Towards Secure Distance Bounding*

Ioana Boureanu[1], Aikaterini Mitrokotsa[2], and Serge Vaudenay[1]

[1] EPFL
CH-1015 Lausanne, Switzerland
http://lasec.epfl.ch
[2] University of Applied Sciences of Western Switzerland (HES-SO)
CH-1227 Geneva, Switzerland
katerina.mitrokotsa@hesge.ch

Abstract. Relay attacks (and, more generally, man-in-the-middle attacks) are a serious threat against many access control and payment schemes. In this work, we present distance-bounding protocols, how these can deter relay attacks, and the security models formalizing these protocols. We show several pitfalls making existing protocols insecure (or at least, vulnerable, in some cases). Then, we introduce the SKI protocol which enjoys resistance to all popular attack-models and features provable security. As far as we know, this is the first protocol with such all-encompassing security guarantees.

1 Why Distance-Bounding?

It is well known that a chess beginner can win against a chess grand-master easily by defeating two grand-masters concurrently, taking different colors in both games, and relaying the move of one master to the other. This is a pure *relay attack* where two masters play against each other while each of them thinks he is playing against a beginner.

In real life, relay attacks find applications in access control. For instance, a car with a wireless key can be opened by relaying the communication between the key (the token) and the car. RFID-based access control to buildings can also be subject to relay attacks [21]. The same goes for (contactless) credit-card payments: a customer may try to pay for something on a malicious terminal which relays to a fake card paying for something more expensive [15].

To defeat relay attacks, Brands and Chaum [9] introduced the notion of *distance bounding protocol*. This relies on the fact that information is local and it cannot travel faster than light. So, an RFID reader can identify when participants are close enough because the round-trip communication time has been small enough. The idea is that a *prover* holding a key x proves to a *verifier* that he is close to him. Ideally, this notion should behave like a traditional interactive proof system in the sense that it must satisfy:

- completeness (i.e., an honest prover close to the verifier will pass the protocol with high probability)

* This invited paper summarizes results from [4,5,6,7,8].

– soundness (i.e., if the verifier accepts the protocol, then it must be the case that the information held by all close participants includes x)
– security (i.e., if the prover honestly runs the protocol, the provided information does not provide any advantage to defeat soundness).

The last property is weaker than zero-knowledge and is generally required in *identification protocols*. In practice, the literature does not define distance-bounding like this but rather considers several popular threat models, as per the following summary.

– *Distance fraud* [9]: a far-away malicious prover tries to pass the protocol.
– *Mafia fraud* [14]: an adversary between a far-away honest prover and a verifier tries to get advantage of his position to make the verifier accept. (This generalizes relay attacks as the adversary may also modify messages.)
– *Terrorist fraud* [14]: a far-away malicious prover, with the help of an adversary, tries to make the verifier accept, but without giving the adversary any advantage to later pass the protocol alone. For instance, the malicious prover wants to make the verifier accept, although he is far away, but does not want to give his secret x to the adversary.
– *Impersonation fraud* [3]: An adversary tries to impersonate the prover and make the verifier accept.
– *Distance hijacking* [13]: A far-away prover takes advantage of some honest provers running the protocol to make the verifier accept.

In our model [8], we factor all these common threats into three possible frauds.

– *Distance fraud*: this is the classical notion in which we also consider concurrency with many other participants. I.e., we include other possible provers (with other secrets) and verifiers. Consequently, our generalized distance fraud also includes distance hijacking.
– *Man-in-the-middle*: we consider an adversary (maybe at several locations) who can interact with many honest provers (possibly with different keys) and verifiers during a *learning phase*. Then, the *attack phase* contains honest provers with the key x, far away from a verifier V, and possibly many other honest provers (with other keys) and other verifiers. The goal of the adversary is to make V accept the prover holding x. Clearly, this generalizes mafia fraud and includes impersonation fraud.
– *Collusion fraud*: A far-away prover holding x helps an adversary to make the verifier accept the proof. This might be in the presence of many other honest participants. However, there should be no man-in-the-middle attack constructed based on this malicious prover. I.e., the adversary should not extract from him any advantage to run (later) a man-in-the-middle attack.

Ideally, we could just keep this last notion which includes all others and is closer to the soundness and the security notion in the interactive proof system.

We summarize the best security results for many existing distance-bounding protocols. Table 1 gives the probability of success of the best known attacks. This table does not consider possibly bad pseudorandom function (PRF) instances [5] nor any terrorist fraud based on noise tolerance [19]. These aspects will be discussed later in the present paper. For collusion-frauds, we consider a prover leaking all but ν bits of his secret.

