57, 58]. 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. Some other works consider different distances, for example distance checking protocols to counter wormholes in wireless networks [13, 14, 32, 33].

Remark 4*.* In an authentication protocol, an attack succeeds if an adversary impersonates a legitimate user. In the same way, an attack against a distance checking protocol succeeds if she makes the verifier believe that she satisfies the distance property while she does not.

Most of the security-related RFID applications require both authentication and distance checking, which leads to the concept of *distance bounding.*

Definition 5 (Distance Bounding)**.** *A distance bounding is a process that combines both authentication and distance-checking. Moreover, the property that is verified in the distance checking is an upper bound on the distance between the two parties.*

Remark 5*.* We say that a distance bounding protocol is *sound* if the verifier rejects with overwhelming probability when the prover is not legitimate and/or is outside of the neighborhood, and *correct* if, when no attack occurs, the verifier accepts with overwhelming probability when the legitimate prover is within the neighborhood.

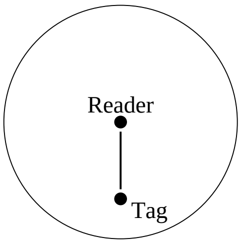

Figure 1: Tag in the neighborhood of a reader.

2.3 Distance Bounding Mitigates MITM Attacks

Distance bounding protocols can be used in such environments to protect either the prover, *i.e.*, the tag, or the verifier, *i.e.*, the reader. Indeed, a tag should not be authenticated without explicit agreement of its holder. Since such an explicit agreement is not available in (low-cost) RFID. Therefore, the presence of the tag in the neighborhood of the reader (Figure 1) is an implicit agreement of authentication. On the other side, the reader may require the presence of the tag during the authentication especially when considering physical access control.

However, Remark 5 is particularly important to understand the goals and the limitations of the RFID distance bounding. Indeed, such a protocol ensures that a given tag is within the environment of the reader, but cannot conclude anything about the fact that a MITM

[1] In such a case, *distance ranging* is also used as synonym of *distance checking.*

occurs between the two parties. In other words, a distance bounding protocol is not expected to distinguish the scenario represented in Figure 1 and those represented in Figure 2 and Figure 3.

Although distance bounding does not avoid any MITM in theory, it can be used to mitigate them in practice when the neighborhood of an RFID reader is small enough that any attack within this zone is detectable. Note that distance bounding protocols may so not be suitable for RFID systems with long-range reading. As an illustration, one may cite the Identify Friend or Foe (IFF) [3, 22] system: an enemy aircraft approaching its target may defeat a detection radar by impersonating a friend aircraft if such one is present within the detection zone.

2.4 Frauds on Distance Bounding

In what follows, we assume that the RFID reader is honest that is it properly follows the definition of the protocol. As commonly admitted, we assume that no two competing attacks occurs during a same instance of the protocol. We define four types of fraud that are illustrated in Figure 4, Figure 5, and Figure 6.

Definition 6 (Impersonation Fraud)**.** *Given a distance bounding protocol, an impersonation fraud is an attack where a lonely prover purports to be another one.*

Definition 7 (Distance Fraud)**.** *Given a distance bounding protocol, a distance fraud is an attack where a dishonest and lonely prover purports to be in the neighborhood of the verifier.*

Example 1. Home confinement is a legal measure by which a person is confined by the authorities to his residence, when prison is not an appropriate measure. Electronic monitoring was originally

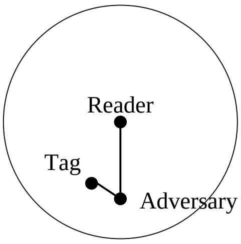

Figure 2: MITM with an inside adversary.

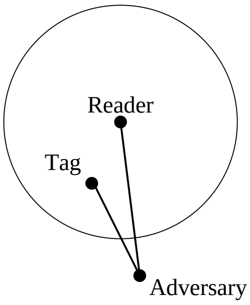

Figure 3: MITM with an outside adversary.

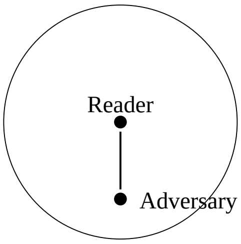

Figure 4: Impersonation Fraud.

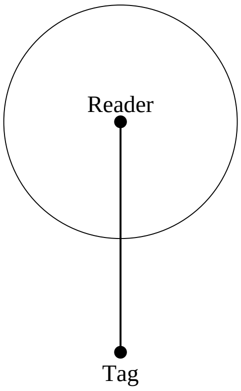

Figure 5: Distance Fraud.

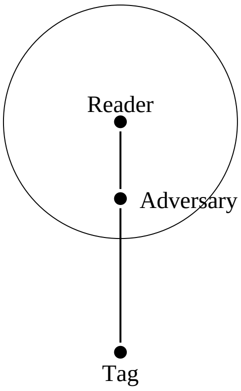

Figure 6: Mafia/Terrorist Frauds.

developed at Harvard in the 1960s, and the first judicially sanctioned program using monitoring devices was launched in 1983 in New Mexico [40]. People as (in)famous as Bernard Madoff and Paris Hilton already benefited from such an electronic monitoring using an ankle bracelet. With such a measure where travels are restricted, a distance attack is definitely relevant, in order to allow the person under monitoring to leave his residence without being detected.

Definition 8 (Mafia Fraud)**.** *A mafia fraud is an attack where an adversary defeats a distance bounding protocol using a man-in-the-middle (MITM) between the reader and an honest tag located outside the neighborhood.*

Example 2*.* Consider a payment system based on contactless credit cards, for example [15, 59]. 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.

Definition 9 (Terrorist Fraud)**.** *A terrorist fraud is an attack where an adversary defeats a distance bounding protocol using a man-in-the-middle (MITM) between the reader and a dishonest tag located outside of the neighborhood, such that the latter actively helps the adversary to maximize her attack success probability, without giving to her any advantage for future attacks.*

Example 3*.* The terrorist attack also makes sense in the case of home confinement because the arrested person may benefit from the help of an accomplice who stays close to the monitoring system while the person under control is away. In such a case, a terrorist fraud is needed because the ankle bracelet cannot be physically removed except by the authorities.

Following the four frauds described above, one may observe that three degenerated cases could also be considered: impersonation, mafia, and terrorist frauds when the adversary is outside the neighborhood. These frauds, depicted in Figure 7 and Figure 8, are not considered because they are weaker than the general corresponding frauds. Note that degenerated distance fraud is neither addressed because self-impersonation does not make sense.

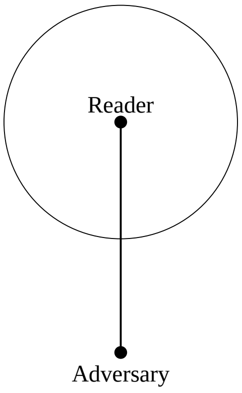

Figure 7: Degenerated Impersonation.

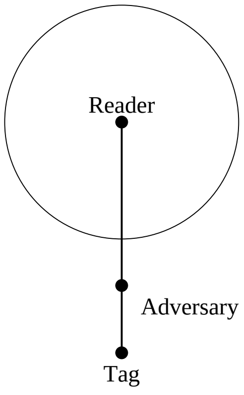

Figure 8: Degenerated Mafia / Terrorist Frauds.

