Efficient Identity Based Signature in Standard Model

Parampalli Udaya, Shivaramakrishnan Narayan
DraftV1.6 29/05/2007

Department of Computer Science and Software Engineering,
University of Melbourne,
Victoria - 3010, Australia.
{udaya,narayans}@csse.unimelb.edu.au

Abstract. In this paper, we present an efficient signature scheme without random oracles using Waters private key construction. Our scheme has shorter public parameter size when compared to Kenny and Schuldt signature, the signature space of our basic scheme consists of three group elements, we further show that the signature space can be reduced to two group elements. In addition, we define a strong-signature version of our basic scheme. The security of our signature scheme is proved in the standard model under adaptive identity security notion.

Keywords: Identity Based Cryptography, Standard Model, Signature, Bilinear Maps.

1 Introduction

The concept of identity (ID) based cryptography (IDC) dates back to 1984 with the work of Shamir [1]. The field of IDC gained focus since 2000 when Sakai, Ohgishi and Kasahara [2, 3], and Boneh-Franklin [4] independently presented concrete ID-based encryption schemes using bilinear pairing. Following the results in 2001, many cryptographic primitives using bilinear maps were proposed [5–16]. These schemes were provably secure using the most common, and well known standard namely, the random oracle model [17]. A scheme which is provably secure in random oracle model rely on the existence of random functions (or in other words hash functions which are perceived to be random oracles). Security in the random oracle model is sufficient in practice. However, there are examples of schemes [18, 19] which are secure in the random oracle model but are prone to cryptographic attacks, when the random oracles are replaced by collision resistant functions.

Since 2004, the standard model proving technique in cryptography has found interest. The standard model technique of proving security of a cryptographic scheme uses no random functions. Here, a proof is desired such that, an adversarial algorithm succeeding in breaking the scheme under an attack, necessarily leads to a reduction in solving the underlying hard mathematical problem. Having such a proof without the assumption of random functions is always a challenging

task. In the standard model, the adversary performs most of the computations without relying on any other entity unlike in the random oracle model.

The first fully secure encryption scheme proved in the standard model was constructed by Boneh-Boyen in 2004 [20], however this was not computationally efficient. Earlier in the same year, Boneh-Boyen presented an efficient encryption scheme proved in slightly weaker notion of security namely selective identity model [21]. In this model, the adversary has to commit to an identity before starting the attack game. Later in 2005, Waters presented the first encryption scheme secure under adaptive identity model which was computationally efficient. The only drawback of this scheme is its long public parameter size. The key construction given by both, Boneh-Boyen and Waters was of interest because, it could be thought of as a signature. Following Waters result, Kenny and Schuldt in 2006 presented the first signature [22] in the standard model provably secure in adaptive identity notion of security. Their scheme based on Waters key construction was computationally efficient, but the main drawback was the public parameter size which is almost doubled compared to that of Waters scheme.

1.1 Motivation and Contribution

The evolving internet and its applications requires secure and authentic data transmission over insecure channels. This can be achieved using cryptographic primitives like encryption and signature, which have to be provably secure in the best known adversarial model. With the increase in computational power of the adversaries, there is a necessity to define a security model in which an adversary is independent, like in a real attack. Though random oracle methodology is practical, it is evident that the adversarial power is limited (relies on an entity namely, "challenger" for random oracle queries) unlike the standard model. Since 2004, many encryption schemes [21, 20, 23, 24] have been defined in the standard model which are provably secure in either selective ID or adaptive ID notion. Among those defined till date, the scheme presented by Gentry [24] is the most efficient in terms of computation and tightness of security reduction. Authentication schemes in the standard model have been proposed by Boneh-Boyen [25], Ateniese et al. [26] and M.H. Au et al. [27, 28]. The construction of ID-based signature using generic signature (uses certificates) has been addressed in [29–31]. Although this results in ID-based signature, the scheme is highly inefficient. The first ID-based signature in the standard model was presented by Kenny and Schuldt [22] based on the hardness of computational Diffie-Hellman problem. This scheme suffers from large public paramter size due to the way the messages are represented. One of our main contribution is reduction in the public parameter size, in addition we present a strong signature version of our basic scheme. To improvize the scheme efficiency, we present how to reduce the signature space of the signature. Lastly, our construction provides a better security reduction when compared to

[22]. A scheme is said to have tight reduction if the probability ϵ of breaking the scheme in time t is equivalent to the probability ϵ' of solving the underlying mathematical assumption in time t' such that $t \simeq t'$.