Table 1. Best Attack Results on Existing Distance-Bounding Protocols [7]

Protocol	Success Probability					
	Distance-Fraud		MIM		Collusion-Fraud	
Brands & Chaum [9]	$(1/2)^n$	[18]	$(1/2)^n$	[25]	1	[25]
Bussard & Bagga [10]	1	[4]	$(1/2)^n$	[10]	1	[4]
Čapkun *et al.* (SECTOR) [11]	$(1/2)^n$	[18]	$(1/2)^n$	[25]	1	[25]
Hancke & Kuhn [20]	$(3/4)^n$	[18]	$(3/4)^n$	[25]	1	[25]
Reid *et al.* [34]	$(3/4)^n$	[18]	$(3/4)^n$ or 1	[26,4]	$(3/4)^v$	[25]
Singelée & Preneel [35]	$(1/2)^n$	[18]	$(1/2)^n$	[25]	1	[25]
Tu & Piramuthu [36]	$(3/4)^n$	[30]	1	[25]	$(3/4)^v$	[30]
Munilla & Peinado [29]	$(3/4)^n$	[18]	$(3/5)^n$	[18]	1	[18]
Swiss-Knife [25]	$(3/4)^n$	[25]	$(1/2)^n$	[25]	$(3/4)^v$	[25]
Kim & Avoine [24]	$(7/8)^n$	[18]	$(1/2)^n$	[18]	1	[18]
Nikov & Vauclair [31]	$1/k^*$	[25]	$(1/2)^n$	[25]	1	[25]
Avoine *et al.* [2]	$(3/4)^n$	[2]	$(2/3)^n$	[2]	$(2/3)^v$	[2]

* k is an additional parameter in this protocol.

2 Towards a Secure Protocol

We first look at the Hancke-Kuhn protocol [20] in Fig. 1. Here, we use a symmetric key x and two vectors a_1, a_2 of n bits which are derived from an exchange of nonces. Then, the distance bounding phase proceeds in n rounds. In each round, the verifier selects a random $c_i \in \{1,2\}$, sends it to the prover and expects to receive r_i, the ith bit of a_{c_i}. The verifier measures the round-trip communication time and rejects the proof if it took too long to respond or the response is incorrect.

This protocol is vulnerable to a trivial terrorist fraud (actually, it was not meant to resist to it): the malicious prover does the initial phase which is not time-critical, then gives a_1 and a_2 to the adversary who can become a proxy for the prover to the verifier. Clearly, a_1 and a_2 do not leak x.

To fix this problem, Reid *et al.* [34] introduce the protocol in Fig. 2 which we call DBENC in [5]. Here, only a_1 is derived from the initial nonces and a_2 is set to $a_1 \oplus x$. So, a malicious prover providing a_1 and a_2 to an adversary would also leak x.

First of all, we stress that nonces must really be "numbers once used", as their name suggests. I.e., they shall not repeat. Otherwise, this protocol (as well as many others) would leak some sensitive information, as noticed in [28].

Second, we observe that this protocol unfortunately becomes vulnerable to a man-in-the-middle attack [25]. The idea of the attack is that the adversary relays, during a learning phase, the communication between a close prover and a verifier, but flips one challenge c_j. The value r_j which is sent as a response to the verifier is selected at random. So, from the prover, the adversary learns the response to c_j, and by the final output of the verifier (acceptance or rejection), the adversary deduces what is the correct answer to $1 - c_j$. So, he learns the jth bit of a_1 and a_2 and deduces x_j. He can repeat this for each j and infer x. Then, the attack phase just impersonates the prover to

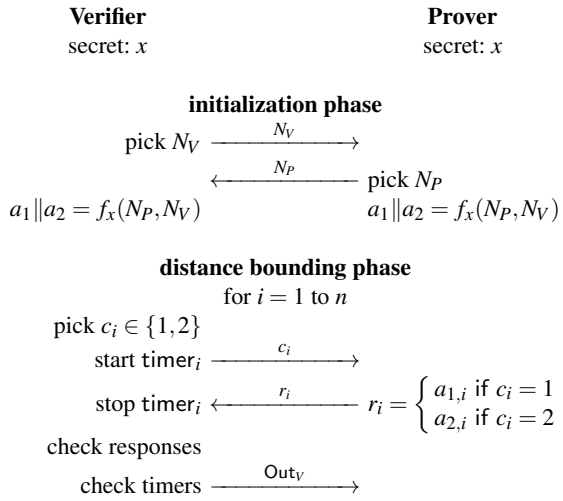

Fig. 1. The Hancke-Kuhn Distance-Bounding protocol [20]