2.5 Terminology

In 1976, Conway [17] introduced the chess grandmaster problem where a little girl - who does not know how to play chess - plays in parallel two correspondence games against two chess grandmasters. By only relaying the moves of the grandmasters, she eventually draws or wins against one of them. Based on the chess postal problem, mafia and terrorist frauds have been both originally proposed by Desmedt, Goutier, and Bengio at Crypto 87 [19], then extended with Brassard and Quisquater in [7]. Their goal was to prove that the Fiat-Shamir zero-knowledge protocol [23] 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 [26]. Hence, mafia and terrorist frauds are also meaningful outside of the scope of distance bounding.

Beth and Desmedt [8] introduced the distance bounding as a countermeasure to these frauds, not as a primary goal. Brands and Chaum [10] then designed the first distance bounding protocol based on the ideas of Desmedt *et al.*. Up to our knowledge, the first distance bounding protocol devoted to RFID is due to Hancke and Kuhn [30].

Since then, most of the works about distance bounding [6, 10–14, 21, 30, 35, 38, 39, 43, 45–47, 52, 54, 55, 57, 58, 60] are related to physical devices and consider mafia and terrorist frauds as defined in this paper, not in the original broad sense.

Note that although many papers about RFID consider mafia and terrorist frauds as relay attacks, we emphasize that they are MITM attacks but not necessarily relay attacks. In the general literature, *mafia fraud* is synonym of *chess grandmaster* attack [1, 8] and *middleman* attack [4, 18]. In RFID, *mafia fraud* is the terminology that should be used.

Also, *distance bounding* [6, 10–14, 21, 30, 35, 38, 39, 43, 45–47, 52, 54, 55, 57, 58, 60] is synonym of *proximity check* in the RFID literature.

3 Adversary Capabilities and Strategies

Below, we introduce the round trip time (RTT) that is the keystone of distance bounding. We then provide a model for the adversary capabilities. Regarding the frauds define in Section 2, the adversary might be a third party or the prover himself. Finally, we present some strategies to counteract the distance bounding protocol.

3.1 Distance Bounding Protocols Based on the Round Trip Time

There exists several solutions to estimate the distance between two devices. For instance, one can measure the received signal strength indication (RSSI) [62], use the global positioning system (GPS) [60] or perform multi-channels communication [2, 56]. These methods are either insecure, e.g., the RSSI can be modified by the adversary and can be fluctuating (indoor/outdoor), or unsuitable to the RFID constraints: a GPS receiver is too expensive to be added to a low-cost RFID and the physical layer is too simple to allow multi-channels communication.

All the papers on distance bounding in RFID [6, 10–14, 21, 30, 35, 38, 39, 43, 45–47, 52, 54, 55, 57, 58, 60] consider that the most promising solution to evaluate the distance between two parties consists in measuring the *Round Trip Time* (RTT). By measuring the RTT of a message, the sender can estimate an upper bound on its distance to the recipient, given that it cannot propagate faster than the light. This solution only requires a single trusted clock on the reader side and no hardware modification for the tag.

Among the existing distance bounding protocols based on RTT, one may distinguish two main families: characterized by the fact that a final signed message is or not required to end the protocol. The final signature can be computed on the challenges and the responses only, or on some other informations, e.g., the nonces. The first family has been introduced by Brands and Chaum [10]. Later on, Hancke and Kuhn [30] proposed a protocol in which there is no need of a final signature. The protocol execution finishes when the measurement of the RTTs is done. Both protocols can be implemented using symmetric-key cryptography.

Brands and Chaum's protocol consists of three phases: the first and final ones are denoted *slow phases*, and the second one is called *fast phase*. The RTT is measured n times during the fast phase, while the slow phases include all the time-consuming operations; in particular the final slow phase is used to complete the authentication. On the other side, Hancke and Kuhn's protocol consists of a single slow phase followed by a fast one with n RTTs measured. In this case, the fast phase allows the verifier to check both authentication and distance.

Most of existing works are based on either Hancke and Kuhn's family [6,30,38,47,52,57] or on Brands and Chaum's family [10,39,45,46,54]. The protocol proposed in [58] can be viewed as an "hybrid" protocol: there is a succession of slow phases and fast phases.

Remark 6. The authentication security parameters of Hancke and Kuhn's protocol and Brands and Chaum's protocol are not the same: in the early case the authentication security parameters are the key size, the nonce sizes and the number of fast phase rounds; in the latter case they are the nonce sizes, the key size and the signature size.

In the sequel, Hancke and Kuhn's protocol (HK) [30] is used to illustrate some concepts. The protocol can be briefly described as follows. The verifier sends a nonce N_v to the prover. The prover replies a nonce N_p. From those nonces, and a shared secret k, both prover and verifier compute $H = f(k, N_v, N_p)$ where f is a pseudorandom function. The value H is then split to obtain two n-bit registers R^0 and R^1. During the fast phase, the verifier picks a random bit c_i and sends it to the prover. The prover replies $R_i^{c_i}$ the i-th bit of the register R^{c_i}.

3.2 Adversary Capabilities

In this section, we define the generic capabilities of the adversary. Achieving a realistic and fair model requires bounds on these capabilities. Two different restrictions are provided below.

3.2.1 Dolev-Yao Model

We consider in our framework a Dolev-Yao adversary [20]. In such a model, the adversary cannot perform unbounded computations and cannot obtain the keys of honest parties. The latter assumption is nevertheless 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.

Designing a distance bounding protocol also requires to define two other bounds on both number of protocol runs executed by the third adversary, and number of cryptographic operations carried on by the tag within one execution. The former bound is discussed below while the latter bound is discussed in Section 4.

3.2.2 Bound on the Number of Protocol Executions

When executing several times the protocol from scratch does not give to the adversary any significant advantage, the security analysis can consider only one protocol execution. However, some protocols do not resist to multiple executions, for example the success probability of a mafia fraud with the original HK protocol [30][2] is $(\frac{3}{4})^n$ if only one execution is considered, while it is 1 when the adversary can run twice the protocol with the same challenge.

3.3 Adversary Strategies for Querying a Prover

Our framework provides three strategies that unify all the existing attacks on distance bounding protocols. The first two strategies depend on the moment the prover is queried by the adversary.

[2] There exists two HK protocols. One with only one nonce sent from the verifier, and the other is described in the previous section. We are speaking here about the former.

These two strategies can be applied to any type of attack scenarios defined in Section 2.

Pre-ask strategy. The adversary relays the first slow phase between the verifier and the prover, then – before the verifier starts the fast phase – executes the fast phase with the prover. Afterward, she carries on the fast phase with the legitimate verifier. She can also finally relay the final slow phase, if any. With such a strategy, the adversary can for example obtain one register among two in Hancke and Kuhn's protocol, or she can retrieve the random values in Brands and Chaum's protocol.

Post-ask strategy. As in the previous strategy, the adversary relays the first slow phase. Afterward, she executes the fast phase with the verifier without asking the prover. Then, she queries the prover with the correct challenges received during the fast phase. Finally, she relays the final slow phase. This strategy only makes sense if such a final 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.

The two previous strategies are used to retrieve informations. In a distance fraud, the *early-reply strategy* is combined with one of these strategies. In a mafia or a terrorist fraud, the early-reply is useless in the regular cases, the adversary is already inside of the neighborhood. However, the strategy should be considered in the degenerated case study.

Early-reply strategy. In this strategy, the adversary, located outside of the neighborhood, relays the first slow phase. During the fast phase, her strategy is to anticipate the challenge: she replies before she is supposed to do so. Finally, she relays the potential final slow phase, if any. Using this strategy affects the RTT measurement. Hence the adversary deceives the verifier on his location. This strategy was first described by Brands and Chaum [10].

