New Short Signature Scheme from Pairings

Pin-Chang Su

Department of Information Management, College of Management, National Defense University

ABSTRACT

Short digital signatures are always desirable. They are necessary in situations in which humans are asked to manually key in the signature or when working in low-bandwidth communication environments. They are also useful in general to reduce the communication environments. We propose a short signature scheme based on knapsack and Gap Diffie-Hellman(GDH) groups whose security is closely related to the discrete logarithm assumption in the random oracle model. The new scheme offers a better security guarantee than existing discrete-logarithm-based signature schemes. Furthermore, our scheme upholds all desirable properties of previous ID-Based signature schemes, and requires general cryptographic hash functions instead of MapToPoint hash function that is inefficient and probabilistic. The new short signature scheme is needed to low-bandwidth communication, low-storage and low-computation environments, and particularly applicable to smart cards and wireless devices.

Keywords: Short signature, GDH groups, knapsack

植基於雙線性曲線對的新短簽章方法

蘇品長

國防大學管理學院資訊管理學系

摘　　要

短數位簽章方法一直吸引學者們的研究。尤其在資源有限、無法提供大量頻寬的通訊環境中，當需要簽章時，更能突顯其重要性。我們將提出一套以 GDH 群及背包理論為主的方法，其安全性與原型一樣等同於離散對數的為數學難題上。我們的研究比現行學者所提的方法，均能有更安全的保障，亦能保有原短簽章的特性，此外，以一段雜湊函數的運算取代「值對點」轉換函數，改善效率及提升安全性的問題。我們的方法適用於低耗能、低計算能力、低頻寬的環境，如智慧卡及無線通訊等。

關鍵詞：短簽章，GDH 群，背包理論

文稿收件日期 99.3.15; 文稿修正後接受日期 99.9.1; *通訊作者
Manuscript received March 15, 2010; revised September 1, 2010; * Corresponding author

I. INTRODUCTION

In public key infrastructure, a certificate authority (CA) is needed to issue digital certificates for users. A certificate binds an entity's identity information with the corresponding public key. It has some well-know and bothersome side-effects such as the need for cross-domain trust and certificate management and certificate revocation, which requires a large amount of storage and computing [1]. In order to avoid the problem and the cost of distributing the public keys, Shamir [2] firstly introduced the concept of ID-based public key cryptosystem in 1984, which allows a user to use his identity information such as name, Email address, IP address or telephone number, *et al.* as his own public key. It means that there is no need for a user to keep a public key directory or obtain other users' certificates before communication. The first ID-based signature (IBS) scheme was proposed by Shamir [2], but the size of generated signature is quite large, which has 2048 bits when one utilizes a 1024-bit RSA modulus. In 1988, Guillou and Quisquater [3] improved Shamir's scheme and shortened the signature size to 1184 bits when one uses 1024-bit RSA modulus and 160-bit hash function. However, the size of signatures generated by the scheme [3] is still too large to be applied widely in practice, especially in environments with stringent bandwidth constraints.

Short digital signatures are important in low-bandwidth communication, low-storage and low-computation environments. Short signatures are needed when printing a signature on a postage stamp, a commerce invoice or a bank bill. Short digital signatures are also needed when a human is asked to key in signatures manually. For instance, product registration systems often ask the users to key in a signature provided on a CD label. Short signatures are particularly applicable to wireless devices such as PDAs, cell phones, RFID chips and sensors, where battery life is the main limitation. At present, many short signatures schemes in public key cryptosystem have been proposed since Boneh, Lynn and Shacham [4] construct a short signature called BLS signature, which is just half the size of the signature in DSA (320 bits) with comparable security. Now, many IBS schemes [5, 6, 7, 8, 9, 10, 11, 12, 13] are proposed based on bilinear pairings. These signatures generated by [5, 6, 7, 8, 9, 10, 11, 12, 13] are much shorter and simpler than signatures from schemes in [2, 3], and have been applied widely in cryptography. Recently, Okamoto *et al.* proposed a new and short signature scheme at ITCC'05, they also proposed a new signature scheme based on their signature scheme [12]. They claimed that their schemes were secure and efficient, especially for signing phase. Zhang *et al.* presented an attack on Okamoto's short signature scheme in [14]. They showed that any one can derive the secret key of the singer from two message-signature pairs and so can forge signature for any message. A main problem of short signature schemes is that they only provide implicit authentication, i.e., the validity of an authentication is verified only after a successful communication [15, 16]. Besides the signature length, another problem is the loose security related to the underlying hard computational problem. Some proposed signature schemes require non-standard security assumptions [17].

In 1991, Girault [18] first proposed a self-certified public key system to resolve the problem of public key verification. A self-certified public key system has three features: First, the secret key can be determined by the user himself/herself or together by the user and CA, and does not be known to CA. Second, the user can use his/her own secret key to verify the authenticity of the self-certified public key issued by CA, and thus no extra certificate is required. Third, the task of public key verification can be further accomplished with subsequent cryptographic application (e.g., key distribution or signature scheme) in a logically single step. Therefore, public key verification of the self-certified approach provides more efficient in saving the communication cost as well as the computation effort compared to that of the certificate-based and the ID-based approaches by storage-wasting and time-consuming drawbacks.

