International Journal of Computer Theory and Engineering, Vol. 3, No. 2, April 2011
ISSN: 1793-8201

A New ID-based Designated Verifier Proxy Multi-Signature Scheme

Shenjun Cui and Fengtong Wen

***Abstract*—Proxy multi-signature allows a proxy signer to generate signatures on behalf of a group of original signers. In a designated verifier signature scheme, the signature only can be verified by a designated person. In this paper, we give the model of ID-based designated verifier proxy multi-signature and present a new ID-based designated verifier proxy multi-signature scheme. Its security is based on the computational Diffie-Hellman (CDH) problem and it is highly efficient.**

***Index Terms*—proxy multi-signature, designated verifier, ID-based**

I. Introduction

The concept of identity(ID)-based cryptosystem was first introduced by Shamir [1] in 1984 where, a user's public key is derived from his/her identity such as his/her name, address or E-mail, etc. The user's private key is generated by a private key generator (PKG). Application of identity-based crypto- system can avoid the use of public key certificates, so it can save system resources and improve the efficiency. In 2001, Boneh and Franklin [2] proposed a secure and efficient ID-based encryption scheme on the random oracle model. At present, there are many types of ID-based signature schemes, such as ID-based ring signature [3], ID-based aggregate signature [4].

In 1996, Jakobasson et al. [5] presented the concept of designated verifier signature. In designated verifier signature, only the designated verifier specified by the signer can check the validity of the signature. This kind of signature mechanism can be widely used in e-commerce and e-government, because it can solve the collision of the authen- tication and the privacy effectively. Sadeenia et al. [6] proposed the strong designated verifier signature scheme, which forces the designated verifier to use his/her private key in verification phase. Then, many designated verifier signature schemes were proposed where many ID-based signature schemes [7-9]. Recently, Kang et al. [10] pointed out Zhang-Mao's scheme [9] can not satisfy the strong property.

The proxy signature primitive and first efficient solution were first introduced by Mambo et al. [11] in 1996, which allows the original signer to delegate his/her signing right to the proxy signer. Afterwards, a lot of proxy signature schemes and some ID-based proxy signature schemes with special features were proposed by scholars at home and abroad, such as identity-based multi-proxy signature [12], identity-based strong designated verifier proxy signature [13], [14].

Proxy multi-signature is a special case of the proxy signature, and it was first proposed in [15]. A proxy multi-signature allows a signer to generate a valid signature on behalf of multiple original signers. Currently, there are many proxy multi-signature schemes based on identity [16], [17].

In this paper, based on the work of Kang et al. [10], we construct a new ID-based designated verifier proxy multi-signature scheme, then we analyze its security and efficiency.

The rest of this paper is organized as follows. Some preliminary works are described in the next section. We give a model of ID-based designated verifier proxy multi-signature in section III. In section IV, we propose a new and efficient designated verifier proxy multi-signature scheme. The analysis of security and efficiency of the scheme is given in section V. Finally, we conclude the paper in section VI.

II. Related Work

In this section, we review some basic primitives and constructions related to our scheme.

A. Bilinear Pairings

Let G_1 be a cyclic additive group generated by P, whose order is a prime q (q is a large prime), G_2 be a multiplicative cyclic group of the same order. Let $e: G_1 \times G_1 \to G_2$ be a bilinear mapping with the following properties:

1) Bilinear: For any $P, Q \in G_1, a, b \in Z_q^*$, $e(aP, bQ)$. $= e(P,Q)^{ab} = e(P, abQ) = e(abP, Q)$
2) Non-degenerate: There exists $P \in G_1, Q \in G_1$ such that $e(P,Q) \neq 1$.
3) Computable: There exists an efficient algorithm to compute $e(P,Q)$ for any $P, Q \in G_1$. Submit your manuscript electronically for review.

B. Computational Diffie-Hellman (CDH) Problem and the CDH Assumption

Definition 1. Given a group G_1 of prime order q with generator P and elements $aP, bP \in G_1$ where a, b are selected at random from Z_q^*, the CDH problem in G_1 is to compute abP.

Manuscript received June 5, 2010.

Shenjun Cui is with the School of Science, University of Jinan, Jinan, 250022 P R China (e-mail: gtzb007@ 163.com).

Fengtong Wen is with the School of Science, University of Jinan, Jinan, 250022 P R China (e-mail: wftwq@163.com).

Definition 2. We say that the (t,ε) -CDH assumption holds in a group G_1 if no algorithm running in time at most t can solve the CDH problem in G_1 with probability at least ε.

