A Strong and Efficient Certificateless Digital Signature Scheme

Mohamed Alfateh Hassouna *Mohsin Hashim*
m.fateh@ribat.edu.sd *m.hashim@uofk.edu*

ABSTRACT

This paper extends the certificateless public key infrastructure model that was proposed by Hassouna et al by proposing new digital signature scheme to provide true non-repudiation, the proposed signature scheme is short and efficient, it is also has strength point that the KGC has no contribution in signature generation/verification process, therefore any compromise of the KGC does not affect the non-repudiation service of the system. Furthermore, even the KGC cannot do signature forgery by (temporary) replacing the user's public key.

I. INTRODUCTION

The Public Key Infrastructure (PKI) is a complete system to provides public key authentication by binding the entity information like subject name, email address and its public key in standard formatted document called (i.e digital certificate). X.509 [1] is the one of the widely used digital certificate standard that is supported by the International Telecommunication Union. This digital certificate is issued according to a set of procedures and policies and then signed by a trusted certificate authority's (CA) private key. Each user within the system can use his/her certificate to provide confidentiality through encryption or authentication and non-repudiation through digital signature.

Each certificate in the PKI system has a validity period after which it expires and consequently revoked. The PKI provides a mechanism to check the validity of the certificate by different methods. The most popular methods are the certificate revocation list(CRL) and the online certificate status protocol(OCSP).

The X.509[1] specifies public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm. In the X.509 system, a certification authority(CA) issues a certificate binding a public key to a particular distinguished name in the X.500[2] tradition, or to an alternative name such as an e-mail address or a DNS-entry. An organization's trusted root certificates can be distributed to all employees so that they can use the company PKI system. Internet Browsers such as MS Internet Explorer, Firefox, Opera, Safari and Chrome come with a predetermined set of root certificates pre-installed, PKI certificates from larger vendors will work instantly, in effect the browsers' developers determine which CAs are trusted third parties for the browsers' users.

X.509[1] also includes standards for certificate revocation list (CRL) implementations. The IETF approved way of checking a certificate's validity is the Online Certificate Status Protocol (OCSP). There are many security

protocols based on the PKI like Secure Socket Layer(SSL), IPSec, S/MIME, VPN, and SSH protocols.

Generally, the PKI suffers two problems, namely: scalability and certificate management[3]. The Identity-based Public Key Cryptography(ID-PKC) [4] came to address these two problems, but could not offer true non-repudiation due to the key escrow problem[3, 5]. In ID-PKC, an entity's public key is derived directly from certain aspects of its identity, for example, an IP address belonging to a network host, or an e-mail address associated with a user. Private keys are generated for entities by a trusted third party called a private key generator(PKG). The first fully practical and secure identity-based public key encryption scheme was presented in[6]. Since then, rapid development of ID-PKC has taken place. Currently, there exist Identity-based Key Exchange protocols (interactive[7] as well as non-interactive[8]), signature schemes [9, 10, 11], Hierarchical schemes[12]. It has also been illustrated in[13, 14, 15] how ID-PKC can be used as a tool to enforce what might be termed "cryptographic work-flows", that is, sequences of operations (e.g. authentications) that need to be performed by an entity in order to achieve a certain goal[3].

In 2003 Al-Riyami and Paterson [3] introduced the concept of Certificateless Public Key Cryptography (CL-PKC) to overcome the key escrow limitation of the identity-based public key cryptography (ID-PKC). In CL-PKC a trusted third party called Key Generation Center (KGC) supplies a user with a partial private key. Then, the user combines the partial private key with a secret value (that is unknown to the KGC) to obtain his full private key. In this way the KGC does not know the user's private key. Then the user combines his secret value with the KGC's public parameters to compute his public key.

The CL-PKC is considered a combination between PKI and identity based cryptography [3]. It combines the best features of the PKI and ID-PKC, such as no key escrow property, reasonable trust to trust authority and lightweight infrastructure[16]. It provides a solution to the non-repudiation problem, through enabling a user to generate his/her full long-term private key, where the trusted third party is unable to impersonate the user. The use of certificateless cryptography schemes have appeared in literature, this includes the uses of certificateless encryption[5], [17], certificateless signatures [18, 19, 20] and certificateless signcryption[21, 22, 23].

