On the Relation Between SIM and IND-RoR Security Models for PAKEs

José Becerra, Vincenzo Iovino, Dimiter Ostrev, and Marjan Škrobot
University of Luxembourg,
Interdisciplinary Centre for Security, Reliability and Trust,
6, avenue de la Fonte, L-4364, Esch-sur-Alzette, Luxembourg
{*jose.becerra, vincenzo.iovino, dimiter.ostrev, marjan.skrobot*}*@uni.lu*

Keywords: Security Models, SIM-based Security, IND-based Security, Password Authenticated Key Exchange.

Abstract: Password-based Authenticated Key-Exchange (PAKE) protocols allow users, who need only to share a password, to compute a high-entropy shared session key despite passwords being taken from a dictionary. Security models for PAKE protocols aim to capture the desired security properties that such protocols must satisfy when executed in the presence of an active adversary. They are usually classified into i) indistinguishability-based (IND-based) or ii) simulation-based (SIM-based). The relation between these two security notions is unclear and mentioned as a gap in the literature. In this work, we prove that SIM-BMP security from Boyko et al. (EUROCRYPT 2000) implies IND-RoR security from Abdalla et al. (PKC 2005) and that IND-RoR security is equivalent to a slightly modified version of SIM-BMP security. We also investigate whether IND-RoR security implies (unmodified) SIM-BMP security.

1 Introduction

The Password Authenticated Key Exchange (PAKE) problem asks for two entities, who only share a password, to engage in a conversation so that they agree on a *session key*. The established session key can be used to protect their subsequent communication. PAKE protocols play a key role in today's world as they allow for authenticated key exchange to occur without the use of Public-Key Infrastructure (PKI), by using a human-memorable password instead. Theoretically, they are fascinating, because of their ability to use a weak secret such as a password to produce a strong cryptographic key in a provably secure way over a hostile communications network.

The nature of passwords makes PAKE protocols vulnerable to *dictionary attacks*. In such attacks, an adversary tries to break the security of the protocol by exhaustively enumerating all possible passwords until a guess is correct. This strategy might not be very successful on AKE schemes where the legitimate entities share as long-term secret a high-entropy key. However, in the PAKE setting the long term secrets come from a small set of values, i.e. a dictionary, posing a genuine security threat.

We distinguish between two types of possible dictionary attacks: *offline* and *online* dictionary attacks. In an offline dictionary attack, the adversary uses interaction with the honest parties – or mere eavesdropping – to get information about the password that allows him to launch an exhaustive offline search. In an online dictionary attack, an attacker takes a password from the set of possible passwords, *interacts* with a legitimate party by running the protocol and checks whether the key exchange succeeds for the candidate password or not.

The cryptographic goal when designing PAKE protocols is to ensure that the attacker essentially cannot do better than an online dictionary attack. This goal recognizes that while online dictionary attacks cannot be avoided, offline dictionary attacks can and should be prevented. Numerous PAKE protocols have been designed trying to meet this goal but have later been found to be flawed (Nam et al., 2013; Clarke and Hao, 2014). Consequently, *security models* for PAKE have been devised to get assurance on the claimed security properties by performing a rigorous analysis.

In this work, we consider the provable security approach, where protocols are analyzed in a complexity-theoretic security model, the goal being that no reasonable algorithm can violate security under various hardness assumptions. The complexity-theoretic security models are classified into indistinguishability-based (IND-based) and simulation-based (SIM-based). In the IND-based approach security means that no probabilistic polynomial-time (PTT) adver-

sary can distinguish an established session key *sk* from a random string, i.e. it guarantees semantic security on *sk*. The SIM-based approach defines two worlds: an *ideal world* which is secure by definition and the *real world* which is the real protocol execution against some PPT attacker. In the SIM-based setting, security asks for the indistinguishability between the ideal world and real world executions.

When dealing with formal security modeling of PAKE, the difference between the two previously mentioned approaches, IND and SIM, has practical consequences. It is accepted that IND-based models are easier to work with for protocol designers that wish to prove the security of their protocols. In fact, currently, most of the security proofs for PAKEs are constructed under the IND-based models Find-then-Guess (IND-FtG) from (Bellare et al., 2000) and Real-or-Random (IND-RoR)[1] from (Abdalla et al., 2005). In contrast, constructing security proofs in SIM-based models is considered more challenging. Two SIM-based models for PAKE that have seen wider use are Boyko, MacKenzie and Patel's (BMP) model (Boyko et al., 2000) that is derived from Shoup's SIM-based model for AKE (Shoup, 1999) and the Universal Composability (UC) framework of Canetti et al. (Canetti et al., 2005) that follows UC paradigm of Canetti (Canetti, 2001). While complex for constructing proofs of security, it is fair to recognize that SIM-based security i) offers a more intuitive and natural approach to defining security, ii) it is simpler to describe and interpret the security properties captured by the model, iii) SIM-secure protocols are well suited to accommodate secure composition results, and iv) it is possible to prove security of PAKE protocols even in the case of correlated passwords that may come from arbitrary password distributions.

Figure 1: Known relations between PAKE security definitions.

The known relations between PAKE security definitions are summarized in Figure 1. In particular, to the best of the knowledge of the authors, no work has been done to formally analyze the relation between the IND-RoR and SIM-BMP security notions for PAKE.[2] As we can see in Figure 1, the only existing result that is known to hold between IND and SIM based definitions is the one from (Canetti et al., 2005). There, the authors show that their SIM-UC definition implies the IND-FtG definition from (Bellare et al., 2000).

In practical terms, the lack of comparison results between IND-based and SIM-based models for PAKEs means that the security of PAKE protocols, such as SPEKE,[3] that have been studied in the SIM-BMP simulation model of (Boyko et al., 2000) can not be compared with other PAKE protocols that are secure according to the SIM-UC or IND definitions.

1.1 Our Contribution

In this work our contributions can be summarized as follows:

- We first reconcile the syntactic differences between the IND-RoR and SIM-BMP models for PAKE thus allowing honest comparison between them. More specifically, we slightly modify the initialization procedure of the IND-RoR model (Abdalla et al., 2005) such that it follows the SIM-BMP model.
- We prove that SIM-BMP security implies IND-RoR security and that IND-RoR security is equivalent to a slightly modified version of SIM-BMP security adapted to the model of (Goldreich and Lindell, 2001). We also investigate whether IND-RoR security implies (unmodified) SIM-BMP security.

1.2 Related Work

Authenticated Key Exchange (AKE). The complexity theoretic treatment of security for AKE protocols was initiated by Bellare and Rogaway in 1993 (Bellare and Rogaway, 1993). In their groundbreaking work, they followed the indistinguishability (IND)

[1] IND-RoR is a refinement of IND-FtG model in which the adversary has access to multiple test queries instead of a single one.

[2] The result by Shoup (Shoup, 1999) on the equivalence between IND-FTG model and SIM model for authenticated key exchange with a high-entropy long-term secret does not carry over to the PAKE setting. The reason for this is that there is a non-negligible upper bound on the advantage of the adversary in IND-based security definitions for PAKE. This, in turn, does not admit loose reductions.

