

Comparing Distance Bounding Protocols: a Critical Mission Supported by Decision Theory

Gildas Avoine^{a,b}, Sjouke Mauw^c, Rolando Trujillo-Rasua^{c,*}

^a*INSA Rennes, IRISA UMR 6074, Institut Universitaire de France*

^b*Université catholique de Louvain, Belgium*

^c*Interdisciplinary Centre for Security, Reliability and Trust
University of Luxembourg*

Abstract

Distance bounding protocols are security countermeasures designed to thwart relay attacks. Such attacks consist in relaying messages exchanged between two parties, making them believe they communicate directly with each other. Although distance bounding protocols have existed since the early nineties, this research topic resurrected with the deployment of contactless systems, against which relay attacks are particularly impactful. Given the impressive number of distance bounding protocols that are designed every year, it becomes urgent to provide researchers and engineers with a methodology to fairly compare the protocols in spite of their various properties. This paper introduces such a methodology based on concepts from the decision making field. The methodology allows for a multi-criteria comparison of distance bounding protocols, thereby identifying the most appropriate protocols once the context is provided. As a side effect, this paper clearly identifies the protocols that should no longer be considered, regardless of the considered scenario.

Keywords: Authentication, Distance Bounding, Comparison, Decision Making, Relay Attack

*Corresponding author. Phone: +352 466 644 5458. Fax: 466 644 3 5458. Email: rolando.trujillo@uni.lu

1. Introduction

Distance bounding protocols are the most popular countermeasures against relay attacks. In a relay attack on an authentication protocol, an adversary aims to convince the verifier that he directly communicates with the genuine prover, while the adversary is actually in the middle and relays the messages exchanged between the two parties. Typically, a relay attack makes the verifier believe the prover is located within his neighborhood while he is far away.

1.1. Relay attacks

Conway [15] introduced in 1976 the concept of a relay attack through the *Chess Grandmaster problem* where a little girl is challenged to defeat a Chess Grandmaster in correspondence chess. The solution suggested by Conway to allow the little girl to be successful is to perform a relay attack between two Chess Grandmasters: the attack consequently consists in relaying the moves received between the two Chess Grandmasters, which results for the little girl in either a won or two draws.

Relay attacks also apply to authentication protocols as originally proposed by Desmedt, Goutier, and Bengio at Crypto 87 [17], whose work was later extended by Brassard and Quisquater in [7]. In their papers, the authors refuted Shamir's claims about the Fiat-Shamir protocol [18] when he says that the protocol is secure even when being executed one million times in a Mafia-owned store [21]. Desmedt *et al.* indeed raised that a relay attack is still possible, and they consequently named the suggested relay attack *mafia fraud*. Since then, both terms, relay attack and mafia fraud, are used interchangeably in the literature. Note however that Avoine *et al.* [1] distinguish mafia fraud from relay attacks by considering that the adversary cannot modify the forwarded messages in a relay attack. This distinction allows for representing an adversary who does not know the specifications of the considered protocol.

Although mafia fraud was suggested late in the eighties, practical implementations of this type of fraud appeared much later. Mafia fraud actually became a real threat with the ubiquity of contactless technologies. For example, practical attacks were developed against Radio Frequency IDentification (RFID) [22, 23], Near Field Communication (NFC) [20], and Passive Keyless Entry and Start Systems (PKES) in modern cars [19]. For example,

off-the-shelves devices to perform relay attacks against PKES can be bought on Internet [12].

1.2. Distance bounding protocols

Mafia fraud does not rely on exploiting security protocol vulnerabilities. Conventional security mechanisms are thus ineffective against it. Based on an idea from Beth and Desmedt [8], Brands and Chaum suggested a countermeasure to mafia fraud that consists in measuring the Round-Trip-Time (RTT) of 1-bit messages exchanged between the parties, using a dedicated communication channel [10]. In their solution, the verifier measures the round-trip time t_m between the moment he sent a challenge and the moment he receives the response from the prover. The verifier can consequently estimate a tight upper-bound on the distance between the prover and the verifier by computing $d = c \cdot (t_m - t_d)/2$, where c is the speed of light and t_d is the delay induced by the prover to compute the response, given the challenge.

Note that distance bounding protocols do not detect relay attacks in a strict sense. Instead, they detect unexpected delays, and conclude in such a case that a mafia fraud attack might have occurred. As a consequence, neither the communication channel, nor the calculation should introduce flexible timing during the protocol execution, since that could be exploited by an adversary. For example, requiring the prover to perform heavy computations in passive contactless systems may allow an adversary to significantly reduce t_d by overclocking the prover’s device, which in turn may allow the adversary to increase t_m without making d above the expected upper-bound. Since Desmedt *et al.*’s seminal work [8], a conservative assumption for designing distance bounding protocols consists in considering minimally sized messages (typically 1-bit messages) and lightweight computations during the time-measurement phase.

1.3. Protocol evaluation

Avoine *et al.* introduced in [1] a *Framework* for analyzing distance bounding protocols. This widely used Framework defines four types of fraud that should be considered in the security evaluation of distance bounding protocols. For the sake of accuracy, the fraud definitions from [1] are provided *in-extenso* below.

- Given a distance bounding protocol, an *impersonation fraud* attack is an attack where a lonely prover purports to be another one.

- A *mafia fraud* attack 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.
- Given a distance bounding protocol, a *distance fraud* attack is an attack where a dishonest and lonely prover purports to be in the neighborhood of the verifier.
- A *terrorist fraud* attack 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.

The security evaluation of a distance bounding protocol then consists in computing the resistance of the protocol for every type of fraud, which is done by computing the probability for an adversary to successfully perform the considered fraud.

Since Brands and Chaum’s breakthrough, many distance-bounding protocols have been proposed¹, which deliver improvements in terms of security (see Section 2). These proposals also introduce new requirements on the protocols, e.g., to be usable on noisy channels, and properties, e.g., to be more computationally efficient or to require less memory. Given the various requirements and properties, a fair methodology to compare distance bounding protocols is strongly needed.

1.4. Contribution

This paper introduces a methodology based on concepts from the decision making field to perform a multi-criteria comparison of distance bounding protocols. The methodology identifies the most desirable protocols, given a set of required properties, and disqualifies protocols that are dominated by better solutions whatever the considered properties. Even though the methodology can be understood without difficulty, applying it on a large set of distance bounding protocols may be time-consuming. As a consequence, an open-source computer tool was released in order to easily include into the comparison future distance bounding protocols and new criteria.

¹<http://www.avoine.net/rfid/>

Table 1: List of protocols and their acronyms.

Authors	Reference	Year	Acronym
Brands and Chaum	[10]	1993	BC
Čapkun, Buttyán, and Hubaux	[13]	2003	MAD
Bussard and Bagga	[11]	2005	BB
Hancke and Kuhn	[24]	2005	HK
Munilla and Peinado	[28]	2006	MP
Kim, Avoine, Koeune, Standaert, and Pereira	[27]	2008	Swiss-Knife
Avoine and Tchamkerten	[5]	2009	Tree-based
Trujillo-Rasua, Martin, and Avoine	[33]	2010	Poulidor
Rasmussen and Čapkun	[29]	2010	RC
Yum, Kim, Hong and Lee	[34]	2010	YKHL
Kim and Avoine	[26]	2011	KA
Boureau, Mitrokotsa, and Vaudenay	[9]	2013	SKI
Trujillo-Rasua, Martin, and Avoine	[31]	2014	TMA

2. Background

Distance bounding protocols are authentication protocols that, in addition, compute an upper bound on the distance between the prover and the verifier. Since we focus on the distance bounding properties of such protocols, we ignore any such protocol that does not even achieve authentication, e.g., due to impersonation attacks or key-recovery attacks [30]. The considered protocols are briefly introduced and classified according to their main features, which are the features that occur most frequently in literature and that should be taken into account to compare the protocols. The protocols are listed in Table 1.

