ID-based Weak Blind Signature From Bilinear Pairings

Ze-mao Zhao
School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, P.R.China
(E-mail:zhaozemao@163.com)
(Received April 2, 2006; revised May 31, 2006, and accepted Dec. 7, 2007)

Abstract

In a blind signature scheme, the user can get a signature $sig(m)$ on message m generated from the signer's blind signature $sig(m')$ on blinded message m', but the signer can't know the contents of the message m. When the signature $sig(m)$ is revealed to public after that have been signed, if the signer can find the linkage between the signature $sig(m)$ and the blind signature $sig(m')$ on blinded message m, the signature is called as weak blind signature, otherwise, called as strong blind signature. In this paper, by using the bilinear pairings, a new ID-based weak blind signature was proposed, which is based on the Discrete Logarithm Problem and Gap Diffie-Hellman Problem. The proposed scheme use ID-based public key instead of public key of digital certification, can effectively simplify the procedure of public key management and reduce the disk storage space. In addition, by choosing different equations, we gained corresponding weak blind signature schemes respectively. Finally, the security of the proposed scheme was discussed.

Keywords: bilinear pairings, ID-based cryptosystem, strong blind signature, weak blind signature

1 Introduction

Blind signature, introduced by Chaum [4], allow a receiver to obtain a signature on message without revealing anything about the message to the signer. Blind signature play an important role in plenty of applications such as electronic voting, electronic cash where anonymity is of great concern. About the formal definition and security of blind signature schemes, refer to [9, 11].

In a certificate-based public key system, before using the public key of a user, the participants must verify the certificate of the user at first. As a consequence, this system requires a large storage and computing time to store and verify each user's public key and the corresponding certificate. In 1984, Shamir [12] proposed ID-based encryption and signature schemes to simplify key management procedures in certificate-based public key setting. This scheme allows a user to use his/her identity as the public key. In other words, the user's public key can be calculated directly from his/her identity rather than being extracted from a certificate issued by a certificate authority (CA). ID-based public key setting can be a good alternative for certificate-based public key setting, especially when efficient key management and moderate security are required. Since then, many ID-based encryption and signature schemes have been proposed, but most of them are impractical for low efficiency. Recently, the bilinear pairings have been found various applications in cryptography, they can be used to realize some cryptographic primitives that were previously unknown or impractical [1, 2, 3]. More precisely, they are basic tools for constructing various signature schemes including ID-based blind signature schemes and it's variations [5, 6, 7, 8, 13].

This paper gave an ID-based weak blind signature scheme from bilinear pairings and discussed the security requirements, and extended it by choosing different parameter in signing equations. So a class of weak blind signature schemes was gained.

2 Basic Concepts On Bilinear Pairings

In this section, we briefly described the basic concept and properties of bilinear pairings and gap Diffie-Hellman group. We also present the ID-based public key setting based on bilinear pairing.

2.1 Bilinear Pairings

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q: A bilinear pairing is a map $e : G_1 \times G_1 \to G_2$ with the following properties:

1) Bilinear: $e(aP, bP) = e(P, Q)^{ab}$;

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

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

2.2 Gap Diffie-Hellman Group

Now we describe some mathematical problems in G_1.

- Discrete Logarithm Problem (DLP): Given two group elements p and Q, to find an integer $n \in Z_q^*$, such that $Q = nP$ whenever such an integer exists.
- Computational Diffie-Hellman Problem (CDHP): Given $P, aP, bP \in G_1$ for $a, b \in Z_q^*$, to compute abP.
- Decision Diffie-Hellman Problem (DDHP): Given $P, aP, bP, cP \in G_1$ for $a, b, c \in Z_q^*$,to decide whether $c = ab \bmod q$.
- Diffie-Hellman Problem (DDHP): Given $P, aP, bP \in G_1$, it is easy to decide whether $c = ab \bmod q$, but it is difficult to compute abP. In other words, DDHP is easy, but CDHP is difficult on the group G_1, so we called G_1 a Gap Diffie-Hellman Group, Such groups can be found on supersingular elliptic curves or hyperelliptic curves over finite field, and the bilinear parings can be derived from the Weil or Tate pairing, referred to [6, 10] for more details.

