On Modeling Terrorist Frauds

Addressing Collusion in Distance Bounding Protocols

Serge Vaudenay

EPFL, Lausanne, Switzerland
http://lasec.epfl.ch

Abstract. Quite recently, distance-bounding protocols received a lot of attention as they offer a good solution to thwart relay attacks. Their security models at still unstable, especially when considering terrorist fraud. This considers the case where a malicious prover would try to bypass the protocol by colluding with an adversary without leaking his credentials. Two formal models appeared recently: one due to Fischlin and Onete and another one by Boureanu, Mitrokotsa, and Vaudenay. Both were proposed with a provably secure distance-bounding protocols (FO and SKI, respectively) providing security against all state-of-the-art threat models. So far, these two protocols are the only such ones.

In this paper we compare both notions and protocols. We identify some errors in the Fischlin-Onete results. We also show that the design of the FO protocol lowers security against mafia frauds while the SKI protocol makes non-standard PRF assumptions and has lower security due to not using post-authentication. None of these protocols provide reasonable parameters to be used in practice with a good security. The next open challenge consists in providing a protocol combining both approaches and good practical parameters.

Finally, we provide a new security definition against terrorist frauds which naturally inspires from the soundness notion for proof-of-knowledge protocols.

1 Introduction

Relay attacks and distance-bounding. Many access control protocols are vulnerable to relay attacks. This is the case of most of RFID-based protocols. To defeat this, distance-bounding protocols offer a practical solution. These protocols, originally proposed by Brands and Chaum [6], consist of proving that a *prover* is within a close distance to a *verifier* by using an interactive protocol. The protocol is based on the physical limits of communication. Namely, transmission cannot go faster than the speed of light. So, these protocols use a rapid-bit exchange phase in which the prover must respond extremely fast and messages are very short (typically: single bits), in order to prove that he is close enough.

Threat models. Clearly, distance-bounding shall resist to *distance fraud*, where a malicious prover tries to defeat the protocol by passing even though he is far away. They shall also defeat relay attacks and more general notions of man-in-the-middle attacks where an adversary abuse of a far-away prover to pass the protocol. This is what makes practitioners like distance-bounding protocols. These types of attacks are often refer to as *mafia frauds*, following a (quite unfortunate) terminology due to Desmedt [9]. A more subtle notion from [9] consists of the *terrorist fraud*. There, the prover is also malicious, but still far away. He is colluding with an adversary (who can be close to the verifier) to pass the protocol, but without leaking his credentials to him. As discussed below, this type of attack is very tricky, not always considered, and quite often incorrectly addressed.

Many protocols and (informal) security notions have been proposed. Some protocols have been semi-formally proven secure but most of results were shown to be incorrect. For instance, some protocols based on a pseudorandom function (PRF) were incorrectly proven secure, as shown in [2]. Consequently, and as far as we know, none existing protocols (except the two which are discussed in this paper) are proven to provide security against all the above threat models. We refer the reader to [5] for a selective survey on the evolution of protocols which has led to the current models and schemes.

There also exist some "more exotic" threat models such as distance hijacking [8] where a far away malicious prover abuses other provers to pass the protocol with the verifier.

The Problem of Terrorist Fraud. Originally, "terrorist fraud" [9] consisted in having a malicious prover helping an adversary to impersonate him but without leaking his credentials. To safeguard against this type of attack means that a malicious prover cannot help an adversary to impersonate him without making this help reusable. Namely, there must be no other way than transferring the credentials to a close participant in order to make the protocol succeed.

The Hancke-Kuhn protocol: a Case Study. To illustrate this notion, we first give the example of a prominent distance-bounding protocol: the Hancke-Kuhn protocol [14]. The prover and the verifier share a long-term secret x. (See Fig. 1.) They first exchange some nonces. Then, a PRF f keyed with x is used to derive some one-time n-bit keys a_1 and a_2. Then, they go through n rounds of rapid bit-exchange: the verifier sends a random challenge $c_i \in \{1, 2\}$ and the prover responds by the ith bit of a_{c_i}. A terrorist fraud is easy: the malicious prover helps the adversary to exchange the nonces then computes a_1 and a_2 and gives them to the adversary. So, the adversary can successfully go through the rapid bit-exchanges. Additionally, disclosing a_1 and a_2 does not expose x since we use a secure PRF.

One difficulty with resistance to terrorist fraud is that it is non-falsifiable. Indeed, we cannot falsify security just by exhibiting an attack. The attack must be such that we could prove that the credentials do not leak, which is not always easy to prove. (In the above example, this is based on the PRF assumption.)

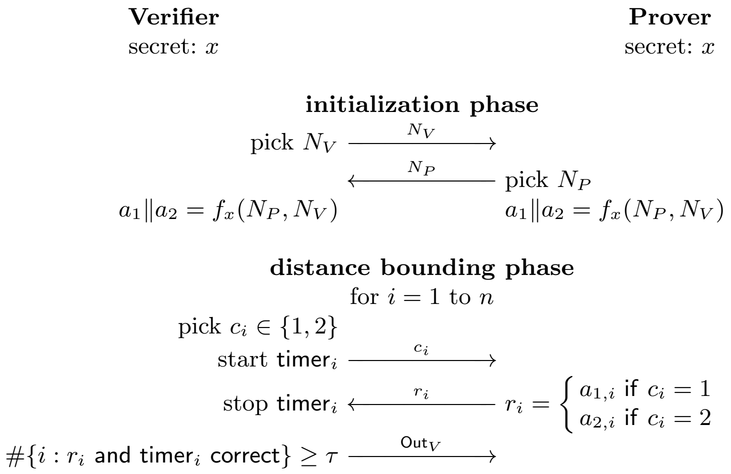


Fig. 1. The Hancke-Kuhn Distance-Bounding protocol [14]

A common technique to strengthen the Hancke-Kuhn protocol consists of using $a_2 = a_1 \oplus x$. This way, the prover cannot disclose a_1 and a_2 without exposing x. Unfortunately, it becomes vulnerable to a man-in-the-middle attack [15] in which the man-in-the-middle flips one challenge c_i and sends $\bar{c}_i$ to the prover. So, he can learn the ith bit from $a_{\bar{c}_i}$ from the prover and deduce from the protocol outcome the ith bit of a_{c_i}. To avoid this attack, Kim *et al.* [15] proposed the Swiss-Knife protocol, in which the protocol transcript is authenticated before the protocol outcome is revealed. (See Fig. 2.)

Terrorist Fraud using resilience to noise. Unfortunately, this does not protect against terrorist fraud as soon as noisy channels are considered. Indeed, the rapid bit-exchange must be done under heavy constraints and it is likely that noise will corrupt a few rounds in honest executions. So, protocols must tolerate a constant number of incorrect rounds. In the protocols, we assume that authentication succeeds when the number of successful rounds is at least τ out of n. In practice, $\frac{\tau}{n}$ must be a constant ratio depending on physical constraints.

It was observed by Hancke [13] that a malicious prover could still provide some noisy versions of a_1 and a_2 so that the number of succeeding rounds is likely to be at least τ (due to noise resilience) but $a_1 \oplus a_2$ would only leak a noisy version of x. Concretely, we can imagine a function g mapping x to a small (but constant-sized) set of indices $g(x)$ and that a_1 and a_2 would be random at all positions specified in $g(x)$. So, the number of possible x is exponential and x does not leak. Without the noiseless version of x, we cannot evaluate the PRF. So, the credential does not leak.