[3] The SPEKE protocol (Jablon, 1996) is one of the most well-known PAKE designs. It has been proposed by Jablon in 1996 and proven secure in the SIM-BMP model under the Random Oracle (RO) assumption by MacKenzie (MacKenzie, 2001). SPEKE is practically relevant as it is specified in the ISO/IEC 11770-4 (ISO/IEC 11770-4:2006, 2009) and IEEE P1363.2 (IEEE P1363.2, 2002) standards.

approach to formalize the notion of security for Key Exchange (KE) protocols, using previously established symmetric keys as long-term secrets and considering the realistic scenario of concurrent sessions running on a network under full control of the adversary. In their model, an AKE protocol is secure if, under the allowed adversary actions, the established session key is computationally indistinguishable from a random string. After this initial work, numerous others have appeared studying the cryptographic security for KE protocols following the IND-based approach (Bellare and Rogaway, 1995; Blake-Wilson and Menezes, 1997; Canetti and Krawczyk, 2001; LaMacchia et al., 2007; Cremers, 2011; Brzuska et al., 2011; Jager et al., 2012).

In parallel, the first simulation (SIM) definition for KE was given by Bellare, Canetti and Krawczyk (Bellare et al., 1998). In 1999, Shoup proposed another security model for AKE protocols in the SIM-based setting (Shoup, 1999) and informally compared his model with the one from (Bellare et al., 1998). In the same work, the author gave a sketch of a proof arguing that SIM-security against both *static* and *adaptive* adversaries is equivalent to the corresponding IND-security notions of (Bellare and Rogaway, 1995). Canetti and Krawczyk in (Canetti and Krawczyk, 2002) took SIM definitions further by expanding the composition guarantees of KE from (Shoup, 1999) to arbitrary protocols within the Universal Composability (UC) framework of Canetti (Canetti, 2001).

Password Authenticated Key Exchange (PAKE). The idea of PAKE has been first put forward by Bellovin and Meritt in (Bellovin and Merritt, 1992). Their proposal, the EKE protocol, was the first to show that it is possible to design a password authentication mechanism that can withstand offline dictionary attacks. The SPEKE protocol from Jablon (Jablon, 1996) soon appeared, following a very different design strategy. However, both of these works included only informal security justifications. The first adequate security models for PAKE appeared in (Bellare et al., 2000) and (Boyko et al., 2000) around the same time. Both models were built upon already existing AKE models. Although the SIM-based model from (Boyko et al., 2000) has been used to prove secure several PAKE protocols (PAK (Boyko et al., 2000), RSA-based SNAPI (MacKenzie et al., 2000), and SPEKE (MacKenzie, 2001)), it is the IND-FtG model from (Bellare et al., 2000) that has established itself as the model of choice when analyzing PAKEs. Using the IND-FtG model, Katz et al. (Katz et al., 2001) managed to achieve a breakthrough: they have shown how one can *efficiently* realize PAKE without random oracles, but instead relying on a common reference string (CRS). In more theoretical work, Goldreich and Lindell (Goldreich and Lindell, 2001) proposed a PAKE in the plain model[4] that follows the simulation tradition. A few years later, Abdalla et al. (Abdalla et al., 2005) showed that a stronger model than IND-FtG is necessary when trying to achieve three-party PAKE. Hence, they proposed a new model, known as the IND-RoR model, which is proven to be stronger than the IND-FtG model in the case of PAKE. The IND-RoR model – enriched to handle forward secrecy – is considered the state-of-the-art model and has been used in the analysis of most recent PAKE protocols (Abdalla et al., 2015; Lancrenon et al., 2016). Another model which is prominent in PAKE research is the Universal Composability (UC) framework for PAKE of Canetti et al. (Canetti et al., 2005). For more relevant papers on PAKE, we refer the reader to Pointcheval's survey (Pointcheval, 2012).

1.3 Organization

The rest of the paper is organized as follows: In Section 2 we describe the Real-or-Random model for PAKE due to Abdalla et al. (Abdalla et al., 2005). Next, in Section 3, we introduce simulation-based model for PAKE from Boyko et al. (Boyko et al., 2000). We assume some familiarity with the models and refer to the original publications for a full description. Section 4 examines the relation between the Real-Or-Random model of (Abdalla et al., 2005) and the simulation-based model of Boyko et al. (Boyko et al., 2000). Finally, we conclude the paper in Section 5.

2 The Real or Random Security Model for PAKE

In this section, we recall the so-called Real-or-Random (IND-RoR) security model for 2-party PAKE, but before doing so, we introduce the notation used throughout this paper.

2.1 Notation

We write $d \xleftarrow{\$} D$ for sampling uniformly at random from set D and $|D|$ its cardinality. The output of a probabilistic algorithm A on input x is denoted by

[4] In the plain model, the security of a cryptosystem is proved using only general complexity assumptions and no trusted setup.

$y \leftarrow A(x)$, while $y := A(x,r)$ denotes the (deterministic) output of an algorithm A on input x and fixed random tape r. Adversaries (respectively, challengers) will be denoted $\mathcal{A}$ (resp. $\mathcal{CH}$) in the IND-RoR model and $\mathcal{B}$ (resp. $\mathcal{RM}$) in the SIM model. The directory of passwords is pw, PPT stands for probabilistic polynomial-time and λ is the security parameter. A function $f : \mathbb{N} \to \mathbb{R}_+$ is said to be negligible if it decreases faster than the inverse of any polynomial and the symbol *negl* designates some unspecified negligible function. We write $A \stackrel{c}{\equiv} B$ to denote two computationally indistinguishable distributions.

2.2 Description of the IND-RoR Model

The IND-RoR model of Abdalla et al. (Abdalla et al., 2005) is built upon the Find-then-Guess (IND-FtG) from (Bellare et al., 2000). As in IND-FtG, security in the IND-RoR model is defined by a *game* played between a challenger $\mathcal{CH}$ and adversary $\mathcal{A}$ whose goal is to distinguish *real* session keys from *random* strings. The main difference between the two models is that the adversary – during the security experiment – is allowed to ask *multiple* test queries in the IND-RoR model, while in IND-FtG she is restricted to a single test query.

Note that we will introduce only a minor change to the IND-RoR and the SIM-BMP model in order to allow meaningful comparison between them. Otherwise, the models would be syntactically incomparable. Whenever possible, we prefer to change the SIM-BMP model rather than IND-RoR since the latter is more widespread.

PROTOCOL PARTICIPANTS. Each participant in a two party PAKE protocol is either a client $C \in \mathcal{C}$ or a server $S \in \mathcal{S}$. Let $\mathcal{U} = \mathcal{C} \bigcup \mathcal{S}$ denote the set of all (honest) participants. Additionally, each *initialized* participant U is associated with a unique identifier id_U. During the execution of the protocol, there might be several running instances of each participant. A running instance i of some participant $U \in \mathcal{U}$ is called an *oracle instance* and is denoted by Π^i_U.

LONG-TERM SECRETS. Server S holds a password π for each client C. In the opposite direction, client C holds a password π for each server S. For simplicity let π also denote the function assigning passwords to pair of users. We will refer to $\pi[id_C, id_S]$ as the password shared between client C and server S. Note that $\pi[id_C, id_S] = \pi[id_S, id_C]$, while $\pi[id_S, id_S]$ or $\pi[id_C, id_C]$ are not allowed in the model. The passwords are assumed to be independent and uniformly distributed.

