ARTICLE IN PRESS

Information Sciences xxx (2014) xxx–xxx

Contents lists available at ScienceDirect

Information Sciences

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

An identity-based strongly unforgeable signature without random oracles from bilinear pairings

Saeran Kwon *

Department of Computer Science and Information, Daelim University College, Bisan-Dong Anyang 526-7, Republic of Korea

ARTICLE INFO

Article history:
Received 21 September 2008
Accepted 6 February 2014
Available online xxxx

Keywords:
Identity-based signature
Standard model
Without random oracle
Strong unforgeability
Bilinear pairing
Computational Diffie-Hellman problem

ABSTRACT

This paper proposes an identity-based (ID-based) signature (IBS) scheme which is strongly unforgeable in the standard model whose security is reduced to the hardness of the computational Diffie-Hellman (CDH) problem in bilinear groups. Currently, the ID-based encryption scheme (IBE) due to Waters is known to be the most practically efficient IBE whose security is guaranteed in the standard model depending on the decisional bilinear Diffie-Hellman (BDH) assumption. While as a solution for an ID-based signature of a total ID-based public key cryptosystem cooperating with Waters IBE, we share Waters's construction and system parameters to keep a key pair corresponding to each identity unchanged, our IBS needs only one group element for signing of messages and two elements for its randomness as supplementary parameters plus the original system parameters. Accordingly, thanks to requiring about half the system parameters against previous ID-based signatures proved secure without using random oracles under the standard complexity assumptions like CDH or BDH, our IBS is the more suitable for storage and communication requirements. In particular, this covers a stronger security property called strong unforgeability in the standard model in itself without applying any transformation technique.

1. Introduction

In view of simplifying certificate management in traditional public key system, Shamir [27] formulated the concept of identity (ID)-based public key cryptography (ID-PKC) in 1984, and Boneh and Franklin [7,8] presented the first fully practical and secure ID-based encryption scheme (IBE) based on bilinear pairings over an elliptic curve in 2001, where an entity's public key is directly derived from its public information such as name, e-mail address and IP address, and the corresponding private key is generated by a trusted party called a private key generator (PKG). Under the frame of the ID-PKC due to Boneh and Franklin [7,8], a number of ID-based signature (IBS) schemes have been proposed [11,17,25,26,31].

However, all works introduced above used the random oracle model [2] assuming hash functions as truly random functions, say, random oracles, in their security proofs. While most existing cryptographic works deploy the random oracle model in deducing provable security, it has been shown that the security of cryptographic schemes in the random oracle model does not always imply the security of the schemes that results from implementing random oracles by concrete cryptographic hash functions [10,15]. Accordingly, it arises interest to construct schemes to be secure in the standard model without

* Tel.: +82 31 467 4422; fax: +82 31 467 4428.
E-mail address: sranie@ewhain.net

http://dx.doi.org/10.1016/j.ins.2014.02.041
0020-0255/

assuming random oracles. In particular, Waters [30] succeeded in constructing an efficient IBE scheme in the standard model. In addition, he naturally drew a signature scheme existentially unforgeable in the standard model from the IBE, via a similar technique applied in the signature scheme of Boneh et al. [9] such that: a signer's public key in the signature scheme corresponds to system parameters in the IBE scheme, then a signature on a message M correspond to the private key of M issued by a trusted party with a secret master (here the signer) in the IBE system if regarding the message M as an identity of the same bit-string.

Yet Waters signature [30] drawn through such an approach is a standard-type signature scheme not being an ID-based scheme in ID-PKC. It is because the public key of a signature is not directly driven from a public information of an entity, say, the signer, such as an e-mail which uniquely identifies him, and accordingly the public key has to be assured of its validity, say, by a certificate as in the traditional public key cryptosystem (PKC). In effect, the first ID-based signature (IBS) scheme provably secure in the standard model was proposed by Paterson and Schuldt [23] in 2006, through a technique such as converting a 2-level hierarchical IBE (HIBE) (obtained by extending the Waters's IBE [30] hierarchically) into an IBS as follows:

- if the first-level identity ID in the hierarchical IBE possesses its private key which is generated by the PKG referred to root-level entity, then the private key of the second-level identity M (in fact, a message M) generated and issued by the first-level ID, can be regarded as an IBS on a message M by the signer ID, as noted by Gentry and Silverberg [14].

