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

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, Forward Secrecy.

Abstract. Password-based Authenticated Key-Exchange (PAKE) protocols allow the establishment of secure communication entirely based on the knowledge of a shared password. Over the last two decades, we have witnessed the debut of a number of prominent security models for PAKE protocols, whose aim is to capture the desired security properties that such protocols must satisfy when executed in the presence of an active adversary. These models are usually classified into i) indistinguishability-based (IND-based) or ii) simulation-based (SIM-based). However, 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. The results obtained also hold when forward secrecy is incorporated into the security models in question.

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 or a pin – 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 a high-entropy key as long-term secret. 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 to meet this goal but have later been found to be flawed [1–3]. 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) adversary 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 [4] and Real-or-Random (IND-RoR)[1] from [5]. 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 [6] that is derived from Shoup's SIM-based model for AKE [7] and the Universal Composability (UC) framework of Canetti et al. [8] that follows the UC paradigm of Canetti [9]. 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.

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

[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.

Fig. 1. Known relations between PAKE security definitions [10].

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 [8]. There, the authors show that their SIM-UC definition implies the IND-FtG definition from [4].

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 [6] can not be compared with other PAKE protocols that are secure according to the SIM-UC or IND definitions.

Forward Secrecy. Commonly referred as Perfect Forward Secrecy (PFS), it is a security property for Authenticated Key-Exchange (AKE) and PAKE protocols. Roughly speaking, it ensures the protection of session keys – negotiated between two honest participants – even if the underlying long-term secret material (passwords for PAKEs) later gets compromised [15]. It is a highly desirable security property specially for PAKEs as unfortunately, there exist in real life different ways in which the adversary could obtain such password information e.g. via phishing attacks a cheated client could reveal his password to some malicious entity or the data base storing the client's password at the server could get compromised resulting in massive password leakage [16–18]. Therefore, it has been explicitly a design goal in relevant PAKEs [19, 20].

The intuition of forward secrecy was first mentioned by Diffie et al. in [15]. It was later formalized and incorporated in AKE [7, 21–23] and PAKE [4, 24] security models. It is indisputable that this formalization enhanced the understanding of forward secrecy by identifying distinct means in which a principal can get compromised and the information revealed to the adversary in such a case. However, it produced a number of definitions and variations on forward secrecy which might make it difficult to tell under which circumstances protocol "P" is *fs-secure*. For example, just in [4] the authors provide three different definitions for forward secrecy.

[2] The result by Shoup [7] 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 [11] 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 [12]. SPEKE is practically relevant as it is specified in the ISO/IEC 11770-4 [13] and IEEE P1363.2 [14] standards.

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 [5] such that it follows the SIM-BMP model.
- We incorporate forward secrecy into the SIM-BMP and IND-RoR security models. We consider only the *weak corruption model* as defined in [4], which is the most used type of forward secrecy.
- 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 [25]. We also investigate whether IND-RoR security implies (unmodified) SIM-BMP security.
- The results in this paper are based on the earlier conference paper [10]. Here, we extend the results obtained earlier and show that they also hold when forward secrecy in the weak corruption model is incorporated into the security models in question.

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 [26]. In their groundbreaking work, they followed the indistinguishability (IND) approach to formalize the notion of security for AKE 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 AKE protocols following the IND-based approach [22, 21, 27–31].

In parallel, the first simulation (SIM) definition for AKE was given by Bellare, Canetti and Krawczyk [32]. In 1999, Shoup proposed another security model for AKE protocols in the SIM-based setting [7] and informally compared his model with the one from [32]. 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 [27]. Canetti and Krawczyk in [33] took SIM definitions further by expanding the composition guarantees of AKE from [7] to arbitrary protocols within the Universal Composability (UC) framework of Canetti [9].

Password Authenticated Key Exchange (PAKE). The idea of PAKE has been first put forward by Bellovin and Meritt in [34]. 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 [11] 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 [4] and [6] around the same time. Both models were built upon already existing AKE models. Although the

SIM-based model from [6] has been used to prove secure several PAKE protocols (PAK [6], RSA-based SNAPI [35], and SPEKE [12]), it is the IND-FtG model from [4] that has established itself as the model of choice when analyzing PAKEs. Using the IND-FtG model, Katz et al. [36] 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 [25] proposed a PAKE in the plain model[4] that follows the simulation tradition. A few years later, Abdalla et al. [5] 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. Recently, Škrobot and Lancrenon [37] have shown that the IND-FtG model may not be enough when looking at composition between PAKEs and arbitrary symmetric key protocols (SKP). However, on the positive side, they have shown that IND-RoR secure PAKE protocols with weak forward secrecy can be safely composed with arbitrary, higher-level SKPs. For these reasons, 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 [38, 39]. Another model which is prominent in PAKE research is the Universal Composability (UC) framework for PAKE of Canetti et al. [8]. This model has been recently extended to treat augmented PAKEs [40] - asymmetric PAKE protocols in which a server holds a hard-to-invert function[5] of the password. For more relevant papers on PAKE, we refer the reader to Pointcheval's survey [41].

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. [5]. Next, in Section 3, we introduce the simulation-based model for PAKE from Boyko et al. [6]. 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 [5] and the simulation-based model of Boyko et al. [6]. Finally, we conclude the paper in Section 5.

2 The Real or Random Security Model for PAKE

The Real-or-Random (IND-RoR) security model for 2-party PAKE was introduced by Abdalla, Fouque and Pointcheval in [5]. In this section, we present an augmented version of the original model that allows us to explicitly incorporate the requirement of forward secrecy. Before we recall the IND-RoR model with forward secrecy, we introduce the notation that will used in the paper.

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

[5] Due to the low entropy of passwords such function can be inverted in practice by applying dictionary attacks.

2.1 Notation

Let S be a set with cardinality $|S|$. We write $s \xleftarrow{\$} S$ to denote sampling uniformly at random from S. The output of a probabilistic algorithm D on input x is denoted by $y \leftarrow D(x)$, while $y := D(x,r)$ denotes the (deterministic) output of an algorithm D on input x and fixed random coins 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 $f : \mathbb{N} \rightarrow \mathbb{R}_+$ 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 with Forward Secrecy

The so called IND-RoR model of Abdalla et al. [5], defines security via a *game* played between a challenger $\mathcal{CH}$ and some adversary $\mathcal{A}$ whose goal is to distinguish *real* session keys from *random* strings. It follows from the Find-then-Guess (IND-FtG) model of [4], however, the IND-RoR model allows $\mathcal{A}$ to ask *multiple* test queries to different instances while the IND-FtG restricts $\mathcal{A}$ to a single test query. This simple yet important change results in the IND-RoR model being strickly stronger than the IND-FtG model for PAKE. This is in contrast with the AKE scenario in which the two models are considered equivalent.