III. Model of ID-based Designated Verifier Proxy Multi-signature

In an ID-based designated verifier proxy multi-signature scheme, there are n original signers, a proxy signer, and a designated verifier. Let $A_1, A_2, ..., A_n$ be the original signers, B be the proxy signer, and C be the designated verifier. They have the identities $ID_{A_i}(i = 1, \ldots, n), ID_B, ID_C$ respectively.

Definition 3. An ID-based designated verifier proxy multi-signature scheme is a tuple (Setup, Extract, KGen, Sign, Veri):

1) Setup $(k) \to (\texttt{params}, s)$: Given a security parameter k, this algorithm outputs the public parameters params of the scheme and a master secret key s. The private key generator PKG stores the master secret key secretly and publishes the public parameters params.
2) Extract $(\texttt{params}, s, ID) \to (S_{ID}, Q_{ID})$: Given params, the master secret key s and an identity ID, this algorithm outputs the private-public key pair (S_{ID}, Q_{ID}). PKG distributes the private keys to their respective owners by a secure channel.
3) KGen $(\texttt{params}, w, S_{ID_i}, S_{ID_B}) \to s_p$: All original signers and the proxy signer input their identities $ID_{A_1}, ..., ID_{A_n}, ID_B$ and their private keys $S_{ID_{A_1}}, ..., S_{ID_{A_n}}, S_{ID_B}$, the original signers also input the delegation warrant w. This algorithm outputs the proxy key s_p.
4) Sign $(\texttt{params}, m, s_p) \to \sigma$: This is a randomized algorithm. Set m as the message to be signed, it inputs params and the proxy key s_p, and outputs a designated verifier proxy multi-signature σ.
5) Veri $(\texttt{params}, \sigma, S_{ID_C}) \to \{0,1\}$: This is a deterministic algorithm. Given a signature tuple σ, the designated verifier uses his/her private key S_{ID_C} to check its validity, and outputs 1 if σ is valid, otherwise outputs 0.

IV. Proposed ID-based Designated Verifier Proxy Multi-signature Scheme

In this section, we present an ID-based designated verifier proxy multi-signature scheme. The participants are n original signers $A_1, A_2, ..., A_n$ a proxy signer B, and a designated verifier C. The details are described as follows:

A. Setup

1) Assume k is a security parameter. G_1 and G_2 are cyclic additive group and cyclic multiplicative group of prime order q respectively, and $e: G_1 \times G_1 \to G_2$ is a bilinear map.
2) PKG picks a master secret key $s \in_R Z_q^*$ and computes $Q = sP$.
3) PKG chooses hash function $H_1: \{0,1\}^* \to G_1$, . $H_2: \{0,1\}^* \times G_2 \to G_1$
4) All public system parameters params are $(G_1, G_2, q, e, P, Q, H_1, H_2)$.

B. Extract

1) Given identities $ID_{A_i}(i = 1, ..., n)$ of n original signers, PKG generates $S_{ID_{A_i}} = sH_1(ID_{A_i})$ and sends them to the n original signers respectively as their private keys and $Q_{ID_{A_i}} = H_1(ID_{A_i})$ are the public keys of them.
2) Given the identity ID_B of the proxy signer, PKG generates $S_{ID_B} = sH_1(ID_B)$ and sends it to the proxy signer as his/her private key, and $Q_{ID_B} = H_1(ID_B)$ is the public key of him/her.
3) Given the identity ID_C of the designated verifier, PKG generates $S_{ID_C} = sH_1(ID_C)$ and sends it to the designated verifier as his/her private key, and $Q_{ID_C} = H_1(ID_C)$ is the public key of him/her.

C. KGen

1) The warrant w contains the identity information of n original signers $A_1, A_2, ..., A_n$, the proxy signer B, the designated verifier C, delegation range, delegation period, and other information of delegation.
2) Every original signer A_i signs the warrant w through the following method:

A_i chooses a random number $r_i \in Z_q^*$, and computes

$$U_i = r_i Q_{ID_{A_i}},$$
$$\sigma_i = H_2(w, e(r_i Q_{ID_B}, S_{ID_{A_i}})),$$

then, sends w and (U_i, σ_i) to the proxy signer B.

1) B checks whether the following n equations hold:

$$\sigma_i = H_2(w, e(U_i, S_{ID_B})).$$

2) If the above n equations hold, B computes proxy key s_p as follows:

B picks a random number $t \in Z_q^*$ and computes

$$\sigma = \sum \sigma_i,$$
$$U = tQ_{ID_B},$$
$$s_p = t^{-1}\sigma + S_{ID_B}.$$

D. Sign

The proxy signer B generates a designated verifier proxy multi-signature on message m:

$$V = H_2(m, w, e(tQ_{ID_C}, s_p)).$$

Finally, the designated verifier proxy multi-signature is (m, w, σ, U, V), and B sends it to the designated verifier C.