PROTOCOL EXECUTION. Protocol P is an algorithm that describes how participants behave in response to inputs from their environment. Each participant can run P in parallel with different partners, which is modeled by allowing an unlimited number of *instances* of each participant to be created. We assume the presence of an adversary $\mathcal{A}$ who has full control over the network i.e. she entirely controls the communication between legitimate entities. She can enumerate, off-line, the words of the password directory pw.

SECURITY EXPERIMENT IN IND-ROR MODEL. Security in the IND-RoR model is defined via a game played between the challenger $\mathcal{CH}$ and adversary $\mathcal{A}$. At the beginning of the experiment, $\mathcal{CH}$ tosses a coin and sets $b \in \{0,1\}$ outside of $\mathcal{A}$'s view. Then $\mathcal{A}$ is given access to i) endless supply of user instances Π^i_U and ii) oracle queries to control them. Oracle queries are answered by the corresponding Π^i_U according to P. $\mathcal{A}$'s goal is to find out the value of the hidden bit b. Next, we summarize the oracle queries $\mathcal{A}$ can access during the security experiment.

- **initialize user**$(U, id_U, role_U)$. $\mathcal{A}$ assigns the string id_U as identity and $role_U \in \{client, server\}$ to user $U \in \mathcal{U}$, subject to the restriction that id_U has not been already assigned to another user. There are two cases:
  - In case $role_U = client$ we shall simply write C instead of U. Then, for every initialized server $S \in \mathcal{S}$ with id_S, a password is picked uniformly at random from the dictionary and assigned to the corresponding pair of client-server, i.e. $\pi[id_C, id_S] \stackrel{\$}{\leftarrow} pw$.
  - If $role_U = server$ we simply write S instead of U. Then, for every initialized client $C \in \mathcal{C}$ do $\pi[id_C, id_S] \stackrel{\$}{\leftarrow} pw$.
- **initialize user instance**$(U, i, role^i_U, pid^i_U)$. An instance $i \in \mathbb{N}$ of initialized user $U \in \mathcal{U}$ is created and denoted by Π^i_U. It is assigned i) a role $role^i_U \in \{open, connect\}$ and ii) a partner identity pid^i_U corresponding to the *identity* of some user U' that Π^i_U is supposed to communicate with in the future. The following constraint must hold:
  - $role_U$ and $role_{U'}$ are complementary, i.e. $role_U = server$ and $role_{U'} = client$ or the other way around.

  User instances are modeled as state machines with implicit access to the protocol description P and its corresponding password, i.e. some Π^i_U with $pid^i_U = id_{U'}$ is given access to $\pi[U, pid^i_U]$.
- **send** (U, i, m). $\mathcal{A}$ sends message m to user instance Π^i_U. The latter behaves according to protocol description, sends back the response m' to $\mathcal{A}$ (if any) and updates its state as follows:

– continue: Π_U^i is ready to receive another message.
– reject: Π_U^i aborts the protocol execution and sets the session key $sk_U^i = \perp$. This can be due to receiving an unexpected message m.
– accept: Π_U^i holds pid_U^i, session identifier sid_U^i and sk_U^i. However, Π_U^i still expects to receive another message to fulfill the protocol specification.
– terminate: Π_U^i holds pid_U^i, sid_U^i and sk_U^i. It has completed the protocol execution and will not send nor receive any other message.

- **execute** (U, i, U', j). The transcript of the execution is returned to $\mathcal{A}$. It models honest execution of the protocol between Π_U^i and $\Pi_{U'}^j$.
- **test** (U, i). $\mathcal{A}$ asks for the session key of user instance Π_U^i, $\mathcal{CH}$ responds as follows:
  – If $status_U^i \neq terminate$ return $\perp$.
  – If $status_U^i = terminate$, $\mathcal{CH}$ responds using the bit b. If $b = 1$ then $\mathcal{A}$ gets the real sk of Π_U^i, if $b = 0$ she gets a random string $r \xleftarrow{\$} \{0,1\}^{l_{sk}}$, where l_{sk} denotes the length of session keys. To ensure consistency, whenever $b = 0$ the same random string is returned for test queries asked to two *partnered* instances.

Matching Instances. Two user instances, Π_U^i and $\Pi_{U'}^j$, are matching instances if:

- $pid_U^i = id_{U'}$, $pid_{U'}^j = id_U$
- Users have complimentary roles, i.e. one has role *client* and the other has role *server*.
- User instances have complimentary roles, i.e. one instance has the role *open* and the other *connect*.

Partnering. Two matching instances Π_U^i and $\Pi_{U'}^j$ are *partners* if both instances *accept* – each holding pid_U^i, sid_U^i, sk_U^i and $pid_{U'}^j$, $sid_{U'}^j$, $sk_{U'}^j$ respectively – and the following holds:

- $sid_U^i = sid_{U'}^j$ and $sk_U^i = sk_{U'}^j$
- No oracle besides Π_U^i and $\Pi_{U'}^j$ accepts with some $sid' = sid_U^i$, except with negligible probability.

Advantage of the adversary. During the experiment, $\mathcal{A}$ is allowed to ask several test queries directed to different oracle instances Π_U^i in the *terminate* state. All these queries are answered depending on the bit b chosen at the beginning of the experiment with either the real session key if $b = 1$ or a random string otherwise. At the end of the game, $\mathcal{A}$ outputs a bit b' and wins the game if $b' = b$, i.e. if she distinguished real session keys from random strings. The advantage of $\mathcal{A}$ in the IND-RoR security game for protocol P and passwords sampled uniformly at random from dictionary pw is defined as follows:

$$Adv_{P,pw}^{RoR}(\mathcal{A}) := 2 \cdot \Pr(b' = b) - 1. \quad (1)$$

Definition 1. *Protocol P is secure in the IND-RoR sense if for any PPT adversary $\mathcal{A}$:*

$$Adv_{P,pw}^{RoR}(\mathcal{A}) \leq \frac{k \cdot n}{|pw|} + negl(\lambda) \ , \quad (2)$$

where n is an upper bound on the number of sessions initialized by $\mathcal{A}$, $k \in \mathbb{N}$ and λ is the security parameter.

Remark 1. *When using passwords as means of authentication, there is a non-negligible probability of an adversary successfully impersonating an honest user by simply guessing its password. This problem is unavoidable and inherent to PAKE protocols. Consequently the security definition considers a PAKE protocol to be secure if only on-line dictionary attacks are possible i.e. the protocol should not leak any information that allows the adversary to obtain the password in an off-line manner. In the remaining of the paper, we consider the best scenario where $k = 1$ i.e. the adversary can test at most one password per active instance.*

3 Security in Simulation Model

SIM-based security requires the definition of two scenarios: i) an *Ideal World* (*IW*) which describes the key exchange *service* that is meant to be provided and ii) a *Real World* (*RW*) to describe the real interaction between honest protocol participants and an adversary attacking the protocol. The *IW* is designed in such a way that it is secure by definition and follows the desired security properties that a PAKE should satisfy.

