Available online at www.sciencedirect.com

ScienceDirect

Information Sciences 177 (2007) 5638–5650

INFORMATION SCIENCES
AN INTERNATIONAL JOURNAL

www.elsevier.com/locate/ins

Hybrid proxy multisignature: A new type multi-party signature

Zecheng Wang [a,b], Haifeng Qian [a], Zhibin Li [a,*]

[a] *Institute of Theoretical Computing, East China Normal University, Shanghai 200062, PR China*
[b] *Department of Computer Science and Technology, Anhui University of Finance and Economics, Bengbu 233041, PR China*

Received 8 November 2006; received in revised form 31 May 2007; accepted 6 June 2007

Abstract

In this paper, we introduce a new type of multi-party signature: hybrid proxy multisignature (HPM). An HPM is collaboratively generated by some signers themselves and some proxy signers on behalf of their original signers. We describe the syntax of general HPM schemes and formalize a notion of security for them. We also construct a concrete HPM scheme and prove its security in the Random Oracle Model, assuming the Co-Diffie-Hellman problem in the underlying groups equipped with a pairing is hard. The size of an HPM in our scheme is independent of the number of the actual signers. Further, the scheme has accountability, that is the signers of an HPM can be identified. Comparing with other types of multi-party signatures such as multisignature, proxy multisignature and multiproxy multisignature, HPM has more flexibility.

Keywords: Digital signature; Proxy signature; Multisignature; Hybrid proxy multisignature; Co-Diffie-Hellman problem; Random oracle model

1. Introduction

A *proxy signature* protocol allows an entity, called the *designator* or *original signer*, to delegate another entity, called a *proxy signer*, to sign messages on its behalf. The delegated proxy signer can compute a *proxy signature* that can be verified by anyone with access to the original signer's certified public key. There are three types of delegations: full delegation, partial delegation and delegation by warrant or delegation by certificate. Since Mambo et al. first introduced this notion [12], proxy signature schemes have enjoyed a considerable amount of interest from the cryptographic research community. Boldyreva et al. [3] formalized a notion of security for proxy signature schemes and presented some delegation-by-certificate proxy schemes. Later, Tan and Liu [17] presented an attack to the delegation-by-certificate schemes and made some improvements to Boldyreva et al. security model.

[*] Corresponding author.
E-mail addresses: w52051201006@hotmail.com (Z. Wang), hfqian@cs.ecnu.edu.cn (H. Qian), lizb@cs.ecnu.edu.cn (Z. Li).

0020-0255/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2007.06.004

A *multisignature* scheme allows any subgroup of a group of players to jointly sign a document such that a verifier is convinced that each member of the subgroup participated in signing. Since Itakura and Nakamura introduced this notion [11], multisignatures have been extensively studied. Micali, Ohta, and Reyzin [13] formalized a strong notion of security for multisignatures and presented a provably secure multisignature scheme similar to Ohta and Okamoto's [15]. Later, based on the short signature scheme [5], Boldyreva [2] proposed a multisignature scheme and proved its security under a new security model.

Combining the ideas of the proxy signatures and multisignatures, some new signatures have been proposed [7–10,20]. For example, *proxy multisignature* is introduced by Yi et al. [20], where a designated proxy signer can generate the signature on behalf of a group of original signers. *Multi-proxy multisignature* scheme is introduced by Hwang and Chen [9], where only the cooperation of all members in the original group can authorize a proxy group and only the cooperation of all members in the proxy group can sign messages on behalf of the original group. *Multi-proxy signature* scheme is first proposed by Hwang and Shi [10], where an original signer can authorize a group of proxy member and only the cooperation of all the signers in the proxy group can generate the proxy signatures on behalf of the original signer. Recently, Wang and Cao [18] formalized a notion of security for proxy multisignature and proposed a provably secure scheme.

Now, suppose there is a company with n departments and each department has a manager and a secretary. Without loss of generality, we denote the n pairs of manager and secretary as $P = \{(m_1,s_1), \ldots, (m_n,s_n)\}$. It is often needed that a document is signed by some department managers $m_{i_1}, \ldots, m_{i_l}$ $(1 \leqslant l \leqslant n)$ jointly. This goal can be achieved by a multisignature scheme. But if one or more managers needed in generating a multisignature are absent, without loss of generality we suppose they are $m_{i_1}, \ldots, m_{i_j}$ $(1 \leqslant j \leqslant l)$, then the multisignature will not be able to be generated.

To solve this problem, we introduce a new kind of multisignature: hybrid proxy multisignature (HPM). In the above case, if each absent manager m_k has delegated his signing power to his secretary s_k, then the secretary can take part in generating a multisignature on behalf of him. Thus the above multisignature can be generated by j secretaries on behalf of their respective managers and $l-j$ managers, i.e. by $s_{i_1}, \ldots, s_{i_j}$, $m_{i_{j+1}}, \ldots, m_{i_l}$. Here $s_{i_1}, \ldots, s_{i_j}$ are proxy signers, $m_{i_{j+1}}, \ldots, m_{i_l}$ are ordinary signers. We call such a multisignature generated jointly by some ordinary signers and some proxy signers a *hybrid proxy multisignature*. An HPM can be verified by any verifier, using the public keys of the actual ordinary signers and the proxy signers as well as their respective original signers, and the warrants. Essentially, an HPM is a combination of a proxy signature and a multisignature in a new way.

We give the formal definition of an HPM scheme and formalize a notion of security for it. Further, based on the short signature scheme [5] and the aggregate signature scheme [4], we propose a concrete HPM scheme and prove its security under our security model, assuming the Co-Diffie-Hellman problem in the underlying groups equipped with a pairing is hard. Meanwhile the size of an HPM in our scheme is independent of the number of the actual signers. The scheme also has accountability, that is the signers of an HPM can be identified.

Here, we briefly point out the difference between an HPM scheme and other aforementioned multi-party signature schemes. Firstly, an HPM scheme is different from a multisignature scheme in the signers. The former may have proxy signers, while the latter only have ordinary signers. That is, a multisignature may be generated by some proxy signers and some ordinary signers jointly in an HPM, while it must be generated only by some ordinary signers in a multisignature scheme. Secondly, an HPM scheme is different from a multiproxy multisignature scheme in the following two points. In the former, each original signer independently generates a warrant and delegates his signing power to a proxy signer. In the latter, a fixed group of original signers jointly generate a warrant and delegate their multisignature signing power to a fixed group of proxy signers. On the other hand, in the former, some ordinary signers and some proxy signers on behalf of their respective original signers cooperatively generate a multisignature. In the latter, the group of proxy signers jointly generate a multisignature on behalf of the whole group of original signers. Since a proxy multisignature scheme is a special case of a multiproxy multisignature scheme, an HPM scheme is different from it as well as in the same ways.

According to above description and comparison, an HPM scheme has flexibility and more functionality. That is any subset L of all ordinary signers and proxy signers, as long as a proxy signer and his original signer do not be in the subset at the same time, may easily jointly sign a document. An HPM actually is an arbitrary combination of some ordinary signers' partial signatures and some proxy signers' partial proxy signatures. Especially, when all actual signers of a multisignature are ordinary signers, the scheme is an ordinary