A Novel Hybrid Threshold Proxy Signature Scheme

Xin Yang , Long Zhang* , Chunming Li , Guoqiang Li

School of Mathematical Sciences, Heilongjiang University, Harbin, 150080, China
E-mail: lzhang@hlju.edu.cn

***Abstract*—In this paper, we propose a new type of threshold proxy signature scheme: hybrid threshold proxy signature (HTPS), in which a signature is cooperatively generated by the partial original signers themselves and the proxy signers on behalf of their own original signer in threshold proxy way. We formalize the notion of security for hybrid threshold proxy signature scheme and prove our scheme's security, such as, distinguishability, verifiability, strong unforgeability, strong nonrepudiation, etc.**

Keywords—threshold proxy signature; Hybrid threshold proxy signature scheme; ID-baesd

I. INTRODUCTION

In 1996, the concept of proxy signature was first introduced by Mambo et al [1]. It allows an original signer to delegate his signing power to a designated person, called the proxy signer, who has the power to act on behalf of the original signer. Following the development of proxy signature, the threshold proxy signature was also widely studied [2-4]. Threshold proxy signature schemes are designed to delegate the signing power to a proxy group of proxy signers. In a (t,n) threshold proxy signature scheme, the proxy signature key is shared among a group of n proxy signers delegated by the original signer. Any t or more proxy signers can cooperatively sign messages on behalf of the original signer.

Now, suppose there is a company with n_1 managers and n_2 secretaries. It is often needed that a document is signed by some department. If one or more managers needed in generating a signature are absent, according to Wang et al introduced hybrid proxy multisignature[5], the secretary can take part in generating a multisignature on behalf of him.

But there is a disadvantage in Wang's scheme: if a manager and his proxy secretary are absent at the same time, Wang's scheme can't solve this problem.

To solve this problem, we introduce a new kind of threshold proxy signature: hybrid threshold proxy signature (HTPS). In a HTPS, the every absent manager delegate the signing power to a group of proxy signers for sharing signing responsibility, the group of proxy signers use (t,n) threshold scheme on behalf of the absent manager, then proxy signers and the present managers cooperatively generate signature.

The HTPS is a special case of threshold proxy signature but more flexibility and functionality. The HTPS actually is an arbitrary combination of the original signers' partial signatures and proxy signers' partial signatures. Especially, when all actual signers are original signers, the HTPS is an ordinary signature scheme; when all actual signers are proxy signers, the HTPS is an ordinary threshold proxy signature scheme.

In this paper, we formalize a notion of security for hybrid threshold proxy signature scheme. Then, we propose a new hybrid threshold proxy signature scheme and prove its security.

II. NOTION OF HYBRID THRESHOLD PROXY SIGNATURE SCHEME

A. Definition of Hybrid Threshold Proxy Signature

In a hybrid threshold proxy signature scheme, suppose there are n_1 departments and each department has an original signer and n_2 proxy signers as (O_i, P_{ij}), here P_{ij} is the j proxy person in O_i group $i=1,\cdots,n_1$, $j=1,\cdots,n_2$. There is a document needed to be signed by original signer jointly. If one or more original signers are absent, the proxy signers in the absent original signer group on behalf their respective original signer to generate proxy partial signature in (t_2,n_2) threshold way. The final hybrid threshold proxy signature is cooperatively generated by the participant original signers and the proxy signers.

We call such a signature generated jointly by some ordinary signers and some proxy signers a hybrid threshold proxy signature.

B. Syntax of Hybrid Threshold Proxy Signature Scheme

The definition details the components of a hybrid threshold proxy signature scheme as following:

A hybrid threshold proxy signature scheme is a tuple $TPTS=\{G,S,V,PDCG,PSG,PSV,ID\}$

- G The system parameters generation algorithm input the secure parameters 1^k, the algorithm output the public and private key for the original signers and the proxy signer are $(Q_{O_i},S_{O_i}),(Q_{P_i},Q_{P_i})$.
- S The standard signing algorithm, $S(m,S_i)=\sigma$, input: message $m\in\{0,1\}^*$ and secret key S_i, output : signature σ.
- V The verification algorithm, $V(m,\sigma,Q_i)=1 \, or \, \perp$, input message m, signature σ, public key of signer Q_i. If the signature is valid, output 1, otherwise, output $\perp$.

