Optimal Security Limits of RFID Distance Bounding Protocols

Orhun Kara[1], Süleyman Kardaş[1,2],
Muhammed Ali Bingöl[1,3], and Gildas Avoine[4]

[1] TUBITAK UEKAE, Gebze, Kocaeli, Turkey
[2] Sabanci University, Istanbul, TR-34956, Turkey
[3] Istanbul Technical University,
Institute of Science and Technology, Istanbul, Turkey
[4] UCL, Information Security Group, Louvain-la-Neuve, Belgium

Abstract. In this paper, we classify the RFID distance bounding protocols having bitwise fast phases and no final signature. We also give the theoretical security bounds for two specific classes, leaving the security bounds for the general case as an open problem. As for the classification, we introduce the notion of *k-previous challenge dependent* (k-PCD) protocols where each response bit depends on the current and k-previous challenges and there is no final signature. We treat the case $k = 0$, which means each response bit depends only on the current challenge, as a special case and define such protocols as *current challenge dependent* (CCD) protocols. In general, we construct a trade-off curve between the security levels of mafia and distance frauds by introducing two generic attack algorithms. This leads to the conclusion that CCD protocols cannot attain the ideal security against distance fraud, i.e. 1/2, for each challenge-response bit, without totally losing the security against mafia fraud. We extend the generic attacks to 1-PCD protocols and obtain a trade-off curve for 1-PCD protocols pointing out that 1-PCD protocols can provide better security than CCD protocols. Thereby, we propose a natural extension of a CCD protocol to a 1-PCD protocol in order to improve its security. As a study case, we give two natural extensions of Hancke and Kuhn protocol to show how to enhance the security against either mafia fraud or distance fraud without extra cost.

Keywords: RFID, distance bounding protocol, security, mafia fraud, distance fraud.

1 Introduction

Radio Frequency IDentification (RFID) is a technology pervasively used in many applications, from supply chain tracking systems to credit card payment systems. Security is a major concern in these applications and is definitely a critical point when tags are required to provide a proof of identity, which is the case in applications like payment, access control, ticketing, e-passport,... Such evolved applications can benefit from powerful tags that implement cryptographic algorithms, which are commonly block and stream ciphers. Standardized and well-established authentication protocols can then be used, e.g., ISO/IEC 9798 or ISO/IEC 11770.

The seminal work of Desmedt *et al.* [3,6,7] on *relay attacks* shows that *mafia fraud* can defeat all the conventional authentication protocols. The mafia fraud, in an RFID challenge-response authentication protocol, can be summarized as follows (Fig. 1). The adversary, who aims to impersonate a legitimate prover (tag), first gets the challenge from the verifier (reader) using a rogue tag, and transmits it to the remote legitimate tag through a rogue reader. The adversary then receives the corresponding response from the legitimate tag, and relays it to the legitimate reader. It really makes sense in practice, especially when considering a payment system with point-of-sale credit card terminals, even though the contactless credit cards are tamper resistant and certified. Feasibility and practical considerations are addressed in [8,10].

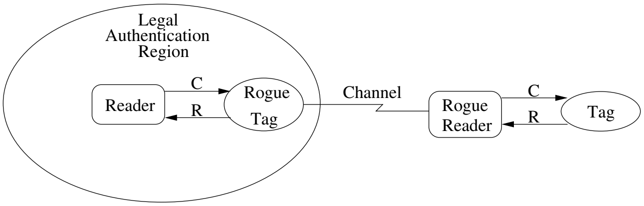

Fig. 1. A mafia fraud scenario

Similar to mafia fraud, there is also another attack called *distance fraud* (Fig. 2). In this attack, a party having access to the secret key persuades a verifier that she is within a certain distance whereas she is not. Home confinement based on electronic monitoring with ankle bracelets is a typical example where distance fraud is definitely relevant. This fraud would allow the person under monitoring to temporary leave his residence without being detected.

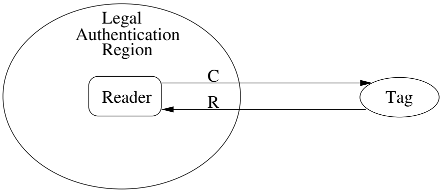

Fig. 2. A distance fraud scenario

Two main approaches have been adopted so far to prevent relay-like attacks. One of them is based on measuring the radio signal strength (RSS), so that the verifier learns whether the prover is close to it. However, this method has a drawback that a capable adversary can regulate the signal strength to convince the verifier of her proximity [9]. The other important approach was introduced by Beth and Desmedt [3], called *distance bounding*, based on calculating the *round trip time* (RTT) of the response after a challenge is sent. The verifier checks the distance of a prover by measuring the RTT given that the speed of the radio signal can not exceed that of light.

Brands and Chaum proposed the first distance bounding protocol at Eurocrypt 93 [4]. This protocol is composed of three phases; *slow phase-I*, *fast phase*, and *slow phase-II*. The slow phases consist of the time-consuming operations such as random nonce generations, commitment and signature calculations. On the other hand, the fast phase includes non-time consuming response generations and rapid bit exchanges. Particularly during the *slow phase-II* the prover has to calculate a *final signature*.

Afterwards, Hancke and Kuhn proposed the first RFID-dedicated distance bounding protocol [9], which does not involve any final signature. Then, several distance bounding protocols based on those two protocols have been proposed to improve security levels against mafia and distance frauds [1, 2, 5, 11–18].

In this paper, we aim at investigating how to achieve the optimum security against mafia fraud and distance fraud without using a final signature. We show that these two frauds are correlated and we express the trade-off between the adversary success probabilities with respect to these frauds. In other words, we prove that, under some assumptions, protocols can be designed to enforce the mafia or distance fraud resistance, but not both at the same time. For that, we define and address Current Challenge-Dependent (CCD) protocols and k-Previous Challenge-Dependent (k-PCD) protocols.

The rest of the paper is organized as follows: In Section 2, we briefly give general definitions and summarize our contributions. Then, in Section 3, we describe two generic attacks for CCD protocols and state the security trade-off between mafia and distance frauds for these attacks. In Section 4, we consider 1-PCD protocols and also provide generic attacks and trade-off between mafia and distance frauds. In Section 5, we introduce the notion of natural extension on CCD protocols and apply two extensions on an existing CCD protocol to enhance the security. Lastly, in Section 6, we give a brief discussion and conclude the paper with some open problems.