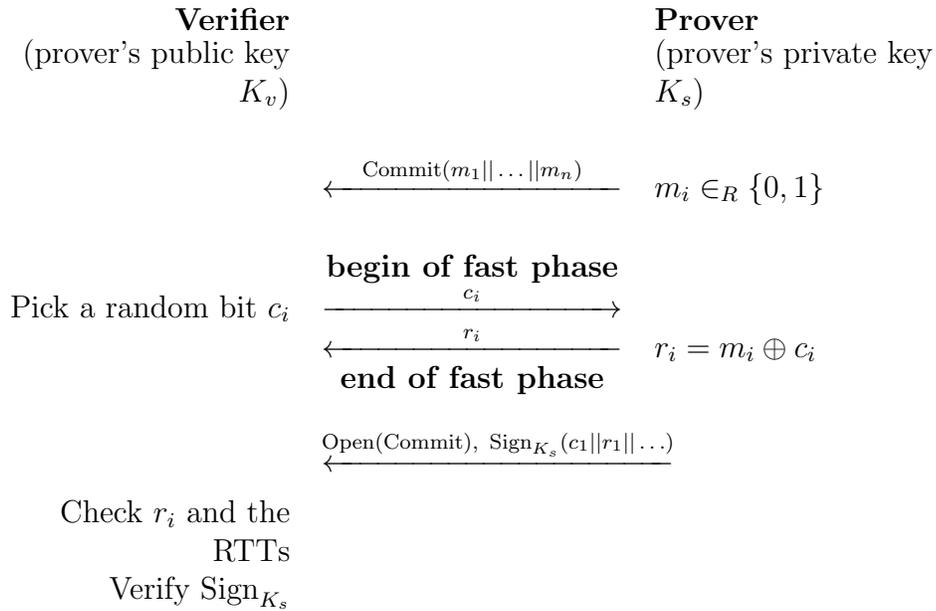
2.1. Compared protocols

2.1.1. Resistance to mafia and distance fraud.

The earliest distance bounding protocol, introduced by Brands and Chaum in 1993 [10], consists of an initial commitment phase, followed by n rounds where the verifier sends a single-bit challenge and receives a single-bit response from the prover. The protocol is then completed with a final phase where the commitment is opened and a signature of the exchanged messages is provided by the prover. The phase during which the round trip time (RTT)

is measured is known as being the *fast phase* while the other ones are known as the *slow phases*. The BC protocol, provided in Algorithm 1, reaches the optimal security bound $(1/2)^n$ against both mafia and distance fraud, where n is the number of rounds². The authors, however, left as an open problem the design of a distance-bounding protocol that resists to terrorist fraud as well.

Algorithm 1: Brands and Chaum’s Protocol



2.1.2. Resistance to terrorist fraud.

The challenge of designing a protocol resistant to terrorist fraud was taken up later in 2005 by Bussard and Bagga [11], who proposed a protocol similar in design to the BC protocol. In addition to commitment and signature schemes, the BB protocol uses a $(2, 2)$ -secret sharing scheme aimed at defeating terrorist fraud. However, Avoine, Lauradoux, and Martin [4]

²For every distance bounding protocol with a single fast phase consisting of n rounds of 1-bit exchanges, an adversary who answers randomly during the fast phase and relays all the other messages succeeds with probability $(1/2)^n$ [1].

demonstrated that a $(2, 2)$ -secret sharing scheme is insufficient to thwart terrorist fraud: a $(3, 3)$ -secret sharing scheme should be used instead.

Later on, in 2008, a first distance-bounding protocol resistant to some extent to terrorist fraud was suggested by Kim *et al.* [27]. This protocol was named the Swiss-knife distance-bounding protocol – in reference to the multi-tool Swiss army knife – due to its ability to deal with mafia, distance, and terrorist fraud at the same time. Nevertheless, its resistance value of $(3/4)^n$ to both mafia and terrorist fraud falls far beyond the optimal security bound $(1/2)^n$.

More recently, in 2013, the SKI family of protocols was designed by Boureanu, Mitrokotsa, and Vaudenay [9] to counter terrorist fraud. The SKI protocols do not perform better than existing protocols, but they benefit from the availability of security proofs.

2.1.3. Final slow phase and lightweight cryptographic operations.

The boom of RFID technology in the early 21st century, impulsed by Walmart's³ announcement of tagging pallets and cases of goods with RFID tags, motivated Hancke and Kuhn to design the first distance-bounding protocol for resource-constrained devices [24]. To do so, they dropped the objective of making the protocol secure against terrorist fraud, and focused on eliminating both the final slow phase and the need of expensive cryptographic primitives, such as commitment and signing. The drawback of the HK protocol is its low resistance to both distance and mafia fraud, which is $(3/4)^n$ [24, 33].

Inspired by the strengths and weaknesses of Hancke and Kuhn's proposal, several other distance-bounding protocols were proposed [5, 28, 26, 33, 31, 34]. All of them aim at improving the security to both mafia fraud and distance fraud, while keeping the simple design of the HK protocol to make them suitable for low-cost devices. The protocols proposed in [34, 31] also aim extra features such as mutual authentication and noise resiliency respectively.

2.1.4. Memory.

Among the protocols inspired by the HK protocol, the tree-based protocol proposed by Avoine and Tchamkerten [5] achieves the best asymptotic security to mafia and distance fraud. Unfortunately, the tree-based protocol requires an exponential amount of memory w.r.t. the number of rounds of

³Walmart is the largest retailer in the world.

the fast phase. To mitigate this problem, the authors [5] suggest a trade-off between memory requirement and security by parameterizing the depth of the tree.

Another approach by Trujillo-Rasua, Martin, and Avoine [33] consists in using a graph instead of a tree. This protocol, named Poulidor, requires a linear memory instead of an exponential one, but degrades the resistance to mafia and distance fraud in comparison to the tree-based protocol. An additional issue is that the analysis of Poulidor is complex [32] and only conservative bounds on the resistance to the various types of fraud have been provided.

To increase the resistance to mafia and distance fraud without significantly increasing the memory requirement, Kim and Avoine [26] proceed differently and suggest a trade-off between distance and mafia fraud resistance, which can be adapted to any given scenario.

2.1.5. Single-bit exchanges.

Based on the HK protocol, Munilla and Peinado introduced a distance-bounding protocol [28] where three-state challenges are used instead of binary challenges. This idea was later improved and generalized by MUSE [2], which assumes a multiple-bit channel during the fast phase. Actually, MUSE is a technique (not a protocol *per se*) that transforms any single-bit challenge protocol into a multiple-bit challenge protocol. Empirical results in [2] suggest that a MUSE transformation achieves better security properties than the single-bit challenge counterpart. For instance, the resistance of the BC protocol [10] to mafia fraud is $(1/2)^n$, while its MUSE transformation with a 2-bit channel achieves $(1/4)^n$. In both protocols, n denotes the number of rounds during the fast phase, which means that the security is measured in terms of number of rounds. However, considering the number of bits exchanged during the fast phase, denoted e , the security of both protocols becomes equal to $(1/2)^e$. This illustrates the difficulty in comparing protocols that require different properties concerning the channels.

2.2. Protocol evaluation

To the best of our knowledge, Kim *et al.* [27] were the first authors comparing their protocol against previously proposed distance bounding protocols. They used a tabular form and evaluated eight different protocols in terms of mafia and terrorist fraud resistance, number of cryptographic operations to be performed by the prover, noise resiliency of the protocol, privacy

preservation, and mutual authentication. In the comparisons published later on, the last three properties are generally not considered, as done for example in [9]. It is worth noting that the mentioned criteria are equally important and cannot be ranked: this implies that protocols can be compared according to one criterion at a time only. Note also that the resistance to attacks is generally evaluated asymptotically, i.e., when the number of rounds tends to infinity. However, a protocol might be asymptotically better than another protocol, while it is worse for some small number of rounds.