In this paper, we present an efficient signature scheme with compact public parameter size. The signature we present is highly efficient and secure against the known existential unforgeability attack in adaptive identity notion of security in the standard model. The scheme is based on the intractability of computational Diffie-Hellman problem. We achieve almost fifty percent reduction in the public parameter size when compared to Kenny and Schuldt scheme [22] and also better security reduction. Further space reduction can be achieved by applying Chatterjee-Sarkar [32] approach.

1.2 Paper Outline

In Section 2, we present the necessary mathematical preliminaries and the related complexity assumptions. The security model for our signature scheme is detailed in Section 3, followed by our signature construction and a note on its efficiency in Section 4. Section 5 presents a detailed proof of our signature scheme. Finally, Section 6 presents our conclusion.

2 Background

Before we decribe the construction of our scheme, we present a brief overview of the notations and other basic mathematical assumptions followed in this paper.

2.1 Bilinear Maps

Let G and G_1 be multiplicative groups of prime order q. Let Z_q^* denote the set of all non-zero integers modulo prime q. A bilinear map is a map $\hat{e} : G \times G \rightarrow G_1$, satisfying the following properties.

1. **Bilinear:** For all $g, g_1 \in G$ and $a, b \in Z_q^*$, we have $\hat{e}(g^a, g_1^b) = \hat{e}(g, g_1)^{ab}$.
2. **Non-degenerate:** $\hat{e}(g, g) \neq 1$.
3. **Efficiently Computable:** We say that the bilinear map $\hat{e}$ is efficiently computable if there exists algorithm to perform the group action in G and there exists a group G_1 such that the map structure holds good.

2.2 Admissible Collision-Resistant Functions

In the signature construction, we assume the existence of collision resistant functions. In our scheme, we use injective mapping of the nature $\{0,1\}^* \longrightarrow G$ which can constructed as given in [23] and $\{0,1\}^n \longrightarrow Z_q^*$ which can be constructed using general hash functions like SHA, MD-5, etc. While proving the security of the signature scheme, we assume the existence of such injective mapping so that one can use any cryptographic hash if needed.

2.3 Complexity Assumptions

Computational Diffie-Hellman Assumption (CDH) Given $(g, g^a, g^b) \in G$, where $a, b \in Z_q$, the computational Diffie-Hellman assumption states that there exists no (t, q_r, ϵ) adversary $\mathcal{A}$ which can solve the computational Diffie-Hellman problem of computing g^{ab} in time t and q_r queries, with a probability of at least ϵ.
We say that an adversary $\mathcal{A}$ has an advantage ϵ if,

$$\Pr[\mathcal{A}(g, g^a, g^b) = g^{ab}] \geq \epsilon,$$

where the probability (Pr) is over randomly chosen a, b.

3 Security Notions

This section briefly describes the security attack game for signature.

3.1 Security Notion of Signature - Existential Unforgeability

Definition 3.11 *We say that an ID-based signature scheme (IDS) has existential unforgeability property against adaptive identity chosen-message attack or (EUF-IDS-CMA), if no polynomially bounded adversary $\mathcal{A}$ has a non-negligible advantage in the following attack game.*

Setup: The challenger runs the **Setup** algorithm of the scheme and sends the global system parameter to the adversary $\mathcal{A}$.

Phase 1**:** $\mathcal{A}$ performs polynomially bounded number of queries as follows:

- **Extract:** The adversary submits an identity to the challenger. The challenger responds with the secret key for that identity.
- **Sign:** The adversary submits a sender identity and a message to the challenger. The challenger responds with the signature of the message processed with private key of the sender.

