Solution of a Conjecture: On 2-PCD RFID Distance Bounding Protocols

Eren KOCAAĞA, Bünyamin TANIL, Muhammed Ali BİNGÖL, Süleyman KARDAŞ

***Abstract*—It is a popular challenge to design distance bounding protocols that are both secure and efficient. Motivated by this, many distance bounding protocols against relay attacks have been advanced in recent times. Another interesting question is whether these protocols provides the best security. In 2010, Kara et al. analysis the optimal security limits of low-cost distance bounding protocols having bit-wise fast phases and no final signature. As for the classification, they have introduced the notion of k-previous challenge dependent (k-PCD) protocols where each response bit depends on the current and the k previous challenges. They have given the theoretical security bounds for two specific classes $k = 0$ and 1, but have left the security bounds for $k \geq 2$ as an open problem. In this paper, we aim to answer the open question concerning the security limits of 2-PCD protocols. We describe two generic attacks for mafia and distance frauds that can be applied on any 2-PCD protocols. Then, we provide the optimal trade-off curve between the security levels of mafia and distance frauds that determines the security limits of 2-PCD protocols. Finally our results also prove the conjecture that 2-PCD protocols enhance the security compared to 0-PCD and 1-PCD cases.**

***Index Terms*—RFID, distance bounding protocol, relay attack, security, trade-off.**

I. Introduction

RADIO Frequency IDentification protocols, as a part of wireless authentication, are commonly used in many applications such as credit cards, toll payment systems, e-passport etc. Since the communication occurs in the air, these protocols are vulnerable to relay attacks in which an attacker defeats the authentication system by only relaying messages verbatim between the legitimate parties (generally a prover and a verifier). The concept of relay attack was originally proposed by Conway using a scenario called "Grand Master Chess Problem" in 1976 [1], and advanced by Desmedt et al. in Crypto'87 [2]. Relay attacks can be simply classified as mafia, terrorist and distance fraud attacks [3].

Based on the authentication protocols that include challenge-response messages, mafia and terrorist fraud scenarios can be defined as follows (Fig. 1). An adversary pretending to be a legitimate prover (or tag) first gets the challenge from the verifier (or reader) and relay it to the legitimate prover which is out of neighbourhood at the beginning of attack. After that she gets the valid response for this challenge and forwards it to the reader as her answer. Some relay attack demonstrations and constructive considerations are given in [4]–[6].

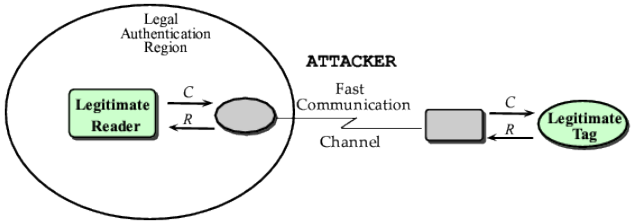

Fig. 1. Mafia and terrorist fraud scenarios

The aforementioned scenario that the prover has no awareness of attack is an example of mafia fraud. In order to give a more realistic illustration, we can think that mafia fraud attack can be completed against the point-of-sale credit card terminal although the credit cards are tamper resistant and certificated. The remaining type of the relay attack is called *distance fraud* attack where adversary has an ability to reach secret key (she is a kind of dishonest legitimate tag) to convince the verifier that she is within the neighbourhood whereas she is not. A typical and easily comprehensible illustration of this attack is home confinement that a person wears a bracelet and electronically monitored. This person would make use of distance fraud attack and leave his home temporarily without being detected. (Fig. 2).

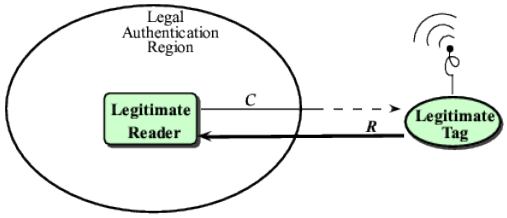

Fig. 2. Distance fraud scenario

Researchers have developed two main approaches to mitigate relay attacks. One of them is related to measuring radio signal strength (RSS) that the verifier measures this value in order to understand whether the prover is close or not. On the other hand, this solution suggestion is not applicable because adversary can have the ability to adjust its signal strength to persuade the verifier that she is in the neighbourhood region. The other approach to prevent these attacks is focused on calculating the round trip time (RTT) of the prover's response after a challenge sent by the verifier. The verifier