However, this scheme in [23] needs relatively large number of public parameters. Furthermore, it does not cover strong unforgeability [1,4] in security proof like Waters signature [30] does not, in that an adversary can easily modify an already existing signature on a message into a new valid signature on the same message.

Recently, in order to provide stronger security enough to prevent the above-mentioned modification at once for existing (weak) unforgeable signature schemes under adaptive chosen-message attacks [16], various generic transformation techniques [3,4,18,19,28,29] were proposed. In short, those transformations convert unforgeable (uf-cma) signature schemes to strongly unforgeable (suf-cma) ones without using random oracle assumption. While most of them consider as start of conversion the uf-cma signature schemes under the traditional PKC rather than the ID-based setting, it was shown that the transformation technique in [18,19] can be extended so as to start on unforgeable ID-based signature schemes in the ID-based setting and then attain suf-cma ID-based ones as outcomes. Though, the transformation in [18,19] yields quite a large-size suf-cma ID-based signature which consists of three parts $(\sigma_1, \sigma_2, vk_{OT})$ as follows: an ID-based signature σ_1 on the one-time public key vk_{OT} of a signer ID via the starting ID-based scheme, a signature σ_2 on a concatenation of the signature σ_1 generated before, a real message M and the identity ID via a strong one-time signature scheme to be employed for converting, and the one-time public key vk_{OT}. Even except for the size of an unforgeable (uf-cma) ID-based signature in the standard model, the one-time public key size and the signature size of an efficient strong one-time scheme in practice [18,19], amount to currently about 256×160 bit and 20×240 bit long respectively.

On the other hand, in 2006, Chatterjee and Sarkar [12] as well proposed a HIBE extending Waters's IBE to a hierarchical IBE protocol secure in the standard model, which improved upon Waters's original HIBE [30] by significantly reducing the number of public parameters. The HIBE due to Chatterjee and Sarkar [12] reuses the parameters used at the first level as ever for higher levels in the hierarchy during the private key generation, except for a set of parameters chosen distinctly one by one by each level. With applying the same technique as in [23,14] described above to the HIBE due to Chatterjee and Sarkar [12] confined to 2-level height, we can obtain a new IBS which reduces roughly half the public parameters as compared to the Paterson and Schuldt's IBS [23]. However, the IBS resulting from this construction has some restriction, that is, respective bit-represented lengths for both a signing identity and a random message are necessary to be the same because of using the same parameters in group representation of the identity and the message. Also, its security does not cover strong unforgeability like that due to Paterson and Schuldt [23].

1.1. Our contribution

In this paper, we present an ID-based signature (IBS) scheme secure in the standard model whose security is reduced to the hardness of the CDH problem. Our IBS supports randomness of signing process in a way of taking advantage of such a property that each entity can easily re-randomize at will its private key issued in a secure channel by the PKG, which is inherent in private key generation of Waters's IBE [30] or its variants. That makes the security reduction more tightly, because in our security proofs whenever an adversary issues signing queries, the simulator can always respond without abort thanks to the randomness of signing process. In addition, the security of our IBS requires just the standard CDH complexity assumption rather than depending on either stronger assumptions or new complexity assumption variants [6,22]. Besides, our IBS is strongly unforgeable against an adaptive chosen message and ID attack, which is a natural ID-based version of [16], in itself without applying any transformation techniques [3,4,18,19,28,29]. As well, our system needs as public parameters only three group elements more for both signing messages and supporting randomness of signing process at once, plus original system parameters for key generation relative to each identity as described in Waters IBE [30]. Our IBS consists of 3 group elements like [23]. Consequently, our IBS meets security in the stronger sense, say strong unforgeability, against an adaptive chosen message and ID attack, and at the same time storage and communication requirements more efficiently than previous schemes of the same kind by virtue of the smaller size of system parameters, having the same signature size.

Please cite this article in press as: S. Kwon, An identity-based strongly unforgeable signature without random oracles from bilinear pairings, Inform. Sci. (2014), http://dx.doi.org/10.1016/j.ins.2014.02.041