New Threshold Proxy One-Time Signature Schemes

Min-Chih Kao and Yi-Shiung Yeh
Department of Computer Science and Information Engineering
National Chia-Tung University.
1001 Ta Hsueh Rd., Hsinchu,
Taiwan 300, R.O.C.
886-3-5914572
E-mail: gau @itri.org.tw; ysyeh@csie.nctu.edu.tw

ABSTRACT

*In a (*w, n*) threshold proxy signature, the original signer can delegate the power of signing messages to* n *proxy signers such that any* w *or more proxy signers cooperatively generate a proxy signature on behalf of the original signer, but (*w*-1) or less of them cannot. Following the same model, we first propose a new threshold proxy one-time signature scheme based on one-way functions. Our scheme still preserves the fast signature verification and low computation power of one-time signature, and so is suitable for various wireless applications.*

1: INTRODUCTIONS

Proxy signatures were first proposed by Mambo et al. [10, 12]. They defined three classes of proxy signature schemes: full delegation, partial delegation, and delegation by warrant schemes. A full delegation scheme assumes that a proxy signer is given the same signing keys that the original signer has. So, the proxy signer has the same signing capability as the original signer. A signature with partial delegation [10, 12, 17] allows the original signer using an original signing key to generate proxy signing keys, so their signatures are distinguishable. Hence, the original signer can delegate the power of a proxy signer in such a way. A signature with partial delegation by warrant limits the range of messages a proxy signer can sign by an additional piece of message (called a warrant). This type of delegation has proposed in [13, 18]. Furthermore, Wang et al. [21] classified proxy signature schemes into proxy-unprotected and proxy-protected schemes dependent on whether a original can generate a validate proxy signature or not. Following the development, there have been many threshold proxy signature schemes [7, 8, 16, 22] proposed for fitting various practical situations. Unlike Mambo et al.‘s proxy signature, a threshold proxy signature allows the original signer to delegate her/his signing capability to a group of proxy signers. In [7, 8, 16, 22], they used the threshold Shamir secret sharing method to share secret proxy signing keys and the homomorphism property of traditional authenticating schemes [5, 15] to combine all the partial proxy signatures, which are generated by the share of secret proxy signing keys, into a valid proxy signature.

One-time signature schemes were first proposed by Rabin [14] and Lamport [9] and are based on one-way functions. With their fast signature verification and low computation power, they have arrested more and more attention, as an ideal option for various wireless applications that use resource-constrained devices such as mobile phones, PDAs etc. Following the history of the traditional signature technology based on public-key cryptography development, the proxy and threshold signature based on one-way functions were also important for various wireless applications. To our best knowledge, there have been three schemes [1, 4, 20] based on one-way functions proposed for proxy signature. In [1], the authors also proposed a threshold proxy signature scheme based on one-way functions. However, their model is different from the previous works [4, 7, 8, 17, 20 and 22]. In the (w, n) threshold proxy one-time signature scheme of [1], the original signer is a group of n signers, and the proxy signers are any w signers. Therefore, their scheme is still a threshold one-time signature scheme regardless of their model. In this paper, we present a threshold proxy-protected signature scheme following the model, that an original signer shares her/his proxy signing key to a group of n proxy signers and any w or more partial proxy signatures generated by w or more proxy signers can be combined into a valid signature, of previous works (called original model).

The rest of this paper is organized as follows. In Section 2, we discuss the related works and some security requirements for threshold proxy signatures. Section 3 briefly reviews Change’s proxy one-time signature scheme and other primitives. In Section 4, we expand this scheme into threshold proxy one-time proxy signature scheme. Section 5 analyzes the security of the proposed scheme. Finally, we conclude this article in Section 6.

2: Related Works

In [7, 8, 16 and 22], the authors provided not only various constructions for threshold proxy signature schemes, but also various security requirements. Hwang et al. summarized the following requirements for a (w, n) threshold proxy signature:

Secrecy. No proxy signers can derive the original's private key from any information such as the shares of the proxy signing key, proxy signature etc. Even if all proxy signers collude together, they cannot get the original signer's private key.

Proxy protected. Only the delegated proxy signer can generate partial proxy signature. It is infeasible for the original signer to forge partial signatures.

Unforgeability. A valid proxy signature can only be cooperatively generated by *w* or more proxy signers. This means that if a signature has been generated by *w* or more proxy signers, (*w*-1) or less proxy signers, or any third parties (not delegated proxy signers) can not forge the signature.