The Identity Based cryptosystem was first proposed to simplify the conventional public key cryptosystem, and make management easier [2]. If the user is led to connect to a spoofing site that appears to be what he/she wants to pay

a visit, he/she may have a secure connection to an adversary who will work maliciously. Thus, identify certification or authentication is imperative to act. In public key cryptosystem, each user has two keys. One is a private key and the other is a public key. In 1997, Saeednia [19] successfully combined the merits inhered in both the ID-based and the self-certified systems, and proposed an ID-based self-certified public key system that can be applied to the realization of key exchange protocols. However, Wu et al. [20] and Kim et al. [21] showed that the original version of Saeednia's ID-based self-certified public key system is not secure enough against withstanding the impersonation attack, and also proposed an improvement to overcome the flaw in the original version. In 2003, Saeednia [22] indicated an important shortcoming of the RSA-based self-certified model proposed by Girault [18], which may be exploited by the authority to compute user's secret keys. Saeednia further showed that the resulting model loses all merits of the original model and does no longer meet the primary contribution of the self-certified notion, while it is possible to make the attack ineffective by taking additional precautions. In other words, if the self-certified model is constructed based on the security of the RSA scheme [23], i.e., relying on the difficulty of factoring a large number into its prime factors, it will expose the above defect. Tsaur [24] expanded Girault's works to ECC-based cryptosystems which are quite suitable for electronic transactions. However, the main problem investigating into self-certified public key schemes was that they only presented an implicit authentication, i.e., the validity of a self-certified public key is verified only after a successful communication.

Since the concept of public key cryptography was invented by Diffie and Hellman in 1976 [25], a lot of public key cryptographic algorithms have been proposed. Most existing cryptosystem designs incorporate just one cryptographic assumption, such as factoring (FC) or discrete logarithm (DLP) or elliptic curve discrete logarithm problems (ECDLP). These assumptions appear secure today; but it is possible that efficient algorithms will be sooner or later developed to break one or more of these assumptions. Unlike the FC and DLP cryptosystems, one of the earliest public key cryptosystems is the knapsack cryptosystem and the underlying scheme implements the subset sum problem. The first knapsack cryptosystem was proposed by Merkle and Hellman [26]. These have all been analyzed and broken, generally through the same cryptographic techniques. Some researchers believed that the broken knapsack cryptosystems were cracked because their construction did not completely disguise the easy knapsack, or their densities were too low [27]. The main contribution of the Merkle-Hellman Knapsack cryptosystem is that it demonstrates how an NP-complete problem can be used for public-key cryptography.

Recently bilinear pairings such as the Weil/Tate pairings on elliptic curves and hyper-elliptic curves have been variously applied to create signature schemes in cryptography [28]. The central idea is the construction of a mapping between two useful cryptographic groups which allow for new cryptographic schemes based on the reduction of one problem in one group to a different group, and usually is easier problem than the other group. In many research papers, the first of these two groups is referred to as a gap group, where the decisional Diffie-Helman problem (DDHP) is easy (because it reduces to an easy problem in the second group), yet the computational Diffie-Helman problem (CDHP) remains hard. Due to the underlying of the Gap Diffie-Hellman (GDH) group structure and the base scheme, e.g., the signature size is efficiently reduced to 160 bits for equivalent security to a 320-bit DSA, the proposed construction is simpler and more efficient than the existing methods on signature constructions, and it has the merits of security in authentication. However, besides obtaining simplicity in construction and efficiency in performance, the signature authenticity, the message integrity, and the signature verification has to be further assured. Dutta *et al.* surveyed a great number of cryptographic protocols which were based on pairings [29]. An open problem is whether we can design a new cryptographic protocol that is based on Diffie-Hellman problem with pairings and Knapsack problem [30].

The motivation of our paper is based on the three points: (1) The Diffie-Hellman related assumptions have played an important role in designing various cryptographic protocols.

Apart from the existing Diffie-Hellman assumptions, is it possible to propose new Diffie-Hellman assumption that will be built upon to design new self-certified short signature schemes? (2) Knapsack cryptosystems had ever received a great deal of attention in the community of cryptography and computational complexity in 1970s' and 1980s'. The basic idea of the scheme is in transforming hard or unfeasible subset sum problems into easy subset sum problems, and the subset sum problem has been proven to be NP-complete [24]. Most of the existing Knapsack cryptosystems were broken. An interesting question is: Has the Knapsack problem already been falling from designing optimistic cryptographic protocols? (3) Pairings over elliptic curves have already been combined with the Diffie-Hellman and thus created a number of Diffie-Hellman assumptions, that have been used to design cryptographic protocols. Is it possible to design a new self-certified short signature scheme of Diffie-Hellman assumptions?

In this paper, we present a self-certified IBS scheme (SCIBS) that is proved to be secure in the random oracle model. Our scheme can uphold all desirable properties of IBS schemes in [5, 6, 7, 8, 9, 10, 11, 12, 13]. However, besides obtaining simplicity in construction and efficiency in performance, the signature authenticity, the message integrity, and the signature verification has to be further assured. To overcome key escrow problems and secure channel problems that seem to be inherent to identity-based cryptography, we thereby propose a new technique for blind signatures. It is based on knapsack Diffie-Hellman problems with bilinear pairings using elliptic curves and is fully self-certified. Also, we give a security model, and further provide a security proof in random oracle model. The scheme incorporates the advantages of self-certified public keys and pairings. The remaining sections are organized as follows. In the next section we will give a brief introduction to some mathematical theory related to the following schemes. Section 3 proposes a SCIBS scheme and gives its security proof, and then analyzes its efficiency. Conclusion is drawn in the last section.

II. BACKGROUND THEORIES

We begin by describing the knapsack cryptosystem, elliptic curve cryptography (ECC), bilinear pairings, short signature and self-certified signature scheme. The procedure can be described as follows.

