Secure Object Identification - or: Solving The Chess Grandmaster Problem

Ammar Alkassar*
Saarland University/Sirrix AG
Im Stadtwald, Gebäude 45
D-66123 Saarbrücken, Germany
alkassar@ieee.org

Christian Stüble
Saarland University
Im Stadtwald, Gebäude 45
D-66123 Saarbrücken, Germany
stueble@acm.org

Ahmad-Reza Sadeghi
Bochum University/Eurobits Center
D-44780 Bochum, Germany
sadeghi@crypto.rub.de

ABSTRACT

Many applications of cryptographic identification protocols are vulnerable against physical adversaries who perform real time attacks. For instance, when identifying a physical object like an automated teller machine, common identification schemes can be bypassed by faithfully relaying all messages between the communicating participants. This attack is known as *mafia fraud*.

The Probabilistic Channel Hopping (PCH) system we introduce in this paper, solves this problem by hiding the conversation channel between the participants. The security of our approach is based on the assumption that an adversary cannot efficiently relay all possible communication channels of the PCH system in parallel.

Keywords

Identification, Mafia fraud, Chessmaster Problem, Fake equipment

1. MOTIVATION

A famous story of the little girl who played ... against two Chess Grandmasters ... How was it possible to win one of the games? Anne-Louise played Black against Spassky. White against Fisher. Spassky moved first, and Ann-Louise just copied his move as the first move of her game against Fisher, then copied Fisher's replay as her own reply to Spassky's first move, and so on. [13]

This problem exploited by Anne-Louise is known in the cryptographic community as *Chess Grandmaster Problem* and the resulting attack is denoted as *mafia-fraud*. A similar problem arises in the context of secure device identification [25]: Today, many users store private data and other security-critical information onto personal platforms like notebooks, mobile phones or Personal Digital Assistants (PDA). In the future, the economical and social value of stored information will increase in accordance to the performance and storage capacity of such devices. Surely, next-generation mobile devices will become more secure, but even if the underlying hardware and the stored information are well-protected by secure mechanisms, adversaries can deceive users by dummy devices performing a mafia fraud. Users cannot be sure that they are really using *their* device and not a similar looking one, since commonly used identification schemes only prove the identity of the end-point of the communication, but give no hint *where* it is.

Solving the mafia fraud problem is also essential for various other civil and military applications. Consider for example an access control system that controls access to rooms within a building. Individuals have different access privileges for different rooms. The access control system plays the role of a verifier to whom the individuals have to prove their identity. A cheating prover Hugo now could cooperate in real-time with another attacker Vicky, who plays the role of an access control terminal. An honest prover Alice, who wants to identify herself towards the alleged verifier Vicky enables Hugo to bypass the access control by pretending to be Alice, and thus, getting an unauthorized access to some room.

Another classic application is the Identification between Friend or Foe (IFF): Today, IFF systems are an essential part of military vehicles and platforms, be it a ship, aircraft, helicopter, tank or even soldiers [12]. Installed in such a platform, common systems use a challenge-response protocol based on cryptographic identification schemes: Pre-set codes within various modes are agreed upon and disseminated among friendly units. Only if an incoming unit responds correctly to these codes it is regarded as friendly.[1]

However, mafia frauds are not only a theoretical problem. For instance, attacks against automated teller machines (ATMs) became popular: ATM crackers set up a faked cash machine in a mall to deceive ignorant users which put their credit card into it and entered their PIN.

Identification schemes (IS), e.g., [18, 22, 5, 28], are used in many applications, but Beth and Desmedt have already observed in [9] that mafia frauds cannot be prevented *only*

*This work is supported in part by the Konrad-Adenauer-Foundation.

[1] Anderson tells in [2] a nice story about a "Mig-in-the-Middle-Attack" in the Angolan civil war. Although it is apocryphal, it illustrates the power of mafia frauds.

by using cryptographic mechanisms.[2]

These schemes only authenticate logical attributes like keys, names or other kinds of ids, but physical attributes like the localization of the identified end-point of the communication are not considered. Thus, it is impossible to detect whether the expected end-point gives the answer himself or by (ab)using a third party. On the one hand, this restriction is harmless as long as the exact position of the end-point is not relevant (e.g., by performing an authenticated key exchange protocol to a logical entity). On the other hand, this property is significant whenever the identification aspect comes to the fore, e.g., if a physical object has to be identified.

Therefore, by designing an identification scheme resisting mafia frauds, we can solve many practical security problems of identification systems.

This paper is organized as follows: The next section discusses related work dealing with approaches against mafia frauds. Section 2 defines the environment and extends the definition of identification schemes in such a way that they cover mafia frauds. Section 3 discusses the general idea of our paradigm, followed by concrete identification protocols based on different identification paradigms in Section 4. Section 5 discusses further constrains to be considered for technical realizations and Section 6 ends up with a short summary. An instantiation of this paradigm was applied with respect to friend or foe identification in [1].

1.1 Related Work

Because mafia frauds cannot be solved by relying only on cryptographic mechanisms, alternative solutions have been proposed in literature.