Nonrepudiation. Any valid proxy signature must be generated by *w* or more proxy signers. That is, the scheme guarantees that proxy signers can not deny that they have signed the message and the original signer can not deny having delegated the power of signing messages to the proxy signers.

Time constraint. The proxy signing keys can be used only during the appointed period. Once they expire, those keys cannot be used to generate a valid signature.

Known signers. For internal auditing purposes, the system is able to identify the signers who actually sign the message on behalf of the proxy group.

Although the above requirements are derived from threshold proxy signature schemes based on public-key cryptography, they are also suitable for a threshold one-time proxy signature scheme (or simply TOTP signature) based on one-way functions. Thus, this paper will follow these security requirements given above.

To our best knowledge, there is only one paper [1] about TOTP signature. Al-Ibrahim's (*w*, *n*) TOTP signature scheme includes a trust party TP and a group of *n* signers P_i, $i = 1, 2, .., n$, together with three phases: *key generation and share distribution*, *signing*, and *verification*. These three phases is roughly depicted as follows. In the first phase, the signers select randomly secret key s_j, $j = 1, 2, \ldots, v$, and divide into *n* shares, $s_{i',j}$ where *i'* = 1,2, …,*n*, by the threshold Shamir secret sharing method, and send securely to $P_{i'}$ where *i'* = 1,2, …,*n*. Then, the signers compute $p_j = h(s_j)$, and send to TP. In signing phase, each signer P_i, $i = 1, 2, .., t$, encodes the message m based on 2 as m = $(j_1, j_2, \ldots, j_r)$. Then, each signer P_i computes partial signature (s_{i,j_1}, $s_{i,j_2}, \ldots,$ s_{i,j_r}) and sends it to each other. Finally, the signers jointly compute the signature (m, j_k, s_{j_k}), $k = 1, 2, \ldots, r$, using Lagrange interpolation, and send it to a verifier. In verification phase, the verifier waits until all ($s_{j_1}, s_{j_2}, \ldots,$ s_{j_r}) and fetches p_j from TP. Then, the verifier checks whether $p_{j_k} = h(s_{j_k})$ where $k = 1, 2, \ldots, r$.

We note that the new model of [1] is different from previous works. If we apply it to the original model, the TOTP signature scheme of [1] does not satisfy some requirements given above. We will discuss some weaknesses caused by their scheme using in the original model. First, the verifier cannot identify the actual proxy signer from the proxy signature. Therefore, the requirement "known signers" is not satisfying. Second, the proxy signing key does not derive from the private key of the original signer. This means that the TP must guarantee that the original signer cannot refuse having delegated the power of signing messages to the proxy signers. Therefore, the TP is not merely to keep the public key and to prevent repeated signing. Third, there is no mechanism about preventing the signer from forging a valid proxy signature. Therefore, some important requirements such as "Nonrepudiation" and "Proxy protected" are not satisfied.

3: Preliminaries

In this section, we briefly describe the necessary cryptographic schemes which are used in our construction of TOTP signatures.

3.1. One-Time Proxy Signature Based One-way Hash Functions

There are various one-time proxy signature schemes [1, 4, and 20] have been proposed. We can summarize as follows.

Definition 1 Let *f* be a one-way function. An original signer produces a proxy signing key set *SK* = $\{s_1, s_2, \ldots, s_t\}$ and public key set *PK* = $\{v_1, v_2, \ldots, v_t\}$ where $v_i = f(s_i)$. Then, the original signer delegates the power of signing by distributing proxy signing keys to a proxy signer.

When the proxy signer receives a message *m*, the signer explains m as a binary string $m_b = (j_1, j_2, \ldots, j_k)$ Then, the signer selects $(s_{j_1}, s_{j_2}, \ldots, s_{j_k})$ as a signature from *SK* according m_b, where $k \leq t$, and the algorithms found in [1, 4, and 19].

To verify $(s_{j_1}, s_{j_2}, \ldots, s_{j_k})$, a verifier checks whether $v_{j_i} = f(s_{j_i})$ for $i = 1, 2, \ldots, k$.

In definition 1, we describe the principal steps of proxy signature schemes. The additional operations are needed for security concerns like [20] in which the authors consider **swallow arracks**. They suppose that the original signer has known a valid proxy signature and *swallows* the signature. Then, the original signer generates a new signature for another new message. Thus, their scheme satisfies the requirement "proxy protected".