As mentioned in (Boyko et al., 2000) and (Canetti et al., 2005), there are two ways to incorporate online dictionary attacks in SIM-based security models:

1. Incorporate the non-negligible probability of an adversary guessing the password into the ideal world, by explicitly allowing the ideal world adversary to verify the guess of a candidate password. Then one defines a protocol to be secure if the real-world execution is computationally indistinguishable from an execution in the ideal world.
2. Do not allow password guessing in the ideal world but relax the requirement of indistinguishability between the real world and ideal world transcripts. One defines a protocol to be secure as one whose

real-world execution is distinguishable from an execution in the ideal world with probability at most $n/|pw| + negl(\lambda)$, where n is the number of active user instances and pw is the dictionary. Keep in mind that we make use of this approach in Section 4 when we prove Theorem 3.

The first approach is considered in (Boyko et al., 2000), (Canetti et al., 2005) and the second is considered in (Goldreich and Lindell, 2001), (Nguyen and Vadhan, 2008).

Next, we describe the simulation model of Boyko et al. (Boyko et al., 2000), which we simply call the SIM-BMP model. Their work is an extension of (Shoup, 1999) to the password setting.

3.1 Ideal World

The ideal world (*IW*) model describes the service that a PAKE aims to provide, i.e. to allow parties to jointly compute a high entropy secret session key, which can be used later in higher level *applications*. In the *IW* there are no messages flowing around the network nor cryptography. The session keys are chosen at random by a trusted party and delivered out-of-band to the honest users.

Formally, the ideal world involves interaction between a trusted entity called ideal world *Ring Master* and an ideal world adversary, denoted by $\mathcal{RM}^*$ and $\mathcal{B}^*$ respectively. The *ring master* is similar to the *challenger* in the IND-RoR experiment. The details of the ideal world execution follow.

PROTOCOL PARTICIPANTS: As defined in the IND-RoR model.

LONG-TERM SECRETS: The SIM-BMP model does not make any assumption on the password distribution. However, to allow a fair comparison to the IND-RoR model, we assume the passwords to be independent and uniformly distributed.

PROTOCOL EXECUTION: There is no protocol execution in the ideal world. The session key of an instance is generated by the $\mathcal{RM}^*$ when $\mathcal{B}^*$ asks that instance the *start session* query. Additionally $\mathcal{B}^*$ is given access to the following oracles:

- **initialize user**$(U, id_U, role_U)$. Identical to that in the IND-RoR model.
  [Transcript:("init. user", $U, role_U$)]
- **initialize user instance**$(U, i, role^i_U, pid^i_U)$. Identical to that in the IND-RoR model.
  [Transcript: ("init. inst.", $U, i, role^i_U, pid^i_U$)]
- **abort user instance** (U, i) Adversary $\mathcal{B}^*$ asks $\mathcal{RM}^*$ to abort user instance Π^i_U. We say then that Π^i_U is *aborted*.
  [Transcript: ("abort. user inst.", U, i)]
- **test instance password** (U, i, π'). For user instance Π^i_U and password guess π', $\mathcal{B}^*$ queries if π' equals $\pi(U, pid^i_U)$. If this is true, the query is called *successful guess on* $\{U, pid^i_U\}$.
  This query can be asked only once per user instance. The user instance must be initialized and not yet engaged in a session, i.e. no start session operation has been performed for that instance. Note that $\mathcal{B}^*$ is allowed to ask a *test instance password* query to an instance that is *aborted*. This query does not leave any records in the transcript.
- **start session**(U, i). $\mathcal{B}^*$ specifies that a session key for user instance Π^i_U must be generated, by specifying one of the three *connection assigments* available:
  - **open for connection from** (U', j). This operation is allowed if: c1) $role^i_U = open$ and user instances Π^i_U and $\Pi^j_{U'}$ are *matching instances*, c2) $\Pi^j_{U'}$ has been *initialized* and not *aborted*, c3) no other instance is *open for connection* from $\Pi^j_{U'}$ and c4) no *test instance password* operation has been performed on Π^i_U. Then $\mathcal{RM}^*$ generates session key sk^i_U at random. Then Π^i_U is said to be *open for connection from* $\Pi^j_{U'}$.
  - **connect to** (U', j). This operation is allowed if: c1) $role^i_U = connect$ and user instances Π^i_U and $\Pi^j_{U'}$ are *matching instances*, c2) $\Pi^j_{U'}$ has been *initialized* and not *aborted*, c3) $\Pi^j_{U'}$ was open for connection from Π^i_U after Π^i_U was initialized and $\Pi^j_{U'}$ is still open for connection and c4) no *test instance password* operation has been performed on Π^i_U. The $\mathcal{RM}^*$ sets $sk^i_U = sk^j_{U'}$ and $\Pi^j_{U'}$ is no longer open for connection.
  - **expose** (U, i, sk). $\mathcal{B}^*$ assigns session key sk to user instance Π^i_U. It requires that there has been a successful test instance password on Π^i_U.

  [Transcript: ("start session", U, i)]
- **application** (f, U, i). The adversary specifies an efficiently computable function f and a user instance Π^i_U for which a session key sk^i_U has already been established. It gets back $f(\{sk^i_U\}, R)$, where R is a global random bit string which user instances are given access to. R is not correlated to the established session keys and usually is referred to as the environment.
  [Transcript: ("application", $f, f(sk^i_U, R)$)]
- **implementation**. This is a do nothing operation. $\mathcal{B}^*$ is allowed to place *implementation* operations without taking any effect in the ideal world. It is needed to allow $\mathcal{B}^*$ to construct *transcripts* that

are equivalent to those in the real world.
[Transcript: ("impl", $cmmt$)]

Transcript. Some of the previously mentioned queries are recorded in a *transcript*. Let IWT^* denote the transcript generated by $\mathcal{B}^*$.

Remark 2. *The SIM-BMP model handles on-line dictionary attacks by introducing the notion of passwords and specifically the* test instance password *query in the IW. This approach allows having ideal world executions which are computationally indistinguishable from real world ones.*

The purpose of running a key exchange protocol is to later use the established session keys in higher-level application protocols, e.g. encryption for secure communication. However, the use of such session keys may leak information about the key to the adversary. The application query models the ability of the adversary to get any information she wishes about the environment and the established session keys. The function f is defined by $\mathcal{B}^*$, the only constraint is that it must be efficiently computable.

3.2 Real World

The real-world (RW) describes the scenario where a PAKE protocol runs. There is a real world Ring Master ($\mathcal{RM}$), whose role is similar to the role of the challenger in the IND-RoR experiment, and a real-world adversary $\mathcal{B}$ who tries to attack the PAKE.

PROTOCOL PARTICIPANTS: Identical to IW.

LONG-TERM SECRETS: Identical to IW.

PROTOCOL EXECUTION: The same as in the IND-RoR model. Also, user instances are defined as state machines with implicit access to id_U, pid_u^i and the corresponding password. The communication between the instances is entirely controlled by $\mathcal{B}$ via the following queries:

- **initialize user**$(U, id_U, role_U)$. Identical to that in the IND-RoR model.
  [Transcript:("init. user", $U, role_U$)]
- **initialize user instance**$(U, i, role_U^i, pid_U^i)$. Identical to that in the IND-RoR model.
  [Transcript: ("init. inst.",$U, i, role_U^i, pid_U^i$)]
- **send** (U, i, m). The same as in the IND-RoR model except that the following is added to the transcript:
  [Transcript: ("impl", "msg", $U, i, m, m', state_U^i$)].
  Additionally, the following record is added to the transcript depending on $state_U^i$.
  If $state_U^i =$ "terminate" add ("start session", U, i).
  If $state_U^i =$ "abort" add ("abort", U, i).
- **application** (f, U, i). The same as in IW.
  [Transcript: ("application", $f, f(sk_U^i, R)$)]

Transcript. Let RWT be the transcript generated by $\mathcal{B}$. This is a sequence of records describing the actions of $\mathcal{B}$ when interacting with the real world protocol. $\mathcal{RM}$ generates $\mathcal{B}$'s random tape and places it in the first record of the transcript.
[Transcript: ("impl","random tape", rt).