Desmedt proposes in [15] a countermeasure against mafia frauds by exchanging the physical locations of the participants in an authenticated way, e.g., by cryptographically signing the location given by a Global Positioning System (GPS) or cell localization in GSM. Denning and MacDoran propose in [14] a location-based authorization mechanism using GPS signals. Both solutions have two important restrictions. First, users have to trust that the underlying systems (GPS, GSM) cannot be fooled. Second, users have to trust the system-providers, e.g., the U.S. government in the case of GPS.

In [8], Bengio et al. propose the isolation of the object to be identified (e.g., a Faraday cage) during the identification process to prevent communication with a third party. A common example are ATMs which isolate ATM card during the authentication process. This solution not only requires that the object's owner trusts the identifying instance, it also seems to be impractical for large objects like aircrafts.

In [9], Beth and Desmedt propose a solution in which all transmission times have to be measured precisely. They argue that speed of light is constant. Considering the inaccuracy in speed of computing, their solution become unpracticable for many applications. An interesting approach within that work is solving a game theoretic problem, the Chess Grandmaster Problem, into which the identification problem is transformed.

Brands and Chaum propose in [10] a solution they call distance-bounding. That promising principle is also based on the constancy in speed of light and faces therefore similar problems like the solution proposed by Beth and Desmedt. They elude the problem in the different speeds in computing by determining an upper-bound on the physical distance between the two parties participating in the identification process. Furthermore, they show how to adapt the principle in known public key identification schemes such as Fiat-Shamir [20].

[2]The mafia fraud should not be mixed up with the classic man-in-the-middle attack on unauthenticated key-exchange protocols like the Diffie-Hellman key agreement. In contrast to mafia frauds, man-in-the-middle attacks could be prevented effectively using build-in authentication mechanisms, e.g., in [29]. That is because of the target of the man-in-the-middle attack is the confidentiality of a specific communication session whereas the mafia fraud's target is the identification process of physical objects.

2. DEFINITIONS

In literature, the terms *identification* and *entity authentication* are often used synonymously (see e.g., [23]). Especially in our context it seems to be useful to be more precise:

Authentication is a term which is used in a very broad sense and is specific to the security objective concerned. Such objectives could be access control, entity authentication, message authentication or key authentication. Entity authentication is usually defined as the process whereby one party is assured of the identity of a second party involved in a protocol, and that the second party has actually participated in the corresponding session.

In our context we denote with *(object-) identification* the entity authentication in which the security objective is to identify an (unknown) physical object at a specific location. Typical object identification according to our definition is performed by an access control system that permits access to some area. Another example is given in the motivation: A user identifying its device before entering critical data. However, the entity authentication for getting remote login into some computer system we do not call object identification, because access is not bound to a physical object (only to a logical entity of the IT-system).

2.1 Communication Channel

DEFINITION 1. ***[Communication Channel]*** *We define χ^{PV} to be an unidirectional communication channel from a party P to another one V with two allowed operations:*

$$send(\chi^{PV}, m)$$

sends the message m on channel χ^{PV} from P to V, and

$$receive(\chi^{PV}, m)$$

indicates that V receives message m sent by P on channel χ^{PV}. If no message was sent on channel χ^{PV} the received message is $\emptyset$.

In the following, the interactions between honest entities are modeled using $send()$ and $receive()$ operations. Furthermore, we work in the synchronous model with fixed rounds t, and in every round only one message could be sent or received on every channel χ.

2.2 Nomenclature

An identification scheme IS enables one entity to identify itself to another. The entity identifying itself is typically called the prover P, while the other one is called the verifier V. More formally, we follow the definition of [21]:

DEFINITION 2. ***[Identification Scheme]*** *An identification scheme (IS) consists of a pair (G, B), where G is a probabilistic polynomial-time algorithm with $pk \leftarrow G_{sk}(id)$ and $B = (P, V)$ is a pair of probabilistic polynomial-time interactive machines satisfying the completeness and soundness condition. We denote by $ID^{P(y),V(z)}(x)$ the random variable representing the (local) output of V when interacting with P on common input x, when the random input to each machine is uniformly and independently chosen, and P (resp., V) has the the auxiliary input y (resp., z).*

To use the identification scheme, the prover, whose identity is encoded by the string id, should first uniformly select a secret sk, compute $pk := G_{sk}(id)$, ask the trusted third party to place the record (id, pk) in the public file, and store the string sk in a safe place. The completeness condition asserts that the prover can convince the verifier of his identity by executing the identification protocol: The prover invokes the program P using the stored string sk as auxiliary input, and the verifier uses the program V and makes sure that the common input is the public record containing id (which is the public file).

Towards the goal of proving identification protocols secure against mafia frauds, we provide now an adequate definition for the security of an identification system:

2.3 Security of Identification Schemes

In the context of identification schemes, several security definitions based on different settings are considered in literature: The trivial case in which the adversary has no access to any prover instance we call the *no-prover*-setting. In the *static* setting (*cc1*) (which is equivalent to [21] and the *cr-1* setting in [5]), the adversary has access to a prover instance *before* performing the attack.

We stress that in the *cc*1-setting the adversary cannot impersonate the prover to the verifier provided that he cannot interact concurrently with both the prover *and* the verifier. As already discussed in Section 1 this restriction does not map real-life for many applications.