Related work. Avoine *et al.* [1] give a complete but very informal security model for distance-bounding. A more promising model is the one due to Dürholz *et*

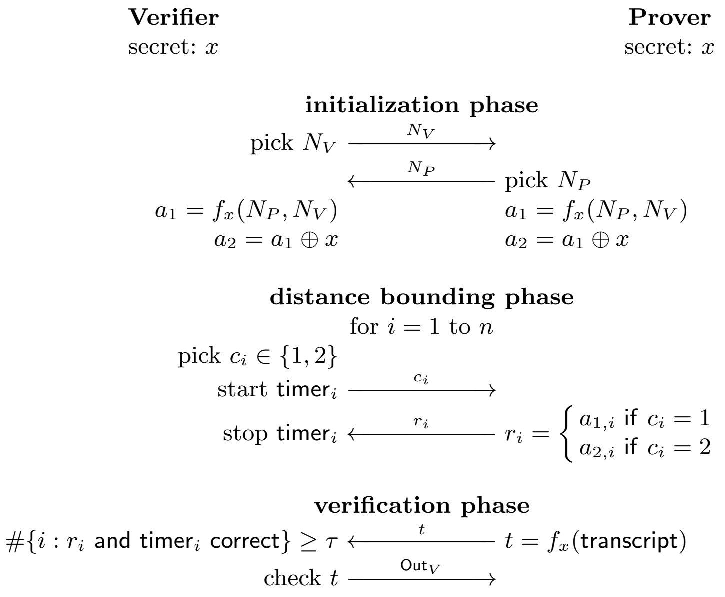

Verifier
secret: x
Prover
secret: x
initialization phase
pick N_V $\xrightarrow{N_V}$
$\xleftarrow{N_P}$ pick N_P
$a_1 = f_x(N_P, N_V)$
$a_2 = a_1 \oplus x$
$a_1 = f_x(N_P, N_V)$
$a_2 = a_1 \oplus x$
distance bounding phase
for $i = 1$ to n
pick $c_i \in \{1, 2\}$
start timer_i $\xrightarrow{c_i}$
stop timer_i $\xleftarrow{r_i}$ $r_i = \begin{cases} a_{1,i} & \text{if } c_i = 1 \\ a_{2,i} & \text{if } c_i = 2 \end{cases}$
verification phase
$\#\{i : r_i \text{ and } \mathsf{timer}_i \text{ correct}\} \geq \tau$ $\xleftarrow{t}$ $t = f_x(\mathsf{transcript})$
check t $\xrightarrow{\mathsf{Out}_V}$

Fig. 2. The Swiss-Knife Distance-Bounding protocol [15]

al. [10]. It separates the use of rapid-bit exchange and regular communication and is based on communication traces in the rapid exchange phase. They propose the notion of SimTF security to model resistance to terrorist frauds. Unfortunately, they show that essentially no existing protocol satisfies this notion and suspect in [11] that this notion may be too demanding. In [12], they finally provide a protocol (called the FO protocol in this paper) providing this security notion and all the above ones. In parallel, Boureanu *et al.* [3,4,5] propose another model which introduces the notion of location and communication time. They also propose to model resistance to terrorist frauds, but with a notion called *collusion fraud*. Additionally, they construct a family of protocols (the SKI protocols) which offer provable security against all the above security notions.

Our results. In this paper, we identify some errors from [12]. Namely, the modified SwissKnife (MSK) protocol does not satisfy the security which is proven in [12] and some probability parameters in the FO protocol are too low.

Then, we compare the FO and SKI protocols. We show that FO has a non-uniform security against distance frauds. We show that the SimTF notion that the FO protocol must satisfy degrades resistance to mafia frauds. Consequently, the number of rounds must be very high to obtain a good security. E.g., 163 rounds are needed for a security level equivalent to a 20-bit symmetric key. With SKI, this is the same for distance fraud (but with a uniform security), this is worse for collusion fraud (with 531 rounds), but the security against man-in-the-middle (what we like distance-bounding for) only requires 76 rounds. All this holds for $\tau/n = 90\%$.

Finally, we compare the security notions to protect against terrorist frauds. We also propose a new one which is naturally inspired from the notion of soundness in proofs-of-knowledge: a distance-bounding protocol is sound if there is an extractor who can extract the secret from the view of close participants by having the protocol successfully executed. We prove that SKI satisfies this notion and prove again $\mathsf{strSimTF}$ security for the FO protocol with corrected parameters.

Notations. In what follows, we will use B defined by

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

It is known [7] that for $\tau = nt$, t and q constant such that $t > q$, and $n \to +\infty$, we have

$$B(n,\tau,q) \sim \frac{1}{\sqrt{2\pi}} \int_{(t-q)\sqrt{\frac{n}{q(1-q)}}}^{+\infty} e^{-\frac{x^2}{2}}\,dx \sim \frac{1}{\sqrt{2\pi}} \sqrt{\frac{q(1-q)}{n(t-q)^2}} e^{-\frac{n(t-q)^2}{2q(1-q)}}$$

So, we have the following result.

Lemma 1. *For t and q constant such that $t > q$, we have*

$$\lim_{n\to+\infty} -\frac{1}{n} \ln B(n,nt,q) = \frac{(t-q)^2}{2q(1-q)}$$

2 The Fischlin-Onete Approach

2.1 SimTF Security

In [10], Dürholz *et al.* propose a way to formalize the security against terrorist fraud. It is referred to as the SimTF security in [12]. This model tells apart communications through a *lazy* (regular) channel from the ones through a time-critical channel. There is a special notion of *tainted* session which depends on the security notion.

Definition 2 (SimTF security). *We consider two experiments. In the first one, the malicious prover P^* and the adversary A interact with the verifier V. A rapid exchange between V and A is tainted if we can make a sequence of messages $m_{VA}, m_{AP^*}, m_{P^*A}, m_{AV}$ in chronological order such that m_{UV} is sent from U then received by V. We denote by p_A the probability that the verifier accepts in this first experiment. In the second experiment, we first run the previous experiment, then provide a simulator S with the final view of A. S then interacts alone with V in a new session. We denote by p_S the probability that the verifier accepts in this last session.*

We say that a terrorist fraud (A, P^*) is successful if for all S we have $p_S \leq p_A$.

So, P^* and A are not allowed to interact during the rapid exchange between V and A. In [11], it was shown that essentially none of the existing protocols offers SimTF security, but it was suggested that this could be due to the notion being too strong.

This notion was strengthened even more in [12] by changing the notion of tainted session. In this strengthened notion, P^* and A can interact during the distance bounding phase, but they are not allowed to have any single round (instead of the session) of rapid bit-exchange which goes through the V-A-P^*-A-V loop. This is the $\mathsf{strSimTF}$ notion.

2.2 GameTF Security

In [12], Fischlin and Onete proposed a weaker notion.

Definition 3 (GameTF security). *Let $\mathsf{Adv}^{\mathsf{MF}}$ be the best probability that a verifier accepts in a mafia-fraud attack. (The maximum is taken over all adversaries with limited complexity and number of queries to P and V.)*

A terrorist fraud (P^*, A) is helpful *to an adversary A' if running an experiment with V, A, and P^* and no tainted session, then running a second experiment with V, A', and P, with A' initialized with the final view of A and no tainted session, makes V accept with a probability $P_{A'}$ which is larger than $\mathsf{Adv}^{\mathsf{MF}}$. (The complexity bounds of $\mathsf{Adv}^{\mathsf{MF}}$ must be satisfied by A'.) We use the notion of tainted session from strSimTF.*

We have ε-GameTF security if all terrorist fraud (P^*, A) succeeding with $p_A \geq \varepsilon$ are helpful for at least one adversary A'.