We also point out that there exists a difficult problem to solve the divergence algorithm of bilinear pairings, i.e., given $P \in G_1$, $r \in G_2$, to find an element $Q \in G_1$, such that $r = e(P, Q)$ whenever such an element exists.

2.3 ID-Based Public Key Setting

In ID-based public key cryptosystem(simply IDPKC), user's public keys are predetermined by information that uniquely identifies them, such as name, address and email address, etc, rather than an arbitrary string. The private key of the user is calculated by a trusted party, called PKG and send to the user via a secure channel.

ID-based public key setting involves a PKG and users. The basic operation consists of Setup and Private Key Extraction (simply Extract). When we use bilinear pairings to construct IDPKC, Setup and Extract can be implemented as follows:

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q: A bilinear pairing is a map $e : G_1 \times G_1 \to G_2$. Define two cryptographic hash functions $H : 0, 1^* \to Z^q$ and $H_1 : 0, 1^* \to G_1$.

- Setup: PKG chooses a random number $s \in Z_q^*$ and sets $P_{pub} = sP$. The center publishes system parameters $params = G_1, G_2, e, q, P_{pub}, H, H_1$, and keeps s as the master key, which is known only by itself.
- Extract: A user submits his/her identity information ID to PKG. PKG computes the user's public key as $Q_{ID} = H_1(ID)$, and returns $S_{ID} = sQ_{ID}$ to the user as his/her private key and sends it to the user via a secure channel.

3 ID-Based Weak Blind Signature Scheme

The concept of blind signature provides anonymity of user in applications such as electronic voting and electronic payment system, etc. In contrast to regular signature schemes, a blind signature scheme is an interactive two-party protocol between a user and a signer. It allows the user to obtain a signature of a message in a way that the signer learns neither the message nor the resulting signature. The latter property means that the signer doesn't find the linkage between the signature $Sig(m^1)$ on blinded message m^1 and the signature $Sig(m)$ on message m which generates from $Sig(m^1)$ by the user after the signature $Sig(m)$ is revealed. So using this linkage, we classify the blind signature into weak blind signature and strong blind signature, i.e., weak blind signature means that the signer can find the linkage, and strong blind signature means that the signer cannot find the linkage.

3.1 Our Scheme

In this section, we present an ID-based weak blind signature scheme, which can be regarded as blind version of ElGamal signature based on the DLP. The proposed scheme consists of the following four algorithms.

System Parameter Setup: This procedure is same to Setup above in Section 2.3.

Extract: Given a user's identity ID, which implies the public key $Q_{ID} = H_1(ID)$, the private key $S_{ID} = sQ_{ID}$.

Blind Signature: Suppose that m is the message to be signed. Let $g \in G_2$ and $g \in e(P, P_{pub})$. The signature procedure is describe as following:

- The signer randomly chooses $k \in_R Z_q^*$, computes $r' = g^k$, and sends r' to the user;
- (Blinding) The user randomly chooses $a, b \in_R Z_q^*$, computes $r = (r')^a g^b$ and $m' = a^{-1} r (r')^{-1} m$, and sends m' to the signer;
- (Signing) The signer computes $S' = m' r' S_{ID} - kP_{pub}$, then sends S' to the user;
- (Unblinding) The user computes $S = aS' - bP_{pub}$. Hence, the final signature is $sig_m = (r, s)$.

Verification: Accept the signature if and only if $e(S, P) = r^{-1} e(Q_{ID}, P_{pub})^{mr}$. The verification of the signature is justified by the following equations:

$$\begin{aligned} e(S, P) &= e(aS' - bP_{pub}, P) \\ &= e(am'r'S_{ID} - akP_{pub}, P) \\ &= e(mrS_{ID}, P) e((ak + b)P_{pub}, P)^{-1} \\ &= r^{-1} e(Q_{ID}, P_{pub}^{mr}). \end{aligned}$$