Because this problem seemed not to be solvable adequately, modeling secure identification systems based on fading out that problem by a different definition (*cc2*[3]): E.g., in [5, 7, 16] concurrent interaction is allowed, but an identification system is said to be secure if the *only* way to make the verifier accept is in relaying all protocol steps.

For our purposes we define and use the *adaptive* setting (*cc3*) in which the adversary has a concurrent access to prover instances *while* attacking the verifier. Loosely speaking, our security condition asserts that an adversary A, who interacts concurrently in the role of a verifier and a prover, cannot make the verifier accept.

Obviously, this setting matches our scenarios given in Section 1. More formally, we obtain the following conditions of our definition:

DEFINITION 3. ***[Security of Identification Schemes]*** *An identification scheme (IS) as described in Definition 2 is secure if it satisfies the following conditions:*

Completeness *The prover P can convince the verifier V of correct statements using a given witness sk. For every protocol session $ID^{P(sk),V}(pk) \in \{accept, reject\}$ between P and V on common input pk, the probability that a verifier V accepts an honest prover P is:*

$$\mathtt{Prob}[ID^{P(sk),V}(pk) = accept] = 1$$

This condition is simply the property that everything works if nobody cheats.

Soundness: *Not even a cheating prover C can convince an honest verifier of wrong statements. The success probability of a probabilistic polynomial-time interactive machine A (adversary), with access to a prover oracle $\mathcal{O}(sk_L)$ acting like a prover instance $P(sk_L)$ with access to the secret sk_L, to convince an honest verifier V is negligible for every sufficiently large security parameter $L \in \mathbb{N}$ and every randomly distributed sk_L with $pk_L \leftarrow G_{sk_L}(id)$:*

$$\mathtt{Prob}[ID^{C^{\mathcal{O}(sk_L)}(aux),V}(pk_L) = accept] < \epsilon$$

where the prover oracle enables the adversary to start (polynomially many) ID sessions with prover instances P and communicate via their public interfaces.

Algorithm G is called the information generating algorithm, and the pair (P, V) is called the identification protocol.

2.4 Channel Hopping (CH) System

Before we can propose the identification protocol, we first define a CH system:

DEFINITION 4. ***[Channel Hopping System]*** *A CH system consists of the triple $(\mathcal{M}, O, N)$, where $\mathcal{M}$ stands for the set of possible communication channels $\chi_1^{PV}..\chi_O^{PV}$, $O := |\mathcal{M}|$ defines the number of channels and N defines the number of channels that are used by the CH system in one round simultaneously. Further, we define two operations on CH systems:*

$$send_{CH}(\{(\chi_{s_i}^{PV} \in \mathcal{M}, m_i) | i = 1..N\})$$

sends in one round from P to V N messages $m_1, .., m_N$ using N communication channels $\chi_{s_1}^{PV}, .., \chi_{s_N}^{PV}$ and

$$receive_{CH}(\{(\chi_{s_i}^{PV} \in \mathcal{M}, m_i) | i = 1..N\})$$

receives in one round N messages $m_1..m_N$ using the N given communication channels $\chi_{s_1}^{PV}, .., \chi_{s_N}^{PV}$, respectively.

For simplicity we define the messages space to be $\{0, 1\}$. The set of N messages (bits) $m_1..m_N$ sent in one round is denoted as *symbol*.

3. A NEW APPROACH TO OBJECT IDENTIFICATION

As aforementioned, the reason why adversaries can perform a *mafia fraud* is because they know the used communication channel and can therefore relay all messages between the honest users without them noticing the attack.

To relay messages an adversary A has to be able to eavesdrop it. Therefore, by preventing that A can *eavesdrop* messages, *mafia frauds* can be prevented.

[3]We call this setting the cc2-setting (and which is equivalent to the cr2-setting in [5]) to remain consistent with increasing security. We will not consider this setting furthermore.

We denote χ^{PV} a *hidden communication channel* or *hidden channel* between P and V if A is unable to read the data transferred by it (the messages are invisible to him).

We denote χ^{PV} a *probabilistic hidden communication channel* or *probabilistic channel* if A can successfully eavesdrop one message with a chance $p_{succ} < 1$. By increasing the number of messages sent by a probabilistic hidden communication channel we can make the probability that A eavesdrops all messages arbitrarily small.

We now introduce how a probabilistic hidden communication channel can be build from a large set of simple communication channels used by a CH system. We assume that the adversary is unable to eavesdrop all communication channels of the underlying CH system in parallel. In Section 5 we show that this assumption holds in practice.

DEFINITION 5. ***[Probabilistic Channel Hopping System]*** *Let $PCH = (\mathcal{M}, O, N)$ denote a CH system and $M < O$ be the number of channels that an adversary A can simultaneously eavesdrop. Further, let $S = \{s_i | s_i \in \{1 \dots O\}, i = 1 \dots N\}$ be secret random values only known to V and P. To provide a probabilistic hidden communication channel between P and V, the symbols to be transferred have to be send/received as described in Definition 4 using randomly chosen communication channels $\chi^{PV}_{s_1}, .., \chi^{PV}_{s_N}$ defined by the shared random value S.*

Loosely speaking, P and V randomly select the channels they use by the CH system to transfer a symbol. We now show that a probabilistic channel hopping system behaves like a probabilistic hidden communication channel.

