Generalized ID-Based Blind Signatures From Bilinear Pairings

Said Kalkan
Department of Computer Engineering
Bilkent University
Ankara, 06800, Turkey
Email: skalkan@cs.bilkent.edu.tr

Kamer Kaya
Department of Computer Engineering
Bilkent University
Ankara, 06800, Turkey
Email: kamer@cs.bilkent.edu.tr

Ali Aydın Selçuk
Department of Computer Engineering
Bilkent University
Ankara, 06800, Turkey
Email: selcuk@cs.bilkent.edu.tr

***Abstract*— Blind signature schemes provide the feature that a user is able to get a signature without giving the actual message to the signer. Recently a number of ID-based blind signatures have been proposed. In this paper, we introduce the concept of generalized ID-based blind signatures based on ElGamal signature variants. We obtain several new ID-based blind signatures from this generalized scheme which have not been explored before and some of them turn out to be more efficient than previously proposed schemes.**

I. Introduction

In 1984, Shamir [12] introduced the concept of ID-based cryptography to simplify key management procedures in public key infrastructures. Following Joux's [9] discovery on how to utilize bilinear pairings in public key cryptosystems, Boneh and Franklin [2] proposed the first practical ID-based encryption scheme in Crypto 2001. Since then, ID-based cryptography has been one of the most active research areas in cryptography and numerous ID-based encryption and signature schemes have been proposed that use bilinear pairings.

ID-based cryptography helps us to simplify the key management process in traditional public key infrastructures. In ID-based cryptography any public information such as e-mail address, name, etc., can be used as a public key. Since public keys are derived from publicly known information, their authenticity is established inherently and there is no need for certificates in ID-based cryptography. The private key for a given public key is generated by a trusted authority and is sent to the user over a secure channel.

Chaum [4] introduced the concept of blind signatures in 1982. By using blind signatures, the user is able to get a signature from an authority without revealing the actual message to the signer. The message is signed with the signers private key in the protocol. However, the signer cannot get any information on the resulting signature. Formally, a signature is blind if the signer's view and the signature are statistically independent, where the signer's view is the set of all values that are available to the signer in the signature protocol. The blindness property is used in many applications such as electronic voting and electronic payment systems.

The first ID-based blind signature scheme was proposed by Zhang and Kim [13] in 2002. After that, there has been several proposals for ID-based blind signatures [14], [8], [6]. In this paper, we introduce the concept of generalized ID-based blind signatures. First we convert a blind ElGamal signature scheme into an ID-based counterpart. Then we generalize the signature scheme by using the ideas in Kalkan et al.'s recent work [10]. The generalized scheme yields many new ID-based blind signatures that have not been explored before and some of them are more efficient than the previously proposed schemes.

The rest of the paper is organized as follows: Background concepts including bilinear pairings and blind ElGamal signatures and its generalizations are discussed in Section II. We describe the basic ID-based blind signature scheme and its blindness proof in Section III. In Section IV, we describe the generalizations of the basic scheme. We modify some of these schemes and produce more efficient signatures in Section V. We give an efficiency comparison between some of our schemes and previously proposed signatures in Section VI. The paper is concluded in Section VII.

II. Background

In this section, we present the tools that will be used in the rest of the paper. We briefly discuss bilinear pairings, blinding a modified ElGamal signature scheme and its generalizations.

A. Bilinear Pairings

Let G_1 be a cyclic additive group of order q generated by P. Let G_2 be a cyclic multiplicative group of the same order. An admissible bilinear pairing is defined as $e : G_1 \times G_1 \rightarrow G_2$ with the following properties:

1) *Bilinearity:* $e(aR, bS) = e(R, S)^{ab}$ where $R, S \in G_1$ and $a, b \in \mathbb{Z}_q$. This can also be stated as $\forall R, S, T \in G_1$ $e(R + S, T) = e(R, T)e(S, T)$ and $e(R, S + T) = e(R, S)e(R, T)$
2) *Non-degeneracy:* The map e does not send all pairs in $G_1 \times G_1$ to the identity of G_2. That is $e(P, P) \neq 1$.
3) *Computability:* There exists an efficient algorithm to compute $e(R, S)$ for any $R, S \in G_1$