E. Veri

After receiving the signature (m,w,σ,U,V), the designated verifier C processes as follows:

1) Verifies whether m, the identities of original signers and proxy signer meet the restrictions in the warrant w. If not, stops the protocol, else continues.
2) Checks whether the following equation holds:

$$V = H_2(m,w,e(Q_{ID_C},\sigma)e(S_{ID_C},U)).$$

If the equation holds, he/she accepts the proxy signature, otherwise, rejects it.

V. Analysis of Our Scheme

A. Correctness

1) The proxy signer checks (w,U_i,σ_i) from A_i through $\sigma_i = H_2(w,e(U_i,S_{ID_B}))$, and it is valid because of the following:

$$\begin{aligned}\sigma_i &= H_2(w,e(r_iQ_{ID_B},S_{ID_{A_i}}))\\ &= H_2(w,e(r_iQ_{ID_B},sQ_{ID_{A_i}}))\\ &= H_2(w,e(r_iQ_{ID_{A_i}},sQ_{ID_B}))\\ &= H_2(w,e(U_i,S_{ID_B})).\end{aligned}$$

2) The verification of the designated verifier proxy multi-signature is correct by the following equations:

$$\begin{aligned}V &= H_2(m,w,e(tQ_{ID_C},s_p))\\ &= H_2(m,w,e(tQ_{ID_C},t^{-1}\sigma+S_{ID_B}))\\ &= H_2(m,w,e(tQ_{ID_C},t^{-1}\sigma)e(tQ_{ID_C},S_{ID_B}))\\ &= H_2(m,w,e(Q_{ID_C},\sigma)e(tQ_{ID_C},sQ_{ID_B}))\\ &= H_2(m,w,e(Q_{ID_C},\sigma)e(sQ_{ID_C},tQ_{ID_B}))\\ &= H_2(m,w,e(Q_{ID_C},\sigma)e(S_{ID_C},U)).\end{aligned}$$

B. Efficiency

Let M represent the point scalar multiplication operation in G_1, E represent the exponentiation operation in G_1, P represent the pairing operation, I represent the inverse operation. We omit the cost of integer addition, integer comparison and hash operation. In the table 1, we analyze the efficiency of our scheme, and it is easy to see our scheme is highly efficient, because there is no exponentiation operation in our scheme.

TABLE1. Computational cost of our scheme

KGen	$(2n+2)M+2nP+I$
Sign	$M+P$
Veri	$M+2P$
Total	$(2n+4)M+(2n+3)P+I$

C. Security

1) Verifiability

After the designated verifier obtains the proxy signature (m,w,σ,U,V), he/she can gain the identities of original signers and proxy signer from the warrant w, obviously, the verifier can check the signature through the verification equation.

2) Unforgeability

Any attacker wants to imitate the proxy signer B to forge a signature delegated by n original signers, he/she needs the private key S_{ID_B} of B, because the generation of the proxy signature needs the proxy key s_p, but $s_p = t^{-1}\sigma + S_{ID_B}$ contains the private key S_{ID_B} of B. Due to the private key S_{ID_B} is kept secretly by B, if the attacker wants to get it from $S_{ID_B} = sH_1(ID_B)$, it is not feasible according to the CDH assumption, so the attacker can not forge the signature. Moreover, on the basis of the CDH problem, and the difficulties of the inverse operation on bilinear pairings and the one-way hash function, if the attacker randomly chooses a message m' he/she can't generate a signature through $V' = H_2(m',w',e(t'Q_{ID_C},s_p))$ or $V' = H_2(m',w,e(Q_{ID_C},\sigma')e(S_{ID_C},U'))$ without knowing the proxy key s_p and the private key S_{ID_C} of the designated verifier.

3) Identifiability

The designated verifier can determine the identity of the proxy signer from the signature because the signature contains the warrant w which includes the information of the proxy signer.

4) Prevention of misuse

The proxy signer can't use the proxy key to generate a designated verifier proxy multi-signature for the purpose other than the n original signers delegated, because of the use of warrant signed by n original signers w.

5) Designated verification

The designated verifier C uses his/her private key to check the validity of the proxy multi-signature, hence, except the designated verifier, anyone can't check the validity of signature. Even any third party gains the private key of the designated verifier he/she can't be convinced by the validity of the signature because the designated verifier C can simulate the same transcripts in an indistinguishable way. To generate a designated verifier proxy multi-signature for any message m' which is corresponding to the warrant w', C chooses two random number r', t', and computes $\sigma' = r'Q, U' = t'Q_{ID_B}, V' = H_2(m',w',e(S_{ID_C},r'P)e(S_{ID_C},U'))$, that is, the designated verifier can simulate the transcripts indistinguishable from the signer's. Therefore, the new scheme is a strong designated verifier proxy multi-signature.

