# A Model of Bilinear-Pairings Based Designated-Verifier Proxy Signatue Scheme*

Fengying Li[1,2], Qingshui Xue[2], Jiping Zhang[1], and Zhenfu Cao[3]

[1] Department of Education Information Technology, East China Normal University, 200062, Shanghai, China
fyli@sjtu.edu.cn, jpzhang@deit.ecnu.edu.cn
[2] School of Techniques, Shanghai Jiao Tong University, 201101, Shanghai, China
xue-qsh@sjtu.edu.cn
[3] Dept. of Computer Science and Engineering, Shanghai Jiao Tong University, 200240, Shanghai, China
zfcao@cs.sjtu.edu.cn

**Abstract.** In a proxy signature scheme, one original signer delegates a proxy signer to sign messages on behalf of the original signer. When the proxy signature is created, the proxy signer generates valid proxy signatures on behalf of the original signer. Based on Cha and Cheon's ID-based signature scheme, a model of designated-verifier proxy signature scheme from the bilinear pairing is proposed. The proposed scheme can provide the security properties of proxy protection, verifiability, strong identifiability, strong unforgeability, strong repudiability, distinguishability and prevention of misuse of proxy signing power. That is, internal attacks, external attacks, collusion attacks, equation attacks and public key substitution attacks can be resisted.

## 1 Introduction

The proxy signature scheme [1], a variation of ordinary digital signature schemes, enables a proxy signer to sign messages on behalf of the original signer. Proxy signature schemes are very useful in many applications such as electronics transaction and mobile agent environment.

Mambo et al. [1] provided three levels of delegation in proxy signature: full delegation, partial delegation and delegation by warrant. In full delegation, the original signer gives its private key to the proxy signer. In partial delegation, the original signer produces a proxy signature key from its private key and gives it to the proxy signer. The proxy signer uses the proxy key to sign. As far as delegation by warrant is concerned, warrant is a certificate composed of a message part and a public signature key. The proxy signer gets the warrant from the original signer and uses the corresponding private key to sign. Since the conception of the proxy signature was brought forward, a lot of proxy signature schemes have been proposed [2]-[14][16-18].

* This paper is supported by the National Natural Science Foundation of China under Grant No. 60673079.

E. Bertino and J.B.D. Joshi (Eds.): CollaborateCom 2008, LNICST 10, pp. 416–424, 2009.

Recently, many threshold proxy signature schemes were proposed [2] [6]-[14]. In threshold proxy signature schemes, a group of n proxy signers share the secret proxy signature key. To produce a valid proxy signature on the message m, individual proxy signers produce their partial signatures on that message, and then combine them into a full proxy signature on m. In a $(t, n)$ threshold proxy signature scheme, the original signer authorizes a proxy group with n proxy members. Only the cooperation of t or more proxy members is allowed to generate the proxy signature. Threshold signatures are motivated both by the demand which arises in some organizations to have a group of employees agree on a given message or document before signing, and by the need to protect signature keys from attacks of internal and external adversaries.

In 1999, Sun proposed a threshold proxy signature scheme with known signers [9]. Then Hwang et al. [7] pointed out that Sun's scheme was insecure against collusion attack. By the collusion, any $t-1$ proxy signers among t proxy signers can cooperatively obtain the secret key of the remainder one. They also proposed an improved scheme which can guard against the collusion attack. After that, [6] showed that Sun's scheme was also insecure against the conspiracy attack. In the conspiracy attack, t malicious proxy signers can impersonate some other proxy signers to generate valid proxy signatures. To resist the attack, they also proposed a scheme. Hwang et al pointed out [8] that the scheme in [7] was also insecure against the attack by the cooperation of one malicious proxy signer and the original signer. In 2002, Li et al. [2] proposed a threshold proxy signature scheme full of good properties and performance.

The multi-proxy signature scheme was first proposed in [14]. The multi-proxy signature scheme is a special case of the threshold proxy signature scheme. The multi-proxy signature scheme allows an original signer to authorize a group of proxy members can generate the multi-signature on behalf of the original signer.

In a designated-verifier proxy signature scheme, the proxy signature will be verified only by a designated verifier chosen by the proxy signer. In 1996, Jakobsson et al. designed a designated-verifier proxy signature scheme for the first time [1]. In [21], Dai et al. proposed a designated-verifier proxy signature scheme based on discrete logarithm problems. However, in 2003, Wang pointed out that the original signer alone can forge valid proxy signatures to frame the proxy signer [16]. In 2004, Li et al. proposed a designated-verifier proxy signature scheme from bilinear pairings [17].