2 General Notions, Definitions and Our Contributions

In this paper, we mainly focus on the distance bounding protocols appropriate to RFID systems in which there is no final signature. These protocols are generally composed of two phases: a slow phase and a fast phase. In the slow phase, both parties constitute the *session secrets* (for example, the session secret in the HK protocol presented in Appendix A consists of two registers) that are used to produce response bits during the fast phase. Throughout the fast phase, both parties use the same *response generating function* which produces a response by using the session secrets and given a challenge value.

In what follows we study on how to achieve the optimum security against mafia fraud and distance fraud. For that, we first define a class of protocols without a final signature and, in which each response bit depends on the current challenge. It is described below.

Definition 1 (Current Challenge-Dependent (CCD) Protocol). *Let $f : \mathbb{F}_2^{m+1} \to \mathbb{F}_2$ be a Boolean function. A CCD protocol $\mathcal{P}$ is a distance bounding protocol that satisfies the following properties:*

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

The protocol $\mathcal{P}$ is denoted as $f(c_i, y_0^i, \ldots, y_{m-1}^i) \to r_i$ CCD protocol. The function f is called the response function of the protocol $\mathcal{P}$.

One popular example of CCD protocols is Hancke and Kuhn (HK) protocol [9]. The protocol is explained in detail in Appendix A. The response function of the protocol can be described as the following Boolean function:

$$f(c_i, y_0^i, y_1^i) = c_i \cdot y_1^i \oplus (1 \oplus c_i) \cdot y_0^i = y_{c_i}^i \tag{1}$$

where $\oplus$ and $\cdot$ are the addition and the multiplication operations of the binary Galois Field respectively.

Let us denote P_{maf}^E the success probability of correctly guessing one bit response for mafia fraud of an attack E, and similarly P_{dis}^E for distance fraud of an attack E. The security levels of a given protocol $\mathcal{P}$ are defined as follows.

Definition 2. *$P_{maf}(\mathcal{P}) = \max_E P_{maf}^E$ and $P_{dis}(\mathcal{P}) = \max_E P_{dis}^E$. That is, $P_{maf}(\mathcal{P})$ is the maximum of P_{maf}^E over all the mafia fraud attacks E mounted on $\mathcal{P}$, and similarly $P_{dis}(\mathcal{P})$ is the maximum of P_{dis}^E over all the distance fraud attacks E mounted on $\mathcal{P}$.*

The security levels of HK protocol are given as $3/4$ for both mafia and distance frauds for the attacks given in [9] and Appendix A, respectively. So $P_{maf}(HK) \geq 3/4$ and $P_{dis}(HK) \geq 3/4$. It has been an open question that these security levels are optimum for CCD protocols. Also, it is not known whether it is possible to improve the security level against mafia fraud without sacrificing the security level against the distance fraud and vice versa. In general, we have the following open questions for CCD protocols:

- What is the best security levels for both mafia fraud and distance fraud among all CCD protocols?
- What is the optimum achievable security level for mafia fraud of a CCD protocol?
- For a CCD protocol, what is the minimum value of P_{maf} if P_{dis} is ideal (i.e. $\frac{1}{2}$)?

The above-mentioned questions are answered in this paper. We first describe two generic attacks for mafia and distance frauds that can be mounted on all CCD protocols. Then, we show that there is a trade-off between mafia fraud and distance fraud, namely $P_{maf}(\mathcal{P}) + P_{dis}(\mathcal{P}) \geq 3/2$. We also prove that for any CCD protocol there is a security limit concerning the mafia fraud such that $P_{maf}(\mathcal{P}) \geq 3/4$ for any CCD protocol $\mathcal{P}$. As a consequence of this result we show that if $P_{dis}(\mathcal{P}) = 1/2$ then the protocol is completely vulnerable to mafia fraud (i.e., $P_{maf}(\mathcal{P}) = 1$).

In order to improve the security levels against these frauds without using a final signature, we introduce the notion of *k-Previous Challenge Dependent* (*k-PCD*) protocol, in which each response bit depends on the current and the k previous challenges during fast phase. We define k-PCD protocol as follows.

Definition 3 (k-Previous Challenge-Dependent (k-PCD) Protocol). *Let $g : \mathbb{F}_2^{m+k+1} \rightarrow \mathbb{F}_2$ be a Boolean function. A k-PCD protocol $\mathcal{P}$ is a distance bounding protocol that satisfies following properties*

- *During the fast phase, each response bit r_i is computed as $r_i := g(c_i, \ldots c_{i-k}, y_0^i, \ldots, y_{m-1}^i)$ where c_j is the j-th challenge bit and $(y_0^i, \ldots, y_{m-1}^i)$ is the i-th string of the session secret shared by both prover and verifier for $i = 1, \ldots, n$, where n is the number of rapid bit exchanges.*
- *There is no final slow phase.*

The protocol $\mathcal{P}$ is denoted as $g(c_i, \ldots, c_{i-k}, y_0^i, \ldots, y_{m-1}^i) \rightarrow r_i$ k-PCD protocol. The function g is called the response function of the protocol $\mathcal{P}$.

Remark 1. From Definitions (1) and (2), a CCD protocol is a k-PCD protocol for $k = 0$.

We provide security analysis of 1-PCD protocols. In order to analyze the security against mafia and distance frauds, we present two generic attacks which can be mounted against all 1-PCD protocols. We show that, there is also a trade-off between the security levels of mafia fraud and distance fraud such that $P_{maf}(\mathcal{P}) + P_{dis}(\mathcal{P}) \geq 5/4$ for any 1-PCD protocol $\mathcal{P}$. Let us remark that, this trade-off curve lies below that of CCD protocols. Therefore, we propose a natural extension concept in order to provide a 1-PCD protocol from a CCD protocol. We claim that, the security of existing CCD protocols can be improved by applying natural extension without using a computationally expensive phase (e.g. a final signature). Moreover, we illustrate two natural extensions on HK protocol to make the protocol more secure against all the known attacks. For the first version, we achieve $P_{dis}(HK') \geq 1/2$ and $P_{maf}(HK') \geq 3/4$, and for the second one $P_{dis}(HK'') \geq 5/8$ and $P_{maf}(HK'') \geq 5/8$, in which both versions are optimum among 1-PCD protocols. Finally, we conclude the paper with several conjectures and open problems related to k-PCD protocols.