B. Modified ElGamal Signature Scheme

Original ElGamal Signature [5] is not suitable to get blind signatures. However, it is possible to get blind signatures based on its variants. The modified ElGamal Signature which is used

as a base tool for the rest of the paper is as follows: Let p be a large prime, q a divisor of $p-1$, and g an element in $\mathbb{Z}_p^*$ of order q. The user chooses $\alpha \in \mathbb{Z}_q$ as his private key and $\beta = g^\alpha \bmod p$ as his public key. The parameters p, q, g, and β are public whereas the user keeps α secret. To sign a message, the user generates a random $k \in_R \mathbb{Z}_q$. Then he computes $r = g^k \bmod p$ and $s = \alpha r + km \bmod q$. The (r, s) pair is the signature of message m. The equation

$$s \equiv \alpha r + km \pmod{q} \tag{1}$$

is called the signature equation, and verification is done by checking the congruence $r \stackrel{?}{\equiv} (\beta^{-r} g^s)^{m^{-1}} \pmod{p}$. Security of ElGamal signatures relies on the discrete logarithm problem (DLP) since solving α from β or s from r, m, β can be reduced to solving DLP in $\mathbb{Z}_p^*$.

C. Basic Blind ElGamal Signature Scheme

Chamenish et al. [3] showed that the above scheme can be extended to provide blindness. The blind signature protocol in Fig. 1. between Alice and Nancy is a blind version of the modified ElGamal signature.

Nancy		Alice
$k \in_R \mathbb{Z}_q^*$		
$\tilde{r} = g^k \bmod p$		
	$\xrightarrow{\tilde{r}}$	
		$a, b \in_R \mathbb{Z}_q^*$
		$r = \tilde{r}^a g^b \bmod p$
		$\tilde{m} = am\tilde{r}r^{-1} \bmod q$
	$\xleftarrow{\tilde{m}}$	
$\tilde{s} = \tilde{r}\alpha + k\tilde{m}$		
	$\xrightarrow{\tilde{s}}$	
		$s = \tilde{s}r\tilde{r}^{-1} + bm \bmod q$
		output (r, s)

Fig. 1. Blind Signature Protocol

In this blind signature protocol, signature equation is $s = k\tilde{m} + r\alpha \bmod q$ and the signature for the message m is (r, s). Verification is done by checking $r \stackrel{?}{\equiv} (\beta^{-r} g^s)^{m^{-1}} \bmod p$, which is the same as the modified ElGamal scheme. By using the above protocol, Alice gets a valid signature for the message m from the notary (Nancy) without revealing the message.

D. Generalized Blind ElGamal Signatures

Horster et al. [7] showed that many variations of the basic blind signature scheme are possible by modifying the signature equation (1). One can use the general equation

$$\tilde{A} \equiv \alpha\tilde{B} + k\tilde{C} \pmod{q} \tag{2}$$

to obtain a signature, where α is the secret key of Nancy and (A, B, C) is the permutation of parameters $(\tilde{m}, \tilde{r}, \tilde{s})$. The parameter $\tilde{r}$ can be computed as $\tilde{r} = g^k$ and Alice blinds $\tilde{r}$ with two random blinding factors a, b such that $\tilde{r} = r^a g^b \bmod p$. Nancy signs the blinded message $\tilde{m}$ by using the generalized signature equation (2). The signature is verified by checking the equation $g^A \equiv \beta^B + r^C \pmod{p}$, where (A, B, C) is the permutation of parameters (m, r, s). In order to get a valid signature, the following two equations must hold.

$$A = a\tilde{A}C\tilde{C}^{-1} + bC \bmod q$$
$$B = b\tilde{B}C\tilde{C}^{-1} \bmod q$$

By using these equations it is possible to extract $\tilde{m}$ and s. Note that, s and $\tilde{s}$ cannot be in the equation for $\tilde{m}$ since $\tilde{m}$ is sent to Nancy before s and $\tilde{s}$ are determined in the protocol. Therefore the value s cannot appear in C. This also prevents getting a blind signature for the original ElGamal scheme.

The generalization can be extended further by choosing A, B, C as general functions of m, r, s. In that case, one of the functions should be chosen as 1 to get efficient variants. Moreover, suitable functions should be chosen to guarantee solvability of parameters $s, \tilde{s}$ and $\tilde{m}$. Further details can be found in Horster et al.'s paper [7].

III. Basic ID-based Blind Signature Scheme

An ID-based blind signature scheme consists of four algorithms: SETUP, EXTRACT, SIGN, and VERIFY. In SETUP, the PKG, chooses a secret as the global secret key and publishes the global public system parameters. In EXTRACT, the PKG verifies a user's identity and computes his private key. In SIGN, the user (Alice) and the signer (Nancy) run the blind signature protocol to get the blind signature for a message. Finally in VERIFY, the verifier verifies the signature and recovers the message by using the public parameters and the signer's identity.