Trujillo-Rasua *et al.* [33, 31] suggested a significantly different technique to compare distance bounding protocols, where the comparison is based on two criteria and is no longer done asymptotically. So, for every protocol and for every (discretized) pair (m, d) of mafia and distance fraud resistance values in $[0, 1]^2$, the technique computes the minimum number of rounds n needed to reach these values. For every pair (m, d) , the *best* protocol is the one that requires the smallest value n . Figure 1 represents the result of the comparison applied to the Poulidor, HK, KA, and tree-based protocols in [33]. The 2D chart displays the best protocol (or one of the best protocols in case of equality) among the four considered ones for every possible value of mafia and distance fraud. For example, when $(m, d) = (1, 1)$, the best protocol is HK.

The comparison methodology introduced by Trujillo-Rasua *et al.* is more advanced than the one suggested by Kim *et al.*, but its usability remains limited. Indeed, Trujillo-Rasua *et al.*'s methodology requires criteria that impact the objective function, which is minimizing the value n . For example, applying the methodology with the criteria “mafia fraud resistance” and “presence of a final slow phase” is meaningless, given that the presence or not of a final slow phase does not depend on n . Another weakness – although the core of the methodology is not concerned – is the 2D representation of the result, which is inappropriate when considering more than two criteria.

3. Methodology

Multi-criteria decision-making actually consists in making a decision, namely selecting the best solution(s) in a set of possible solutions, when the evaluation of solutions depends on several criteria. For example, buying a car is a multi-criteria decision making problem, because price, size, horsepower, color, etc. are different criteria that influence the decision. Similarly, choosing a distance bounding protocol is a multi-criteria decision-making problem

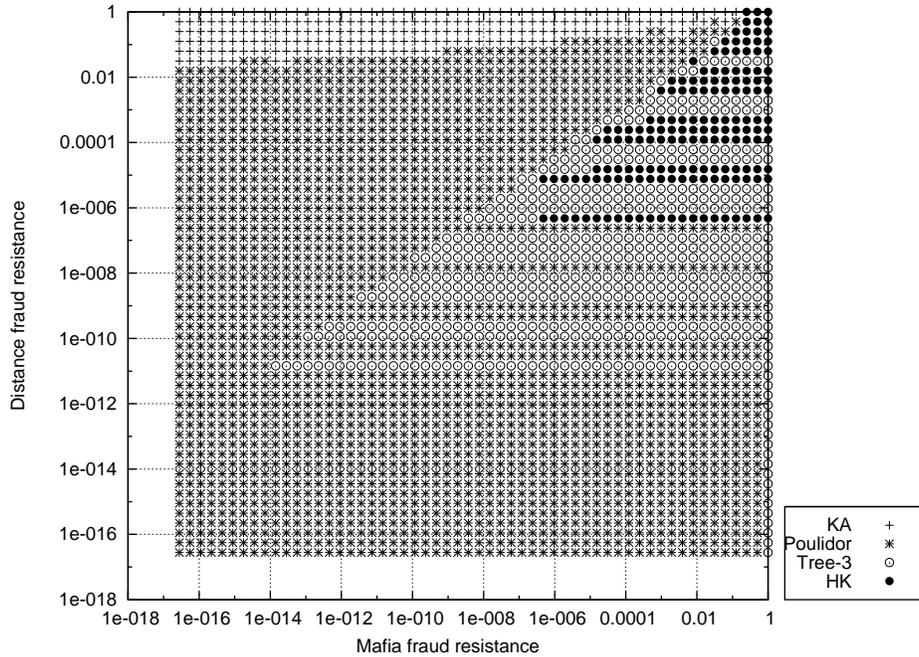


Figure 1: A visual representation [33] of the comparison of Poulidor [33], the HK protocol [24], the KA protocol [25], and the tree-based protocol using trees of depth 3 (Tree-3) [5].

where several security and implementability criteria need to be considered. This section defines the relevant *attributes* that ought to be considered in distance bounding protocols, together with the concepts of *approximate equality*, *attribute spaces*, *dominant relation*, and *protocol instance*.

3.1. Attributes

Decision criteria are built on atomic attributes that characterize the options available, namely the distance bounding protocols in our case. The most common attributes used in the literature to evaluate distance bounding protocols are related to security and implementability. These attributes are introduced below.

3.1.1. Security-related attributes.

The security challenge aims to reduce the adversary’s probability to successfully perform a mafia, distance, or terrorist fraud attack⁴. The three following attributes are consequently considered in this paper:

- *Mafia fraud resistance* (p_m). Probability for an adversary to successfully perform a mafia fraud attack according to the Framework [1] already mentioned in Section 1.
- *Distance fraud resistance* (p_d). Probability for an adversary to successfully perform a distance fraud attack according to the Framework.
- *Terrorist fraud resistance* (p_t). Probability for an adversary to successfully perform a terrorist fraud attack according to the Framework.

Other security-related attributes are the number of rounds n and the size t of the messages exchanged during the fast phase. On the one hand, most distance bounding protocols can arbitrarily increase t while keeping n constant [2], which enhances their security. On the other hand, security can also be improved by simply increasing n . Both attributes are indeed related by the equation $e = 2 \cdot n \cdot t$, where e represents the number of bits exchanged during the fast phase. We therefore consider e to be a security-related attribute that encompasses both n and t .

- *Number of bits exchanged* (e). Number of bits exchanged during the fast phase.

3.1.2. Implementability-related attributes.

When Hancke and Kuhn [24] proposed a simple and lightweight design of distance bounding protocol, the objective was to reduce the number of cryptographic operations to be performed by the prover, and to avoid the use of a final slow phase. Consequently, these two implementability-related attributes are considered in this paper.

- *Number of cryptographic operations performed by the prover* (c). The number of cryptographic operations performed by the prover is considered, because it provides a preliminary technology-independent evaluation of the computational cost of the protocols.

⁴Another type of fraud, named distance hijacking, was recently introduced by Cremers, Rasmussen, Schmidt, and Čapkun [16], but this fraud is usually disregarded in the analysis.

- *Final slow phase (f)*. Presence (or not) of a final slow phase in the protocol.

Later on, memory usage became a concern as well, because the prover in the tree-based protocol [5] pre-computes a tree whose size is exponential w.r.t. the number of rounds of the fast phase. Memory is consequently considered as an implementability-related attribute:

- *Memory used by the prover (s)*. Maximum size of the volatile memory that the prover needs in order to store the values used during the protocol execution. Note that in practice, the actual size of the memory can be smaller because memory cells might be released and subsequently refilled with other values during the execution of the protocol. Considering the prover’s memory instead of the verifier’s memory is motivated by the prevailing design of distance bounding protocols where the prover needs to pre-compute all the possible answers before the fast phase, whereas verifying the prover’s answers might not require heavy pre-computation and can be performed at the end of the protocol.

Finally, the implementation complexity of a distance bounding protocol strongly depends on the technology considered. This makes it challenging to perform an objective evaluation with that respect. In particular, some protocols require channels that carry atomic symbols containing more than one bit of information. Although technologically feasible, this requirement is strong enough to be taken into account when comparing two protocols. In the same vein, some protocols use multiple-bit exchanges during the fast phase, while a conservative assumption since Desmedt *et al.*’s work [8] consists in considering 1-bit messages. This clear distinction between those distance bounding protocols that use single-bit exchanges during the fast phase and those that use multiple-bit exchanges is captured by the following implementability-related attribute.

- *Multiple-bit exchange (b)*. A binary attribute stating the use (or not) of multiple-bit exchanges.

3.2. Attribute spaces and (non)domination

When solving decision-making problems, it is important to consider a notion of *approximate equality* on the domains of the attributes. To illustrate this, consider someone who wants to buy a second-hand car among cars that

differ on mileage and price only. When mileages are different but very close, they can be considered in the same mileage range, and only the price should lead the decision.

In this section, we first provide the general terminology and notation, afterwards we define the attribute domain and approximate equality for every considered attribute.