Al-Riyami and Paterson[3] scheme proposed binding technique to link the public key by one-to-one correspondence with the identity to guarantee that every user in the system has one public/private key pair, the big contribution of using this binding technique is that upgrade the CL-PKC to trust level 3 as Girault's[24] definition of the trust levels. Al-Riyami and

Paterson[3] proved that their certificateless encryption scheme is secure against fully-adaptive chosen ciphertext attack(IND-CCA) and also proposed certificateless digital signature scheme along with certificateless key agreement protocol and hierarchal certificateless encryption scheme(HCL-PKE).

Hassouna et al[25] proposed an integrated certificateless public key infrastructure model that provided many nice and practical features like two-factor private key authentication, private key recovery, private key portability and private key archiving, these features provided because Hassouna et al[25] separated the generation of private key from public key generation and used an enhanced different binding technique that proposed by Mohammed et al[26]. However, Hassouna et al[25] focused on the public/private key management issues and did not have digital signature scheme to provide non-repudiation.

The binding technique that proposed by Hassouna et al[25] scheme raised very important and non-mentioned feature, it makes the CL-PKC resistance to the public key replacement attack that can be done by the KGC or any adversary in case of sending the user's partial private key in a no secure channel because the user's full private key is generated from different secret value that used to calculate the user's public key.

In this paper we used the binding technique that proposed by Hassouna et al[25] to avoid the attacks that Al-Riyami and Paterson scheme[3] has, then we extend Hassouna et al's[25] scheme by proposing new strong and efficient digital signature scheme to provide true non-repudiation service.

The rest of this paper is organized as follows. Section [2] gives backgrounds about pairing in elliptic curves and its related cryptographic primitives. In Section[3], we introduce the concept of certificateless public key cryptography, Al-Riyami and Paterson[3] scheme and Hassouna et al[25] scheme. In Section [4], we introduce the proposed Certificateless Short Signature scheme and its security features. Finally, Section [5] concludes the paper.

II. Backgrounds

In this section we give some backgrounds about pairing in elliptic curves and its related cryptographic primitives.

A. Pairings in Elliptic Curve:

Throughout the paper, G_1 denotes an additive group of prime order q and G_2 a multiplicative group of the same order. We let P denote a generator of G_1. For us, a pairing is a map $e : G1 \times G1 \longrightarrow G2$ with the following properties:

1) The map is bilinear: given $Q,W,Z \in G_1$ we have: $e(Q,, W + Z) = e(Q,W).e.(Q,Z).$
   Consequently, for any $a,b \in Z_q$, we have:
   $e(aQ,bW) = e(Q, W)^{ab} = e(abQ, W)$ etc.
2) The map e is non-degenerate: $e(P, P) \neq 1_{G_2}$.
3) The map e is efficiently computable.

Typically, the map *e* will be derived from either the Weil or Tate pairing on an elliptic curve over a finite field. We refer to [30, 31, 6, 32, 33, 34, 35, 36] for a more comprehensive description of how these groups, pairings and other parameters should be selected in practice for efficiency and security. We also introduce here the computational problems that will form the basis of security for our CL-PKC schemes.

B. Bilinear Diffie-Hellman Problem(BDHP):

Let *G1,G2, P* and *e* be as above. The BDHP in *G1,G2, e* is as follows: Given *P, aP, bP, cP* with uniformly random choices of a, b, $c \in Z^*_q$, compute $e(P, P)^{abc} \in G_2$. An algorithm *A* has advantage ϵ in solving the DHP in G_1,G_2, *e* if:

$\Pr[A(P, aP, bP, cP) = e(P, P)^{abc}] = \epsilon$. Here the probability is measured over the random choices of $a, b, c \in Z_q$ and the random bits of *A*.

C. Generalized Bilinear Diffie-Hellman Problem (GBDHP):

Let G_1,G_2, *P* and *e* be as above. The GBDHP in G_1,G_2, *e* is as follows: Given *P, aP, bP, cP* with uniformly random choices of a,b, $c \in Z^*_q$, output a pair $(Q \in G_1 , e(P,Q)^{abc} \in G_2)$. An algorithm *A* has advantage ϵ in solving the GBDHP in G_1,G_2, *e* if: $\Pr[A(P, aP, bP, cP) = (Q, e(P, Q)^{abc})] = \epsilon$.