An ID-based blind signature scheme can be obtained from the blind signature scheme described in Section II-C as follows:

- SETUP: Let G_1 be cyclic additive group of order q generated by P. Let G_2 be a cyclic multiplicative group of the same order and $e : G_1 \times G_1 \to G_2$ be an admissible bilinear pairing. The PKG chooses $s \in_R \mathbb{Z}_q^*$ as the global secret key and computes $P_{pub} = sP$ as the global public key. The PKG publishes system parameters $\langle G_1,\ G_2,\ e,\ P,\ P_{pub},\ H,\ H_1 \rangle$ where H and H_1 are secure hash functions.

- EXTRACT: PKG verifies the user's identity ID and computes $Q_{ID} = H_1(ID)$ and $S_{ID} = sQ_{ID}$ as user's public and private keys respectively.

- SIGN: To sign a message $m \in \mathbb{Z}_q$, Alice and Nancy run the blind signature protocol: First Nancy chooses $k \in_R \mathbb{Z}_q^*$, then computes $\tilde{r} = e(P, P)^k$ and sends $\tilde{r}$ to the Alice. After receiving $\tilde{r}$ from Nancy, Alice chooses $a, b \in_R \mathbb{Z}_q^*$, then computes $r = \tilde{r}^a e(P, P)^b$ and blinds the message m as $\tilde{m} = am\tilde{r}r^{-1}$ and sends $\tilde{m}$ to Nancy. Nancy signs the blinded message $\tilde{m}$ by using the signature equation ($\tilde{U} = \tilde{r}S_{ID} + k\tilde{m}P$) and

sends $\tilde{U}$ to Alice. Alice checks whether $(\tilde{r}, \tilde{U})$ is a valid signature for $\tilde{m}$, then computes the signature U as $U = \tilde{U}r\tilde{r}^{-1} + bmP$. Finally Alice outputs the signature (r, U) for the message m. The protocol can be seen in Fig. 2.

- VERIFY: Given ID, the message m and a signature $(\tilde{r}, \tilde{U})$, the signature is valid if the following equation holds.

$$e(U, P)e(Q_{ID}, P_{pub})^{-r} = r^m$$

Nancy		Alice
$k \in_R \mathbb{Z}_q^*$ $\tilde{r} = e(P, P)^k$		
	$\xrightarrow{\tilde{r}}$	
		$a, b \in_R \mathbb{Z}_q^*$ $r = \tilde{r}^a e(P, P)^b$ $\tilde{m} = am\tilde{r}r^{-1}$
	$\xleftarrow{\tilde{m}}$	
$\tilde{U} = \tilde{r}S_{ID} + k\tilde{m}P$		
	$\xrightarrow{\tilde{U}}$	
		$e(\tilde{U}, P)e(Q_{ID}, P_{pub})^{-\tilde{r}} \stackrel{?}{=} \tilde{r}^{\tilde{m}}$ $U = \tilde{U}r\tilde{r}^{-1} + bmP$ output (r, U)

Fig. 2. ID-based Blind Signature Protocol

Correctness of the given scheme can be shown by using the bilinearity properties of e. Notice that, if (r, U) is a valid signature for m, then $e(U, P)e(Q_{ID}, P_{pub})^{-r}$ is

$$\begin{aligned}
&= e(\tilde{U}r\tilde{r}^{-1} + bmP, P)e(Q_{ID}, P_{pub})^{-r} \\
&= e(\tilde{U}r\tilde{r}^{-1} + bmP, P)e(-rS_{ID}, P) \\
&= e((\tilde{r}S_{ID} + k\tilde{m}P)r\tilde{r}^{-1} + bmP, P)e(-rS_{ID}, P) \\
&= e(rS_{ID} + k\tilde{m}r\tilde{r}^{-1}P + bmP, P)e(-rS_{ID}, P) \\
&= e(k\tilde{m}r\tilde{r}^{-1}P + bmP, P) \\
&= e(k(am\tilde{r}r^{-1})r\tilde{r}^{-1}P + bmP, P) \\
&= e(kamP + bmP, P) \\
&= (\tilde{r}^a + e(P, P)^b)^m \\
&= r^m
\end{aligned}$$