Definition 1 (Approximate equality). *Let $(D, <)$ be a totally ordered set. An approximate equality relation $\sim: D \times D$ is a relation satisfying, for all $x, y, z \in D$,*

$$\begin{aligned} x &\sim x \\ x \sim y &\implies y \sim x \\ x \sim z \wedge x < y < z &\implies x \sim y \wedge y \sim z. \end{aligned}$$

The first two properties state that approximate equality satisfies reflexivity and symmetry. The third property expresses that it is consistent with the total order on D . Notice that approximate equality is not an equivalence relation, because it doesn't satisfy transitivity. The reason is that many small differences can add up to a large difference.

Given a totally ordered set with approximate equality, we can define the relation $\prec: D \times D$ by

$$x \prec y \iff x < y \wedge x \not\sim y.$$

Similarly, we define $x \preceq y$ by $x \prec y \vee x \sim y$ and the symmetric cases $x \succ y$ and $x \succeq y$ by $y \prec x$ and $y \preceq x$, respectively. Next, we extend these comparison operators to attribute spaces.

Definition 2. *Let I be an index set, then a family of ordered sets with approximate equality $(D_i, <_i, \sim_i)_{i \in I}$ is called an attribute space.*

For an index set $I = \{1, \dots, n\}$, we simplify notation by stating that $\Delta = D_1 \times \dots \times D_n$ is an attribute space and that its elements are of the form $\bar{x} = (x_1, \dots, x_n)$. We define the *dominant relation* $\prec: \Delta \times \Delta$ for $\bar{x}, \bar{y} \in \Delta$ by

$$\bar{x} \prec \bar{y} \iff \forall i \in I (x_i \preceq y_i) \wedge \exists i \in I (x_i \prec y_i).$$

If $\bar{x} \prec \bar{y}$, we say that \bar{x} *dominates* \bar{y} , otherwise, if $\bar{x} \not\prec \bar{y}$, we say that \bar{y} is *nondominated* by \bar{x} . Similarly, given $E \subseteq \Delta$ and $\bar{x} \in E$, we say that \bar{x} is *nondominated* in E if

$$\neg \exists \bar{y} \in E (\bar{y} \prec \bar{x}).$$

Given that we are considering eight different attributes, we next define a totally ordered set with approximate equality relation for the eight considered attributes: $p_m, p_d, p_t, e, c, s, f$, and b .

- $(D_i, <_i, \sim_i)_{i \in \{p_m, p_d, p_t\}}$: The attributes related to the three types of fraud are in the probability domain $[0, 1]$, i.e., $D_i = [0, 1]$ for $i \in \{p_m, p_d, p_t\}$. In order to provide reasonable approximate equality relations for the three probability-based attributes, we consider that the adversary's probability of success should be more refined as it approaches 0. Therefore, a security value x can be represented by the interval $(\frac{x}{2}, 2x)$. The approximate equality relations are thus defined as follows.

$$\forall i \in \{p_m, p_d, p_t\} (x \sim_i y \iff \frac{x}{2} < y < 2x).$$

The fact that this relation satisfies the three requirements from Definition 1 follows from simple algebraic reasoning.

- $(D_i, <_i, \sim_i)_{i \in \{e, c\}}$: Both the number of bits exchanged (e) in the fast phase and the number of cryptographic operations (c) are in the domain of the natural numbers \mathbb{N} . Their approximate equality relations \sim_c and \sim_e are simply the equality in \mathbb{N} .
- $(D_s, <_s, \sim_s)$: Memory (s) is in the domain of the natural numbers \mathbb{N} , and its approximate equality relation is defined by scaling from bits to kilobits. Defining \sim_s in that way is a pragmatic approach based on experience in the field of contactless systems where any saving on a single kilobit is worthy. However, decision makers could use a different relation, based on, e.g., megabytes. Formally, \sim_s is defined as follows.

$$x \sim_s y \iff |x - y| < 1024.$$

- $(D_f, <_f, \sim_f)$: Presence of a final slow phase (f) is a nominal attribute in the Boolean domain. Protocols avoiding this phase are normally designed for low-cost devices [24]. We thus define both the total order and the approximate equality relations as follows.

$$x <_f y \iff x = \text{false} \wedge y = \text{true}.$$

$$x \sim_f y \iff x = y.$$

- $(D_b, <_b, \sim_b)$: Use of a multiple-bit channel (b) is also in the Boolean domain. A single-bit exchange protocol can be easily improved by transforming it to a multiple-bit protocol [2]. Consequently, we define the total order and the approximate equality relation as follows.

$$x <_b y \iff x = \mathbf{false} \wedge y = \mathbf{true}.$$

$$x \sim_b y \iff x = y.$$

3.3. Solution

The methodology introduced in this paper does not aim to identify the best protocol in a general way but, instead, to identify the set of *nondominated protocols*. Intuitively, a nondominated protocol satisfies that it is not possible to improve by moving away from it to another protocol without degrading the result w.r.t. at least one attribute.

Providing a given protocol with attribute values typically requires one to specify values for protocol-specific parameters, *e.g.*, the number of rounds. We thus consider *protocol instances*, which are protocols for which all such parameters have been instantiated and whose attribute values can be unambiguously determined. In order to not introduce additional notation, we simply represent this one-to-many relation from protocols to protocol instances by means of identifiers. In short, a *protocol instance* is a pair (PI, x) where PI is an identifier that uniquely identifies a full-specification of a protocol, and $x \in \Delta$ provides the attribute values for the fully-specified protocol PI . We recall that $\Delta = D_{p_m} \times D_{p_d} \times D_{p_t} \times D_e \times D_c \times D_s \times D_f \times D_b$ is the attribute space defined in Section 3 over the index set $I = \{p_m, p_d, p_t, e, c, s, f, b\}$.

Definition 3 (Solution). *Given a set of protocol instances E , a solution in our methodology is the subset $S \subseteq E$ of maximum cardinality such that for every $(P_x, \bar{x}) \in S$ there does not exist $(P_y, \bar{y}) \in E$ such that $\bar{y} \prec \bar{x}$. We say, in this case, that (PI, \bar{x}) is nondominated in E .*

We also say that a protocol instance (P_x, \bar{x}) dominates another protocol instance (P_y, \bar{y}) if and only if $\bar{x} \prec \bar{y}$. If $\bar{x} \not\prec \bar{y}$, we say that (P_y, \bar{y}) is nondominated by (P_x, \bar{x}) .

To illustrate the nondominated relation between two protocol instances, we make use of spider charts [14]. Spider charts (also known under various other names, such as radar charts) are simple graphs that make it possible to

quickly compare the relative scores of a number of alternatives along various axes. An example of a spider chart is given in Figure 2. There we present two protocol instances: one corresponds to Brands and Chaum’s protocol [10] (labeled “BC- $\{16\}$ ”) when $n = 16$, and the other one to the tree-based protocol [5] (labeled “Tree- $\{16, 8\}$ ”) with depth equal to 8 and $n = 16$. The axes related to the types of fraud are logarithmically scaled from 1 (chart center) to $\log_2(\frac{1}{2^n})$ (chart outer); the axes related to the Boolean attributes are graduated with **true** (chart center) and **false** (chart outer). Finally, the axes concerning memory size and number of cryptographic operations are graduated from 10 (chart center) to 0 (chart outer). In order to focus on the differences between the protocols, we will often only display the attribute axes for which the protocols have different values and the security-related attributes. Consequently, in the current example, we omitted the e and b axes.

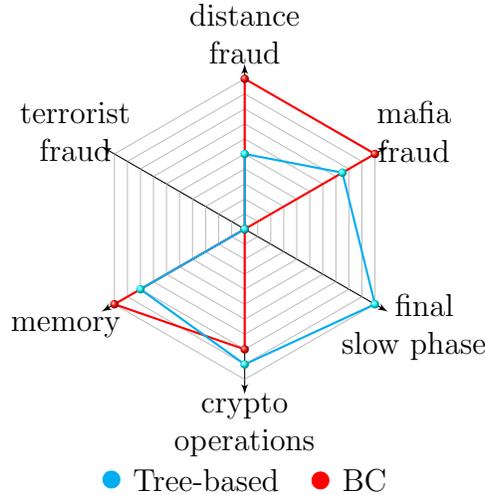


Figure 2: Spider chart for the protocol instances BC- $\{16\}$ and Tree- $\{16, 8\}$.