LEMMA 1. *A Probabilistic Channel Hopping System used as described in Definition 5 is a probabilistic hidden (meta-) channel with an adversaries success probability of*

$$p_{sym} = \sum_{s=0}^{N} [\frac{\binom{N}{s}\binom{O-N}{M-s}}{\binom{O}{M}} \frac{1}{2^{n-s}}]$$

to relay one complete symbol transferred by the PCH system.

We first show that the adversary's success probability p_{sym} to guess one symbol correctly is less than 1. Next, we show that there is no better way for an adversary to convince a verifier of being a legitimate prover than guessing the channels.

PROOF. The probability for hitting exactly s of the N used channels correctly by guessing M channels is:

$$p_{guess}(s, N, M) = \frac{\binom{N}{s}\binom{O-N}{M-s}}{\binom{O}{M}}$$

Note that we do not make assumptions on the number of *send*() operations an adversary can perform. Therefore A can guess the other $O - M$ messages by sending values on all other channels. Because the messages of one symbol contain only one bit, the adversary's success probability to correctly guess one is $\frac{1}{2}$. Moreover, we obtain the overall success probability

$$p_{sym} = \sum_{s=0}^{N} [\frac{\binom{N}{s}\binom{O-N}{M-s}}{\binom{O}{M}} \frac{1}{2^{N-s}}]$$

of guessing one independent symbol correctly (and completely). □

LEMMA 2. *The adversary's maximum probability of successfully relaying one symbol is less than 1.*

PROOF. In our setting M is restricted to be smaller than O, so the adversary has a maximum success probability with $M = O - 1$. Two cases are possible: The adversary guesses all channels correctly or the message of one channel has to be guessed.

The probability for guessing *all* N used channels correctly ($s := N$) is

$$\begin{aligned} p_{guess}(N, N, M) &= \frac{\binom{N}{N}\binom{O-N}{M-N}}{\binom{O}{M}} \\ &= \frac{(O-N)! \quad (O-M)! \quad M!}{(O-N-M+N)! \quad (M-N)! \quad O!} \\ &= \frac{(O-N)! \quad M!}{(M-N)! \quad O!} \\ &= \frac{\binom{M}{N}}{\binom{O}{N}} \end{aligned}$$

With $M = O - 1$ holds:

$$\begin{aligned} p_{max}(N) &= \frac{\binom{M}{N}}{\binom{O}{N}} = \frac{\binom{O-1}{N}}{\binom{O}{N}} \\ &= \frac{(O-1)! \quad (O-N)! \quad N!}{(O-N-1)! \quad N! \quad O!} \\ &= \frac{O-N}{O} \end{aligned}$$

The probability for guessing the missing message (one bit) if guessing the correct channel fails is

$$p_m(N, N, M) = (1 - \frac{O-N}{O}) \cdot \frac{1}{2}$$

Therefore, the attackers overall success probability to intercept one message is

$$\begin{aligned} p_{max}(N, N, M) &= \frac{O-N}{O} + (1 - \frac{O-N}{O}) \cdot \frac{1}{2} \\ &= \frac{O-N}{2 \cdot O} + \frac{1}{2} < 1 \end{aligned}$$

□

4. CONCRETE IDENTIFICATION SCHEMES

The most natural way to treat identification schemes is by relating them to the general concept of proofs of ability (to do something). Within this concept there are some well-known paradigms for constructing secure identification schemes. For instance, it is everydays practice to identify people by their ability to produce signatures. This practice has been carried into the digital setting by using *digital signature* schemes (see, e.g., [28]). Another paradigm used in the earlier treatments is the *encryption-based identification* scheme using secure encryption functions. The entity identifying itself convinces the other entity by being "able to" decrypt arbitrary ciphertext.

A relatively new paradigm which is strongly linked with identification in contemporary cryptography is that of *proof of knowledge*. A natural way to determine a person's identity

is to ask him to provide a proof of knowledge of a fact that only this person is supposed to know.

In this contribution we add another paradigm we call *key-exchange based identification*. We reduce the security of the constructed identification scheme to that of a secure authenticated key-exchange protocol that is secure in the sense of simulability (see [26] and [29]).

For simplicity matters we only consider unilateral identification from which mutual identification could be easily derived by executing the protocol once in every direction. Therefore, only prover have to provide a public record and distribute it in an authentic way.

The following subsections present identification schemes secure in the sense of Definition 3, based on different underlying cryptographic mechanisms. An encryption-based system could be found in [1].

4.1 An Authenticated Key-Exchange Based Protocol

In this Section, we present a general identification protocol based on an authenticated key establishment protocol (AKE) that is secure according to Definition 3.

An AKE allows two interactive machines V and P with common input pk_P and P's secret input sk_P to exchange a session key key. We demand the following properties (which are mainly adapted from [23] and [29]):

Authenticity V is assured that no other party than P may gain access to a particular session key key.

Freshness The resulting key key has to be new and independent of preliminary created session keys.

Semantically secure Every single bit of the resulting session key key should be unpredictable.

We first outline the general structure of the scheme. Let $\mathcal{KE}$ be an authenticated key establishment protocol between P and V that is secure according to [29]. After the last message both P and V have a fresh, authentic and semantically secure session key key.