Forge: The adversary chooses a challenge identity ID^* and returns a signature forgery Z on a message M.

Response: The adversary wins if $ID_i \neq ID^*$ and **Verify**$(Z, M, ID^*) = \top$. The adversary should not have made extract query on ID^* and the forgery did not result from a sign query made to **Sign** algorithm using (M, ID^*).

The adversary's advantage is defined to be $Adv(\mathcal{A}) = \Pr[\mathcal{A}wins]$[1].

[1] Pr[] denotes probability of an event occurring.

4 Our Signature Scheme

In this section, we present our signature construction which has reduced public parameter size when compared to [22].

Setup:

1. Let $g \in G$ denote a generator of order q and $g_2, u' \in_R G$
2. Assign $g_1 = g^s$,where $s \in_R Z_q^*$ is kept private.
3. Let $\vec{U} = (u_i)$ be a vector of length n_u whose entries are random elements from G.
4. $H_u : \{0,1\}^{n_u} \longrightarrow G$ which can be computed as follows:
$$g_{ID} = u' \prod_{i \in \mathcal{V}} u_i,$$
$\mathcal{V} \subseteq \{1, ...n\}$ for a given identity v denotes the set of all i's such that $v_i = 1$.
5. $H_m : \{0,1\}^{n_m} \longrightarrow Z_q^*$ where n_m is the length of the message string.

The public parameter for the system is $params = \left(g, g_1 = g^s, g_2, u', \vec{U}, H_u, H_m\right)$.

Extract:

1. Let $r \in Z_q^*$.
2. $K = g_2^s \ (g_{ID})^r$, where $g_{ID} = H_u(\text{“}Identity\text{”})$.
3. $d_{ID} = (K, g^r)$.

Sign:

1. $t \in Z_q^*$.
2. $m' = H_m(M)$.
3. $Z = g_A^{tm'} \ d_A[1] = g_A^{tm'} \ K_A$.
4. Send $(Z, U = g^t, V = g^{r_A})$.

Verify:

1. $m' = H_m(M)$.
2. Accept M if,
$$\hat{e}(g, Z) = \hat{e}(g_1, g_2) \ \hat{e}(V, g_A) \ \hat{e}(U, g_A^{m'}).$$

4.1 Efficiency of Our Scheme

The security of our scheme relies on the intractability of computational Diffie-Hellman problem. In regards to the time complexity of our scheme compared to Kenny and Schuldt [32], our scheme uses $O(n)$ multiplications in both extract and sign queries, and $O(1)$ exponentiations.in both extract and sign queries. If t is the time taken by adversary $\mathcal{A}$, then the time taken by $\mathcal{B}$ is given by, $t + O((Q_e.n + Q_s.n)\rho + (Q_e + Q_s)\tau)$. Our signature proves to be efficient in terms of public parameter size $(G^4 \times G^{n_u})$ and also saves one group exponentiation over G when compared to [22].

In order to reduce the public parameter size without any loss of security, we can apply the idea suggested by Chatterjee-Sarkar for Waters Scheme. This is done by increasing the size of G which in turn increases the security level provided

by G to compensate the loss of security. But by using this approach we would increase the computational cost of the scheme. A detailed approach in achieving reduced public parameter size with a trade off in computational cost can be found in [32].

Reducing Signature Space The signature scheme presented above can be further improvised in terms of signature space with an additional cost of exponentiation over G. We outline the short signature version of our scheme below:

Sign:

1. $t \in Z_q^*$.
2. $m' = H_m(M)$.
3. $Z = g_A^{tm'}\ d_A[1] = g_A^{tm'}\ K_A$.
4. Send $\left(Z, U = g^{t+(m')^{-1}r_A}\right)$.

Verify:

1. $m' = H_m(M)$.
2. Accept M if,

$$\hat{e}(g, Z) = \hat{e}(g_1, g_2).\hat{e}(U, g_A^{m'}).$$

The above transformation results in short signature pair which of size $160 - 512$ bits depending on the class of elliptic curve used. It reduces one pairing operation, at a cost of one exponentiation over G.