Remark 4. The probability $\mathsf{Adv}^{\mathsf{MF}}$ of the best mafia-fraud attack is not a well-defined quantity if we do not impose an *exact* limitation on the adversary (e.g. in terms of complexity and number of queries). Indeed, if we consider all polynomially bounded adversaries, for each value of the security parameter, there is always a polynomially bounded attack (namely, the one making an exhaustive search up to this value of the security parameter and doing nothing beyond) succeeding with probability close to 1.

Remark 5. For every mafia-fraud adversary A, it is always possible to design another adversary A' with a small complexity overhead and doing a bit better: we assume that A makes enough observations. We define A' by first making a guess for the secret. Then, A' simulates A. If, during the observations, A' realizes that the guess for the secret is consistent with the information collected by A, then it stops simulating A and uses the guess to impersonate the prover. Otherwise, the simulation continues normally. By tuning the number of observations so that the probability that an incorrect guess is consistent is negligible against the probability to guess the secret correctly, this new adversary A' performs better and A.

In [12], Fischlin and Onete modify the Swiss-Knife protocol to make it GameTF-secure. The protocol is on Fig. 3.[1] We call it the MSK protocol (as for *Modified Swiss-Knife*). Essentially, they introduce a new shared secret y: x is only used for the PRF computation while y is used in $a_2 = a_1 \oplus y$. This protocol is GameTF-secure for $\varepsilon = \mathsf{Adv}^{\mathsf{MF}}$ [12, Prop.1]. It is further claimed that $\mathsf{Adv}^{\mathsf{MF}} = B(n, \tau, \frac{1}{2}) + \mathsf{negl}$ for a targeted reader session[2] where B is defined by Eq.(1).

$$\begin{array}{rcl}
\textbf{Verifier} & & \textbf{Prover} \\
\text{secret: } x, y & & \text{secret: } x, y \\
 & \textbf{initialization phase} & \\
\text{pick } N_V & \xrightarrow{N_V} & \\
 & \xleftarrow{N_P} & \text{pick } N_P \\
a_1 = f_x(N_P, N_V) & & a_1 = f_x(N_P, N_V) \\
a_2 = a_1 \oplus y & & a_2 = a_1 \oplus y \\
 & \textbf{distance bounding phase} & \\
 & \text{for } i = 1 \text{ to } n & \\
\text{pick } c_i \in \{1, 2\} & & \\
\text{start } \mathsf{timer}_i & \xrightarrow{c_i} & \\
\text{stop } \mathsf{timer}_i & \xleftarrow{r_i} & r_i = \begin{cases} a_{1,i} & \mathsf{if}\ c_i = 1 \\ a_{2,i} & \mathsf{if}\ c_i = 2 \end{cases} \\
 & \textbf{verification phase} & \\
\#\{i : r_i \ \mathsf{and\ timer}_i \ \mathsf{correct}\} \geq \tau & \xleftarrow{t} & t = f_x(\mathsf{transcript}) \\
\text{check } t & \xrightarrow{\mathsf{Out}_V} &
\end{array}$$

Fig. 3. The Modified Swiss-Knife (MSK) Distance-Bounding protocol [11]

Introducing a new secret y besides the one x used in PRF is a clever choice to avoid the problems based on PRF programming [2] making security results incorrect. We still need to have y honestly selected (as specified in [12]) for distance fraud. Otherwise, registering $y = 0$ leads to a trivial distance fraud.

[1] For the sake of clarity in this paper, our description slightly differs from the one in [12]. The main difference resides in that [12] uses two separate counters to count the number of rounds for which the timer expires, and for which the timer is acceptable but the response is incorrect. Our analysis remains valid for the original version in [12].

[2] We can infer this bound from [12, Prop.3] which applies to the original protocol. In this result, the first term of $\mathsf{Adv}^{\mathsf{MF}}$ is $q_R 2^{-\tau}$ where q_R is the number of (untargeted) adversary-reader sessions, other terms being negligible as they express that nonces may repeat or that the PRF property may be defeated.

Terrorist fraud against the MSK protocol. We now show a *practical* terrorist fraud contradicting the security proof for GameTF-security from [12]. We consider a malicious prover helping the adversary in the nonce exchange and the final transcript authentication, and just disclosing a_1 and y to the adversary. Clearly, the adversary using a_1 and $a_2 = a_1 \oplus y$ succeeds with probability 1. We have now to show that this adversary is not helpful *in practice.* He only discloses y. The (a_1, a_2) pairs can be learnt by running the protocol with the honest prover. So, we just have to consider a mafia fraud adversary getting y as an auxiliary input. We can show (see the Lemma below) that such an adversary is incapable of succeeding, except with negligible probability. So, it is clear that we do have a terrorist fraud succeeding with probability 1 and leaking no useful information to mount a mafia fraud attack.

Lemma 6. *In the MSK protocol, we consider an experiment with a far-away prover P, an adversary A receiving y as an auxiliary input, and a verifier V. The probability that a target session of V accepts is limited by $B(n, \tau, \frac{1}{2}) + \mathsf{negl}$.*

Proof. We first reduce to cases where nonces do not repeat and the PRF is replaced by a random function. Then, using hybrids, we reduce to a single session on P and V using the same nonces. Finally, we assume that if P and V see different transcripts, the protocol fails due to an incorrect t. All this induces a negligible term in the probability of success.

Due to the large distance between P and V, A can either send a random c'_i to P before he receives c_i from V (the Go-Early strategy), or answers to c_i without any clue and ask for some c'_i to P later (the Go-Late strategy).

Since A knows y, in the Go-Early strategy, A deduces the answer to all possible challenge c_i at round i. However, the correct tag t can only be obtained from P if $c_i = c'_i$, which happens with probability $\frac{1}{2}$.

In the Go-Late strategy, A has no clue about the response, so the probability to be correct is $\frac{1}{2}$.

Hence, in any case, the probability that one round is correct is $\frac{1}{2}$. Since we need τ correct rounds, the probability to win is $B(n, \tau, \frac{1}{2})$. □

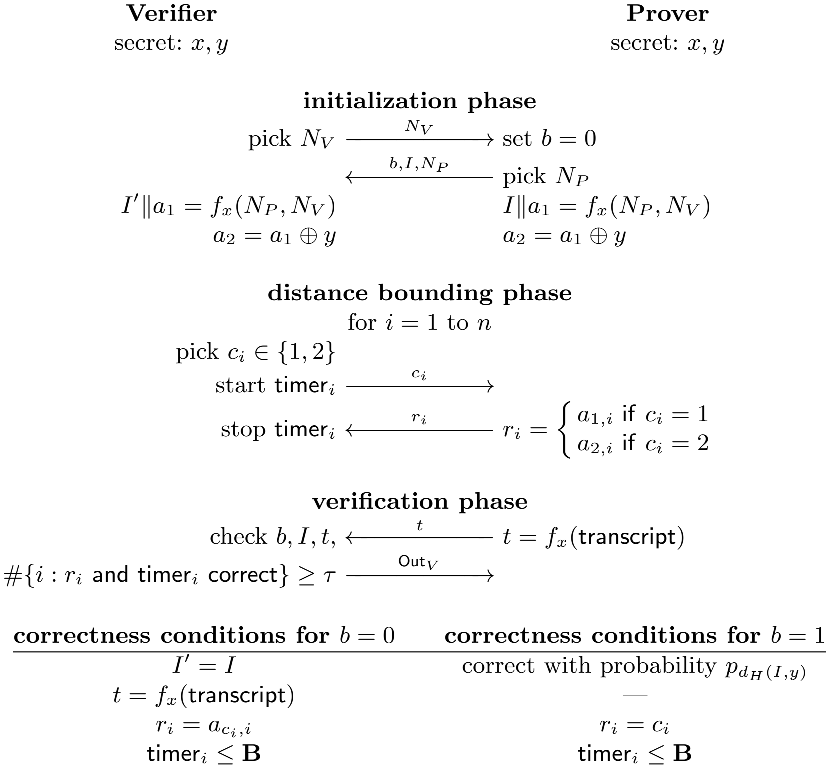
It was proven in [12, Prop.1] that the MSK protocol is GameTF-secure. However, the proof makes no reference to the authenticating t in the protocol, which makes us believe that the result is incorrect. The above attack shows that either this is the case, or the GameTF security does not capture well the resistance to terrorist fraud. Indeed, it could be the case that a helpful attack is still relevant in practice, although ruled out by this notion, because the help provided is negligible.