Notice that the BDHP is a special case of the GBDHP in which the algorithm outputs the choice $Q = P$. While the GBDHP may appear to be in general easier to solve than the BDHP because the solver gets to choose *Q*, we know of no polynomial-time algorithm for solving either when the groups G_1,G_2 and pairing *e* are appropriately selected. If the solver knows $s \in Z_q$ such that $Q = sP$, then the problems are of course equivalent. The GBDHP is related to generalized versions of the computational Diffie-Hellman problems in G_1 and G_2 in the same way that the BDHP is related to the standard computational Diffie-Hellman problem in those groups[6], [37].

As in [6], a randomized algorithm *IG* is a BDH parameter generator if *IG*:

1) takes security parameter k >= 1,
2) runs in polynomial time in k, and
3) outputs the description of groups G_1, G_2 of prime order *q* and a pairing *e*: $G_1 \times G_1 \longrightarrow G_2$.

Formally, the output of the algorithm $IG(1^k)$ is (G_1,G_2, e). There are other computational hardness assumptions related to pairings and are infeasible in polynomial time[6], [33].

1) **Elliptic Curve Discrete Logarithm Problem:** Given $P,Q \in G_1$, find an element $a \in Z^*_q$ such that $Q = aP$.
2) **Computation Elliptic Curve Diffie-Hellman Problem:** Given *(P, aP, bP)* in G_1 where $a,b \in Z^*_q$, compute abP.

III. CERTIFICATELESS PUBLIC KEY CRYPTOGRAPHY(CL-PKC)

In 2003 Al-Riyami and Paterson [3] introduced the concept of Certificateless Public Key Cryptography (CL-PKC) to overcome the key escrow limitation of the Identity-based Cryptography. In CL-PKC a trusted third party called Key Generation Center (KGC) supplies a user with partial private key, the user then combine the partial private key with a secret value (unknown to the KGC) to obtain his/her full private key. In this way the KGC does not know users private keys. Then the user combines the same secret value with the KGC's public parameters to compute his/her public key. Compared to Identity-based Public Key Cryptography (IDPKC), the trust assumptions made of the trusted third party in CL-PKC are much reduced. In ID-PKC, users must trust the private key generator (PKG) not to abuse its knowledge of private keys in performing passive attacks, while in CL-PKC, users need only trust the KGC not to actively propagate false public keys [3].

In CL-PKC users can generate more than one pair of key (private and public) for the same partial private key. To guarantee that KGC does not replace user's public keys Al-Riyami and Paterson[3] introduced a binding technique to bind a user's public key with his/her private key. In their binding scheme, the user first fixes his/her secret value and his/her public key and supplies the KGC his/her public key. Then the KGC redefine the identity of the user to be the user's identity concatenated with his/her public key. By this binding scheme the KGC replacement of a public key apparent, and equivalent to a CA forging a certificate in a traditional PKI.

A. Al-Riyami and Paterson Scheme:

In this section we give a general description to Setup, Set-Secret-Value, Partial-Private-Key-Extract, Set-Private-Key and Set-Public-Key algorithms as introduced by Alriyami and Paterson [3]. Let k be a security parameter given to the Setup algorithm and IG be a Bilinear Diffie-Hellman Problem (BDH) parameter generator with input k.

1) Setup (running by the KGC): this algorithm runs as follows:

a) Run IG on input k to generate output $<G_1, G_2, e>$ where G_1 and G_2 are groups of same order q and $e: G_1 \times G_2 \longrightarrow G_1$.

b) Choose an arbitrary generator $P \in G_1$.

c) Select a master-key s uniformly at random from Z_q and set $P_0 = sP$.

d) Choose cryptographic hash functions:

$H_1 : \{0, 1\}^* \longrightarrow G_1^*$
and
$H_2 : G_2 \longrightarrow \{0, 1\}^n$.

where n is the bit-length of plaintexts taken from some message space $M = \{0, 1\}^n$ with a corresponding ciphertext space $C = G_1 \times \{0, 1\}^n$. Then, the KGC publishes the system parameters $params = < G_1, G_2, e, n, P, P_0, H_1, H_2 >$, while the secret master-key s is saved secure by the KGC.