In 1984, Shamir proposed identity (ID)-based cryptography to simplify key management and remove the necessity of public key certificates [18]. In 2001, a practical ID-based encryption scheme was found by Boneh and Franklin, who took advantage of the properties of suitable bilinear parings (the Weil or Tate pairing) over supersingular elliptic curves [19].

Designated-verifier proxy signature scheme provides both the security properties of designated verifier signatures and those of proxy signatures. As far as the property of verifiability is concerned, the designated-verifier proxy signature scheme should meet the property of restrictive verifiability which means that only the designated verifier can verifier the validity of proxy signatures.

In 2003, Cha and Cheon [20] designed an ID-based signature scheme using GDH groups. Under the random oracle model, their scheme is proved to be secure against existential forgery on adaptively chosen messages and ID attacks supposing CDHP (Computational Diffie-Hellman Problem) is intractable.

Based on Cha and Cheon's ID-based signature scheme, a model of designated-verifier proxy signature scheme is proposed. The proposed scheme can provide the security properties of proxy protection, verifiability, strong identifiability, strong unforgeability, strong nonrepudiability, distinguishability, known signers and prevention of misuse of proxy signing power. That is, internal attacks, external attacks, collusion attacks and public key substitution attacks can be efficiently resisted.

In the paper, we organize the content as follows. In section 2, we will detail the related knowledge. We will review Cha and Cheon's ID-based signature scheme in section 3. In section 4, we will propose our model of proxy signature scheme using bilinear pairings. The correctness of the proposed scheme will discuss in section 5. Finally, the conclusion is given.

## 2 Related Knowledge

The In the section, the bilinear pairings and the related mathematical problems are introduced [19].

### 2.1 Bilinear Pairings

Let $G_1$ be a cyclic additive group produced by $P$ , with a prime order $q$ , and $G_2$ be a cyclic multiplicative group with the same order $q$ . Then, $e: G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing with the following properties:

(1) Bilinearity: $e(aP,bQ) = e(P,Q)^{ab}$ for all $P,Q \in G_1, a,b \in Z_q$ .

(2) Non-degeneracy: There exists $P,Q \in G_1$ such that $e(P,Q) \neq 1$ .

(3) Computability: There exists an efficient algorithm to calculate $e(P,Q)$ for all $P,Q \in G_1$ .

A bilinear map satisfied the three properties above is said to be an admissible bilinear map. It is well known that Weil and Tate pairings related with supersingular elliptic curves or abelian varieties can be modified to get such bilinear maps.

### 2.2 Some Mathematical Problems

(1) DLP (Discrete Logarithm Problem): Given two group elements $P$ and $Q$ , find an integer $a \in Z_q^*$ such that $Q = aP$ whenever such an integer exists.

(2) DDHP (Decision Diffie-Hellman Problem): For $a,b,c \in Z_q^*$ , given $P, aP, bP, cP$ , decide whether $c \equiv ab \bmod q$ . If it holds, $(P, aP, bP, cP)$ is called a valid Diffie-Hellman tuple.

(3) CDHP (Computational Diffie-Hellman Problem): For $a,b \in Z_q^*$ , given $P, aP, bP$ , compute $abP$ .

(4) GDHP (Gap Diffie-Hellman Problem): A class of problem where DDHP is easy while CDHP is hard.

When the DDHP is easy but the CDHP is hard on the group $G_1$, we call $G_1$ a gap Diffie-Hellman (GDH) group.

### 2.3 Basic ID-Based Designated-Verifier Proxy Signature Scheme

Usually, the kind of scheme consists of five phases: Setup, Extract, Proxy key pair generation, Proxy signature generation and proxy signature verification. In the phase of Setup, a security parameter $k$ is taken as input and system parameters which include a description of a finite message space $M$ and master key are returned. In general, the system parameters will be publicly known, while the master key will be known only to the Private Key Generator (PKG).

In the phase of Extract, the system parameters, master key and an arbitrary $ID \in \{0,1\}^*$ are taken as input and a corresponding private key $d_{ID}$ is returned as output.

In the phase of Proxy key pair generation, the original signer's private key, a warrant which specifies the original signer, the proxy signer and other application dependent delegation information explicitly, and the proxy signer's identity are taken as input, and a proxy key is returned as output. Only the proxy signer can get the knowledge of the proxy private key, while the proxy public key is public.