2.1 Knapsack Cryptosystem

The knapsack cryptosystem is based on the knapsack problem: a combinatorial question of determining which objects can fit into a container, where the knapsack's weight capacity is given and each object has a particular weight. The problem is to find a subset of the objects that can fit into the knapsack.

The mathematical description of the knapsack cryptosystem is as follows:

- *Underlying Problem:*

Subset Sum Problem (or Knapsack Problem)

- *Underlying Mathematical Structure:*

The integers modulo *M*, where *M* > the sum of a superincreasing sequence.

- *Parameters:*

Public Key parameters: $(a_1,...,a_n)$ disguised positive integers

Private Key parameters: $(b_1,...,b_n)$ Superincreasing sequence

Choose *M* and *W* with:

$M > \sum_{j=1}^{n} b_j$, $(M,W) = 1$ Compute:

$a_j \equiv b_j W \bmod M$

M, W- parameters for disguising $b_1,...,b_n$ with a modular multiplication and permutation

- *Encryption:*

A message $(x_1,...,x_n)$ is encoded as:

$$s = \sum_{j=1}^{n} x_j a_j$$

- *Decryption:*

$c \equiv sW^{-1} \bmod M, 0 \le c \le M$, the b_j are super-increasing easy to solve.

2.2 Elliptic Curve Cryptography

Miller [25] and Koblitz [26] first suggested the use of elliptic curves for implementing public key cryptosystems. A general Elliptic curve has the form, $y^2 + axy + by = x^3 + cx^2 + dx + e$, where *a*, *b*, *c*, *d* and *e* are real numbers. A special addition operation is defined over elliptic curves, and this with the inclusion of a point ∞ called point at infinity. If three points are on a line that intersects an elliptic curve, then their sum equals the point at infinity ∞. If the characteristic of *q* is neither two nor three (e.g., $K = F_q$ where $q > 3$ is a prime), then an elliptic group over the Galois Field $E(F_q)$ can be obtained by computing $y^2 = x^3 + ax + b \bmod q$ *for* $0 \le x < q$. The contents *a*, *b* are non-negative integers that are smaller than the prime number *q* and satisfy the condition $4a^3 + 27b^2 \bmod q \neq 0$. Let the points $A=(x_1, y_1)$ and $B=(x_2, y_2)$ be in the elliptic group $E(F_q)$. The rules for addition over the elliptic group $E(F_q)$ are:

- $P + \infty = \infty + P = P$
- If $x_2 = x_1$ and $y_2 = -y_1$, that is $P = (x_1, y_1)$ and $Q = (x_2, y_2) = (x_1, -y_1) = -P$, then $P + Q = \infty$
- If $Q \neq P$, then the sum $P + Q = (x_3, y_3)$ is given by:

$$x_3 \equiv \lambda^2 - x_1 - x_2 \mod q$$
$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \mod q$$

where $\lambda = (y_2 - y_1)/(x_2 - x_1)$ *If* $x_1 \neq x_2$ *or* $\lambda = (3x_1^2 + a)/2y_1$ *If* $x_1 = x_2, y_1 \neq 0$.

To double for a point *P*, it is equivalent to do *P* + *P*. Similarly, we can calculate 3*P* = 2*P* + *P* and so on. One important property is that it is very difficult to find an interger *s* such that *sP* = *Q*.

2.3 Bilinear Pairings

We now describe Bilinear Pairings as discussed in [27]. 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:

- *Bilinear:*

For all $P, Q \in G_1$ and $a, b \in Z_q^*, e(aP, bQ) = e(abP, Q) = e(P, abQ) = e(P, Q)^{ab}$.

- *Non-degenerate:*

There exists $P \in G_1$, such that $e(P, P) \neq 1$.

- *Computable:*

Given $P, Q \in G_1$, there is an efficient algorithm to compute $e(P, Q)$.

With such group G_1, we can define the following hard cryptographic problems:

- *Discrete Logarithm (DL) Problem:*

Given $P, P' \in G_1$, find an integer *n* such that $P = nP'$ whenever such an integer exists.

- *Computational Diffie-Hellman (CDH) Problem:*

Given a triple $(P, aP, bP) \in G_1$ for $a, b \in Z_q^*$, find the element abP.

- *Decision Diffie-Hellman (DDH) Problem:*

Given a quadruple $(P, aP, bP, cP) \in G_1$ for $a, b, c \in Z_q^*$, decide whether *c* = *ab* (mod *q*) or not.

- *Gap Diffie-Hellman (GDH) Problem:*

A class of problems where the CDH problem is hard but DDH problem is easy.

Groups where the CDH problem is hard but the DDH problem is easy are called Gap Diffie-Hellman (GDH) groups. Details about GDH groups can be found in [35, 36].

2.4 Short Signature Scheme

In [4], Boneh *et al.*'s gave a simple, deterministic signature scheme where the signatures are very short. Security is proven under the random-oracle model.

- *Key generation:*

The signer's secret key is a random number s chosen from Z_q^*. The public key, $P_{pub} = sP$, an element in G_1, $H : \{0,1\}^* \to G_1$ is a hash function.

- *Signing:*

The signature σ on message $m \in \{0,1\}^*$ is $sH(m)$ $(in\ G_1)$.