2) Set-Secret-Value (running by the user): The inputs of this algorithm are *params* and entity m's identifier ID_m. It selects $x_m \epsilon Z_q$ at random and output x_m as m's secret value. Then, the entity m computes $X_m = x_m P$ and sends X_m to the KGC.

3) Partial-Private-Key-Extract (running by the KGC):
The inputs of this algorithm are an identifier $ID_m \epsilon \{0, 1\}^*$ and X_m. The algorithm carries out the following steps to construct the partial private key for entity m with identifier ID_m.

- Compute $Q_m = H_1(ID_m \,||\, X_m)$.
- Output the partial private key $D_m = sQ_m \epsilon G_1$.

Entity m when armed with it's partial private key D_m, it can verify the correctness of the partial private key D_m by checking $e(D_m, P) = e(Q_m, P_0)$.

4) Set-Private-Key (running by the user): The inputs of this algorithm are *params*, D_m (the partial private key of entity m) and $x_m \epsilon Z_q$ (the secret value of entity m). It transforms the partial private key D_m to a private key S_m by computing $S_m = x_m D_m = x_m s Q_m \epsilon G_1$.

5) Set-Public-Key (running by the user): The inputs of this algorithm are *params* and $x_m \epsilon Z_q$ which is the secrete value of entity m. It then constructs the public key of identity m as $P_m = < X_m, Y_m >$, where $X_m = x_m P$ and $Y_m = x_m P_0 = x_m s P$.

The purpose of binding technique used in Al-Riyami and Paterson[3] scheme is to enforce users to have one public/private key pairs in the system, and if there are two working public keys of any user, then the other key was generated by the KGC and this is equivalent to CA certificate forgery in traditional PKI. There are some modified schemes appeared in the literature from the original Al-Riyami and Paterson scheme[3], for example Mokhtarnameh et al[38] proposed little modification on original scheme by setting the user's public key $P_A = x_A Q_A$ and used the new public key in his proposed two party key agreement protocol in the same paper, Yang et al[16] showed that the two party key agreement protocol that proposed by Mokhtarnameh et al[38] is attackable by the man-in-the-middle attack and also explained that the Mokhtarnameh et al[38] did not provide one-to-one correspondence between the user's identity and user' public key as they claimed, Mohammed et al[26] explained that Mokhtarnameh[38] and Yang et al[16] schemes suffer from key escrow problem by that the KGC can

computer the user's private key $S_A = sY_A$ because the public key components $Y_A = x_A Q_A$. Hassouna et al's[25] enhanced the efficiency of the binding technique that was proposed by Mohammed et al[26] and used it to propose new Certificateless Public Key Infrastructure model that provided many nice and practical security features.

***B*. Hassouna et al's Certificateless Public Key Infrastructure Model:**

In this section we state Hassouna et al's[25] model and discuss it security features.