E.Kocaağa and B. Tanıl are with Istanbul Technical University Maslak, Istanbul, and M. A. Bingöl, and S. Kardaş are with National Research Institute of Electronics and Cryptology (TUBITAK UEKAE), Gebze 41470 Kocaeli/Turkey and Sabanci University Istanbul/Turkey, e-mail: {muhammedali.bingol, suleyman.kardas}@tubitak.gov.tr

checks the distance of a prover under favour of measuring RTT of a signal. Upper bound for the speed of radio signal, which has importance in this approach, can not be faster than that of light. Brands and Chaum took the first step in their seminal work [7] and they offered the rapid bit exchange conception to design a protocol that includes measurement of RTT in 1993. Afterwards, Hancke and Kuhn proposed the first RFID-related distance bounding protocol [8], which does not involve any final signature. These studies triggered the other researchers and several distance bounding protocols that use round trip time method have been proposed to increase security conditions against relay attacks which are mafia fraud, distance fraud and terrorist fraud [9]–[14]. We refer to [3] for further introduction on distance bounding protocols.

It is still a popular challenge to design distance bounding protocols that are both secure and efficient. In 2010, optimal security limits of low-cost RFID distance-bounding protocols are analyzed by Kara, Kardaş, Bingöl, and Avoine [15]. They focus on the low-cost distance-bounding protocols having bit-wise fast phases and no final signature. As for the classification, they introduce the notion of k-previous challenge dependent (k-PCD) protocols where each response bit depends on the current and the k previous challenges. They provide trade-off curves between the optimal security limits of mafia and distance frauds for $k = 0$ and 1. The authors leave as an open question to find the best the trade-off curves for $k \geq 2$, and they conjecture that the security should be enhanced when k is increased.

In this paper, we aim at to support anticipations about the open questions of k-PCD protocols (general extension). In this respect, we analysis 2-PCD protocols and make attack resistance calculations of this protocol against mafia and distance fraud attacks. Our results show that when we increase the number 'k', the security level of distance bounding protocols enhanced as it is expected. We also demonstrate the results calculated on software program and observe 2-PCD trade-off curve below that of 1-PCD. The most important property of previous challenge dependent distance bounding protocols is that the current response bit in the rapid bit phase depends on previous challenges as well. It is observed that the security of protocols against mafia fraud and distance fraud attacks improved without any supplementary overhead on the computation by virtue of k-PCD protocols can be succeeded. The another expected properties of distance bounding protocols such as resistance of channel errors in noisy environment and preservation of privacy also provided by these protocols. Moreover, mutual authentication is also made between prover and verifier without generating any overhead in these protocols. In conclusion, development of k-PCD protocols has crucial importance on RFID framework and this is what we try to do in general of this study.

The composition of the paper is following: In Section II we briefly explain the current challenge dependent (CCD) protocols. In Section III, conjectures and open questions of k-PCD protocols and some relevant definitions are given. Section IV consists of our results and analysis related to 2-PCD protocols that answers the previous conjectures and simulations that supports theoretical results.

II. Current Challenge Protocols (CCD)

In general, distance bounding protocols consist of three phases; slow phase-I, fast phase and slow phase-II. However slow phase-II usually contains time consuming message namely a final signature. Therefore, we focus on CCD protocols that have no slow phase-II as it is primarily defined in [15]. For instance, Hancke and Kuhn's protocol as an example of current challenge dependent protocols includes only the first two phases. In slow phase-I, parties interchange nonces. After that, responses are generated by parties using the same pseudo random functions. During the fast phase each response r_i only corresponds to a current challenge c_i. This protocol satisfies the following properties:

- During the fast phase, each response bit r_i is computed as $r_i := f(c_i, y_i^0, ..., y_{m-1}^i)$, where c_i is the i-th bit and $(y_i^0, ..., y_{m-1}^i)$ is the i-th string of the session secret shared by both prover and verifier for $i = 1, ..., n$, where n is the number of rapid bit exchanges. The response function f is defined as: $r_i := f(c_i, y_i^0, ..., y_{m-1}^i) = c_i.y_1^i \bigoplus ((1 \bigoplus c_i).y_0^i)$
- There is no final slow phase.