- *Verification:*

Check whether the following equation holds:

$$e(\sigma, P) = e(H(m), P_{pub}).$$

2.5 Model of Self-Certified Signatures

A sophisticated approach, first introduced by Girault [18], is called self-certified public key (SCPK), which can be regarded as intermediate between the identity-based approaches and the traditional PKI approaches. In this section, we first present a formal definition for self-certified signature (SCS) schemes. The two main entities involved in the SCS scheme are a certificate authority and a client. Then we propose a concrete SCS scheme from pairings. The SCS scheme consists of four randomized algorithms [37]: KeyGenparam, Extract, Sign, and Verify. The details are as follows.

- *KeyGenparam:*

The certificate authority CA chooses a master-key s and computes the corresponding public key P_{CA}. Each client U_A chooses partial private key s_A and computes the corresponding partial public key Y_A. The actual public key of the user consists of public key of CA, partial public key and identity of the user together with system parameters.

- *Extract:*

CA runs the extract algorithm, which takes as input the system parameters, the master-key s, the partial public key Y_A and an arbitrary $ID_A \in \{0,1\}^*$, the infinite set of all binary strings, and returns the partial private key d_A. The CA sends d_A securely to the client with (P_{CA}, ID_A, Y_A) over a public channel. The actual private key of the client is (s_A, d_A), the actual public key is (P_{CA}, ID_A, Y_A).

- *Sign:*

A client with his actual private key (s_A, d_A) uses the sign algorithm to compute signature σ for any message m.

- *Verify:*

Any verifier can validate the signature σ by checking the verification equation with respect to the actual public key (P_{CA}, ID_A, Y_A).

These algorithms must satisfy the standard consistency constraint, namely when (s_A, d_A) is the actual private key generated by algorithm Extract when it is given the actual public key (P_{CA}, ID_A, Y_A), then $\forall m \in \{0,1\}^*$:

$Verify((P_{CA}, ID_A, Y_A), m, \sigma) = Valid$ where

$\sigma = Sign(P_{CA}, ID_A, Y_A), (s_A, d_A), m)$

III. OUR PROPOSED SCHEME

In this section, we present the ID-Based knapsack-type public key short signature scheme based on the GDH groups.

3.1 Definition

Definition 1 (*Knapsack Diffie-Hellman*)**.** The following is the proposed computational knapsack Diffie-Hellman (CKDH) problem in G_1.

- *Given:*

$P, Q \in G_1$ (P is a generator), and

$(n+1) - tuple\ (P_1, P_2, ..., P_n, H)$, and

$P_i = b_i P (1 \le i \le n)$, and $H = tQ$; where

$b_i \in Z^+$ (Z^+ denotes the set of all positive integers)

$(b_1, b_2, ..., b_n)$ and t are all unknown elements.

- *Output:*

A binary string $x=(x_1,x_2,...,x_n)\in\{0,1\}^n$, which satisfies $e(\sum_{i=1}^{n}x_iP_i,Q)=e(H,P)$.

If there exists $x=(x_1,x_2,...,x_n)\in\{0,1\}^n$ such that $e(\sum_{i=1}^{n}x_iP_i,Q)=e(H,P)$, then we call $(P,Q,P_1,P_2,...,P_n,H)$ a knapsack Diffie-Hellman tuple. CKDH assumption is reasonable, since its computational complexity is comparable with the computational complexity of the computational Diffie-Hellman problem.

Definition 2 (*Decisional Posterior Knapsack Diffie-Hellman*). The decisional posterior knapsack Diffie-Hellman (DPKDH) problem is defined as follows:

- *Given:*

$P,Q\in G_1$ (P is a generator), and $(n+1)-tuple$ $(P_1,P_2,...,P_n,H)$, and $P_i=b_iP(1\le i\le n)$, and $H=tQ$; where $b_i\in Z^+$ (Z^+ denotes the set of all positive integers), $(b_1,b_2,...,b_n)$ and t are all unknown elements.

- *Output:*

Yes, if there exists an $x=(x_1,x_2,...,x_n)\in\{0,1\}^n$ such that $(P,Q,P_1,P_2,...,P_n,H)$ is a knapsack Diffie-Hellman tuple; Otherwise, output *No*.

DPKDH assumption is reasonable as well, since the DPKDH problem is computationally equivalent to the CKDH problem, while the CKDH problem's computational complexity is comparable with the computational complexity of the computational Diffie-Hellman problem.

3.2 Description of Our Signature Scheme

The detailed scheme is defined as follows.

Generate:

Step 1: The certificate authority CA selects two groups G_1,G_2 of order q, an admissible bilinear map $e:G_1\times G_1\to G_2$ and a random generator $P\in G_1$.

Step 2: Choose two cryptographic hash functions $H:G^*_1\times\{0,1\}^*\times G^*_1\to G^*_1$, $f:\{0,1\}^*\times G^*_2\times G^*_1\to Z^*_q$. The security analysis will view H, f as random oracles. The system parameters are Params $=\{q,G_1,G_2,e,P,H,f\}$.

Step 3: The CA picks a random $s\in Z_q^*$ as its private master-key and sets $P_{CA}=sP$ as its public key.

Step 4: Each user (U_A) with a given identity $ID_A\in\{0,1\}^*$, picks a random $s_A\in Z_q^*$ as its partial private key and sets $Y_A=s_AP$ as its partial public key.