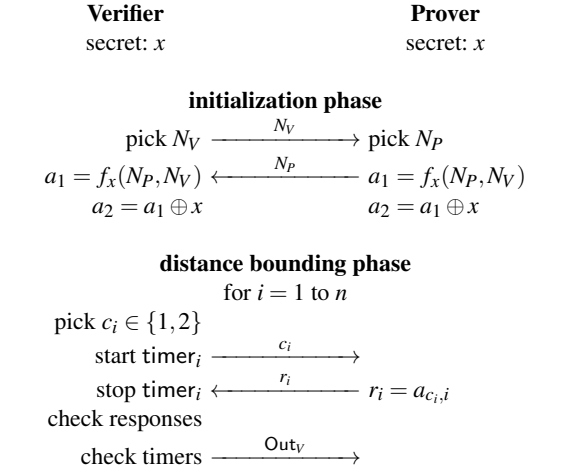

Fig. 2. The DBENC Distance-Bounding protocol [34,5]

the verifier, thanks to x. Other instances of DBENC where $a_2 = a_1 \oplus x$ are replaced by addition modulo some q or addition with a random factor, can also be broken, as shown in [4].

In [28], it was suggested to replace $a_1 = f_x(N_P, N_V)$ and $a_2 = a_1 \oplus x$ by $a_1 \| a_2 = f_x(N_P, N_V)$ and a release of $(R, x \oplus h_R(a_1, a_2))$ for some random R, where h is a universal hash function. However, proving the security of such a protocol does not seem to be easy.

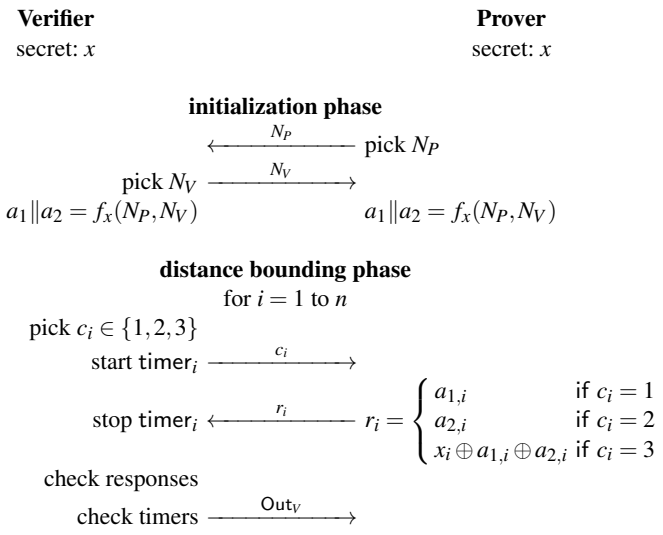

Fig. 3. The TDB Distance-Bounding protocol [2]

The problem seems more easily amended by considering the TDB protocol [2] in Fig. 3. Now, there are three possible challenges $c_i \in \{1,2,3\}$. The answer to 1 and to 2 consists of bits from a_1 and a_2, respectively. Both a_1 and a_2 are derived from the nonces. The answer to 3 is a bit from $a_3 = a_1 \oplus a_2 \oplus x$. The main idea is that we use a threshold secret-sharing scheme to split x_i into three shares, so that two shares alone leak no information.

The security of TDB assumes that f is a PRF. Unfortunately, this assumption alone is not enough to guarantee the security and some related security results from the literature are incorrect. Indeed, as shown in [5], we can artificially construct PRFs which make the protocol insecure. The PRF construction is done by *PRF programming*. For instance, given a PRF g, we construct a new function f defined by the following instances:

$$f_x(N_P, N_V) = \begin{cases} x \| x & \text{if } N_P = x \\ g_x(N_P, N_V) & \text{otherwise} \end{cases}$$

We can easily show that f is also a PRF [5]. When the TDB protocol is instantiated with this f, a malicious prover can mount a distance fraud by selecting $N_P = x$. Indeed, we

would have $a_1 = a_2 = a_3$. So, the response r_i is predicted before receiving the challenge c_i. Consequently, the prover can make sure that the response arrives on time, without even knowing c_i: he just replies before receiving c_i.

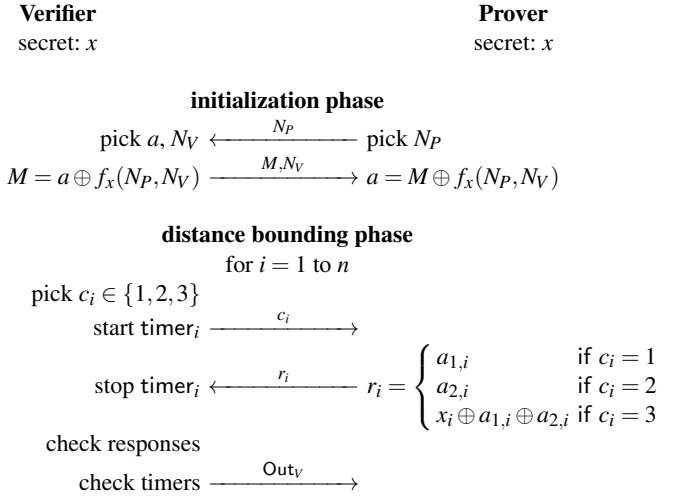

Fig. 4. The TDB Distance-Bounding protocol with PRF Masking [5]

We fix this PRF-based problem by using PRF masking [5,7,8] as shown in Fig. 4. There, the vectors a are chosen by the verifier. So, the malicious prover cannot induce some properties onto a to mount distance frauds.