- **Setup (running by the KGC):** same as Al-Riyami and Paterson scheme[3] except that H_2: $\{0, 1\}^* \longrightarrow \{0, 1\}^n$.
- **Set-Secret-Value (running by the user):** the user m with the identity ID_m downloads the system parameters, picks a two random secret values x_m, $x'_m \epsilon Z_q$ Then, the user m computes $X_m = x'_m P$ and sends X_m to the KGC. To provide two factor authentication and protecting the user's private key in case of device theft or compromise, the proposed scheme then enforce the user to choose a strong password *pass*, the system at client hashes the password to be $z_m = H_2(pass)$, multiplies the base point P by the hashed password to be $z_m P$(using special hash function to reserve the large size of the hashed value z_m to prevent brute-force attack on the point $z_m P$ and by that get the user's hashed password), use the hashed value z_m as key along with the MAC function to encrypt the secret value x_m as $MACz_m(x_m)$, sends copy of it to the KGC's public directory and store copy of it along with the point $z_m P$ locally. Note that here there is no need to store the password *pass* or it's hash value z_m.
- **Partial-Private-Key-Extract (running by the KGC):** on receiving X_m computed by user m with identity ID_m, the KGC first computes $Q_m = H_1(ID_m \,||\, X_m)$, then it generates the partial private key of user m as $D_m = sQ_m$. User m when armed with its partial private key D_m, it can verify the correctness of the partial private key D_m by checking $e(D_m, P) = e(Q_m, P_0)$.
- **Set-Public-Key (running by the user):** the user m with identity ID_m computes $Q_m = H_1(ID_m \,||\, X_m)$, $Y_m = x'_m Q_m$ and sets $< X_m, Y_m >$ as his/her long-term public key P_m. Finally, user m sends Y_m to the KGC.
- **Set-Private-Key (running by the user):** every time the user needs to calculate and use his/her full private key, he/she enters his/her password, the system hashes it as z'_m , calculates $z'_m P$ and comparing it with stored $z_m P$, if it is equals then the password is correct and the user is authentic, use it(z_m) as key to decrypt the stored $MACz_m(x_m)$, and after that use the extracted x_m to calculate the full private key S_m by $S_m = (x_m + z_m)D_m$, otherwise the system aborts the process. We

must note here that the private key is never stored on the client and it will be deleted after every usage.

The purpose of the secret value x'_m is to prevent the key escrow problem that can be performed by the KGC[26]. Hassouna et al's[25] scheme assumes that the user uses his/her password every time he/she needs to use his/her full private key, calculates the private key as previous and use it and after that delete it, the private key is never stored on the device storage, this separation of calculating the public and private keys if it is controlled well it will be very usefully feature in public key revocation when the private key is compromised or stolen, other features provided by this separation are private key recovery, private key portability and private key archiving.

Furthermore, Hassouna et al's[25] scheme provides two authentication factor, sine the authenticated user need to have the device that store the secret number x_m as first factor and after that authenticate himself/herself to the device by correct password, because the hashed value of the user's password is involved in private key calculation, even if the attacker somehow get the user's device, he/she can't calculate the private key because he/she does not know the user's password.

Hassouna et al's[25] mentioned that the secret value $MACz_m(x_m)$ would decrypted every time the user m needs to calculate his/her private key, but the MAC function is not decryptable, it is a one-way function. Instead, the user can use any Password-based secure symmetric cryptosystem like AES for that purpose as we will in our proposed scheme with z_m as the secret key.

Since Al-Riyami and Paterson's certificateless signature scheme[3], many CLS schemes such as[39], [40], [41], [42], [43], [44] have been proposed. However, most of these certificateless signature schemes are provably secure in the random oracle model[45], some other CLS schemes that are secure in the standard model[19],[46],[47], [48]. This paper extends Hassouna et al's[25] model to provide non-repudiation service by providing new strong and efficient certificateless signature scheme that is secure in the standard model.

IV. The Proposed Certificateless Short Signature Scheme(CL-SS)

In this section we describe the proposed CL-SS scheme, the Setup, Set-Secret-Value, Extract-Partial-Private-Key, Set- Public-Key are same as Hassouna et al's[25] scheme:

- **Set-Private-Key:** The user private key is $S_m = (x_m + z_m)D_m = (x_m + z_m)sQ_m = (x_m + z_m)sH_1(ID_m||X_m)$ where $X_m = x'_mP$. Also, the user generates the secret term $Z_m = x_m x'_m P$.
- **Sign:** The user generates the signature of the message M using his secret terms $\{x_m, Z_m\}$ as follows:

1. the signer generates large random integer $a \epsilon G_2^*$.
2. the signer calculates $MP_m = H_1(M) \epsilon G_1^*$, $MP_{1m} = ax_m MP_m \epsilon G_1^*$.
3. the signer calculates $s_m = e(MP_m, Z_m)^a = e(MP_{m,,} P)^{axmx'm}$.
4. the signer sends (M, MP_{1m}, s_m) as the signature.