- *Extract:*

U_A sends his (ID_A,Y_A) securely to the CA, after authenticating himself to CA. CA computes $H_A=H(P_{CA},ID_A,Y_A)\in G_1^*$ and sets the partial private key $d_A=sH_A$, where s is the master key of CA. Then CA chooses a random integer $r\in Z_q^*$ and computes

$$W=rP,$$
$$V=d_A+rY_A.$$

Finally CA sends (W,V) to U_A over a public channel. Registration must be in person or using some form of secure authenticated communication. U_A first recovers d_A by computing $d_A=V-s_AW$. Then U_A verifies d_A by checking the following equations:

$$H_A=H(P_{CA},ID_A,Y_A)$$
$$e(d_A,P)=e(H_A,P_{CA})$$

Here d_A is the secret certificate of the CA's public key P_{CA}, the partial public key Y_A and the identifier ID_A of U_A. Thus U_A obtains his actual private key (s_A,d_A). Hence, the certificate of the actual public key is used as the private key

for signing.

- *Signing:*

Assume Alice and Bob are the two users who join the signature interactively. Alice selects a sequence $\overline{B} = (b_1P, b_2P, ..., b_nP), (i.e., b_i > \sum_{j=1}^{i-1} b_j)$, and transfer $\overline{B}$ into a pseudorandom sequence $\overline{A} = (a_1P, a_2P, ..., a_nP)$ by the following modulo transformation: $a_i = b_i \times s_A \bmod q$, with $q > \sum_{i=1}^{n} b_i$. Signing the message m , computes $\lambda = h(m)$, here $h : \{0,1\}^* \to Z_q$ is a hash function, and picks up a random binary set $\overline{x} = (x_1, x_2, ..., x_n)$ then computes the x_i's whose corresponding bit is 1:

$$U_1 = \sum_{i=1}^{n} x_i b_i P,$$

$$U_2 = \lambda \sum_{i=1}^{n} x_i a_i P,$$

Alice computes

$$H_{Alice} = H(P_{CA}, ID_{Alice}, Y_{Alice})$$
$$r_{Alice} = e(U_2, P)$$
$$f_{Alice} = f(\lambda, r_{Alice}, H_{Alice})$$
$$V_{Alice} = U_2 + f_{Alice} H_{Alice} + f_{Alice}^2 d_{Alice}$$

Then Alice sends the signature $(P_{CA}, ID_{Alice}, Y_{Alice}, f_{Alice}, V_{Alice})$ *and* (U_1, U_2, m) to the Bob.

- *Verification*:

Bob checks whether the following equation holds:

$$H'_{Alice} = H(P_{CA}, ID_{Alice}, Y_{Alice})$$
$$r'_{Alice} = e(V_{Alice}, P) e(-H_{Alice}, fY_{Alice} + f^2 P_{CA})$$

Finally, Bob checks these equations

$$f_{Alice} \stackrel{?}{=} f(\lambda, r'_{Alice}, H'_{Alice}),$$
$$e(U_1, Y_{Alice})^{\lambda} = e(U_2, P)$$

Consistency: Because

$$\begin{aligned} e(V_{Alice}, P) &= e(U_2 + f_{Alice} H_{Alice} + f_{Alice}^2 d_{Alice}, P) \\ &= e(U_2, P) e((f_{Alice} + f_{Alice}^2 s_{Alice}) H_{Alice}, P) \\ &= r_{Alice} e(H_{Alice}, (f_{Alice} + f_{Alice}^2 s_{Alice}) P) \\ &= r_{Alice} e(H_{Alice}, f_{Alice} Y_{Alice} + f_{Alice}^2 P_{CA}) \end{aligned}$$

$$\begin{aligned} r'_{Alice} &= e(V_{Alice}, P) e(-H_{Alice}, f_{Alice} Y_{Alice} + f_{Alice}^2 P_{CA}) \\ &= r_{Alice} \end{aligned}$$

By convention, the output is verified as true if it accepts the self-certified signature and false otherwise.

IV. EVALUATION OF OUR SCHEME

In this section, we will first provide the security evaluation and analysis for the CKDH problem. The security of our signature scheme relies on the hardness of the Computational CKDH problem. Relations of knapsack Diffie-Hellman assumptions, we will proof the relations between the subset sum problem and the proposed knapsack Diffie-Hellman problems. We also prove the relations between the various Diffie-Hellman problems including CDH, DDH, CKDH and DPKDH in G_1 . Following that, we will analyze the various issues of security in the short signature protocols. In order to analyze the security of our blind scheme, we propose four challenged questions of attack to analyze the security.

- *Security consideration of bilinear map*

A bilinear pairing function $e : G_1 \times G_1 \to G_2$, given four elements $P, c_1P, c_2P, c_3P \in G_1$, compute $e(P, P)^{c_1c_2c_3}$, where c_1, c_2, c_3 are randomly chosen from Z_q^*. An algorithm is said to solve the CDH problem with an advantage of ε if $Pr[A(P, c_1P, c_2P, c_3P) = e(P, P)^{c_1c_2c_3}] \geq \varepsilon.$ The probability Pr is taken over the coin tosses of algorithm A [16]. The CDH problem is hard which means that there is no polynomial time algorithm to solve the CDH problem with non-negligible probability.