3 Optimal Security Limits for CCD Protocols

In this section, we show the security trade-off between mafia and distance frauds for CCD protocols. In order to analyze the security against mafia and distance frauds, we consider the characteristics of the response function f used in a CCD protocol. We assume that all the challenges and the shared session secrets, which are used to compute response bits, are uniformly random. For a given response function f, let us define the sets:

$$\mathcal{A} = \{y = (y_0, y_1, \dots, y_{m-1}) \in \mathbb{F}_2^m : f(0, y_0, \dots, y_{m-1}) \neq f(1, y_0, \dots, y_{m-1})\},$$

$$\mathcal{B} = \{y = (y_0, y_1, \dots, y_{m-1}) \in \mathbb{F}_2^m : f(0, y_0, \dots, y_{m-1}) = f(1, y_0, \dots, y_{m-1})\}.$$

Let us denote a and b as the cardinalities of the sets $\mathcal{A}$ and $\mathcal{B}$, respectively. Then, $a + b = 2^m$. We describe a generic distance fraud attack which can be mounted on all CCD protocols given in Algorithm 3.1.

Algorithm 3.1. A Generic Distance Fraud Attack For CCD Protocols(n)

```
n: Number of rounds
for $i \leftarrow 1$ to $n$
  then {
    $t \leftarrow f(0, y_0^i, \dots, y_{m-1}^i) + f(1, y_0^i, \dots, y_{m-1}^i)$
    if $t = 0$
      then Send 0

      else if $t = 2$
      then Send 1

      else
      then Send a random bit
  }
```

We also describe a generic mafia fraud attack that can be mounted on all the CCD protocols. During the slow phase, the adversary relays the messages (e.g nonces or commitments etc.) between the verifier and the prover. Then, during the fast phase she executes the attack described in Algorithm 3.2. We assume that, the protocol is public. So, a and b can be computed during the off-line phase.

Algorithm 3.2. A Generic Mafia Fraud Attack For CCD Protocols(n, a, b)

```
n: Number of rounds
flip: Deciding on flipping the response
if $b \leq a$
  then $flip \leftarrow 1$

  else $flip \leftarrow 0$
for $i \leftarrow 1$ 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*/
for $i \leftarrow 1$ to $n$
  do { record i-th challenge of the verifier in $c_i$
       if $c'_i = c_i$
         then Send $r'_i$

         else Send $r'_i \oplus flip$
```

The following statement gives a trade-off between mafia fraud and distance fraud for CCD protocols.

Theorem 1. *Let $\mathcal{P}$ be a $f(c_i, y_0^i, \ldots, y_{m-1}^i) \rightarrow r_i$ CCD protocol. Assume that c_i and y_j^is used during the fast phase of $\mathcal{P}$ are uniformly random. Then, (i) $P_{maf}(\mathcal{P}) \geq 3/4$, and (ii) $P_{maf}(\mathcal{P}) + P_{dis}(\mathcal{P}) \geq 3/2$.*

Proof. Let us first consider the distance fraud attack described in Algorithm 3.1. For any challenge c_i, the adversary always produces a correct response if $y_0^i, y_1^i, \ldots, y_{m-1}^i$ are in the set $\mathcal{B}$. Otherwise, i.e., when they are in the set $\mathcal{A}$, she successfully predicts the response with a probability of 1/2 because c_i, and y_j^i s are uniformly random. Thus, the success probability of P_{dis} for the attack given in Algorithm 3.1 is equal to $\frac{b}{2^m} \cdot 1 + \frac{a}{2^m} \cdot \frac{1}{2} = \frac{a+2b}{2^{m+1}} = \frac{1}{2} + \frac{b}{2^{m+1}}$.

Concerning the mafia fraud attack given in Algorithm 3.2, let the adversary receive the r'_i responses from the prover for her predicted challenges c'_i. Then, she executes the attack against the verifier. Since c_is are randomly produced by the verifier, there are two equally likely cases. (a) If $c_i = c'_i$ the adversary knows the answer then sends r'_i. (b) If $c_i \neq c'_i$ she has to predict the response bit r_i. The probability that r'_i and r_i are equal is $\frac{b}{2^m}$, and that are not equal is $\frac{a}{2^m}$. The adversary chooses the larger probability in order to decide whether she flips the response bit (i.e., $r'_i \oplus 1$). Then, we have $P_{maf} = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \max\{\frac{a}{2^m}, \frac{b}{2^m}\}$. Since $a + b = 2^m$, $\max\{\frac{a}{2^m}, \frac{b}{2^m}\} \geq \frac{1}{2}$ and this implies that $P_{maf} \geq \frac{3}{4}$.

If $b \leq 2^{m-1}$ $(b \leq a)$, then, $P_{maf} = \dfrac{1}{2} + \dfrac{a}{2^{m+1}}$ for the attack. So, we have $P_{dis} + P_{maf} = \dfrac{3}{2}$. On the other hand, when $b \geq 2^{m-1}$ $(b \geq a)$, $P_{maf} = \dfrac{1}{2} + \dfrac{b}{2^{m+1}} \geq \dfrac{3}{4}$. Thus, $P_{dis}(\mathcal{P}) + P_{maf}(\mathcal{P}) \geq \dfrac{3}{2}$. □

The first part of Theorem 1 indicates that there is a security limit for CCD protocols concerning the mafia fraud, and the second part attests the security trade-off between mafia and distance frauds. Figure 3 depicts the *trade-off curve* between the success probabilities of these frauds for any CCD protocol.

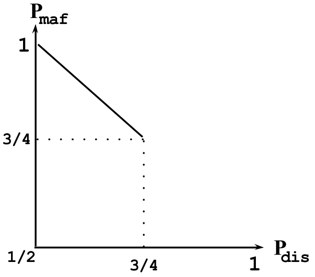

Fig. 3. The trade-off curve between distance and mafia frauds for CCD protocols

One interesting result of Theorem 1 is that CCD protocols cannot attain the ideal security level against the distance fraud without being vulnerable against mafia fraud. This is stated in Corollary 1.