Definition 2. *(Simulatability). A protocol is SIM-BMP secure if for every efficient real-world adversary $\mathcal{B}$, there exists an efficient ideal world adversary $\mathcal{B}^*$, such that $RWT \stackrel{c}{\equiv} IWT^*$. Alternatively:*

$$\forall \mathcal{B}\ \exists \mathcal{B}^*\ \forall \mathcal{D}: \ |\Pr[1 \leftarrow \mathcal{D}(RWT)] - \Pr[1 \leftarrow \mathcal{D}(IWT^*)]| \leq negl(\lambda) \quad (3)$$

4 Relations between IND-RoR and SIM-BMP

In this section, we establish the relations between IND-RoR and SIM-BMP security models for PAKE. We start by showing that SIM-BMP security implies IND-RoR security.

Table 1: Correspondence of $\mathcal{A}$'s and $\mathcal{B}$'s queries.

IND-RoR	SIM-BMP
init user	init user
init user instance	init user instance
send	send
execute	send
test	application

Theorem 1. *(SIM-BMP Security $\Rightarrow$ IND-RoR Security). If protocol P is secure in the SIM-BMP model, then P is also secure in the IND-RoR model.*

Proof. We show that if protocol P satisfies SIM-BMP security, then the advantage of any adversary $\mathcal{A}$ in the IND-RoR experiment is bounded by $n/|pw| + negl(\lambda)$, where n is an upper bound on the number of instances created by $\mathcal{A}$.

For simplicity the proof is divided in two parts: i) Building a *real-world* adversary $\mathcal{B}$ from $\mathcal{A}$ and ii) Building a distinguisher $\mathcal{D}$. Details follow:
i) First we construct $\mathcal{B}$ using an $\mathcal{A}$ as a subroutine, where $\mathcal{B}$ uses his own $\mathcal{RM}$ to answer $\mathcal{A}$'s queries. $\mathcal{B}$, using his own queries, can perfectly simulate the IND-RoR experiment to $\mathcal{A}$ (see Table 1). The interaction $\mathcal{RM}$ vs $\mathcal{B}$ produces a transcript RWT. Next we describe the procedure in detail:

- The interaction $\mathcal{RM}$ vs $\mathcal{B}$ starts when the former initializes $\mathcal{B}$ with random tape $rt_{\mathcal{B}}$ - as described in Section 3. Next $\mathcal{B}$, who simulates the challenger $\mathcal{CH}$ in the IND-RoR game, generates a uniformly distributed bit-string $rt_{\mathcal{A}}$ and initializes $\mathcal{A}$ with random tape $rt_{\mathcal{A}}$.
- $\mathcal{B}$ sets $b \xleftarrow{\$} \{0,1\}$ outside $\mathcal{A}$'s view.
- $\mathcal{B}$ interacts with his $\mathcal{RM}$ as follows: When $\mathcal{A}$ makes *initialize user*, *initialize user instance* or *send* queries, $\mathcal{B}$ simply forwards them to his $\mathcal{RM}$ and its response (if any) is forwarded back to $\mathcal{A}$. When $\mathcal{A}$ makes *execute* queries, they are converted into *send* queries appropriately.
- $\mathcal{B}$ answers $\mathcal{A}$'s *test* query using his *application* query and bit b. If $b = 1$ then $\mathcal{B}$ uses his *application* query to reveal sk_U^i, however, if $b = 0$, then $\mathcal{B}$ generates a random string $r \leftarrow \{0,1\}^{l_{sk}}$ and gives it to $\mathcal{A}$. As in the IND-RoR experiment, in order to avoid strategies where $\mathcal{A}$ could trivially win the game, whenever $b = 0$ the same r is returned for test queries asked to two *partnered* instances [5].
- The game continues and $\mathcal{A}$ is allowed to make more queries as she wishes. Eventually, $\mathcal{A}$ outputs her guess b' and the IND-RoR game finishes.
- $\mathcal{B}$ makes an application query and writes in the transcript the string "$b, rt_{\mathcal{A}}$".
- The transcript created is RWT. We recall that SIM-BMP security definition guarantees that $\forall \mathcal{B}\ \exists \mathcal{B}^*$ such that $RWT \stackrel{c}{\equiv} IWT^*$.

ii) Build a PPT distinguisher $\mathcal{D}$ whose aim is to distinguish real-word from ideal-world transcripts. $\mathcal{D}$ gets as input a transcript $t \in \{RWT, IWT^*\}$, which $\mathcal{D}$ uses to initialize a PPT adversary $\mathcal{A}$ and simulate an IND-RoR experiment to $\mathcal{A}$. We show that, if SIM-security holds, $\mathcal{A}$ can not win his IND-RoR experiment with advantage greater than $n/|pw| + negl(\lambda)$. On input some transcript t, $\mathcal{D}$ proceeds as follows:

- Look for the last record of the transcript containing the string "$b, rt_{\mathcal{A}}$".
- $\mathcal{D}$ "simulates" the challenger in the IND-RoR experiment. He initializes $\mathcal{A}$ on random tape $rt_{\mathcal{A}}$. Since $\mathcal{A}$ is given $rt_{\mathcal{A}}$, she behaves (deterministic) the same way as recorded in the transcript t. Every query asked by $\mathcal{A}$ can be answered by $\mathcal{D}$ by just reading t.
- Eventually $\mathcal{A}$ outputs her guess b' and $\mathcal{D}$ proceeds as follows: If $b = b'$ $\mathcal{D}$ outputs "1" and if $b \neq b'$ it outputs "0". Additionally, when a bad event occurs, e.g. $\mathcal{A}$ can not be initialized, or her queries can not be answered by reading t, then $\mathcal{D}$ outputs $\perp$.

$\mathcal{A}$ wins her IND-RoR game whenever she outputs $b' = b$. By construction of $\mathcal{D}$ it holds that:

$$\Pr[1 \leftarrow \mathcal{D}(RWT)] = \Pr[\mathcal{A} \text{ wins } \mid t = RWT]$$

and

$$\Pr[1 \leftarrow \mathcal{D}(IWT^*)] = \Pr[\mathcal{A} \text{ wins } \mid t = IWT^*]$$

From Equation 3 of SIM-BMP security we know the following holds:

$$|\Pr[\mathcal{A} \text{ wins } \mid t = RWT] - \Pr[\mathcal{A} \text{ wins } \mid t = IWT^*]| \leq negl(\lambda) \quad (4)$$

The term $\Pr[\mathcal{A} \text{ wins } \mid t = RWT]$ is actually the probability of $\mathcal{A}$ winning on a perfectly simulated IND-RoR experiment. In order to prove SIM-BMP $\Rightarrow$ IND-RoR we have to show that $\Pr[\mathcal{A} \text{ wins } \mid t = IWT^*] \leq n/(2 * |pw|) + 1/2$.