The above scheme is the ID-based version of the modified blind ElGamal signature described in Section II-C. In that scheme, the signature equation is $\tilde{s} = \alpha\tilde{r} + k\tilde{m} \bmod q$ where $\tilde{r} = g^k$ and the signature is (r, s). Since additive elliptic curve groups are used in the ID-based structure, the signing equation and $\tilde{r}$ are slightly different. The signing equation for the ID-based ElGamal signature becomes,

$$\tilde{U} = \tilde{r}S_{ID} + k\tilde{m}P$$

In this signature equation, uppercase letters are used to denote the elements of the elliptic curve group. S_{ID} is the private key of the user; so it is a natural replacement for α in the original scheme. U is the second part of the signature, replacing s. A natural choice for $\tilde{r}$ in the ID-based scheme is $\tilde{r} = e(P, P)^k$ since $\tilde{r} = g^k$ in the original scheme.

A. Blindness Proof

A signature is said to be blind if a given message-signature pair and Nancy's view are statistically independent. That is, the signer cannot get any information on the actual message and the resulting signature. If there always exists a unique mapping between any view of the signer and any given message signature pair, we can say that the signature is blind.

In order to prove blindness we will show that for a given message-signature pair (m, r, U) and any view of Nancy $(\tilde{m}, \tilde{r}, \tilde{U})$, there always exists a unique pair of blinding factors a, b that maps $(\tilde{m}, \tilde{r}, \tilde{U})$ to (m, r, U). Since Alice chooses a, b randomly, Nancy cannot get any information from her view and the signature scheme will be blind.

For a signature (r, U) generated for message m during the protocol, the following equations must hold.

$$\tilde{m} = am\tilde{r}r^{-1} \tag{3}$$

$$r = \tilde{r}^a e(P, P)^b \tag{4}$$

$$U = \tilde{U}r\tilde{r}^{-1} + bmP \tag{5}$$

The blinding factors a and b can be uniquely determined from the first two equations. a is determined uniquely from (3) as $a = \tilde{m}m^{-1}r\tilde{r}^{-1}$. From (4), $e(P, P)^b = r\tilde{r}^{-a}$, since $e(P, P)$ is a generator for G_2, therefore b is also unique. If these a and b satisfy (5), the desired mapping will be found and the signature will be blind. We know that

$$U = \tilde{U}r\tilde{r}^{-1} + bmP \iff e(U, P) = e(\tilde{U}r\tilde{r}^{-1} + bmP, P).$$

So it is sufficient to show that $e(U, P) = e(\tilde{U}r\tilde{r}^{-1} + bmP, P)$ to complete the proof. Notice that, since (r, U) is a valid signature, the signature equation $\tilde{U} = \tilde{r}S_{ID} + k\tilde{m}P$ and the verification equation $e(U, P)e(Q_{ID}, P)^{-r} = r^m$ should hold.

Hence, we have $e(\tilde{U}r\tilde{r}^{-1} + bmP, P)$ equals

$$\begin{aligned}
&= e(\tilde{U}r\tilde{r}^{-1}, P)e(P, P)^{bm} \\
&= e(\tilde{U}r\tilde{r}^{-1,P})(r\tilde{r}^{-a})^m \\
&= e(\tilde{U}, P)^{r\tilde{r}^{-1}} r^m \tilde{r}^{-am} \\
&= e(\tilde{r}S_{ID} + k\tilde{m}P, P)^{r\tilde{r}^{-1}} r^m \tilde{r}^{-am} \\
&= e(\tilde{r}S_{ID}, P))^{r\tilde{r}^{-1}} e(k\tilde{m}P, P)^{r\tilde{r}^{-1}} r^m \tilde{r}^{-am} \\
&= e(S_{ID}, P)^r \tilde{r}^{\tilde{m}r\tilde{r}^{-1}} r^m \tilde{r}^{-am} \\
&= e(Q_{ID}, P)^r \tilde{r}^{am} r^m \tilde{r}^{-am} \\
&= e(Q_{ID}, P)^r r^m \\
&= e(U, P).
\end{aligned}$$

