Practical & Provably Secure Distance-Bounding

Ioana Boureanu[1], Aikaterini Mitrokotsa[2], and Serge Vaudenay[3]

[1] University of Applied Sciences Western Switzerland, HEIG-VD
Yverdon-les-Bains, Switzerland
ioana.carlson@heig-vd.ch
[2] Chalmers University of Technology
Gothenburg, Sweden
aikaterini.mitrokotsa@chalmers.se
[3] Ecole Polytechnique Fédérale de Lausanne (EPFL)
Lausanne, Switzerland
serge.vaudenay@epfl.ch

Abstract. From contactless payments to remote car unlocking, many applications are vulnerable to relay attacks. Distance bounding protocols are the main practical countermeasure against these attacks. At FSE 2013, we presented **SKI** as the *first* family of *provably secure* distance bounding protocols. At LIGHTSEC 2013, we presented the best attacks against **SKI**. In this paper, we present the security proofs. More precisely, we explicate a general formalism for distance-bounding protocols. Then, we prove that **SKI** and its variants is provably secure, even under the real-life setting of noisy communications, against the main types of relay attacks: distance-fraud and generalised versions of mafia- and terrorist-fraud. For this, we reinforce the idea of using secret sharing, combined with the new notion of a *leakage scheme*. In view of resistance to mafia-frauds and terrorist-frauds, we present the notion of *circular-keying* for pseudorandom functions (PRFs); this notion models the employment of a PRF, with possible *linear reuse* of the key. We also use *PRF masking* to fix common mistakes in existing security proofs/claims.

1 Introduction

Recently, we proposed the **SKI** [6,7,8] family of distance-bounding (DB) protocols.[4] In this paper, we present a formalism for distance-bounding, which includes a sound communication and adversarial model. We incorporate the notion of time-of-flight for distance-based communication. We further formalise security against distance-fraud, man-in-the-middle (MiM) generalising mafia-frauds, and an enhanced version of terrorist-fraud that we call *collusion-fraud*. Our formalisations take noisy communications into account.

Mainly in the context of security against generalised mafia-frauds (when TF-resistance is also enforced), we introduce the concept of *circular-keying security* to extend the security of a pseudorandom function (PRF) f to its possible uses

[4] Due to space constraints, we refer to these papers for an overview of DB protocols.

in maps of the form $y \mapsto L(x) + f_x(y)$, for a secret key x and a transformation L. We also introduce a *leakage scheme*, to resist to collusion frauds, and adopt the *PRF masking* technique from [4,5] to address distance-fraud issues. These formal mechanisms come to counteract mistakes like those in proofs based on PRF-constructions, errors of the kind exposed by Boureanu *et al.* [4] and Hancke [13].

We analyse and propose variants of **SKI** [6,7] and conclude that **SKI is historically the first practical class of distance-bounding protocols enjoying full provable security**.[5] On the way to this, we formalise the DB-driven requirements of the **SKI** protocols' components.

2 Model for Distance-Bounding Protocols

We consider a multiparty setting where each participant U is modelled by a probabilistic polynomial-time (PPT) interactive Turing machine (ITM), has a location loc_U, and where communication messages from a location to another take some time, depending on the distance to travel.

Consider two honest participants P and V, each running a predefined *algorithm*. Along standard lines, a general communication is formalised via an *experiment*, generically denoted $exp = (P(x; r_P) \longleftrightarrow V(y; r_V))$, where $r_{\langle\cdot\rangle}$ are the random coins of the participants. The experiment above can be "enlarged" with an adversary $\mathcal{A}$ which interferes in the communication, up to the transmitting-time constraints. This is denoted by $(P(x; r_P) \longleftrightarrow \mathcal{A}(r_\mathcal{A}) \longleftrightarrow V(y; r_V))$. At the end of each experiment, the participant V has an output bit Out_V denoting acceptance or rejection. The *view* of a participant on an experiment is the collection of all its initial inputs (including coins) and his incoming messages. We may group several participants under the same symbolic name.

We have a fixed integer constant $\mathbb{B}$ denoting the *distance-bound*. It defines what it means to be "close-enough" to a verifier V.

The crux of proving security of DB protocols lies in Lemma 1: if V sends a challenge c, the answer r in a time-critical challenge-response round is locally computed by a close participant $\mathcal{A}$ from its own view and incoming messages from far-away participants $\mathcal{B}$ which are independent from c. Clearly, it also captures the case where the adversary collects information during the previous rounds. On the one hand, we could just introduce a full model in which such a lemma holds. We do so in our eprint report [8]. On the other hand, we could also just state the text of the lemma and take it axiomatically.