We proceed to analyze the term $\Pr[\mathcal{A} \text{ wins } \mid t = IWT^*]$. Let γ be the event that a successful *test instance password* query occurs during the execution of $\mathcal{B}^*$ interacting with $\mathcal{RM}^*$. Let β be the complement of γ.

Claim 1: $Pr(b = b' \mid \beta) = 1/2$.

Proof. Given that β occurred, the sk's placed in IWT^* were generated according to the open and connect assignments of the start session query. Therefore, the part of the IWT^* used to answer $\mathcal{A}$'s queries is independent of the hidden bit b so $Pr(b = b' \mid \beta) = 1/2$. ■

Claim 2: $Pr(\gamma) \leq n/|pw|$.

Proof. For a single user instance, the probability of a successful password guess by $\mathcal{B}^*$ is $1/|pw|$. We apply the union bound, and get that if there are at most n instances, $Pr(\gamma) \leq n/|pw|$. ■

Using Claim 1 and Claim 2 we get:

$$\begin{aligned}\Pr[\mathcal{A} \text{ wins} \mid IWT^*] &= \Pr[\beta] \cdot \Pr\left[(b' = b) \mid \beta\right] \\ &\quad + \Pr[\gamma] \cdot \Pr\left[(b' = b) \mid \gamma\right] \\ &\leq \frac{1}{2} + \frac{n}{2 \cdot |pw|} \end{aligned} \quad (5)$$

We combine with Equation 4 and obtain:

$$\Pr[\mathcal{A} \text{ wins} \mid RWT] \leq \frac{1}{2} + \frac{n}{2 \cdot |pw|} + negl(\lambda)$$

We get that, if SIM-BMP-security holds, then $\forall$ PPT $\mathcal{A}$ $Adv^{RoR}_{P,pw}(\mathcal{A}) \leq n/|pw| + negl(\lambda)$, proving that SIM-BMP $\Rightarrow$ IND-RoR. □

[5] In order to achieve sound simulation, we assume that partnering information is publicly computable (Brzuska et al., 2011).

Now we investigate the reverse, i.e. whether IND-RoR security implies SIM-BMP security. We obtain the following result:

Theorem 2. *If P is not SIM-BPM secure, then* $\exists \mathcal{A}$ *s.t.* $Adv^{RoR}_{P,pw}(\mathcal{A},n) > n_A/|pw| + \omega$*, where* n_A *is the number of explicit password guesses of* $\mathcal{A}$ *and* ω *is a non-negligible function of the security parameter.*

Proof. We build $\mathcal{A}$ as the sequential composition of two adversaries: $\mathcal{A}_1$ and $\mathcal{A}_2$. First, $\mathcal{A}$ invokes $\mathcal{A}_1$. $\mathcal{A}_1$ tries a number of online dictionary attacks. If one of these is successful, then $\mathcal{A}$ can win the IND-RoR experiment. If none of the online dictionary attacks is successful, then $\mathcal{A}$ invokes $\mathcal{A}_2$. Next, we describe the details of $\mathcal{A}_1$ and $\mathcal{A}_2$.
i) Build $\mathcal{A}_1$. Let $\mathcal{A}_1$ be an adversary who tries to impersonate user U to user V n_A times. Each time, $\mathcal{A}_1$ chooses a new candidate password and runs the protocol with V. If one of the password guesses is successful, then $\mathcal{A}_1$ can win the IND-RoR experiment. By construction,

$$\Pr[\mathcal{A}_1 \ \ wins] = \frac{n_A}{|pw|} \tag{6}$$

ii) Build $\mathcal{A}_2$. We have assumed that SIM security does not hold. Then $\exists \mathcal{B} \ \ \forall \mathcal{B}^* \ \ \exists \mathcal{D}$ s.t.:

$$|\Pr[1 \leftarrow \mathcal{D}(RWT)] - \Pr[1 \leftarrow \mathcal{D}(IWT^*)]| > \omega \ , \tag{7}$$

where ω is non-negligible term.

Let $\mathcal{A}_2$ be an adversary in the IND-RoR experiment which uses $\mathcal{B}$ and $\mathcal{D}$ as subroutine. The game $\mathcal{A}_2$ vs $\mathcal{CH}$ proceeds as follows:

- At the beginning of the experiment, $\mathcal{CH}$ chooses a bit b at random and outside $\mathcal{A}_2$'s view.
- $\mathcal{A}_2$ uses $\mathcal{B}$ as subroutine and answers $\mathcal{B}$'s queries as follows: When $\mathcal{B}$ asks for initialize user, initialize user instance or send queries, $\mathcal{A}_2$ simply forwards them to her $\mathcal{CH}$ and its response (if any) is forwarded back to $\mathcal{B}$.
- $\mathcal{A}_2$ uses her test query to answer $\mathcal{B}$'s application queries. When $\mathcal{B}$ asks for an application of the efficiently computable function f on sk^i_U and a global random string R, $\mathcal{A}_2$ asks Test(U,i) to her $\mathcal{CH}$, obtains sk^i_U, computes $f(sk^i_U,R)$ and sends the result to $\mathcal{B}$.
- The game continues until $\mathcal{B}$ decides to stop. Let n_B be the number of instances initialized by $\mathcal{B}$. $\mathcal{B}$'s actions produce a transcript t. Based on whether $b=1$ or $b=0$ this is either a real-world or ideal world transcript. Indeed, depending on the bit b, Test(U,i) either returns the *real* session keys or a *random* string. Therefore, when $b=1$, $\mathcal{A}_2$ can perfectly simulate the $\mathcal{RM}$ to $\mathcal{B}$ and the transcript produced is RWT. However, when $b=0$, application queries are computed with random strings, in which case the transcript produced is IWT^*.
- Next, $\mathcal{A}_2$ invokes $\mathcal{D}(t)$ and simply forwards $\mathcal{D}$'s output to $\mathcal{CH}$.

By construction, $\mathcal{A}_2$ wins whenever $\mathcal{D}$ is able to distinguish real-world from ideal-world transcripts. Therefore:

$$\begin{aligned}\Pr[\mathcal{A}_2 \ \ wins] = \Pr[b=1]\cdot\Pr[1 \leftarrow \mathcal{D}(RWT)] \\ + \Pr[b=0]\cdot\Pr[0 \leftarrow \mathcal{D}(IWT^*)] \ ,\end{aligned}$$

which using Equation 7 gives:

$$\Pr[\mathcal{A}_2 \ \ wins] > \frac{1}{2} + \omega \tag{8}$$

We build $\mathcal{A}$ as the sequential composition of $\mathcal{A}_1$ and $\mathcal{A}_2$. It follows that:

$$\begin{aligned}\Pr[\mathcal{A} \ \ wins] = \Pr[\mathcal{A}_1 \ \ wins] + \Pr[\mathcal{A}_2 \ \ wins] \\ - \Pr[\mathcal{A}_1 \ \ wins]\cdot\Pr[\mathcal{A}_2 \ \ wins],\end{aligned}$$

which from Equations 6 and 8 yields:

$$\Pr[\mathcal{A} \ \ wins] > \frac{n_A}{2\cdot pw} + \frac{1}{2} + \omega$$

$$Adv^{RoR}_{P,pw}(\mathcal{A}) > \frac{n_A}{pw} + \omega \ , \tag{9}$$

where ω is a non-negligible function. □

Unfortunately, Theorem 2 is not enough to prove that IND-RoR $\Rightarrow$ SIM-BMP. The reason is that the total number of instances initialized by $\mathcal{A}$ is $n_A + n_B$. Therefore, proving by contradiction that IND-RoR $\Rightarrow$ SIM-BMP would require $Adv^{RoR}_{P,pw}(\mathcal{A}) > (n_A + n_B)/pw + \omega$.