No.	$\tilde{r}$	$\tilde{U}$	r	U	$\tilde{m}$	Verification
BL I.1	$e(P,P)^k$	$\tilde{r}S_{ID} + k\tilde{m}P$	$\tilde{r}^a e(P,P)^b$	$\tilde{U}r\tilde{r}^{-1} + bmP$	$am\tilde{r}r^{-1}$	$e(U,P)e(Q_{ID},P_{pub})^{-r} = r^m$
BL I.2	$e(P,P)^k$	$\tilde{m}S_{ID} + k\tilde{r}P$	$\tilde{r}^a e(P,P)^b$	$ar\tilde{r}^{-1}\tilde{U} + brP$	$a^{-1}m\tilde{r}r^{-1}$	$e(U,P)e(Q_{ID},P_{pub})^{-m} = r^r$
BL II.1	$e(P,P)^k$	$S_{ID} + k\tilde{m}\tilde{r}P$	$\tilde{r}^a e(P,P)^b$	$\tilde{U} + bmrP$	$amr\tilde{r}^{-1}$	$e(U,P)e(Q_{ID},P_{pub}) = r^{mr}$
BL II.2	$e(P,P)^k$	$\tilde{m}\tilde{r}S_{ID} + kP$	$\tilde{r}^a e(P,P)^b$	$a\tilde{U} + bP$	$a^{-1}mr\tilde{r}^{-1}$	$e(U,P)e(Q_{ID},P_{pub})^{-mr} = r$
BL III.1	$a^{-1}r$	$\tilde{r}S_{ID} + kP$	$H(m,t)$	$a\tilde{U} + bP$	–	$H(m, e(U,P)e(Q_{ID},P_{pub})^{-r}) = r$
BL III.2	ar	$-S_{ID} + k\tilde{r}P$	$H(m,t)$	$\tilde{U} + brP$	–	$H(m, e(U,P)^{r^{-1}}e(Q_{ID},P_{pub})^{r^{-1}}) = r$

TABLE I

GENERALIZED ID-BASED BLIND SIGNATURES, WHERE $\tilde{t} = e(P,P)^k$ AND $t = \tilde{t}^a e(P,P)^b$

IV. GENERALIZED ID-BASED BLIND SIGNATURES

We can generalize the above signature scheme by using different signature equations. Instead of using $\tilde{U} = \tilde{r}S_{ID} + k\tilde{m}P$ as the signature equation, we can use

$$A = BS_{ID} + kC$$

in general, where (A, B, C) is the permutation of the parameters $(\tilde{m}, \tilde{r}, \tilde{U})$. Note that, we can use P, $\tilde{m}P$ and $\tilde{r}P$ instead of 1, $\tilde{m}$ and $\tilde{r}$ in cases where they need to be members of the elliptic curve group. However, not all the permutations generate useful variants. We should consider that $\tilde{U}$ is a member of the elliptic curve group so it cannot be used for B. Moreover, $\tilde{U}$ cannot be in the position of C. Since, in that case, U and $\tilde{U}$ are needed to extract $\tilde{m}$; but, $\tilde{m}$ is sent to Nancy before U and $\tilde{U}$ are determined in the protocol. Therefore we can get only two variants. The signing equation for these variants are:

$$\tilde{U} = \tilde{m}S_{ID} + k\tilde{r}P \tag{6}$$

$$\tilde{U} = \tilde{r}S_{ID} + k\tilde{m}P \tag{7}$$

Two more variants can be generated by using the permutations of $(\tilde{m}\tilde{r}, \tilde{U}, 1)$. The signing equation for these variants are:

$$\tilde{U} = S_{ID} + k\tilde{m}\tilde{r}P \tag{8}$$

$$\tilde{U} = \tilde{m}\tilde{r}S_{ID} + kP \tag{9}$$

The verification equations and other details for these signatures are summarized in Table I. Note that, we can also use a general function $f(\tilde{m}, \tilde{r})$ instead of just the product $\tilde{m}\tilde{r}$.

Another way of using ElGamal signatures to sign a message m is to mix m into r by a hash function, instead of using m in the computation of U. In this way, it is possible to remove $\tilde{m}$ from the signing equations by modifying the blind signature protocol. If we remove $\tilde{m}$ from (6), the signing equation will be,

$$\tilde{U} = \tilde{r}S_{ID} + kP. \tag{10}$$

If we use (10) as the signature equation, we modify the blind signature protocol as follows: Instead of sending $\tilde{r}$, Nancy computes $\tilde{t} = e(P,P)^k$ and sends $\tilde{t}$ to Alice. Alice computes $t = \tilde{t}^a e(P,P)^k$ and $r = H(m,t)$, where H is a secure hash function. Then, she computes $\tilde{r} = a^{-1}r$ and sends $\tilde{r}$ to Nancy. Nancy computes $\tilde{U}$ by using the signature equation (6) and sends $\tilde{U}$ to Alice. Alice checks whether the signature is valid, computes $U = a\tilde{U} + bP$, and outputs the signature (r, U). The modified protocol can be found in Fig. 3.

