ARTICLE IN PRESS

Information Sciences xxx (2014) xxx–xxx

Contents lists available at ScienceDirect

Information Sciences

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

One forward-secure signature scheme using bilinear maps and its applications ☆

Jia Yu [a,b,*], Fanyu Kong [c,d], Xiangguo Cheng [a], Rong Hao [a], Guowen Li [e]

[a] College of Information Engineering, Qingdao University, 266071 Qingdao, China
[b] Shandong Provincial Key Laboratory of Computer Network, 250014 Jinan, China
[c] Institute of Network Security, Shandong University, 250100 Jinan, China
[d] Key Lab of Cryptographic Technology and Information Security, Ministry of Education, Jinan 250100, China
[e] School of Computer Science and Technology, Shandong Jianzhu University, 250100 Jinan, China

ARTICLE INFO

Article history:
Received 6 December 2008
Received in revised form 14 March 2014
Accepted 19 March 2014
Available online xxxx

Keywords:
Forward security
Key exposure
Bilinear map
Digital signature
Threshold signature
Intrusion-resilient signature

ABSTRACT

Forward-secure signatures are proposed to deal with the key exposure problem. Compared to regular signatures, forward-secure signatures have a special update algorithm that can evolve the new private key in each time period. Therefore, it can protect the security of signatures previous to the time period of key exposure. The efficiency is an important issue of forward-secure signatures. In this paper, we construct a new forward-secure signature scheme using bilinear maps. In this scheme, all performance parameters have complexities of log magnitude in terms of the total time periods. In addition, our scheme needs very few (only triple) pairing operations in the verifying algorithm, which is very important because the pairing operation is very time-consuming. This scheme is proved to be forward secure in the random oracle model assuming the CDH problem is hard. Finally, we give some applications of this scheme including constructing an intrusion-resilient signature scheme and constructing a forward-secure threshold signature scheme.

1. Introduction

1.1. Key exposure problem of digital signatures

The problem of secret key exposure has attracted much attention because it threatens the security of digital signatures greatly. For example, once a signing secret key is lost, all signatures become untrustworthy and have to be resigned no matter whether they are produced before the secret key exposure. Therefore, how to reduce the damage of key exposure for digital signatures is an important issue.

There are two kinds of cryptologic approaches to deal with this problem. The first kind is to make key exposure difficult. Threshold signatures belong to this kind of approach. In a threshold signature scheme, a secret key is divided into multiple pieces, and each server has one piece. Only more than threshold servers can cooperate to generate signatures. However, threshold signature requires multiple servers to jointly execute an interactive protocol when the signature is generated. Such a communication can be inefficient, inconvenient, and even impossible in some circumstance. The second kind is to limit the

☆ The extended abstract of this work has appeared in the Second International Conference on Provable Security (ProvSec 2008) [32].

* Corresponding author at: College of Information Engineering, Qingdao University, 266071 Qingdao, China. Tel.: +86 053285953151.
E-mail addresses: yujia@qdu.edu.cn (J. Yu), fanyukong@sdu.edu.cn (F. Kong), Chengxg@qdu.edu.cn (X. Cheng), hr@qdu.edu.cn (R. Hao), liguowen@sdjzu.edu.cn (G. Li).

http://dx.doi.org/10.1016/j.ins.2014.03.082
0020-0255/

damage of key exposure. Forward-secure digital signatures belong to this kind of approach. In a forward-secure signature scheme, the whole time is divided into multiple regular time periods. Each secret key is not only used to sign the messages in the current time period but also used to compute the secret key of the next time period by a one-way function. So the adversary is computationally infeasible to forge any signature previous to the period of key exposure even if the current key is exposed. In addition, key-insulated signatures and intrusion-resilient signatures can protect the security of signatures in other time periods when the secret key in one time period is exposed.

1.2. Related work

Anderson [3] firstly proposed to apply forward security to digital signatures. In the recent ten years, several forward-secure signature schemes have been proposed. These forward-secure signature schemes can be divided into two categories: the first is generic schemes that use any ordinary signature scheme as a black-box to construct forward-secure signature schemes; the second is specific schemes that construct specific forward-secure signature schemes through different methods.