4.2 Strong Signature Version of Our Scheme

As pointed out by Boneh-Boyen in [25], for some applications the signature might have to exhibit the property of strongness. This means, an adversary should not be able to create another signature for a message given its signature. We show how we can achieve this property for the basic version of our scheme given above.

Sign:

1. $t \in Z_q^*$.
2. $m' = H_m(M)$.
3. $Z = g_A^{\frac{1}{t+m'}}\ d_A[1] = g_A^{\frac{1}{t+m'}}\ K_A$.
4. Send $\left(Z, U = g^{\frac{1}{t+m'}+r_A}\right)$.

Verify:

1. $m' = H_m(M)$.
2. Accept M if,

$$\hat{e}(g, Z) = \hat{e}(g_1, g_2)\ \hat{e}(U, g_A).$$

5 Security Proof - Existential Unforgeability

Theorem 5.01 *If there is an adversary $\mathcal{A}$ that succeeds against the EUF-IDS-CMA security of our scheme with probability ϵ and making Q queries. Then there is a challenger (ϵ', Q')-$\mathcal{B}$ running in polynomial time that solves the CDH problem with a probability at least $\frac{\epsilon}{4(n+1)(Q_e+Q_s)}$.*

Proof 5.01 *Let $\mathcal{A}$ be an adversary having an advantage (ϵ, Q) in breaking the scheme under chosen message attack. We show how to construct an algorithm $\mathcal{B}$ which learns from the adversary and solves the CDH assumption with an advantage (ϵ', Q'). We present the proof along the lines of [23, 22].*
The challenger will be given a generator g of group G and the elements g^a and g^b. In order to learn from the adversary $\mathcal{A}$ on how to solve the CDH problem, the challenger must simulate an environment as in a real attack and should be able to answer $\mathcal{A}$'s queries effectively without aborting the simulation. Such a simulation can be created in the following way:

Setup:

The challenger sets $m = 2(Q_e+Q_s)$, where Q_e is the number of queries made to the extract oracle and Q_s is the number of queries made to the signature oracle. Let n denote the length of an identity, the challenger then chooses $k \in_R Z_n$. We will assume that $m(n+1) < q$, for a given Q_e, Q_s and n. The challenger then chooses $x' \in_R Z_m$ and a random n-length vector, $\overrightarrow{X} = (x_i)$, where the elements of $\overrightarrow{x}$ are chosen uniformly random from the integers between 0 and $m-1$. Additionally, the challenger chooses a random $y' \in Z_q$ and an n-length vector $\overrightarrow{y} = (y_i)$, where the elements of $\overrightarrow{Y}$ are chosen at random in Z_q. These values are kept internal and is not a part of public parameter.
For an identity u, we define the following functions,

$$F(u) = x' + \sum_{i \in \mathcal{U}} x_i - mk, \tag{1}$$

$$J(u) = y' + \sum_{i \in \mathcal{U}} y_i, \tag{2}$$

where $\mathcal{U} \subseteq \{1, ...n\}$, given an identity denotes the set of all i such that $u_i = 1$.
Now, $\mathcal{B}$ constructs a set of public parameter which is given to the adversary as follows.

$$g_1 = g^a,\ g_2 = g^b$$
$$u' = g_2^{-mk+x'}\ g^{y'}$$
$$u_i = g_2^{x_i}\ g^{y_i}$$

The above given public parameters will have the uniform random distribution in the game is played between $\mathcal{A}$ and $\mathcal{B}$. The master secret for the scheme will be $g_2^a = g^{ab}$. The public key generation would be as given below:

$$g_u = u' \prod_{i \in \mathcal{U}} u_i = g_2^{-mk+x'} \ g^{y'} \ \prod_{i \in \mathcal{U}} g_2^{x_i} \ g^{y_i}$$
$$g_u = g_2^{x'-mk+\sum_{i \in \mathcal{U}} x_i} \ g^{y'+\sum_{i \in \mathcal{U}} y_i}$$
$$g_u = g_2^{F(u)} g^{J(u)}$$