We further assume that P and V are using a PCH system as defined in Definition 5 that uses N channels in parallel and that A is able to eavesdrop M channels with $N \leq M < O$. It follows a short outline of the general protocol as described in 1.

Step 1 The prover and the verifier exchange a secret session key

$$key := m_1^1 \dots m_N^L | d_1^1 \dots d_N^L$$

with $m_n^l \in \{0,1\}$ and $d_n^l \in \{1 \dots O\}$ using the KE protocol, based on common input pk_P and P's secret input sk_P.

Step 2 The message $msg = m_1^1 \dots m_N^L$ is sent from P to V using the PCH system as described in Definition 5 using the secret input $d_1^1 \dots d_N^L$.

Step 3 The verifier accepts, if the received message msg is similar to the earlier exchanged part of the session key $m_1^1 \dots m_N^L$

Now we can formulate the main security theorem:

THEOREM 1. *Let $\mathcal{KE}$ be an authenticated key establishment protocol that provides an authentic, fresh and semantically secure key 'key' between P and V. Then the protocol described in Figure 1 is a secure identification scheme according to Definition 3.*

Proof Sketch. The adversary does not know the session key key and therefore also not the messages m_n^l because of the *authenticity* property of the underlying AKE protocol. Due to the *freshness* property an adversary gains no useful information from different sessions.

It remains to show that the probability of intercepting the prover's last message is negligible in L. This message is sent via the PCH system using the channels defined by the random secret key key. So, the randomly selected channels d_n^l will remain independent from each other. According to Lemma 1 the adversary's probability of relaying the last message is $(p_{sym})^L$. Finally, we get

$$\begin{aligned} &\texttt{Prob}[ID^{A^{P(sk_L),V}}(pk_L) = accept] \\ &= (p_{sym})^L \\ &= (\sum_{s=0}^{N} [\frac{\binom{N}{s}\binom{O-N}{M-s}}{\binom{O}{M}} \frac{1}{2^{n-s}}])^L \end{aligned}$$

and with Lemma 2, the adversary's probability p_{sym} of guessing one symbol correctly is smaller than 1 and thus

$$\texttt{Prob}[ID^{A^{P(sk_L),V}}(pk_L) = accept] < \epsilon$$

for all sufficiently large L. ϵ is a (fixed) system variable that only depends on the security parameter L and the relation of M, N and O.

4.2 Proof of Knowledge Based Protocol

We will now describe an identification protocol based on common proof of knowledge techniques and that is resistant against mafia frauds using the channel hopping technique.

The protocol is based on [11] for proving knowledge of a discrete representation and the modifications of [24]. Whereby the security is based on the intractability of discrete log.

Initialization Initially the prover (or a trusted third party) generates a public key $pk := (p, q, g_1, g_2, h, l)$ and a secret key $sk := (m_1, m_2)$, where p and q are primes such that $q|p-1$, g_1, g_2 are of order q in the group $\mathbb{Z}_p^*$, $l = O(|p|)$, $m_1, m_2 \in_R \mathbb{Z}_q$ and $h := g_1^{-m_1} g_2^{-m_2} \bmod p$. $RG(\cdot)$ is a secure pseudorandom generator following [6] and $E_u(x)$ is a function that enlarges the bit-length of x without altering the probability distribution of x using the the random variable d. We represent $d := d_1^1 ... d_N^1 | d_1^2 ... d_N^2 | ... | d_1^L ... d_N^L$ and $d^i := d_1^i ... d_N^i$.

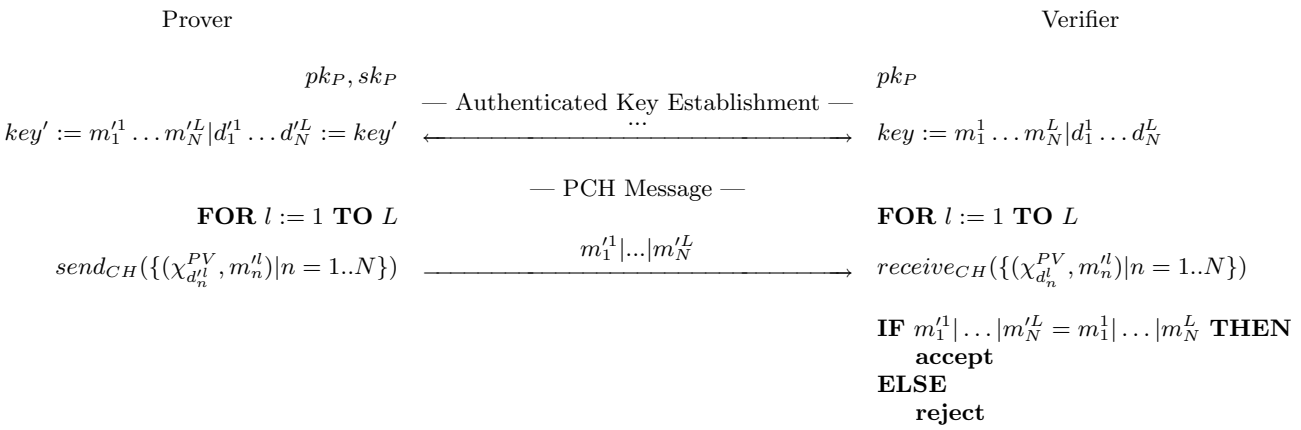
Protocol See Figure 2

Security Considerations. To show the security of the identification scheme, we use the notion of *witness-hiding* [19] rather than the stronger notion of *zero-knowledge*. Mostly, zero-knowledge-proofs are not proven to be secure in the concurrent setting we are faced with in the mafia fraud [4].