Final signature is not a compulsory phase for practical solutions to suitable requirements of RFID tags. On the other hand, these protocols are vulnerable to terrorist attacks without final signature. However, CCD protocols satisfy some security levels against mafia and distance frauds. Success probabilities of mafia and distance frauds have the following property [15]:

$$P_{maf} + P_{dis} \geq \tfrac{3}{2}.$$

III. k-PCD Protocols

k-Previous Challenge Dependent (k-PCD) protocol is a natural extension of CCD protocols. In CCD protocols, the response is only related to current challenge. On the other side, the response depends on both current challenge and k previous challenges in k-PCD protocols. This protocol satisfies the properties below

- During the fast phase, each response bit r_i is computed as $r_i := f(c_i, ..., c_{i-k}, y_i^0, ..., y_{m-1}^i)$, where c_i is the i-th bit and $(y_i^0, ..., y_{m-1}^i)$ is the i-th string of the session secret shared by both prover and verifier for $i = 1, ..., n$, where n is the number of rapid bit exchanges.
- There is no final slow phase.

Remark : From definitions, a CCD protocol can be thought as a k-PCD protocol when k=0.

As a result, protocols that the response of the prover in fast bit exchange phase depends on previous challenges are more secure against relay attacks compared to CCD protocols. Hence, k-PCD protocols are expected to reach the optimum security against mafia fraud and distance fraud when k tends to be infinity. This conjecture is generated from calculations that take part in following sections.

IV. The Security Analysis of 2-PCD Protocols

In this section, we introduce and analyze the security of 2-PCD protocols. First of all, description of security regions

for analysis of distance fraud attack is given in order to easily comprehend the idea of the generic attack. Second, we receive some help from different sets which defined in this section just as used in CCD and 1-PCD protocols [15]. Then, we verify optimum security limits for 2-PCD protocols against mafia and distance fraud, and plot the trade-off curve for k-PCD protocols where $k = 0, 1$ and 2.

A. Security Regions for Distance Fraud

k-PCD protocols are composed of two main parties; reader and prover. When the subject matter is a distance fraud attack against these protocols, another party called adversary emerges in addition to main parties. In distance fraud attack, the adversary has a right to access while staying on legal authentication region. Besides, the adversary may stay on the outside of this region and pretend to be in the authentication region. In brief, distance fraud attacks are based on this scenario in RFID framework.

When an adversary is outside of legal authentication region, receiving and time requirement to receive challenges depend on the distance between the adversary and bounds of this region. Therefore, in order to make the analysis of distance fraud attacks simpler, we describe four spherical regions (Z_1, Z_2, Z_3, Z_4) in which the adversary can communicate with the verifier.

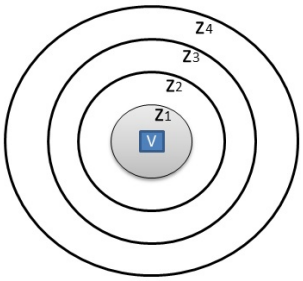

Fig. 3. Security Regions for Distance Fraud

TABLE I
DISTANCE FRAUD SCENARIOS IN DIFFERENT REGIONS

Where is adversary?	What should she do?
Z_1	She always access
Z_2	Send r_i before c_i
Z_3	Send r_i before c_i, c_{i-1}
Z_4	Send r_i before $c_i, c_{i-1}, ..., c_{i-k}$

While designing the distance fraud attack scenario we assume that the adversary is in Z_4 region since the dependency parameter k is equal to 2. In the next subsection, calculations of security limits of 2-PCD protocols against distance fraud attacks are made based on this scenario.

B. Security Trade-off for 2-PCD Protocols

Let g be the response function that have inputs c_i, c_{i-1}, c_{i-2}, y and output response bit r_i. To analyze the distance and mafia fraud attack, we define a variable a_y as the equation below,

$$\begin{aligned} a_y &= \sum g(c_i, c_{i-1}, c_{i-2}, y) - 4 \\ & c_i \in (0,1) \\ & c_{i-1} \in (0,1) \\ & c_{i-2} \in (0,1) \end{aligned}$$

Also we define the following sets:

$$\begin{aligned} A &= y \in F_2^m : |a_y| = 4, \\ B_1 &= y \in F_2^m : |a_y| = 3, \\ B_2 &= y \in F_2^m : |a_y| = 2, \\ B_3 &= y \in F_2^m : |a_y| = 1, \\ C &= y \in F_2^m : |a_y| = 0. \end{aligned}$$

$a + b_1 + b_2 + b_3 + c = 2^m$, where a is the cardinality of the set A, b_1 is the cardinality of the set B_1, b_2 is the cardinality of the set B_2, b_3 is the cardinality of the set B_3 and c is the cardinality of the set C.