VI. Conclusion

In this paper, we constructed a new and efficient ID-based designated verifier proxy multi-signature. We analyzed its security and showed that the new scheme satisfied all the security requirements for designated verifier proxy multi-signature. In addition, our scheme is more computation- ally efficient.

Acknowledgment

The authors would like to thank the Natural Science Foundation of shandong province (No.Y2008A29), the Science and Technique Foundation of shandong province

(No.2008GG30009008), the graduate education innovation program of shandong Educational Committee (No.SDYY 08029).

REFERENCES

[1] A. Shamir, "Identity-based ryptosystems and signature schemes," G.R, Blakley, D. Chaum ed. Proceedings of the Crypto'84, LNCS 196. Berlin: Springer-Verlag, 1984, pp. 47-53.
[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing, " Advances in Cryptology-Crypto'01, LNCS 2139. Berlin: Springer-Verlag, 2001, pp. 213-229.
[3] M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong, "ID-based ring signature scheme secure in the standard model," H. Yoshiura et al. (Eds.): IWSEC 2006, LNCS 4266, 2006, pp. 1–16.
[4] C. Gentry and Z. Ramzan, "Identity-based aggregate signatures," M. Yung et al. (Eds.): PKC 2006, LNCS 3958, 2006, pp. 257–273.
[5] M. Jakobasson, K. Sako and K. R. Impaliazzo, "Designated verifier proofs and their applications," Eurocrypt 1996, LNCS 1070, Berlin: Springer-Verlag, 1996, pp. 142-154.
[6] S. Saeednia, S. Kreme and O. Markotwich, "An efficient strong designated verifier signature scheme," ICICS 2003, LNCS 2971, Berlin: Springer-Verlag, 2003, pp. 40-54.
[7] K. Kumar, G. Shailaja and A. Saxena. (2006). Identity based strong designated verifier signature scheme. Cryptography eprint Archive Report 2006/134 [Online]. Available: http://eprint.iacr.org/complete/ 2006/134.pdf.
[8] W. Susilo, F. Zhang and Y. Mu, "Identity-based strong designated verifier signature schemes," ACISP 2004, LNCS 3108, Berlin: Springer-Verlag, 2004, pp. 313-324.
[9] J. Zhang and J. Mao, "A novel ID-based strong designated verifier signature scheme," Information Science, 2008, 178, pp. 733-766.
[10] B. Kang, C. Boyd and E. Dawson, "Identity-based strong designated verifier signature schemes: Attacks and new construction," Computers and Electical Engineering, 2009, 35, pp. 49-53.
[11] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signature for delegating signing operation," Proc.3rd ACM Conference on computer and communication security, 1996, pp. 48-57.
[12] F. Cao, Z. F. Cao, "A secure identity-based multi-proxy signature scheme," Computers and Electrial Engineering, 2009, 35, pp. 86-95.
[13] L. Sunder and V. Vandani. (2006). Identity base strong designated verifier proxy signature schemes. Cryptography eprint Archive Report 2006/394 [Online]. Available: http://eprint.iacr.org/complete/2006 /394.pdf.
[14] Q. Wang and Z. F. Cao, "An identity-based strong designated verifier proxy signature scheme," Wuhan Univeraity Journal of Natural Sciences, 2006, 11(6), pp. 1633-1635.
[15] L. J. Yi, G. Q. Bai and G. Z. Xiao, "Proxy multi-signature:A new type of proxy signature schemes," Acta Electronica Sinica, 2001, 29(4), pp. 569-570.
[16] X. X. Li and K. F. Chen, "ID-based multi-proxy signature, proxy multi-signature and multi-proxy multi-signature schemes from bilinear pairings," Applied Mathematics and Computation, 2005, 169(1), pp. 437-450.
[17] F. Cao and Z. F. Cao, "A secure identity-based proxy multi-signature scheme," Information Sciences, 2009, 179, pp. 192-302.

Shenjun Cui female, born in 1988, bachelor's degree of information and computing science in the University of Jinan, Jinan, P R China.

She is a master student now. Her paper "Improvement of a forward-secure proxy signature scheme" was published in Computer Engineering and Technology (ICCET), 2010 2nd International Conference, 2010, 1, pp. 441-444. Current interests are cryptography, digital signature, proxy signature, etc.