3.2 Perfect Hash Families (PHF) and Cover Free Family (CFF)

We review the definition of PHF (*N*; *n*, *m*, *w*) and (*n*, *m*, *w*)-CFF as follows.

Definition 2 [2] Let *n*, *m* and *w* be integers such that $n \geqq m \geqq w \geqq 2$. Let *V* be a set with $|V| = n$ and let *F* be a set with $|F| = m$. Let *A* be an $N \times n$ array with entries in F. A set *X* of columns of *A* is *separated* by the *i*th row of *A* if the *i*th components of columns in *X* are all distinct. An (*n*, *m*, *w*)-perfect hash family is an $N \times n$ array *A* with entries in the set F if for every subset *X* of the columns of *A* with $|X| = w$ there exists at least one row that separates *X*. Let PHF (*N*; *n*, *m*, *w*) denote an (*n*, *m*, *w*)-perfect hash family which has *N* rows.

Definition 3 [6] Let (X, F) be a set system with X = $\{x_1, x_2, \ldots, x_m\}$ and F = $\{ B_i \subseteq \mathrm{X} \mid i = 1, 2, \ldots, n\}$. We call (X, F) be an (*n*, *m*, *w*)-CFF (or (*n*, *m*, *w*)-CFF for short) if $B_i \not\subset B_{j_1} \cup B_{j_2} \cup \ldots \cup B_{j_w}$ for all B_{j_1}, B_{j_2},…, $B_{j_w} \in$ F, where $i \notin \{j_1, j_2, \ldots, j_w\}$.

4: The Proposed Method

This paper proposes a new (*w*, *n*) TOTP signature scheme that combines the one-time proxy signature scheme and combinatorial object PHFs. There are three entities: an original signer, proxy signers, and a trust party (or simply TP) in the scheme and it works as follows.

(Key Generation)

Given an array *A* which is PHF (*N; n, m, w*) and a one-way function *f* with three inputs, the algorithm consists of the following three steps.

Given $t > N$, the original signer generates *m* private key sets $SK_i = \{s_{i1},\ s_{i2}, \ldots, s_{it}\}$ for *i* = 1, 2, …, *m*. Then, computes public key set $PK_i = \{v_{i1},\ v_{i2}, \ldots, v_{it}\}$, where $v_{i1} = f(s_{i1})$, …, $v_{it} = f(s_{it})$, for *i* = 1, 2, …, *m*.

For every SK_{j_1}, …, SK_{j_N}, the signer generate a private key matrix $S=(s_{ik})$, where *i* = 1,2, …, *N* and *k* is the entry a_{il} of *A* where *l* = 1, 2, …, *n*. Thus, the original signer will produces C_N^m matrixes like *S*. Then, the original signer send the *i*th columns of C_N^m matrixes to ith proxy signers for *i* = 1,2, …, *n*.

Through TP, the *n* proxy signers determine one matrix (say *S*) jointly.

(Proxy Signature Generation)

Suppose that any *w* proxy signers $\{j_1, j_2, \ldots, j_w\}$ want to sign a proxy signature on message *m* with binary string $m_b = (i_1,\ i_2,\ \ldots,\ i_k)$, where $w \leq k$. It works as following three steps.

The proxy signers compute $r = h(m)$ and send to TP.

Suppose that all proxy signers have the matrix *A*. The *w* proxy signers get at least one row that separate *X* as definition 2 according *A*. Then, they use the row with minimum row index to generate partial signature. Suppose that the row index is *l*.

The j_ith proxy signer will contributes $s_{la_{lj_h}}$ as a partial signature when $h \in \{ i_1, i_2, \ldots, i_k \}$. Then, proxy signer sends (*l*, *m*, $s_{la_{lj_h}}$) to a verifier who request the signature for *m* for all $h \in \{ i_1, i_2, \ldots, i_k \}$ and the other private keys are also sent. .

(Proxy Signature Verification)

The verifier gets *r* from TP and checks whether $r = h(m)$.

The verifier get public key from PK_l.

The verifier checks whether $v_{la_{lj_h}} = f(s_{la_{lj_h}})$, *i*=1, 2,.., *w*.