The set A includes the session secrets that produce the same response bits r_i. The other three sets B_1, B_2 and B_3 are the majority groups that have same response bits with probability $\frac{7}{8}, \frac{3}{4}$ and $\frac{5}{8}$ respectively. Finally, set C has same response bits in half.

Success probabilities of mafia fraud and distance fraud attacks depend on the cardinality of sets in 2-PCD protocol. Success probability calculations of distance fraud attack for 2-PCD protocols as follows:

$$\begin{aligned} P_{dis} &= \frac{a}{2^m} + \frac{7}{8} \cdot \frac{b_1}{2^m} + \frac{6}{8} \cdot \frac{b_2}{2^m} + \frac{5}{8} \cdot \frac{b_3}{2^m} + \frac{4}{8} \cdot \frac{c}{2^m} \\ &= \frac{1}{2} + \frac{4a + 3b_1 + 2b_2 + b_3}{2^{m+3}} \end{aligned}$$

Success probability calculations of mafia fraud attack for 2-PCD protocols as follows:

$$\begin{aligned} P_{maf}^{no-flip} &= \frac{1}{8} + \frac{7}{8} \cdot [\frac{a}{2^m} + \frac{3}{4} \cdot \frac{b_1}{2^m} + \\ & \quad \frac{4}{7} \cdot \frac{b_2}{2^m} + \frac{13}{28} \cdot \frac{b_3}{2^m} + \frac{3}{7} \cdot \frac{c}{2^m}] \\ &= \frac{1}{2} + \frac{16a + 9b_1 + 4b_2 + b_3}{2^{m+5}} \end{aligned}$$

$$\begin{aligned} P_{maf}^{flip} &= \frac{1}{8} + \frac{7}{8} \cdot [\frac{1}{4} \cdot \frac{b_1}{2^m} + \frac{3}{7} \cdot \frac{b_2}{2^m} + \\ & \quad \frac{15}{28} \cdot \frac{b_3}{2^m} + \frac{4}{7} \cdot \frac{c}{2^m}] \\ &= \frac{1}{8} + \frac{7b_1 + 12b_2 + 15b_3 + 16c}{2^{m+5}} \end{aligned}$$

Success probabilities of distance fraud attack and mafia fraud attack inversely related to each other. Trade-off curve calculations between mafia fraud and distance fraud for 2-PCD protocols as follows:

$$P_{maf}^{flip} + P_{dis} = \frac{9}{8} + \frac{3b_1 + 4b_2 + 3b_3}{2^{m+5}}$$
$$P_{maf}^{no-flip} + P_{dis} = \frac{9}{8} + \frac{28a + 17b_1 + 8b_2 + b_3 - 4c}{2^{m+5}}$$

This implies that, $P_{maf} + P_{dis} \geq \frac{9}{8}$. Thus, lower success probability bound for the summation of both mafia fraud attack and distance fraud attack is calculated as $\frac{9}{8}$.

TABLE II
MAXIMUM SECURITY LIMITS

DB Protocols	$P_{dist} + P_{maf} \geq$
CCD	3/2
1-PCD	5/4
2-PCD	9/8

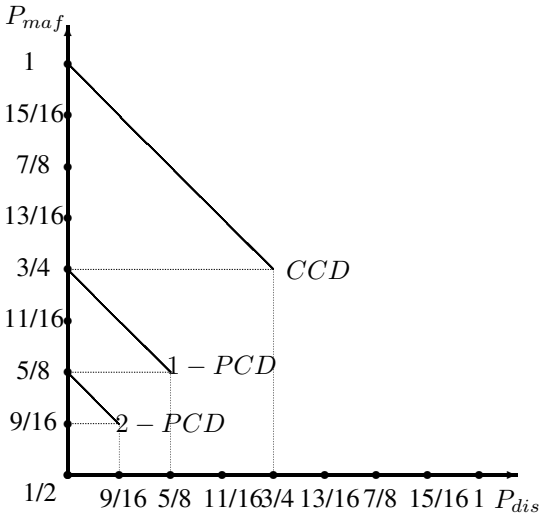

Fig. 4. Trade-off Curve for CCD,1-PCD,2-PCD

As it is shown in the Figure 4 when the parameter k goes the infinity k-PCD protocols will reach the ideal security level.

C. The Optimum Design of Mafia and Distance Fraud Attack Algorithm Against 2-PCD Protocols

Compatibility between calculations and verification of distance fraud attack and mafia fraud attack with algorithms provides huge contributions on the optimum security results.