A solution S , in the sense of Definition 3, can be seen as the set of relevant protocol instances a decision maker should focus on. A similar use can be given by distance bounding protocol designers, whose ultimately goal must be to include their protocols in S w.r.t. some set of criteria. The role of S is empirically illustrated in the next section where several state-of-the-art distance bounding protocols are evaluated and compared by applying our methodology.

4. Methodology applied to current protocols

This section reports on the results obtained after applying our methodology to the protocols listed in Table 1. Instead of computing raw data to be served as input to a state-of-the-art decision making tool, the methodology has been implemented and published as an open source Java project⁵. The computer tool, based on Table 2, comprises the thirteen distance bounding protocols listed in Table 1 so as to generate protocol instances as defined in Section 3. The decision to develop a computer tool is supported by the growing number of distance bounding protocols proposed and the continual refinement of their security analysis [6, 1, 27]. Our tool therefore is aimed at facilitating the addition and modification of new protocols and criteria.

4.1. Protocol instances

Protocol instances are built by assigning values to protocol-specific parameters. In order to create a comprehensive set of protocol instances, we use ranges of values a bit wider than those considered in the literature. For instance, we consider protocols executing from 1 to 256 rounds during the fast phase, while in the literature this number varies from 16 to 64. Other security-related parameters, namely the size of nonces (δ), secret keys (κ), and cryptographic primitives (σ), are considered to be large enough so that attacks based on, for example, short keys, are unfeasible. The remaining parameter values are detailed in Table 3.

Once all parameter values are defined, we use Table 2 to obtain all protocol instances. This leads to a set E of 29184 protocol instances, which is used as input to our methodology.

4.2. Comparison

Comparing is definitely a decision making task. Decisions ought to be made for the sake of providing meaningful results. Nevertheless, the comparison problem differs from classical decision making problems in the role of the decision maker. The former problem should not reflect the point of view of the decision maker, but conciliate decisions and criteria based on a proper understanding of the problem and an exhaustive literature research.

⁵The source code can be freely downloaded from https://github.com/rolandotr/db_comparison

Table 2: Formulas to compute the attribute values for every considered protocol. References to the sources of the formulas are included when applicable. Additional notation is introduced below.

- σ : size of signature, commitment, and MAC.
- δ : size of the random nonces.
- ℓ : depth of the tree in the tree-based approach [5].
- α : number of predefined challenges in KA [26].
- p_f : probability of occurrence of a void-challenge in MP [28].
- t : size of the messages exchanged in the fast phase.

Protocols	p_m	p_d	p_t	f	b	c	s
BC	$(\frac{1}{2})^n$ [10]	$(\frac{1}{2})^n$ [10]	1	Y	Y	2	$2n + 3\sigma$
BB	$(\frac{1}{2})^n$ [11]	$(\frac{1}{2})^n$ [11]	1 [4]	Y	Y	4	$3n + \delta$
MAD	$(\frac{1}{2})^n$ [13]	$(\frac{1}{2})^n$ [13]	1	Y	Y	4	$2n + 2\delta + 5\sigma$
HK	$(\frac{3}{4})^n$ [24]	$(\frac{3}{4})^n$ [33]	1	N	Y	1	$3n + 2\delta$
MP	cf. [1]	cf. [1]	1	Y	Y	2	$4n + 2\delta + \sigma$
Swiss-Knife	$(\frac{1}{2})^n$ [27]	$(\frac{3}{4})^n$ [27]	$(\frac{3}{4})^n$ [27]	Y	Y	2	$3n + 3\delta + 2\sigma$
Tree-based	$\left(\left(\frac{1}{2}\right)^\ell \left(\frac{\ell}{2} + 1\right)\right)^{\lfloor \frac{n}{\ell} \rfloor}$	cf. [33]	1	N	Y	1	$(2^{\ell+1} - 1) \lfloor \frac{n}{\ell} \rfloor + 2\delta + n$
Poulidor	cf. [33]	cf. [33]	1	N	Y	1	$5n + 2\delta$
RC	$(\frac{1}{2})^n$ [29]	$(\frac{1}{2})^n$ [29]	1	Y	N	3	$2\delta + 2\sigma$
YKHL	cf. [3]	$(\frac{7}{8})^n$	1	N	Y	1	$5n + 2\delta$
KA	cf. [26]	$(\frac{3}{4})^{n-\alpha}$ [26]	1	N	Y	1	$4n + 2\delta$
SKI	$(\frac{t+1}{2t})^n$ [9]	$\leq (\frac{3}{4})^n$ [9]	$(\frac{2t-2}{2t})^n$ [9]	N	N	1	$n(t+1) + 2\delta + 2\sigma$
TMA	cf. [31]	cf. [31]	1	N	N	1	$4n + 2\delta$

Table 3: Parameter values for the considered protocols. For the KA protocol we use the parameter p_d instead of α given that $\alpha = \lfloor p_d \times n \rfloor$ [26].

Protocol	Identifier	Parameter values
BC	BC- $\{n\}$	$n \in \{1, \dots, 256\}$
MAD	MAD- $\{n\}$	$n \in \{1, \dots, 256\}$
BB	BB- $\{n\}$	$n \in \{1, \dots, 256\}$
HK	HK- $\{n\}$	$n \in \{1, \dots, 256\}$
MP	MP- $\{n, p_f\}$	$n \in \{1, \dots, 256\}$ $p_f \in \{0, 0.05, 0.01, \dots, 1\}$
Swiss-Knife	Swiss-Knife- $\{n\}$	$n \in \{1, \dots, 256\}$
Tree-based	Tree- $\{n, \ell\}$	$n \in \{1, \dots, 256\}$ $\ell \in \{1, 2, \dots, 32\}$
Poulidor	Poulidor- $\{n\}$	$n \in \{1, \dots, 256\}$
RC	RC- $\{n\}$	$n \in \{1, \dots, 256\}$
YKHL	YKHL- $\{n\}$	$n \in \{1, \dots, 256\}$
KA	KA- $\{n, p_d\}$	$n \in \{1, \dots, 256\}$ $p_d \in \{0, 0.05, 0.01, \dots, 1\}$
SKI	SKI- $\{n, t\}$	$n \in \{1, \dots, 256\}$ $t \in \{2, 3, \dots, 32\}$
TMA	TMA- $\{n\}$	$n \in \{1, \dots, 256\}$

Along this article we have made a couple of decisions already. For instance, distance bounding protocols that fail on achieving any sort of authentication were discarded in Section 2. Section 3 limits the number of considered attributes to 8 by choosing those frequently used in the literature. And Section 4 defines a wide range of parameter values in order to generate a comprehensive set of protocol instances. We claim that all these decisions are consistent with the state-of-the-art in distance bounding and, therefore, keep our experiments as fair as possible.

Our last decision concerns a security criterion: mafia fraud resistance. All distance bounding protocols *must* resist to mafia fraud to some extent. We thus consider different upper-bounds on the probability of success of an adversary mounting this type of fraud. More precisely, given the set E of 29184 protocol instances defined previously and a probability value $y \in [0, 1]$,

we define the set $E[y] = \{(PI, x) \in E | y \leq x_{p_m}\}$ ⁶ containing those protocols whose resistance to mafia fraud is bounded by y . In what follows we do not longer consider the whole set E , but subsets $E[y]$ for different values of y .

To illustrate further the need of this decision let us consider a protocol that does nothing. Because this protocol requires no resource to be implemented, it would be nondominated even though it can be hardly considered a distance bounding protocol. Considering $E[y]$ for some $y < 1$ instead of E , provides a quantifiable security guarantee in terms of mafia fraud that can only be provided by actual distance bounding protocols. Moreover, varying y allows us to see how the set of nondominated protocols evolves when y decreases. Table 4 shows such evolution considering y to range within the set $\{2^{-1}, 2^{-16}, 2^{-32}, 2^{-64}, 2^{-96}, 2^{-128}\}$.