Proof. First, suppose CDH can be solved in time t with probability at least ε. We give an algorithm to show that the map is not (t,ε)-secure. Let $P,U,V \in G_1$ where both $U,V \neq P$ and $e(U,V) \neq 1$. We wish to find $H \in G_1$ such that $e(P,U) = e(H,V)$. Since G_1 is cyclic of prime order q there exists an $a \in Z_q^*$ such that $U = aV$. Let $H = aP$. Then H satisfies

$$e(H,V) = e(aP,V) = e(P,V)^a = e(P,aV) = e(P,U).$$

Therefore, $H = aP$, which is the solution to the CDH problem (P,V,U), is the required H. Hence, if the map is (t,ε)-secure then CDH is (t,ε)-hard. Conversely, suppose there is a t-time algorithm that given random (P,V,U) outputs $H \in G_1$ such that $e(P,U) = e(H,V)$ with probability at least ε. We show how to solve CDH. Let (P,V,U) be a random instance of the CDH problem, where $V \neq 1$. Write $U = aV$ for some $a \in Z_q^*$. Let H be such that $e(P,U) = e(H,V)$. Then $e(H,V) = e(P,U) = e(P,aV) = e(aP,V)$ and hence $e(H/aP,V) = 1$. Since $V \neq P$ it follows that $H = aP$, since otherwise the map e would be degenerate. Hence, if CDH is (t,ε)-hard then the map is (t,ε)-secure.

- *Security consideration of* CKDH

Under the condition that the discrete logarithm problem is hard in G_1 and G_2, the CKDH problem is computationally equivalent to the computational version of subset sum (SS) problem.

Proof. As the setting of Definition 3.1 in Section 3, we can draw the following equivalent relation:

$$e(\sum_{i=1}^{n} x_i P_i, Q) = e(H, P)$$

$$e(P,Q)^{\sum_{i=1}^{n} x_i b_i} = e(sQ, P)$$

$$e(P,Q)^{\sum_{i=1}^{n} x_i b_i} = e(Q,P)^s$$

$$e(P,Q)^{\sum_{i=1}^{n} x_i b_i} = e(P,Q)^s$$

Therefore, $\sum_{i=1}^{n} x_i b_i = s$. This is the general subset sum problem.

- *Security consideration of* DPKDH

The DPKDH problem is computationally equivalent to the CKDH problem.

Proof. If there is a polynomial time algorithm Ω which can solve the CKDH problem, then there is a polynomial time algorithm Ω' which can solve the DPKDH problem. In fact, given an instance of DPKDH problem $(P, Q, P_1, P_2, ..., P_n, sQ), \Omega'$ works as follows:

(1) Take this instance as the input of the oracle Ω, then Ω will return a solution $\bar{x} = (x_1, x_2, ..., x_n)$ (provided that such x exists) in polynomial time.

(2) Compute $A = \sum_{i=1}^{n} x_i P_i \in G_1$ in polynomial time.

(3) Check whether $e(\sum_{i=1}^{n} x_i P_i, Q) = e(sQ, P)$. If it holds, then output '*yes*'; otherwise, *no*.

(4) Given any instance of the DPKDH problem in G_1, Ω' can success as above the steps (1)-(3) in polynomial time.

If there is a polynomial time algorithm Ω which can solve the DPKDH problem, then there is a polynomial time algorithm Ω' which can solve the CKDH problem. In fact, given an instance of CKDH problem $(P, Q, P_1, P_2, ..., P_n, sQ), \Omega'$ works as follows:

(1) Take this instance as the input of the oracle Ω, then Ω will check whether there exists an $\bar{x} = (x_1, x_2, ..., x_n)$ (provided that such x exists) such that $e(\sum_{i=1}^{n} x_i P_i, Q) = e(sQ, P)$ in polynomial time.

(2) If such $\bar{x}$ exists, then output "*yes*"; otherwise, "*no*".

(3) Output that $\bar{x}$ in step (1). Therefore, $\bar{x}$ is a solution to the instance $(P, Q, P_1, P_2, ..., P_n, sQ)$ of CKDH.

- *Security consideration of our protocol*

Under the condition that ECDL problems are hard in G_1 and G_2, the CDH, CKDH and DPKDH problem is computationally equivalent to the computational version of subset sum problem.

Proof. As the setting of definition in Verification, we can draw the following equivalent relation:

$$e(U_1, Y_{Alice})^{\lambda} = e(\sum_{i=1}^{n} x_i b_i P, s_{Alice} P)^{\lambda}$$

$$= e(P,P)^{\lambda \cdot s_{Alice} \sum_{i=1}^{n} x_i b_i}$$

$$e(U_2, P) = e(\lambda \sum_{i=1}^{n} x_i a_i P, P)$$

$$= e(P,P)^{\lambda \sum_{i=1}^{n} x_i a_i}$$

$$= e(P,P)^{\lambda \cdot s_{Alice} \sum_{i=1}^{n} x_i b_i}$$

Therefore $\sum_{i=1}^{n} x_i b_i$, this is a subset problem.

In this scheme, an adversary tries to reveal the message from the public key for any user. First, any adversary must solve the ECDLP problem given by Y_{Alice} to determine s_{Alice}. Second, the adversary must solve the NPC problem to determine the message from (U_1, U_2). Given that (U_1, U_2) are publicly known information, deriving s_{Alice} is unfeasible.

- *Security under impersonation attack*

An impersonation-attack characteristic is that any attacker can, without stealing the identities, easily masquerade as a legitimate user at any time.

Proof. Alic*e* selects a sequence $\overline{B} = (b_1 P, b_2 P, ..., b_n P)$ and transfer $\overline{B}$ into a pseudorandom sequence $\overline{A} = (a_1 P, a_2 P, ..., a_n P)$ and picks up a random binary set $\overline{x} = (x_1, x_2, ..., x_n)$ then computes the x_i's whose corresponding bit is 1: $U_1 = \sum_{i=1}^{n} x_i b_i P$, $U_2 = \lambda \sum_{i=1}^{n} x_i a_i P$. Signing the message m, Alice sends the signature (U_1, U_2, m) to the Bob.. Accordingly, an adversary can play the role of $U_{Alice'}$ to forge $ID_{Alice'}$. However, before the attacker chooses the binary vector $\overline{x'}$ and secret keys $(s_{A'}, d_{A'})$, to obtain the verification is required. As mentioned above, the attacker must again solve the Knapsack and Bilinear pairing problems.