Similarly, if we remove $\tilde{m}$ from (7) the signing equation will be,

$$\tilde{U} = S_{ID} + k\tilde{r}P.$$

The verification equation and other details for these signatures can be found in Table I. Note that, removing $\tilde{m}$ from (8) and (9) does not generate new variants.

Nancy		Alice
$k \in_R \mathbb{Z}_q^*$ $\tilde{t} = e(P,P)^k$		
	$\xrightarrow{\tilde{t}}$	
		$a, b \in_R \mathbb{Z}_q^*$ $t = \tilde{t}^a e(P,P)^b$ $r = H(m,t)$ $\tilde{r} = a^{-1}r$
	$\xleftarrow{\tilde{r}}$	
$\tilde{U} = \tilde{r}S_{ID} + kP$		
	$\xrightarrow{\tilde{U}}$	
		$e(\tilde{U},P)e(Q_{ID},P_{pub})^{-\tilde{r}} \stackrel{?}{=} \tilde{r}$ $U = a\tilde{U} + bP$ output (r, U)

Fig. 3. Modified Blind Signature Protocol

V. MORE EFFICIENT ID-BASED BLIND SIGNATURES

Computing a signature requires two to four scalar multiplications in G_1 and three or four exponentiations in G_2, depending on the signature equation, as well as one pairing evaluation. The other pairing $e(Q_{ID}, P_{pub})$ can be precomputed before the signature protocol.

The cost of verifying a signature will be dominated by the pairing computations, which is the most expensive operation. Two pairing computations and an exponentiation in G_1 are needed to verify a signature. Note that, in the proposed schemes, the value $e(Q_{ID}, P_{pub})$ is used, which is fixed for a particular user and needs to be computed only once for each user.

The number of pairing operations can be reduced to one by changing the definitions of S_{ID} and Q_{ID} as in [1] and [11].

No.	$\tilde{r}$	$\tilde{U}$	r	U	$\tilde{m}$	Verification
BL IV.1	$e(P,Q_{ID})^k$	$\tilde{r}S_{ID}+k\tilde{m}P$	$\tilde{r}^a e(P,Q_{ID})^b$	$\tilde{U}r\tilde{r}^{-1}+bmP$	$am\tilde{r}r^{-1}$	$e(U,Q_{ID})e(P,P)^{-r}=r^m$
BL IV.2	$e(P,Q_{ID})^k$	$\tilde{m}S_{ID}+k\tilde{r}P$	$\tilde{r}^a e(P,Q_{ID})^b$	$ar\tilde{r}^{-1}\tilde{U}+brP$	$a^{-1}m\tilde{r}r^{-1}$	$e(U,Q_{ID})e(P,P)^{-m}=r^r$
BL IV.3	$e(P,Q_{ID})^k$	$S_{ID}+k\tilde{m}\tilde{r}P$	$\tilde{r}^a e(P,Q_{ID})^b$	$\tilde{U}+bmrP$	$amr\tilde{r}^{-1}$	$e(U,Q_{ID})e(P,P)=r^{mr}$
BL IV.4	$e(P,Q_{ID})^k$	$\tilde{m}\tilde{r}S_{ID}+kP$	$\tilde{r}^a e(P,Q_{ID})^b$	$a\tilde{U}+bP$	$a^{-1}mr\tilde{r}^{-1}$	$e(U,Q_{ID})e(P,P)^{-mr}=r$
BL IV.5	$a^{-1}r$	$\tilde{r}S_{ID}+kP$	$H(m,t)$	$a\tilde{U}+bP$	–	$H(m,e(U,Q_{ID})e(P,P)^{-r})=r$
BL IV.6	ar	$-S_{ID}+k\tilde{r}P$	$H(m,t)$	$\tilde{U}+brP$	–	$H(m,e(U,Q_{ID})^{r^{-1}}e(P,P)^{r^{-1}})=r$
BL V.1	$e(P,P)^k$	$(\tilde{r}+k\tilde{m})S_{ID}$	$\tilde{r}^a e(P,Q_{ID})^b$	$\tilde{U}r\tilde{r}^{-1}+bmP$	$am\tilde{r}r^{-1}$	$e(U,Q_{ID})e(P,P)^{-r}=r^m$
BL V.2	$e(P,P)^k$	$(k+\tilde{r}\tilde{m})S_{ID}$	$\tilde{r}^a e(P,Q_{ID})^b$	$ar\tilde{r}^{-1}\tilde{U}+brP$	$a^{-1}m\tilde{r}r^{-1}$	$e(U,Q_{ID})e(P,P)^{-m}=r^r$
BL V.3	$e(P,P)^k$	$(\tilde{m}+k\tilde{r})S_{ID}$	$\tilde{r}^a e(P,Q_{ID})^b$	$\tilde{U}+bmrP$	$amr\tilde{r}^{-1}$	$e(U,Q_{ID})e(P,P)=r^{mr}$
BL V.4	$e(P,P)^k$	$(1+k\tilde{m}\tilde{r})S_{ID}$	$\tilde{r}^a e(P,Q_{ID})^b$	$a\tilde{U}+bP$	$a^{-1}mr\tilde{r}^{-1}$	$e(U,Q_{ID})e(P,P)^{-mr}=r$
BL V.5	$a^{-1}r$	$(\tilde{r}+k)S_{ID}$	$H(m,t)$	$a\tilde{U}+bP$	–	$H(m,e(U,Q_{ID})e(P,P)^{-r})=r$
BL V.6	ar	$(1+k\tilde{r})S_{ID}$	$H(m,t)$	$\tilde{U}+brP$	–	$H(m,e(U,Q_{ID})^{r^{-1}}e(P,P)^{r^{-1}})=r$