Recall that in [4], several variants of the IND-FtG model are described: these models can be differentiated depending on the type of forward secrecy they are trying to capture. Nevertheless, the original IND-RoR model from [5] does not include a forward secrecy requirement. In this section, we present an augmented version[6] of the original IND-RoR model to incorporate forward secrecy by following [42, 4], which we will simply refer as FS-IND-RoR to differentiate from the original IND-RoR model.

PROTOCOL PARTICIPANTS. Each participant in a two party PAKE protocol is either a client $C \in \mathcal{C}$ or a server S. Let $\mathcal{U} = \mathcal{C} \bigcup S$ 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_U^i.

LONG-TERM SECRETS. Server S holds a password π for each client C, i.e. it holds a vector $L =< \pi_i >_{i \in \mathcal{C}}$. In the opposite direction, client C shares a single password π with 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 $\pi[id_C, id_C]$ is not allowed in the model. The passwords are assumed to be independent and uniformly distributed.

[6] Note that, in addition to the treatment of forward secrecy, we will introduce a minor change to the IND-RoR and the SIM-BMP model to allow for 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 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 FS-IND-ROR MODEL. Security in the IND-RoR model with forward secrecy 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_U^i and ii) oracle queries to control them. Oracle queries are answered by the corresponding Π_U^i 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:
  - If $role_U = server$ we simply write S instead of U. Then, for every initialized client $C \in \mathcal{C}$ with id_C, a password is picked uniformly at random from the dictionary pw and assigned to the corresponding pair of client-server, i.e. $\pi[id_C, id_S] \xleftarrow{\$} pw$.
  - In case $role_U = client$ we shall simply write C instead of U. Then, provided that S has already been initialized with id_S, do $\pi[id_C, id_S] \xleftarrow{\$} pw$.
- **Initialize user instance**$(U, i, role_U^i, pid_U^i)$. An instance $i \in \mathbb{N}$ of initialized user $U \in \mathcal{U}$ is created and denoted by Π_U^i. It is assigned i) a role $role_U^i \in \{open, connect\}$ and ii) a partner identity pid_U^i corresponding to the *identity* of some user U' that Π_U^i 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_U^i with $pid_U^i = id_{U'}$ is given access to $\pi[U, pid_U^i]$.
- **Send** (U, i, m). $\mathcal{A}$ sends message m to user instance Π_U^i. The latter behaves according to the 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 $\Pi_{U'}^j$.
- **Corrupt**(U). $\mathcal{A}$ learns the long-term secret information of some initialized user U. If $role_U = client$, then $\mathcal{A}$ gets π_U. Otherwise, if $role_U = server$, then $\mathcal{A}$ receives $L = < \pi_i >_{i \in \mathcal{C}}$.

– **Test** (U,i). $\mathcal{A}$ asks for the session key of user instance Π_U^i. Provided that $status_U^i = terminate$, $\mathcal{CH}$ responds as follows [7]:
  - If there was a Corrupt (U^*) query -where U^* can be any user- and a Send query directed to Π_U^i before the sk is computed, then $\mathcal{A}$ gets the real sk of Π_U^i. Otherwise:
  - $\mathcal{CH}$ 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 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 FS-IND-RoR security game for protocol P and passwords sampled uniformly at random from dictionary pw is defined as follows:

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

Definition 1. *Protocol P is FS-IND-RoR secure if*

1. *(Completeness) If protocol messages are faithfully transmitted between two matching instances then both instances accept and compute the same key.*
2. *(Bounded Adversary Advantage) For all PPT adversaries $\mathcal{A}$:*

$$Adv_{P,pw}^{FS-RoR}(\mathcal{A}) \leq \frac{n}{|pw|} + negl(\lambda) \ , \tag{2}$$

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

Remark 1. As we mentioned before, different flavors of forward secrecy exist in the literature, e.g. just in [4] the authors provide three particular definitions which could either weaken or strengthen the security guaranteed by the model in case of compromise of long term secret information. While the intuition of forward secrecy and the security guarantee that it aims to provide are understood, it is

[7] This is commonly referred as *freshness* condition.

unclear which definition of forward secrecy is *de facto* the right one for PAKE protocols. Therefore, to be explicit, we consider forward secrecy in the *weak corruption model* described in [4], where corruption of some principal leaks only its password to the adversary, i.e. no internal state is revealed.
In the Client-Server setting, it is reasonable to assume that compromise of the server leaks the whole password data file to the adversary, even for *asymmetric* PAKEs. Thus, the model pessimistically renders every instance, whose session key was negotiated after *someone* got corrupted, as *compromised* and no security is guaranteed. Such a case is formalized in the Test query, which is answered with the *real* session key, i.e. *independently* of the bit b, whenever the previously mentioned scenario occurs. We note that it is possible to fine-tune the model by distinguishing compromise of a server from a client's one, however, it will place new cumbersome conditions to the Test query making the analysis more complex and without gaining some significant improvement.

Remark 2. 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.

3 Security in the Simulation Mode with Forward Secrecy

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.
When dealing with passwords as long-term secret information for authentication, the security model has to acknowledge the non-negligible probability of an adversary guessing the correct password and successfully impersonating an honest user. There are two ways to incorporate this *defect* due to the low entropy of passwords in the SIM-based security model; the first approach is considered in [6, 8] while the second in [25, 43]:

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.

For now we consider only the first approach. We augment the original SIM-BMP model of Boyko et al. [6] to account for scenarios where *forward secrecy* is required. For clarity, we refer to the later simulation model with forward secrecy as FS-SIM-BMP to distinguish from the original one. The inclusion of this security property in the SIM-BMP model allows us to provide a fair comparison to the IND-RoR model with forward secrecy as described in Section 2, otherwise, the models would be incomparable simply because they aim for different security guarantees. We consider forward secrecy in the *weak corruption model* as described in [4, 7] for this task.

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 FS-IND-RoR experiment. The details of the ideal world execution follow.

