# A NEW EFFICIENT ID-BASED PROXY BLIND SIGNATURE SCHEME[1]

Ming Yang Wang Yumin
(*State Key Lab of Integrated Service Network, Xidian University, Xi'an 710071, China*)

**Abstract** In a proxy blind signature scheme, the proxy signer is allowed to generate a blind signature on behalf of the original signer. The proxy blind signature scheme is useful in several applications such as e-voting, e-payment, *etc.* Recently, Zheng, *et al.* presented an IDentity (ID)-based proxy blind signature. In this paper, a new efficient ID-based proxy blind signature scheme from bilinear pairings is proposed, which can satisfy the security properties of both the proxy signatures and the blind signature schemes. Analysis of the scheme efficiency shows that the new scheme is more efficient than Zheng, *et al.*'s scheme. The proposed scheme is more practical in the real world.

**Key words** Blind signature; Proxy signature; Bilinear pairing

**CLC indexs** TN918.1

**DOI** 10.1007/s11767-006-0146-x

## I. Introduction

The concept of blind signature was first introduced by Chaum[1] in 1983. A blind signature scheme is a protocol played by two parties in which a user obtains a signer's signature for a desired message and the signer learns nothing about the message. Apart from unforgeability, the blind signature schemes ensure untraceability and unlinkability. With such properties, the blind signature schemes are useful in several applications such as e-voting and e-payment.

In 1996, Mambo, *et al.*[2,3] introduced the concept of proxy signature. In this scheme, an original signer delegates his/her signing authority to the proxy signer in such way that the proxy signer can sign any message on behalf of the original signer and the verifier can verify and distinguish between normal signature and proxy signature. There are three types of proxy signature schemes[3]: full delegation, partial delegation and delegation by warrant. After Mambo, *et al.*'s first scheme was announced, many proxy signature schemes have been proposed[4,5].

Recently, the bilinear pairings[6] have been found various applications in cryptography, for they can be used to realize some cryptographic primitives that were basic tools for construction of IDentity (ID)-based cryptographic schemes. In 1984, Shamir[7] proposed the concept of ID-based public key cryptography where user's public key is indeed his identity (such as an email, IP address, *etc.*). It can simplify key management procedures in certificate-based public key systems, so it can be an alternative for certificate-based public key systems in some occasions, especially when efficient key management and moderate security are required. Since then, many ID-based schemes have been proposed.

In 2002, Tan, *et al.*[8] introduced the concept of proxy blind signature. A proxy blind signature is a digital signature which has the advantages of both the proxy signature and blind signature schemes. In a proxy blind signature scheme, the proxy signer is allowed to generate a blind signature on behalf of the original signer. Ref.[8] also defined the security properties for a good proxy blind signature scheme as follows:

(1) Distinguishability The proxy blind signatures are distinguishable from normal signatures by everyone.

(2) Verifiability From a proxy blind signature, the verifier can be convinced of the original signer's agreement on the signed message.

(3) Nonrepudiation Neither the original signer nor the proxy signer can sign message instead of the other party. Both the original signer and the proxy signer cannot deny their signatures

[1] Manuscript received date: July 17, 2006; revised date: January 16, 2007.
Supported by the National Natural Science Foundation of China (No.60473027).
Communication author: Ming Yang, born in 1979, male, Ph.D. State Key Lab of Integrated Service Network, Xidian University, Xi'an 710071, China.
Email: mingyang2001@sohu.com.

against anyone.

(4) Unforgeability Only a designated proxy signer can create a valid proxy blind signature for the original signer (even the original signer cannot do it).

(5) Unlinkability After proxy blind signature is created, the proxy signer cannot associate it with his view.

Tan, *et al.*'s scheme is a proxy blind signature scheme which is based on Schnorr blind signature. But Awasthi and Lal[9] showed a forgery attack on Tan, *et al.*'s scheme and proposed a more secure proxy blind signature scheme. Recently Sun, *et al.*[10] pointed out that neither Tan, *et al.*'s scheme nor Awasthi-Lal's scheme satisfies the unlinkability property of the proxy blind signature scheme. But they did not give an improved scheme to overcome the insecurity. In Ref.[11], a new proxy blind signature scheme based DLP is presented to overcome the insecurity. Li, *et al.*[12] proposed a secure and efficient proxy blind signature scheme using the verifiable self-certified public key. For the first time, Zhang, *et al.*[13] proposed a proxy blind signature scheme from bilinear pairings. In 2004, Zheng, *et al.*[14] proposed an ID-based proxy blind signature scheme which uses bilinear pairings of elliptic curves or hyperelliptic curves.