Phase 1**:**

In Phase 1*, the adversary is allowed to ask extraction and signature queries. $\mathcal{B}$ answers the queries of $\mathcal{A}$ as follows.*

Extract Queries: *Consider a private key for identity u. $\mathcal{B}$ is not privy to the master secret in the game. However, assuming $F(u) \neq 0 \pmod q$, the private key can be constructed by choosing $r_u \in_R Z_q$ as given below:*

$$d_u = (d_0, d_1) = \left(g_1^{-J(u)/F(u)} \ g_u^{r_u}, g_1^{-1/F(u)} \ g^{r_u} \right).$$

Let $\bar{r}_u = r_u - \frac{a}{F(u)}$, we can show that how the above key results in a valid private key of identity u as in a real construction.

$$d_0 = g_1^{-J(u)/F(u)} \ g_u^{r_u}$$
$$d_0 = g_2^a . (g_2^{F(u)} \ g^{J(u)})^{-a/F(u)} \ g_u^{r_u}$$
$$d_0 = g_2^a \ (g_u)^{-a/F(u)} \ g_u^{r_u}$$
$$d_0 = g_2^a \ g_u^{\bar{r}_u},$$

and

$$d_1 = g_1^{-1/F(u)} \ g^{r_u}$$
$$d_1 = g^{-a/F(u)} \ g^{r_u} = g^{\bar{r}_u}.$$

Thus, the key $d_u = (d_0, d_1)$ is a valid private key construction for an identity u.

$\mathcal{B}$ can construct the private keys for all identities apart from those for which $F(u) = 0 \pmod q$. The simulation will abort for such cases. For the sake of our analysis we assume that the simulation would abort if $F(u) = 0 \pmod m$. Given the assumption that $m(n+1) < q$, which implies $0 \leq mk < q$ and $0 \leq x' + \sum_{i \in \mathcal{U}} x_i < q$, it is evident that $F(u) = 0 \pmod q$ implies $F(u) = 0 \pmod m$.

Sign Queries:

Consider a signature query on a given message M for u, assuming that $\mathcal{A}$ has not made an extraction query on the identity u. If $F(u) \neq 0 (\text{mod } m)$, $\mathcal{B}$ can construct a private key for the identity u and then uses the signature algorithm to present a signature of u given an message M as given below.

1. $t \in Z_q^*$.
2. $M' = H_m(M)$.
3. $Z = g_u^{tM'} \ d_u[1] = g_u^{tM'} \ g_2^a \ g_u^{r_u}$.

For $F(u) = 0 \pmod m$, $\mathcal{B}$ can construct a signature given an message M as given below.

1. *Select a random u_i such that $F(u_i) \neq 0 \pmod m$.*

2. $t \in Z_q^*$.
3. $M' = H_m(M)$.
4. $Z = g^{M't}\ d_{u_i}[1] = g^{tM'}\ g_2^a\ g_{u_i}^{r_{u_i}}$.
5. *For* $F(u) = 0\ (mod\ m)$, $g_u = g^{J(u)}$, *let* $u'' = J(u)$.
6. *Send* $(Z,\ U = g^{u''^{-1}t},\ V = g^{r_{u_i}u''^{-1}})$.

