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

José Becerra, Marjan Skrobot, and Vincenzo Iovino

University of Luxembourg
{jose.becerra, marjan.skrobot, vincenzo.iovino}@uni.lu

Abstract. 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 the SIM-based model of Boyko, Mackenzie and Patel [3] and the IND-based model of Abdalla, Fouque and Pointcheval [1] are equivalent, in the sense that a protocol proven secure in one model is also secure in the other model.

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

1 Introduction

The Password Authenticated Key Exchange (PAKE) problem asks for two entities, who only share a password, to engage on a conversation so that they agree on a *session key*. The established session key can be used to protect their subsequent communication. PAKE's 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, by using instead a human memorable password. Theoretically they are extremely interesting, because of their ability to use a weak secret to produce a strong one 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 simply brute forcing all possible combinations of passwords. One must keep in mind that *on-line* dictionary attacks cannot be entirely prevented in PAKE protocols. An attacker could enumerate (off-line) the words in the directory being likely to be passwords. Then simply take a password at random, *interact* with a legitimate party by running the protocol and check whether the key exchange succeeds for the candidate password or not. The cryptographic goal, when defining security for PAKE protocols is to ensure that the attacker essentially cannot do better than this trivial strategy, which implies resistance to *off-line* dictionary attacks.

We consider the provable secure 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. These complexity-theoretic security models are classified into indistinguishability based (IND-based) and simulation-based (SIM-based). Roughly speaking, in the IND-based approach security means that no computationally bounded adversary can distinguish an established session key *sk* from a random string. The SIM-based approach defines two worlds: an *ideal world* which is secure by definition and a *real world* which is the real protocol execution against some computationally bounded attacker. In the SIM-based setting, security asks for the computational indistinguishability between ideal world and real world executions.

The first IND-base security model for PAKEs was proposed by Bellare, Pointcheval and Rogaway in 2000 [2]. They consider that for a good PAKE protocol, the chances of an adversary defeating the protocol goal should depend on how much she interacts with the protocol participants rather on her off-line computing power. We will refer to this model as IND-FtG model. In 2005 Abdalla, Fouque and Pointcheval proposed a security model for PAKE [1] which is usually known as the IND-RoR model. It is built upon IND-FtG model. In [1] the authors proved that model the IND-RoR model is strictly stronger than the IND-FtG model.

Boyko, Mackenzie and Patel proposed a SIM-based security model for PAKEs in 2000 [3]. Their work is an extension of Shoup's security notion for Authenticated Key Exchange (AKE) protocols [5].

Contributions: While the equivalence between SIM and IND models for AKEs is shown in [5], there is no work on the relation between these security notions for PAKEs. In fact it is mentioned as a gap in [1] and [4]. In this work, we fill the gap by proving the equivalence between the SIM model of Boyko, MacKenzie and Patel [3] and the IND-RoR model of Abdalla, Fouque and Pointcheval [1].

References

1. M. Abdalla, P.-A. Fouque, and D. Pointcheval. Password-based authenticated key exchange in the three-party setting. volume 3386 of *Lecture Notes in Computer Science*, pages 65–84. Springer, 2005.
2. M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. EUROCRYPT'00, pages 139–155, Berlin, Heidelberg, 2000. Springer-Verlag.
3. V. Boyko, P. MacKenzie, and S. Patel. Provably secure password-authenticated key exchange using diffie-hellman. EUROCRYPT'00, pages 156–171, Berlin, Heidelberg, 2000. Springer-Verlag.
4. P. MacKenzie. The pak suite: Protocols for password-authenticated key exchange. In *IEEE P1363.2*, 2002.
5. V. Shoup. On formal models for secure key exchange. *IACR Cryptology ePrint Archive*, 1999:12, 1999.