Corollary 1. *For a CCD protocol $\mathcal{P}$, if the security level for the distance fraud is ideal (i.e. $P_{dis}(\mathcal{P}) = 1/2$) then, $P_{maf}(\mathcal{P})$ is* 1.

Proof. The probability $P_{dis}(\mathcal{P})$ satisfies the condition in Theorem 1, so $P_{maf}(\mathcal{P})$=$3/2 - 1/2 \geq 1$. □

Remark 2. Recall that the security levels of the HK protocol against the mafia and distance frauds are both 3/4. Security levels of HK protocol lie on the trade-off curve.

4 Optimal Security Limits for k-PCD Protocols

In this section, we analyze the security of k-PCD protocols. We first describe the several neighborhood concept that is useful for the distance fraud analysis. Then, we introduce two generic attacks for the mafia and the distance frauds that can be mounted on all 1-PCD protocols.

While designing k-PCD distance bounding protocol, there are n-round one-bit challenge/response during fast phase. There is an exceptional case for the first round of this phase. In the first round, the verifier sends k initial challenges before sending c_1. For example, in the first round of a 1-PCD protocol, the verifier first sends c_0 and c_1 then waits for r_1.

4.1 Security Regions for Distance Fraud

Let us consider an adversary who tries to cheat on the distance against a verifier. While producing a response bit r_i, the adversary may use some of the received previous challenges in her attack. This can increase the success probability of the attack. However, receiving the challenges earlier depends on how far the adversary is away from the verifier. Therefore, in order to make the attack analysis simpler, we describe three spherical regions (Z_1, Z_2, Z_3) in which the adversary can communicate with the verifier (see Figure 4). Let d_1 be the maximum radius of Z_1 that is the legal authentication region, and t_1 be the elapsed time for a signal to travel the distance d_1. Z_2 is the annulus region between two concentric spheres with radius of d_1 and $d_1 + d_2$ where $d_2 \geq k \cdot d_1$, and $k = 0, 1, 2, \ldots$. Z_3 is the outside of Z_2. We assume that the speed of the signal is constant.

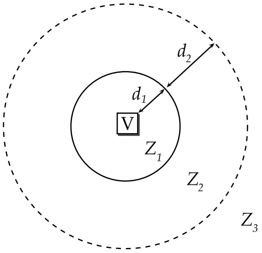

Fig. 4. Regions for distance fraud

When the adversary is in the region Z_1, she always accesses to all the challenges and produces valid responses on time. However, when the distance between the adversary and the verifier is $d_1 + \delta_d$ $(\delta_d > 0)$, any signal traveling this distance takes $t'_1 > t_1$, i.e., $t'_1 = t_1 + \delta_t$. In order to run her attack successfully, the adversary should send each current response (r_i), at least $2\delta_t$ before receiving the current challenge (c_i). When $\delta_t > k \cdot t_1$, she is in region Z_3, she should send the response r_i before receiving $c_i, c_{i-1}, \ldots, c_{i-k}$. However, when the adversary is in Z_2, she accesses some of the previous challenges to send r_i. This may increase the attacker's success probability. As a result, while analyzing the security of a k-PCD protocol against distance fraud, the region of the adversary should be considered.

In the next subsection, we focus on the security of *k-PCD* protocols against mafia and distance frauds when $k = 1$. To make the analysis easier for distance fraud, we assume that the adversary is in Z_3.

4.2 Security Trade-off for 1-PCD Protocols

Let g be the function that outputs the response bit r_i from the challenges c_{i-1}, c_i and the precomputed session secrets $y_0^i, y_1^i, \ldots, y_{m-1}^i$. The function g is executed n times to form the whole set of responses. For $y = (y_0, y_1, \ldots, y_{m-1}) \in \mathbb{F}_2^m$, let α_y be

$$\alpha_y = \sum_{\substack{c_i \in \{0,1\} \\ c_{i-1} \in \{0,1\}}} g(c_i, c_{i-1}, y) - 2.$$

Also, we define the following sets:

$$\begin{aligned} \mathcal{A} &= \{y \in \mathbb{F}_2^m : |\alpha_y| = 2\}, \\ \mathcal{B} &= \{y \in \mathbb{F}_2^m : |\alpha_y| = 1\}, \\ \mathcal{C} &= \{y \in \mathbb{F}_2^m : \ \alpha_y = 0\}, \end{aligned}$$

where $|\cdot|$ denotes the absolute value.

Algorithm 4.1. A Generic Mafia Fraud Attack For 1-PCD Protocols(n, a, c)

```
n: Number of rounds
flip: Deciding on flipping the response
Send a random challenge $c'_0 \in \{0,1\}$ to the prover
if $c \geq 3a$
  then $flip \leftarrow 1$

  else $flip \leftarrow 0$
for $i \leftarrow 1$ 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 of the verifier $c_p$
for $i \leftarrow 1$ to $n$
  do { record i-th challenge of the verifier in $c_i$
       if $c'_i = c_i$ and $c'_{i-1} = c_p$
         then Send $r'_i$

         else Send $r'_i \oplus flip$
       $c_p \leftarrow c_i$
```

The set $\mathcal{A}$ includes the session secrets that produce the same response bit for any c_i and c_{i-1}. The set $\mathcal{B}$ consists the session secrets that produce the responses, majority of them are equal, for any c_i and c_{i-1}. The set $\mathcal{C}$ contains the session secrets that produce the responses, half of them are equal, for any c_i and c_{i-1}.

Let us denote a, b and c as the cardinalities of the sets $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$, respectively. Then we have $a + b + c = 2^m$. We assume that all the challenges and the precomputed session secret bits, which are used to compute response bits, are uniformly random.