We compare mafia fraud attacks $max(P_{maf}^{no-flip}, P_{maf}^{flip})$ with an approximation (neglecting b_1, b_2 and b_3). Then, this approximation gives that optimum security limit for mafia fraud is satisfied when $c = 7a$. So, it is clear that flipping the response is more preferable under the condition of $c > 7a$ in order to learn each bit of register for an adversary.

We design a generic mafia fraud attack algorithm for 2-PCD protocols which is given in Algorithm IV.1.

Algorithm IV.1: MAFIA FRAUD ATTACK FOR 2-PCD PROTOCOLS(n, a, c)

n: Number of rounds
flip: Deciding on flipping the response
Send a random challenge $c_0' \in \{0,1\}$ and $c_1' \in \{0,1\}$ to the prover
if $c \geq 7a$
  then $flip \leftarrow 1$
  else $flip \leftarrow 0$
for $i \leftarrow 0$ **to** n
  do { Send a random challenge $c_i' \in \{0,1\}$ to the prover
  Record the prover's response r_i'
*/*Then, Mafia continues the protocol with the verifier*/*
Record first challenge c_{i-1} and second challenge c_{i-2} of the verifier
for $i \leftarrow 2$ **to** n
  do { record i-th challenge of the verifier in c_i
  if $c_i' = c_i$ **and** $c_{i-1}' = c_{i-1}$ **and** $c_{i-2}' = c_{i-2}$
    then Send r_i'
    else Send $r_i' \oplus flip$
  $c_{i-1} \leftarrow c_i$ **and** $c_{i-2} \leftarrow c_{i-1}$

We also design a generic distance fraud attack algorithm for 2-PCD protocols which is given in Algorithm IV.2.

Algorithm IV.2: DISTANCE FRAUD ATTACK FOR 2-PCD PROTOCOLS(n)

n: Number of rounds
$c_0' \in \{0,1\}$ and $c_1' \in \{0,1\}$
for $i \leftarrow 2$ **to** n
  if $a_y = 3$ **or** $a_y = 2$ **or** $a_y = 1$
    Send 1
    if $g(0, c_{i-1}, c_{i-2}, y) = 1$
      if $c_{i-1} = 0$
      then $c_{i-2} \leftarrow 0$
      else $c_{i-1} \leftarrow 0$ **and** $c_{i-2} \leftarrow 1$
    else
      if $c_{i-1} = 0$
      then $c_{i-1} \leftarrow 1$ **and** $c_{i-2} \leftarrow 0$
      else $c_{i-1} \leftarrow 1$ **and** $c_{i-2} \leftarrow 1$
  else if $a_y = -3$ **or** $a_y = -2$ **or** $a_y = -1$
  do { Send 0
    if $g(0, c_{i-1}, c_{i-2}, y) = 1$
      if $c_{i-1} = 0$
      then $c_{i-2} \leftarrow 0$
      else $c_{i-1} \leftarrow 0$ **and** $c_{i-2} \leftarrow 1$
    else
      if $c_{i-1} = 0$
      then $c_{i-1} \leftarrow 1$ **and** $c_{i-2} \leftarrow 0$
      else $c_{i-1} \leftarrow 1$ **and** $c_{i-2} \leftarrow 1$
  else
    Send $g(0, c_{i-1}, c_{i-2}, y)$
    then $c_{i-1} \leftarrow 0$ **and** $c_{i-2} \leftarrow c_{i-1}$

D. Simulation Results

We implement four different 2-PCD response generating functions on HK protocol structure. We simulate the attacks given in Algorithms IV.1 and IV.2 for each of them. The simulation for each protocol is repeated 2^{20} times with fresh nonces. We have shown that the experimental results, which are shown in Table III, are in parallel with the results obtained in Section IV-B.

TABLE III
THE SIMULATION RESULTS FOR SUCCESS PROBABILITIES OF MAFIA FRAUD AND DISTANCE FRAUD.

a	$\sum_{i=1}^{3} b_i$	c	P_{maf}^{flip}	$P_{maf}^{no-flip}$	P_{dis}
1	0	7	0.5626	0.5656	0.5626
4	2	2	0.3260	0.7942	0.8200
0	0	8	0.6242	0.4992	0.4969
0	8	0	0.4485	0.6818	0.7821

Note that, in all experiments we took $b_1 = b_2 = b_3$ for the sake of simplicity.