According to Table 4, seven out of the thirteen considered protocols have at least one instance that is nondominated for some set $E[y]$. In this case, we say that these protocols are nondominated. The seven nondominated protocols are BC, KA, SKI, Swiss-Knife, TMA, Poulidor, and Tree-based. We intuitively explain this result as follows.

- BC, BB, MAD, and RC, achieve the optimal security in terms of both mafia and distance fraud (see Figures 4 and 5 in the Appendix). Consequently, none of them can be dominated by any of the remaining nine protocols. However, BC leaves out BB, MAD, and RC, from the set of nondominated protocols because it requires fewer calls to cryptographic functions.
- Swiss-Knife and SKI are the only protocols that resist to terrorist fraud (see Figure 6 in the Appendix). They do not dominate each other as it is illustrated by the Spider Chart 3(b). Both are thus nondominated.
- Tree-based, Poulidor, and TMA, are the best in terms of distance fraud (see Figure 5) among the protocols using single-bit exchanges and a single cryptographic operation. Because they do not dominate each other (see the Spider Chart 3(a)), the three are included in the set of nondominated protocols.

⁶We recall that x is in the attribute space $\Delta = D_{p_m} \times D_{p_d} \times D_{p_t} \times D_e \times D_c \times D_s \times D_f \times D_b$ and $x_i \in D_i$ for every $i \in \{p_m, p_d, p_t, e, c, s, f, b\}$.

Table 4: Nondominated protocol instances for different sets $E[y]$. Every security value p and memory value m has been scaled according to the equations $2^{\lceil \log_2 p \rceil}$ and $\lfloor m/1024 \rfloor$ respectively. For the sake of compactness, this table only shows for each protocol the nondominated protocol instance (if any) with fewer bits exchanged during the fast phase. The total number of nondominated protocols is given in the last column.

y	Nondominated Prot. Instances	Attribute values								total
		n	p_m	p_d	p_t	b	c	s	f	
2^{-1}	BC- $\{1\}$	1	2^{-1}	2^{-1}	2^0	false	2	0Kb	true	256
	KA- $\{2, 0.5\}$	2	2^{-1}	2^{-0}	2^0	false	1	0Kb	false	10
	SKI- $\{3, 2\}$	3	2^{-1}	2^{-1}	2^{-3}	true	1	1Kb	false	254
	SwissKnife- $\{1\}$	1	2^{-1}	2^{-0}	2^{-0}	false	2	1Kb	true	255
	TMA- $\{2\}$	2	2^{-1}	2^{-1}	2^0	false	1	0Kb	false	1
	Tree- $\{2, 2\}$	2	2^{-1}	2^{-0}	2^0	false	1	0Kb	false	400
2^{-16}	BC- $\{16\}$	16	2^{-16}	2^{-16}	2^0	false	2	0Kb	true	241
	KA- $\{22, 0.55\}$	22	2^{-16}	2^{-4}	2^0	false	1	0Kb	false	4
	Poullidor- $\{23\}$	23	2^{-16}	2^{-8}	2^0	false	1	0Kb	false	1
	SKI- $\{39, 2\}$	39	2^{-16}	2^{-16}	2^{-39}	true	1	0Kb	false	218
	SwissKnife- $\{16\}$	16	2^{-16}	2^{-6}	2^{-6}	false	2	0Kb	true	241
	TMA- $\{27\}$	27	2^{-16}	2^{-16}	2^0	false	1	0Kb	false	1
Tree- $\{24, 6\}$	24	2^{-16}	2^{-10}	2^0	false	1	0Kb	false	394	
2^{-32}	BC- $\{32\}$	32	2^{-32}	2^{-32}	2^0	false	2	0Kb	true	225
	KA- $\{37, 0.85\}$	37	2^{-32}	2^{-2}	2^0	false	1	0Kb	false	2
	Poullidor- $\{42\}$	42	2^{-32}	2^{-16}	2^0	false	1	0Kb	false	1
	SKI- $\{78, 2\}$	78	2^{-32}	2^{-32}	2^{-78}	true	1	0Kb	false	179
	SwissKnife- $\{32\}$	32	2^{-32}	2^{-13}	2^{-13}	false	2	0Kb	true	225
	TMA- $\{53\}$	53	2^{-32}	2^{-32}	2^0	false	1	0Kb	false	1
Tree- $\{48, 6\}$	48	2^{-32}	2^{-21}	2^0	false	1	1Kb	false	368	
2^{-64}	BC- $\{64\}$	64	2^{-64}	2^{-64}	2^0	false	2	0Kb	true	193
	KA- $\{73, 0.8\}$	73	2^{-64}	2^{-6}	2^0	false	1	0Kb	false	4
	Poullidor- $\{78\}$	78	2^{-64}	2^{-32}	2^0	false	1	0Kb	false	1
	SKI- $\{155, 2\}$	155	2^{-64}	2^{-64}	2^{-155}	true	1	0Kb	false	102
	SwissKnife- $\{64\}$	64	2^{-64}	2^{-26}	2^{-26}	false	2	0Kb	true	193
	TMA- $\{106\}$	106	2^{-64}	2^{-64}	2^0	false	1	0Kb	false	1
Tree- $\{96, 6\}$	96	2^{-64}	2^{-43}	2^0	false	1	2Kb	false	295	
2^{-96}	BC- $\{96\}$	96	2^{-96}	2^{-96}	2^0	false	2	0Kb	true	161
	KA- $\{113, 0.75\}$	113	2^{-96}	2^{-12}	2^0	false	1	0Kb	false	5
	Poullidor- $\{114\}$	114	2^{-96}	2^{-49}	2^0	false	1	0Kb	false	1
	SKI- $\{232, 2\}$	232	2^{-96}	2^{-96}	2^{-232}	true	1	1Kb	false	25
	SwissKnife- $\{96\}$	96	2^{-96}	2^{-39}	2^{-39}	false	2	1Kb	true	161
	TMA- $\{158\}$	158	2^{-96}	2^{-96}	2^0	false	1	0Kb	false	1
Tree- $\{144, 6\}$	144	2^{-96}	2^{-64}	2^0	false	1	3Kb	false	223	
2^{-128}	BC- $\{128\}$	128	2^{-128}	2^{-128}	2^0	false	2	0Kb	true	129
	KA- $\{145, 0.8\}$	145	2^{-128}	2^{-12}	2^0	false	1	0Kb	false	4
	Poullidor- $\{148\}$	148	2^{-128}	2^{-15}	2^0	false	1	0Kb	false	1
	SKI- $\{219, 3\}$	219	2^{-128}	2^{-90}	2^{-128}	true	1	1Kb	false	1
	SwissKnife- $\{128\}$	128	2^{-128}	2^{-53}	2^{-53}	false	2	1Kb	true	129
	TMA- $\{210\}$	210	2^{-128}	2^{-128}	2^0	false	1	1Kb	false	1
Tree- $\{160, 16\}$	160	2^{-128}	2^{-77}	2^0	false	1	1280Kb	false	150	

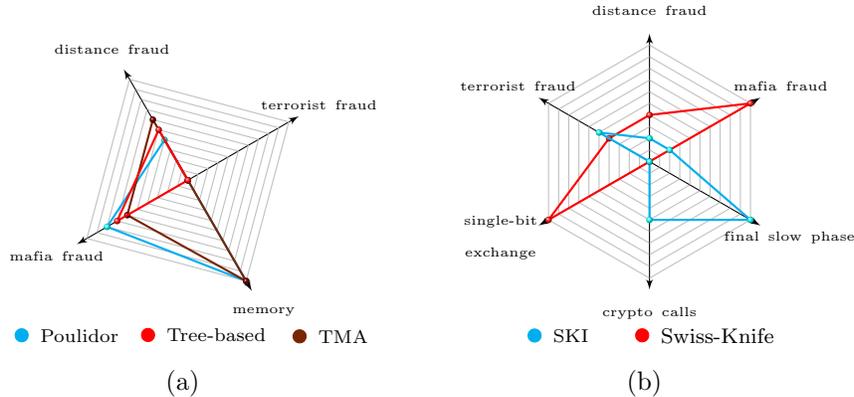


Figure 3: Two spider charts showing nondominated protocol instances. Figure 3(a) considers the protocol instances Tree-based- $\{128\}$, Poulidor- $\{128\}$, and TMA- $\{128\}$. Figure 3(b) considers the protocol instances Swiss-Knife- $\{128\}$ and SKI- $\{64, 2\}$. All axes have been normalized with respect to an ideal protocol instance executing 128 rounds that takes the optimal value for each attribute.