Algorithm 4.2. A Generic Distance Fraud Attack For 1-PCD Protocols(n)

```
n: Number of rounds
$c_p \leftarrow \{0,1\}$
for $i \leftarrow 1$ to $n$
  then
    if $\alpha_{y^i} = 1$
      then
        Send 1
        if $g(0, c_p, y_0^i, \dots, y_{m-1}^i) = 1$
          then $c_p \leftarrow 0$
          else $c_p \leftarrow 1$
    else if $\alpha_{y^i} = -1$
      then
        Send 0
        if $g(0, c_p, y_0^i, \dots, y_{m-1}^i) = 0$
          then $c_p \leftarrow 0$
          else $c_p \leftarrow 1$
    else
      then
        Send $g(0, c_p, y_0^i, \dots, y_{m-1}^i)$
        $c_p \leftarrow 0$
    $c_p \leftarrow c_i$
```

We introduce a generic mafia fraud attack and a generic distance fraud attack which can be mounted on all 1-PCD protocols. The mafia fraud attack and the distance fraud attack, given in Algorithm 4.1, Algorithm 4.2 are the extensions of the the attacks given in Algorithm 3.2 and Algorithm 3.1 to 1-PCD protocols, respectively. The values a, b, and c are computed during the off-line phase from the function g. Given a response generating function g, the cardinalities are computed as the expected number of elements in each set. In addition, during the slow phase the adversary relays the messages (e.g. nonces or commitments) between the verifier and the prover.

The following statement defines a security bound for mafia fraud in any rapid bit exchange round of the 1-PCD protocols and gives a trade-off between P_{dis} and P_{maf} for 1-PCD protocols. The statement is obtained by computing P_{maf} and P_{dis} of the Algorithm 4.1 and 4.2, respectively.

Theorem 2. *Let $\mathcal{P}$ be a $f(c_i, c_{i-1}y_0^i, \dots, y_{m-1}^i) \rightarrow r_i$ 1-PCD protocol. Assume that c_is and y_j^is used in the fast phase of the protocol $\mathcal{P}$ are uniformly random. Then $P_{maf}(\mathcal{P}) \geq 5/8$, and $P_{maf}(\mathcal{P}) + P_{dis}(\mathcal{P}) \geq 5/4$.*

Proof. Considering distance fraud attack depicted in Algorithm 4.2, for any challenge value, the adversary can always guess a correct response if y^i is in the set $\mathcal{A}$. If it is in the set $\mathcal{B}$, she can predict the response with probability 3/4. However, if it is in the set $\mathcal{C}$, she can predict the response with probability 1/2. Therefore, the success probability P_{dis} for this attack is computed as follows:

$$\begin{aligned} P_{dis} &= \frac{a}{2^m} \cdot 1 + \frac{b}{2^m} \cdot \frac{3}{4} + \frac{c}{2^m} \cdot \frac{1}{2} \\ &= \frac{1}{2} + \frac{2a+b}{2^{m+2}}. \end{aligned} \tag{2}$$

Considering the mafia fraud attack described in Algorithm 4.1, let an adversary first query the prover with predicted challenges c'_i and get the corresponding responses r'_i. Then, the adversary carries out the attack against the verifier. The adversary knows the correct response (i.e., $r'_i = r_i$) if $c_{i-1} = c'_{i-1}$ and $c_i = c'_i$. The probability of this event is 1/4 since all the challenge bits are produced uniformly random. For the remaining cases, the adversary has to predict the corresponding response bit r_i.

The attacker has to predict the response bit r_i corresponding to a different pair of challenge bits (c_i, c_{i-1}). If the corresponding session secret y^i is in the set $\mathcal{A}$, then the probability that $r_i = r'_i$ is 1 by definition. This probability reduces to 1/2 if y^i is in the set $\mathcal{B}$ since this happens only if both the input vectors (c_i, c_{i-1}, y^i) and (c'_i, c'_{i-1}, y^i) produce the same response even though the vectors are not equal. Similarly, the probability is 1/3 if y^i is in the set $\mathcal{C}$. Then, the probabilities that $r_i \neq r'_i$ are deduced straightforward.

The attacker has two strategies for predicting a response value corresponding to a different pair of challenge bits.

(i) She sends the same response value received from the prover (r'_i) and the success probability of mafia fraud $(P^{no-flip}_{maf})$ is computed as follows.

$$\begin{aligned} P^{no-flip}_{maf} &= \frac{1}{4} + \frac{3}{4} \cdot (\frac{a}{2^m} \cdot 1 + \frac{b}{2^m} \cdot \frac{1}{2} + \frac{c}{2^m} \cdot \frac{1}{3}) \\ &= \frac{1}{2} + \frac{4a+b}{2^{m+3}}. \end{aligned} \tag{3}$$

(ii) She sends the complement of the response value and the success probability of mafia fraud with this strategy is computed as follows.

$$\begin{aligned} P^{flip}_{maf} &= \frac{1}{4} + \frac{3}{4} \cdot (\frac{a}{2^m} \cdot 0 + \frac{b}{2^m} \cdot \frac{1}{2} + \frac{c}{2^m} \cdot \frac{2}{3}) \\ &= \frac{1}{4} + \frac{3b+4c}{2^{m+3}}. \end{aligned} \tag{4}$$

Both $P^{no-flip}_{maf}$ and P^{flip}_{maf} probabilities depend on the characteristic of function g. The adversary chooses the larger probability. Hence, we get

$$P_{maf} = \max(P_{maf}^{no-flip}, P_{maf}^{flip}) \\ = \frac{1}{2} + \frac{b}{2^{m+3}} + \max(\frac{4a}{2^{m+3}}, \frac{2c-2a}{2^{m+3}}). \tag{5}$$

When $c \geq 3a$, we have $P_{maf}^{flip} \geq P_{maf}^{no-flip}$. So,

$$P_{maf} = \frac{1}{2} + \frac{b+2c-2a}{2^{m+3}} \\ = \frac{5}{8} + \frac{c-3a}{2^{m+3}} \\ \geq \frac{5}{8}. \tag{6}$$

Then we have $P_{dis} + P_{maf}^{flip} = 1 + \frac{2 \cdot (a+b+c)+b}{2^{m+3}} \geq \frac{5}{4}$ for the attacks in Algorithms (4.1) and (4.2). On the other hand, if $c \leq 3a$, then $P_{maf}^{no-flip} \geq P_{maf}^{flip}$. Hence,

$$P_{maf} = \frac{1}{2} + \frac{4a+b}{2^{m+3}} \\ = \frac{5}{8} + \frac{3a-c}{2^{m+3}} \\ \geq \frac{5}{8}. \tag{7}$$