Remark 7. In some articles (e.g., [39]), a fourth strategy is mentioned, where the adversary does not interact at all with the prover during the whole attack. This is actually a classical impersonation that is not specific to distance bounding, and so not considered in this paper. Nevertheless, authors of distance bounding protocols must pay attention to this attack especially when if the length of the secret is small regarding the number of rounds.

4 Prover Model

Up to our knowledge, all works addressing the distance bounding problem consider that the prover has full control on the execution of the algorithm. This is not always relevant in RFID, where one may clearly distinguish the Human prover from the prover's device. We model these concepts by introducing the *black-box* [9, 61] and *white-box* [16, 53] models in our framework. This allows to refine the success probabilities of an adversary and point out that some published works underestimate the success probabilities when the prover has a full control on the execution of the algorithm.

4.1 Tampering Capabilities of the Prover

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 a white-box model, the prover has full access to the implementation of the algorithm and a complete control over the execution environment.*

Remark 8. We emphasize that the two models only concern the capability of the prover in observing or tampering with the execution of the algorithm. Indeed, a man-in-the-middle adversary is neither able to directly observe nor to tamper with the execution of the algorithm performed by the prover. This implies that these models are not relevant when considering the impersonation fraud (Definition 6), and they are equivalent when considering the mafia fraud (Definition 8), as it will be stressed in Section 4.4.

4.2 Computing Capabilities of the Prover

Section 3.2 addresses the adversary capabilities in terms of protocol executions. It states that, when executing the protocol several times does not increase the success probability of the adversary in the next executions, the security analysis can consider only one execution. This limitation also applies to the prover when the latter is malicious, *i.e.*, in distance fraud and terrorist fraud.

In the white-box model, restricting the computation capabilities of the prover within one protocol execution is also required. This computation bound should be provided by the designers of distance bounding protocols and the security analysis should be based on it, which is not done in the existing literature. We illustrate this issue, by analyzing the resistance of HK [30] faced to a distance fraud in the white-box model, and show with a numerical example that the adversary almost certainly wins if there is a 1-second latency between the slow and fast phases.

In order to increase her success probability when performing a distance fraud against HK, the prover can exploit the fact that the verifier is the first party who commits. Using the notations defined in Section 3, we can state that the success probability of the adversary is increased when $d_H(R_i^0, R_i^1)$, the hamming distance between R^0 and R^1 is low. This case occurs if the prover runs the pseudo-random function as many as possible and keep the optimal nonce that maximizes the number of pairs (R_i^0, R_i^1) where $R_i^0 = R_i^1$. "As many as possible" is the bound that should be provided by the designer of the distance bounding protocol.

More precisely, the prover succeeds in a given round of the protocol with probability 1 if $R^0 = R^1$ and probability $\frac{1}{2}$ otherwise. For a $i \in \{0, \cdots, n\}$, we obtain so the success probability of the adversary when considering the distance fraud against HK:

$$\Pr(\text{success}|d_H(R^0, R^1) = i) = \left(\frac{1}{2}\right)^i, \tag{1}$$

where d_H denotes the Hamming distance. Let X be a random variable that represents the value of the Hamming distance between R^0 and R^1. We have:

$$\Pr(X = x) = \frac{\binom{n}{x}}{2^n}, \quad 0 \leq x \leq n.$$

Suppose from now that the prover is allowed to run p times the pseudo-random function f defined in Section 3. For all i in $\{1, \ldots, p\}$, let X_i be the random variable associated to $d_H(R^0, R^1)$ produced by $f(k, N_V, N_i)$ with N_i being the nonce tested by the adversary at the i-th tries. We define $Y = \min(X_1, \ldots, X_p)$.

For any y such that $0 \leq y < n$ and i such that $i \in \{1, \ldots, p\}$, we define the event $\mathcal{A}_i^y$: exactly i among p X_js are equal to y, and the $p - i$ remaining are strictly greater than y. As the X_js are independent and follow the same distribution, we can define a random variable X following the same distribution as the X_js, and conclude:

$$\Pr\left(\mathcal{A}_i^y\right) = \binom{p}{i} \Pr(X = y)^i \Pr(X > y)^{p-i}. \tag{2}$$

Hence, we deduce that, for a given $0 \leq y < n$, Y is equal to y if one of the events $\mathcal{A}_i^y$ occurs, *i.e.*, $\{Y = y\} = \bigcup_{i=1}^{i=p} \mathcal{A}_i^y$. The $\mathcal{A}_i^y$s are such that they are pairwise disjoint, so the probability that Y is equal to y is:

$$\mathrm{P}(Y = y) = \sum_{i=1}^{i=p} \mathrm{P}\left(\mathcal{A}_i^y\right). \tag{3}$$

Then, from Equation (2) and Equation (3), we compute:

$$\Pr(Y = y) \quad = \quad \frac{1}{2^{pn}} \left(\left(\sum_{j=y}^{i=n} \binom{n}{j} \right)^p - \left(\sum_{j=y+1}^{i=n} \binom{n}{j} \right)^p \right). \tag{4}$$

The special case where $Y = n$ occurs if all the random variables $X_j = n$ for all j such that $1 \leq j \leq p$. As previously, we define the random variable X following the same distribution as the X_js and obtain:

$$\Pr(Y = n) = (\Pr(X = n))^p = \frac{1}{2^{np}}. \tag{5}$$

Now, we can calculate, P_{succ}, the success probability of the adversary when she is allowed to run p times the pseudo-random function between the slow and fast phases of HK in order to carry out a distance fraud as:

$$P_{succ} = \sum_{i=0}^{i=p} \Pr(\text{success}|Y = i) \cdot \Pr(Y = i).$$

Finally, Equation (4), Equation (5), and Equation (1) yields:

$$P_{succ} = \frac{1}{2^{pn}} \cdot \left(\sum_{i=0}^{i=n-1} \left(\frac{1}{2}\right)^i \cdot \left[\left(\sum_{j=i}^{j=n} \binom{n}{j} \right)^p - \left(\sum_{j=i+1}^{j=n} \binom{n}{j} \right)^p \right] + 1 \right).$$

Figure 9 shows this success probability when p is between 1 and 2^{23}, for $n = 20{,}40{,}60{,}80$ and 128, *i.e.*, some common values found in the literature [5, 38, 39, 50]. $p = 2^{23}$ is still a realistic value and roughly represents the number of hashes that can be computed today per second on a single PC. Note that we consider here the white-box model, which justifies that the prover can use a computer more powerful than an RFID tag in order to carry out the attack. The figure clearly illustrates that the success probability quickly increases up-to 1 when p increases, while the value usually claimed in the literature is $\left(\frac{3}{4}\right)^n$ [38].

4.3 Distance Between Verifier and Prover

There exists some distance bounding protocols in which each response bit depends on some previous challenges during the fast phase [6, 57]. Considering such protocols, an adversary who tries to cheat on the distance may receive some of the previous challenges that may increase the success probability of the attack. Receiving the previous challenges depends on how far the prover is away from the verifier. Assume a prover just outside of the neighborhood cannot receive the current challenge c_i however, can receive all the previous challenges to produce a current response r_i. As she diverges from the verifier after a certain range she cannot receive also c_{i-1}, and so on. This causes the appearance of some concentric neighborhoods around the verifier which is addressed in [36]. The success probability of the attack may increase as the prover locates in a closer region between those neighborhoods. Thus, while analyzing the security against either distance or terrorist fraud, with the early-reply strategy, the region of the prover should be considered.