Lemma 1. *Consider an experiment $\mathcal{B}(z; r_\mathcal{B}) \leftrightarrow \mathcal{A}(u; r_\mathcal{A}) \leftrightarrow V(y; r_V)$ in which the verifier V broadcasts a message c, then waits for a response r, and accepts if r took at most time $2\mathbb{B}$ to arrive. In the experiment, $\mathcal{A}$ is the set of all participants which are within a distance up to $\mathbb{B}$ to V, and $\mathcal{B}$ is the set of all other participants.*

[5] As far as we know, there exists only one other protocol with full provable security. It was presented at ACNS 2013 [12] and compared with **SKI** at PROVSEC 2013 [17]. All other protocols fail against at least one threat model. (See [7, Section 2].)

For each user U, we consider his view $View_U$ just before the time when U can see the broadcast message c. We say that a message by U is independent from c if it is the result of applying U on $View_U$, or a prefix of it. There exists an algorithm $\mathcal{A}$ and a list w of messages independent from c such that if V accepts, then $r = \mathcal{A}(View_{\mathcal{A}}, c, w)$, where $View_{\mathcal{A}}$ is the list of all $View_A$, $A \in \mathcal{A}$.

When modelling distance-bounding protocols, we consider provers P and verifiers V. $\mathcal{A}$ denotes the adversary and P^* denotes a dishonest prover.

Definition 2 (DB Protocols). *A **distance-bounding protocol** is a tuple $(Gen, P, V, \mathbb{B})$, where Gen is a randomised, key-generation algorithm such that (x, y) is the output*[6] *of $Gen(1^s; r_k)$, where r_k are the coins and s is a security parameter; $P(x; r_P)$ and $V(y; r_V)$ are PPT ITM running the algorithm of the prover and the verifier with their own coins, respectively; and $\mathbb{B}$ is a distance-bound. They must be such that the following two facts hold:*

- ***Termination**: $(\forall s)(\forall R)(\forall r_k, r_V)(\forall loc_V)$ when doing $(\cdot, y) \leftarrow Gen(1^s; r_k)$ and $(R \longleftrightarrow V(y; r_V))$, it is the case that V halts in $Poly(s)$ computational steps, where R is any set of (unbounded) algorithms;*
- *p-**Completeness**: $(\forall s)$ $(\forall loc_V, loc_P$ such that $d(loc_V, loc_P) \leq \mathbb{B})$ we have*

$$\Pr_{r_k, r_P, r_V}\left[\mathsf{Out}_V = 1 : \begin{array}{c}(x, y) \leftarrow Gen(1^s; r_k) \\ P(x; r_P) \longleftrightarrow V(y; r_V)\end{array}\right] \geq p.$$

Our model implicitly assumes *concurrency.*

Definition 3 (α-resistance to distance-fraud). *$(\forall s)$ $(\forall P^*)$ $(\forall loc_V$ such that $d(loc_V, loc_{P^*}) > \mathbb{B})$ $(\forall r_k)$, we have*

$$\Pr_{r_V}\left[\mathsf{Out}_V = 1 : \begin{array}{c}(x, y) \leftarrow Gen(1^s; r_k) \\ P^*(x) \longleftrightarrow V(y; r_V)\end{array}\right] \leq \alpha$$

where P^* is any (unbounded) dishonest prover. In a concurrent setting, we implicitly allow a polynomially bounded number of honest $P(x')$ and $V(y')$ close to $V(y)$ with independent (x', y').[7]

We now formalise resistance to MiM attacks. During a learning phase, the attacker $\mathcal{A}$ interacts with m provers and z verifiers. In the attack phase, $\mathcal{A}$ tries to win in an experiment in front of a verifier which is far-away from $\ell - m$ provers.

Definition 4 (β-resistance to MiM). *$(\forall s)(\forall m, \ell, z)$ polynomially bounded, $(\forall \mathcal{A}_1, \mathcal{A}_2)$ polynomially bounded, for all locations such that $d(loc_{P_j}, loc_V) > \mathbb{B}$, where $j \in \{m+1, \ldots, \ell\}$, we have*

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

[6] In this paper, there is just one common input, i.e., we assume $x = y$.
[7] This is to capture distance hijacking [10]. (See [8].)

over all random coins, where $View_{\mathcal{A}_1}$ is the final view of $\mathcal{A}_1$. In a concurrent setting, we implicitly allow a polynomially bounded number of $P(x')$, $P^*(x')$, and $V(y')$ with independent (x', y'), anywhere.

The classical notion of mafia-fraud [1] corresponds to $m = z = 0$ and $\ell = 1$. The classical notion of impersonation corresponds to $\ell = m$.

We now formalise the terrorist-fraud by [6,8].

Definition 5 ((γ, γ')-resistance to collusion-fraud). $(\forall s)(\forall P^*)$ *$(\forall loc_{V_0}$ s.t. $d(loc_{V_0}, loc_{P^*}) > \mathbb{B})$ $(\forall \mathcal{A}^{\mathsf{CF}}$ 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)[8] MiM attack with some parameters $m, \ell, z, \mathcal{A}_1, \mathcal{A}_2, P_i, P_j, V_{i'}$ 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 $P^{(*)} \in \{P, P^*\}$. Following the MiM requirements, $d(loc_{P_j}, loc_V) > \mathbb{B}$, for all $j \in \{m+1, \ell\}$. In a concurrent setting, we implicitly allow a polynomially bounded number of $P(x')$, $P^*(x')$, $V(y')$ with independent (x', y'), but no honest participant close to V_0.