In this paper, we propose a new efficient ID-based proxy blind signature scheme based on Zhang, *et al.*'s ID-based blind signature[15]. Compared with the scheme in Ref.[14], our proposed scheme is more efficient than Zheng, *et al.*'s scheme in terms of computation overhead.

The rest of this paper is organized as follows: Some definitions and preliminaries are given in Section II. In Section III, a new efficient ID-based proxy blind signature scheme is proposed. In Section IV, the security and efficiency of the new scheme are analyzed. Finally Section V concludes the paper.

## II. Preliminaries

In this section, we briefly describe the basic definition and properties of bilinear pairings and related mathematical problems.

### 1. Bilinear pairings

Bilinear pairing is an important cryptographic primitive. Let $(G_1,+)$ be an additive group generated by $P$, whose order is a prime $q$, and $(G_2,\cdot)$ be a cyclic multiplicative group of the same prime order $q$. The bilinear map is given as $\hat{e}: G_1 \times G_1 \to G_2$, which satisfies the following properties:

(1) Bilinear For all $P, Q, R \in G_1$ and $a, b \in Z_q^*$ such that

$$\hat{e}(P, Q+R) = \hat{e}(P,Q)\hat{e}(P,R)$$

$$\hat{e}(P+Q, R) = \hat{e}(P,R)\hat{e}(Q,R)$$

$$\hat{e}(aP, bQ) = \hat{e}(abP, Q) = \hat{e}(P, abQ) = \hat{e}(P,Q)^{ab}$$

(2) Non-degenerate There are $P, Q \in G_1$ such that $\hat{e}(P,Q) \neq 1$.

(3) Computable There is an efficient algorithm to compute $\hat{e}(P,Q)$ for all $P, Q \in G_1$.

Such a bilinear map is called an admissible bilinear pairing. The Weil pairings and the Tate pairings of elliptic curves can be used to construct efficient admissible bilinear pairings.

### 2. Mathematical problems

Now we recall some mathematical problems in $G_1$.

(1) Discrete Logarithm Problem (DLP) Given two group elements $P$ and $Q$, find an integer $n$, such that $Q = nP$ whenever such an integer exists.

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

(3) Decision Diffie-Hellman Problem (DDHP) For all $a, b, c \in Z_q^*$, given $P, aP, bP, cP$, decide whether $c = ab \bmod q$.

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

When the DDHP is easy but the CDHP is hard on $G_1$, we call $G_1$ a Gap Diffie-Hellman (GDH) group. GDH group can be found on supersingular elliptic curves or hyperelliptic curves over finite field, and the bilinear pairings can be derived from the Weil or Tate pairing. We assume through this paper that CDHP and DLP are intractable, which means there is no polynomial time algorithm to solve CDHP and DLP with non-negligible probability.

## III. Our Proposed Scheme

In this section, we propose an ID-based proxy blind signature scheme from bilinear pairings,

which consists of five procedures: setup, extract, proxy phase, signing phase, and verification phase. We assume there is a Key Generation Center (KGC) that establishes the ID-based cryptosystem and generates private keys for users.

**1. Setup**

Initially, KGC selects $q$, $G_1$, $G_2$ and $\hat{e}$, as defined in the previous section. The KGC chooses $P$ as the generator of $G_1$ and defines two cryptographic hash functions $H_1 : \{0,1\} \to Z_q^*$ and $H_2 : \{0,1\} \to G_1$. KGC chooses a random number $s \in_R Z_q^*$ and sets $P_{\text{pub}} = sP$. The center publishes system parameters $\text{params} = \{q, G_1, G_2, \hat{e}, P, H_1, H_2, P_{\text{pub}}\}$, and keeps $s$ as the master-key, which is known only by itself.