In contrast, witness-hiding is preserved under arbitrary composition of protocols (sequential and parallel) including concurrent execution.

[4]More about concurrent zero-knowledge systems can be found in [16, 17]

Figure 1: Authenticated Key Establishment Based Protocol.



According to [19] an identification scheme is secure in sense of our definition 3 if the scheme is witness-hiding and an interactive proof of knowledge. This is roughly because if there exists an adversary A with non-negligible probability of success, we can construct a knowledge extractor (from the knowledge soundness), which leads to contradiction with witness hiding.

Proof Sketch. First we proof that the scheme provides a proof of knowledge by constructing a knowledge extractor K. We follow the idea of [11]:

Program for K (on input of public values (p, q, g_1, g_2, l, h)):

Step 1 Let P^* run from its initial state, with a random tape chosen uniformly and independently of other runs, until it sends a value a. Chose y randomly. Store the current state as *state*.

Step 2 Send challenge c and b_1, b_2 as in protocol description. Let P^* continue until it sends a value r via channel χ^{PV}_d.

Step 3 Reset P^* to *state*, send it the challenge c', and let it run again (with the same b_i) until it sends a value r'.

Step 4 Repeat Step 3 until P^* responds correctly to different *challenges* (for the same a). Now, we can calculate the witness as $(m_1, m_2) = ((r_1 - r'_1)/(c - c'), (r_x - r'_2)/(c - c'))$.

End K

Note, that normally the knowledge-extractor do *not* work in the concurrent setting. The verifier faces the possibility that the prover with which it is interacting is actually using some concurrently running second interaction as an oracle (according to Definition 3) to help answer verifiers queries - without being in possession of the witness.

Technically, the extractor fails because K can certainly reset the prover instance directly connected with, but the malicious prover fails in resetting the oracle. Hence, we receive a "correct" prover without being able to extract the witness.

Using the channel-hopping technique and under the assumption that the probability of eavesdropping the last message is negligible, reseting the oracle to its random tape is of no use: Apart from the random a the prover receives no new message.

It remains to show that the protocol is witness-hiding. The easiest way to show that is in proofing witness indistinguishability:
As proved in [19], if a protocol is witness indistinguishable and if the witness set contains at least two independent witnesses, then the protocol must be witness hiding. And indeed our protocol has q different witnesses (m_1, m_2) which satisfy $h = g_1^{-m_1} g_2^{-m_2}$, given (p, q, g_1, g_2, l, h). The idea for the witness indistinguishability is as follows: For two different witnesses (m_1, m_2) and (m^*_1, m^*_2) satisfying $h \equiv g_1^{-m_1} g_2^{-m_2} = g_1^{-m^*_1} g_2^{-m^*_2} \mod p$) we show that even an unrestricted attacker A^V (playing the role of a verifier) can not determine which witness was used from a, r_1 and r_2. With choosing $t_1 := r_1 + c(m_1 - m^*_1) \mod q$ and r_2 resp. the following equations hold:

$$x = g_1^{t_1} g_2^{t_2} = g_1^{t^*_1} g_2^{t^*_2}$$
$$t_1 := r_1 + cm_1 = r^*_1 + cm^*_1$$
$$t_2 := r_2 + cm_2 = r^*_2 + cm^*_2$$

And we receive exactly equivalent distributions. The CH-system doesn't affect the witness indistinguishability property because everything used by the prover (s, d) is also calculated by the verifier and depends only on the system parameter and the verifier's random y.