Def. 5 expresses the following. If a prover P^*, situated far-away from V_0, can help an adversary $\mathcal{A}^{\mathsf{CF}}$ to pass, then a malicious $(\mathcal{A}_1, \mathcal{A}_2)$ could run a rather successful MiM attack playing with possibly multiple instances of $P^*(x)$ in the learning phase. In other words, a dishonest prover P^* cannot successfully collude with $\mathcal{A}^{\mathsf{CF}}$ without leaking some private information. We can find in [17] a discussion on the relation with other forms of terrorist frauds, including SimTF [11,12].

3 Practical and Secure Distance-Bounding Protocols

The protocol **SKI** [6,7] follows a long dynasty originated from [14]. It is sketched in Fig. 1. We use the parameters $(s, q, n, k, t, t', \tau)$, where s is the security parameter. The **SKI** protocols are built using a function family $(f_x)_{x \in GF(q)^s}$, with q being a small power of prime. In the DB phase, n rounds are used, with $n \in \Omega(s)$. Then, **SKI** uses the value $f_x(N_P, N_V, L) \in GF(q)^{t'n}$, with nonces $N_P, N_V \in \{0,1\}^k$ and a mask $M \in GF(q)^{t'n}$, where $k \in \Omega(s)$. The element $a = (a_1, \ldots, a_n)$ is established by V in the initialisation phase, and it is sent encrypted as $M := a \oplus f_x(N_P, N_V, L)$, with $M \in GF(q)^{t'n}$. Similarly, V selects a random linear transformation L from a set $\mathcal{L}$ (the *leakage scheme*), which is specified by the **SKI** protocol instance, and the parties compute $x' = L(x)$. The purpose of $\mathcal{L}$ is to leak $L(x)$ in the case of a collusion-fraud. Further, $c = (c_1, \ldots, c_n)$

[8] Here, we deviate from Def. 4 a bit by introducing $P^*(x)$ in the MiM attack.

is the challenge-vector with $c_i \in \{1,\dots,t\}$, $r_i := F(c_i, a_i, x'_i) \in GF(q)$ is the response to the challenge c_i, $i \in \{1,\dots,n\}$, with F (the *F-scheme*) as specified below. The protocol ends with a message Out_V denoting acceptance or rejection.

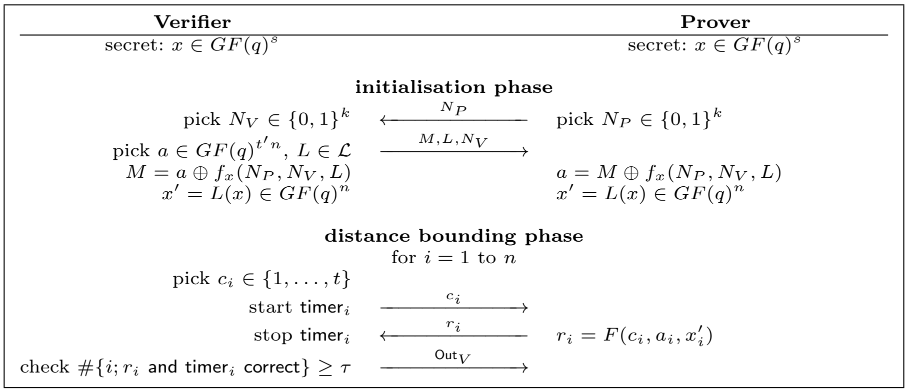

Fig. 1. The **SKI** schema of Distance-Bounding Protocols

In [6,7], several variants of **SKI** were proposed. We concentrate on two of them using $q = 2$, $t' = 2$, and the response-function

$$F(1, a_i, x'_i) = (a_i)_1 \qquad F(2, a_i, x'_i) = (a_i)_2 \qquad F(3, a_i, x'_i) = x'_i + (a_i)_1 + (a_i)_2,$$

where $(a_i)_j$ denotes the jth bit of a_i. In the $\mathbf{SKI_{pro}}$ variant, we have $t = 3$ and $\mathcal{L} = \mathcal{L}_{\mathsf{bit}}$, consisting of all L_μ transforms defined by $L_\mu(x) = (\mu \cdot x, \dots, \mu \cdot x)$ for each vector $\mu \in GF(q)^s$. I.e., n repetitions of the same bit $\mu \cdot x$, the dot product of μ and x. In the $\mathbf{SKI_{lite}}$ variant, we have $t = 2$ with the transform-set $\mathcal{L} = \{\emptyset\}$. Namely, $\mathbf{SKI_{lite}}$ never uses the $c_i = 3$ challenge or the leakage scheme.