**2. Extract**

A user submits his/her identity information ID to KGC, KGC computes the user's public key as $\text{PK}_{\text{ID}} = H_2(\text{ID})$, and returns $\text{SK}_{\text{ID}} = s\text{PK}_{\text{ID}}$ to the user as his/her private key. In this way, the public and private key of the original signer $A$ and proxy signer $B$ can be denoted as $\text{PK}_A$, $\text{SK}_A$ and $\text{PK}_B$,$\text{SK}_B$.

**3. Proxy phase**

(1) Proxy generation The original signer $A$ creates a warrant $m_w$ where there is an explicit description of the delegation relation including the identity of the original signer and the proxy signer, the message to be signed, and so on. $A$ chooses a random number $r \in_R Z_q^*$, and computes $R = rP$, $h = H_1(R \,||\, m_w)$, $S = rP_{\text{pub}} + h \cdot \text{SK}_A$.

(2) Proxy delivery The original signer $A$ sends $(m_w, R, S)$ to the proxy signer $B$, and makes $(m_w, R)$ public.

(3) Proxy verification The proxy signer $B$ computes $h = H_1(R \,||\, m_w)$, and checks whether the following equation holds or not

$$\hat{e}(P,S) = \hat{e}(P_{\text{pub}}, R + h \cdot \text{PK}_A)$$

If it holds, the proxy signer $B$ computes the proxy key pair as

$$\text{SK}_{\text{pr}} = S + h \cdot \text{SK}_B,\ \text{PK}_{\text{pr}} = R + h \cdot (\text{PK}_A + \text{PK}_B)$$

Otherwise, $B$ rejects it. In the later case he either requests for another key, or simply stops the protocol.

**4. Signing phase**

When the user $C$ wants the proxy signer $B$ to blindly sign a message $m$, they execute the ordinary signing operation using $\text{SK}_{\text{pr}}$ as a private key; and the created proxy blind signature by $B$ on $m$ is $(m, m_w, R, \sigma_{\text{SK}_{\text{pr}}}(m))$, $\sigma_{\text{PK}_{\text{pr}}}(m)$ is generated as follows:

(1) The user $C$ computes the proxy public key

$$\begin{aligned}\text{PK}_{\text{pr}} &= R + h \cdot (\text{PK}_A + \text{PK}_B) \\ &= R + H_1(R \,||\, m_w) \cdot (\text{PK}_A + \text{PK}_B)\end{aligned}$$

(2) The proxy signer $B$ randomly chooses a number $k \in_R Z_q^*$, and computes $K = kP$, then sends $K$ to the user $C$.

(3) The user $C$ chooses randomly $\alpha, \beta \in_R Z_q^*$, and computes $U = \alpha K + \alpha\beta\text{PK}_{\text{pr}}, h' = \alpha^{-1}H_1(m \,||\, U) + \beta$, then $C$ sends $h'$ to the proxy signer $B$.

(4) After receiving $h'$, the proxy signer $B$ computes $V' = kP_{\text{pub}} + h' \cdot \text{SK}_{\text{pr}}$, and sends it to the user $C$.

(5) The user $C$ computes $V = \alpha V'$.

Then $(m, m_w, R, \sigma_{\text{SK}_{\text{pr}}}(m) = (U,V))$ is the proxy blind signature of the message $m$.

**5. Verification phase**

A verifier can verify the validity of the proxy blind signature as follows:

Compute

$$\begin{aligned}\text{PK}_{\text{pr}} &= R + h \cdot (\text{PK}_A + \text{PK}_B) \\ &= R + H_1(R \,||\, m_w) \cdot (\text{PK}_A + \text{PK}_B)\end{aligned}$$

Accept the signature if and only if

$$\hat{e}(V,P) = \hat{e}(U + H_1(m \,||\, U) \cdot \text{PK}_{\text{pr}}, P_{\text{pub}}) \qquad (1)$$