Table 1: Equations in weak signature scheme

No.	Signing equation	Blinded message	Signature variable	Verifying equation
1	$S' = m'r'S_{ID} - kP_{pub}$	$m' = a^{-1}r(r')^{-1}m(\mathrm{mod}q)$	$S = aS' - bP_{pub}$	$e(S,P) = e(Q_{ID}, P_{pub})^{mr}r^{-1}$
2	$S' = m'r'S_{ID} + kP_{pub}$	$m' = a^{-1}r(r')^{-1}m(\mathrm{mod}q)$	$S = aS' + bP_{pub}$	$e(S,P) = e(Q_{ID}, P_{pub})^{mr}r$
3	$S' = r'S_{ID} + km'P_{pub}$	$m' = ar(r')^{-1}m(\mathrm{mod}q)$	$S = r(r')^{-1}S' + mbP_{pub}$	$e(S,P) = e(Q_{ID}, P_{pub})^{r}r^{m}$
4	$S' = r'S_{ID} - km'P_{pub}$	$m' = ar(r')^{-1}m(\mathrm{mod}q)$	$S = r(r')^{-1}S' - mbP_{pub}$	$e(S,P) = e(Q_{ID}, P_{pub})^{r}r^{-m}$
5	$S' = m'S_{ID} + kr'P_{pub}$	$m' = a^{-1}r'r^{-1}m(\mathrm{mod}q)$	$S = ar(r')^{-1}S' + brP_{pub}$	$e(S,P) = e(Q_{ID}, P_{pub})^{m}r^{r}$
5[1]	$S' = m'S_{ID} + kr'P_{pub}$	$m' = a^{-1}r'm(\mathrm{mod}q)$	$S = a(r')^{-1}S' + bP_{pub}$	$e(S,P) = e(Q_{ID}, P_{pub})^{m}r$
6	$S' = m'S_{ID} - kr'P_{pub}$	$m' = a^{-1}r'r^{-1}m(\mathrm{mod}q)$	$S = ar(r')^{-1}S' - brP_{pub}$	$e(S,P) = e(Q_{ID}, P_{pub})^{m}r^{-r}$
6[1]	$S' = m'S_{ID} - kr'P_{pub}$	$m' = a^{-1}r'm(\mathrm{mod}q)$	$S = a(r')^{-1}S' - bP_{pub}$	$e(S,P) = e(Q_{ID}, P_{pub})^{m}r^{-1}$

3.2 Security Analysis

1) Blindness. To the signer, he/she can't learn the contents of original m, since he/she only get the blinded message m'. On the other hand, it is impossible to solve m from the equation $m' = a^{-1}r(r')^{-1}m$.

2) Linkage. In the weak blind signature scheme described above, if signer keeps the (m',r',S',k') secret, when the user make the $sig(m) = S$ public, the signer computes $a' = r(r')^{-1}m(m')^{-1}$, $b'P_{pub} = a'S' - S$, and then computes $r = (r')^{a'}e(P, b'P_{pub})$, if $r = r'$ is correct, he/she can get conclusion that $a' = a, b' = b$, and determines that $Sig(m)$ is linked to $Sig(m')$. Of course, if the above signer is real participator, the equation $r = (r')^{a'}$ should hold true. All of these can explain the above conclusion.

3) Suppose the attacker intercept the signature $Sig(m) = (r, S)$, it is impossible for him/her to gain the private key of signer. Since $S = aS' - bP_{pub}$, where there exist three unknown variables a, b and S_{ID}, he/she faces DLP on elliptic curve to solve S_{ID} from the equation.

4 Extension of the Scheme

In the blind signature phase of the scheme in Section 3.1, the signing equation is $S' = m'r'S_{ID} - kP_{pub}$, however, we can choose different parameters to gain different signing equations. For example, the signing equations can be chose as $S' = m'r'S_{ID} + kP_{pub}$, $S' = r'S_{ID} + km'P_{pub}$, $S' = r'S_{ID} - km'P_{pub}$, $S' = m'S_{ID} + kr'P_{pub}$, $S' = m'S_{ID} - kr'P_{pub}$. Hence, we gained corresponding weak blind signature schemes, the main equations and variables of these schemes were listed in a Table 1.

Specially, No.1 in Table 1 was the proposed weak blind signature scheme in Section 3, all procedures of other weak blind signature schemes were the same like as No.1, only to choose their equations according with Table 1.

We can suppose there are many methods to construct weak blind signature, only the necessary condition to be satisfied is the linkage. However, some combination of parameter couldn't form a weak blind signature scheme, such as $S' = km'S_{ID} - r'P_{pub}$, there aren't verifying equation under this situation.