V. CONCLUSION

In this paper, we have explained RFID distance bounding protocols and briefly reviewed at current challenge dependent protocols. We also introduced the notion of k-PCD protocols. Thus, we have shown that when we increase the dependency parameter 'k', security level against mafia fraud attack and distance fraud attack increase as they are expected. We have supported these expectations by calculating success probabilities of distance fraud and mafia fraud attacks for 2-PCD protocols. On the other hand, trade-of curve of 2-PCD protocol is plotted and compared with CCD and 1-PCD protocols.

We also prove the conjecture that the best trade-off curve for k_1-PCD protocols lies above the best trade-off curve for k_2-PCD protocols where $k_1 < k_2$.

We also claim that a general formula for k-PCD protocols can be obtained but we also left this problem as an future work.

VI. ACKNOWLEDGEMENTS

We would like to thank Oğuz Yildiz for his helpful contributions.

REFERENCES

[1] J. H. Conway, *On Numbers and Games*, ser. London Mathematical Society Monographs. Academic Press, London-New-San Francisco, 1976, no. 6.

[2] Y. Desmedt, C. Goutier, and S. Bengio, "Special uses and abuses of the fiat-shamir passport protocol," in *Advances in Cryptology – CRYPTO'87*, ser. Lecture Notes in Computer Science, C. Pomerance, Ed., vol. 293. Santa Barbara, California, USA: Springer-Verlag, August 1988, pp. 21–39.

[3] G. Avoine, M. A. Bingöl, S. Kardaş, C. Lauradoux, and B. Martin, "A Framework for Analyzing RFID Distance Bounding Protocols," *Journal of Computer Security – Special Issue on RFID System Security*, vol. 19, no. 2, pp. 289–317, March 2011.

[4] G. Hancke, K. Mayes, and K. Markantonakis, "Confidence in Smart Token Proximity: Relay Attacks Revisited," in *Elsevier Computers & Security*, ser. 7, vol. 28, June 2009, pp. 615–627.

[5] G. P. Hancke, "A Practical Relay Attack on ISO 14443 Proximity Cards," Manuscript, University of Cambridge, United Kingdom, February 2005.

[6] L. Sportiello and A. Ciardulli, "Long distance relay attack," in *Workshop on RFID Security – RFIDSec'13*, Graz, Austria, July 2013.

[7] S. Brands and D. Chaum, "Distance-Bounding Protocols," in *EUROCRYPT'93: Advances in Cryptology*. Secaucus, NJ, USA: Springer-Verlag Newyork Inc, 1994, pp. 344–359.

[8] G. P. Hancke and M. G. Kuhn, "An RFID Distance Bounding Protocol," in *SECURECOMM '05: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*. Washington, DC, USA: IEEE Computer Society, 2005, pp. 67–73.

[9] S. Kardaş, M. S. Kiraz, M. A. Bingöl, and H. Demirci, "A Novel RFID Distance Bounding Protocol Based on Physically Unclonable Functions," in *Workshop on RFID Security – RFIDSec'11*, ser. Lecture Notes in Computer Science, A. Juels and C. Paar, Eds., vol. 7055. Amherst, Massachusetts, USA: Springer Berlin Heidelberg, June 2012, pp. 78–93.

[10] 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*, ser. Lecture Notes in Computer Science. Seoul, Korea: Springer-Verlag, 2008, pp. 98–115.

[11] G. Avoine, C. Lauradoux, and B. Martin, "How secret-sharing can defeat terrorist fraud," in *Proceedings of the 4th ACM Conference on Wireless Network Security – WiSec'11*, ACM. Hamburg, Germany: ACM Press, June 2011.

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

[13] J. Reid, J. M. G. Nieto, T. Tang, and B. Senadji, "Detecting Relay Attacks with Timing-Based Protocols," in *ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security*. New York, NY, USA: ACM, 2007, pp. 204–213.

[14] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "Secure and Lightweight Distance-Bounding," in *Second International Workshop on Lightweight Cryptography for Security and Privacy – LightSec 2013*, Gebze, Turkey, May 2013.

[15] O. Kara, S. Kardaş, M. A. Bingöl, and G. Avoine, "Optimal Security Limits of RFID Distance Bounding Protocols," in *Workshop on RFID Security – RFIDSec'10*, ser. Lecture Notes in Computer Science, S. O. Yalcin, Ed., vol. 6370. Istanbul, Turkey: Springer, June 2010, pp. 220–238.