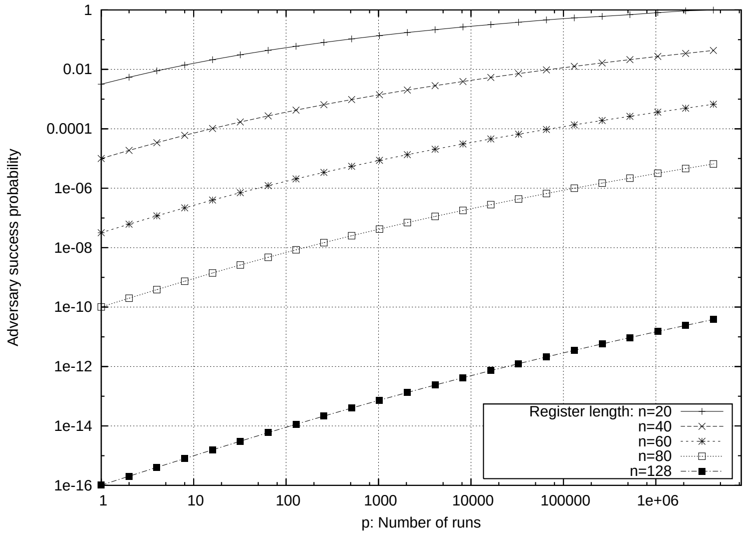

Figure 9: Adversary success probability for given registers of length n and depending on the number of pseudo random function runs.

4.4 Relations Between the Frauds and the Models

Figure 10 presents the relation between the frauds when considering the white-box and black-box models. An arrow from A to B means that: for any attack in A that succeeds with probability p_A, then there exists an attack in B that succeeds with probability p_B such that $p_B \geq p_A$. To ensure fairness in the analysis, we bound the adversary to one protocol execution with the prover, and the prover is not allowed to perform more cryptographic operations than what is defined in the protocol.

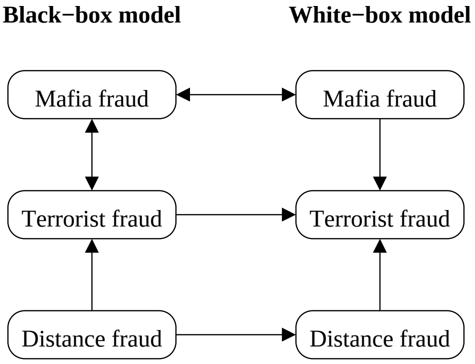

Figure 10: Relations between the frauds in the white-box and black-box models.

4.4.1 Relations Between the Models

Distance fraud. The adversary is the prover in a distance fraud. Because she has access to more information in the white box model, her success probability is obviously greater or equal in the white-box model than in the black box model.

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, the success probability of the adversary is the same in both white-box model and black-box model. This proves the equivalence stated in Figure 10.

Terrorist fraud. The prover colludes with the adversary in the terrorist fraud. Similarly to the distance fraud, the prover has access to more information in the white box model than in the black model, and so does the adversary. This proves the implication from the black-box model to the white-box model.

4.4.2 Relations Between the Frauds

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 the prover colludes with the adversary, he has no way to provide information that the adversary 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 as in the black-box one. This proves the implication.

Distance fraud vs terrorist fraud. In both models, if a dishonest prover is able to carry on a distance fraud, he also can mount a terrorist fraud with the same or higher probability. Indeed, with some help from an accomplice who only relays his answers, the malicious prover capable of a distance fraud will have the capability to execute a terrorist fraud.

Remark 9. Given the previous relations, analyzing the security of a distance bounding protocol requires to consider only 4 cases: distance fraud in the black-box model, distance 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 10. Clearly defining the prover model is quite important in the security analysis of the distance bounding protocols. This has never been done before, which led to incorrect security proofs in the literature. 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 Study Case: Munilla and Peinado's Protocol

In this section we apply our framework to a protocol proposed by Munilla and Peinado [46]. This protocol is a variant of Hancke and Kuhn's protocol [30]. In this analysis, we consider both black-box and white-box prover model and we compute the success probabilities of each fraud. First, we give a more precise upper bound than the one found in [46] for the adversary success probability using a pre-ask strategy. Moreover, we analyze another modified protocol suggested by the authors in [46]. We show that the security level of this version is lower than what they expected.

5.1 Protocol Description

In order to decrease the adversary success probability in mafia-fraud probability of Hancke and Kuhn's protocol [30], Munilla and Peinado introduce the concept of void challenges in [45, 46]. 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 and the verifier share a secret k and agree on (a) a security parameter n, (b) a public hash function f whose output size is $3n$ bits, and (c) a given timing bound $\Delta t_{\max}$.

Slow phase 1. V and P exchange nonces N_V and N_P and compute $H = f(k, N_P, N_V)$ to obtain three registers as follows: $T = H_1 \dots H_n$, $H^0 = H_{n+1} \dots H_{2n}$ and $H^1 = H_{2n+1} \dots H_{3n}$.

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 to confirm that no attack was detected. The protocol succeeds when the fast phase succeeds, *i.e.*, the RTTs measured by the verifier are correct, and the final signature is valid.

Remark 11. It should be noticed that in the original paper [45], the authors have not specified explicitly if it is the verifier or the prover who sends its nonce first. So any choice is possible. Figure 11 suggests that it is the verifier.

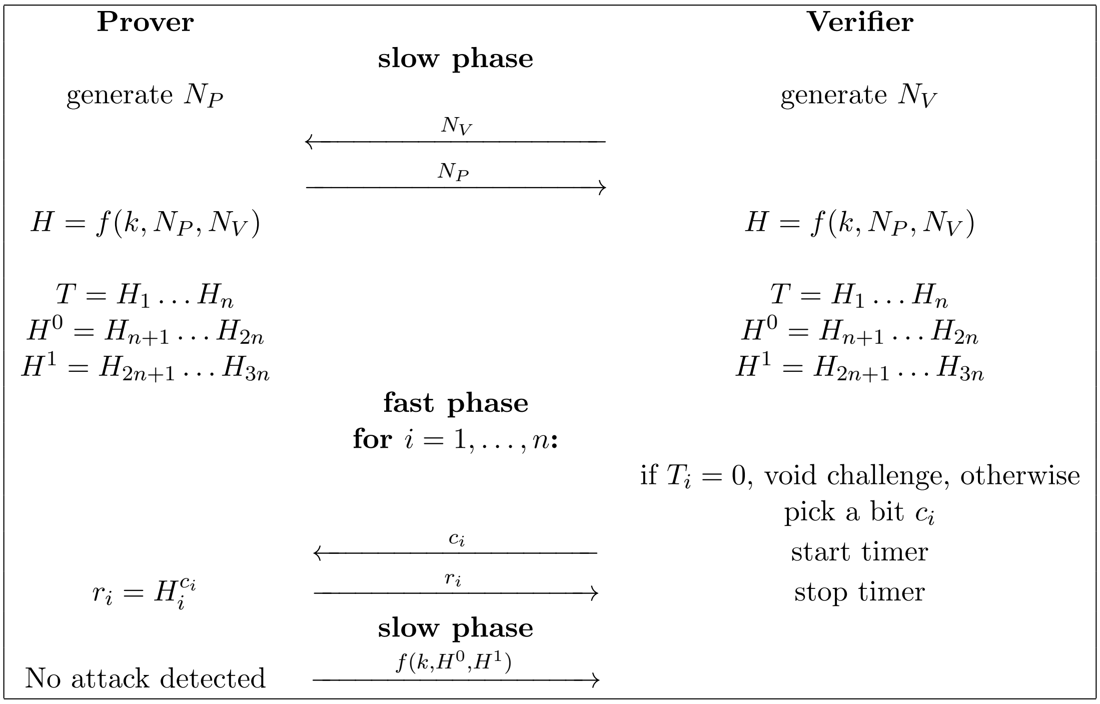

Figure 11: Munilla and Peinado's protocol.

