Information Sciences xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Strongly secure identity-based authenticated key agreement protocols without bilinear pairings

Q1 Liang Ni[a,b,*], Gongliang Chen[b], Jianhua Li[b], Yanyan Hao[c]

[a] *School of Computer Science, Zhongyuan University of Technology, 41 Zhongyuan Road (M), Zhengzhou 450007, PR China*
[b] *School of Information Security Engineering, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai 200240, PR China*
[c] *Experiment Management Center, Zhongzhou University, Zhengzhou 450044, PR China*

ARTICLE INFO

Article history:
Received 25 September 2010
Revised 5 December 2015
Accepted 15 May 2016
Available online xxx

Keywords:
Authenticated key agreement
Identity-based cryptography
Provable security
Diffie–Hellman assumption
The extended Canetti–Krawczyk model

ABSTRACT

In this paper, we present two strongly secure pairing-free identity-based (ID-based) two-party authenticated key agreement (AKA) protocols achieving implicit authentication, which are proven secure in the extended Canetti–Krawczyk (eCK) model. The proposals can offer provable security against both passive and active adversaries in the random oracle model. Our schemes capture all basic desirable security properties including key-compromise impersonation resilience, ephemeral secrets reveal resistance, (weak) perfect forward secrecy and master key forward secrecy etc. We show the security of one of these proposals can be reduced to the standard computational Diffie–Hellman assumption, and the security of the other relies on the gap Diffie–Hellman assumption while having a lower computational overhead. Currently, there are few pairing-free ID-based AKA protocols that are provably secure in such strong security models as the eCK model. Our schemes can provide strong security assurances and in the meanwhile achieve a good computational efficiency. Compared with previous related schemes, our protocols have advantages over them in security, efficiency or both.

1. Introduction

Key agreement (KA) is a cryptographic primitive, which plays an important role in secure communications and networks. By a KA protocol, two or more parties can generate a shared session key by making use of their long-term keys and ephemeral messages exchanged over an open network. The shared secret session key is then used for secure communication. Authenticated key agreement (AKA) protocols not only allow parties to compute the shared session key but also ensure the authenticity of the involved parties [6]. In a traditional public key infrastructure (PKI) based KA setting, where a trusted third party called the Certificate Authority (CA) issues public key certificates for registered users, each party needs to obtain a certificate from the CA, extract the public key, check certificate chains and finally apply a KA protocol to generate a shared secret. Such a process is tedious. Different from this traditional cryptographic setting based on the PKI, in the identity-based (ID-based) cryptographic setting [28] a user's unique identifier (i.e., his unique identity string) serves as the user's public key; each user's private key is generated by a trusted Key Generation Center (KGC) and acts as the user's implicit certificate. Although such an implicit certificate is known only to the user and the KGC, its validity can be verified publicly. Thereby

Q2 [*] Corresponding author at: School of Computer Science, Zhongyuan University of Technology, 41 Zhongyuan Road (M), Zhengzhou 450007, PR China. Tel.: +86 371 67698742; fax: +86 371 67698742.
E-mail address: niliang402@126.com, niliang402@hotmail.com, 1165060759@qq.com (L. Ni).

http://dx.doi.org/10.1016/j.ins.2016.05.015
0020-0255/© 2016 Elsevier Inc. All rights reserved.

the need for a public key certificate is removed. This avoids the requirement of an expensive PKI and greatly simplifies the management of public keys in cryptosystems.

The security analysis of an AKA protocol should be performed with a rigorous formal proof before it is deployed. Since Bellare and Rogaway [3] proposed the first formal security model for authentication and key distribution, there have been several extensions to this model [4,5,8]. Among them, the Canetti–Krawczyk (CK) model [8] is regarded as possibly promising one. Choo et al. [14] compared the most commonly used security models for key agreement. All these models attempt to cover desirable security properties as many as possible. In 2007, LaMacchia et al. [19] presented a new security model—the extended Canetti–Krawczyk (eCK) model for AKA protocols. The eCK model captures a very strong security property called *maximal-exposure-resilience* (MEX-resilience); that is, even though an adversary can reveal any non-trivial[1] combination of ephemeral secret keys and static secret keys, any information of the session key is not exposed. MEX-resilience implies many desirable security properties for AKA protocols including key-compromise impersonation (K-CI) resilience, (weak) perfect forward secrecy and ephemeral secrets reveal resistance (refer to Section 3.1 for the definitions of all these terms) etc. Therefore, the eCK model is considered a very strong security model while the original CK model [8] does not cover K-CI attacks.