In this case, we have $P_{dis} + P_{maf}^{no-flip} = 1 + \frac{8a+3b}{2^{m+3}} = \frac{5}{4} + \frac{b+2 \cdot (3a-c)}{2^{m+3}} \geq \frac{5}{4}$. Hence, (6) and (7) yield that the success probability of mafia fraud cannot be less than 5/8. Thus, $P_{maf}(\mathcal{P}) + P_{dis}(\mathcal{P}) \geq \frac{5}{4}$. □

Figure 5 compares the trade-off curves for 1-PCD and CCD protocols, between the success probabilities of mafia and distance frauds. The figure shows that, the trade-off curve for 1-PCD is closer to the ideal security than the curve for CCD protocols. Another interesting result of the theorem is that 1-PCD protocols can attain the ideal security level against the distance fraud while $P_{maf} \geq 3/4$.

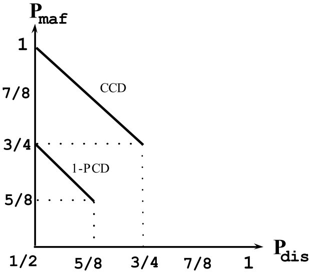

Fig. 5. Comparison of the trade-off curves for CCD and 1-PCD protocols

Corollary 2. *For a* 1*-PCD protocol* $\mathcal{P}$*, if the security level for the distance fraud is ideal (i.e* $P_{dis}(\mathcal{P}) = 1/2$*) then,* $P_{maf}(\mathcal{P}) \geq 3/4$*.*

Proof. The probability $P_{dis}(\mathcal{P})$ satisfies the condition in Theorem 2, so P_{maf} $(\mathcal{P}) \geq \frac{5}{4} - \frac{1}{2} = \frac{3}{4}$. □

4.3 Simulation

We implement four different 1-PCD response generating functions on HK protocol structure. We simulate the attacks given in Algorithms 4.1 and 4.2 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 1, are in parallel with the results in Theorem 2.

Table 1. The simulation results for success probabilities of mafia fraud and distance fraud

a	b	c	P_{maf}	P_{dis}
1	0	3	0.6247	0.6249
2	1	1	0.7813	0.8124
0	0	4	0.7498	0.4996
0	4	0	0.6251	0.7500

5 Enhancing Security of CCD Protocols by Extending to 1-PCD

In the previous section, we have shown that 1-PCD protocols can provide better security than the CDD protocols. In this section, we aim to give a method to ameliorate the security of CCD protocols by extending them to 1-PCD protocols. We first introduce the notion of a natural extension. Then, we apply this extension on an existing protocol to show the security enhancement.

Let $\mathcal{P}$ be a CCD protocol with the response function $f(c_i, y_0^i, \ldots, y_{m-1}^i) \rightarrow r_i$ and $\mathcal{P}'$ be a 1-PCD protocol with the response function $g(c_i, c_{i-1}, y_0^i, \ldots, y_{m-1}^i)$ $\rightarrow r_i'$. We give the definition for a natural extension of a CCD protocol to provide a 1-PCD protocol as follows.

Definition 4 (Natural Extension for CCD to 1-PCD). $\mathcal{P}'$ *is called a* natural extension *of* $\mathcal{P}$ *if* $g(c_i, c_{i-1}, y_0^i, \ldots, y_{m-1}^i)$ *is a Boolean function of the variables* $f(Q(c_i, c_{i-1}), y_0^i, \ldots, y_{m-1}^i)$ *and* $T(c_i, c_{i-1})$*, where* Q *and* T *are Boolean functions of two variables.*

The objective of the natural extension is not to propose a new distance bounding protocol but enhancing the security level of a given protocol via extending its response function by using simple polynomial arithmetic. We want to show that the security level can be improved without using a computationally expensive final signature.

We study HK protocol as an example of CCD protocols which has the security levels as 3/4 against both mafia and distance frauds. We provide two natural extensions on this protocol: (i) The first version is to provide the ideal security level for distance fraud (i.e., 1/2), and (ii) The second one is to achieve the best security against mafia fraud (i.e. 5/8) among 1-PCD protocols.

5.1 A Natural Extension of HK Protocol for Improving Distance Fraud Resistance

In order to obtain the ideal security against distance fraud, we construct a response generating function such that $a = 0$, $b = 0$ and $c = 4$ (see Equation (2)). Therefore, we extend the response function of the original HK protocol (see Equation 1) by choosing $Q(c_{i-1}, c_i) = c_i$ and $T(c_{i-1}, c_i) = c_{i-1}$. We have the extended response function as follows.

$$\begin{aligned} g(c_i, c_{i-1}, y_0^i, y_1^i) &= f(c_i, y_0^i, y_1^i) \oplus c_{i-1} \\ &= c_i \cdot y_1^i \oplus ((1 \oplus c_i) \cdot y_0^i) \oplus c_{i-1} \\ &= y_{c_i}^i \oplus c_{i-1} \end{aligned} \tag{8}$$

Equation (8) shows that, we obtain the natural extension by only XORing the original HK protocol's response function with c_{i-1}. In what follows, we analyse this extended version-1 to show the security enhancement of distance fraud.

Security analysis of extended version-1. As stated in Section 4, we apply the generic attacks for mafia fraud and distance fraud on extended protocol as follows.

Considering the mafia fraud attack described in Algorithm 4.1, the adversary uses the strategy of sending complement of the response received from the tag when she does not guess the challenges correctly since $c \geq 3a$. Therefore, by using Equation (4) the success probability of mafia is computed as $P_{maf} = \frac{1}{4} + \frac{3 \cdot 0 + 4 \cdot 2^m}{2^{m+3}} = \frac{3}{4}$.

While considering the distance fraud attack given in Algorithm 4.2 three regions should be taken into account as described in Section 4.