Forgery:

If $\mathcal{B}$ *does not abort, the adversary will return* (u^*, M^*, C^*) *with a probability* ϵ, *where* $C^* = (Z, A = g^t, B = g^{r_{u^*}})$ *a valid signature forgery of* (u^*, M^*). *If* $F(u^*) \neq 0(mod\ q)$ *then* $\mathcal{B}$ *will abort. If on the other hand* $F(u^*) = 0(mod\ q)$, $\mathcal{B}$ *solves the CDH problem as given below:*

$$\frac{Z}{A^{J(u^*)}\ b^{J(u^*)}} = \frac{g_2^a\ g_{u^*}^{r_{u^*}}\ g_{u^*}^{M'\ t}}{g_{u*}^{t\ M'}\ g_{u^*}^{r_{u^*}}} = g^{ab}$$

This completes the description of the simulation. In order to assess the probability of success of $\mathcal{B}$ *we have to analyse the probability of* $\mathcal{B}$ *not aborting. For the simulation to be complete without aborting, it is necessary that identities on which the extraction query was made should satisfy the condition* $F(u) \neq 0(mod\ m)$, *the signature queries made on all* (u, M) *pair should have* $F(u) \neq 0(mod\ m)$. *Thus, we present a lower bound on the probability that* $\mathcal{B}$ *aborts.*
Let us look at the probability of $\mathcal{B}$ *not aborting such that* $u \neq u^*$ *and all identities have* $F(u) \neq 0(mod\ m)$. *Consider* $u_1, ...u_{Q_I}$ *as the identities appearing in either extract queries or in signature queries not involving the challenged identity. Then we have,* $Q_I \leq Q_e + Q_s$ $\dashv$. *Let* E_1, E_2 *be two events such that,*

E_1**:** $F(u_i) \neq 0\ (mod\ m)$
E_2**:** $F(u^*) = 0\ (mod\ q)$.

The probability of $\mathcal{B}$ *not aborting is,*

$$\Pr[\neg abort] \geq \Pr[\bigwedge_{I=1}^{Q_I} E_1 \wedge E_2].$$

Since $m(n+1) < q$, $F(u) = 0(mod\ q) \implies F(u) = 0(mod\ m)$*is true for certain* u, *there exists an unique* k *in the range* $[0, n]$ *such that* $F(u) = 0(mod\ q)$. *Since* k, x' *and* $\overrightarrow{X}$ *are chosen at random, we have*

$$Pr[E_2] = Pr[F(u^*) = 0(mod\ q) \wedge F(u^*) = 0(mod\ m)]$$
$$Pr[E_2] = Pr[F(u^*) = 0(mod\ m)]Pr[F(u^*) = 0(mod\ q)|F(u^*) = 0(mod\ m)]$$
$$Pr[E_2] = \frac{1}{m}\ \frac{1}{n+1}$$

Thus, the success of $\mathcal{B}$ *can be calculated as follows.*

$$\Pr[\bigwedge_{I=1}^{Q_I} E_1 \wedge E_2] = \Pr[E_2]\Pr[\bigwedge_{I=1}^{Q_I} E_1|E_2].$$

We know that,

$$\Pr[\bigwedge_{I=1}^{Q_I} E_1|E_2] = 1 - \Pr[\bigvee_{I=1}^{Q_I} \neg E_1|E_2] = 1 - \sum_{I=1}^{Q_I} \Pr[\neg E_1|E_2].$$

If $F()$ is evaluated for two identities u_1 and u_2, the sum would differ in atleast one randomly chosen value and the events $F(u_1) = 0(mod\ m)$ and $F(u_2) = 0(mod\ m)$ will be independent. Thus the events E_1 and E_2 are independent for any i, and $Pr[\neg E_1|E_2]=\frac{1}{m}$. Therefore we have,

$$\Pr[\bigwedge_{I=1}^{Q_I} E_1 \wedge E_2] = \frac{1}{m(n+1)}\ (1 - \frac{Q_e + Q_s}{m}).$$