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

LONG-TERM SECRETS: The FS-SIM-BMP model does not make any assumption on the password distribution. However, to allow a fair comparison to the FS-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 FS-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 FS-IND-RoR model.
  [Transcript: ("init. inst.",U, i, pid_U^i)][8]
- **Abort user instance** (U, i) Adversary $\mathcal{B}^*$ asks $\mathcal{RM}^*$ to abort user instance Π_U^i. We say then that Π_U^i is *aborted.*
  [Transcript: ("abort. user inst.",U, i)]

[8] Note that the original SIM-BMP model [6] also places $role_U^i$ in the transcript, but we have chosen to remove it. This is because in the ideal world, from two partnered instances, the one with the role "open" will always start session first. On the other hand, in the real world, the adversary is free to choose which instance is assigned role "open" and which "connect". Thus, a real world adversary could make an honest execution of a protocol between an instance with role "connect" that terminates first, and an instance with role "open" that terminates second. Such a transcript, which constitutes an honest execution of a protocol, would not be simulatable in the ideal world if the roles "open" and "connect" are placed in the transcript.

– **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.
– **Corrupt** (U). $\mathcal{B}^*$ learns the long-term secret information of some initialized user U. If $role_U = client$, then $\mathcal{B}^*$ gets π_U. Otherwise, if $role_U = server$, then $\mathcal{B}^*$ receives $L =< \pi_i >_{i \in \mathcal{C}}$.
  [Transcript: ("Corrupt", U, π_U)]
– **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 of his choice to user instance Π^i_U. This connection assignment is allowed if at least one of the following conditions hold: i) there has been a successful test instance password on Π^i_U or ii) there was a Corrupt query, directed to any user, before the *start session* operation.

  [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 3. The SIM-BMP model handles on-line dictionary attacks, which are unavoidable and inherent to PAKEs, by introducing the notion of passwords and

specifically the *test instance password* query in the ideal world definition. This approach places the fundamental requirement that an active adversary can test at most one password per protocol execution. In fact, provided that the PAKE in question should be deemed SIM-BMP secure, the test instance password allows the simulator to create ideal world transcripts which are computationally indistinguishable from real world ones.
In a more general sense, the *expose* connection assignment is allowed whenever the adversary could compute by his own the session key shared with some instance Π_U^i, e.g. a successful online dictionary attack or a Corrupt query asked before the connection assignment. This is similar to the freshness condition defined for IND-based models, which prevents the adversary from winning the experiment by *trivial* means.

The purpose of running PAKE protocol is to later use the established session keys in higher-level application protocols, e.g. the construction of secure communication channels is their most natural application. However, partial information about the established session key could potentially be leaked to the adversary through the usage of such keys, e.g. cryptanalysis, side channel attacks, etc. 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 FS-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 FS-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 FS-IND-RoR model.
  [Transcript:("init. user", $U, role_U$)]
- **Initialize user instance**$(U, i, role_U^i, pid_U^i)$. This is identical to that in the FS-IND-RoR model.
  [Transcript: ("init. inst.",U, i, pid_U^i)]
- **Send** (U, i, m). The same as in the FS-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).
- **Corrupt** (U). The same as in IW.
  [Transcript: ("Corrupt",U, π_U)]
- **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. *A protocol is FS-SIM-BMP secure if*

1. *(Completeness) If protocol messages are faithfully transmitted between two matching instances then both instances accept and compute the same key.*
2. *(Simulatability) 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 FS-IND-RoR and FS-SIM-BMP

In this section, we establish the relations between FS-IND-RoR and FS-SIM-BMP security models for PAKEs. The results obtained follow from earlier conference paper [10]. The difference is that in the present work the considered security models incorporate the notion of forward secrecy as security requirement.
We start by showing that FS-SIM-BMP security implies FS-IND-RoR security.

Table 1. Correspondence of $\mathcal{A}$'s and $\mathcal{B}$'s queries. It follows from Table 1 in the earlier conference paper [10], however, in this work we additionally consider the Corrupt query.

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

Theorem 1. *(FS-SIM-BMP Security $\Rightarrow$ FS-IND-RoR Security). For any PAKE protocol P secure in the SIM-BMP model with forward secrecy, P is also secure in the IND-RoR model with forward secrecy.*

Proof. We demonstrate that if protocol P satisfies FS-SIM-BMP security, then the advantage of any adversary $\mathcal{A}$ in the FS-IND-RoR experiment is bounded by $n/|pw| + negl(\lambda)$, where n is an upper bound on the number of sessions initialized by $\mathcal{A}$.
For clarity the proof is divided in two parts which we summarize here:

1. First we build a *real-world* adversary $\mathcal{B}^{\mathcal{A}}$ from $\mathcal{A}$. The motivation is to generate a real-world *transcript* RWT according to the FS-SIM-BMP model but following $\mathcal{A}$'s commands. Additionally, since P is FS-SIM-BMP secure, the simulatability definition guarantees the existence of an ideal-world transcript

IWT^* that is computationally indistinguishable from the RWT. Additionally, we show that one can use the previously generated RWT to instantiate again $\mathcal{A}$ and obtain *identical executions* of the previously simulated experiment to $\mathcal{A}$. The same reasoning applies when initializing $\mathcal{A}$ according to IWT^*.

2. We build a distinguisher $\mathcal{D}^{\mathcal{A}}$ using $\mathcal{A}$ as a subroutine, whose goal is to tell apart RWT from IWT^* transcripts. The distinguisher looks at whether $\mathcal{A}$ wins his security challenge when initialized with the given transcript. From this, we can bound the advantage of $\mathcal{A}$ in the FS-IND-RoR experiment to at most $n/|pw| + negl(\lambda)$.

Concrete details of Part 1 and Part 2 follow:

Part 1. We construct $\mathcal{B}^{\mathcal{A}}$ using an $\mathcal{A}$ as a subroutine, where $\mathcal{B}^{\mathcal{A}}$ uses his own $\mathcal{RM}$ to answer $\mathcal{A}$'s queries. $\mathcal{B}^{\mathcal{A}}$ can perfectly simulate the FS-IND-RoR experiment to $\mathcal{A}$ (see Table 1). The objective is to generate a transcript RWT from the interaction $\mathcal{RM}$ vs $\mathcal{B}^{\mathcal{A}}$. The resulting transcript will be used in the second part of the proof. We detail the construction of $\mathcal{B}^{\mathcal{A}}$, however, a reader familiar with FS-SIM-BMP and FS-IND-RoR security models could simply go to Table 1 and notice that $\mathcal{B}^{\mathcal{A}}$ can *perfectly* simulate the FS-IND-RoR experiment to $\mathcal{A}$.