Though the formal method using the above models are generally accepted to analyze the security of AKA protocols, the security analysis of many AKA protocols is carried out only in a heuristic way. The main obstacle in formal security proofs is that, without knowledge of the private key owned by the participants or the ability to solve the underlying hard problems, it is hard for the simulator to answer the *reveal* query which captures the *known-key security* property (see Section 3.1). In order to solve this problem, many previous AKA protocols employ strong non-standard assumptions (e.g., Gap assumptions [24]) or additional artificial oracles. In 2008, Cash et al. [11] put forward a new computational problem—the twin Diffie–Hellman problem, whose core is the "trapdoor test" which makes us able to implement an effective decisional oracle for the twin Diffie–Hellman problem without knowing the corresponding discrete logarithm. The trapdoor test technique makes it possible to remove strong non-standard assumptions and artificial oracles in security proof for AKA protocols. This provides a new approach to the design of AKA protocols under weak standard security assumptions.

Pioneered by the work of Sakai et al. (the first ID-based key construction from pairings [26]) and Boneh and Franklin (the ID-based encryption from pairings with provable security [7]), many ID-based AKA protocols have been proposed making use of bilinear pairings (e.g., [18,20–23]). In spite of the significant improvements in speeding up its computation, a pairing is still regarded as one of the most expensive operations. The relative computation cost of a pairing is approximately twenty times higher than that of a scalar multiplication over the elliptic curve group [12]. Therefore, pairing-free ID-based AKA protocols would be more appealing in terms of efficiency.

Currently, there are a few ID-based AKA protocols without bilinear pairings in literature. However, some of them have been shown to be insecure or have no acceptable formal security proof, others are only proven secure in weak models (e.g., they do not fully support both the adversary's *SessionKeyReveal* and *EphemeralSecretReveal* queries) and hence cover only limited desirable security properties. Several related proposals are given as follows.

In 2007, Zhu et al. [32] proposed an ID-based KA protocol without bilinear pairings, which is constructed using the CK model. However, their protocol does not capture the security property of ephemeral secrets reveal resistance. Additionally, their proposal, which integrates a pairing-free ID-based signature with the Diffie–Hellman (DH) key exchange, employs explicit signature-based authentication, and thus results in additional communication overhead. In 2008, Cao et al. [9] proposed a pairing-free ID-based KA protocol with implicit authentication. The proposal rests on the combination of the computational Diffie–Hellman (CDH) problem [15] and the divisible CDH (DCDH) problem [2]. Though their modified Bellare-Rogaway (mBR) model fully supports *SessionKeyReveal* queries, it does not support *EphemeralSecretReveal* queries, and their protocol cannot provide security against leakage of both parties' ephemeral secrets. Furthermore, their scheme requires three message exchanges, which is the same as Zhu et al.'s scheme [32]. In 2009, Fiore and Gennaro [16] put forward a pairing-free ID-based KA protocol which is proven secure in the CK model using forking lemma. The security of their protocol is based on the strong Diffie–Hellman (SDH) Assumption [1]. Also, they showed how to modify their protocol to obtain security under the standard CDH assumption at the cost of some degradation in efficiency. Although their protocol satisfies a good few desirable security properties, their CK model does not fully catch ephemeral secrets reveal resistance. This also makes their protocol susceptible to an ephemeral key compromise attack [13,16]. Furthermore, as for their modified protocol with its security based on the CDH assumption, the cost in computation and communication is rather too high. In 2010, Cao et al. [10] proposed a pairing-free ID-based AKA protocol with two message exchanges. They showed that their protocol can provide desirable security guarantees. However, their mBR model does not deal with the *EphemeralSecretReveal* queries, and as for their protocol the leakage of both parties' ephemeral secrets will compromise the session key. Furthermore, the security of their protocol is essentially based on the Gap Diffie–Hellman (GDH) assumption [24].

Also, we remark that three new related proposals [29–31] have been put forward before this revision of our paper is finished. In 2012, Xie and Wang [31] presented an efficient ID-based AKA protocol without relying on bilinear pairings, which achieves perfect forward secrecy and provable security in the CK model. Unfortunately, their protocol does not resist the ephemeral key reveal attacks which are also effective against the schemes proposed by Fiore and Gennaro [16]. In 2013, Vivek et al. [30] put forward a pairing-free ID-based AKA protocol provably secure under the SDH assumption in

[1] If both the static key and the ephemeral key of a party in the target session are revealed, the adversary trivially obtains the session key for any protocol.