- **Verify:** the user after receiving the signature (M, MP_{1m}, s_m), use the user m's public key $< X_m, Y_m >$ to verify the signature as follows:
  1. the verifier calculates $MP'_m = H_1(M) \epsilon G_1^*$.
  2. if $MP_{1m} = MP'_m$ or $s_m = e(H_1(M), X_m)$ then the verifier rejects the signature.
  3. otherwise, the verifier calculates $r_m = e(MP_{1m}, X_m) = e(ax_m MP_m, x'_m P) = e(MP_{m,} P)^{axmx'm}$.
  4. the verifier accepts the signature iff $r_m = s_m$, otherwise he/she rejects the signature.

Note that the verifier rejects the signature if the term MP_{1m} equals MP'_m or $x'_m MP'_m$ because this is evidence of signature forgery using public-key-replacement attack, in that case the adversary replaces the original public key of the user m with one of his choice(after generates secret number y'_m) and the new public key will be $X_m = y'_m P$, $Y_m = y'_m Q_m$. Therefore, either the attacker replaces the term MP_{1m} by $H_1(M)$ and replace the signature term s_m by $s_m = e(MP_{1m}, X_m) = e(H_1(M), P)^{y'm}$, or the attacker replaces the term MP_{1m} by $y'_m H_1(M)$ and replace the signature term s_m by $s_m = e(MP_{1m,} P) = e(H_1(M), P)^{y'm} = e(H_1(M), X_m)$, and in both cases the verifier will accept the signature because the calculated term $r_m = e(MP_{1m}, X_m)$ will equals the replaced term s_m where X_m is the replaced public key.

The proposed signature scheme is strong because the signature generation/verification does not depends on the KGC, i.e the master secret s of the KGC is not involved in the signature generation/verification and that raise two strength points: the one is that any compromise of the secret of the KGC does not affect the non-repudiation service of the scheme, the other is that the proposed scheme is resistant to *Type II* attacker (malicious KGC), therefore the KGC cannot forge the user's signature by first falsify the public parameters for that purpose because it has no direct contribution in signature generation. Furthermore, the proposed scheme contains one point multiplication/one pairing operation in signing process and one pairing operation in verification process(without the public-key replacement attack verification). Also, the security of the proposed scheme depends on the hardness of the Generalized Bilinear Diffie-Hellman problem(GBDHP) and Elliptic Curve Discrete Logarithm Problem(ECDLP) which are believed infeasible. Therefore, the proposed signature scheme is strong and efficient.

.

V. Conclusions and Remarks

This paper extends the certificateless infrastructure model that proposed by Hassouna et al[25] by adding certificateless short signature scheme, the proposed signature scheme is strong and efficient, we showed that the proposed signature scheme is resistance to the key-replacement attack, thereafter we used the proposed signature scheme to provide true non-repudiation service. The security of the proposed signature scheme depends on the hardness of the ECDLP and GBDHP, therefore the proposed signature scheme is secure in standard security model. By using this proposed signature scheme, Hassouna et al's[25] certificateless public key infrastructure model became provide true non-repudiation service along with the already security features that have and the non mentioned strength point: natural-resistance to public-key-replacement attack, then the extended model provides very efficient, strong and practical certificateless public key infrastructure model.

REFERENCES

[1] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet x.509 public key infrastructure certificate and crl profile," Network Working Group, 1999, ftp://ftp.isi.edu/in-notes/rfc2459.txt.

[2] T. Howes, S. Kille, W. Yeong, and C. Robbins, "The x.500 string representation of standard attribute syntaxes," Network Working Group, 1993, http://www.apps.ietf.org/rfc/rfc1488.html.

[3] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in *Asiacrypt 2003*, ser. Lecture Notes in Computer Science, C. Laih, Ed., 2003, pp. 452–473, full version available at Cryptology ePrint Archive.

[4] A. Shamir, "Identity-based cryptosystems and signature schemes," in *In Advances in Cryptology-CRYPTO'84*, vol. 196, 1984, pp. 47–53.

[5] A. W. Dent, B. Libert, and K. G. Paterson, "Certificateless encryption schemes strongly secure in the standard model," in Public *Key Cryptography, 2008*, pp. 344–359.

[6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology(CRYPTO 2001, volume 2139 of LNCS, Springer-Verlag)*, 2001, pp. 213–229.