- The interaction $\mathcal{RM}$ vs $\mathcal{B}^{\mathcal{A}}$ starts when the former initializes $\mathcal{B}^{\mathcal{A}}$ with random tape $rt_{\mathcal{B}}$ - as described in Section 3. Next $\mathcal{B}^{\mathcal{A}}$, who simulates the challenger $\mathcal{CH}$ in the FS-IND-RoR game, generates a uniformly distributed bitstring $rt_{\mathcal{A}}$ and initializes $\mathcal{A}$ with random tape $rt_{\mathcal{A}}$.
- $\mathcal{B}^{\mathcal{A}}$ sets $b \xleftarrow{\$} \{0,1\}$ outside $\mathcal{A}$'s view.
- $\mathcal{B}^{\mathcal{A}}$ uses his $\mathcal{RM}$ to answer $\mathcal{A}$'s queries: When $\mathcal{A}$ makes *Initialize user*, *Initialize user instance* or *Send* queries, $\mathcal{B}^{\mathcal{A}}$ simply forwards them to his $\mathcal{RM}$ and its response (if any) is forwarded back to $\mathcal{A}$. *Execute* queries asked by $\mathcal{A}$ are converted into *Send* queries appropriately. See Table 1.
- $\mathcal{B}^{\mathcal{A}}$ answers $\mathcal{A}$'s *Test* query using his *Application* query and the bit b. If there was a *Corrupt* and a *Send* query, then $\mathcal{B}^{\mathcal{A}}$ uses his *Application* query to reveal sk_U^i. Otherwise, if $b = 1$ then $\mathcal{B}^{\mathcal{A}}$ uses his *Application* query to reveal sk_U^i, however, if $b = 0$, then $\mathcal{B}^{\mathcal{A}}$ generates a random string $r \leftarrow \{0,1\}^{l_{sk}}$ and gives it to $\mathcal{A}$. 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 [9].
- The experiment continues and $\mathcal{A}$ is allowed to make more queries as she wishes. Eventually, $\mathcal{A}$ outputs her guess b' and the FS-IND-RoR game finishes.
- $\mathcal{B}^{\mathcal{A}}$ makes an application query and writes in the transcript the string "$b, rt_{\mathcal{A}}$". For the sake of the proof, it is not necessary to write the bit b' in the transcript.

The real-world transcript created is RWT. Furthermore, the FS-SIM-BMP definition guarantees the existence of a corresponding ideal-world transcript IWT^*, i.e. $\forall \mathcal{B}\ \exists \mathcal{B}^*$ such that $RWT \stackrel{c}{\equiv} IWT^*$.

Remark 4. Given either RWT or IWT^*, it is possible create instances of $\mathcal{A}$ as needed, simulate to $\mathcal{A}$ the FS-IND-RoR experiment and obtain *identical executions* as recorded in the corresponding transcript. The reason is that $\mathcal{A}$ can be

[9] In order to achieve sound simulation, we assume that partnering information is publicly computable [30].

initialized with random tape $rt_{\mathcal{A}}$ contained in the transcript, and then $\mathcal{A}$'s behavior is deterministic and known in advance – given the corresponding transcript –. *Rewinding* the adversary to a *specific* state is a standard proof technique [44]. However, our requirement is simpler since we only need to initialize and run $\mathcal{A}$ from the beginning.

Part 2. We use sequence of games and the previously generated transcript to demonstrate that FS-SIM-BMP Security $\Rightarrow$ FS-IND-RoR Security.
Let G_0 be the experiment where $\mathcal{A}$ is initialized according to the real-world transcript RWT, i.e. a real-world adversary $\mathcal{B}^{\mathcal{A}}$ is simulating the FS-IND-RoR experiment to $\mathcal{A}$. Let S_0 be the event where $\mathcal{A}$ outputs $b' = b$ in G_0. It holds that $\Pr[S_0] = \Pr[\mathcal{A} \text{ wins } \mid t = RWT]$.
Let G_1 be the experiment where $\mathcal{A}$ is initialized according to the ideal-world transcript IWT^*. Let S_1 be the event where $\mathcal{A}$ wins his FS-IND-RoR experiment in G_1; then $\Pr[S_1] = \Pr[\mathcal{A} \text{ wins } \mid t = IWT^*]$.
We first analyze the term $\Pr[\mathcal{A} \text{ wins } \mid t = IWT^*]$. Provided that FS-SIM-BMP security holds, we will then show that $\mathcal{A}$ can not notice the transition from G_0 to G_1, and this will give us a bound on the advantage of $\mathcal{A}$ in the FS-IND-RoR experiment.
Assume for now we are in experiment G_1 and consider how the keys in IWT^* were generated. Let γ be the event that at least one *sk* is generated via *expose* connection assignment as a result of a *test instance password* query that occurs during the execution of $\mathcal{B}^*$ interacting with $\mathcal{RM}^*$, i.e. a successful online dictionary attack. Let β be the complement of γ, i.e. the event that no successful password guess occurred during the interaction of $\mathcal{B}^*$ and $\mathcal{RM}^*$.

Claim 1 $Pr(\gamma) \leq n/|pw|$. [10]

Proof. For a single user instance, by definition of the ideal world, 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, $Pr(\gamma) \leq n/|pw|$. □

Claim 2 $Pr(b = b' \mid \beta) = 1/2$. [10]

Proof. Given than β occurs, the session keys placed in IWT^* were generated either by i) *expose* connection assignment -provided that there was a Corrupt query before the connection assignment- or ii) *open* or *connect* connection assignment. Then, whenever $\mathcal{A}$ makes a Test query to an instance whose session key was generated via case i), the simulator answers with the real *sk* computed at the tested instance, i.e. the answer is independent of the bit b by definition of the FS-IND-RoR experiment. Similarly, whenever $\mathcal{A}$ makes a Test query to an instance whose session key was generated via case ii), the simulator answers with a random string independent of the bit b. Therefore, the view of $\mathcal{A}$ is independent of the hidden bit b so $Pr(b = b' \mid \beta) = 1/2$. □

[10] While these equations looks similar to that of earlier conference paper [10], the interpretation is different. In the present work, the underlying security models incorporate forward secrecy as explicity requirement.