□

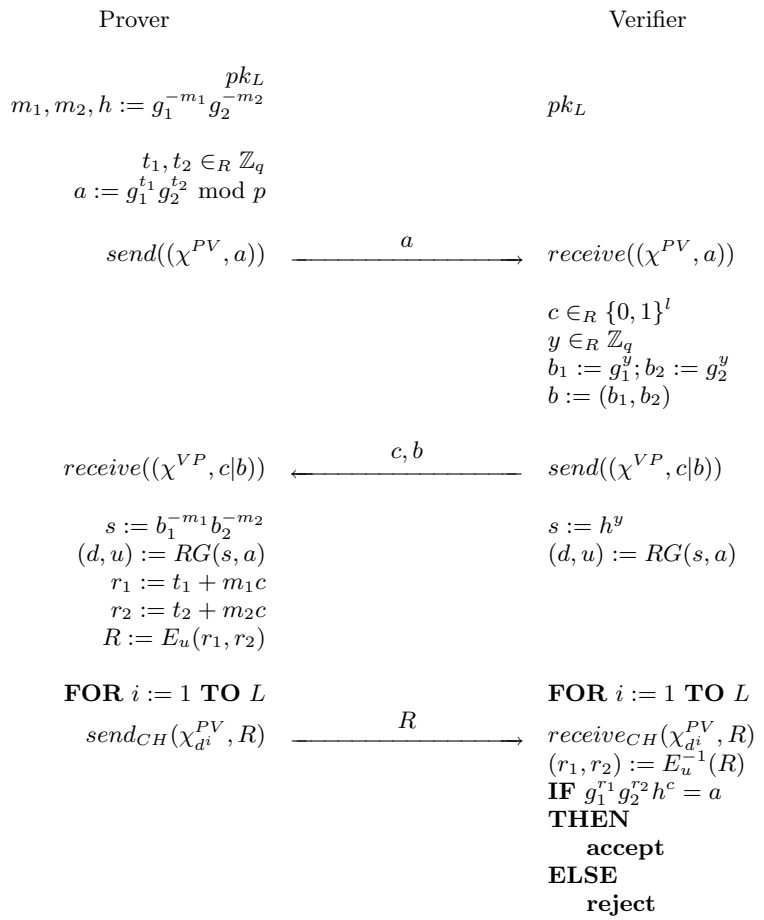
5. TECHNICAL REALIZATION

A possible implementation of a channel hopping system could be realized using Spread Spectrum Frequency Hopping (FHSS) techniques [27].

However, it is not trivial to build such a system that resists attacker who use, e.g., broad-band repeaters.

Possible ideas for making an unrecognized relaying of the whole frequency spectrum harder are:

Figure 2: Proof of Knowledge Based Identification Protocol.



- Using a broad but low spectrum makes it more difficult to build linear working repeater-systems, since the bandwidth of antennas is limited. The FHSS system itself could bypass this limitation by using smart antennas, adapting the antenna according to the selected frequency. However, using low frequencies limits the application of the channel hopping system to slow objects.
- Identifying small objects, e.g., mobile phones or PDAs, makes relaying of large bandwidth very expensive because of the limited size of these devices. Compared to the size of a FHSS system and a smart antenna, the size of a transmitter which relays the whole bandwidth is large.
- The power consumption of a repeater is higher compared to the power consumption of an FHSS system. Since the attacker device (which includes the repeater) should have the same size as the original one, it is difficult for an attacker to realize it, especially with respect to mobile devices which have only a very limited amount of power.
- In some applications, the attacker has to relay the spectrum over vast ranges, e.g., over hundreds of miles in an IFF-system. That requires a significant (and lossless) channel transmission.

We pick up the scenario given in Section 1 to describe how secure identification of a personal mobile device could be realized using the proposed scheme. Basically, we distribute the trust among two different devices. The first one, D_U is the user device to be identified and the second one, D_T is another personalized device identifying the user device D_U. D_T needs only a very simple user interface (e.g., a LED) to indicate a successful identification of D_U, therefore it can be very small. To prevent loss, it could be designed as part of the clothes (wearable), key fob or jewelery. We shortly outline the general device identification protocol: Before users enter security-critical data into device D_U, they invoke the token D_T to identify the device. If identification was successful, this is indicated by the simple user interface of D_T.

Because the identification problem is symmetric (either the user has to identify its device, or the device has to identify its user), the protocol can further be improved. Whenever the device D_U decides (e.g., whenever a security critical input has to be made, frequently, for unlocking, or whatever policy seems to be sufficient), it identifies the token D_T. Only if identification was successful, it allows user access.

The advantages are that the user cannot forget to identify its device and that D_T does not have to have a user interface at all, which makes it cheaper and allows to make it even smaller.

6. CONCLUSION AND OUTLOOK

We showed that, in general, the problem of secure identification of physical objects is not solved by existing cryptographic identification schemes. We argue that adversaries can perform a simple attack, called mafia fraud, to make the verifier of a cryptographic identification scheme to accept a malicious prover. We compared existing solutions to solve the mafia fraud problem and discuss their advantages and disadvantages. Moreover, we propose a new approach based on channel hopping technology. The main improvement of our approach is the use of random channels by a channel hopping system to prevent an adversary from eavesdropping the communication between the participating entities. In opposite to other solutions, our approach additionally provides a fresh and semantically secure key shared between verifier and prover. This is an important requirement in the context of secure bootstrap architectures [3, 4] and to be able to use secure channels after identification, e.g., for secure ad-hoc networks.

We presented concrete identification schemes based on different identification paradigms providing different security properties.

However, there are still open problems which are crucial for realizing the paradigm. Therefore, more efforts have to be done in working on the assumptions related to radio frequency engineering.

7. REFERENCES

[1] A. Alkassar and C. Stüble. Towards secure IFF: preventing mafia fraud attacks. In *MILCOM 2002. 21st Century Military Communications Conference*, volume 2, pages 1139–1144, Anaheim, CA, Oct. 2002. IEEE.

[2] R. J. Anderson. *Security Engineering — A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, 2001.

[3] W. A. Arbaugh, D. J. Farber, and J. M. Smith. Reliable bootstrap architecture. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 65–71, Oakland, CA, May 1997. IEEE Computer Society, Technical Committee on Security and Privacy, IEEE Computer Society Press.