5.2 Computation of the Impersonation Success Probability

In the impersonation attack, the adversary must successfully answer to the challenges during the fast phase and to guess the final signature. In what follows we denote p_f the probability that a full challenge is expected by the prover and the verifier. Let p_{sign} be the probability that the adversary successfully forges the 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. The probability of this event is $(1 - p_f) \cdot 1$. (b) When a challenge is full (different from void), the adversary replies with an arbitrary answer. The probability that this event occurs and that the adversary gives the correct answer to the verifier is $p_f \cdot \frac{1}{2}$. The probability of impersonation is given by:

$$p_{\text{imp}} \;=\; \left(1 - \frac{p_f}{2}\right)^n \cdot p_{\text{sign}}. \tag{6}$$

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 and computing the right signature.

5.3 Computation of the Mafia Fraud Success Probability

We remind that black-box and white-box models are equivalent when considering the mafia fraud, as stated in Section 4. The adversary achieves her attack with one of the following strategies.

Post-ask strategy. The adversary first executes the fast phase with the verifier, trying to guess the right answers and learning the registers T. Afterward, knowing the T register she executes the fast phase with the prover in order to obtain the acknowledgment signature. The adversary succeeds with the same probability as in the impersonation attack except that she does not have to predict the signature. Her success probability is:

$$p_{\text{post}-\text{ask}} = \left(1 - \frac{p_f}{2}\right)^n. \tag{7}$$

Pre-ask strategy. In order to carry out the attack, the adversary executes the protocol with the prover and the verifier respectively. We define three events:

- A: The event that the adversary is not detected by the prover and gets the final signature, *i.e.*, she sends a void challenge if and only if a void challenge is expected.
- $\bar{A}$: The event that the adversary is detected by the prover in at least one round of the fast phase and does not get the final signature.
- S: The event that the adversary succeeds the protocol executed by the verifier.

The adversary can accomplish the attack in two cases (a) she is not detected by the prover during the fast phase, gets the final signature, and she gives the correct answers to the verifier (probability $P(\mathrm{S} \cap \mathrm{A})$) , and (b) she is detected by the prover during the fast phase, and she gives the correct responses to the verifier and predict the final signature (probability $P(\mathrm{S} \cap \bar{\mathrm{A}})$). Thus, success probability of the adversary is equal to:

$$P(\mathrm{S}) = P(\mathrm{S} \cap \mathrm{A}) + P(\mathrm{S} \cap \bar{\mathrm{A}}). \tag{8}$$

When the prover is queried by the adversary, the latter can obtain the value H_i^0 corresponding to the i^{th} full challenge for $i = 1 \ldots n$. Then, when she executes the fast phase with the verifier, and is challenged by the latter, the following cases occurs:

- the challenge is a void challenge, and the adversary knows the answer,

- the response expected is from register H^0, she knows the answer,
- the response expected is from register H^1, she randomly guesses the answer.

In each round the adversary wins without being detected if (i) she sends a void challenge to the prover when a void challenge is expected, or (ii) she sends a full challenge to the prover when a full challenge is expected, and she sends the correct responses to the verifier. The probability of the former is equal to $(1-p_f)\cdot(1-p_c)$ where p_c is the probability that the adversary sends at a given round a full challenge to the prover. The probability of the latter is equal to $p_f \cdot p_c \cdot \frac{3}{4}$. Since the adversary has to be successful in each of the n fast round then the success probability without being detected is:

$$P(\mathrm{S} \cap \mathrm{A}) = [(1-p_f)\cdot(1-p_c) + p_f \cdot p_c \cdot 3/4]^n. \tag{9}$$

Let us assume that the adversary is detected at the j^{th} round by the prover and completes the protocol with the verifier. The success probability of this event is computed below:

$$\begin{aligned} P(\mathrm{S} \cap \bar{\mathrm{A}}_\mathrm{j}) &= [(1-p_f)\cdot(1-p_c)\cdot 1 + p_f \cdot p_c \cdot 3/4]^{j-1} \\ &\cdot\ [(1-p_f)\cdot p_c \cdot 1 + p_f \cdot (1-p_c)\cdot 1/2] \\ &\cdot\ [(1-p_f)\cdot 1 + p_f \cdot 1/2]^{n-j} \cdot p_{sign}. \end{aligned} \tag{10}$$

where $\bar{A}_j$ is the event that the adversary is detected at the j^{th} round by the prover. From the Equation 10, the probability that the adversary succeeds with being detected in any round is computed as follows:

$$\begin{aligned} P(\mathrm{S} \cap \bar{\mathrm{A}}) &= p_{sign} \cdot \sum_{j=1}^{n} ([(1-p_f)\cdot(1-p_c)\cdot 1 + p_f \cdot p_c \cdot 3/4]^{j-1} \\ &\cdot\ [(1-p_f)\cdot p_c \cdot 1 + p_f \cdot (1-p_c)\cdot 1/2] \\ &\cdot\ [(1-p_f)\cdot 1 + p_f \cdot 1/2]^{n-j}). \end{aligned} \tag{11}$$

We notice that if the adversary is detected by the prover, the latter becomes mute, and she does not get the final signature. In this case, she has to guess this signature, but this highly reduces the success probability which can be neglected. Hence, from Equation 8, Equation 9 and Equation 11 the success probability of the adversary can be considered as follows.

$$\begin{aligned} P(\mathrm{S}) &= P(\mathrm{S} \cap \mathrm{A}) \\ &= [(1-p_f)\cdot(1-p_c)\cdot 1 + p_f \cdot p_c \cdot 3/4]^n. \end{aligned} \tag{12}$$

In order to maximize the attack probability, the optimal p_c values for each p_f value can be computed from Equation 12:

$$p_c = \begin{cases} 0, & if \quad 0 \le p_f < 4/7, \\ 1, & if \quad 4/7 < p_f \le 1, \\ any, & if \quad p_f = 4/7. \end{cases} \tag{13}$$

By combining Equation 12 and Equation 13 the success probability for pre-ask strategy is:

$$p_{\text{pre-ask}} = \begin{cases} (1-p_f)^n & \text{if } 0 \le p_f < 4/7 \\ (p_f \cdot \frac{3}{4})^n & \text{if } 4/7 < p_f \le 1 \end{cases} \tag{14}$$

Comparison between the strategies. We now compare the different adversary strategies. By combining Equation 7 and Equation 14, we find the equality between the two strategies when $p_f = 0.8$. Hence, to maximize to success probability the adversary chooses the pre-ask strategy for $p_f > 0.8$, otherwise she prefers the post-ask strategy. Below, we provide the optimal mafia fraud success probability, (p_{maf}), regarding p_f:

$$p_{\text{maf}} = \begin{cases} p_{\text{post-ask}} & \text{if } p_f < 0.8, \\ p_{\text{pre-ask}} & \text{if } p_f > 0.8. \end{cases} \tag{15}$$