Using Claim 1 and Claim 2 we get:

$$\Pr[\mathcal{A} \text{ wins} \mid t = IWT^*] = \Pr\big[(b' = b) \mid \gamma\big] \cdot \Pr[\gamma] + \Pr\big[(b' = b) \mid \beta\big] \cdot \Pr[\beta]$$

$$\Pr[\mathcal{A} \text{ wins} \mid t = IWT^*] \leq \frac{1}{2} + \frac{n}{2 \cdot |pw|}. \quad [10] \tag{4}$$

Equation 4 expresses the observation that, by construction of the ideal-world, an adversary cannot do better than online dictionary attacks.
Now, we build a PPT algorithm $\mathcal{D}^{\mathcal{A}}$ whose aim is to distinguish real-word from ideal-world transcripts. $\mathcal{D}^{\mathcal{A}}$ gets as input a transcript $t \in \{RWT, IWT^*\}$, and uses it to initialize a PPT adversary $\mathcal{A}$ and simulate a FS-IND-RoR experiment to $\mathcal{A}$. The simulation will be either G_0 or G_1. If SIM-security holds, then $\mathcal{D}^{\mathcal{A}}$ cannot distinguish real world and ideal world transcripts, and so $\mathcal{A}$ cannot win his FS-IND-RoR experiment with advantage greater than $n/|pw| + negl(\lambda)$.
In more details, on input some transcript t, $\mathcal{D}^{\mathcal{A}}$ 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 FS-IND-RoR experiment and 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. $\mathcal{A}$ cannot be initialized, or her queries cannot be answered by reading t, then $\mathcal{D}$ outputs $\perp$.

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

$$\Pr[1 \leftarrow \mathcal{D}(RWT)] = \Pr[S_0]$$

and

$$\Pr[1 \leftarrow \mathcal{D}(IWT^*)] = \Pr[S_1].$$

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

$$|\Pr[1 \leftarrow \mathcal{D}(RWT)] - \Pr[1 \leftarrow \mathcal{D}(IWT^*)]| \leq negl(\lambda). \quad [10] \tag{5}$$

Then it holds that $|\Pr[S0] - \Pr[S_1]| \leq negl(\lambda)$. By definition of G_0 and G_1:

$$|\Pr[\mathcal{A} \text{ wins } \mid t = RWT] - \Pr[\mathcal{A} \text{ wins } \mid t = IWT^*]| \leq negl(\lambda). \quad [10] \tag{6}$$

The term $\Pr[\mathcal{A} \text{ wins } \mid t = RWT]$ is actually the probability of $\mathcal{A}$ winning on a perfectly simulated FS-IND-RoR experiment. We combine with Equation 4 and get:

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

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

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

Theorem 2. *If P is not FS-SIM-BMP secure, then* $\exists \mathcal{A}$ *s.t.* $Adv^{RoR}_{P,pw}(\mathcal{A}) > n_A/|pw| + \omega$*, 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 a FS-IND-RoR adversary $\mathcal{A}^{\mathcal{B}}$, as the sequential composition of two adversaries: $\mathcal{A}_1$ and $\mathcal{A}_2^{\mathcal{B}}$. First, $\mathcal{A}^{\mathcal{B}}$ invokes $\mathcal{A}_1$. $\mathcal{A}_1$ tries a number of online dictionary attacks. If one of these is successful, then $\mathcal{A}^{\mathcal{B}}$ can win the FS-IND-RoR experiment. If none of the online dictionary attacks is successful, then $\mathcal{A}^{\mathcal{B}}$ invokes $\mathcal{A}_2^{\mathcal{B}}$. Next, we describe the details of $\mathcal{A}_1$ and $\mathcal{A}_2^{\mathcal{B}}$.
i) Construction of $\mathcal{A}_1$. Let $\mathcal{A}_1$ be an adversary who tries to masquerade 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,

$$\Pr[\mathcal{A}_1 \ \ wins] = \frac{n_A}{|pw|}.^{10} \tag{7}$$

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

$$|\Pr[1 \leftarrow \mathcal{D}(RWT)] - \Pr[1 \leftarrow \mathcal{D}(IWT^*)]| > \omega \ \ ,^{10} \tag{8}$$

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

- At the beginning of the experiment, $\mathcal{CH}$ chooses a bit b at random and outside $\mathcal{A}_2^{\mathcal{B}}$'s view.
- $\mathcal{A}_2^{\mathcal{B}}$ uses $\mathcal{B}$ as subroutine and answers $\mathcal{B}$'s queries as follows: When $\mathcal{B}$ asks for Initialize user, Initialize user instance, Send or Corrupt queries, $\mathcal{A}_2^{\mathcal{B}}$ simply forwards them to her $\mathcal{CH}$ and its response (if any) is forwarded back to $\mathcal{B}$.
- $\mathcal{A}_2^{\mathcal{B}}$ 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_U^i and a global random string R, $\mathcal{A}_2^{\mathcal{B}}$ asks Test(U,i) to her $\mathcal{CH}$, obtains sk_U^i, computes $f(sk_U^i, R)$ and sends the result to $\mathcal{B}$.

Claim 3 *The transcript produced by* $\mathcal{A}_2^{\mathcal{B}}$ *is either* RWT *or* IWT^*.

Proof. $\mathcal{B}$'s actions produce a transcript t. Consider the following scenario: $\mathcal{B}$ asks an Application query and $\mathcal{A}_2^{\mathcal{B}}$ answers it by asking a Test query to his own challenger. Without loss of generality, let us consider fresh instances, i.e. those where we give credit to the adversary if he answers with $b' = b$: If $b = 1$, $\mathcal{A}_2^{\mathcal{B}}$'s Test queries are answered with real session keys, else if $b = 0$ $\mathcal{A}_2^{\mathcal{B}}$ gets a random string taken from the session key space. Therefore, $\mathcal{A}_2^{\mathcal{B}}$'s answer to $\mathcal{B}$'s application queries is either a function of the real session key or a function of a random string. Looking at the definition of the real and ideal-world transcripts, we conclude that whenever $b = 1$ the transcript generated is real-world while if $b = 0$ the transcript is ideal world. The reason is that in the real-world, the user instances compute their *sk*'s according to the description of the protocol and only such *computed sk*'s are placed transcript. However, in the ideal-world, the session keys placed in the transcript are i) random strings provided that freshness

condition is satisfied or ii) no restriction about sk provided that freshness is not satisfied, i.e. the simulator is given the freedom to specify the session key as he wishes. □