* Corresponding author. E-mail: lzhang@hlju.edu.cn

- *PDCG* The proxy delegation certificate generation algorithm, the original signers and the proxy signers generate $PDCG(k_{O_i}, S_{O_i}, k_{P_{ij}}, S_{P_{ij}}) = (U_{O_iP}, S_i)$ cooperatively, input: random number and public key of each group, output: proxy delegation certificate of each group, then the clerk generate the final proxy delegation certificate (U, S).
- *HSG* The hybrid signature generation algorithm, the participant original signers and the proxy signers in the absent original signers group collaboratively generate. $HSG(m, m_\omega, (U,S), S_{O_i}, S_{P_{ij}}) = \sigma$, input: message $m \in \{0,1\}^*$, secret key of actual signers $S_{O_i}, S_{P_{ij}}$, the proxy delegation certificate q and a warrant m_ω , and m satisfies the requirements stated in m_ω , output: hybrid proxy signature $h\sigma$.
- *HSV* The hybrid signature verification algorithm, 1.verify (U, S) . If it is hold, do the next, otherwise $\perp$; 2. $HSV((U,S), m, m_\omega, h\sigma, Q_{O_i}, Q_{P_{ij}}) = 0 \text{ or } 1$. Everyone can verify the valid of hybrid signature with this algorithm. If valid, output 1, otherwise output 0.
- *ID* The actual signers identification algorithm, input a hybrid threshold proxy signature $h\sigma$, output the actual signers identification, or $\perp$ in case of an error.

A hybrid threshold proxy signature is the extension of threshold proxy signature, so a security hybrid threshold proxy signature scheme also satisfies the security such as strong unforgeability, strong nonrepudiation, distinguishability, resistance to conspiracy attack, etc.

III. A Secure Hybrid Threshold Proxy Signature Scheme

A. Setup

PKG chooses G_1 and G_2 be two cyclic groups of prime q , Let P be a generator of G_1 , $e: G_1 \times G_1 \to G_2$ be a secure bilinear pairing，and choose two cryptographic hash function $H_1: \{0,1\}^* \to Z_q, H_2: \{0,1\}^* \to G_1$ .PKG pick a random number s from Z_q^* , compute $P_{pub} = sP$, keep s as secret key. Publish $\{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$.

B. The Private Key Generation

Given each original signer $O_i (i = 1, 2, \cdots, n_1)$ his identity ID_{O_i} , PKG computers $S_{O_i} = sQ_{O_i} = sH_2(ID_{O_i})$ as private key.

Given each proxy signer $P_{ij} (i = 1, 2, \cdots, n_1; j = 1, 2, \cdots, n_2)$ his identity $ID_{P_{ij}}$, PKG computers $S_{P_{ij}} = sQ_{P_{ij}} = sH_2(ID_{P_{ij}})$ as private key.

C. The Proxy Delegation Certificate Generation

1) The original signers $O_i (i = 1, \cdots, n_1)$ choose k_i from Z_q^*, compute $U_i = k_i Q_{O_i}$, $h_i = H_1(m_\omega \| U_i)$, $V_i = (k_i + h_i) S_{O_i}$. Here m_ω is proxy warrant which records the identities of the original signers and the proxy signers, correspondence, the parameters t_1, t_2 , the valid delegation time, authorities. etc. $O_i (i = 1, \cdots, n_1)$ chooses a random polynomial $f(x)$ over G_1 of degree $t_2 - 1$:

$$f_i(x) = V_i + a_{i1}x + a_{i2}x^2 + \cdots + a_{it_2-1}x^{t_2-1}.$$

Computes $V_{P_{ij}} = f_i(ID_{P_{ij}}), (j = 1, 2, \cdots, n_2)$, and sends $h_i V_{P_{ij}}$ to the proxy signers as their secret in secure ways, computes $A_{ij} = e(h_i V_{P_{ij}}, P)$, $A_i = \prod_{j=1}^{n_2} A_{ij}$, and publish $(h_i, A_i, m_\omega, U_i)$.