Let $m = 2(Q_e + Q_s)$, thus we get,

$$\Pr[\bigwedge_{I=1}^{Q_I} E_1 \wedge E_2] \geq \frac{1}{4(n+1)(Q_e + Q_s)}.$$

Thus, the probability of simulation not aborting is equivalent to $\mathcal{A}$ creating a valid forgery with a probability atleast ϵ. This provides us the success probability of $\mathcal{B}$ in solving CDH problem which is atleast,

$$\frac{\epsilon}{4(n+1)(Q_e + Q_s)}.$$

5.1 Security Reduction and Improving Efficiency

The reduction achieved by our construction is comparitively better than [22]. This is because in [22], the signature construction by the challenger is based on $F(u) \neq 0$ and $(F(u) = 0, K(m) \neq 0)$, where $m \in G$ is the message. Thus, in the simulation the challenger will need to assume $K(m) \neq 0$ when $F(u) = 0$. Whereas in our scheme, since the message is over Z_q^* the simulator need not check that condition and hence can answer all signature queries issued by the adversary.
Since the identities are of length n_u, the public parameter consists of a vector of length n_u and the size of each element in the vector being $|G|$. Due to this, the public parameter size is $G^4 \times G^{n_u}$, which is not efficient in practice. One of the approach to improve the public parameter size is to fix the length of the identity to l, thereby reducing the vector length to l, where $1 < l \leq n$ (when $l = n_u$, this is equivalent to our actual public parameter size). In this case, an identity u is represented as $(u_1, ...u_l$ which is of length l and each element u_i is an n_u/l bit string. This idea was proposed by Chatterjee and Sarkar in [32]. We would like to highlight the fact that, this approach of reducing the public parameter size is at a cost of security tightness or at a cost of group size G (increase in computational cost).

6 Conclusion

In this paper, we presented an efficient signature construction with reduced public size parameter. The security of the scheme is based on intractability of computational Diffie-Hellman in adaptive identity model. Further, we showed how a strong signature can be defined using the basic version of our scheme. In addition, we show how to reduce the signature size by one group element. We provide a comparison of the complexity of our scheme with respect to the ID-based signature presented by Kenny and Schuldt.

References

1. A.Shamir: Identity-based cryptosystems and signature schemes. Lecture Notes in Computer Science **196** (1984) 47–53
2. R.Sakai, K.Ohgishi, M.Kasahara: Cryptosystems based on pairing. 2000 Symposium on Cryptography and Information Security (SCIS2000)
3. R.Sakai, K.Ohgishi, M.Kasahara: Cryptosystems based on pairing over elliptic curve. The 2001 Symposium on Cryptography and Information Security (2001)
4. D.Boneh, M.Franklin: Identity based encryption from weil pairing. In J. Kilian, editor, CRYPTO 2001, Lecture Notes in Computer Science **2139** (2001) 213–229
5. D.Boneh, H.Sacham, B.Lynn: Short signatures from the weil-pairing. Advances in Cryptology-Asiacrypt 2001 Lecture Notes in Computer Science **2248** (2001) 514–532
6. J.Baek, R.Safavi-Naini, W.Susilo: Efficient multi-receiver identity-based encryption and its application to broadcast encryption. Public Key Cryptography, 2005 (2005) 380–397
7. F.Zhang, R.Safavi-Naini, W.Susilo: An efficient signature scheme from bilinear pairings and its applications. In Public Key Cryptography PKC 2004, Lecture Notes in Com Science **2947** (2004) 277–290
8. K.G.Paterson: Id-based signatures from pairingson elliptic curves. Electronics Letters **38, Issue-18** (2002) 1025–1026
9. J.C.Cha, J.H.Cheon: An identity-based signature from gap diffie-hellman groups. In the Proceedings of Public Key Cryptography - PKC 2003: 6th International Workshop on Practice and Theory in Public Key Cryptography, Lecture Notes in Computer Science **2567** (2003) 19–30
10. F.Hess: Efficient identity based signature schemes based on pairings. In Selected Areas in Cryptography: 9th Annual International Workshop, SAC 2002, Lecture Notes in Computer Science **2585** (2003) 310–324
11. B.Libert, J.J.Quisquater: New identity-based signcryption schemes from pairings. In IEEE Information Theory Workshop, 2003 (2003) 155–158
12. X.Boyen: Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography. In Proceedings of Crypto 2003, Lecture Notes in Computer Science **2729** (2003) 383–399
13. D.Nalla, K.C.Reddy: Signcryption scheme for identity-based cryptosystems. Cryptology ePrint Archive, Report 2003/066 (2003)
14. S.S.M.Chow, S.M.Yiu, L.C.K.Hui, K.P.Chow: Efficient forward and provably secure id-based signcryption scheme with public verifiability and public ciphertext authenticity. In Proceedings of the 6th Annual International Conference on Information Security and Cryptology (ICISC 2003), Lecture Notes in Computer Science **2971** (2004) 352–369
15. N.McCullagh, P.S.L.M.Barreto: Efficient and forward-secure identity based signcryption. Cryptology ePrint Archive, Report 2004/117 (2004)
16. J.Malone-Lee: Identity-based signcryption. IACR eprint, report 2002/098 (2002)
17. M.Bellare, P.Rogaway: Random oracles are practical:a paradigm for designing efficient protocols. First ACM Conference on Computer and Communications Security, ACM (1993) 62–72
18. M.Bellare, M.Boldyreva, A.Palacio: An uninstantiable random oracle model scheme for a hybrid-encryption problem. In Cachin and Camenisch [CC04] (2004) 171–188