[7] R.Sakai, K.Ohgishi, and M.Kasahara, "Cryptosystems based on pairing," in *In The 2000 Symposium on Cryptography and Information Security*, 2000.

[8] N.P.Smart, "An identity based authenticated key agreement protocol based on the weil pairing," *Electronics Letters*, vol. 13, 2002.

[9] J.C.Cha and J.H.Cheon, "An identity-based signature from gap diehellman groups," in *Public Key Cryptography - PKC 2003*, Y. Desmedt, Ed., vol. 2567, 2002, pp. 18–30.

[10] F.Hess, "Efficient identity based signature schemes based on pairings," in *Selected Areas in Cryptography 9th Annual International Workshop*, K. Nyberg and H. Heys, Eds., vol. 2595, 2003, pp. 310–324.

[11] K.G.Paterson, "Id-based signatures from pairings on elliptic curves," *Electronics Letters*, vol. 18, pp. 1025–1026, 2002.

[12] C. Gentry and A. Silverberg, "Heirarchical id-based cryptography," in *ASIACRYPT 2002*, vol. 2501, 2002, pp. 548–566.

[13] L. Chen, K. Harrison, A. Moss, D. Soldera, and N. Smart, "Certification of public keys within an identity based system," in *Information Security, 5th International Conference*, vol. 2433, 2002, pp. 322–333.
[14] K. Paterson, "Cryptography from pairings: a snapshot of current research," *Information Security Technical Report*, vol. 3, pp. 41–54, 2002.
[15] N.P.Smart, "Access control using pairing based cryptography," in *Proceedings CT-RSA 2003*, vol. 2612, 2003, pp. 111–121.
[16] H. Yang, Y. Zhang, and Y. Zhou, "An improved certificateless authenticated key agreement protocol," Cryptology ePrint Archive, Report 2011/653, 2011, http://eprint.iacr.org/.
[17] S. S. D. Selvi, S. S. Vivek, and C. P. Rangan, "Cca2 secure certificateless encryption schemes based on rsa," *IACR Cryptology ePrint Archive*, vol. 2010, p. 459, 2010.
[18] C. Wang, D. Long, and Y. Tang, "An efficient certificateless signature from pairing," *International Journal of Network Security*, vol. 8, no. 1, pp. 96–100, 2009.
[19] H. Xiong, Z. Qin, and F. Li, "An improved certificateless signature scheme secure in the standard model," *Fundamenta Informaticae*, vol. 88, 2008.
[20] L. Zhang and F. Zhang, "A new provably secure certificateless signature scheme," in *08 IEEE International Conference on Communications*, 2008, pp. 1685–1689.
[21] S. S. D. Selvi, S. S. Vivek, and C. P. Rangan, "Certificateless kem and hybrid signcryption schemes revisited," in *ISPEC*, 2010, pp. 294–307.
[22] W. Xie and Z. Zhang, "Certificateless signcryption without pairing," *IACR Cryptology ePrint Archive*, vol. 2010, p. 187, 2010.
[23] Wenjian Xie and Zhang Zhang, " Efficient and provably secure certificateless signcryption from bilinear maps", in WCNIS book 2010, pp.294-307.
[24] Girault, "Self-certified public keys," in *In Advances in Cryptology-EUROCRYPT'91*, vol. 547, 1992, pp. 490–497.
[25] Mohammed Hassouna, Bazara Barri, Nashwa Mohamed and Eihab Bashier, "An integrated public key infrastructure model based on certificateless cryptography," *International Journal of Computer Science and Information Security(IJCSIS)*, vol. 11, 2013.
[26] N. Mohamed, M. Hassouna, and E. Bashier, "A secure and efficient key agreement protocol based on certificateless cryptography," *International Journal of Intelligent Computing Research(IJICR)*, vol. 3, 2012.
[27] A. M. D. S. L. Chen, K. Harrison and N. Smart, "Certification of public keys within an identity based system," *ISC 2002, LNCS 2433, Springer-Verlag*, p. 322-333, 2002.
[28] G. Price and C. J. Mitchell, "Interoperation between a conventional pki and an id-based infrastructure," *LNCS 3545, Springer-Verlag*, pp. 73–85, 2005.
[29] B. Lee, "Unified public key infrastructure supporting both certificate-based and id-based cryptography," *International Conference on Availability, Reliability and Security*.
[30] P. Barreto, H. Kim, B. Lynn, ¸and M. Scott, "Efficient algorithms for pairing-based cryptosystems," in *In Advances in Cryptology(CRYPTO 2002,volume 2442 of LNCS, Springer-Verlag)*, 2002, pp. 354–368.
[31] P. Barreto, B. Lynn, and M. Scott, "Constructing elliptic curves with prescribed embedding degrees," in *In Security in communication networks(SCN'2002, volume 2576 of LNCS, Springer-Verlag)*, 2002, pp. 263–273.
[32] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," pp. 586–615, 2003.
[33] D. Boneh, H. Shacham, and B. Lynn, "Short signatures from the weil pairing," in *In C. Boyd, editor, Advances in Cryptology(ASIACRYPT 2001, volume 2248 of LNCS, Springer-Verlag)*, 2001, pp. 514–532.