Let $\mathcal{D}$ be the PPT distinguisher whose existence is guaranteed by the negation of FS-SIM-BMP security.[11] Next, $\mathcal{A}_2^{\mathcal{B}}$ invokes $\mathcal{D}(t)$ and simply forwards $\mathcal{D}$'s output to $\mathcal{CH}$. By construction, $\mathcal{A}_2^{\mathcal{B}}$ wins whenever $\mathcal{D}$ is able to distinguish real-world from ideal-world transcripts. Therefore:

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

which using Equation 8 gives:

$$\Pr\left[\mathcal{A}_2^{\mathcal{B}} \ \ wins\right] > \frac{1}{2} + \omega. \ ^{10} \tag{9}$$

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

$$\Pr\left[\mathcal{A}^{\mathcal{B}} \ \ wins\right] = \Pr[\mathcal{A}_1 \ \ wins] + \Pr\left[\mathcal{A}_2^{\mathcal{B}} \ \ wins\right] \ - \Pr[\mathcal{A}_1 \ \ wins]\cdot\Pr\left[\mathcal{A}_2^{\mathcal{B}} \ \ wins\right],$$

which from Equations 7 and 9 yields:

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

$$Adv_{P,pw}^{FS-RoR}(\mathcal{A}^{\mathcal{B}}) > \frac{n_A}{pw} + \omega, \ ^{10} \tag{10}$$

where ω is a non-negligible function. □

Unfortunately, Theorem 2 is not enough to prove that FS-IND-RoR security implies FS-SIM-BMP security. The reason is that the total number of instances initialized by our construction of $\mathcal{A}$ is $n_A + n_B$, where n_A is the number of explicit password guesses of subroutine $\mathcal{A}_1$ and n_B is the number of instances initialized while subroutine $\mathcal{A}_2^{\mathcal{B}}$ is simulating the real world ring master to $\mathcal{B}$. Therefore, proving by contradiction that FS-IND-RoR $\Rightarrow$ FS-SIM-BMP would require $Adv_{P,pw}^{FS-RoR}(\mathcal{A}) > (n_A + n_B)/pw + \omega$.
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 SIM-based model Boyko, MacKenzie and Patel [6] follows the first style. We modify it so it follows the second style. We call the modified model FS-SIM-BMP'. The only changes are the following:

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

[11] Without loss of generality, we can assume $\mathcal{D}$ is more likely to output 1 on a real world than on an ideal world transcript; otherwise, flip the output bit of $\mathcal{D}$.

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

$$|\Pr[1 \leftarrow \mathcal{D}(RWT)] - \Pr[1 \leftarrow \mathcal{D}(IWT^*)]| \leq \frac{n}{|pw|} + negl(\lambda), \quad [10] \tag{11}$$

where n is an upper bound on the number of sessions initialized by $\mathcal{B}$.
Next, we show that FS-IND-RoR security implies FS-SIM-BMP' security.

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

Proof. This is a proof by contradiction and the strategy is similar to the one employed in Theorem 2.
We assume that FS-SIM-BMP' security does not hold. Then $\exists\mathcal{B}\ \forall\mathcal{B}^*\ \exists\mathcal{D}$ s.t.:

$$|\Pr[1 \leftarrow \mathcal{D}(RWT)] - \Pr[1 \leftarrow \mathcal{D}(IWT^*)]| > \frac{n}{|pw|} + \omega, \quad [10] \tag{12}$$

where n is an upper bound on the number of sessions initialized and ω is a non-negligible function.
Then, we build an adversary $\mathcal{A}^{\mathcal{B}}$ using $\mathcal{B}$ and $\mathcal{D}$ as subroutines such that $\mathcal{A}$ breaks FS-IND-RoR security. We construct $\mathcal{A}^{\mathcal{B}}$ from $\mathcal{B}$ and $\mathcal{D}$ in exactly the same way as we built $\mathcal{A}_2^{\mathcal{B}}$ 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:

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

which using Equation 12 gives:

$$\Pr\left[\mathcal{A}^{\mathcal{B}}\ \ wins\right] > \frac{1}{2} + \frac{n}{2 \cdot |pw|} + \omega\ ,$$

And finally from Equation 1:

$$Adv_{P,pw}^{FS-RoR}(\mathcal{A}^{\mathcal{B}}) > \frac{n}{|pw|} + \omega, \quad [10]$$

but ω is not negligible, a contradiction. □

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

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

Proof. We follow the same argument as in the proof of Theorem 1 up to Equation 5, which we simply update according to the FS-SIM-BMP' security definition given in Equation 11. Hence:

$$|\Pr[\mathcal{A} \text{ wins } | t = RWT] - \Pr[\mathcal{A} \text{ wins } | t = IWT^*]| \leq \frac{n}{|pw|} + negl(\lambda). \quad [10] \tag{13}$$

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, $\Pr[\mathcal{A} \text{ wins } | t = RWT] = 1/2 + 1/2 \cdot Adv^{FS-RoR}_{P,pw}(\mathcal{A})$ as result of $\mathcal{A}$ running on a perfectly simulated FS-IND-RoR experiment. Following Equation 13 we obtain:

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

□

The guarantee that $\forall \mathcal{A}, Adv^{FS-RoR}_{P,pw}(\mathcal{A}) \leq 2 \cdot n/|pw| + negl(\lambda)$ means that protocol P satisfies the definition of FS-IND-RoR security (Definition 1) with a degradation factor $c = 2$. A similar constant factor appears in the reduction used in [5] to prove that IND-RoR security implies IND-FtG security.
Using the results of Theorem 1 and Theorem 3 from [10], as well as the known relation IND-RoR ⇒ IND-FtG [5], 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 that SIM-BMP' ⇒ SIM-BMP would imply that the three security notions IND-RoR, SIM-BPM and SIM-BMP' are equivalent. A similar reasoning can be applied when considering forward secrecy in the aforementioned security models.