- *Security under man-in-the-middle attack*

When U_{Alice} sends $(P_{CA}, ID_{Alice}, Y_{Alice}, f_{Alice}, V_{Alice})$ to U_{Bob}, an adversary can intercept the datum from the public channels, and then play the role of U_{Alice} to cheat U_{Bob} or other users by $(P_{CA}, ID_{Alice}, Y_{Alice}, f_{Alice}, V_{Alice})$.

Proof. The attacker does not pass the verification of $f_{Alice} \stackrel{?}{=} f(\lambda, r'_{Alice}, H'_{Alice})$, and $e(U_1, Y_{Alice})^{\lambda} = e(U_2, P)$. Nevertheless, we know that obtaining (s_A, d_A) from f_{Alice} is equal of computing the Knapsack and Bilinear pairing assumptions.

- *Security consideration of the malicious CA attack*

An intruder might try to impersonate *CA* by determining a relationship from the public message for (W, V).

Proof. We say that a self-certified scheme is presently counterfeited against adaptive chosen message attack if no polynomial bounded adversary A has a non-negligible advantage against the challenger in the following game: The challenger takes the security parameters (s', d_i') and runs the generate algorithm. It gives the adversary the resulting system parameters and a public key P_{CA} of the CA. If an attacker attempts to carry out an attack by revealing the private key (s', d_i') from the public key of the (W, V), then he or she can play the role of (ID_i, CA) to forge. In case of that, the attacker must solve the CKDH problem given by (W, V) to determine (s', d_i')

VI. EFFICIENCY

ECC delivers the highest strength per bit of any known public-key system because of the difficulty of the hard problem upon which it is based. This greater difficulty of the hard problem - the elliptic curve discrete logarithm problem (ECDLP) - means that smaller key sizes yield equivalent levels of security. In practice, the size of the element in group G_1 can be reduced by a factor of 2 using compression techniques. So, like BLS scheme [4], our signature scheme is a short IBS scheme. If we choose a group and the bilinear map from elliptic curves [4], which results in a group of 160 bits size, signatures generated by our scheme is 160 bits length which is half–size compared to the proposed IBS schemes [5, 6, 7, 8, 9, 10, 11]. A comparison between our IBS scheme with other schemes is listed in Table 1.

VI. CONCLUSIONS

We have proposed a secure and robust short signature scheme using self-certified public keys from pairings, which combines the best aspects of identity-based (implicit certification) and public key signatures (no key escrow). The users can choose their secret information independently. The actual public key consists of the partial public key chosen by the user and the public key of the certificate authority explicitly. The scheme was proven as secure as the short signature scheme in random oracle model. In addition, it is best to compare systems based on the best knowledge currently available, and only then consider less tangible factors, like guessing the likelihood of new developments in mathematics. The dilemma for the cryptosystem designer is that a trapdoor is easily discovered if the knapsack density is high. This letter proposed a new short signature design that fully exploits the difficulty of the knapsack and GDH problem with a difficult-to-discover trapdoor. The proposed schemes have three notable advantages: (1) the scheme does not need an on-line CA to verify a blind signature and the validity of public key; (2) when verifying the validity of public key, it does not need to spend extra much time to verify the signature in the digital certificate used in the certificate-based public key cryptosystem; (3) security depends on the computational complexity of multiple assumptions.

REFERENCES

[1] Shi, W., and Zhou, Y., "An Improvement of Sui et al's Second ID-based Key Issuing Protocol" , The 3rd International Conference on Innovative Computing Information and Control (ICICIC'08), 18-20 June 2008, pp. 114-117.

[2] Shamir, A., "Identity-based cryptosystems and signature schemes", in Proc. Crypto'84, Santa Barbara, CA, Aug. 1984, pp. 47-53.

[3] Guillou, L.C., and Quisquater, J.J., "A'paradoxical' identitybased signature scheme resulting from zero-knowledge", in Proc. Crypto'88, Santa Barbara, CA, Aug. 1988, pp. 216-231.

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

[5] Cha, J.C., and Cheon, J.H., "An identity-based signature from gap diffie-hellman groups", Cryptology ePrint Archive, Report 2002/018, 2002.

[6] Hess, F., "Efficient identity based signature schemes based on pairings", In Proceedings of 9th workshop on selected areas in Cryptography - SAC 2002, LNCS, Springer-Verlag(2002), pp. 310-324.

[7] Paterson, K.G., "Id-based signatures from pairings on elliptic curves", Cryptology ePrint Archive, Report 2002/004, 2002.

[8] Smart, N.P., "An identity based authenticated key agreement protocol based on the weil pairing", Electronic Letters, 38(13), 2002, pp.630-632.

[9] Yi, X., "An Identity-Based Signature Scheme from the Weil Pairing", IEEE Communications Letters, Vol. 7(2), 2003, pp. 76-78.

[10] Cha, J.C., and Cheon, J.H., "An identity-based signature from gap Diffie-Hellman groups", PKC 2003, LNCS 2567, Springer-Verlag(2003), pp. 18-30.