We recall from Section 3 that there are two ways to take account of online dictionary attacks in SIM-based security models for PAKEs:

1. Include a *test instance password* query in IW and require computational indistinguishability of RWT and IWT^*.
2. Do not include a *test instance password* in IW but allow a non-negligible bound on the distinguishability of RWT and IWT^*.

The original SIM-BMP model follows the first style. Now we modify it to follow the second style. We call the modified model SIM-BMP'. The only changes are the following:

1. Remove the *test instance password* query from IW in SIM-BMP.
2. Relax the requirement of indistinguishability between real and ideal world.

SIM-BMP' security. Protocol P is SIM-BMP' secure if for all adversaries $\mathcal{B}$, there exits an *Ideal World* adversary $\mathcal{B}^*$ such that for all distinguishers $\mathcal{D}$:

$$|\Pr[1 \leftarrow \mathcal{D}(RWT)] - \Pr[1 \leftarrow \mathcal{D}(IWT^*)]| \leq \frac{n}{|pw|} + negl(\lambda) \quad (10)$$

Next, we show that IND-RoR security implies SIM-BMP' security.

Theorem 3. *(IND-RoR Security ⇒ SIM-BMP' Security). If protocol P is secure in the IND-RoR model, then P is also secure in the SIM-BMP' model.*

Proof. This is a proof by contradiction and the strategy is similar to the one employed in Theorem 2.

We assume that SIM-BMP' security does not hold. Then $\exists\mathcal{B}\ \forall\mathcal{B}^*\ \exists\mathcal{D}$ s.t.:

$$|\Pr[1 \leftarrow \mathcal{D}(RWT)] - \Pr[1 \leftarrow \mathcal{D}(IWT^*)]| > \frac{n}{|pw|} + \omega \ , \quad (11)$$

where n is an upper bound on the number of sessions initialized and ω is non-negligible function.

Then, we build an adversary $\mathcal{A}$ using $\mathcal{B}$ and $\mathcal{D}$ as subroutines such that $\mathcal{A}$ breaks IND-RoR security. We construct $\mathcal{A}$ from $\mathcal{B}$ and $\mathcal{D}$ in exactly the same way as we built $\mathcal{A}_2$ from $\mathcal{B}$ and $\mathcal{D}$ in the proof of Theorem 2.

Using the same analysis as in the proof of Theorem 2, we get:

$$\Pr[\mathcal{A}\ \ wins] = \Pr[b=1]\cdot\Pr[1 \leftarrow \mathcal{D}(RWT)] + \Pr[b=0]\cdot\Pr[0 \leftarrow \mathcal{D}(IWT^*)] \ ,$$

which using Equation 11 gives:

$$\Pr[\mathcal{A}\ \ wins] = \frac{1}{2} + \frac{n}{2\cdot|pw|} + \omega \ ,$$

And finally from Equation 1:

$$Adv^{RoR}_{P,pw}(\mathcal{A}) > \frac{n}{|pw|} + \omega$$

but ω is not negligible, a contradiction. □

We investigate the reverse, i.e. whether SIM-BMP' security implies IND-RoR security. We obtain the following results:

Theorem 4. *(SIM-BMP' Security ⇒ IND-RoR Security). If protocol P is SIM-BMP' secure, then for all PPT $\mathcal{A}$, $Adv^{RoR}_{P,pw}(\mathcal{A}) \leq 2\cdot n/|pw| + negl(\lambda)$.*

Proof. We follow the same argument as in the proof of Theorem 1 up to Equation 4, which we simply update according to the SIM-BMP' security definition given in Equation 10. Hence:

$$|\Pr[\mathcal{A}\text{ wins } | t = RWT] - \Pr[\mathcal{A}\text{ wins } | t = IWT^*]| \leq \frac{n}{|pw|} + negl(\lambda) \quad (12)$$

It is easy to see that $\Pr[\mathcal{A}\text{ wins } | t = IWT^*] = 1/2$ since $\mathcal{A}$ cannot gain any information about the hidden bit b. However, $\Pr[\mathcal{A}\text{ wins } | t = RWT] = 1/2 + 1/2\cdot Adv^{RoR}_{P,pw}(\mathcal{A})$ as result of $\mathcal{A}$ running on a perfectly simulated IND-RoR experiment. Following Equation 12 we obtain:

$$Adv^{RoR}_{P,pw}(\mathcal{A}) \leq \frac{2\cdot n}{|pw|} + negl(\lambda)$$

□

The guarantee $\forall\mathcal{A}$, $Adv^{RoR}_{P,pw}(\mathcal{A}) \leq \frac{2\cdot n}{|pw|} + negl(\lambda)$ means that protocol P satisfies the definition of IND-RoR security (Definition 1) with parameter $k = 2$. A similar factor of 2 appears in the reduction used in (Abdalla et al., 2005) to prove that IND-RoR security implies IND-FtG security.

Using the results of Theorem 1 and Theorem 3, as well as the known relation IND-RoR ⇒ IND-FtG (Abdalla et al., 2005), we obtain the following corollary:

Corollary 1. *The following relations hold*

- *SIM-BMP Security ⇒ IND-FtG Security*
- *SIM-BMP Security ⇒ SIM-BMP' Security*

The question of whether SIM-BMP' Security ⇒ SIM-BMP Security remains open. Note SIM-BMP' ⇒ SIM-BMP would imply that the three security notions IND-RoR, SIM-BPM and SIM-BMP' are equivalent.

5 Conclusion and Future Work

Although PAKE is a widely studied primitive and found in real-world security protocols, a clear relation between its major security notions (IND and SIM) was missing in the literature. In this work, we aimed at filling this gap. We have summarized the relations obtained in this paper in Figure 2.

During our work on this topic, we identified some delicate definitional issues veiled under the many subtleties of the security notions for PAKE. Among them, we mention that in previous works the advantage of an IND-RoR attacker is formulated according to parameter n, which represents the number of instances

created by such adversary. As nothing else is said about n, we interpret it as the *worst-case* number of instances created by the adversary. Note that such naive definition does not specify or take into account the fact that the adversary's strategy is randomized, and thus n may be a randomized function as well. For instance, an adversary could create a large number of instances with negligible probability making the bound on its advantage grow. Another related issue is about the password correlation between the instances. We leave the quest for a more precise definition that would take into account the above-mentioned remarks for future work.