In the phase of Proxy signature generation, a message, the warrant, the designated verifier's identity and the proxy private key are taken as input and a designated-verifier signature is returned as output.

In the phase of Proxy signature verification, a signature and the designated verifier's private key are taken as input, and 1 or 0 is returned as output, meaning accept or reject, the information that the signature is valid with respect to a specific original signer and a proxy signer.

## 3 Review of Cha and Cheon's ID-Based Signature Scheme

The scheme consists of four phases: Setup, Extract, Sign, Verify.

(1) Setup: Select a random integer $s \in Z_q^*$ and set $P_{pub} = sP$ . $H_1 : \{0,1\}^* \to G_1^*$ and $H_2 : \{0,1\}^* \times G_1^* \to Z_q^*$ are two cryptographic hash functions. The system parameters are params= $(q, G_1, G_2, e, P, P_{pub}, H_1, H_2)$ . $s \in Z_q^*$ is the master key.

(2) Extract: For a given string $ID \in \{0,1\}^*$ , the PKG computes $Q_{ID} = H_1(ID)$, and get the corresponding private key $d_{ID} = sQ_{ID}$ .

(3) Sign: Given a secret key $d_{ID}$ and a message $m$ , select an integer $r \in Z_q^*$ randomly, compute

$$U = rQ_{ID}, h = H_2(m, U) \tag{1}$$

and

$$V = (r + h)d_{ID} . \tag{2}$$

output a signature $\sigma = (U, V)$ .

(4) Verify: To verify a signature $\sigma = (U, V)$ of a message $m$ for an identity $ID$, check whether

$$e(P,V) = e(P_{pub}, U + H_2(m,U)Q_{ID}) . \tag{3}$$

# 4 A Model of Bilinear-Pairings Based Designated-Verifier Proxy Signature Scheme

The following participants are involved in the scheme: the original group $G_o$, the proxy group $G_p$, the designated verifier or receiver Cindy, etc.

In the scheme, we specify that any $t_1$ or more out of $n_1$ original signers $(1 \le t_1 \le n_1)$ can delegate the signing capability to the proxy group on behalf of $G_o$. Similarly, any $t_2$ or more out of $n_2$ proxy signers $(1 \le t_2 \le n_2)$ can represent $G_p$ to sign a message on behalf of $G_o$. Only designated verifier $V$ can verify the proxy signature.

Throughout the paper, the system parameters are defined as follows: $m_w$ : a warrant that records the identities of the original signers in $G_o$ and the proxy signers in $G_p$, the parameters $(t_1, n_1)$, $(t_2, n_2)$, the valid delegation period, etc; AOSID: (Actual original signers' ID) the identities of the actual original signers; APSID: (Actual proxy signers' ID) the identities of the actual proxy signers.

In addition, each user $U_i$ has a randomly selected private key $d_{Ui}$ and public key $Q_{Ui}$. For each user $U_i$, its identity is $ID_i$. Suppose that $G_o = \{O_1, O_2, ..., O_{n1}\}$ and $G_p = \{P_1, P_2, ..., P_{n2}\}$ are the groups of $n_1$ original signers and $n_2$ proxy signers respectively. The proposed scheme is stated as follows.

The scheme is composed of three phases: proxy share generation phase, proxy signature generation phase and proxy signature verification phase.

## 4.1 Proxy Share Generation Phase

**Step 1.** Each of actual original signers $O_i$ $(i = 1,2,...,t_1';t_1' \ge t_1)$ selects a random integer $r_i \in Z_q^*$, calculates

$$U_i = r_i Q_{ID_{Oi}} \tag{4}$$

and sends $U_i$ to other original signers.

**Step 2.** After $O_i$ receives $O_j(j = 1,2,...,t_1'; j \ne i)$, $O_i$ computes

$$U = \sum_{i=1}^{t_1'} U_i \tag{5}$$

and

$$V_i = (r_i + H_2(m_w, AOSID, U))d_{ID_{Oi}} \tag{6}$$

passes $(m_w, AOSID, U, U_i, V_i)$ to all of proxy signers.

**Step 3.** Each of proxy signers $P_j$ $(j = 1,2,...,n_2)$ accepts $(m_w, AOSID, U, U_i, V_i)$ by checking whether the following equation holds:

$$e(P, V_i) = e(P_{pub}, U_i + H_2(m_w, AOSID, U)Q_{ID_{Oi}}) \tag{7}$$

Step 4 If all $(m_w, AOSID, U, U_i, V_i)'s$ are valid, $P_j$ computes his proxy key pair as

$$d_{Pj} = \sum_{i=1}^{t_1'} V_i + H_2(m_w, AOSID, U)d_{ID_{Pj}} \tag{8}$$

and

$$Q_{Pj} = U + H_2(m_w, AOSID, U)(\sum_{i=1}^{t_1'} Q_{ID_{Oi}} + Q_{ID_{Pj}}) . \tag{9}$$

Then $P_j$ can sign messages which conforms to $m_w$ on behalf of the original signers.