2) Each proxy signer P_{ij} verifies $e(h_i V_{P_{ij}}, P) = A_{ij}$ received $h_i V_{P_{ij}}$. If the verification is hold, accept, otherwise, reject.

3) $O_i (i = 1, 2, \cdots, n_1)$ chooses k_{O_i} from Z_q^* , compute $U_{O_i} = e(P, P)^{k_{O_i}}$.

$P_{ij} (j = 1, 2, \cdots, n_2)$ chooses $k_{P_{ij}}$ from Z_q^* , compute $U_{P_{ij}} = e(P, P)^{k_{P_{ij}}}$, and publish $U_{O_i}, U_{P_{ij}}$.

Each group O_i and P_{ij} cooperatively compute

$$U_{O_iP} = U_{O_i} \prod_{j=1}^{n_2} U_{P_{ij}}, h_i' = H_1(m \| U_{O_iP}).$$

O_i compute $s_i = S_{O_i} h_i' + k_{O_i} P$

P_{ij} compute $l_{ij} = S_{P_{ij}} h_i' + k_{P_{ij}} P$, send l_{ij} to O_i in secure ways.

4) O_i verifies $e(l_{ij}, P) = e(Q_{P_{ij}}, P_{pub})^{h_i'} U_{P_{ij}}$ received l_{ij} . If the verification is hold，

O_i computes $S_i = s_i + \sum_{j=1}^{n_2} l_{ij}$, and sends (U_{O_iP}, S_i) to O_1 and P_{ij} as their proxy certificate.

5) After O_1 and P_{ij} received (U_{O_iP}, S_i) , they verify

$$e(S_i, P) = e(Q_{O_i}, P_{pub})^{h_i'} e(\sum_{j=1}^{n_2} Q_{P_{ij}}, P_{pub})^{h_i'} U_{O_iP}.$$

If the verification is hold, accept (U_{O_iP}, S_i) .

O_1 compute $U = \prod_{i=1}^{n_1} U_{O_iP}$, $S = \sum_{i=1}^{n_1} S_i$ and publish (U, S) as the final proxy delegation certificate.

D. The Hybrid Threshold Proxy Signature Generation

In order to sign message m , without loss of generality, we assume that $O_1, \cdots, O_{t_1}$ are the attendant original signers and $O_{t_1+1}, \cdots, O_{n_1}$ are the absent original signers, $P_{i1}, \cdots, P_{it_2}$ $(i = t_1 + 1, \cdots, n_1)$ are the actual proxy signers of absent original signers group.

1) $O_i (i = 1, \cdots, t_1)$ open his U_{O_i} , every group's actual

proxy signers compute and publish

$$U_i = \prod_{j=1}^{t_2} U_{P_{ij}} \ , i = t_1 + 1, \cdots, n_1 .$$

$O_i (i = 1, \cdots, t_1)$, $P_{ij} (i = t_1 + 1, \cdots n_1; j = 1, \cdots, t_2)$ cooperatively compute $D_{OP} = \prod_{i=1}^{t_1} U_{O_i} \prod_{i=t_1+1}^{n_1} U_i$, $v = H_1(m \| D_{OP})$.

2) $P_{ij} (i = t_1 + 1, \cdots n_1; j = 1, \cdots, t_2)$ compute

$$y_{P_{ij}} = (h_i V_{P_{ij}} \eta_{ij} + S_{P_{ij}}) v + k_{P_{ij}} P$$

here $\eta_{ij} = \prod_{k=1, j \neq k}^{t_2} (-ID_{P_{ik}})(ID_{P_{ij}} - ID_{P_{ik}})^{-1}$,

every group verify $e(y_{P_{ij}}, P) = A_{ij}^{\eta_{ij} v} e(Q_{P_{ij}}, P_{pub})^v U_{P_{ij}}$,

if the verification is hold, compute $y_{P_i} = \sum_{j=1}^{t_2} y_{P_{ij}}$ as partial signature from O_i to P_{ij} .