But, we can also mount a man-in-the-middle attack by PRF programming. Given a PRF g, we first define a predicate $\mathsf{trapdoor}_x(\bar{\alpha}\|t) \iff t = g_x(\bar{\alpha}) \oplus \mathsf{right\_half}(x)$. It must be hard, by playing with a g_x oracle, to construct a string satisfying this predicate. However, when playing with the prover in a learning phase, and using the challenges $c = (1,\ldots,1,3,\ldots,3)$, the adversary obtains such a string $\bar{\alpha}$. We define

$$f_x(N_P, N_V) = \begin{cases} a_1 \| a_2 = \alpha\|\beta\|\gamma\|\beta \oplus g_x(\alpha) & \text{if } \neg\mathsf{trapdoor}_x(N_V) \\ & \text{where } (\alpha,\beta,\gamma) = g_x(N_P, N_V) \\ a_1 \| a_2 = x\|x & \text{otherwise} \end{cases}$$

We can easily see that f is a PRF. Then, the learning phase works as follows:

1: play with P and send $c = (1,\ldots,1,3,\ldots,3)$ to obtain from the responses $\bar{\alpha}\|t$ satisfying $\mathsf{trapdoor}_x$
2: play with P again with $N_V = \bar{\alpha}\|t$ and get x

Based on x, the adversary can impersonate the prover.

In [5], we report other protocols which are weak, with respect to PRF programming (see Table 2).

We do not fix this problem by primarily proposing another protocol but by firstly requiring a new security assumption on the PRF f. Indeed, we somehow require that

Table 2. Protocol which can be Broken by PRF Programming Techniques [5]

Protocol	Distance-Fraud	MIM
TDB Avoine-Lauradoux-Martin [2]	$\surd$	$\surd$
Dürholz-Fischlin-Kasper-Onete [17]	$\surd$	–
Hancke-Kuhn [20]	$\surd$	–
Avoine-Tchamkerten [3]	$\surd$	–
Reid-Nieto-Tang-Senadji [34]	$\surd$	$\surd$
Swiss-Knife Kim-Avoine-Koeune-Standaert-Pereira [25]	–	$\surd$

leaking $f_x(y)$, sometimes $f_x(y) \oplus x$, and sometimes a mixture of both, does not compromise the security. More precisely, we require the (ε, T)-*circular keying* property [8]. This assumes that an adversary $\mathcal{A}$ of complexity at most T making queries of the form (y_i, a_i, b_i) to an oracle

$$y, a, b \mapsto (a \cdot x') + (b \cdot f_x(y))$$

cannot distinguish (up to an advantage ε) whether x and x' have been selected by having $x = x'$ or x and x' are independent. To make it possible, the adversary must follow the constraint that for each $i_1, \ldots, i_q, c_1, \ldots, c_q$ satisfying $y_{i_1} = \cdots = y_{i_q}$ and $\sum_{j=1}^{q} c_j b_{i_j} = 0$, we have that $\sum_{j=1}^{q} c_j a_{i_j} = 0$. As a sanity check, we prove that this notion makes sense by constructing a circular-keying secure PRF in the random oracle model [8]. Furthermore, this property excludes programmed PRFs as per mentioned before.

All the previous protocols assume that there is no noise to harm the protocol execution. However, the distance bounding phase is subject to high constraints. Indeed, an allowed error of one microsecond in the time measurement will correspond to an imprecision of 300 meters in the distance estimate, due to the speed of light. Clearly, this may not defeat relay attacks. To reach a precision of 10 meters, the prover shall not spend more than 33 nanoseconds for receiving c_i, computing r_i, and sending r_i. So, computation or transmission will eventually be subject to noise. To keep the completeness property, we need to tolerate a linear number of errors, depending on the noise level. Thus, in the following protocol (depicted on Fig. 5), only τ out of n rounds should be correct for a successful run of the protocol.

As noticed by Hancke [19], this introduces a new vulnerability to terrorist fraud. The idea of his attack is that the malicious prover will run the initialization phase, then for τ out of n values of i he will reveal the response function $c_i \mapsto r_i$ to the adversary. This will only leak τ bits of x which is not enough to impersonate the prover. Then, the adversary will be able to correctly answer τ rounds to pass the protocol. (To make the attack work, the selection of the τ out of n values of i must be fixed.)