TABLE II

GENERALIZED ID-BASED BLIND SIGNATURES, WHERE $\tilde{t}=e(P,Q_{ID})^k$ IN IV.5, IV.6, $\tilde{t}=e(P,P)^k$ IN V.5, V.6 AND $t=\tilde{t}^a e(P,Q_{ID})^b$

If we define

$$Q_{ID}=(H_1(ID)+s)P$$
$$S_{ID}=(H_1(ID)+s)^{-1}P,$$

the number of pairing evaluations can be reduced to one. Note that Q_{ID} can be computed by anyone, since the value of sP is public, but S_{ID} cannot be computed without knowing the value of s.

By changing the definitions of S_{ID} and Q_{ID} as described, we can get more efficient variants of the proposed schemes. The computation of r should also be changed in order to adapt to the changes. Instead of computing $r=e(P,P)^k$, we have

$$r=e(P,Q_{ID})^k.$$

This modification does not affect the efficiency of the signature computation, since the value $e(P,Q_{ID})$ can be precomputed by the sender.

The verification equations and other details of the efficient versions of the signatures modified in this fashion are given in Group IV of Table II.

Further variants with a reduced signing cost can be obtained by modifying the generalized signature equation as,

$$U=AS_{ID}+kBS_{ID}, \tag{11}$$

where the signing cost is reduced by one scalar multiplication in the elliptic curve group G_1. Note that, this kind of generalization is not possible over the basic ElGamal signatures, because when k and α are used together, we cannot extract s from the signing equation.

We can get six more efficient variants by this modification whose signing equations are:

$$U=(r+km)S_{ID}$$
$$U=(k+rm)S_{ID}$$
$$U=(m+kr)S_{ID}$$
$$U=(1+kmr)S_{ID}$$
$$U=(r+k)S_{ID}$$
$$U=(1+kr)S_{ID}$$

Scheme	Signing Cost	Verification Cost
Group I	$1B+4M+4E$	$2B+2E$
Group II	$1B+$(2-4)$M+3E$	$2B+1E$
Group III	$1B+$(2-4)$M+3E$	$2B+1E$
Group IV	$1B+$(2-4)$M+$(3-4)E	$1B+$(1-2)E
Group V	$1B+$(2-3)$M+$(3-4)E	$1B+$(1-2)E
ZK02 [13]	$2B+6M$	$2B+1E$
ZK03 [14]	$2B+6M$	$2B+1M$
HCW05 [8]	$1B+3M+3E$	$2B+1M$
GWWL07 [6]	$3B+7M$	$4B$

TABLE III

COMPARISON OF ID-BASED BLIND SIGNATURE SCHEMES

The verification equations and other details of these signatures are given in Group V of Table II.

VI. PERFORMANCE COMPARISON

In this section, we give a performance comparison of our proposed schemes and the four available ID-based blind signature schemes [13], [14], [8], [6] based on bilinear pairings. As the main computational cost, we consider the number of bilinear pairings (denoted by B), modular exponentiations, (denoted by E), and scalar multiplications in elliptic curve group (denoted by M). We assume the value of $e(P,P)$ is precomputed by every party, and the value of $e(P,Q_{ID})$ is precomputed by the signer but not the verifier.