$O_i (i = 1, \cdots, t_1)$ compute $y_{O_i} = S_{O_i} v + k_{O_i} P$ as his partial signature, publish y_{O_i}, y_{P_i} to O_1 in secure ways.

3) O_1 received y_{O_i}, y_{P_i} , verifies

$$e(y_{O_i}, P) = e(Q_{O_i}, P_{pub})^v U_{O_i}$$

$$e(y_{P_i}, P) = e(h_i (U_i + h_i Q_{O_i}), P_{pub})^v e(\sum_{j=1}^{t_2} Q_{P_{ij}}, P_{pub})^v U_i$$

If the verification is hold, computes

$$Y = \sum_{i=1}^{t_1} y_{O_i} + \sum_{i=t_1+1}^{n_1} y_{P_i} \ .$$

The proxy signature on m is $(m, m_\omega, (U, S), (v, Y))$.

E. Proxy Signature Verification

To verify a proxy signature $(m, m_\omega, (U, S), (v, Y))$ for message m , any verifier performs the following steps:

1) Verifies proxy certificate (U, S) with verification

$$e(S, P) = e(\sum_{i=1}^{n_1} Q_{O_i}, P_{pub})^{h_i'} e(\sum_{i=1}^{n_1} \sum_{j=1}^{n_2} Q_{P_{ij}}, P_{pub})^{h_i'} U$$

2)

$$D_{OP} = e(Y, P)[e(h_i \sum_{i=t_1+1}^{n_1} (U_i + h_i Q_{O_i}), P_{pub}) e(\sum_{i=1}^{t_1} Q_{O_i}, P_{pub}) e(\sum_{i=t_1+1}^{n_1} \sum_{j=1}^{t_2} Q_{P_{ij}}, P_{pub})]^{-v}$$

if and only if $v = H_1(m \| D_{OP})$ accept this proxy signature.

IV. CORRECTNESS AND SECURITY ANALYSIS

A. Correctness Analysis

1) The proxy delegation certificate is valid because of the following:

$$e(S, P) = e(\sum_{i=1}^{n_1} S_i, P) = e(\sum_{i=1}^{n_1} (s_i + \sum_{j=1}^{n_2} l_{ij}), P)$$

$$= e(\sum_{i=1}^{n_1} (S_{O_i} h_i' + k_{O_i} P) + \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} (S_{P_{ij}} h_i' + k_{P_{ij}} P), P)$$

$$= e(\sum_{i=1}^{n_1} S_{O_i} h_i', P) e(\sum_{i=1}^{n_1} k_{O_i} P, P) e(\sum_{i=1}^{n_1} \sum_{j=1}^{n_2} S_{P_{ij}} h_i', P)$$

$$e(\sum_{i=1}^{n_1} \sum_{j=1}^{n_2} k_{P_{ij}} P, P)$$

$$= e(\sum_{i=1}^{n_1} Q_{O_i}, P_{pub})^{h_i'} e(\sum_{i=1}^{n_1} \sum_{j=1}^{n_2} Q_{P_{ij}}, P_{pub})^{h_i'} U$$

2) The verifier can verify $v = H_1(m \| D_{OP})$ to prove hybrid threshold proxy signature $(m, m_\omega, (U_P, S), (v, Y))$ on m .

$$e(Y, P) = e(\sum_{i=1}^{t_1} y_{O_i} + \sum_{i=t_1+1}^{n_1} y_{P_i}, P)$$

$$= e(\sum_{i=1}^{t_1} [S_{O_i} v + k_{O_i} P] + \sum_{i=t_1+1}^{n_1} \sum_{j=1}^{t_2} y_{P_{ij}}, P)$$

$$= e(\sum_{i=1}^{t_1} S_{O_i} v, P) e(\sum_{i=1}^{t_1} k_{O_i} P, P) e(\sum_{i=t_1+1}^{n_1} \sum_{j=1}^{t_2} h_i V_{P_{ij}} \eta_{ij} v, P)$$

$$e(\sum_{i=t_1+1}^{n_1} \sum_{j=1}^{t_2} S_{P_{ij}} v, P) e(\sum_{i=t_1+1}^{n_1} \sum_{j=1}^{t_2} k_{P_{ij}} P, P)$$