## 4.2 Proxy Signature Generation Phase

**Step 1.** Each of proxy signers $P_j$ $(j = 1,2,...,t_2'; t_2' \geq t_2)$ chooses two random integers $a_j, b_j \in Z_q^*$ and calculates

$$X_j = a_j P , \tag{10}$$

$$Y_j = (e(Q_{ID_{Cindy}}, P_{pub}))^{a_j} \tag{11}$$

and

$$B_j = b_j Q_{Pj} . \tag{12}$$

Meanwhile, he/she passes $(X_j, Y_j, B_j)$ to other proxy signers.

**Step 2.** $P_j$ also computes

$$X = \sum_{j=1}^{t_2'} X_j , \tag{13}$$

$$Y = \prod_{j=1}^{t_2'} Y_j , \tag{14}$$

$$B=\sum_{j=1}^{t_2'}B_j \tag{15}$$

and

$$S_j=(b_j+H_3(m,APSID,X,Y,B))d_{Pj}\ . \tag{16}$$

$H_3$ is a secure hash function.

**Step 4.** $P_j$ sends $(m,m_w,AOSID,APSID,X,U,B,S_j)$ to the signature combiner.

**Step 5.** Upon The signature combiner receives all of individual proxy signature $(m,m_w,AOSID,APSID,X,U,B,S_j)$ from all of proxy signers, he or she calculates $S=\sum_{j=1}^{t_2'}S_j$ , then the signature combiner passes $(m,m_w,AOSID,APSID,X,U,B,S)$ as the proxy signature on the message $m$ to the designated proxy signature verifier Cindy.

### 4.3 Proxy Signature Verification Phase

After receiving the proxy signature $(m,m_w,AOSID,APSID,X,U,B,S)$ , the designated verifier Cindy operates as follows.

**Step 1.** Check whether the message $m$ and parameters $t_1',t_2'$ conforms to the warrant $m_w$ . If not, the scheme stop. Otherwise, continue.

**Step 2.** Check whether the actual original signers and the actual proxy signers are specified as the original signers and the proxy signers, respectively, in the warrant $m_w$ . If not, stop. Otherwise, continue.

**Step 3.** Cindy calculates

$$Y'=e(d_{ID_{Cindy}},X) \tag{17}$$

and

$$Q_P=t_2'U+t_2'H_2(m_w,AOSID,U)(\sum_{i=1}^{t_1'}Q_{ID_{O_i}})+H_2(m_w,AOSID,U)\sum_{j=1}^{t_2'}Q_{ID_{P_j}}). \tag{18}$$

He or she accepts the proxy signature $(m,m_w,AOSID,APSID,X,U,B,S)$ if and only if the following congruence holds:

$$e(P,S)=e(P_{pub},B+H_3(m,APSID,X,Y',B)Q_P)\ . \tag{19}$$

## 5 Correctness of above Scheme

Theorem 1: If the tuple $(m,m_w,AOSID,APSID,X,U,B,S)$ is a signature by the above scheme, the designated verifier Cindy will accept it.

*Proof:*

$$\begin{aligned}S &= \sum_{j=1}^{t_2'} S_j \\ &= \sum_{j=1}^{t_2'} ((b_j + H_3(m, APSID, X, Y, B))d_{Pj} \\ &= \sum_{j=1}^{t_2'} (b_j d_{Pj} + H_3(m, APSID, X, Y, B)d_{Pj})) \\ &= s\sum_{j=1}^{t_2'} (b_j Q_{Pj} + H_3(m, APSID, X, Y, B)Q_{Pj}))\end{aligned} \tag{20}$$

$$\begin{aligned}&e(P, S) \\ &= e(P, s\sum_{j=1}^{t_2'} (b_j Q_{Pj} + H_3(m, APSID, X, Y, B)Q_{Pj})) \\ &= e(P_{pub}, \sum_{j=1}^{t_2'} b_j Q_{Pj} + H_3(m, APSID, X, Y, B)\sum_{j=1}^{t_2'} Q_{Pj}) \\ &= e(P_{pub}, B + H_3(m, APSID, X, Y, B)Q_P)\end{aligned} \tag{21}$$

## 6 Conclusions

In the paper, based on Cha and Cheon's ID-based signature scheme, a model of bilinear-pairings based designated-verifier proxy signature scheme is proposed.