## IV. Analysis of the Proposed Scheme

**1. Correctness**

The correction of the proxy blind signature can be justified by the following equation:

$$\begin{aligned}\hat{e}(V,P) &= \hat{e}(\alpha V', P) \\ &= \hat{e}(\alpha(kP_{\text{pub}} + h'\text{SK}_{\text{pr}}), P) \\ &= \hat{e}(\alpha kP_{\text{pub}} + \alpha h'(rP_{\text{pub}} + h\text{SK}_A + h\text{SK}_B), P) \\ &= \hat{e}(\alpha ksP + \alpha h'(rsP + hs\text{PK}_A + hs\text{PK}_B), P) \\ &= \hat{e}(s(\alpha kP + \alpha h'(R + h\text{PK}_A + h\text{PK}_B)), P) \\ &= \hat{e}(\alpha kP + \alpha h'\text{PK}_{\text{pr}}, sP) \\ &= \hat{e}(\alpha K + \alpha(\alpha^{-1}H_1(m \,||\, U) + \beta)\text{PK}_{\text{pr}}, P_{\text{pub}}) \\ &= \hat{e}(\alpha K + (H_1(m \,||\, U) + \alpha\beta)\text{PK}_{\text{pr}}, P_{\text{pub}})\end{aligned}$$

$$= \hat{e}(\alpha K + \alpha\beta \mathrm{PK}_{\mathrm{pr}} + H_1(m \,||\, U)\mathrm{PK}_{\mathrm{pr}}, P_{\mathrm{pub}})$$
$$= \hat{e}(U + H_1(m \,||\, U)\mathrm{PK}_{\mathrm{pr}}, P_{\mathrm{pub}})$$

## 2. Security analysis

(1) Distinguishability In the proposed scheme, when the proxy blind signature $(m, m_w, R, U, V)$ is verified, not only the proxy signer but also the original signer's public keys are used in the verification Eq.(1), so we can regard it as a proxy signature, not a normal signature. Thus anyone can distinguish the proxy blind signature from normal signature.

(2) Verifiability In the proposed scheme, on one hand, the verifier can know who are the original signer and proxy signer from the warrant $m_w$. On the other hand, when the proxy blind signature is verified, the public keys of the original signer and proxy signer are used in Eq.(1). Thus the original signer cannot deny having delegated his signing authority to the designated proxy signer. That is to say, any verifier can be convinced of the original signer's agreement on the signed message.

(3) Nonrepudiation When the proxy blind signature $(m, m_w, R, U, V)$ is verified, the warrant $m_w$ is checked and the public keys $\mathrm{PK}_A$ and $\mathrm{PK}_B$ of the original signer and the proxy signer are used in Eq.(1). So the proxy signer cannot deny having signed the message $m$ on behalf of the original signer to any person.

(4) Unforgeability Firstly, as far as the known proxy blind signature $(m, m_w, R, U, V)$ is concerned, if the original signer $A$ can forge $(m, m_w, R, U', V)$, $(m, m_w, R, U, V')$ or $(m, m_w, R, U', V')$, from Eq.(1), $A$ has to solve the discrete logarithm problem and break the hash function $H_1$. However, we have known that it is impossible for $A$. Therefore, for the original signer $A$, proxy blind signature cannot be forged in the proposed scheme. Secondly, the third party cannot forge valid proxy blind signatures as the third party knows less than the original signer $A$. The original signer $A$ can not generate valid proxy blind signatures, neither can the third party.

(5) Unlinkability Unlinkability is an important security property in blind signature scheme, which implies that when the signature is verified, the proxy signer $B$ knows neither the message nor the resulting signature, *i.e.* blindness. In the proposed scheme, the proxy signer $B$ can get a valid signature $(m, m_w, R, U, V)$ and the view $(K, h', V')$, there is always a unique pair of blinding factors $\alpha, \beta \in Z_q^*$. Since the blinding factors $\alpha, \beta \in Z_q^*$ are chosen randomly, the proxy signer $B$ cannot get the link between the proxy blind signature and his view. Given a valid proxy blind signature $(m, U, V)$, *i.e.*, $\hat{e}(V, P) = \hat{e}(U + H_1(m \,||\, U) \cdot \mathrm{PK}_{\mathrm{pr}}, P_{\mathrm{pub}})$ and the view $(K, h', V')$, it is obvious that $\alpha \in Z_q^*$ existed uniquely from $V = \alpha V'$ denoted by $\log_{V'} V$. So we can get $\beta = h' - \log_{V'} V \cdot H_1(m \,||\, U)$ from $h' = \alpha^{-1} H_1(m \,||\, U) + \beta$ and it is unique in $Z_q^*$. To show that such $\alpha, \beta$ satisfy $U = \alpha K + \alpha\beta \mathrm{PK}_{\mathrm{pr}}$, we only need to show that $\alpha, \beta$ satisfy $\hat{e}(U, P_{\mathrm{pub}}) = \hat{e}(\alpha K + \alpha\beta \mathrm{PK}_{\mathrm{pr}}, P_{\mathrm{pub}})$.