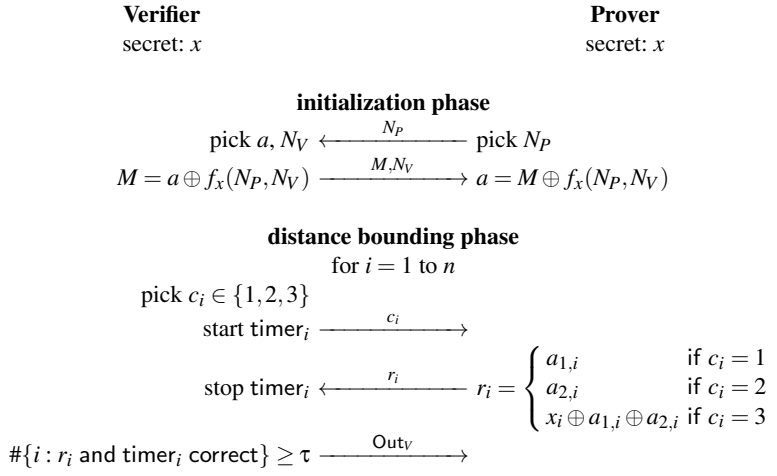

Fig. 5. The TDB Distance-Bounding protocol with PRF Masking and Noise Tolerance

3 The SKI Protocol

To address all previously noticed vulnerabilities, we introduce the SKI protocol.[1] This protocol appeared in [7,8]. It enjoys provable security. The protocol is depicted in Fig. 6. There, the function f must be a PRF with circular-keying security.

Given a vector μ, the linear function L_μ is defined by

$$L_\mu(x) = (\mu \cdot x, \ldots, \mu \cdot x)$$

Namely, all bits are set to the dot product between μ and x. With $x' = L_\mu(x)$, Hancke's terrorist fraud would reveal a majority of the bits of x' thus leaking $L_\mu(x)$. Since L_μ is not chosen by the prover, by repeating the attack, we can collect enough information about x to reconstruct x. So, Hancke's terrorist fraud is prevented.

We let s denote the bit-length of the secret x. I.e., it is no longer necessarily equal to n, the number of rounds.

We define the following function:

$$B(n, \tau, q) = \sum_{i=\tau}^{n} \binom{n}{i} q^i (1-q)^{n-i}$$

To study *completeness*, we assume that there is a probability of p_{noise} that one round is incorrectly executed by honest players. The probability that an honest prover, close to the verifier, passes the protocol is $B(n, \tau, 1 - p_{\mathsf{noise}})$. By using the Chernoff bound [12], this is greater than $1 - e^{-2\varepsilon^2 n}$ for

$$\frac{\tau}{n} < 1 - p_{\mathsf{noise}} - \varepsilon \tag{1}$$

[1] The name *SKI* comes from the first names of the authors: Serge, Katerina, and Ioana.

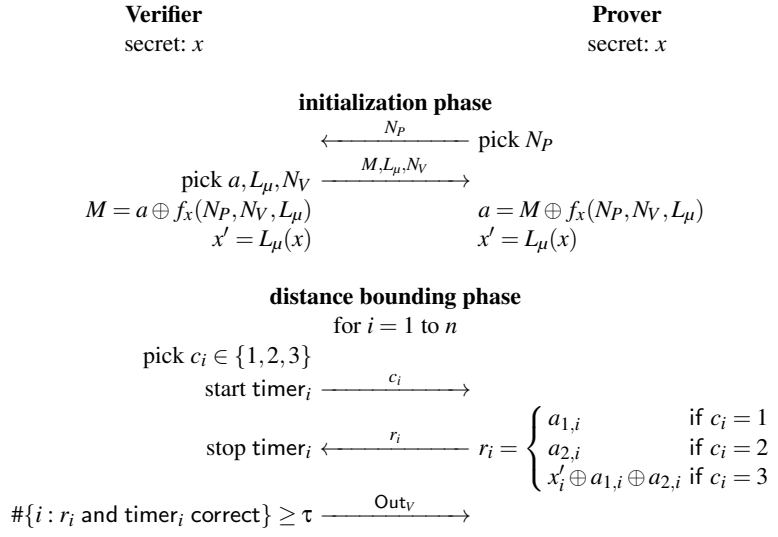

Fig. 6. The SKI Distance-Bounding Protocol [7,8]