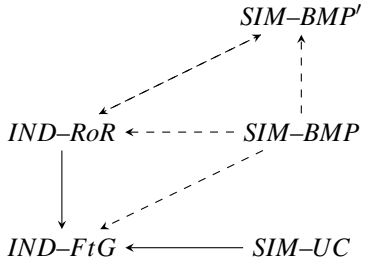

Figure 2: Relation between PAKE security definitions. In dashed arrows are the new results of this paper.

ACKNOWLEDGEMENTS

We are especially grateful to Jean Lancrenon for all his suggestions and fruitful discussions. This work was supported by the Luxembourg National Research Fund (CORE project AToMS and CORE Junior grant no. 11299247).

REFERENCES

Abdalla, M., Benhamouda, F., and MacKenzie, P. (2015). Security of the J-PAKE Password Authenticated Key Exchange Protocol. In *2015 IEEE Symposium on Security and Privacy, SP 2015*, pages 571–587. IEEE Computer Society.

Abdalla, M., Fouque, P., and Pointcheval, D. (2005). Password-Based Authenticated Key Exchange in the Three-Party Setting. In Vaudenay, S., editor, *Public-Key Cryptography – PKC 2005*, volume 3386 of *LNCS*, pages 65–84. Springer.

Bellare, M., Canetti, R., and Krawczyk, H. (1998). A Modular Approach to the Design and Analysis of Authentication and Key Exchange Protocols. In Vitter, J. S., editor, *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, STOC '98*, pages 419–428. ACM.

Bellare, M., Pointcheval, D., and Rogaway, P. (2000). Authenticated Key Exchange Secure Against Dictionary Attacks. In *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 139–155. Springer.

Bellare, M. and Rogaway, P. (1993). Entity Authentication and Key Distribution. In Stinson, D. R., editor, *Advances in Cryptology — CRYPTO 1993*, volume 773 of *LNCS*, pages 232–249. Springer.

Bellare, M. and Rogaway, P. (1995). Provably Secure Session Key Distribution: the three party case. In Leighton, F. T. and Borodin, A., editors, *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing, STOC '95*, pages 57–66. ACM.

Bellovin, S. M. and Merritt, M. (1992). Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks. In *1992 IEEE Symposium on Research in Security and Privacy, SP 1992*, pages 72–84.

Blake-Wilson, S. and Menezes, A. (1997). Entity Authentication and Authenticated Key Transport Protocols Employing Asymmetric Techniques. In Christianson, B., Crispo, B., Lomas, T. M. A., and Roe, M., editors, *Security Protocols, 5th International Workshop*, volume 1361 of *LNCS*, pages 137–158. Springer.

Boyko, V., MacKenzie, P. D., and Patel, S. (2000). Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman. In Preneel, B., editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 156–171. Springer.

Brzuska, C., Fischlin, M., Warinschi, B., and Williams, S. C. (2011). Composability of Bellare-Rogaway Key Exchange Protocols. In Chen, Y., Danezis, G., and Shmatikov, V., editors, *Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS 2011*, pages 51–62. ACM.

Canetti, R. (2001). Universally Composable Security: A New Paradigm for Cryptographic Protocols. In *42nd Annual Symposium on Foundations of Computer Science, FOCS 2001*, pages 136–145. IEEE Computer Society.

Canetti, R., Halevi, S., Katz, J., Lindell, Y., and MacKenzie, P. D. (2005). Universally Composable Password-Based Key Exchange. In Cramer, R., editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 404–421. Springer.

Canetti, R. and Krawczyk, H. (2001). Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. In Pfitzmann, B., editor, *Advances in Cryptology - EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 453–474. Springer.

Canetti, R. and Krawczyk, H. (2002). Universally Composable Notions of Key Exchange and Secure Channels. In Knudsen, L. R., editor, *Advances in Cryptology - EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 337–351. Springer.

Clarke, D. and Hao, F. (2014). Cryptanalysis of the Dragonfly Key Exchange Protocol. *IET Information Security*, 8(6):283–289.

Cremers, C. (2011). Examining Indistinguishability-based Security Models for Key Exchange Protocols: the

case of CK, CK-HMQV, and eCK. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2011*, pages 80–91. ACM.

Goldreich, O. and Lindell, Y. (2001). Session-Key Generation Using Human Passwords Only. In Kilian, J., editor, *Advances in Cryptology — CRYPTO 2001*, volume 2139 of *LNCS*, pages 408–432. Springer.

IEEE P1363.2 (2002). Standard Specifications for Password-Based Public Key Cryptographic Techniques. Standard, IEEE Standards Association, Piscataway, NJ, USA.

ISO/IEC 11770-4:2006 (2009). ISO/IEC 11770-4:2006/cor 1:2009, Information Technology – Security techniques – Key Management – Part 4: Mechanisms Based on Weak Secrets. Standard, International Organization for Standardization, Genève, Switzerland.

Jablon, D. P. (1996). Strong Password-Only Authenticated Key Exchange. *ACM SIGCOMM Computer Communication Review*, 26(5):5–26.

Jager, T., Kohlar, F., Schäge, S., and Schwenk, J. (2012). On the security of TLS-DHE in the standard model. In Safavi-Naini, R. and Canetti, R., editors, *Advances in Cryptology - CRYPTO 2012*, volume 7417 of *LNCS*, pages 273–293. Springer.

Katz, J., Ostrovsky, R., and Yung, M. (2001). Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords. In Pfitzmann, B., editor, *Advances in Cryptology – EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 475–494. Springer.

LaMacchia, B. A., Lauter, K. E., and Mityagin, A. (2007). Stronger Security of Authenticated Key Exchange. In Susilo, W., Liu, J. K., and Mu, Y., editors, *Provable Security, First International Conference, ProvSec 2007*, volume 4784 of *LNCS*, pages 1–16. Springer.

Lancrenon, J., Skrobot, M., and Tang, Q. (2016). Two More Efficient Variants of the J-PAKE Protocol. In Manulis, M., Sadeghi, A., and Schneider, S., editors, *Applied Cryptography and Network Security – ACNS 2016*, volume 9696 of *LNCS*, pages 58–76. Springer.

MacKenzie, P. (2001). On the Security of the SPEKE Password-Authenticated Key Exchange Protocol. Cryptology ePrint Archive, Report 2001/057. http://eprint.iacr.org/2001/057.

MacKenzie, P. D., Patel, S., and Swaminathan, R. (2000). Password-Authenticated Key Exchange Based on RSA. In *Advances in Cryptology - ASIACRYPT 2000*, LNCS, pages 599–613. Springer.

Nam, J., Choo, K. R., Paik, J., and Won, D. (2013). An Offline Dictionary Attack against a Three-Party Key Exchange Protocol. *IACR Cryptology ePrint Archive*, 2013:666. http://eprint.iacr.org/2013/666.

Nguyen, M. and Vadhan, S. P. (2008). Simpler Session-Key Generation from Short Random Passwords. *J. Cryptology*, 21(1):52–96.

Pointcheval, D. (2012). Password-Based Authenticated Key Exchange. In Fischlin, M., Buchmann, J. A., and Manulis, M., editors, *Public Key Cryptography - PKC 2012*, volume 7293 of *LNCS*, pages 390–397. Springer.

Shoup, V. (1999). On Formal Models for Secure Key Exchange. Cryptology ePrint Archive, Report 1999/012. http://eprint.iacr.org/1999/012.