$$\begin{aligned}
&\hat{e}(\alpha K + \alpha\beta \mathrm{PK}_{\mathrm{pr}}, P_{\mathrm{pub}}) \\
&\quad = \hat{e}(\log_{V'} V \cdot K + \log_{V'} V \\
&\qquad \cdot (h' - \log_{V'} V \cdot H_1(m \,||\, U))\mathrm{PK}_{\mathrm{pr}}, P_{\mathrm{pub}}) \\
&\quad = \hat{e}(\log_{V'} V \cdot kP + \log_{V'} V \cdot h' \cdot \mathrm{PK}_{\mathrm{pr}}, P_{\mathrm{pub}}) \\
&\qquad \cdot \hat{e}(H_1(m \,||\, U)\mathrm{PK}_{\mathrm{pr}}, P_{\mathrm{pub}})^{-1} \\
&\quad = \hat{e}(\log_{V'} V \cdot (kP_{\mathrm{pub}} + h'\mathrm{SK}_{\mathrm{pr}}), P) \\
&\qquad \cdot \hat{e}(V, P)^{-1} \hat{e}(U, P_{\mathrm{pub}}) \\
&\quad = \hat{e}(\log_{V'} V \cdot V', P) \hat{e}(V, P)^{-1} \hat{e}(U, P_{\mathrm{pub}}) \\
&\quad = \hat{e}(U, P_{\mathrm{pub}})
\end{aligned}$$

Thus the blinding factors $\alpha, \beta$ always exist which lead to the same relation defined in the proxy blind signature issuing protocol regardless of the values of $(m, U, V)$ and $(K, h', V')$. Therefore, our proposed scheme is unconditional blind.

All in all, our proposed scheme can provide all of security properties of proxy blind signature scheme. In other words, the new scheme is secure and practical in the real world.

## 3. Efficient analysis

We compare the proposed identity-based proxy blind signature scheme with Zheng, *et al.*'s scheme[14] from the computation overhead and summarize the results in Tab.1 (we ignore the operation of hash in all schemes). We denote pa as the pairing operation, psm as the point scalar multiplication on $G_1$, ad as the point addition on $G_1$, mu as the multiplication in $Z_q$, div as the division in $Z_q$, $\mathrm{mu}_2$ as the multiplication in $G_2$.

**Tab.1 Comparison of the proposed scheme and, Zheng, *et al.*'s scheme[14]**

| Phase | Zheng, *et al.*'s scheme[14] | The proposed scheme |
|---|---|---|
| Proxy generation | 3psm+1ad+1pa | 3psm+1ad |
| Proxy verification | 1psm+1mu$_2$+4pa | 1psm+1ad+2pa |
| Proxy blind signature generation | Proxy signer: 3psm+1ad<br>User: 3psm+3ad+1ps | Proxy signer: 3psm+1ad<br>User: 3psm+1ad+1mu+1div |
| Proxy blind signature verification | 1psm+1mu$_2$+2pa | 1psm+1ad+2pa |

From Tab.1, it is easy to see that the proposed scheme is more efficient than Zheng, *et al.*'s scheme[14]. We note that the computation of the pairing is the most-consuming. Although there have been many papers discussing the complexity of pairings and how to speed up the pairing computation, the pairing computation is the operation which by far takes the most running time. In both proxy generation phase and proxy verification phase, the computation cost of our scheme is less than that of the Zheng, *et al.*'s scheme; in proxy blind signature generation phase, the user needs not compute the pairing in our scheme, but needs one pairing in Zheng, *et al.*'s scheme[14]. To sum up, our scheme outperforms Zheng, *et al.*'s scheme.