5 Conclusions

To the weak blind signature, there are many applications in the fields where the anonymity is needed. Suppose an old man writes his will, i.e. the will is an important file, he need a lawyer to sign his will. After he died, the will became very useful. So he ask a lawyer to sign, but doesn't hope the lawyer to know the content of the will. Thus the blind signature can be used in this situation.

For the verifying equation $e(S,P) = r^{-1}e(Q_{ID}, P_{pub})^{mr}$, public key Q_{ID} of the signer and public key P_{pub} of trust party PKG were required, this explains that the user's will is to be signed by the signer. When the dispute happened, the signer can pursue and prove that the signature has been signed by himself/herself with the middle variable (m', r', S', k).

On the other hand, weak blind signature may use to create proxy signature [10], and strong blind signature can apply to e-commerce or e-voting, in which anonymity of requester and confidentiality of message are required, but the signer can't pursue the owner of the message, in this condition, when the dispute happened, anyone except owner of the message couldn't find the real owner.

References

[1] A. Boldyreva, "Efficient threshold signature, multisignature and blind signature schemes based on the Gap-Diffie-Hellman-group signature scheme,". *Public Key Cryptography - PKC 2003,* LNCS 2139, pp. 31-46, Springer-Verlag, 2003.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *Advances in Cryptology-Crypto 2001,* LNCS 2139, pp. 213-229, Springer-Verlag, 2001.

[3] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *Advances in Cryptology-Asiacrypt 2001,* LNCS 2248, pp. 514-532, Springer-Verlag, 2001.

[4] D. Chaum, "Blind signature for untraceable payments," *Advances in Cryptology-Eurocrypt'82,* pp. 199-203, Plenum Press, 1982.
[5] J.C. Cha and J.H. Cheon, "An identity-based signature from gap Diffie-Hellman groups," *Public Key Cryptography - PKC 2003,* LNCS 2139, pp. 18-30, Springer-Verlag, 2003.
[6] S.M. Chow and C.K.Hui et.al, "Two improved partially blind signature schemes from bilinear pairings," *ACISP 2005,* LNCS3574, pp. 316-328, Springer-Verlag, 2005.
[7] X. Chen, F. Zhang and S. Liu, "ID-based restrictive partially blind signature," *IACR ePrint Archive,* http://eprint.iacr.org/2005/319.
[8] F. Hess, "Efficient identity based signature schemes based on pairings," *SAC 2002,* LNCS 2595, pp. 310-324, Springer-Verlag, 2002.
[9] A. Juels, M. Luby and R. Ostrovsky, "Security of blind digital signatures," *Advances in Cryptology-Crypto 97,* LNCS 1294, pp.150-164, Springer-Verlag, 1997.
[10] Qi Ming, Xu botong, "New proxy signatures based on weak blind signature scheme," *Computer Engineering and Design,* vol. 21, no. 5, pp. 57-60, 2001.
[11] C. P. Schnorr, "Security of blind discrete log signatures against interactive attacks," *ICICS 2001,* LNCS 2229, pp.1-12, Springer-Verlag, 2001.
[12] A. Shamir. "Identity-based cryptosystems and signature schemes," *Advances in Cryptology-Crypto 84,* LNCS 196, pp.47-53, Springer-Verlag, 1984.
[13] F. Zhang and K. Kim, "ID-based blind signature and ring signature from pairings," *Advances in Cryptology - ASIACRPT'02,* pp. 533-547, Springer-Verlag, New Zealand, 2002.
[14] F. Zhang and K. Kim, "Efficient ID-based blind signature and proxy signature from bilinear pairings," *In Advances in Cryptology-Crypto's2003,* LNCS2727, pp. 312-323, Springer-Verlag, 2003.

Ze-mao Zhao received his B.S. degree in Mathematics in 1985 from Sichuan Normal University, and received his M.S. degree in Applied Mathematics in 1990 from Central South University, and received his Ph.D. degree in Computer Science in 2005 from Nanjing University of Science and Technology respectively. He is currently a professor of School of Communication Engineering, Hangzhou Dianzi University, P.R.China. His current research interests include cryptography and information security.