We note that both instances are efficient. Indeed, we could precompute the table of $F(\cdot, a_i, x'_i)$ and just do a table lookup to compute r_i from c_i. For $\mathbf{SKI_{pro}}$, this can be done with a circuit of only 7 NAND gates and depth 4. For $\mathbf{SKI_{lite}}$, 3 NAND gates and a depth of 2 are enough. The heavy computation lies in the f_x evaluation, which occurs in a non time-critical phase.

In [8], we also consider other variants with different F-schemes.

***SKI** Completeness (in Noisy Communications).* Each (c_i, r_i) exchange is time-critical, so it is subject to errors. To address this, we introduce the probability p_{noise} of one response being erroneous. In practice, we take p_{noise} as a constant. Then, our protocol specifies that the verifier accepts only if the number of correct answers is at least a linear threshold τ. The probability that at least τ responses out of n are correct is given by:

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

Thanks to the Chernoff-Hoeffding bound [9,15], $\tau \leq (1 - p_{\mathsf{noise}} - \varepsilon)n$ implies $B(n, \tau, 1 - p_{noise}) \geq 1 - e^{-2\varepsilon^2 n}$. So, we obtain the following result.

Lemma 6. *For $\varepsilon > 0$ and $\frac{\tau}{n} \leq 1 - p_{\mathsf{noise}} - \varepsilon$, **SKI** is $(1 - e^{-2\varepsilon^2 n})$-complete.*

PRF masking. Importantly, **SKI** applies a random mask M on the output of f_x to thwart weaknesses against PRF programming [4]. This was called *PRF masking* in [4,5]. So, the malicious prover cannot influence the distribution of a.

F-scheme. Related to the response-function F, we advance the concept of *F-scheme*. This will take the response-function based on secret sharing by Avoine *et al.* [2] further, beyond protection against terrorist-fraud *only*, offering formalised sufficient conditions to protect against *all* three possible frauds.[9] Thus, we stress that using a secret sharing scheme in computing the responses may be too strong and/or insufficient to characterise the protection against frauds mounted onto DB protocols, and we amend this with Def. 7 and Def. 11.

Definition 7 (F-scheme). *Let $t, t' \geq 2$. An **F-scheme** is a function $F : \{1, \ldots, t\} \times GF(q)^{t'} \times GF(q) \to GF(q)$ characterised as follows.*

*We say that the F-scheme is **linear** if for all challenges c_i in their domain, the $F(c_i, \cdot, \cdot)$ function is a linear form over the $GF(q)$-vector space $GF(q)^{t'} \times GF(q)$ which is non-degenerate in the a_i component.*

*We say the F-scheme is **pairwise uniform** if*

$$(\forall I \subsetneq \{1, \ldots, n\}, \#I \leq 2)(H(x'_i | F(c_i, a_i, x'_i)_{c_i \in I}) = H(x'_i)),$$

where $(a_i, x'_i) \in_U GF(q)^{t'} \times GF(q)$, $\#S$ denotes the cardinality of a set S, and H denotes the Shannon entropy.

*We say the F-scheme is **t-leaking** if there exists a polynomial time algorithm E such that for all $(a_i, x'_i) \in GF(q)^{t'} \times GF(q)$, we have*

$$E\big(F(1, a_i, x'_i), \ldots, F(t, a_i, x'_i)\big) = x'_i.$$

*Let F_{a_i, x'_i} denote $F(\cdot, a_i, x'_i)$. We say that the F-scheme is **σ-bounded** if for any $x'_i \in GF(q)$, we have*

$$\mathbb{E}_{a_i}\left(\max_y \left(\#(F^{-1}_{a_i, x'_i}(y))\right)\right) \leq \sigma,$$

where $x'_i \in GF(q)$ and the expected-value is $\mathbb{E}$ taken over $a_i \in GF(q)^{t'}$.

The pairwise uniformity and the t-leaking property of the F-scheme say that knowing the complete table of the response-function F for a given c_i leaks x'_i, yet knowing only up to 2 entries challenge-response in this table discloses no information about x'_i. The σ-boundedness of the schemes says that the expected value (taken on the choice of the subsecrets a_i) of the largest preimage of the map $c_i \mapsto F(c_i, a_i, x'_i)$ is bounded by a constant σ. We have $\frac{t}{q} \leq \sigma \leq t$ due to the pigeonhole principle, since $\sum_y \#(F^{-1}_{a_i, x'_i}(y)) = t$. Furthermore, $\sigma \geq 1$.

[9] Secret sharing is used to defeat an attack from [16] which is further discussed in [3].

Lemma 8. *The F-scheme of* $\mathbf{SKI_{pro}}$ *is linear, pairwise uniform, $\frac{9}{4}$-bounded, and t-leaking. The F-scheme of* $\mathbf{SKI_{lite}}$ *is linear, pairwise uniform, $\frac{3}{2}$-bounded, but not t-leaking.*

The proof is available in [8].