- In region Z_1, the prover can access all the challenges and there is no attack.
- In Z_2, the prover can access c_{i-1} challenge but she has no knowledge on c_i while sending r_i. She can compute two different r_i values using session secrets. In the first case, the adversary can always send a valid response r_i when $y_0^i = y_1^i$. In other case, she guesses r_i value with probability of 1/2 when $y_0^i \neq y_1^i$. Hence, the distance fraud probability for a single challenge-response is $1/2 \cdot 1 + 1/2 \cdot 1/2 = 3/4$. Therefore, it is concluded that when the prover is in Z_2 the security of the extended version is equivalent to the original HK protocol.
- In Z_3, the prover is not able to access both c_{i-1} and c_i challenges while computing the response r_i. Equation (2) yields $P_{dis} = 1/2$.

5.2 A Natural Extension of HK Protocol for Improving Mafia Fraud Resistance

We apply another natural extension for HK protocol to obtain an optimum security level for mafia fraud among 1-PCD protocols (i.e. $P_{maf} = \frac{5}{8}$). Considering the Equations (6) and (7), we construct a response function that satisfies $c = 3a$, also $a = 1$, $b = 0$ and $c = 3$. The natural extension on the response function is given below.

$$\begin{aligned} g(c_i, c_{i-1}, y_0^i, y_1^i) &= f(c_i, y_0^i, y_1^i) \oplus f((1 \oplus c_{i-1}), y_0^i, y_1^i) \\ &= y_{c_i}^i \oplus y_{\bar{c}_{i-1}}^i, \end{aligned} \tag{9}$$

where $\bar{c}_{i-1}$ is the complement of c_{i-1} (i.e. $1 \oplus c_{i-1}$).

Security analysis of extended version-2. While analyzing the mafia fraud attack described in Algorithm 4.1, the adversary may use any of the strategies described in Section 4 since $c = 3a$. Therefore, both Equations (6) and (7) yields that, $P_{maf} = 5/8$.

Considering the distance fraud in region Z_2, the security level is same as the original HK protocol (i.e. 3/4) since the response function becomes same as in the HK protocol when the adversary receives c_{i-1}. In Z_3, the prover cannot access both c_{i-1} and c_i challenges while computing the response r_i. By using Equation (2), the success probability of distance fraud is calculated as $P_{dis} = 5/8$.

6 Discussion and Open Problems

In this paper, we have classified the low-cost RFID distance bounding protocols having no final signature and introduced the notion of CCD protocols and k-PCD protocols. We have shown that there is a trade-off between the security levels of mafia fraud and distance fraud for both CCD protocols and 1-PCD protocols. We have constructed trade-off curves by introducing generic attacks mounted on CCD protocols and 1-PCD protocols. On the other hand, there are several questions left open. The most natural questions may be the following ones:

- Are the attacks given in Algorithm 3.1 and Algorithm 3.2 the best generic attacks mounted on CCD protocols? In other words, is there a trade-off curve lying above the curve $P_{maf} + P_{dis} = 3/2$ for CCD protocols?
- Similar question for 1-PCD protocols can be given as: Is there a trade-off curve lying above the curve $P_{maf} + P_{dis} = 5/4$ for 1-PCD protocols?

We conjecture that the both curves deduced in the paper are the best trade-off curves. That is, the answer to the both questions above seems to be "no". Apart from the security analysis of CCD protocols and 1-PCD protocols, it is still an open question to construct trade-off curves for k-PCD protocols where $k > 1$. In general, we expect the security to be enhanced when k is increased. More formally, we have the following conjecture:

Conjecture 1. The best trade-off curve for k_1-PCD protocols lies above the best trade-off curve for k_2-PCD protocols where $k_1 < k_2$.

The most general question may be how far the security is enhanced when k is increased. Could we attain the ideal security when k is large enough? We have the following conjecture for this:

Conjecture 2. $P_{maf} + P_{dis}$ tends to 1 when k and n both tends to infinity.

In summary, we claim that the security levels approach the ideal security when k is increased. If it is really true, then the next question is how fast $P_{maf} + P_{dis}$ tends to 1? For practical purpose, it must be quite fast and we believe it is really fast.

Acknowledgment

This work has been partially funded by FP7-Project ICE under the grand agreement number 206546, and by the Walloon Region Marshall plan through the SPW DG06 Project TRASILUX. The authors wish to thank Mehmet Sabir Kiraz, Benjamin Martin, and Umut Uludag for their helpful comments.

References

1. Avoine, G., Floerkemeier, C., Martin, B.: RFID Distance Bounding Multistate Enhancement. In: Roy, B., Sendrier, N. (eds.) INDOCRYPT 2009. LNCS, vol. 5922, pp. 290–307. Springer, Heidelberg (2009)
2. Avoine, G., Tchamkerten, A.: An Efficient Distance Bounding RFID Authentication Protocol: Balancing False-acceptance Rate and Memory Requirement. In: Samarati, P., Yung, M., Martinelli, F., Ardagna, C.A. (eds.) ISC 2009. LNCS, vol. 5735, pp. 250–261. Springer, Heidelberg (2009)
3. Beth, T., Desmedt, Y.: Identification Tokens - or: Solving the Chess Grandmaster Problem. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 169–177. Springer, Heidelberg (1991)
4. Brands, S., Chaum, D.: Distance-Bounding Protocols. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 344–359. Springer, Heidelberg (1994)
5. Capkun, S., Butty'an, L., Hubaux, J.-P.: SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In: ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN 2003, Fairfax, Virginia, USA, pp. 21–32. ACM Press, New York (October 2003)
6. Desmedt, Y.: Major security problems with the' Unforgeable' (Feige)-Fiat-Shamir proofs of identity and how to overcome them. In: SecuriCom 1988, pp. 15–17 (1988)
7. Desmedt, Y., Goutier, C., Bengio, S.: Special uses and abuses of the fiat-shamir passport protocol. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 21–39. Springer, Heidelberg (1988)
8. Hancke, G.: A Practical Relay Attack on ISO 14443 Proximity Cards. (February 2005) (manuscript)
9. Hancke, G., Kuhn, M.: An RFID Distance Bounding Protocol. In: Conference on Security and Privacy for Emerging Areas in Communication Networks, SecureComm 2005, Athens, Greece. IEEE Computer Society Press, Los Alamitos (September 2005)