$$= e(h_i \sum_{i=t_1+1}^{n_1} (U_i + h_i Q_{O_i}), P_{pub})^v e(\sum_{i=1}^{t_1} Q_{O_i}, P_{pub})^v$$

$$e(\sum_{i=t_1+1}^{n_1} \sum_{j=1}^{t_2} Q_{P_{ij}}, P_{pub})^v D_{OP}$$

$$D_{OP} = e(Y, P)[e(h_i \sum_{i=t_1+1}^{n_1} (U_i + h_i Q_{O_i}), P_{pub}) e(\sum_{i=1}^{t_1} Q_{O_i}, P_{pub})$$

$$e(\sum_{i=t_1+1}^{n_1} \sum_{j=1}^{t_2} Q_{P_i}, P_{pub})]^{-v}$$

So $v = H_1(m \| D_{OP})$

B. Security Analysis

Like the general threshold proxy signature, the hybrid threshold proxy signature scheme should satisfy the following requirement:

1) Distinguishability

The valid proxy signature contains warrant m_ω , there are the public key of original signers and proxy signers in verification equation.

2) Verifiability

In a valid proxy signature $(m, m_\omega, (U, S), (v, Y))$ on m , the verifier can be convinced of the original signer delegated the proxy signers, because there is proxy delegation certificate (U, S) in proxy signature.

3) Strong unforgeability

Firstly, in proxy signature verification, the verifier verifies proxy certificate (U, S) which contains secret, private keys of original signers and private keys of proxy signers, the others unknown these parameters. Secondly, the signers use Hess scheme to generate proxy signature, Hess scheme[6] has already verified Security in the insider-attack and outsider-attack.

4) Strong nonrepudiation

Verification equation contains original signers and proxy signers' public keys, once a proxy signer creates a valid proxy signature of an original signer, he can't repudiate the signature creation.

5) Resistance to conspiracy attack

The clerk send blind factors instead of $V_{P_{ij}} = f_i(ID_{P_{ij}})$, to the users, so anyone can't get the secret polynomial $f(x)$.

6) Prevention of misuse

The valid proxy signature contains warrant m_ω and m_ω contains the valid delegation time authorities, etc.

V. CONCLUSIONS

In this paper, we propose a new threshold proxy signature: hybrid threshold proxy signature scheme. Firstly,

we formalize a notion of security for hybrid threshold proxy signature scheme, and then we propose an identity-based hybrid threshold proxy signature scheme with the bilinear pairing. With analyzing, we find our scheme has many secure characters, such as, distinguishability, verifiability, strong unforgeability, strong nonrepudiation, resistance to conspiracy attack, prevention of misuse, etc.

ACKNOWLEDGMENT

The authors thank the editors and the anonymous referees for their valuable comments and suggestions. This work is supported by Scientific Research Fund of Heilongjiang Provincial Education Department (Grant No. 12521405).

REFERENCES

[1] Mambo M, Usuda K, and Okamoto E. Proxy signature: Delegation of the Power to sign messages. IEICE Trans. on Fundatamentals of Electronics, Communications and Computer Sciences 1996, E79-A(9): 1338-1354.

[2] Zhang K. Threshold proxy signature schemes. In: Proceedings of the Information Security Workshop (ISW'97), Lecture Notes in Computer Science, Springer-Verlag, 1998, 1396: 282-290.

[3] S Kim, S Park, and D Won. Proxy signatures, revisited. In: Proceedings of the Information and Communications Security (ICICS'97) , Lecture Notes in Computer Science, Springer-Verlag, 1997, 1334:223-232.

[4] Sun H M, Lee N Y, and Hwang T.Threshold proxy signatures.IEE Proceedings-Computers and Digital Techniques, 1999, 146(5): 259-263.

[5] Zecheng Wang, Haifeng Qian,and Zhibin Li. Hybrid proxy multisignature: A new type multi-party signature. Information Sciences, 2007, 177(6): 5638−5650.

[6] Hess F.Efficient identity based signature schemes based on pairings. Proceedings of Selected Areas in Cryptography 2002, Newfoundland, Canada, 2002, 310-324.