We now describe the best distance fraud against SKI. The malicious prover just runs the initialization phase. During the distance-bounding phase, he anticipates the challenge c_i by sending some r_i such that r_i has the largest preimage set by the $c_i \mapsto r_i$ response function. This maximizes the chances to win. We can easily see that a single round will pass with probability $\frac{3}{4}$. So, the distance fraud succeeds with probability $B(n, \tau, \frac{3}{4})$. By using the Chernoff bound, this is lower than $e^{-2\varepsilon^2 n}$ when

$$\frac{\tau}{n} > \frac{3}{4} + \varepsilon \tag{2}$$

The best man-in-the-middle attack runs as follows: the adversary first relays messages between the prover and the verifier in the initialization phase. Then, he plays with the prover a distance-bounding phase to learn some answers. He can then play with the verifier, with the responses that he has learnt, or with random ones if he ignores the correct one. The probability to pass a round correctly is $\frac{2}{3}$. So, the man-in-the-middle attack succeeds with probability $B(n, \tau, \frac{2}{3})$. By using the Chernoff bound, this is lower than $e^{-2\varepsilon^2 n}$ when

$$\frac{\tau}{n} > \frac{2}{3} + \varepsilon \tag{3}$$

The best collusion fraud consists of running the initialization phase between the malicious prover and the verifier. Then, the prover selects some $c_1^*, \ldots, c_n^*$ and set $F_i^*(c) = F_i(c)$ for each $c \neq c_i^*$, where F_i is the response function $c_i \mapsto F_i(c_i) = r_i$. The $F_i^*(c_i^*)$ values are set to random bits. Then, the prover gives the table of F^* to the adversary who uses it as a response function. Clearly, this leaks no information about x'. The probability to pass a round correctly is $\frac{5}{6}$. So, the collusion fraud succeeds with probability

$B(n,\tau,\frac{5}{6})$. By using the Chernoff bound, this is lower than $e^{-2\varepsilon^2 n}$ when

$$\frac{\tau}{n} > \frac{5}{6} + \varepsilon \tag{4}$$

To summarize equations (1)-(2)-(3)-(4), whenever $p_{\mathsf{noise}} < \frac{1}{6} - 2\varepsilon$, we can adjust τ and have the failure cases bounded by $e^{-2\varepsilon^2 n}$. Actually, we can formally prove that the above attacks are optimal. We obtain the following result.

Theorem 1 (Boureanu-Mitrokotsa-Vaudenay [8]). *If f is a (ε, T)-circular-keying secure PRF and the verifier requires at least τ correct rounds,*

- *all distance frauds (with complexity bounded by T) have a success probability bounded by* $\Pr[\mathsf{success}] \geq B(n,\tau,\frac{3}{4}) + \varepsilon$*;*
- *all man-in-the-middle attacks (with complexity bounded by T) have a success probability bounded by* $\Pr[\mathsf{success}] \geq B(n,\tau,\frac{2}{3}) + \frac{r^2}{2}2^{-k} + \varepsilon$*, where k is the nonce length and r is the number of participants in the experiment;*
- *for all collusion frauds such that $p = \Pr[\mathsf{CF\ succeeds}] \geq B(\frac{n}{2},\tau-\frac{n}{2},\frac{2}{3})^{1-c}$ and p^{-1} polynomially bounded, there is an associated man-in-the-middle attack with P^* such that* $\Pr[\mathsf{MiM\ succeeds}] \geq \left(1 - B(\frac{n}{2},\tau-\frac{n}{2},\frac{2}{3})^c\right)^s$*, for any c.*

Although it does not explicitly appear for distance-fraud and man-in-the-middle, we note that s plays a role in the ε anyway: if s is too small, f cannot be a secure PRF so ε cannot be negligible.

To optimize τ with respect to the expected loss in the case of a failed authentication or of an attack, we can follow the method in [16]. It requires to quantify all possible types of losses.

There exist several variants of SKI with different properties. Namely, we can consider secret sharing schemes other than the one in Fig. 6. We can consider other leakage schemes L_μ as well. We refer to [7,8] for details.

4 Conclusion

Modeling the different types of frauds for distance-bounding is not easy. When adopting an appropriate model, we can see that none of the existing distance-bounding protocols in the literature resist all frauds, with the exception of SKI. SKI is very lightweight, with several possible variants, of which herein we showed two. Under the assumption that the underlying primitive is a PRF with circular-keying security and that the level of noise in each round (in honest executions) is lower than $\frac{1}{6}$, we can achieve provable secure distance-bounding.

As future work, we will optimize the protocol to adjust the key sizes and number of rounds in an adequate way. We also leave open the problem of making a secure protocol without the $p_{\mathsf{noise}} < \frac{1}{6}$ limitation. For instance, we could try to defeat man-in-the.middle attacks in a different way than by introducing a secret sharing scheme [2]. Namely, we could use a challenge set of two elements and authenticate the received challenges at the end, as done in the Swiss-Knife protocol [25]. This way, we could reach a level of

noise p_{noise} close to $\frac{1}{4}$. One problem with this option is that proving security does not seem easy and, finally, it may be weak against PRF programming [5].

Another line of research consists of adding privacy preservation. People already suggested to protect *location privacy* [33], but this suffers from severe limitations as shown in [1,27]. Anonymity could also be considered in a way similar to RFID protocols [37,32,23]. One proposal is made in [22] but without terrorist fraud protection.