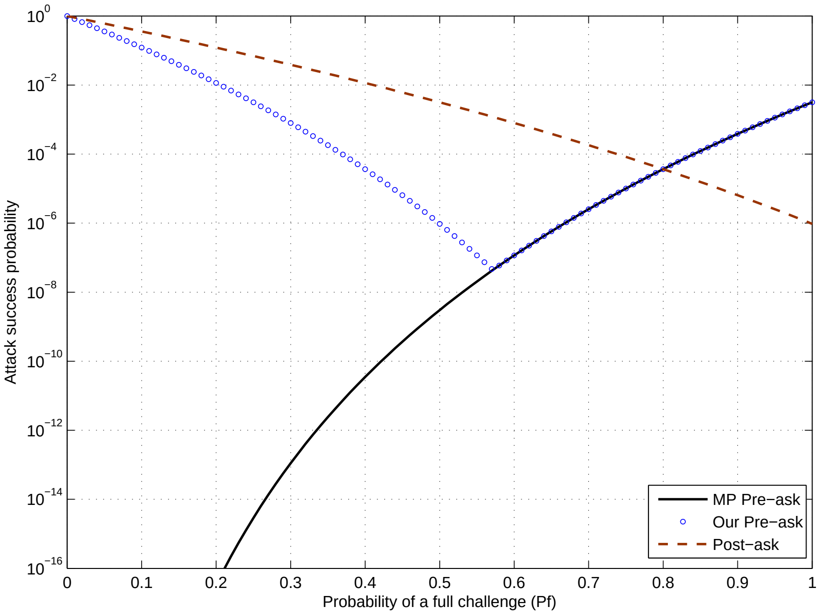

Figure 12: Attack success probability depending on p_f for a given number of rounds $n = 20$.

Remark 12 (Notes on Munilla and Peinado's Results). In the original paper [46], the authors consider an upper bound for the pre-ask strategy:

$$p_{\text{mp-pre-ask}} = \left(\frac{3}{4} \cdot p_f\right)^n. \tag{16}$$

This bound is convenient for the authors [46] to compute the average success probability of the adversary. Figure 12 shows that our result, $p_{\text{pre-ask}}$, is more accurate than the original bound $p_{\text{mp-pre-ask}}$.

5.4 Computation of the Terrorist Fraud Success Probability

In the white-box model, the registers H^0 and H^1 are provided to the adversary by the prover without any leakage on long term key. Therefore, the terrorist fraud is always achieved with probability equal to one. As stated in Section 4, the terrorist fraud is equivalent to the mafia fraud in the the black-box model.

5.5 Computation of the Distance Fraud Success Probability

As mentioned in Section 4, the adversary carries out the early-reply strategy in the white-box and black-box models.

5.5.1 White-Box Model

We remind that we assume that the verifier sends his nonce first. The adversary may run the hash function one or several times with different random nonces depending on her capability. Therefore, we analyze two different adversary capabilities in this model. Moreover, combining an early-reply strategy with a post-ask or pre-ask strategies does not make sense. The adversary does not need to query the tag to get a specific register or a final signature: she has everything at hand.

Restricted adversary. The adversary is allowed to run only once the hash function to compute H^0 and H^1. The adversary is provided all the registers used in the protocol. She knows whenever a void challenge or a full challenge is expected in each round. If $H_i^0 = H_i^1$ and the challenge is full, she replies the good answer with probability 1. Otherwise, $H_i^0 \neq H_i^1$ and the challenge is full, her early reply is correct with probability $\frac{1}{2}$. The probability $P_{correct}$ to send the correct reply when a full challenge is expected is $P_{correct} = \frac{3}{4}$. When the void challenge occurs, she waits until next challenge. After the fast phase, the adversary always produces a valid final signature. Hence the success probability of the distance fraud (P_{dist}) is computed as follows:

$$P_{dist} \quad = \quad ((1 - p_f) \cdot 1 + p_f \cdot P_{correct})^n. \tag{17}$$

With $P_{correct} = \frac{3}{4}$, we have $P_{dist} = (1 - \frac{p_f}{4})^n$. Moreover, this case also corresponds to a protocol in which the prover sends its nonce first, *i.e.*, the prover can not tamper with any of the registers.

Powerful adversary. Assume that the adversary is allowed to run the hash function 2^{23} times with different inputs. In this case Equation 17 still applies but she can minimize the Hamming distance $d_H(H^0,\, H^1)$ between the two registers to obtain $P_{correct} \approx 1$. Indeed, after running the hash function 2^{23} times, the adversary keeps the best run, *i.e.*, the run such that $d_H(H^0, H^1)$ is minimum. Let, $d_H(H^0, H^1)$ be equal to k $(0 \leq k \leq n)$ for that given run. The probability that the adversary gives the correct answer when a full challenge is expected is then:

$$\Pr(\text{correct}|d_H(H^0, H^1) = k) = 1 - \frac{k}{n} \cdot \frac{1}{2}.$$

The previous probability yields $P_{correct}$, the probability that, when a full challenge is expected, the adversary sends a correct response:

$$P_{correct} = \sum_{i=0}^{i=n} \Pr(\text{correct}|d_H(H^0, H^1) = i) \cdot \Pr(d_H(H^0, H^1) = i) = 1 - \frac{1}{2} \cdot \frac{\mathbb{E}\left(d_H(H^0, H^1)\right)}{n},$$

where $\mathbb{E}\left(d_H(H^0, H^1)\right)$ is the expected Hamming distance between H^0 and H^1 after running 2^{23} times the hash function.

Table 1 shows the effect of the register length on the probability $P_{correct}$ for an adversary able to try 2^{23} operations. Increasing the register length decreases slowly $P_{correct}$ and the overall success probability of the distance fraud. We emphasize the need for the prover to send its nonce N_p first in the slow phase.

Length n of H^i	20	30	40	50	60	70	80	90	100
$\approx P_{correct}$	1	0.96	0.94	0.92	0.91	0.90	0.89	0.88	0.87

Table 1: Probability $P_{correct}$ for a powerful adversary.

5.5.2 Black-Box Model

The adversary is not able to observe the contents of H^0 and H^1 in order to increase the success probability of her early-reply strategy. Therefore, she needs to query the tag to gain information. She can use the pre-ask or the post-ask strategies.

Post-ask strategy. The adversary does not know when a void challenge or a full challenge is expected contrarily to the post-ask for the mafia fraud or the terrorist fraud. She tries to anticipate the challenge. The only advantage gained by the adversary is the final signature. Two cases have to be considered for analyzing the fast phase: a) the adversary should predict when a void challenge occurs; b) the adversary should predict when a full challenge occurs and she should reply with the correct answer. As previously, let p_c denote the probability of sending a full challenge. The distance fraud success probability P_{dist} for this strategy is:

$$P_{dist} = \left((1-p_c)\cdot(1-p_f) + p_c\cdot p_f\cdot\frac{1}{2}\right)^n.$$

The optimal value for p_c is zero if $p_f < 2/3$; otherwise, $p_c = 1$. For any strategy, the success probability of the adversary is upper bounded by $\left(\frac{p_f}{2}\right)^n$.

Pre-ask strategy. The adversary first queries the tag and then executes the fast phase anticipating the challenge. The adversary utilizes the pre-ask strategy used in the mafia fraud. However, in this case, the adversary does not know the value of the verifier's challenge. Therefore, the adversary uses another strategy to produce an answer to the challenge. In each round, if a full challenge occurs, she sends to the verifier the response from the register obtained by querying the tag. With this approach, when a full challenge occurs, the probability of succeeding one round of the fast phase is 3/4 because in half of the cases, the verifier sends a challenge corresponding to the adversary answer thus she wins; in other half of the cases, there is still 1/2 chance that the response is correct. Similarly to the computation of the success probability of the pre-ask strategy in the mafia fraud, the probability of success for the distance fraud P_{dist} is given by:

$$P_{dist} = \left((1-p_c)\cdot(1-p_f) + p_c\cdot p_f\cdot\frac{3}{4}\right)^n.$$

The optimal value for p_c is one, if $p_f < 4/7$; otherwise, zero. For any strategy, the success probability of the adversary is upper bounded by $\left(p_f\cdot\frac{3}{4}\right)^n$.