If the validation goes through, the verifier accepts the proxy signature (*l*, j_{i_1}, j_{i_2}, ..., j_{i_k}, $s_{la_{li_1}}$,…, $s_{la_{li_k}}$, *m*, *other private keys*) which is collaboratively generated by the signers $\{j_1, j_2, \ldots, j_w\}$ on behalf of the proxy group {1, 2, ..., *n*}.

5: Discussion

In this section, we examine the correctness and the security of this scheme.

5.1 Correctness

In our scheme, the proxy signers choose a matrix *S* from C_N^m matrixes that are constructed as description above. By definition 2, every *w* proxy signers can hold *w* distinct proxy signing keys from at least one row of s. Thus, (*l*, j_{i_1}, j_{i_2}, ..., j_{i_k}, $s_{la_{li_1}}$,…, $s_{la_{li_k}}$, *m*) is a validate proxy signature by definition 1, where *l* is the row index.

Example 1 Given PHF as follows**.**

	1	2	3	4	5	6	7	8	9
row 1	1	1	1	2	2	2	3	3	3
row 2	1	2	3	1	2	3	1	2	3
row 3	1	2	3	3	1	2	2	3	1
row 4	1	2	3	2	3	1	3	1	2

Suppose that 9 proxy signers determine *S* which constructed by private key sets SK_1, …, SK_4, as follows.

	1	2	3	4	5	6	7	8	9
SK_1	s_{11}	s_{11}	s_{11}	s_{12}	s_{12}	s_{12}	s_{13}	s_{13}	s_{13}
SK_2	s_{21}	s_{22}	s_{23}	s_{21}	s_{22}	s_{23}	s_{21}	s_{22}	s_{23}
SK_3	s_{31}	s_{32}	s_{33}	s_{33}	s_{31}	s_{32}	s_{32}	s_{33}	s_{31}
SK_4	s_{41}	s_{42}	s_{43}	s_{42}	s_{43}	s_{41}	s_{43}	s_{41}	s_{42}

When proxy signers {2, 3, 4} want to generate a proxy signature for m with m_b = (1, 3), they will get row index 2 and proxy signers 3 and 4 will contribute s_{23} and s_{21}, respectively. Then, they can generate a validate proxy signature (2, 2, 3, 4, s_{23} ,s_{21}, m, s_{22}). □

5.2 Security

In this section, we will show that the proposed is a secure (n, w)-threshold proxy signature scheme. First, we will show that our scheme has "proxy protected" property and is secure again the swallow attacks.

Lemma 1 The probability that the original signer, without seeing any signature, can forge a validate proxy signature is at most $1/m$.

Proof In this attack, the original signer generates a proxy signature and then claims that is generated by some proxy signers. The original signer succeeds if she/he must get the right private key set and the row index corresponding to the private key matrix S. We know that there are m right private key sets and C_N^m private key matrixes. □

Lemma 2 The proposed scheme is secure again the swallow attacks.

Proof The original signer can swallow the message and the signature, and then generate another one. To avoid such attack, the proxy signers register the hash of the message with TP and any verifier can check the message from TP in our scheme. Therefore, the original signer can not substitute for proxy signers. □

Consider the proxy signing key matrix $S= (s_{ij})$. The index of entry s_{ij} is constructed from (i, a_{ij}), where I is the row index and aij is the entry of PHF(N; n, m, w). From [16], we know that S is a (n, Nm)-CFF. Thus, the union of any w-1 columns in S can not cover the remaining one. This means that (w-1) or less proxy signers can not generate a validate proxy signature. Therefore, the property of unforgability is satisfied. It is easy to see that the other properties are satisfied.

6. Conclusion

Based on perfect hash families, we present a new (w, n) threshold proxy one-time signature scheme that meets most of the requirements of [15] under the original model. Our scheme preserves the fast signature verification and low computation power of one-time signature, and so is suitable for various wireless applications. Furthermore, the proposed scheme improves the security of Change's one-time proxy signature scheme as well.

REFERENCES

[1] M. Al-Ibrahim and A. Cerny, "Proxy and Threshold One-Time Signatures," *In: Proc. of the 1th International Conference Applied Cryptography and Network Security* (ACNS'03), LNCS 2846, pp. 123-136, Springer-Verlag, 2003.

[2] S. R. Blackburn, "Combinatorics and Threshold Cryptology," *in Combinatorial Designs and their Applications* (*Chapman and Hall/CRC Research Motes in Mathematics*), *CRC Press*, pp. 49-70, 1999.