[4] W. A. Arbaugh, A. D. Keromytis, D. J. Farber, and J. M. Smith. Automated recovery in a secure bootstrap process. In *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS '98)*, pages 155–167, San Diego, California, Mar. 1998. Internet Society.

[5] M. Bellare, M. Fischlin, S. Goldwasser, and S. Micali. Identification protocols secure against reset attacks. In B. Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT '2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 493–508, Innsbruck, Austria, 2001. Springer-Verlag, Berlin Germany.

[6] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In V. Ashby, editor, *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pages 62–73, Fairfax, Virginia, Nov. 1993. ACM Press.

[7] M. Bellare and P. Rogaway. Entity authentication and key distribution. In D. R. Stinson, editor, *Advances in Cryptology – CRYPTO '93*, volume 773 of *Lecture Notes in Computer Science*, pages 232–249. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1994.

[8] S. Bengio, G. Brassard, Y. G. Desmedt, C. Goutier, and J.-J. Quisquater. Secure implementation of identification systems. *Journal of Cryptology*, 4(3):175–183, 1991.

[9] T. Beth and Y. Desmedt. Identification tokens — or: Solving the chess grandmaster problem. In A. Menezes and S. Vanstone, editors, *Advances in Cryptology – CRYPTO '90*, volume 537 of *Lecture Notes in Computer Science*, pages 169–176. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1991.

[10] S. Brands and D. Chaum. Distance-bounding protocols. In T. Helleseth, editor, *Advances in Cryptology – EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 344–359. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1994.

[11] D. Chaum, J.-H. Evertse, and J. van de Graaf. An improved protocol for demonstrating possession of discrete logarithms and some generalizations. In D. Chaum and W. L. Price, editors, *Advances in Cryptology – EUROCRYPT '87*, volume 304 of *Lecture Notes in Computer Science*, pages 127–141. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1988.

[12] D. J. Chiang, M. C. Zari, C. S. Anderson, A. F. Zwilling, J. W. Fikes, D. A. Hess, and R. N. Ward. Personnel identification system utilizing low probability of intercept techniques for covert operations. Security Technology, 1996. 30th Annual 1996 International Carnahan Conference, 1996.

[13] J. H. Conway. *On numbers and games*. Academic Press, London, U.K., 1976.

[14] D. E. Denning and P. F. MacDoran. Location-based authentication: Grounding cyberspace for better security. In D. E. Denning and P. J. Denning, editors, *Internet Besieged: Countering Cyberspace Scofflaws*, pages 167–174. ACM Press / Addison-Wesley, New York, 1998. Reprint from Computer Fraud and Security, Elsevier Science, Ltd, February 1996.

[15] Y. Desmedt. Major security problems with the 'unforgeable' (feige)-fiat-shamir proofs of identity and how to overcome them. In *SecuriCom '88*, SEDEP Paris, France, 1988.

[16] D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. *SIAM Journal on Computing*, 30(2):391–437, 2000. A preliminary version appeared in 23rst STOC, 1991.

[17] C. Dwork, M. Naor, and A. Sahai. Concurrent zero-knowledge. 30th Symposium on Theory of Computing (STOC) 1998, ACM, New York 1998, 409-418.

[18] U. Feige, A. Fiat, and A. Shamir. Zero-knowledge

proofs of identity. *Journal of Cryptology*, 1(2):77–94, 1988.

[19] U. Feige and A. Shamir. Witness indistinguishable and witness hiding protocols. In *Proceedings of the 22nd Annual Symposium on Theory of Computing (STOC)*, pages 416–426, Baltimore, MD, USA, May 1990. ACM Press.

[20] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. M. Odlyzko, editor, *Advances in Cryptology – CRYPTO '86*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194, Santa Barbara, CA, USA, 1987. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany.

[21] O. Goldreich. *Foundations of Cryptography*, volume Basic Tools. Cambridge University Press, 2001.

[22] N. Ikram and S. J. Shepherd. A new approach towards secure IFF techniques. In *IEEE Military Communications Conference (MILCOM '98)*, pages 18–21, Boston, Massachusetts, Oct. 1998.

[23] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press series on discrete mathematics and its applications. CRC Press, 1997. ISBN 0-8493-8523-7.

[24] T. Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In E. Brickell, editor, *Advances in Cryptology – CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 31–44. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1993.

[25] B. Pfitzmann, J. Riordan, C. Stüble, M. Waidner, and A. Weber. The PERSEUS system architecture. Technical Report RZ 3335 (#93381), IBM Research Division, Zurich Laboratory, Apr. 2001.

[26] B. Pfitzmann, M. Schunter, and M. Waidner. Cryptographic security of reactive systems. *Electronic Notes in Theoretical Computer Science (ENTCS)*, 32, 2000. Workshop on Secure Architectures and Information Flow, Royal Holloway, University of London, December 1 - 3, 1999.

[27] D. Schilling, R. Pickholz, and L. Milstein. Spread spectrum goes commercial. *IEEE Spectrum*, pages 41–45, Aug. 1990.

[28] C. P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161–174, 1991.

[29] V. Shoup. On formal models for secure key exchange. Research Report RZ 3120 (#93166), IBM Research, Apr. 1999. A revised version 4, dated November 15, 1999, is available from `http://www.shoup.net/papers/`.