2.3 FO: A SimTF-Secure Protocol

In [12], Fischlin and Onete propose another protocol which is SimTF and str-SimTF-secure. The protocol is on Fig. 4.[3] We call it the *FO protocol.* In a normal

[3] Like for the MSK protocol, the original FO protocol uses two separate counters. Our analysis for the original protocol will be discussed in Remark 7.

execution, we always have $b = 0$ and the protocol works like the one on Fig. 3. For $b = 1$, a special procedure is run: the accepted response r_i is different, and the verification for I is a bit special. Namely, the verifier now accepts $r_i = c_i$ as the correct answer.[4] For $b = 0$, the verifier checks that $I' = I$. Additionally, for $b = 1$, I is accepted with a probability $p_{d_H(I,y)}$ which depends on the Hamming distance between I and y. The value of p_d is adjusted to have SimTF security. So, the mafia fraud resistance corresponds to the terrorist fraud resistance. The idea is that the $b = 0$ case protects against distance frauds and mafia frauds, and that terrorist frauds leak some information y' close to y, and the $b = 1$ case protects against distance frauds only but requires such information y'.



Verifier secret: x, y — **Prover** secret: x, y

initialization phase

pick N_V $\xrightarrow{N_V}$ set $b = 0$

$\xleftarrow{b,I,N_P}$ pick N_P

$I' \| a_1 = f_x(N_P, N_V)$ — $I \| a_1 = f_x(N_P, N_V)$

$a_2 = a_1 \oplus y$ — $a_2 = a_1 \oplus y$

distance bounding phase

for $i = 1$ to n

pick $c_i \in \{1, 2\}$

start timer_i $\xrightarrow{c_i}$

stop timer_i $\xleftarrow{r_i}$ $r_i = \begin{cases} a_{1,i} & \mathsf{if}\ c_i = 1 \\ a_{2,i} & \mathsf{if}\ c_i = 2 \end{cases}$

verification phase

check $b, I, t,$ $\xleftarrow{t}$ $t = f_x(\mathsf{transcript})$

$\#\{i : r_i\ \mathsf{and}\ \mathsf{timer}_i\ \mathsf{correct}\} \geq \tau$ $\xrightarrow{\mathsf{Out}_V}$

correctness conditions for $b = 0$	**correctness conditions for $b = 1$**
$I' = I$	correct with probability $p_{d_H(I,y)}$
$t = f_x(\mathsf{transcript})$	—
$r_i = a_{c_i,i}$	$r_i = c_i$
$\mathsf{timer}_i \leq \mathbf{B}$	$\mathsf{timer}_i \leq \mathbf{B}$

Fig. 4. The Fischlin-Onete Distance-Bounding protocol [12]

[4] In [12], it is written that the verifier *also* accepts $r_i = c_i$ which seems to mean that both $r_i = (a_{c_i})_i$ and $r_i = c_i$ are accepted. However, having two different possible responses could lead to an easy distance fraud: if for some value of c_i both answers are correct, we just prepare the answer for the other value $\bar{c}_i$. So, *only* the $r_i = c_i$ answer should be accepted.

We first note that it is pretty weird to have a piece of code (namely, the $b = 1$ case) which shall never be used for $b = 1$, and which provides an escape way to pass the protocol without knowing x. It may also introduce some strange attack models similar to distance hijacking [8], where far-away malicious provers take advantage of the proximity of honest participants to feed responses for them. Here, a far-away prover only needs someone to echo the challenges. We could also have a malicious participant $P_1^*(x)$ carrying the initialization and verification phases himself, and hijacking some $(P_2^*(x), A(x))$ pair running a terrorist fraud with $b = 1$. So, this protocol modification may induce some new "exotic" kinds of frauds in the family of distance fraud and distance hijacking.

Distance fraud. A malicious far-away prover could anticipate responses corresponding to $y_i = 0$ since they are independent of the challenge. Others are correct with probability $\frac{1}{2}$. *On average* over the distribution of y, one round succeeds with probability $\frac{3}{4}$. With y fixed, the probability of success of the distance fraud is $B(w, \tau - n + w, \frac{1}{2})$ with B defined by Eq.(1), where $w = d_H(0, y)$ is the Hamming weight of y. So, user receiving a key y with a low weight have a better incentive to cheat in a distance fraud! It could also induce some weird behaviors of malicious users asking for new credentials until they have a better Hamming weight. Another bad property is that the probability of $B(w, \tau - n + w, \frac{1}{2})$ is fixed once for all: a user succeeding to get a low w offline has always better chances to defeat distance fraud online. Clearly the security is non-uniform about the selection of y. On average, it is of $B(n, \tau, \frac{3}{4})$.