Leakage scheme. We can consider several sets $\mathcal{L}$ of transformations to be used in the PRF-instance, of the **SKI** initialisation phase. The idea of the set $\mathcal{L}$ is that, when leaking some noisy versions of $L(x)$ for some random $L \in \mathcal{L}$, the adversary can reconstruct x without noise to defeat the terrorist fraud by Hancke [13].

Definition 9 (Leakage scheme). *Let $\mathcal{L}$ be a set of linear functions from $GF(q)^s$ to $GF(q)^n$. Given $x \in GF(q)^s$ and a PPT algorithm $e(x, L; r)$, we define an oracle $\mathcal{O}_{\mathcal{L},x,e}$ producing a random pair $(L, e(x, L))$ with $L \in_U \mathcal{L}$. $\mathcal{L}$ is a (T, r)-**leakage scheme** if there exists an oracle PPT algorithm $\mathcal{A}^{\langle\cdot\rangle}$ such that for all $x \in GF(q)^s$, for all PPT e, $\Pr[\mathcal{A}^{\mathcal{O}_{\mathcal{L},x,e}} = x] \geq \Pr_r[d_H(e(x, L), L(x)) < T]^r$, where d_H denotes the Hamming distance.*

Lemma 10. *$\mathcal{L}_{\mathsf{bit}}$ is a $(\frac{n}{2}, s)$-leakage scheme.*

Proof. $\mathcal{A}$ calls the oracle s times, then —by computing the majority– $\mathcal{A}$ deduces $\mu \cdot x$ with probability p, for each of the obtained μ. We run $\mathcal{O}_{\mathcal{L},x,e}$ until we collect s linearly independent μ values. All the s obtained $\mu \cdot x$ are correct with probability p^s. Then, we deduce x by solving a linear system. ☐

Circular-Keying Security. We introduce the notion of *security against circular-keying*, which is needed to prove security in the context in which the key x is used not only in the f_x computation.

Definition 11 (Circular-Keying). *Let s be some security parameter, let b be a bit, let $q \geq 2$, let $m \in Poly(s)$, and let $x, \overline{x} \in GF(q)^s$ be two row-vectors. Let $(f_x)_{x \in GF(q)^s}$ be a family of (keyed) functions, e.g., $f_x : \{0,1\}^* \to GF(q)^m$. For an input y, the output $f_x(y)$ can be represented as a row-vector in $GF(q)^m$.*

*We define an oracle $\mathcal{O}_{f_x,\overline{x}}$, which upon a query of form (y_i, A_i, B_i), $A_i \in GF(q)^s$, $B_i \in GF(q)^m$, answers $(A_i \cdot \overline{x}) + (B_i \cdot f_x(y_i))$. The game $Circ_{f_x,\overline{x}}$ of **circular-keying** with an adversary $\mathcal{A}$ is described as follows: we set $b_{f_x,\overline{x}} := \mathcal{A}^{\mathcal{O}_{f_x,\overline{x}}}$, where the queries (y_i, A_i, B_i) from $\mathcal{A}$ must follow the restriction that*

$$(\forall c_1, \ldots, c_k \in GF(q))\Big(\#\{y_i; c_i \neq 0\} = 1, \sum_{j=1}^{k} c_j B_j = 0 \Longrightarrow \sum_{j=1}^{k} c_j A_j = 0\Big).$$

*We say that the family of functions $(f_x)_{x \in GF(q)^s}$ is an (ε, C, Q)-*circular-PRF *if for any PPT adversary $\mathcal{A}$ making Q queries and having complexity C, it is the case that $\Pr[b_{f_x,x} = b_{f^*,\overline{x}}] \leq \frac{1}{2} + \varepsilon$, where the probability is taken over the random coins of $\mathcal{A}$ and over the random selection of $x, \overline{x} \in GF(q)^s$ and the random function f^*.*

The condition on the queries means that for any set of queries with the same value y_i, any linear combination making B_j vanish makes A_j vanish at the same time. (Otherwise, we would trivially extract some information about $\overline{x}$ by linear combinations.)

We note that it is possible to create secure circular-keying in the random oracle model. Indeed, any "reasonable" PRF should satisfy this constraint. Special constructions (e.g., the ones based on PRF programming from [4]) would not.

Lemma 12. *Let $f_x(y) = H(x, y)$, where H is a random oracle, $x \in \{0,1\}^s$, and $y \in \{0,1\}^*$. Then, f is a $(T2^{-s}, T, Q)$-circular PRF for any T and Q.*

The proof is available in [8].

We now state the security of **SKI**.