19. R.Canetti, O.Goldreich, S.Halevi: The random oracle methodology, revisited. In STOC (1998) 209218
20. D.Boneh, X.Boyen: Secure identity based encryption without random oracles. Advances in Cryptology CRYPTO 2004, Lecture Notes in Computer Science **3152** (2004) 443–459
21. D.Boneh, X.Boyen: Efficient selective-id secure identity based encryption without random oracles. **3027** (2004) 223–238
22. K.G.Paterson, J.C.N.Schuldt: Efficient identity-based signatures secure in the standard model. ACISP 2006, Lecture Notes in Computer Science **4058** (2006) 207–222
23. B.Waters: Efficient identity based encryption without random oracles. IIn Advances in CryptologyEUROCRYPT 2005, Lecture Notes in Computer Science **3494** (2005) 114–127
24. C.Gentry: Practical identity-based encryption without random oracles. In the Proceedings of Eurocrypt-06, Lecture Notes in Computer Science **4004** (2006) 445–464
25. D.Boneh, X.Boyen: Short signatures without random oracles. In Advances in Cryptology - EUROCRYPT 2004, Lecture Notes in Computer Science **3027** (2004) 5673
26. G.Ateniese, J.Camenisch, S.Hohenberger, Medeiros, B.: Practical group signatures without random oracles. Cryptology ePrint Archive, Report 2005/385, 2005. http://eprint.iacr.org/ (2005)
27. M.H.Au, J.K.Liu, T.H.Yuen, D.S.Wong: Efficient hierarchical identity based signature in the standard model. Cryptology ePrint Archive, Report 2007/068, 2007. http://eprint.iacr.org/ (2007)
28. M.H.Au, J.K.Liu, T.H.Yuen, D.S.Wong: Id-based ring signature scheme secure in the standard model. In: IWSEC, http://dx.doi.org/ (2006) 1–16
29. C.Gentry, A.Silverberg: Hierarchical id-based cryptography,. In: Y.Zheng, editor, ASIACRYPT 2002. Volume 2501., Lecture notes in computer science, Springer, Berlin, ALLEMAGNE (2002) 548–566
30. E.Kiltz, A.Mityagin, S.Panjwani, B.Raghavan: Append-only signatures. In: L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, editors, ICALP. Volume 3580., Lecture notes in computer science, Springer, Berlin, ALLEMAGNE (2005) 434–445
31. Y.Dodis, J.Katz, S.Xu, M.Yung: Strong key-insulated signature schemes. In: Public Key Cryptography - PKC 2003: 6th International Workshop on Practice and Theory in Public Key Cryptography Miami. Volume 2567., Lecture notes in computer science, Springer, Berlin, ALLEMAGNE (2003) 130–144
32. S.Chatterjee, P.Sarkar: Trading time for space: Towards an efficient ibe scheme with short(er) public parameters in the standard model. Proceedings of ISISC - 2005, Lecture Notes in Computer Science **3935** (2005) 424–440