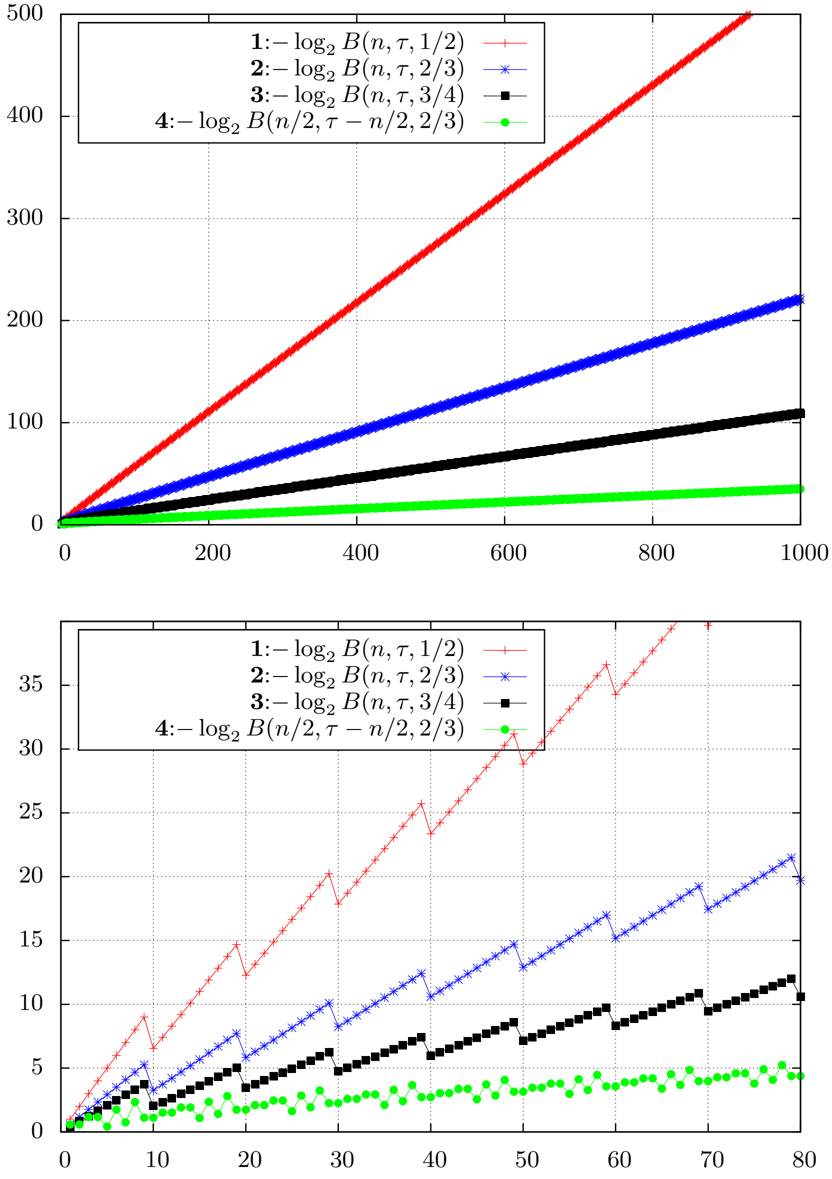
Mafia fraud. Due to the design of the FO protocol, terrorist frauds induce mafia frauds. Let us consider the following terrorist fraud (A, P^*) depending on a parameter e: let $g(x)$ be a set of indices of cardinality e. Then, we consider a malicious prover P^* disclosing y' such that $g(x) = \{i; y_i \neq y'_i\}$ and $\#g(x) = e$. Additionally, he helps the adversary A in the nonce exchange and provides a'_1 matching a_1 on each position which is not in $g(x)$ and set to random bits in positions in $g(x)$. The adversary using a'_1 and $a'_2 = a'_1 \oplus y'$ instead of a_1 and a_2 wins if the number of errors is below $n - \tau$. We know that errors happen randomly in a set of e. So, the probability to pass is $\rho_e = B(e, e - n + \tau, \frac{1}{2})$. Now, for an adversary S trying to pass the protocol by only knowing y', since he cannot forge t in the verification phase, the best strategy is to use the escape strategy with $b = 1$. Since he has no information about $g(x)$, y' remains the best approximation of y to him. By using $I = y'$, he passes with probability p_e. For instance, for $e = 2(n - \tau)$, we have $\rho_e = \frac{1}{2}$: it shall be enough to provide a y with twice more errors than allowed. Due to the SimTF definition, this attacks requires that we have $p_e \geq \rho_e$ for all e. In Th. 8, we will show that this condition is also sufficient.

However, the $p_e \geq \rho_e$ bounds creates a new mafia fraud attack: Now, we consider a mafia-fraud adversary who just tries to guess y' within a small distance to y and who uses the escape $b = 1$ in the protocol with this guess. Trying to guess vector at a distance e works with probability of success $\binom{n}{e} 2^{-n}$. Finally, the attack using $b = 1$ and a random I works with probability

$$\begin{aligned}
p &= \sum_{e=0}^{n} \binom{n}{e} 2^{-n} p_e \\
&\geq \sum_{e=0}^{n} \binom{n}{e} 2^{-n} \rho_e \\
&= \sum_{e=0}^{n} \binom{n}{e} 2^{-n} B\left(e, e-n+\tau, \frac{1}{2}\right) \\
&= \sum_{e=0}^{n} \sum_{i=e-n+\tau}^{e} \binom{n}{e} \binom{e}{i} 2^{-n-e} \\
&= \sum_{e=0}^{n} \sum_{i=0}^{n-\tau} \binom{n}{e} \binom{e}{i} 2^{-n-e} \\
&= \sum_{i=0}^{n-\tau} \sum_{e=0}^{n} \binom{n}{e} \binom{e}{i} 2^{-n-e} \\
&= \sum_{i=0}^{n-\tau} \sum_{e=0}^{n} \binom{n}{i} \binom{n-i}{n-e} 2^{-n-e} \\
&= \sum_{i=0}^{n-\tau} \sum_{e=i}^{n} \binom{n}{i} \binom{n-i}{n-e} 2^{-n-e} \\
&= \sum_{i=0}^{n-\tau} \binom{n}{i} 2^{-2n} 3^{n-i} \\
&= \sum_{j=\tau}^{n} \binom{n}{j} \left(\frac{3}{4}\right)^{j} \left(\frac{1}{4}\right)^{n-j} \\
&= B\left(n, \tau, \frac{3}{4}\right)
\end{aligned}$$

with B defined by Eq.(1). In contrast, the probability of success of the regular (i.e. with $b = 0$) mafia fraud is $B(n, \tau, \frac{1}{2})$ which is much lower. So, this modification of the Swiss-Knife protocol induces a significant security loss for mafia-fraud resistance.

As an application, we take $n - \tau = \frac{n}{10}$ (that is, we want 90% of the rounds to be correct to tolerate a noise level below 10%). For $n = 144$ rounds, we obtain $B(n, \tau, \frac{1}{2}) \approx 2^{-80}$, but $B\left(n, \tau, \frac{3}{4}\right) \approx 2^{-18}$. To reach $B\left(n, \tau, \frac{3}{4}\right) \approx 2^{-80}$, we need $n \geq 724$ to secure the FO protocol against the mafia fraud. On Fig. 5, we plot $-\log_2 B(n, \tau, p)$ for $\tau = \lceil n * 0.9 \rceil$ and $p \in \{\frac{1}{2}, \frac{3}{4}\}$. (Note that discontinuities are due to rounding τ.) Due to Lem. 1, it is clear that these curves are close to a line with slope $\frac{(\frac{\tau}{n} - p)^2}{2p(1-p)\ln 2}$. So, for the number of rounds n, we are loosing a factor $\frac{3}{4}\left(\frac{\frac{\tau}{n} - \frac{1}{2}}{\frac{\tau}{n} - \frac{3}{4}}\right)^2$ which is $\frac{16}{3}$ in this case.



The security of FO follows the curve **3** for distance fraud, mafia fraud, and terrorist fraud while the security of MSK follows the curve **1** for mafia fraud. The security of SKI follows the curves **3**, **2**, and **4** for distance fraud, man-in-the-middle, and collusion fraud, respectively.

Fig. 5. Security (Equivalent Bitlength) in Terms of the Number of Rounds n for $\tau = \lceil n * 0.9 \rceil$

Note that this attack can self-improve: assuming that an adversary has got a good y', his probability of success in a mafia fraud will always be at least ρ_e. Furthermore, if this probability is low enough, by doing some statistics and using a hill climbing approach, the adversary can find a better y' and eventually obtain one within a distance $n-\tau$, which makes the attack work with probability 1. Fortunately, except in a terrorist fraud case, there is no better way to find a good y' than a random guess.

Another interesting observation is that we need $n - \tau \ll \frac{n}{4}$ for security. Indeed, for $n - \tau \approx \frac{n}{4}$, we have $p \approx \frac{1}{2}$ which makes the protocol insecure.