Theorem 13. *The **SKI** protocols are secure distance-bounding protocols, i.e.,:*

- *A. If the F-scheme is linear and σ-bounded, if $(f_x)_{x\in GF(q)^n}$ is a (ε, nN, C)-circular PRF, then the **SKI** protocols offer α-resistance to distance-fraud, with $\alpha = B(n, \tau, \frac{\sigma}{t}) + \varepsilon$, for attacks limited to complexity C and N participants. So, we need $\frac{\tau}{n} > \frac{\sigma}{t}$ for security.*
- *B. If the F-scheme is linear and pairwise uniform, if $(f_x)_{x\in GF(q)^n}$ is a $(\varepsilon, n(\ell+z+1), C)$-circular PRF, if $\mathcal{L}$ is a set of linear mappings, the **SKI** protocols are β-resilient against MiM attackers with parameters ℓ and z and a complexity bounded by C,*

  $$\beta = B\left(n, \tau, \frac{1}{t} + \frac{t-1}{t} \times \frac{1}{q}\right) + 2^{-k}\left(\frac{\ell(\ell-1)}{2} + \frac{z(z+1)}{2}\right) + \varepsilon.$$

  So, we need $\frac{\tau}{n} > \frac{1}{t} + \frac{t-1}{t} \times \frac{1}{q}$ for security.
- *B′. If the F-scheme is linear and pairwise uniform, if $(f_x)_{x\in GF(q)^n}$ is a $(\varepsilon, n(\ell+z+1), C)$-PRF, if the function $F(c_i, a_i, \cdot)$ is constant for each c_i, a_i, the **SKI** protocols are β-resilient against MiM attackers as above.*
- *C. If the F-scheme is t-leaking, if $\mathcal{L}$ is a (T, r)-leakage scheme, for all $\theta \in]0,1[$, the **SKI** protocols offer (γ, γ')-resistance to collusion-fraud, for γ^{-1} polynomially bounded, and*

  $$\gamma \geq B(T, T+\tau-n, \frac{t-1}{t})^{1-\theta} \quad , \quad \gamma' = \left(1 - B\left(T, T+\tau-n, \frac{t-1}{t}\right)^{\theta}\right)^{r}.$$

  So, we need $\frac{\tau}{n} > 1 - \frac{T}{tn}$ for security.

Th. 13 is tight for $\mathbf{SKI_{pro}}$ and $\mathbf{SKI_{lite}}$, due to the attacks shown in [6,7]. Following Lem. 8 and Th. 13, we deduce the following security parameters:

	α	β	γ
$\mathbf{SKI_{pro}}$	$B(n, \tau, \frac{3}{4})$	$B(n, \tau, \frac{2}{3})$	$B(\frac{n}{2}, \tau - \frac{n}{2}, \frac{2}{3})$
$\mathbf{SKI_{lite}}$	$B(n, \tau, \frac{3}{4})$	$B(n, \tau, \frac{3}{4})$	1

According to the data in the table above, we must take $1-p_{\mathsf{noise}}-\varepsilon \geq \frac{\tau}{n} \geq \frac{3}{4}+\varepsilon$ to make the above instances of **SKI** secure, with a failure probability bounded by $e^{-2\varepsilon^2 n}$ (by the Chernoff-Hoeffding bound [9,15]). If we require TF-resistance (as per Th. 13.C), we also get a constraint of $\frac{\tau}{n} > \frac{5}{6} + \frac{\varepsilon}{2}$, similarly.

The proof of Th. 13.B$'$ is similar (and simplified) as the one of Th. 13.B. So, we prove below the A, B, and C parts only.

Proof (Th. 13.A). For each key $x' \neq x$ for which there is a $P(x')$ close to V, we apply the circular-PRF reduction and loose some probability ε. (Details as for why we can apply this reduction will appear in the proof of Th. 13.B.)

If r_i comes form $P(x')$, due to the F-scheme being linear, r_i is correct with probability $\frac{1}{t}$. If r_i now comes from P^*, due to Lem. 1, r_i must be a function independent from c_i. So, for any secret x and a, the probability to get one response right is given by $p_i = \Pr_{c_i \in \{1,\ldots,t\}}[r_i = F(c_i, a_i, x_i')]$. Thanks to PRF masking, the distribution of the a_i's is uniform.

Consider the partitions I_j, $j \in \{1,\ldots,t\}$ as follows: I_j is the set of all i's such that $\max_y \left(\#(F^{-1}_{a_i,x_i'}(y)\right) = j$. Then, we are looking at the probability

$$P_j(x_i') := \Pr_{a_i}\left[\max_y \left(\#(F^{-1}_{a_i,x_i'}(y))\right) = j\right],$$

Given x' fixed, each iteration has a probability to succeed equal to $\sum_j \frac{jP_j}{t} = \frac{\sigma}{t}$. So, the probability to win the experiment is bounded by $p = B(n, \tau, \frac{\sigma}{t})$. □

Proof (Th. 13.B). Let $Game_0$ be the MiM attack-game described in Def. 4. Below we consider a prover P_j and a verifier V_k in an experiment, $j \in \{1,\ldots,\ell\}, k \in \{1,\ldots,z+1\}$. Let $(N_{P,j}, \overline{M}_j, \overline{L}_j, \overline{N}_{V,j})$ be the values of the nonces (N_P, N_V), of the mask M, and of the transformation L that the prover P_j generates or sees respectively, and $(\overline{N}_{P,k}, M_k, L_k, N_{V,k})$ be the values of the nonces (N_P, N_V), mask M, and transformation L that a verifier V_k generates or sees at his turn, $j \in \{1,\ldots,\ell\}, k \in \{1,\ldots,z+1\}$.