In this case, the pre-ask strategy have the best success probability. Hence, this strategy assesses the security of the protocol regarding to distance fraud.

5.6 Modified Version of Munilla and Peinado's Protocol

In [46], the authors propose another version of the protocol and claim that it still provides better security level than Hancke and Kuhn's protocol [30]. In this version, they propose to generate $3n+1$ bits $(f(k, N_P, N_V) = H_1\cdots H_{3n+1})$. As in the original version of the protocol, a register T is used to define if we have a void challenge or a full challenge. It is assumed here that $p_f = \frac{3}{4}$, so $2n$ are needed to produce the register T. The value $\{01, 10, 11\}$ are mapped to 1 and $\{00\}$

is mapped to 0 in T. The remaining $n+1$ bits are used to answer to the verifier challenges. The least significant bit or most significant bit is taken out from this register, depending on the challenges. For instance, if the challenge is zero the prover takes the response from the left edge, otherwise from the right edge. Once a bit has been used, it is deleted. We show that this approach dramatically decreases the security level of the protocol.

5.6.1 The Mafia Security Analysis

Using the post-ask strategy the success probability of the adversary is the same as the one provided by Equation 7. In what follows, we show that the success probability of the adversary is greater than what is claimed in [46].

Pre-ask strategy. From the pre-ask strategy used in the original protocol, it is observed that there are two optimal conditions for the adversary. For some values of p_f, the adversary always sends full challenges to the prover and for the others, she only sends void challenges.

Assuming that the adversary always sends full challenges to the prover, she succeeds the protocol executed on the prover side with probability p_f^n. However, she only learns n bits of the register, and one bit remains unknown. When she queried the prover, if the adversary successfully guessed which bit is not used during the fast phase executed with verifier, she succeeds her attack with probability p_f^n. Otherwise, one bit is unknown and she must try a response at random, so her success probability is $\frac{1}{2} \cdot p_f^n$. Since the verifier produces the full challenges with probability 1/2, the bit not used during the fast phase will be in the middle of the register with high probability.

Assuming that the bit not used in the protocol is the one in the middle, the number of ones and the number of zeros in the register is $n/2$. There is only $\binom{n}{n/2}$ combinations of registers fulfilling this assumption. Since the total number of combinations is 2^n, the probability that the unused bit is in the middle of the register is $\binom{n}{n/2}/2^n$.

When the adversary uses a strategy to get all the responses from the prover except the bit in the middle of the register, the probability of success when performing a mafia fraud with the pre-ask strategy is:

$$\frac{1}{2} \cdot p_f^n \cdot \left(1 + \frac{\binom{n}{n/2}}{2^n}\right). \tag{18}$$

Assuming that the adversary sends only void challenges, her success probability is $(1-p_f)^n$.

Comparing the strategies. Figure 13 depicts the adversary success probabilities for each strategy, depending on p_f, when considering a 20-bit register. For comparison, we additionally provide the success probability of HK.

6 Conclusion

In this paper, a systematic method has been proposed to analyze distance bounding protocols. The fair evaluations provided by our framework can be used to design or analyze distance bounding protocols. We defined the capabilities and strategies of the adversary and illustrated our framework on the distance bounding protocol of Munilla and Peinado [46]. For the mafia fraud, we showed a more precise upper bound than the one found in [46] for the adversary success probability using a pre-ask strategy. We also proved that the security level of the evolved version of the protocol is lower than what is claimed in [46].

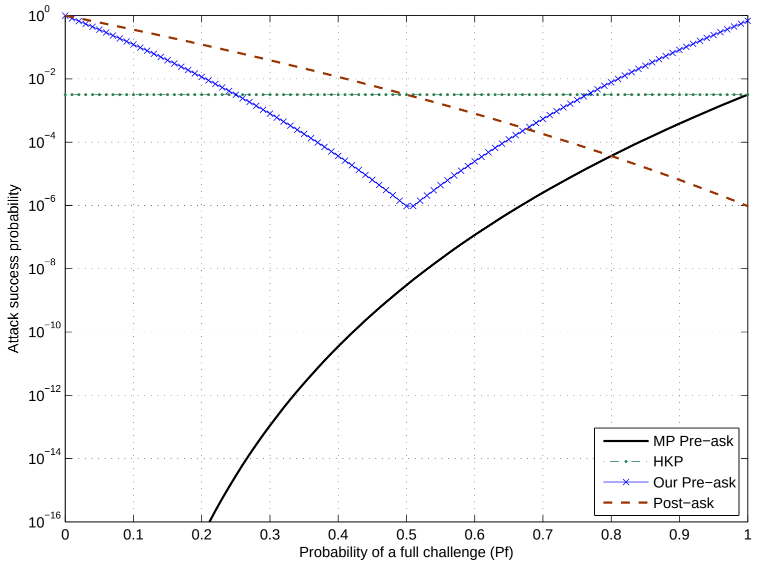

Figure 13: Attack success probability depending on p_f for a given number of rounds $n = 20$.

Acknowledgments

This work has been partially founded by FP7-Project ICE under the grand agreement number 206546, and by the Walloon Region Marshall plan through the SPW DG06 Project TRASILUX. The authors thank to Jorge Munilla and Marc Vauclair for their interesting comments.

References

[1] A. Alkassar, C. Stüble, and A.-R. Sadeghi. Secure Object Identification-or: Solving the Chess Grandmaster Problem. In *Proceedings of the 2003 Workshop on New Security Paradigms*, pages 77–85, Ascona, Switzerland, August 2003. ACM.

[2] A. Alkassar, C. Stble, and A.-R. Sadeghi. Secure Object Identification - or: Solving The Chess Grandmaster Problem. In *Proceedings of the 2003 Workshop on New Security Paradigms*, pages 77–85, Ascona, Switzerland, 2003. ACM Press.

[3] R. J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, Inc., 2001. in Chapter 2: the MIG-in-the-Middle Attack.

[4] R. J. Anderson. Position Statement in RFID S&P Panel: RFID and the Middleman. In *Financial Cryptography*, volume 4886 of *Lecture Notes in Computer Science*, pages 46–49, Scarborough, Trinidad and Tobago, February 2007. Springer-Verlag.

[5] 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.

[6] G. Avoine and A. 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*, pages 250–261, Pisa, Italy, September 2009. Springer-Verlag.

[7] S. Bengio, G. Brassard, Y. Desmedt, C. Goutier, and J.-J. Quisquater. Secure implementation of identification systems. *Journal of Cryptology*, 4(3):175–183, 1991.

[8] 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.

[9] M. Blaze. Looking on the Bright Side of Black-Box Cryptography (Transcript of Discussion). In *Security Protocols Workshop*, volume 2133 of *Lecture Notes in Computer Science*, pages 54–61, Cambridge, UK, April 2000. Springer-Verlag.

[10] 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.

[11] 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.

[12] L. Bussard and Y. Roudier. Embedding distance-bounding protocols within intuitive interactions. In D. Hutter, G. Müller, W. Stephan, and M. Ullmann, editors, *Security in Pervasive Computing – SPC*, volume 2802 of *Lecture Notes in Computer Science*, pages 119–142, Boppard, Germany, March 2003. Springer-Verlag.