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 work 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. We recall what we consider the most relevant:

- In IND-based models [4, 5] the possible states in which a user instance could be are continue, reject, accept and terminate. Roughly speaking, an instance is in *accept* state whenever it has computed the *sk* but is still waiting to receive another message – typically a confirmation code – to fulfill the protocol specification, while an instance in *terminate* state means that it has computed the *sk*, has finished the protocol execution and is not sending nor receiving any other message. Particularly in the IND-FtG model, a Reveal query can be asked to instances in *accept* state while a Test query can only be directed to instances in *terminate* state. The aforementioned distinction between accept and terminate states does not exist in SIM-based models due to how the ideal world is modeled. The idea is the following:
  - In the SIM-BMP model, the Application query models the leakage of session keys in higher level protocols. The implicit requirement is that the corresponding user instance has *terminated* his protocol execution, which is modeled in the Ideal-World via connection assignments.

- In IND-FtG model, the Reveal query models i) the leakage of session keys in higher level protocols and ii) leakage of session keys before the protocol is finished, i.e. *accept* state.

The aforementioned peculiarity is specially relevant for Corollary 1. In order for the implication SIM-BMP $\Rightarrow$ IND-FtG to hold, we require the Reveal (U,i) query in the IND-FtG model to be legitimate only if the instance Π_U^i is in *terminate* state. It might be a minor difference between IND-based and SIM-based models, yet we consider it is worth mentioning, specially because it is generally assumed that SIM-based security definitions are stronger than their corresponding IND-based ones. However, as we have just explained, there are technicalities that need to be addressed when formally stating the relation between the security models.

– A more remarkable difference between IND and SIM models for PAKEs is how online dictionary attacks are captured in the security model. In IND-base models, the advantage of an adversary is formulated according to parameter n, which represents the number of active instances created by the adversary in question. Note that such a 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. The difference between models with an explicit formulation of a non-negligible bound on the advantage and models without such an explicit formulation seems to be related to the difficulty in proving IND-RoR $\Rightarrow$ SIM-BMP. Another related issue is about the password distribution and the correlation of passwords between users. We leave the quest for a more precise definition that would take into account the above-mentioned remarks for future work.
– The SIM-BMP model offers a more meaningful security definition by better capturing the capabilities of an attacker against a PAKE protocol, for instance online dictionary attacks. Additionally, the SIM-BMP model does not place any artificial constraints on the passwords distribution, whereas the IND-RoR requires the passwords to be uniformly distributed and independent. The last requirement might be difficult to satisfy in real scenarios. In particular, it is known that certain passwords are more likely to be selected than others and that users tend to choose similar passwords when connecting to different services.

Finally, we demonstrated that the results obtained in [10] are still satisfied when the corresponding security models incorporate forward secrecy as required security property.

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).

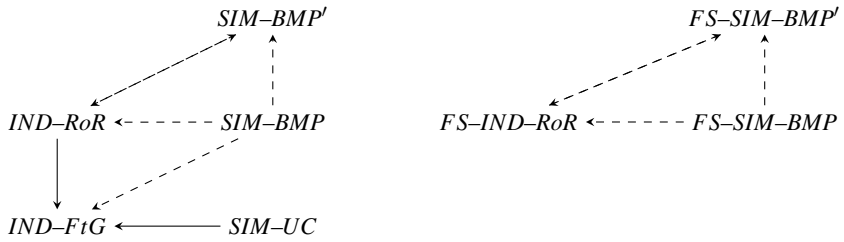

Fig. 2. Relation between PAKE security definitions. In dashed arrows are the results of i) this paper and ii) earlier conference paper [10].

References

1. Nam, J., Choo, K.R., Paik, J., Won, D.: An Offline Dictionary Attack against a Three-Party Key Exchange Protocol. IACR Cryptology ePrint Archive **2013** (2013) 666 http://eprint.iacr.org/2013/666.
2. Clarke, D., Hao, F.: Cryptanalysis of the Dragonfly Key Exchange Protocol. IET Information Security **8**(6) (2014) 283–289
3. Becerra, J., Šala, P., Škrobot, M.: An Offline Dictionary Attack against zkPAKE Protocol. Cryptology ePrint Archive, Report 2017/961 (2017) https://eprint.iacr.org/2017/961.
4. Bellare, M., Pointcheval, D., Rogaway, P.: Authenticated Key Exchange Secure Against Dictionary Attacks. In: Advances in Cryptology – EUROCRYPT 2000. Volume 1807 of LNCS., Springer (2000) 139–155
5. Abdalla, M., Fouque, P., Pointcheval, D.: Password-Based Authenticated Key Exchange in the Three-Party Setting. In Vaudenay, S., ed.: Public-Key Cryptography – PKC 2005. Volume 3386 of LNCS., Springer (2005) 65–84
6. Boyko, V., MacKenzie, P.D., Patel, S.: Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman. In Preneel, B., ed.: Advances in Cryptology – EUROCRYPT 2000. Volume 1807 of LNCS., Springer (2000) 156–171
7. Shoup, V.: On Formal Models for Secure Key Exchange. Cryptology ePrint Archive, Report 1999/012 (1999) http://eprint.iacr.org/1999/012.
8. Canetti, R., Halevi, S., Katz, J., Lindell, Y., MacKenzie, P.D.: Universally Composable Password-Based Key Exchange. In Cramer, R., ed.: Advances in Cryptology – EUROCRYPT 2005. Volume 3494 of LNCS., Springer (2005) 404–421
9. Canetti, R.: Universally Composable Security: A New Paradigm for Cryptographic Protocols. In: 42nd Annual Symposium on Foundations of Computer Science, FOCS 2001, IEEE Computer Society (2001) 136–145
10. Lopez Becerra, J.M., Iovino, V., Ostrev, D., Skrobot, M.: On the relation between sim and ind-ror security models for pakes. In: Proceedings of the International Conference on Security and Cryptography, SCITEPRESS (2017)
11. Jablon, D.P.: Strong Password-Only Authenticated Key Exchange. ACM SIGCOMM Computer Communication Review **26**(5) (1996) 5–26
12. MacKenzie, P.: On the Security of the SPEKE Password-Authenticated Key Exchange Protocol. Cryptology ePrint Archive, Report 2001/057 (2001) http://eprint.iacr.org/2001/057.