Remark 7. In [12], there are specific counters for the response errors and the timer errors. Namely, there should be no more than $E_{\max}$ errors and no more than $T_{\max}$ timeouts. Furthermore, it is specified that $p_d = \min(1, 2^{-d+T_{\max}+E_{\max}})$. We can adapt our strategy above by having the malicious prover to use two disjoin sets $g(x)$ and $g'(x)$ and disclosing y' with errors in $g(x)$ and holes in $g'(x)$. The adversary would run for a time out for every hole and work as above otherwise. For $e = 2E_{\max}$, the probability of success is $\frac{1}{2}$. Now, to approximate y, we have to fill the holes with random bits. So, we have a probability of success

$$\begin{aligned}
\sum_{i=0}^{T_{\max}} \binom{T_{\max}}{i} 2^{-T_{\max}} p_{e+i} &= \sum_{i=0}^{T_{\max}} \binom{T_{\max}}{i} 2^{-T_{\max}} \min(1, 2^{-e-i+T_{\max}+E_{\max}}) \\
&= \sum_{i=0}^{T_{\max}} \binom{T_{\max}}{i} 2^{-T_{\max}} \min(1, 2^{-E_{\max}-i+T_{\max}}) \\
&= \sum_{i=0}^{T_{\max}} \binom{T_{\max}}{i} 2^{-E_{\max}-i} \\
&= \left(\frac{1}{2}\right)^{E_{\max}} \left(\frac{3}{2}\right)^{T_{\max}}
\end{aligned}$$

when $E_{\max} \geq T_{\max}$. This is smaller than $\left(\frac{3}{4}\right)^{T_{\max}}$. Clearly, this is not larger than $\frac{1}{2}$, when $E_{\max} \geq T_{\max} \geq 2$. So, the probabilities p_d provided in [12] are incorrect in this case.

Security proof for the FO protocol. With similar techniques as in [4], we can prove the $\mathsf{strSimTF}$ security with a p_e value matching the necessary condition which was identified above.

Theorem 8 (TF-Resistance of the FO protocol). *For $p_e = B(e, e-n+\tau, \frac{1}{2})$ for every e, the FO scheme is $\mathsf{strSimTF}$-secure.*

Proof. In the experiment, we let A denote all participants close to V (by definition, they are all malicious) and P^* denote all far-away participants. We let View_i be the view of A just before receiving the challenge c_i and View be the final view. If View includes $b = 1$, it is clear that it leaks some I which is enough for a simulator S to pass the protocol with *exactly* the same probability. So, we only have to focus on the $b = 0$ case in the terrorist fraud.

We let w_i be the extra information (obtained from P^*), not contained in View_i, which is received by A before it is critical to answer r_i, and we denote $r_i = A(\mathsf{View}_i, c_i, w_i)$. If A takes too long time, the answer r_i is unimportant and we denote $r_i = \perp$. Note that w_i is still defined as the information before it is critical to answer in this case. I.e., there is no time to have a round trip between A and P^* from the time A receives c_i to the time we set w_i. Due to the assumptions on tainted sessions and that c_i is randomly selected by V, we note that (View_i, w_i) is independent from c_i. We define a vector y' by

$$y'_i = A(\mathsf{View}_i, 1, w_i) \oplus A(\mathsf{View}_i, 2, w_i)$$

We consider a simulator S computing y' and using it with $b = 1$ to pass the protocol. We want to show that $p_S \geq p_A$. Let $e = d_H(y, y')$. Clearly, what we have to prove is that $E(p_e) \geq p_A$.

We let C_i be the set of all c's such that $A(\mathsf{View}_i, c, w_i) = a_{c,i}$ with a computed from V. I.e., C_i is the set of challenges to which A answers correctly in round i. We let S be the set of all i such that $c_i \in C_i$. I.e., A answers correctly in round i. Clearly, $p_A = \Pr[\#S \geq \tau]$.

We let R be the set of all i's such that C_i has cardinality 2, i.e., A always answers correctly. Clearly, for $i \in R$, we have

$$y'_i = A(\mathsf{View}_i, 1, w_i) \oplus A(\mathsf{View}_i, 2, w_i) = a_{1,i} \oplus a_{2,i} = y_i$$

Since p_e is decreasing, we have $p_e \geq p_{n-\#R}$. Now, we want to prove that $E(p_{n-\#R}) \geq p_A$.

For every possible set R, we have $\Pr[\#S \geq \tau | R] \leq B(n - \#R, \tau - \#R, \frac{1}{2}) = p_{n-\#R}$. By averaging over R, we obtain $E(p_{n-\#R}) \geq p_A$. □

3 The Boureanu-Mitrokotsa-Vaudenay Approach

3.1 A Two-Dimensional Notion

In [3], Boureanu *et al.* proposed another definition of terrorist fraud security which is sketched as follows:

Definition 9 ((γ, γ')-resistance to TF [3]). *We say that a DB protocol is* (γ, γ')-resistant to terrorist-fraud *if for any far-away, coerced prover P^*, it is the case that, below,* (1) *implies* (2)
— (1). *an adversary $\mathcal{A}$ interfering up to his powers with an interaction between P^* and verifier V on their shared secret, where this interaction is successful with probability at least γ (over the random choices of V and $\mathcal{A}$),*
— (2). *$\mathcal{A}$ can later succeed on his own to make the verifier accept in a new protocol run with a probability greater than γ' (taken over the new random choices made by V and $\mathcal{A}$).*

It is further said that this easily extends in a multiparty setting.

Interestingly, this definition separates the probability of success γ of the terrorist fraud and the one γ' of the further impersonation. This avoids having to consider a hard-to-define notion of optimal probability of success of an attack which cannot be asymptotic (see remark 4) but makes security be based on two dimensions (γ and γ') instead of one.

3.2 Collusion Fraud

In [5], Boureanu *et al.* proposed to replace this definition by the notion of *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."

which is further formulated in Vaudenay's FSE 2013 invited talk[5] as

> "$P(x)$ far from all $V(x)$'s interacts with $\mathcal{A}$ and makes one $V(x)$ accept, but $\mathsf{View}(\mathcal{A})$ does not give any advantage to mount a man-in-the-middle attack"

This resembles the GameTF notion where the final view of the adversary is provided in a further mafia fraud adversary. This notion is further made more precise in [4]:

Definition 10 ((γ, γ')-resistance to collusion-fraud [4]).
$(\forall s)(\forall P^*)$ $(\forall \mathsf{loc}_{V_0}$ *such that* $d(\mathsf{loc}_{V_0}, \mathsf{loc}_{P^*}) > \mathbf{B})$ $(\forall \mathcal{A}^{\mathsf{CF}}$ *ppt.) such that*

$$\Pr\left[\mathsf{Out}_{V_0} = 1 : \begin{array}{l} (x,y) \leftarrow Gen(1^s) \\ P^*(x) \longleftrightarrow \mathcal{A}^{\mathsf{CF}} \longleftrightarrow V_0(y) \end{array}\right] \geq \gamma$$

over all random coins, there exists a (kind of) MiM attack $m, \ell, z, \mathcal{A}_1, \mathcal{A}_2, P_i, P_j, V_{i'}$ *using* P *and* P^* *in the learning phase, such that*

$$\Pr\left[\mathsf{Out}_V = 1 : \begin{array}{l} (x,y) \leftarrow Gen(1^s) \\ P_1^{(*)}(x), \ldots, P_m^{(*)}(x) \longleftrightarrow \mathcal{A}_1 \longleftrightarrow V_1(y), \ldots, V_z(y) \\ P_{m+1}(x), \ldots, P_\ell(x) \longleftrightarrow \mathcal{A}_2(View_{\mathcal{A}_1}) \longleftrightarrow V(y) \end{array}\right] \geq \gamma'$$

where P^* *is any (unbounded) dishonest prover and* $P^{(*)}$ *runs either* P *or* P^**. Following the MiM requirements,* $d(\mathsf{loc}_{P_j}, \mathsf{loc}_V) > \mathbf{B}$*, for all* $j \in \{m+1, \ell\}$*. In a concurrent setting, we implicitly allow a polynomially bounded number of* $P(x')$*,* $P^*(x')$*, and* $V(y')$ *with independent* (x', y')*, but no honest participant close to* V_0*.*[6]