[11] Cheng, X. G., Liu, J. M., and Wang, X.M., "Identity-based aggregate and verifiably encrypted signatures from bilinear pairing",

2005ICCSA, Berlin Heidelberg, LNCS 3483, Springer-Verlag(2005), pp. 1046-1054.

[l2] Okamoto, T., Inomata, A., and Okamoto, E., "A proposal of short proxy signature using pairing", In the proceedings of the international Conference on Information Technology: Coding and Computing (ITCC05), 2005, pp.631-635.

[13] Zhang, Z., and Chen, X., " Yet Another Short Signatures Without Random Oracles from Bilinear Pairings", ICAR Cryptology ePrint Archive, available at http://eprint.iacr.org , 2005.

[14] Zhang, Z., and Chen, X., "Yet Another Short Signatures Without Random Oracles from Bilinear Pairings", ICAR Cryptology ePrint Archive, available at http://eprint.iacr.org , 2005.

[15] Yoon, H., Cheon, J.H., and Kim, Y., "Batch verifications with ID-based signatures", ICISC 2004, LNCS 3506, Springer-Verlag (2005), pp. 223-248.

[16]. Boneh, D., and Franklin, M., "Identity-based encryption from the weil paring", Proc. CRYPTO 2001, Springer-Verlag (2001), pp. 213-229.

[17] Du, H., and Wen, Q., "An Efficient Identity-based Short Signature Signature Scheme from Bilinear Pairings" , 2007 International Conference on Computational Intelligence and Security, 2007, pp. 725-729.

[18] Girault, M., "Self-certified public keys", Proceedings of the Eurocrypt'91, 1991, pp. 491-497.

[19] Saeednia, S., "Identity-based and self-certified key exchange protocols", Proceedings of Second Australasian Conference on Information Security and Privacy (ACISP_97)LNCS, vol. 1270, Springer-Verlag(1997), New York, pp. 303-313.

[20] Wu, T.C., Chang, Y.S., and Lin, T.Y., "Improvement of Saeednia's self-certified key exchange protocols", Electronics Letters, 34 (11), 1998, pp. 1094-1095.

[21] Kim, S., Oh, S., Park, S., and Won, D., "On Saeednia's key-exchange protocols, in: Proceedings of KICS_98", Korean Institute of Communication Sciences Summer Conference ,17 (2), 1998, pp. 1001–1004.

[22] Saeednia, S., "A note on Girault's self-certified model", Information rocessing Letters 86 , 2003, pp.323-327.

[23] Rivest, R., Shamir, A., and Adleman, L., "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 21 (2) , 1978, pp.120-126.

[24] Tsaur, W. J., "Several security schemes constructed using ECC-based self-certified public key cryptosystems", Applied Mathematics and Computation, 168, 2005, pp.447-464.

[25] Diffie, W., and Hellman, M.E., "New directions in Cryptography", IEEE Transactions on Information Theory, Vol. 22(6), 1976, pp. 644-654.

[26] Merkle, R., and Hellman, M.E., "Hiding information and signatures in trapdoor knapsack", IEEE Transactions on Information Theory, Vol. 24(5), 1978, pp. 525-530.

[27] Su, P.C., Lu, E.H., and Chang, H.C.C., "A knapsack public-key cryptosystem based on elliptic curve discrete logarithm", Applied Mathematics and Computation Vol. 168(1), 2005, pp. 40-46.

[28] Shim, K., "Efficient one round tripartite authenticated key agreement protocol from Weil pairing", Electronics Letters, Vol. 39(2), 2003, pp. 208-209.

[29] Dutta, R., Barua, R., and Sarkar, P., "Pairing-based cryptographic protocols : a survey ", Cryptology ePrint Archive, Report 2004/064, 2004.

[30] Han, S., Chang, E., and Dillon, T., "Knapsack Diffie-Hellman: a new family of Diffie-Hellman", Cryptology ePrint Archive: Report 2005/347, pp. 1-17. http://eprint.iacr.org/2005/347.

[31] Michael, R., and David, S., Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman & Co., New York, 1979.

[32] Miller, V., "Use of Elliptic curves in Cryptography", Advances in Cryptology-CRYPTO 85, LNCS, Springer-Verlag(1986), Vol. 218, pp. 417-426.

[33] Koblitz, N., "Elliptic Curves Cryptosystems", Mathematics of computation, Vol. 48(177), 1987, pp. 203-209.

[34] Sadeghi, A.R., and Steiner, M., "Assumptions related to Discrete

Logarithms: Why Subtleties Make a Real Difference", Advances in Cryptology - EUROCRYPT 2001, LNCS 2045, Springer-Verlag(2001), pp.244-261.

[35] Tan, Z., Liu, Z. and Tang, C., "Digital proxy blind signature schemes based on DLP and ECDLP", MM Research Preprints, No. 21, 2002, pp.212-217.

[36] Lysyanskaya, A., and Ramzan, Z., "Group blind digital signatures: A scalable solution to electronic cash", Financial Cryptography, LNCS 1465, Springer-Verlag(1998), pp.184-197.

[37] Shao, Z., "Self-certified signature scheme from pairings", Journal of Systems and Software, 2007, 80, (3), pp. 388-395.

Table 1. Efficiency comparisons

Scheme	BLS[4]	CLW[11]	YCK[15]	The proposal
Signing method	Deterministic	Deterministic	Deterministic	Probabilistic
IBS	NO	YES	YES	YES
self-certified approach	NO	NO	NO	YES
Signing algorithm	Diffie-Hellman	Diffie-Hellman	Diffie-Hellman	Knapsack Diffie-Hellman