As far as we know, it is the first model of bilinear-pairings based designated-verifier proxy signature scheme. The proposed scheme can provide the security properties of proxy protection, verifiability, strong identifiability, strong unforgeability, strong nonrepudiability, distinguishability and prevention of misuse of proxy signing power, i.e., internal attacks, external attacks, collusion attacks, equation attacks and public key substitution attacks can be resisted.

## References

1. Mambo, M., Usuda, K., Okamoto, E.: Proxy Signature for Delegating Signing Operation. In: Proceedings of the 3rd ACM Conference on Computer and Communications Security, pp. 48–57. ACM Press, New York (1996)
2. Li, J.G., Cao, Z.F.: Improvement of a Threshold Proxy Signature Scheme. Journal of Computer Research and Development 39(11), 515–518 (2002) (in Chinese)
3. Li, J.G., Cao, Z.F., Zhang, Y.C.: Improvement of M-U-O and K-P-W Proxy Signature Schemes. Journal of Harbin Institute of Technology (New Series) 9(2), 145–148 (2002)

4. Li, J.G., Cao, Z.F., Zhang, Y.C.: Nonrepudiable Proxy Multi-signature Scheme. Journal of Computer Science and Technology 18(3), 399–402 (2003)
5. Li, J.G., Cao, Z.F., Zhang, Y.C., Li, J.Z.: Cryptographic Analysis and Modification of Proxy Multi-signature Scheme. High Technology Letters 13(4), 1–5 (2003) (in Chinese)
6. Hsu, C.L., Wu, T.S., Wu, T.C.: New Nonrepudiable Threshold Proxy Signature Scheme with Known Signers. The Journal of Systems and Software 58, 119–124 (2001)
7. Hwang, M.S., Lin, I.C., Lu Eric, J.L.: A Secure Nonrepudiable Threshold Proxy Signature Scheme with Known Signers. International Journal of Informatica 11(2), 1–8 (2000)
8. Hwang, S.J., Chen, C.C.: Cryptanalysis of Nonrepudiable Threshold Proxy Signature Scheme with Known Signers. Informatica 14(2), 205–212 (2003)
9. Sun, H.M.: An Efficient Nonrepudiable Threshold Proxy Signature Scheme with Known Signers. Computer Communications 22(8), 717–722 (1999)
10. Sun, H.M., Lee, N.Y., Hwang, T.: Threshold Proxy Signature. IEEE Proceedings-computers & Digital Techniques 146(5), 259–263 (1999)
11. Zhang, K.: Threshold Proxy Signature Schemes. In: Information Security Workshop, Japan, pp. 191–197 (1997)
12. Hsu, C.L., Wu, T.S., Wu, T.C.: Improvement of Threshold Proxy Signature Scheme. Applied Mathematics and Computation 136, 315–321 (2003)
13. Tsai, C.S., Tzeng, S.F., Hwang, M.S.: Improved Nonrepudiable Threshold Proxy Signature Scheme with Known Signers. Informatica 14(3), 393–402 (2003)
14. Hwang, S.J., Shi, C.H.: A Simple Multi-Proxy Signature Scheme. In: Proceeding of the Tenth National Conference on Information Security, Taiwan (2000)
15. Jakobsson, M., Sako, K., Impagliazzo, R.: Designated verifier proofs and their application. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 143–154. Springer, Heidelberg (1996)
16. Wang, G.: Designated-verifier proxy signatures for e-commerce. In: Proc. IEEE 2004 Int. Conf. on Multimedia and Expo (ICME 2004), vol. 3, pp. 1731–1734 (2004)
17. Li, X., Chen, K., Li, S.: Designated-verifier proxy signatures for e-commerce from bilinear pairings. In: Proc. of Int. Conf. on Computer Communication, pp. 1249–1252 (2004)
18. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
19. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
20. Cha, J.C., Cheon, J.H.: An identity-based signature from gap diffie-hellman groups. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 18–30. Springer, Heidelberg (2002)
21. Dai, J., Yang, X., Dong, J.: Designated-receiverproxy signature scheme for electronic commerce. In: Proc. of IEEE International Confernece on System, Man and Cybernetics, October 5-8, vol. 1, pp. 384–389 (2003)