Using a reduction by failure-event F, the game $Game_0$ is indistinguishable to game $Game_1$ where no repetitions on $N_{P,j}$ or on $N_{V,k}$ happen, $j \in \{1,\ldots,\ell\}$, $k \in \{1,\ldots,z+1\}$ based on $\Pr[F] \leq 2^{-k}\left(\frac{\ell(\ell-1)}{2} + \frac{z(z+1)}{2}\right)$.

Since the F-scheme is linear, we can write $F(c_i, a_i, x_i') = u_i(c_i)x_i' + (v_i(c_i)\cdot a_i)$ where $u_i(c_i) \in GF(q), v_i(c_i) \in GF(q)^{t'}$. Note that, in terms of i, the vectors $(v_i(1),\ldots,v_i(t))$ span independent linear spaces. In $Game_1$, each (N_P, N_V, L, i) tuple can be invoked only twice (with a prover and a verifier) by the adversary. The pairwise uniformity of the F-scheme implies that $yv_i(c_i) + y'v_i(c_i') = 0$ implies $yu_i(c_i) + y'u_i(c_i') = 0$ for all $c_i, c_i' \in \{1,\ldots,t\}$ and all $y, y' \in GF(q)$. So, we deduce that the condition to apply the circular-keying reduction is fulfilled. We can thus apply the circular-PRF reduction and reduce to $Game_2$, where $F(c_i, f_x(N_P, N_V, L)_i, x_i')$ is replaced by $u_i(c_i)\tilde{x}_i + (v_i(c_i)\cdot f^*(N_P, N_V, L)_i)$, where f^* is a random function. This reduction has a probability loss of up to ε.

From here, we use a simple bridging step to say that the adversary $\mathcal{A}$ has virtually no advantage over $Game_2$ and a game $Game_3$, where the vector $a =$

$f^*(N_P, N_V, L)$ is selected at random. So, the probability p of $\mathcal{A}$ of succeeding in $Game_3$ is the probability that at least τ rounds have a correct r_i. Due to Lem. 1, r_i must be computed by $\mathcal{A}$ (and not P_j). Getting r_i correct for c_i can thus be attained in two distinct ways: 1. in the event $e1$ of guessing $c'_i = c_i$ and sending it beforehand to P_j and getting the correct response r_i, or 2. in the event $e2$ of simply guessing the correct answer r_i (for a challenge $c'_i \neq c_i$). So, $p = B(n, \tau, \Pr[e1] + \Pr[e2]) = B(n, \tau, \frac{1}{t} + \frac{t-1}{t} \times \frac{1}{q})$. □

Proof (Th. 13.C). Assume as per the requirement for resistance to collusion-fraud that there is an experiment $exp^{\mathsf{CF}} = (P^*(x) \longleftrightarrow \mathcal{A}^{\mathsf{CF}}(r_{\mathsf{CF}}) \longleftrightarrow V_0(y; r_{V_0}))$, with P^* a coerced prover who is far away from V_0 and that $\Pr_{r_{V_0}, r_{\mathsf{CF}}}[\mathsf{Out}_{V_0} = 1] = \gamma$. Given some random $c_1, \ldots, c_n$ from V_0, we define $View_i$ as being the view of $\mathcal{A}^{\mathsf{CF}}$ before receiving c_i from V, and w_i as being all the information that $\mathcal{A}^{\mathsf{CF}}$ has received from P^* before it would be too late to send r_i on to V_0. This answer r_i done by $\mathcal{A}^{\mathsf{CF}}$ is formalised in Lem. 1. So, $r_i := \mathcal{A}^{\mathsf{CF}}(View_i \| c_i \| w_i)$.

Let C_i be the set of all possible c_i's on which the functions $\mathcal{A}^{\mathsf{CF}}(View_i \| \cdot \| w_i)$ and $F(., a_i, x'_i)$ match. Let $C_i = \{c \in \{1, \ldots, t\} \mid \mathcal{A}^{\mathsf{CF}}(View_i \| c \| w_i) = F(c, a_i, x'_i)\}$, $S = \{i \in \{1, \ldots, n\} \mid c_i \in C_i\}$, and $R = \{i \in \{1, \ldots, n\} \mid \#C_i = t\}$. The adversary $\mathcal{A}$ succeeds in exp^{CF} if $\#S \geq \tau$.