- KA does not perform well in terms of distance fraud (see Figure 5). However, its resistance to mafia fraud can be as good as the one provided by the Tree-based protocol without demanding an exponential amount of memory (see Figure 4). Therefore, KA is also nondominated.

It is worth remarking that, according to Table 4, the set of nondominated protocols is rather stable with y . The only exception is Poulidor, that becomes a member of the set of nondominated protocols for $y \leq 2^{-16}$. This behavior is likely to be due to the fact that the actual distance fraud resistance of the Poulidor protocol cannot be computed yet [33, 32], but an upper-bound only.

5. Conclusion

In this article, we have proposed a methodology to evaluate and compare distance bounding protocols. The methodology benefits from experiences in the decision making field, and defines the most relevant attributes that ought to be considered in terms of security and implementability. An open-source computer software implementing our methodology has been released, which supported the evaluation and comparison of thirteen state-of-the-art distance

bounding protocols. Among the evaluated protocols, only seven are relevant (nondominated) in terms of the considered criteria, namely resistance to mafia, distance, and terrorist fraud, number of cryptographic operations, memory, presence of a final slow phase, and use of a multiple-bit channel. Clearly, most disqualified protocols had an important role in the evolution of distance bounding protocols, but they are obsolete today. Future designs of distance bounding protocols must, therefore, prove to be nondominated with respect to a set of relevant criteria. Our results also show that the asymptotic analysis of distance bounding protocols, as done commonly in the literature, is inadequate and misleading. Finally, a clear side effect of our methodology is that it can be used for ad-hoc decision making where the decision maker is free to prioritize some attributes over others.

References

- [1] Gildas Avoine, Muhammed Ali Bingöl, Süleyman Kardaş, Cédric Lauradoux, and Benjamin Martin. A framework for analyzing RFID distance bounding protocols. *Journal of Computer Security – Special Issue on RFID System Security*, 19(2):289–317, March 2011.
- [2] Gildas Avoine, Christian Floerkemeier, and Benjamin Martin. RFID Distance Bounding Multistate Enhancement. *The 10th International Conference on Cryptology in India – Indocrypt’09*, pages 290–307, New Delhi, India, 2009.
- [3] Gildas Avoine and Chong Hee Kim. Mutual distance bounding protocols. *IEEE Transactions on Mobile Computing*, 12(5):830–839, May 2013.
- [4] Gildas Avoine, Cédric Lauradoux, and Benjamin Martin. How secret-sharing can defeat terrorist fraud. *The 4th ACM Conference on Wireless Network Security – WiSec’11*, pages 145–156, Hamburg, Germany, 2011.
- [5] Gildas Avoine and Aslan Tchamkerten. An efficient distance bounding RFID authentication protocol: balancing false-acceptance rate and memory requirement. *Information Security Conference – ISC’09*, pages 250–261, Pisa, Italy, 2009.

- [6] Asli Bay, Ioana Cristina Boureanu, Aikaterini Mitrokotsa, Iosif-Daniel Spulber, and Serge Vaudenay. The Bussard-Bagga and other distance-bounding protocols under attacks. *The 8th China International Conference on Information Security and Cryptology – Inscrypt’12*, pages 371–391, Beijing, China, 2012.
- [7] 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.
- [8] Thomas Beth and Yvo Desmedt. Identification tokens - or: Solving the chess grandmaster problem. *Advances in Cryptology – CRYPTO ’90*, pages 169–177, Santa Barbara, California, USA, 1990.
- [9] Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. Secure and lightweight distance-bounding. *The 2nd International Workshop on Lightweight Cryptography for Security and Privacy – LightSec’13*, pages 97–113, Gebze, Turkey, 2013.
- [10] Stefan Brands and David Chaum. Distance-bounding protocols. *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology – EUROCRYPT’93*, pages 344–359, Secaucus, NJ, USA, 1994.
- [11] Laurent Bussard and Walid Bagga. Distance-bounding proof of knowledge to avoid real-time attacks. *Security and Privacy in the Age of Ubiquitous Computing*, pages 223–238, Chiba, Japan, 005.
- [12] Bundpol Security Systems. Car Locksmith Tools. <http://www.bundpol.com/>, 2014.
- [13] Srdjan Čapkun, Levente Buttyán, and Jean-Pierre Hubaux. SECTOR: Secure tracking of node encounters in multi-hop wireless networks. *The 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, SASN ’03, pages 21–32, New York, NY, USA, 2003.
- [14] John M. Chambers, William S. Cleveland, Paul A. Tukey, and Beat Kleine. *Graphical Methods for Data Analysis*. CA: Wadsworth, 1983.
- [15] John H. Conway. *On Numbers and Games*. AK Peters, Ltd., 2nd edition, 2000.

- [16] Cas Cremers, Kasper B. Rasmussen, Benedikt Schmidt, and Srdjan Čapkun. Distance hijacking attacks on distance bounding protocols. *The 2012 IEEE Symposium on Security and Privacy*, pages 113–127, Washington, DC, USA, 2012.
- [17] Yvo Desmedt, Claude Goutier, and Samy Bengio. Special uses and abuses of the fiat-shamir passport protocol. *Advances in Cryptology – CRYPTO’87*, pages 21–39, Santa Barbara, California, USA, 1988.
- [18] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. *Advances in Cryptology – CRYPTO’86*, pages 186–194, Santa Barbara, California, USA, 1986.
- [19] Aurélien Francillon, Boris Danev, and Srdjan Čapkun. Relay attacks on passive keyless entry and start systems in modern cars. *Network and Distributed System Security Symposium*, San Diego, California, USA, 2011.
- [20] Lishoy Francis, Gerhard P. Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical NFC peer-to-peer relay attack using mobile phones. *Workshop on RFID Security – RFIDSec’10*, pages 35–49, Istanbul, Turkey, 2010.
- [21] James Gleick. A new approach to protecting secrets is discovered. *The New York Times*, February, 17th 1987.
- [22] Gerhard P. Hancke. Practical attacks on proximity identification systems (short paper). *The 2006 IEEE Symposium on Security and Privacy*, pages 328–333, Washington, DC, USA, 2006.
- [23] Gerhard P. Hancke and Markus Kuhn. Attacks on Time-of-Flight Distance Bounding Channels. *The 1st ACM Conference on Wireless Network Security – WiSec’08*, pages 194–202, Alexandria, Virginia, USA, 2008.
- [24] Gerhard P. Hancke and Markus G. Kuhn. An RFID distance bounding protocol. *The First International Conference on Security and Privacy for Emerging Areas in Communications Networks – SECURECOMM ’05*, pages 67–73, Washington, DC, USA, 2005.