13. : 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 (2009)
14. : Standard Specifications for Password-Based Public Key Cryptographic Techniques. Standard, IEEE Standards Association, NJ, USA (2002)
15. Diffie, W., Van Oorschot, P.C., Wiener, M.J.: Authentication and authenticated key exchanges. Designs, Codes and Cryptography **2**(2) (Jun 1992) 107–125
16. Cameron, D.: Over 560 million passwords discovered in anonymous online database. `https://bit.ly/2vgJqli` (2017)
17. Perlroth, N., Gelles, D.: Russian hackers amass over a billion internet passwords. `https://nyti.ms/2Apak05` (2014)
18. Ian, P.: Linkedin confirms account passwords hacked. `https://bit.ly/2v2qjMh` (2012)
19. Hao, F., Ryan, P.: J-PAKE: Authenticated Key Exchange without PKI. Transactions on Computational Science **11** (2010) 192–206
20. MacKenzie, P.: The PAK Suite: Protocols for Password-Authenticated Key Exchange. DIMACS Technical Report 2002-46 (2002)
21. LaMacchia, B.A., Lauter, K.E., Mityagin, A.: Stronger Security of Authenticated Key Exchange. In Susilo, W., Liu, J.K., Mu, Y., eds.: Provable Security, First International Conference, ProvSec 2007. Volume 4784 of LNCS., Springer (2007) 1–16
22. Canetti, R., Krawczyk, H.: Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. In Pfitzmann, B., ed.: Advances in Cryptology - EUROCRYPT 2001. Volume 2045 of LNCS., Springer (2001)
23. Krawczyk, H.: Hmqv: A high-performance secure diffie-hellman protocol. In Shoup, V., ed.: Advances in Cryptology – CRYPTO 2005, Berlin, Heidelberg, Springer Berlin Heidelberg (2005) 546–566
24. Katz, J., Ostrovsky, R., Yung, M.: Forward Secrecy in Password-Only Key Exchange Protocols. In Cimato, S., Galdi, C., Persiano, G., eds.: Security in Communication Networks – SCN 2002. Volume 2576 of LNCS., Springer (2002) 29–44
25. Goldreich, O., Lindell, Y.: Session-Key Generation Using Human Passwords Only. In Kilian, J., ed.: Advances in Cryptology — CRYPTO 2001. Volume 2139 of LNCS. Springer (2001) 408–432
26. Bellare, M., Rogaway, P.: Entity Authentication and Key Distribution. In Stinson, D.R., ed.: Advances in Cryptology — CRYPTO 1993. Volume 773 of LNCS., Springer (1993) 232–249
27. Bellare, M., Rogaway, P.: Provably Secure Session Key Distribution: the three party case. In Leighton, F.T., Borodin, A., eds.: Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing, STOC '95, ACM (1995) 57–66
28. Blake-Wilson, S., Menezes, A.: Entity Authentication and Authenticated Key Transport Protocols Employing Asymmetric Techniques. In Christianson, B., Crispo, B., Lomas, T.M.A., Roe, M., eds.: Security Protocols, 5th International Workshop. Volume 1361 of LNCS., Springer (1997) 137–158
29. Cremers, C.: 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, ACM (2011) 80–91

30. Brzuska, C., Fischlin, M., Warinschi, B., Williams, S.C.: Composability of Bellare-Rogaway Key Exchange Protocols. In Chen, Y., Danezis, G., Shmatikov, V., eds.: Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS 2011, ACM (2011) 51–62
31. Jager, T., Kohlar, F., Schäge, S., Schwenk, J.: On the security of TLS-DHE in the standard model. In Safavi-Naini, R., Canetti, R., eds.: Advances in Cryptology - CRYPTO 2012. Volume 7417 of LNCS., Springer (2012)
32. Bellare, M., Canetti, R., Krawczyk, H.: A Modular Approach to the Design and Analysis of Authentication and Key Exchange Protocols. In Vitter, J.S., ed.: Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, STOC '98, ACM (1998) 419–428
33. Canetti, R., Krawczyk, H.: Universally Composable Notions of Key Exchange and Secure Channels. In Knudsen, L.R., ed.: Advances in Cryptology - EUROCRYPT 2002. Volume 2332 of LNCS., Springer (2002) 337–351
34. Bellovin, S.M., Merritt, M.: Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks. In: 1992 IEEE Symposium on Research in Security and Privacy, SP 1992. (1992) 72–84
35. MacKenzie, P.D., Patel, S., Swaminathan, R.: Password-Authenticated Key Exchange Based on RSA. In: Advances in Cryptology - ASIACRYPT 2000. LNCS, Springer (2000) 599–613
36. Katz, J., Ostrovsky, R., Yung, M.: Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords. In Pfitzmann, B., ed.: Advances in Cryptology – EUROCRYPT 2001. Volume 2045 of LNCS., Springer (2001) 475–494
37. Škrobot, M., Lancrenon, J.: On Composability of Game-based Password Authenticated Key Exchange. In Piessens, F., Smith, M., eds.: 3rd IEEE European Symposium on Security and Privacy — EuroS&P 2018, IEEE (2018)
38. Abdalla, M., Benhamouda, F., MacKenzie, P.: Security of the J-PAKE Password Authenticated Key Exchange Protocol. In: 2015 IEEE Symposium on Security and Privacy, SP 2015, IEEE Computer Society (2015) 571–587
39. Lancrenon, J., Skrobot, M., Tang, Q.: Two More Efficient Variants of the J-PAKE Protocol. In Manulis, M., Sadeghi, A., Schneider, S., eds.: Applied Cryptography and Network Security – ACNS 2016. Volume 9696 of LNCS., Springer (2016) 58–76
40. Jarecki, S., Krawczyk, H., Xu, J.: OPAQUE: An Asymmetric PAKE Protocol Secure Against Pre-Computation Attacks. In Dunkelman, O., ed.: Advances in Cryptology – EUROCRYPT 2018. LNCS, Springer (2018)
41. Pointcheval, D.: Password-Based Authenticated Key Exchange. In Fischlin, M., Buchmann, J.A., Manulis, M., eds.: Public Key Cryptography - PKC 2012. Volume 7293 of LNCS., Springer (2012) 390–397
42. Kunz-Jacques, S., Pointcheval, D.: About the security of mti/c0 and mqv. In De Prisco, R., Yung, M., eds.: Security and Cryptography for Networks, Berlin, Heidelberg, Springer Berlin Heidelberg (2006) 156–172
43. Nguyen, M., Vadhan, S.P.: Simpler Session-Key Generation from Short Random Passwords. J. Cryptology **21**(1) (2008) 52–96
44. Canetti, R., Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T.: Adaptive security for threshold cryptosystems. In Wiener, M., ed.: Advances in Cryptology — CRYPTO' 99, Springer Berlin Heidelberg (1999) 98–116