Among the proposed schemes, Group I, Group II, and Group III are the least efficient schemes with signing cost of one pairing, two to four scalar multiplications, and three or four exponentiations and verification cost of two pairings, and one or two exponentiations. Group IV and Group V are the most efficient schemes with the signing cost of one pairing, two to four scalar multiplications, and three or four exponentiations and verification cost of one pairing, and one or two exponentiations.

Compared to the previously proposed schemes, ZK02 [13] has the signing cost of $2B+6M$ and verification cost of $2B+1E$. In ZK03 [14], signing cost is $2B+6M$ and verification cost is $2B+1M$. In HCW05 [8], signing cost is $1B+3M+3E$ and verification cost is $2B+1M$. In GWWL07 [6] signing cost is $3B+7M$ and verification cost

is $4B$; however, GWWL07 [6] has the advantage that blind signature protocol needs only one round.

Performance comparison of our schemes to the previously proposed schemes can be found in Table III. As the table shows Group IV and Group V are the most efficient signatures with the smallest number of pairing evaluations.

VII. Conclusion

In this paper, ID-based blind signatures are investigated. We showed how a modified blind ElGamal signature can be converted to an ID-based blind signature. We extended our basic ID-based blind signature scheme into a generalized ID-based blind signatures as in the work of Horster et al. [7] on the basic blind ElGamal signature. We also presented some original variants which were not possible in the non-ID-based setting. Then, we modified some of our signatures to get more efficient signature schemes.

Among the existing schemes, Group IV and Group V with just one pairing operation in signature verification, become the most efficient ID-based blind signatures in the literature.

References

[1] P. S. L. M. Barreto, B. Libert, N.McCullagh, and J. Quisquater. Efficient and provably-secure Identity-based signatures and signcryption from bilinear maps. In *Proc. of ASIACRYPT'05*, volume 3778 of *LNCS*, pages 515–532, 2005.

[2] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In *Proc. of CRYPTO'01*, volume 2139 of *LNCS*, pages 213–229. Springer-Verlag, 2001.

[3] Jan L. Camenisch, Jean-Marc Piveteau, and Markus A. Stadler. Blind signatures based on the discrete logarithm problem. In *Proc. of Eurocrypt 1994*, volume 950 of *LNCS*, pages 428–432, 1995.

[4] D. Chaum. Blind signatures for untraceable payments. In *Proc. of Crypto'82*, pages 199–203. New York: Plenum Press, 1983.

[5] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Information Theory*, 31(4):469–472, 1985.

[6] W. Gao, X. Wang, G. Wang, and F.Li. One-round ID-based blind signature scheme without ROS assumption. Cryptology ePrint Archive, Report. http://eprint.iacr.org/2007/007.

[7] P. Horster, M. Michels, and H. Petersen. Meta-message recovery and meta-blind signature schemes based on the discrete logarithm problem and their applications. In *Proc. of ASIACRYPT 1994*. LNCS, Springer-Verlag, 1994.

[8] Z. Huang, K. Chen, and Y. Wang. Efficient identity-based signatures and blind signatures. In *Proc. of CANS 2005*, volume 3810 of *LNCS*, pages 120–133, 2005.

[9] A. Joux. A one round protocol for tripartite Diffie-Hellman. In *Proc. of ANTS-IV*, volume 1838 of *LNCS*, pages 385–394, 2000.

[10] S. Kalkan, K. Kaya, and A. A. Selcuk. Generalized ID-based ElGamal signatures. In *The 22nd International Symposium on Computer and Information Sciences (ISCIS 2007)*, 2007.

[11] S. Kalkan, K. Kaya, and A. A. Selcuk. Generalized ID-based ElGamal signatures with message recovery. In *Information Security and Cryptology Conference (ISC 2007)*, 2007.

[12] A. Shamir. Identity-based cryptosystems and signature schemes. In *Proc. of CRYPTO'84*, volume 196 of *LNCS*, pages 47–53. Springer-Verlag, 1984.

[13] F. Zhang and K. Kim. ID-based blind signature and ring signature from pairings. In *Proc. of Asiacript 2002*, volume 2501 of *LNCS*, pages 533–547, 2002.

[14] F. Zhang and K. Kim. Efficient ID-based blind signature and proxy signature from bilinear pairings. In *Proc. of ACISP2003*, volume 2727 of *LNCS*, pages 312–323, 2003.