- [25] Chong Hee Kim and Gildas Avoine. RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks. *The 8th International Conference on Cryptology And Network Security – CANS’09*, pages 119–133, Kanazawa, Ishikawa, Japan, 2009.
- [26] Chong Hee Kim and Gildas Avoine. RFID distance bounding protocols with mixed challenges. *IEEE Transactions on Wireless Communications*, 10(5):1618–1626, May 2011.
- [27] Chong Hee Kim, Gildas Avoine, François Koeune, François-Xavier Standaert, and Olivier Pereira. The Swiss-knife RFID distance bounding protocol. *International Conference on Information Security and Cryptology – ICISC 2008*, pages 98–115, Seoul, Korea, 2008. Springer.
- [28] 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.
- [29] Kasper B. Rasmussen and Srdjan Čapkun. Realization of RF distance bounding. *19th USENIX Security Symposium – USENIX’10*, Washington, DC, USA, August 2010.
- [30] Douglas R. Stinson. *Cryptography – theory and practice*. CRC Press, 1995.
- [31] Rolando Trujillo-Rasua, Benjamin Martin, and Gildas Avoine. Distance-bounding facing both mafia and distance frauds. *IEEE Transactions on Wireless Communications*, 3(10): 5690–5698, 2014.
- [32] Rolando Trujillo-Rasua. Complexity of distance fraud attacks in graph-based distance bounding. *The 10th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services – MobiQ-uitous’13*, pages 289–302, Tokyo, Japan, 2013.
- [33] Rolando Trujillo-Rasua, Benjamin Martin, and Gildas Avoine. The Poulidor distance-bounding protocol. *Workshop on RFID Security – RFIDSec’10*, pages 239–257, Istanbul, Turkey, 2010.
- [34] Dae Hyun Yum, Jin Seok Kim, Sung-Je Hong, and Pil Joong Lee. Distance bounding protocol for mutual authentication. *IEEE Transactions on Wireless Communications*, 10(2):592–601, February 2011.

Appendix

Figures 4, 5, and 6, depict the resistance of each protocol to mafia, distance, and terrorist fraud respectively. The attribute value for each fraud come from the protocol instance that minimizes it. For example, given $e = 32$, the resistance to mafia fraud of the KA protocol is taken from the protocol instance KA- $\{32, 1\}$. On the contrary, its distance fraud resistance considering again $e = 32$ is taken from the protocol instance KA- $\{32, 0\}$.

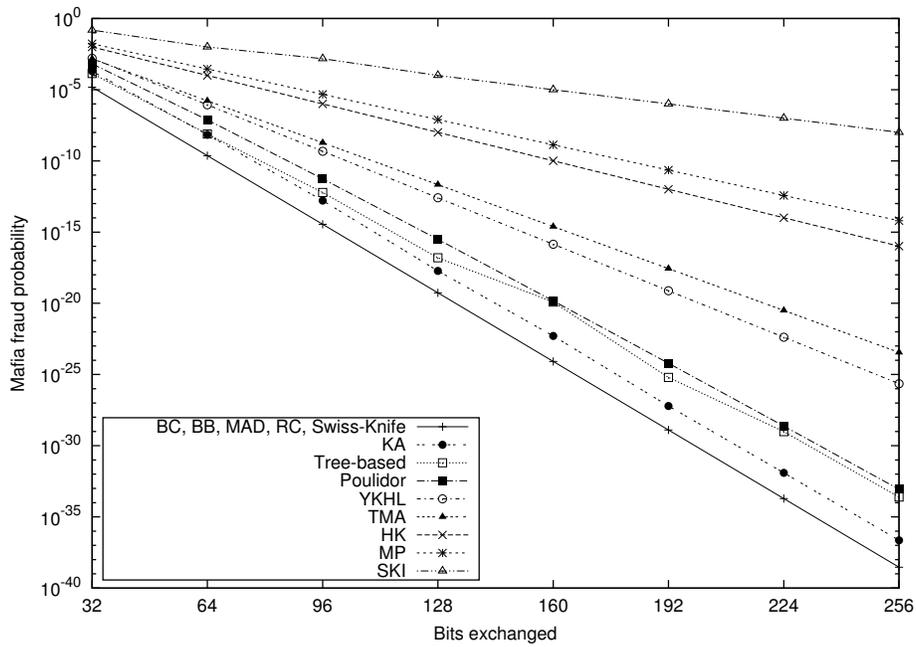


Figure 4: Mafia fraud resistance of the considered protocols for $e \in \{32, 64, \dots, 258\}$.

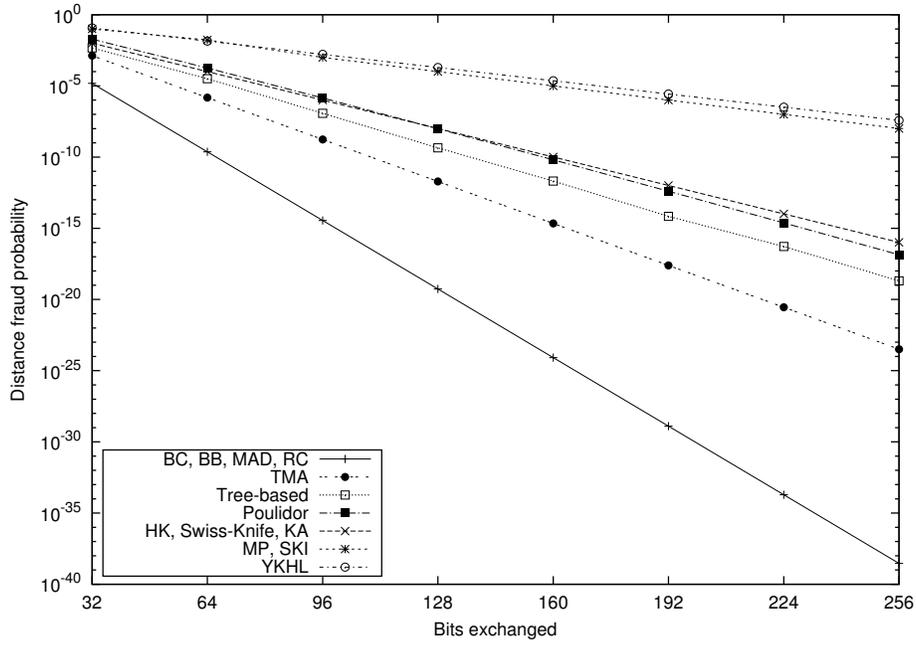


Figure 5: Distance fraud resistance of the considered protocols for $e \in \{32, 64, \dots, 258\}$.

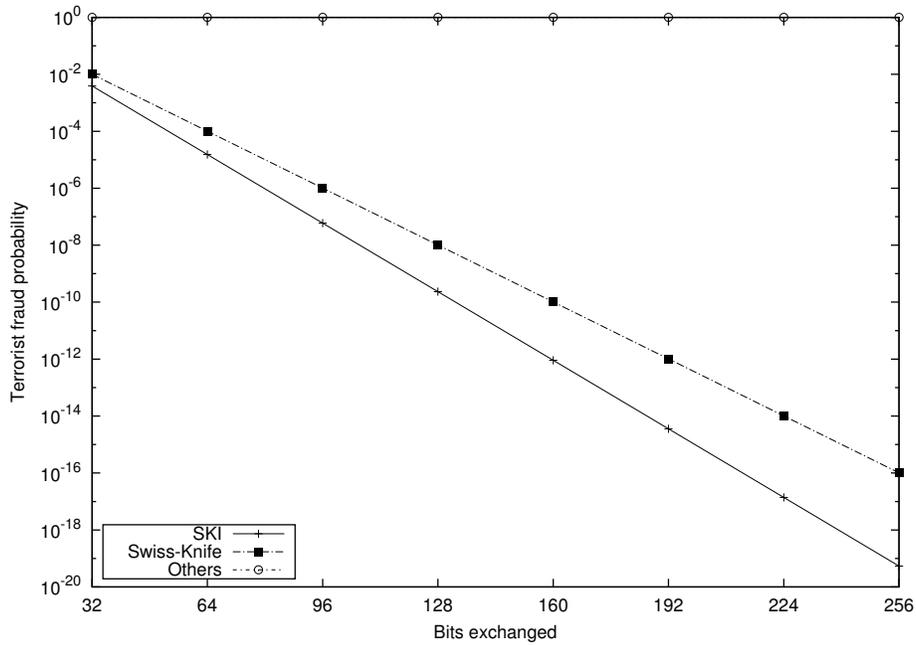


Figure 6: Terrorist fraud resistance of the considered protocols for $e \in \{32, 64, \dots, 258\}$.