Acknowledgements

We warmly thank Shiho Moriai, program chair of FSE'13, and her program committee, for inviting us to present our results on distance bounding.

This work was partially supported by

- the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), under the Swiss National Science Foundation;
- the Marie Curie IEF Project Grant No. 252323 "PPIDR: Privacy-Preserving Intrusion Detection and Response in Wireless Communications".

References

1. J.-P. Aumasson, A. Mitrokotsa, P. Peris-Lopez. A Note on a Privacy-Preserving Distance-Bounding Protocol. In *Information and Communications Security ICICS'11*, Beijing, China, Lecture Notes in Computer Science 7043, pp. 78–92, Springer-Verlag, 2011.
2. G. Avoine, C. Lauradoux, B. Martin. How Secret-Sharing can Defeat Terrorist Fraud. In *ACM Conference on Wireless Network Security WISEC'11*, Hamburg, Germany, pp. 145–156, ACM, 2011.
3. G. Avoine, A. Tchamkerten. An Efficient Distance Bounding RFID Authentication Protocol: Balancing False-Acceptance Rate and Memory Requirement. In *Information Security ISC'09*, Pisa, Italy, Lecture Notes in Computer Science 5735, pp. 250–261, Springer-Verlag, 2009.
4. A. Bay, I. Boureanu, A. Mitrokotsa, I. Spulber, S. Vaudenay. The Bussard-Bagga and Other Distance-Bounding Protocols under Attacks. To appear in the proceedings of INSCRYPT'12.
5. I. Boureanu, A. Mitrokotsa, S. Vaudenay. On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols - PRF-ness alone Does Not Stop the Frauds! In *LATINCRYPT'12*, Santiago, Chile, Lecture Notes in Computer Science 7533, pp. 100–120, Springer-Verlag, 2012.
6. I. Boureanu, A. Mitrokotsa, S. Vaudenay. On the Need for Secure Distance-Bounding. To appear in the proceedings of ESC'13.
7. I. Boureanu, A. Mitrokotsa, S. Vaudenay. Secure & Lightweight Distance-Bounding. To appear in the proceedings of LightSec'13.
8. I. Boureanu, A. Mitrokotsa, S. Vaudenay. Practical & Provably Secure Distance-Bounding. Submitted.
9. S. Brands, D. Chaum. Distance-Bounding Protocols (Extended Abstract). In *Advances in Cryptology EUROCRYPT'93*, Lofthus, Norway, Lecture Notes in Computer Science 765, pp. 344–359, Springer-Verlag, 1994.
10. L. Bussard, W. Bagga. Distance-Bounding Proof of Knowledge to Avoid Real-Time Attacks. In *IFIP TC11 International Conference on Information Security SEC'05*, Chiba, Japan, pp. 223–238, Springer, 2005.