[34] R. Dupont, A. Enge, and F. Morain, "Building curves with arbitrary small mov degree over finite prime fields," 2002.
[35] S. Galbraith, "Supersingular curves in cryptography," in *In C. Boyd, editor, Advances in Cryptology(ASIACRYPT 2001, volume 2248 of LNCS, Springer-Verlag)*, 2001, pp. 495–513.
[36] S. Galbraith, K. Harrison, and D. Soldera, "Implementing the tate pairing," in *In Algorithmic Number Theory 5th International Symposium(ANTS-V, volume 2369 of LNCS, Springer-Verlag)*, 2002, pp. 324–337.
[37] S. Galbraith, "Supersingular curves in cryptography," in *In C. Boyd, editor, Proceedings of AsiaCrypt 2001, volume 2248 of LNCS, Springer-Verlag*, 2001, pp. 495–513.
[38] R. Mokhtarnameh, S. Ho, and N. Muthuvelu, "An enhanced certificateless authenticated key agreement protocol," in *in Proc. of the 13th International Conference on Advanced Communication Technology(ICACT)*, 2011, pp. 802–806.
[39] J. X. Z. Zhang, D. Wong and D. Feng, "Certificateless public-key signature: security model and efficient construction," in *In ACNS'06, volume 3989 of LNCS, Springer-Verlag*, 2006, pp. 293–308.
[40] M. Gorantla and A. Saxena, "An efficient certificateless signature scheme," in *In ACIS 2005. LNCS, vol. 3802 Springer-Verlag*, 2005, pp. 110–116.
[41] S.-H. H. W.-S. Yap and B.-M. Goi, "An efficient certificateless signature scheme," in *In EUC workshops 2006, LNCS, vol.4097 Springer-Verlag*, 2006, pp. 322–331.
[42] J. Zhang and J. Mao, "An efficient rsa-based certificateless signature scheme," *The Journal of Systems and Software*, vol. 85, pp. 638–642, 2012.
[43] K. C. X. Li and L. Sun, "Certificateless signature and proxy signature schemes from bilinear pairings," *Lithuanian Mathematical Journal*, vol. 45(1), pp. 76–83, 2005.
[44] M. A. J.K. Liu and W. Susilo, "Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model," in *In Proceedings of the 2nd ACM symposium on Information, computer and communications security, ACM*, 2007, pp. 273–283.
[45] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *In Proceedings of the 1st ACM conference on Computer and communications security,Fairfax, Virginia, USA*, 1993, pp. 62–73.
[46] L. T. Y. Yuan, D. Li and Z. H, "Certificateless signature scheme without random oracles," in *In ISA 2009, LNCS vol.5576, Springer*, 2009, pp. 31–40.
[47] C. X. Q. Xia and Y. Yu, "Key replacement attack on two certificateless signature schemes without random oracles," *Key Engineering Materials*, p. 16061611, 2010.
[48] G. W. Q. X. Y. Yu, Y. Mu and B. Yang, "Improved certificateless signature scheme provably secure in the standard model," *IET Information Security*, vol. 6, p. 102110, 2012.
[49] T. Dierks and E. Rescorla, "The transport layer security(tls) protocol version 1.2," Network Working Group, 2008.