[5] http://fse2013.spms.ntu.edu.sg/slides/Slides02.pdf

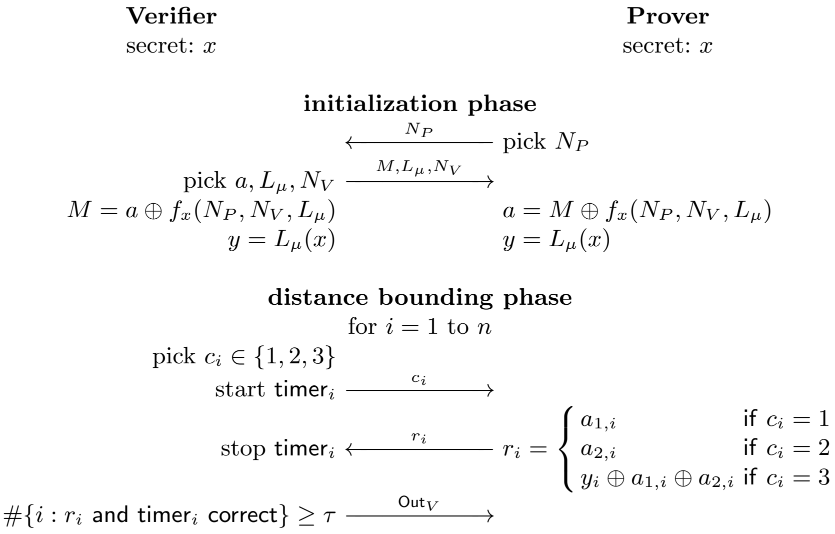
[6] "ppt." means "probabilistic polynomial-time algorithm".

Essentially, it allows the collusion fraud to be run several times until the adversary can extract enough information to mount an attack. In the definition, we assume that every running algorithms M are given a location which is denoted by loc_M. The value $\mathbf{B}$ is the maximal distance until which the prover is considered too far from the verifier. The man-in-the-middle (MiM) attack separates a *learning phase* with m provers and z verifiers, from an *attack phase* with $\ell - m$ far-away provers and one verifier. The learning phase can run with either the honest prover or the malicious one P^* which is being considered in the collusion fraud. The above theorem refers to a *kind of* MiM since it is assumed that the man-in-the-middle plays also with P^*, which is not the case in regular MiM attacks.

Clearly, this captures the scenario used in GameTF security.

3.3 SKI: A Collusion-Fraud Resistant Protocol

Boureanu *et al.* [3,4,5] further proposed the SKI distance-bounding protocols which provide security against collusion fraud. Compared to the protocols in the Swiss-Knife family, these protocols do not have a post-authentication phase, but require a larger set of challenges (namely, 3 instead of 2). (See Fig. 6.) The second secret y is further derived from the first one x by using a *leakage scheme* L_μ. Essentially, running a collusion fraud is bound to leak y which, based being run several times, allows to fully reconstruct x.



Verifier
secret: x
Prover
secret: x
initialization phase
$\xleftarrow{N_P}$ pick N_P
pick a, L_μ, N_V $\xrightarrow{M, L_\mu, N_V}$
$M = a \oplus f_x(N_P, N_V, L_\mu)$
$y = L_\mu(x)$
$a = M \oplus f_x(N_P, N_V, L_\mu)$
$y = L_\mu(x)$
distance bounding phase
for $i = 1$ to n
pick $c_i \in \{1, 2, 3\}$
start timer_i $\xrightarrow{c_i}$
stop timer_i $\xleftarrow{r_i}$
$r_i = \begin{cases} a_{1,i} & \text{if } c_i = 1 \\ a_{2,i} & \text{if } c_i = 2 \\ y_i \oplus a_{1,i} \oplus a_{2,i} & \text{if } c_i = 3 \end{cases}$
$\#\{i : r_i \text{ and } \mathsf{timer}_i \text{ correct}\} \geq \tau$ $\xrightarrow{\mathsf{Out}_V}$

Fig. 6. The SKI Distance-Bounding Protocol [3,4]

The SKI security requires $n - \tau \ll \frac{n}{6}$, which imposes some restriction on the noise probability. Another disadvantage is that we need a stronger notion of PRF: a *circular-keying secure PRF*. The security of SKI is stated as follows.

Theorem 11 (Boureanu-Mitrokotsa-Vaudenay [4]). *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.*

B is defined by Eq.(1). On Fig. 5 we plot $-\log_2 B(n, \tau, p)$ for $p \in \{\frac{2}{3}, \frac{3}{4}\}$ and $-\log_2 B(\frac{n}{2}, \tau - \frac{n}{2}, \frac{2}{3})$ for $\tau = \lceil n * 0.9 \rceil$. Due to Lem. 1, it is clear that the first two curves are close to a line with slope $\frac{(\frac{\tau}{n} - p)^2}{2p(1-p)}$. By applying Lem. 1 with n and t replaced by $\frac{n}{2}$ and $2t - 1$, we obtain that the slope of the third one is $\frac{(2\frac{\tau}{n} - 1 - p)^2}{2p(1-p)}$ with $p = \frac{2}{3}$. To reach a security of 2^{-80} for distance fraud, we need a pretty high $n = 724$. For man-in-the-middle, $n = 353$ is enough. For collusion fraud, we still need a very high $n = 2\,388$, but this has no influence on the security against man-in-the-middle. If a security of 2^{-20} is considered as enough, we need $n = 76$ for man-in-the-middle, $n = 163$ for distance fraud, or $n = 531$ for collusion fraud. (Of course, figures become better with a larger τ/n ratio.)

Compared to the FO protocol, every distance fraud attacks is limited to a success probability of $B(n, \tau, \frac{3}{4})$. Furthermore, there is no auxiliary input such as some y' vector to ease a mafia fraud. All man-in-the-middle attacks are limited to a success probability of $B(n, \tau, \frac{2}{3})$.

3.4 Soundness

The idea behind SKI is that the secret is extractable from the collusion. Extractability may not always be necessary to protect against terrorist fraud but it looks like a convenient and easy-to-deal-with notion. As a matter of fact, Boureanu *et al.* [5] mentions that collusion resistance looks like some notion of *soundness* in interactive proofs.