[3] C. C. Lindner and C. A. Rodger, *Design Theory, CRC Press*, Boca Raton, 1997.

[4] M. H. Chang and Yi-Shiung Yeh, "Improving Lamport One-Time Signature Scheme," *Applied Mathematic and Computation*, vol. 167/1 pp. 118-124, 2005

[5] T. ElGamal, "A Public-Key Cryptosystem and a signature Scheme Based on Discrete Logarithm," *IEEE Trans. Information Theory*, vol. 31, no. 4, pp. 469-472, 1985.

[6] P. Erdös, P. Frankl, and Z. Furedi, "Families of finite sets in which no set is covered by the union of r others," *Israel Journal of Mathematics*, 51(1985), pp. 79-89, 1985.

[7] M.-S. Hwang, E. J.-L. Lu, and I.-C. Lin, "A Practical (t, n) Threshold Proxy Signature Scheme Based on the RSA Cryptosystem," *IEEE Trans. Knowledge and Data Engineering*, vol. 15, no. 6, pp. 1552-1560, 2003.

[8] [S. Kim, S. Park, D. Won, "Proxy signatures," revisited. *ICICS'97*, LNCS 1334, pp. 223-232, Springer, Berlin, 1997.

[9] L. Lamport, "Constructing digital signatures from a one-way function," *Technical report CSL-98, SRI International, Palo Alto*, 1979.

[10] M. Mambo, K. Usuda, E. Okamota, "Proxy signatures: delegation of the power to sign messages," *IEICE Trams. Fundamentals E79-A* (9) (1996), pp. 1338-1354, 1996.

[11] M. Mambo, K. Usuda, E. Okamota, "Proxy signatures for delegating signing operation," *Proc. 3rd ACM Conference on Computer and Communication Security*, ACM press, pp.48 1996.

[12] K. Martin, J. Pieprzyk. R. Safavi-Naini, H. Wang, and P. Wild, "Threshold MACs," *Information Security and Cryptology - ICISC* 2002, LNCS 2587, Springer-Verlag, pp. 237-252, 2003.

[13] B.C. Neuman, "Proxy-based authorization and accounting for distributed systems," *Proc. 13th International Conference on Distributed Systems*, pp. 283-291, 1993.

[14] M. O. Rabin, "Digitalized signatures," Foundations of Secure Communication," *Academic* Press, pp. 155-168, 1979.

[15] R.L. Rivest, A. Shamir, and L.M. Adleman, "A Method for Obtaining Digital Signatures and

Public-Key Cryptosystems," *Comm. ACM*, vol. 21, pp. 120-126, 1978.

[16] J. N. Staddon, D. R. Stinson, and R. Wei, "Combinatorial properties of frame-proof and traceability codes," *IEEE Trans. On Information Theory*, vol. 47, pp. 1042-1049, 2001.

[17] H.-M. Sun, "An Efficient Nonrepudiable Threshold Proxy Signature Scheme with Known Signers," *Computer Comm*., vol. 22, no. 8, pp. 717-722, 1999.

[18] K. Usuda, M. Mambo, T. Uyematsu, E. Okamota, "Proposal of an automatic signature scheme using a compiler," *IEICE Trans. Fundamentals E79-A* (1) (1996), pp. 94-101, 1996.

[19] V. Varadharajan, P. Allen, and S. Black, "Analysis of the proxy problem in distributed systems," *Proc. 1991 IEEE Computer Society Symposium on Research in Security and Privacy*, 1991, pp. 255-275.

[20] H. Wang and J. Pieprzyk "Efficient One-Time Proxy Signatures," *Advances in Cryptology-ASIACRYPT 2003* (ASIA- CRYPT'03), LNCS 2894, Springer-Verlag, pp. 507-522, 2003.

[21] Guilin Wang, Feng Bao, Jianying Zhou, and Robert H. Deng, "Proxy Signature Scheme with Multiple Original Signers for Wireless E-Commerce Applications," *Proceedings of 60th IEEE Vehicular Technology Conference, Session 4.6: Wireless Sensor/Network Security*, Los Angles, California, September 2004, IEEE Vehicular Technology Society Press.

[22] K. Zhang, "Threshold proxy signature schemes," *1997 Information Security Workshop*, Japan, September, pp. 191-197, 1997.