## V. Conclusions

ID-based public key cryptosystem can be an alternative for certificate-based public key infrastructures. In this paper, we propose a new efficient ID-based proxy blind signature scheme. The proposed scheme can fulfill the security properties of both proxy signature and blind signature schemes. Zheng, *et al.*'s scheme and our proposed scheme are compared according to the computation overhead. Our ID-based proxy blind signature scheme is more efficient than Zheng, *et al.*'s scheme. In a word, the proposed scheme is more practical in the real world.

## References

[1] D. Chaum. Blind signatures for untraceable payments. Advances in Cryptology-Crypto'82, Santa Barbara, California, USA, August 1983, 199–203.

[2] M. Mambo, K. Usuda, and E. Okamoto. Proxy signatures: Delegation of the power to sign messages. *IEICE Trans. on Fundamentals*, **E79-A**(1996)9, 1338–1353.

[3] M. Mambo, K. Usuda, and E. Okamoto. Proxy signatures for delegating signing operation. Proceedings of the 3rd ACM Conference on Computer and Communications Security-CCS'96, New Delhi, India, March 14–16, 1996, 48–57.

[4] S. Kim, S. Park, and D. Won. Proxy signatures, revisited. Proceedings of the first International Conference on Information and Communications Security-ICICS'97, LNCS 1334, Beijing, P. R. China, November 11–13, 1997, 223–232.

[5] T. Okamoto, M. Tada, and E. Okamoto. Extended proxy signatures for smart cards. Proceedings of the 2nd International Information Security Workshop-ISW'99, LNCS 1729, Kuala Lumpur, Malaysia, November 6–7, 1999, 247–258.

[6] S. D. Galbraith, K. Harrison, and D. Soldera. Implementing the Tate pairing. Proceedings of the 5th International Algorithmic Number Theory Symposium-ANTS-V'02, LNCS 2369, Sydney, Australia, July 7–12, 2002, 324–337.

[7] A. Shamir. Identity-based cryptosystems and signature schemes. Advances in Cryptology-Crypto'84, LNCS 196, Santa Barbara, California, USA, August 19–22, 1984, 47–53.

[8] Z. Tan, Z. Liu, and C. Tang. Digital proxy blind signature schemes based on DLP and ECDLP. MM Research Preprints, MMRC, AMSS, Academia Sinica, Beijing, December 21, 2002, 212–217.

[9] A. K. Awasthi and S. Lal. Proxy blind signature scheme. *JFCR Trans. on Cryptology*, **2**(2005)1, 5–11.

[10] H. M. Sun, B. T. Hsieh, and S. M. Tseng. On the security of some proxy signature schemes. *Journal of System and Software*, **74**(2005)3, 297–302.

[11] Shaobin Wang, Hong Fan, and Guohua Cui. Secure efficient proxy blind signature schemes based DLP. Proceedings of the 7th IEEE International Conference on E-Commerce Technology-CEC'05, Münich, Germany, July 19–22, 2005, 452–455.

[12] Jiguo Li and Shuhong Wang. New efficient proxy blind signature scheme using verifiable self-certified public key. *International Journal of Network Security*, **4**(2007)2, 193–200.

[13] F. G. Zhang, S. N. Reihanch, and C. Y. Lin. New proxy new proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairings. Cryptology ePrint Archive, Report 2003/104.

http://eprint.iacr.org/2003/104.

[14] Zheng Dong, Huang Zheng, Kefei Chen, *et al.* ID-based proxy blind signature. Proceedings of the 18th International Conference on Advanced Information Networking and Applications-AINA'04, Fukuoka, Japan, March 29–31, 2004, vol.2, 380–383.

[15] F. G. Zhang and K. Kim. Efficient ID-based blind signature and proxy signature from pairings. Proceedings of the 8th Australasia Conference on Information Security and Private-ACISP'03, LNCS 2727, Wollongong, Australia, July 9–11, 2003, 312–323.