[13] S. Capkun, L. Buttyan, and J.-P. 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, Fairfax, Virginia, USA, October 2003. ACM.

[14] S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *INFOCOM*, pages 1917–1928, Miami, Florida,USA, March 2005. IEEE.

[15] M. Card. Mastercard paypass. http://www.mastercard.com/, 2010.

[16] S. Chow, P. A. Eisen, H. Johnson, and P. C. van Oorschot. White-Box Cryptography and an AES Implementation. In *Selected Areas in Cryptography - SAC*, volume 2595 of *Lecture Notes in Computer Science*, pages 250–270, Newfoundland, Canada, August 2002. Springer-Verlag.

[17] J. H. Conway. *On Numbers and Games.* Number 6 in London Mathematical Society Monographs. Academic Press, London-New-San Francisco, 1976.

[18] Y. Desmedt. Position Statement in RFID S&P Panel: From Relative Security to Perceived Secure. In *Financial Cryptography*, volume 4886 of *Lecture Notes in Computer Science*, pages 53–56, Scarborough, Trinidad and Tobago, February 2007. Springer-Verlag.

[19] 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.

[20] D. Dolev and A. C.-C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–207, 1983.

[21] S. Drimer and S. J. Murdoch. Keep your enemies close: distance bounding against smartcard relay attacks. In *16th USENIX Security Symposium on USENIX Security Symposium*, pages 1–16, Santa Clara, California, USA, June 2007. USENIX Association.

[22] J. Eagle. RFID: The Early Years 1980-1990. MIT, 2001.

[23] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. 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.

[24] A. Francillon, B. Danev, and S. Capkun. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. Cryptology ePrint Archive, Report 2010/332, 2010.

[25] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis. Practical NFC Peer-to-Peer Relay Attack using Mobile Phones. In *Workshop on RFID Security – RFIDSec'10*, to appear in Lecture Notes in Computer Science, Istanbul, Turkey, June 2010. Springer-Verlag.

[26] J. Gleick. A new approach to protecting secrets is discovered. *The New York Times*, February, 17th 1987.

[27] M. Halváč 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.

[28] G. Hancke. A Practical Relay Attack on ISO 14443 Proximity Cards. Manuscript, February 2005.

[29] G. Hancke. Practical Attacks on Proximity Identification Systems. In *IEEE Symposium on Security and Privacy - S&P 2006*, pages 328–333, Berkeley, California, USA, May 2006. IEEE Computer Society.

[30] 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.

[31] G. Hancke, K. Mayes, and K. Markantonakis. Confidence in Smart Token Proximity: Relay Attacks Revisited. In *Elsevier Computers & Security*, June 2009.

[32] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. In *INFOCOM*, San Francisco, California, USA, March-April 2003.

[33] Y.-C. Hu, A. Perrig, and D. B. Johnson. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):370–380, 2006.

[34] ISO/IEC 14443. Identification cards – contactless integrated circuit(s) cards – proximity cards.

[35] G. Kapoor, W. Zhou, and S. Piramuthu. Distance Bounding Protocol for Multiple RFID Tag Authentication. In *EUC '08: Proceedings of the 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, pages 115–120, Shanghai, China, December 2008. IEEE Computer Society.

[36] O. Kara, S. Kardas, M. A. Bingol, and G. Avoine. Optimal Security Limits of RFID Distance Bounding Protocols. In *Workshop on RFID Security – RFIDSec'10*, to appear in Lecture Notes in Computer Science, Istanbul, Turkey, June 2010. Springer-Verlag.

[37] Z. Kfir and A. 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.

[38] C. H. Kim and G. Avoine. RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks. In J. A. Garay, A. Miyaji, and A. Otsuka, editors, *8th International Conference on Cryptology And Network Security – CANS'09*, volume 5888 of *Lecture Notes in Computer Science*, pages 119–133, Kanazawa, Ishikawa, Japan, December 2009. Springer-Verlag.

[39] 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.

[40] J. Klein-Saffran. Electronic monitoring vs. halfway houses: A study of federal offenders. *Alternatives to Incarceration*, pages 24–28, Fall 1995.

[41] A. Laurie. Website. http://www.rfidiot.org/, 2010.

[42] A. Levi, E. Çetintas, M. Aydos, Çetin Kaya Koç, and M. U. Çaglayan. Relay Attacks on Bluetooth Authentication and Solutions. In *International Symposium Computer and Information Sciences - ISCIS 2004*, volume 3280 of *Lecture Notes in Computer Science*, pages 278–288, Kemer-Antalya, Turkey, October 2004. Springer-Verlag.

[43] C. Meadows, R. Poovendran, D. Pavlovic, L. Chang, and P. 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.

[44] A. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1996.

[45] J. Munilla, A. Ortiz, and A. Peinado. Distance Bounding Protocols with Void-Challenges for RFID. In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006.

[46] 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.

[47] V. Nikov and M. Vauclair. Yet Another Secure Distance-Bounding Protocol. Cryptology ePrint Archive, Report 2008/319, 2008.

[48] NXP. NXP mifare plus – benchmark security for mainstream applications. http://mifare.net/downloads/NXP_Mifare_Plus_leaflet.pdf, 2009.

[49] Y. Oren and A. Wool. Relay Attacks on RFID-Based Electronic Voting Systems. Cryptology ePrint Archive, Report 2009/442, 2009.

[50] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and J. C. A. van der Lubbe. Shedding Some Light on RFID Distance Bounding Protocols and Terrorist Attacks. arXiv.org, Computer Science, Cryptography and Security, 2009.

[51] K. B. Rasmussen, C. Castelluccia, T. Heydt-Benjamin, and S. Capkun. Proximity-based access control for implantable medical devices. In *ACM Conference on Computer and Communications Security – CCS'09*, pages 410–419, Chicago, Illinois, USA, November 2009. ACM.

[52] 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.

[53] A. Saxena, B. Wyseur, and B. Preneel. Towards Security Notions for White-Box Cryptography. In *Information Security Conference- ISC 2009*, volume 5735 of *Lecture Notes in Computer Science*, pages 49–58, Pisa, Italy, September 2009. Springer-Verlag.

[54] D. Singelée and B. 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, July 2007. Springer-Verlag.

[55] 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.

[56] F. Stajano, F.-L. Wong, and B. Christianson. Multichannel protocols to prevent relay attacks. In *Proceedings of Financial Cryptography 2010*, volume 6052 of *Lecture Notes in Computer Science*, pages 4–19, Tenerife, Spain, January 2010. Springer-Verlag.

[57] R. Trujillo Rasua, B. Martin, and G. Avoine. The Poulidor Distance-Bounding Protocol. In *Workshop on RFID Security – RFIDSec'10*, to appear in Lecture Notes in Computer Science, Istanbul, Turkey, June 2010. Springer-Verlag.

[58] Y.-J. Tu and S. Piramuthu. RFID Distance Bounding Protocols. In *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.

[59] Visa. Visa conctless credit card. http://usa.visa.com/personal/cards/paywave/index.html, 2010.

[60] B. R. Waters and E. W.Felten. Secure, private proofs of locations. Princeton Computer Science, TR-667-03, 2003.

[61] A. Young and M. Yung. The Dark Side of "Black-Box" Cryptography, or: Should We Trust Capstone? In *Advances in Cryptology - CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 89–103, Santa Barbara, California, USA, August 1996. Springer-Verlag.

[62] J. Zhou and J. Shi. RFID Localization Algorithms and Applications – a Review. *Journal of Intelligent Manufacturing*, 20(6):695–707, December 2008.