Indeed, a distance-bounding protocol is an interactive proof for holding a secret (this is the authentication part) and of close distance. An associated notion of soundness for this proof could be formalized by means of an extractor. We propose the following definition:

Definition 12 (γ-m-soundness). *We say that a distance-bounding protocol is* γ-sound *if for all experiment* $\mathsf{exp}(\mathcal{V}, \mathsf{ID})$ *such that*

- *all provers and verifiers work for the same identity* ID*,*
- *there is no close prover,*
- *there is no close verifier,*
- $\mathcal{V}$ *accepts with probability at least* γ*,*

there exists a ppt algorithm $\mathcal{E}$ *called* extractor*, such that by running* m *times* $\mathsf{exp}(\mathcal{V},\mathsf{ID})$ *in some executions* $\mathsf{exp}_i(\mathcal{V},\mathsf{ID})$*,* $i=1,\ldots,m$*, if* View_i *denotes the view of all close participants in* $\mathsf{exp}_i(\mathcal{V},\mathsf{ID})$ *and* Succ_i *is the event that* $\mathcal{V}$ *accepts in this experiment, we have*

$$\Pr\left[\mathcal{E}(\mathsf{View}_1,\ldots,\mathsf{View}_m)=x_{\mathsf{ID}}\,|\,\mathsf{Succ}_1,\ldots,\mathsf{Succ}_m\right]=1-\mathsf{negl}(n)$$

Lemma 13 (Link between soundness and collusion frauds). *For any* $p\geq\gamma$ *such that* p^{-1} *is polynomially bounded, if the protocol is* γ*-*m*-sound, then it* $(p,1-\mathsf{negl}(n))$*-resists to collusion fraud (in the sense of Def.10).*

Proof. Given a collusion fraud with a malicious prover $P^*(x_{\mathsf{ID}})$ succeeding with probability $p\geq\gamma$, we have an experiment Exp satisfying the properties of the definition of γ-m-soundness. Thus, there must exist some extractor $\mathcal{E}$. This defines a learning phase of a man-in-the-middle attack involving $P^*(x_{\mathsf{ID}})$, which just simulates, for $\Omega(mp^{-1})$ times the experiment so that at least m simulations succeed with probability $1-\mathsf{negl}(n)$. At the end of this learning phase, $\mathcal{A}$ computes x_{ID} by using $\mathcal{E}$. Then, we define an attack phase with an adversary alone with $V(y_{\mathsf{ID}})$, receiving the x computed by $\mathcal{A}$. This attack succeeds with probability $1-\mathsf{negl}(n)$. So, the protocol $(p,1-\mathsf{negl}(n))$-resists to collusion fraud. □

With the new soundness definition, we can prove the following result.

Theorem 14 (Soundness of the SKI protocol). *For any* $\frac{\tau}{n}>\frac{5}{6}$ *and* γ *such that* $\gamma^{-1}B(\frac{n}{2},\tau-\frac{n}{2},\frac{2}{3})=\mathsf{negl}(n)$*, the SKI scheme is* γ*-*s*-sound.*

We cannot prove the soundness of the FO protocol (since the x part of the secret never leaks).

Proof. Again, we use techniques from [5]. The proof is similar to the one of Th. 8. With the same notations, R now denotes the set of i's such that the cardinality of C_i is 3, and we define

$$y'_i=A(\mathsf{View}_i,1,w_i)\oplus A(\mathsf{View}_i,2,w_i)\oplus A(\mathsf{View}_i,3,w_i)$$

For $i\in R$, we have $y'_i=\mu\cdot x$. So, we are interested in the majority of the y'_i's. Again, we have $\Pr[\#S\geq\tau|R]\leq B(n-\#R,\tau-\#R,\frac{2}{3})$. For $\#R\leq\frac{n}{2}$, we have $\Pr[\#S\geq\tau|R]\leq B(n-\#R,\tau-\#R,\frac{2}{3})\leq B(\frac{n}{2},\tau-\frac{n}{2},\frac{2}{3})$. By averaging over all R's such that $\#R\leq\frac{n}{2}$, we obtain $\Pr[\#S\geq\tau,\#R\leq\frac{n}{2}]\leq B(\frac{n}{2},\tau-\frac{n}{2},\frac{2}{3})$ from which we deduce $\Pr[\#R\leq\frac{n}{2}|\#S\geq\tau]\leq\gamma^{-1}B(\frac{n}{2},\tau-\frac{n}{2},\frac{2}{3})$. So, with probability larger than $1-\gamma^{-1}B(\frac{n}{2},\tau-\frac{n}{2},\frac{2}{3})$, the majority of the y'_i's equals $\mu\cdot x$. After s such attempts, we recover s linear bits of x, so we extract x. □

4 Conclusion

We have identified some mistakes in [12]: The security result about the MSK protocol is incorrect, as well as the original probabilities specified in the FO protocol.

We have compared two notions of terrorist fraud resistance: SimTF and collusion fraud resistance. We have also compared the two protocols offering these resistance: FO and SKI, respectively. The advantages of FO are that

- it uses binary challenges;
- it is resilient to noise at a higher level $\frac{1}{4}$;
- it relies on standard PRF security.

The drawbacks are that

- it includes a weird code, not supposed to be used;
- its resistance to mafia fraud is lowered to $B(n, \tau, \frac{3}{4})$ due to the (too) strong requirements of SimTF security;
- it has a non uniform security $B(w, \tau - n + w, \frac{1}{2})$ for distance fraud.

About the prominent proposal for the SKI protocol, the advantages are that

- it has a uniform security of $B(n, \tau, \frac{3}{4})$ for distance fraud;
- it has a better security $B(n, \tau, \frac{2}{3})$ against man-in-the-middle;
- all elements of the protocol are used.

The drawbacks are that

- it uses non-binary challenges;
- it is only resilient to noise at a level of $\frac{1}{6}$;
- it relies on non-standard PRF security.

Clearly, designing a protocol offering all these types of resistance, still with reasonable parameters in practice, remains an important challenge.

Finally, we extended the collusion fraud resistance by the notion of soundness. This notion justifies itself by comparison to interactive proofs of knowledge based on an extractor.

We believe that an ideal protocol could combine both approaches of the FO and SKI protocols: to provide better security parameters, we should adopt the leakage scheme approach of SKI (at the cost of a non-standard PRF assumption) instead of the escape protocol with $b = 1$ (which lowers security) and adopt, like FO, the Swiss-Knife frame with only two possible challenges instead of three. It would provide uniform security for distance fraud and be resilient to noise up to a $\frac{1}{4}$ ratio. The only remaining drawback would be the non-standard PRF assumption. Designing such a provably secure protocol remains an open problem.

Acknowledgements

The author thanks Marc Fischlin and Cristina Onete for their feedbacks. Also: many thanks to Ioana Boureanu for some memorable discussions about terrorism in distance bounding.

References

1. G. Avoine, M. Bingöl, S. Kardas, C. Lauradoux, B. Martin. A Framework for Analyzing RFID Distance Bounding Protocols. *Journal of Computer Security*, vol. 19(2), pp. 289–317, 2011.
2. 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.
3. I. Boureanu, A. Mitrokotsa, S. Vaudenay. Secure & Lightweight Distance-Bounding. To appear in the proceedings of LightSec'13.
4. I. Boureanu, A. Mitrokotsa, S. Vaudenay. Practical & Provably Secure Distance-Bounding. Available on http://eprint.iacr.org/2013/465.pdf
5. I. Boureanu, A. Mitrokotsa, S. Vaudenay. Towards Secure Distance Bounding. To appear in the proceedings of FSE'13.
6. 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.
7. W. Bryc. A Uniform Approximation to the Right Normal Tail Integral. *Applied Mathematics and Computation*, vol. 127, pp. 365–374, 2002.
8. 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.
9. 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.
10. 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.
11. M. Fischlin, C. Onete. Subtle Kinks in Distance-Bounding: an Analysis of Prominent Protocols. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks WISEC'13*, Budapest, Hungary, pp. 195–206, ACM, 2013.
12. M. Fischlin, C. Onete. Terrorism in Distance Bounding: Modelling Terrorist-Fraud Resistance. In *Applied Cryptography and Network Security ACNS'13*, Banff AB, Canada, Lecture Notes in Computer Science 7954, pp. 414–431, Springer-Verlag, 2013.
13. 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.
14. 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.
15. 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.