10. Hancke, G., Mayes, K., Markantonakis, K.: Confidence in Smart Token Proximity: Relay Attacks Revisited. Elsevier Computers & Security (June 2009)
11. Kapoor, G., Zhou, W., Piramuthu, S.: Distance Bounding Protocol for Multiple RFID Tag Authentication. In: Proceedings of the 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, EUC 2008, Shanghai, China, pp. 115–120. IEEE Computer Society Press, Los Alamitos (December 2008)
12. Kim, C.H., Avoine, G.: RFID distance bounding protocol with mixed challenges to prevent relay attacks. In: Garay, J.A., Miyaji, A., Otsuka, A. (eds.) CANS 2009. LNCS, vol. 5888, pp. 119–133. Springer, Heidelberg (2009)
13. Kim, C.H., Avoine, G., Koeune, F., Standaert, F.-X., Pereira, O.: The Swiss-Knife RFID Distance Bounding Protocol. In: Lee, P.J., Cheon, J.H. (eds.) ICISC 2008. LNCS, vol. 5461, pp. 98–115. Springer, Heidelberg (2009)
14. Munilla, J., Peinado, A.: 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)
15. Nikov, V., Vauclair, M.: Yet Another Secure Distance-Bounding Protocol. Cryptology ePrint Archive, Report 2008/319 (2008)
16. Reid, J., Gonzalez Neito, J., Tang, T., Senadji, B.: Detecting relay attacks with timing based protocols. In: Bao, F., Miller, S. (eds.) Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, ASIACCS 2007, Singapore, Republic of Singapore, pp. 204–213. ACM Press, New York (March 2007)
17. Singelée, D., Preneel, B.: Distance Bounding in Noisy Environments. In: Stajano, F., Meadows, C., Capkun, S., Moore, T. (eds.) ESAS 2007. LNCS, vol. 4572, pp. 101–115. Springer, Heidelberg (2007)
18. Tu, Y.-J., Piramuthu, S.: RFID Distance Bounding Protocols. In: First International EURASIP Workshop on RFID Technology, Vienna, Austria (September 2007)

A Hancke and Kuhn's Protocol

Hancke and Kuhn [9] proposed a simple and efficient distance bounding protocol that has been used as a key-reference in RFID context. Hancke and Kuhn's protocol consists of two phases: *Slow phase* and *fast phase* (or rapid bit exchange phase). As depicted in Figure 6 the protocol steps are as follows.

Slow phase – The prover and the verifier exchange randomly generated nonces. From these nonces and a shared secret x both party compute two $n-bit$ registers y_0 and y_1, using a pseudo-random function h. These registers are used as session secrets during the fast phase.

Fast phase – The verifier sends a random challenge c_i to the prover, then the later replies with r_i, by using the challenge and shared session secrets such that $f(c_i, y_0^i, y_1^i) = y_{c_i}^i$, where $i = 1, 2 \ldots n$. For each rapid bit exchange the verifier measures the round trip time Δt_i. After n rapid bit exchanges the verifier checks the correctness of r_i's and $\Delta t_i \leq t_{max}$ where n is the security parameter and t_{max} is the maximum allowed time delay for each rapid bit exchange.

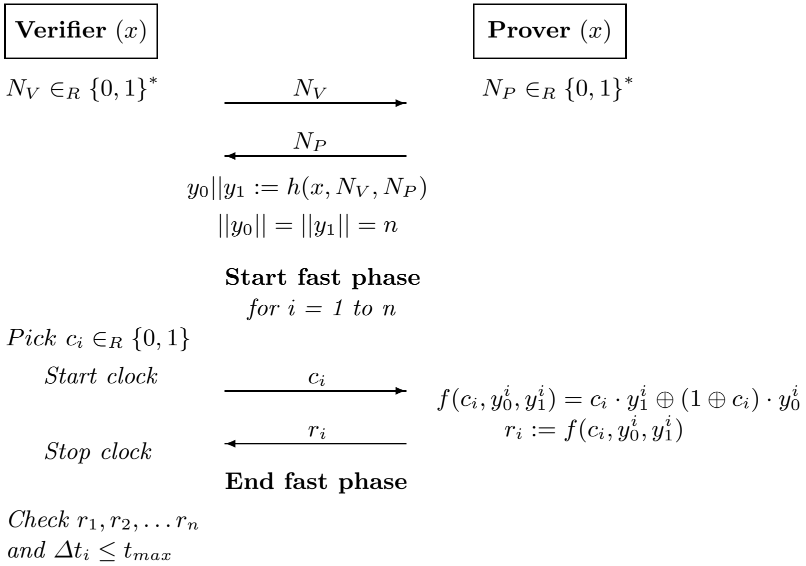
Verifier (x)
Prover (x)
$N_V \in_R \{0,1\}^*$
N_V
$N_P \in_R \{0,1\}^*$
N_P
$y_0||y_1 := h(x, N_V, N_P)$
$||y_0|| = ||y_1|| = n$
Start fast phase
for i = 1 to n
Pick $c_i \in_R \{0,1\}$
Start clock
c_i
$f(c_i, y_0^i, y_1^i) = c_i \cdot y_1^i \oplus (1 \oplus c_i) \cdot y_0^i$
$r_i := f(c_i, y_0^i, y_1^i)$
r_i
Stop clock
End fast phase
Check $r_1, r_2, \ldots r_n$
and $\Delta t_i \leq t_{max}$

Fig. 6. Hancke and Kuhn's protocol

Distance Fraud Analysis. Let P be the prover who carries out the attack, and V be the verifier who wants to be sure that P is inside the authentication region. P can compute all session secrets (i.e. two $n - bit$ registers) as soon as they exchanged the nonces. During the rapid bit exchange, P should send a response r_i before receiving the challenge c_i in order to accomplish the attack. She computes two response r_i values using two registers. In half of the cases, they are the same and P always sends the correct r_i. In the remaining cases, they are not the same and P correctly predict r_i value with probability 1/2. Hence, for any i, P sends a valid r_i corresponding to the challenge c_i with probability $\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$. Since n rounds occurs during the fast phase, the success probability of the attack is $(\frac{3}{4})^n$.