If we were to pick a set of challenges such that $\#S \geq \tau$ and $\#R \leq n - T$, we should select a good challenge (from no more than $t-1$ existing out of t), for at least $T + \tau - n$ rounds out of T. In other words, $\Pr[\#S \geq \tau, \#R \leq n - T] \leq B(T, T + \tau - n, \frac{t-1}{t})$. But, by the hypothesis, $\Pr[\#S \geq \tau] \geq \gamma$. So, we deduce immediately that $\Pr[\#R \leq n - T | \#S \geq \tau] \leq \gamma^{-1} B(T, T + \tau - n, \frac{t-1}{t})$. Therefore, $\Pr[\#R > n - T | \#S \geq \tau] \geq 1 - \gamma^{-1} B(T, T + \tau - n, \frac{t-1}{t})$.

We use $m = \ell = z = \mathcal{O}(\gamma^{-1} r)$ (i.e., $\mathcal{A}_2$ will directly impersonate P to V after $\mathcal{A}_1$ ran m times the collusion fraud, with P^* and V). We define $\mathcal{A}_2$ such that, for each execution of the collusion fraud with P^* and V, it gets $View_i$, w_i. For each i, $\mathcal{A}_2$ computes the table $c \mapsto \mathcal{A}^{\mathsf{CF}}(View_i \| c \| w_i)$ and apply the t-leaking function E of the F-scheme on this table to obtain $y_i = E(c \mapsto \mathcal{A}^{\mathsf{CF}}(View_i \| c \| w_i))$. For each $i \in R$, the table matches the one of $c \mapsto F(c, a_i, x'_i)$ with $x' = L(x)$, and we have $y_i = x'_i$. So, $\mathcal{A}_2$ computes a vector y. If V accepts the proof, then y coincides with $L(x)$ on at least $n - T + 1$ positions, with a probability of at least $p := 1 - \gamma^{-1} B(T, T + \tau - n, \frac{t-1}{t})$. That is, after $\mathcal{O}(\gamma^{-1})$ runs, $\mathcal{A}_2$ implements an oracle which produces a random $L \in \mathcal{L}$ and a y which has a Hamming distance to $L(x)$ up to $T - 1$.

By applying the leakage scheme decoder e on this oracle, with r samples, it can fully recover x, with probability at least p^r. Then, by taking $\gamma = B(T, T + \tau - n, \frac{t-1}{t})^{1-\theta}$ and $\gamma' = \left(1 - B(T, T + \tau - n, \frac{t-1}{t})^{\theta}\right)^s$, we obtain our result. □

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. G. Avoine, C. Lauradoux, B. Martin. How Secret-Sharing can Defeat Terrorist Fraud. In *ACM Conference on Wireless Network Security WISEC'11*, Hamburg, Germany, pp. 145–156, ACM, 2011.
3. A. Bay, I. Boureanu, A. Mitrokotsa, I. Spulber, S. Vaudenay. The Bussard-Bagga and Other Distance-Bounding Protocols under Attacks. In *Information Security and Cryptology INSCRYPT'12*, Beijing, China, Lecture Notes in Computer Science 7763, pp. 371–391, Springer-Verlag, 2012.
4. 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 *Progress in Cryptology LATINCRYPT'12*, Santiago, Chile, Lecture Notes in Computer Science 7533, pp. 100–120, Springer-Verlag, 2012.
5. I. Boureanu, A. Mitrokotsa, S. Vaudenay. On the Need for Secure Distance-Bounding. In *Early Symmetric Crypto ESC'13*, Mondorf-les-Bains, Luxembourg, pp. 52–60, University of Luxembourg, 2013.
6. I. Boureanu, A. Mitrokotsa, S. Vaudenay. Towards Secure Distance Bounding. To appear in the proceedings of FSE'13.
7. I. Boureanu, A. Mitrokotsa, S. Vaudenay. Secure & Lightweight Distance-Bounding. In *Lightweight Cryptography for Security and Privacy LightSec'13*, Gebze, Turkey, Lecture Notes in Computer Science 8162, pp. 97–113, Springer-Verlag, 2013.
8. I. Boureanu, A. Mitrokotsa, S. Vaudenay. Practical & Provably Secure Distance-Bounding. Eprint technical report, 2013. http://eprint.iacr.org/2013/465.pdf
9. H. Chernoff. A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the sum of Observations. *Annals of Mathematical Statistics*, vol. 23 (4), pp. 493–507, 1952.
10. 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, California, USA, pp. 113–127, IEEE Computer Society, 2012.
11. 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.
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. W. Hoeffding. Probability Inequalities for Sums of Bounded Random Variables. *Journal of the American Statistical Association*, vol. 58, pp. 13–30, 1963.
16. 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.
17. S. Vaudenay. On Modeling Terrorist Frauds. In *Provable Security ProvSec'13*, Melaka, Malaysia, Lecture Notes in Computer Science 8209, pp. 1–20, Springer-Verlag, 2013.