11. S. Čapkun, L. Buttyán, 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*, Fairfax VA, USA, pp. 21–32, ACM, 2003.
12. H. Chernoff. A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the sum of Observations. *Annals of Mathematical Statistics*, vol. 23 (4), pp. 493-507, 1952.
13. C.J. F. Cremers, K.B. Rasmussen, B. Schmidt, S. Čapkun. Distance Hijacking Attacks on Distance Bounding Protocols. In *IEEE Symposium on Security and Privacy S&P'12*, San Francisco CA, USA, pp. 113–127, IEEE Computer Society, 2012.
14. Y. Desmedt. Major Security Problems with the "Unforgeable" (Feige-)Fiat-Shamir Proofs of Identity and How to Overcome Them. In *Congress on Computer and Communication Security and Protection Securicom'88*, Paris, France, pp. 147–159, SEDEP Paris France, 1988.
15. S. Drimer, S.J. Murdoch. Keep your Enemies Close: Distance Bounding Against Smartcard Relay Attacks. In *USENIX Security Symposium*, Boston MA, USA, pp. 87–102, USENIX, 2007.
16. C. Dimitrakakis, A. Mitrokotsa, S. Vaudenay. Expected Loss Bounds for Authentication in Constrained Channels. In *Proceedings of the IEEE INFOCOM'12*, Orlando FL, USA, pp. 478–485, IEEE, 2012.
17. U. Dürholz, M. Fischlin, M. Kasper, C. Onete. A Formal Approach to Distance-Bounding RFID Protocols. In *Information Security ISC'11*, Xi'an, China, Lecture Notes in Computer Science 7001, pp. 47–62, Springer-Verlag, 2011.
18. A. Gürel, A. Arslan, M. Akgün. Non-uniform Stepping Approach to RFID Distance Bounding Problem. In *Data Privacy Management and Autonomous Spontaneous Security DPM/SETOP'10*, Athens, Greece, Lecture Notes in Computer Science 6514, pp. 64–78, Springer-Verlag, 2011.
19. G.P. Hancke. Distance Bounding for RFID: Effectiveness of Terrorist Fraud. In *Conference on RFID-Technologies and Applications RFID-TA'12*, Nice, France, pp. 91–96, IEEE, 2012.
20. G.P. Hancke, M.G. Kuhn. An RFID Distance Bounding Protocol. In *Conference on Security and Privacy for Emerging Areas in Communications Networks SecureComm'05*, Athens, Greece, pp. 67–73, IEEE, 2005.
21. G.P. Hancke, K. Mayes, K. Markantonakis, Confidence in Smart Token Proximity: Relay Attacks Revisited. *Computer & Security*, vol. 28, pp. 615–627, 2009.
22. J. Hermans, C. Onete, R. Peeters. Efficient, Secure, Private Distance Bounding without Key Updates. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks WISEC'13*, Budapest, Hungary, pp. 207–218, ACM, 2013.
23. J. Hermans, A. Pashalidis, F. Vercauteren, B. Preneel. A New RFID Privacy Model. In *Computer Security ESORICS'11*, Leuven, Belgium, Lecture Notes in Computer Science 6879, pp. 568–587, Springer-Verlag, 2011.
24. C.H. Kim, G. Avoine. RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks. In *Cryptology and Network Security, 8th International Conference CANS'09*, Kanazawa, Japan, Lecture Notes in Computer Science 5888, pp. 119–133, Springer-Verlag, 2009.
25. C.H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, O. Pereira. The Swiss-Knife RFID Distance Bounding Protocol. In *Information Security and Cryptology ICISC'08*, Seoul, Korea, Lecture Notes in Computer Science 5461, pp. 98–115, Springer-Verlag, 2009.
26. A. Mitrokotsa, C. Dimitrakakis, P. Peris-Lopez, J.C. Hermandez-Castro. Reid et al.'s Distance Bounding Protocol and Mafia Fraud Attacks over Noisy Channels. *IEEE Communications Letters*, vol. 14, pp. 121–123, 2010.
27. A. Mitrokotsa, C. Onete, S. Vaudenay. Mafia Fraud Attack against the RČ Distance-Bounding Protocol. In *Conference on RFID-Technologies and Applications RFID-TA'12*, Nice, France, pp. 74–79, IEEE, 2012.

28. A. Mitrokotsa, P. Peris-Lopez, C. Dimitrakakis, S. Vaudenay. On Selecting the Nonce Length in Distance-Bounding Protocols. To appear in the Computer Journal (Oxford), Special Issue on "Advanced Semantic and Social Multimedia Technologies for Future Computing Environment". 2013. doi: 10.1093/comjnl/bxt033
29. J. Munilla, A. Peinado. Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels. *Wireless Communications and Mobile Computing*, vol. 8, pp. 1227–1232, 2008.
30. J. Munilla, A. Peinado. Security Analysis of Tu and Piramuthu's Protocol. In *Conference on New Technologies, Mobility and Security NTMS'08*, Tangier, Morocco, pp. 1–5, IEEE, 2008.
31. V. Nikov, M. Vauclair. Yet Another Secure Distance-Bounding Protocol. In *International Conference on Security and Cryptography*, Porto, Portugal, pp. 218–221, INSTICC Press, 2008.
32. K. Ouafi, S. Vaudenay. Strong Privacy for RFID Systems from Plaintext-Aware Encryption. In *Cryptology and Network Security, 8th International Conference CANS'12*, Darmstadt, Germany, Lecture Notes in Computer Science 7712, pp. 247–262, Springer-Verlag, 2012.
33. K.B. Rasmussen, S. Čapkun. Location Privacy of Distance Bounding Protocols. In *15th ACM Conference on Computer and Communications Security*, Alexandria VA, USA, pp. 149–160, ACM Press, 2008.
34. J. Reid, J.M.G. Nieto, T. Tang, B. Senadji. Detecting Relay Attacks with Timing-Based Protocols. In *ACM Symposium on Information, Computer and Communications Security ASI-ACCS'07*, Singapore, pp. 204–213, ACM, 2007.
35. D. Singelée, B. Preneel. Distance Bounding in Noisy Environments. In *Security and Privacy in Ad-hoc and Sensor Networks ESAS'07*, Cambridge, UK, Lecture Notes in Computer Science 4572, pp. 101–115, Springer-Verlag, 2007.
36. Y.J. Tu, S. Piramuthu. RFID Distance Bounding Protocols. In *EURASIP Workshop on RFID Technology*, Vienna, Austria, 2007.
37. S. Vaudenay. On Privacy Models for RFID. In *Advances in Cryptology ASIACRYPT'07*, Kuching, Malaysia, Lecture Notes in Computer Science 4833, pp. 68–87, Springer-Verlag, 2007.