The schemes constructed in [23,26,24] belong to the first category. The main contribution of [23] is to give the generic construction of forward-secure signature scheme from any regular signature scheme, which is based on generating all of the certificates in a pseudorandom manner. The generic construction of forward-secure signature scheme in [26] practically supports unlimited time periods, so it makes the scheme more flexible. Libert et al. [24] gave a generic construction of forward-secure signatures in untrusted update environments, which can be used to some special security architectures such as Gnu Privacy Guard (GPG) and S/MIME.

The schemes constructed in [4,2,19,22,15] belong to the second category. The main contribution of [4] is to formalize forward-secure signatures and give the first practical scheme. Bellare and Miner also provided the definitions of forward-secure signature and its security in [4]. Unfortunately, the public key and the secret key were very long, and signing and verifying are not very efficient. Subsequently, Abdalla and Reyzin proposed a new forward-secure signature scheme [2] which achieved shorter public key and secret key compared with [4]. However, key generation, signing and verifying algorithms were slower than those in [4]. Itkis and Reyzin proposed another forward-secure signature scheme [19] that had optimal signing and verifying algorithms at the expense of slower key update. While the scheme [22] proposed by Kozlovet al. could achieve fast key update but had slower signing and verifying algorithms. In above schemes, not all of key generation, key update, signing and verifying algorithms were very efficient because the operations costs for at least one algorithm were linear in the total number of time periods T. Therefore, how to construct a forward-secure signature scheme with higher efficiency has been a hot topic in research for a long time [17]. Hierarchical ID-based cryptography advocated by Gentry and Silverberg [14] could be used to construct efficient forward-secure signature schemes. Based on hierarchical ID-based cryptography [14] and ke-PKE [8], the first forward-secure signature scheme using bilinear maps was proposed in [15], whose efficiency was balanced across all its aspects because each parameter in the scheme had a complexity no larger than O ($\log T$). However, as the authors pointed out, the verifying algorithm in this scheme needed O ($\log T$) pairing operations. Because the pairing operation is time-consuming, reducing the time of pairing operations in forward-secure signature using bilinear maps is very important to improve the efficiency. Vo and Kim [28] tried to reduce the pairing operations and proposed yet another forward-secure signature from bilinear pairings in 2005. They claimed that the operations of all sub-algorithms in their scheme did not increase with T increasing. Unfortunately, it was proved that the scheme did not satisfy the forward security [31].

A fine-grained forward-secure signature scheme was proposed in [7], which allowed the signer to specify which signatures of the current time period remained valid when revoking the public key. Boyen et al. presented a forward-secure signature with untrusted update in [6]. Forward-secure public key encryption was studied in [8]. Forward-secure threshold signatures were also researched in [1,27,29,30]. Forward-secure identity-based signature and forward-secure identity-based encryption have been researched in [33,34]. Key insulated cryptography [11,12,35,25] and intrusion-resilient cryptography [20,10,9,18] were proposed to achieve a high level of security. These methods needed synchronization and the signer's communication with a safe device for each time period.

1.3. Our contribution

The main contributions of this paper can be summarized as follows:

(1) We construct a new forward-secure signature scheme using bilinear maps. The scheme has a nice performance. We make use of the binary tree structure similar to that in [15], as a result, the scheme has an advantage that all the complexities of the running time of key generation, key update, signing and verifying algorithms and the size of public key, secret key, and signature are no more than $O(\log T)$ in terms of the total number of time periods T. Because the scheme is operating over a particular elliptic curve, the signature size and the secret key size are short. In addition, we solve the problem that there are $O(\log T)$ pairing operations in the verifying algorithm of [15]. There are only triple pairing operations in our verifying algorithm. It is very important because the pairing operation influences the efficiency of the verifying algorithm greatly. We give the detailed performance comparison between our scheme and previous work.
(2) We prove our proposed scheme to be forward secure in the random oracle model assuming the CDH problem is hard. In order to prove the security of our scheme, we utilize different strategies to deal with different hash functions. In our

Please cite this article in press as: J. Yu et al., One forward-secure signature scheme using bilinear maps and its applications, Inform. Sci. (2014), http://dx.doi.org/10.1016/j.ins.2014.03.082