Theoretical Computer Science 595 (2015) 143–158

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Practical (fully) distributed signatures provably secure in the standard model

Yujue Wang [a,b,c,*], Duncan S. Wong [a], Qianhong Wu [d,g,i], Sherman S.M. Chow [e], Bo Qin [f], Jianwei Liu [d], Yong Ding [h]

[a] Department of Computer Science, City University of Hong Kong, Hong Kong, China
[b] The State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, China
[c] Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Computer, Wuhan University, Wuhan, China
[d] School of Electronics and Information Engineering, Beihang University, Beijing, China
[e] Department of Information Engineering, Chinese University of Hong Kong, Hong Kong, China
[f] School of Information, Renmin University of China, Beijing, China
[g] The State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[h] School of Mathematics & Computing Science, Guilin University of Electronic Technology, Guilin, China
[i] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China

ARTICLE INFO

Article history:
Received 30 September 2014
Received in revised form 14 March 2015
Accepted 13 June 2015
Available online 19 June 2015
Communicated by X. Deng

Keywords:
Distributed signature
Threshold signature
Secret sharing
Verifiable secret sharing
Monotone span program
Multipartite access structure
Standard model

ABSTRACT

A distributed signature scheme allows participants in a qualified set to jointly generate a signature which cannot be forged even when any unqualified set of participants collude together. In this paper, we propose an efficient scheme that supports any monotone access structures and show its unforgeability and robustness under the computational Diffie–Hellman (CDH) assumption in the standard model. For 192-bit security, its secret key shares and signature fragments are as short as 511 bits and 1022 bits, which are shorter than existing schemes assuming random oracle. We then propose two extensions. The first one allows new participants to dynamically join the system without any help from the dealer. The second one supports a type of multipartite access structures, where the participant set is divided into multiple disjoint groups, and each group is bounded so that a distributed signature cannot be generated unless a pre-defined number of participants from multiple groups work together. Finally, we present a fully distributed signature scheme such that the centralized trusted dealer can be removed from the system, and the secret keys (shares) can be jointly computed by the involved participants.

1. Introduction

Distributed signature [26,27,12], a useful cryptographic primitive in the multi-user setting, which enables a qualified set of participants to jointly generate a signature on a message. Each participant has a share of a (secret) signing key so that she/he can generate a signature fragment for a given message. A full signature can then be reconstructed by anyone who collects a qualified set of the signature fragments, i.e., these signature fragments belong to a qualified set of participants.

* Corresponding author.
E-mail addresses: wyujue2-c@my.cityu.edu.hk (Y. Wang), duncan@cityu.edu.hk (D.S. Wong), qianhong.wu@buaa.edu.cn (Q. Wu), sherman@ie.cuhk.edu.hk (S.S.M. Chow), bo.qin@ruc.edu.cn (B. Qin), liujianwei@buaa.edu.cn (J. Liu), stone_dingy@126.com (Y. Ding).

http://dx.doi.org/10.1016/j.tcs.2015.06.029
0304-3975/

Table 1
Comparison of distributed signature schemes for $\kappa = 192$ (bits).

Schemes	Key size	Key share size	Signature (fragment) size	Standard model
DL-based [27]	384	768	8064	×
RSA-based [26]	7680	7680	> 15360	×
RSA-based [12]	7680	7680	15360	✓
Our CDH-based	384–511	384–511	768–1022	✓

Usually, there are two requirements for such full signature. On one hand, this full signature should be computationally indistinguishable from the one generated directly using the signing key. On the other hand, it should be unforgeable even if all the participants in an unqualified set collude together. How the qualified set is represented may differ from construction to construction. The qualified set can be simply a threshold structure (which reduces distributed signature to its special case of threshold signature), or a more general notion of monotone access structure. For instance, consider a secret signing key is shared among three participants $\{p_1, p_2, p_3\}$ such that the minimal qualified sets are $\{p_1, p_2\}$ and $\{p_1, p_3\}$. Since $\{p_2, p_3\}$ is not qualified, existing threshold signature schemes cannot be employed in this distributed setting.

As multiple signers are involved in a distributed signature scheme, there are at least two properties we may expect. First, we want *robustness* such that the full signature can be successfully reconstructed even if some invalid signature fragments were collected. That is, the malicious participants cannot prevent the qualified ones from recovering the full signature. Second, it is also desirable if the scheme is *non-interactive* for both producing signature fragment and reconstructing the final full signature, i.e., for any given message, each signature fragment can be locally computed by every participant, and after all these fragments are collected, full signature reconstruction can take place without further help from any participants.

Non-interactive robust distributed crypto-system has been extensively used in distributed systems [39]. As a canonical example, it can be used to issue signature from a number of parties for the sake of security and availability, such as issue digital certificates and certify transactions between companies. Daza, Herranz, and Sáez [13] investigated its application in metering, which offers a publicly-verifiable cryptographic proof for counting the number of interactions between servers and clients, such as counting the number of visits to a web server (say, for advertisement accounting) by collecting signature fragments from the clients. Moreover, one may use this scheme in another way, e.g., a company can launch a promotion campaign such that users can get reward when they see the ad-banner of this company from a sufficient number of different web sites.

1.1. Our contributions

There are several distributed signature schemes [26,27,12] have been presented. Our basic scheme improves the state-of-the-art in a few different dimensions. In detail, our scheme achieves the following appealing properties:

1. *Provable security under standard assumption.* Our scheme is proven secure under the CDH assumption *without* relying on random oracles. Among the prior works, there exists only one RSA-based distributed signature scheme is proved secure without using random oracles due to Damgård and Dupont [12].
2. *Expressive access structure.* Our construction is generic and applicable to any linear secret sharing schemes. As a result, our scheme supports expressive access structure since monotone span programs are equivalent to linear secret sharing schemes [2] and every monotone access structure can be realized by a linear secret sharing scheme [26,45]. Sharing secret key can be tricky. Especially, in existing RSA-based distributed signature schemes such as [12,26], the Euler's totient function of RSA modulus should keep unknown even for share-holders. Besides, since any non-trivial linear dependence of the rows in the monotone span program allows to recover the Euler's totient function, all the sub-matrices regarding all unqualified sets should be full rank.
3. *Practical efficiency.* Compared to the existing schemes (refer to Table 1), our scheme offers better efficiency as its secret key shares and signature fragments are 2 times and 8 times shorter than the comparable ones. Take as an example for 192-bit security, the sizes of secret key shares and signature fragments in our scheme are as short as 511 bits and 1022 bits, respectively. Furthermore, our construction enjoys the *non-interactive* property, while all the existing comparable schemes [26,27,12] are interactive.

1.2. Extensions

We also extend our basic distributed signature scheme in two ways.

Dynamic joining. In some real scenarios such as ad-hoc networks, new participants are expected to join the system dynamically. A trivial solution to this issue needs the help from a trusted dealer who can distribute the corresponding secret key shares to the newly joined participants. We thus present an extension which is a threshold signature scheme and supports dynamic join without the presence of a dealer. A new participant just needs to talk to at least t existing users for a threshold t. As far as we know, the only existing such scheme is presented by Gennaro et al. [21] under the RSA assumption