A new identity based signcryption scheme from pairings

Benoît Libert,
Jean-Jacques Quisquater

UCL, Microelectronics Laboratory,
Crypto Group, Place du Levant, 3,
B-1348, Louvain-La-Neuve, Belgium
Telephone: +32(0)10 47.80.62,
Fax: +32(0)10 47.25.98
{libert,quisquater}@dice.ucl.ac.be

Abstract — **We present a new identity based scheme using pairings over elliptic curves. It combines the functionalities of signature and encryption and is provably secure in the random oracle model. We compare it with Malone-Lee's one from security and efficiency points of view. We give a proof of semantical security under the Decisional Bilinear Diffie-Hellman assumption for this new scheme.**

I. Introduction

Identity based cryptosystems were introduced by Shamir in 1984 ([26]). The idea was to get rid of public key certificates by allowing the user's public key to be the binary sequence corresponding to an information identifying him in a non ambiguous way (e-mail address, IP address combined to a user name, social security number,...). This kind of system allows to avoid trust problems encountered in certificate based public key infrastructures (PKIs): there is no need to bind a public key to its owner's identity since those are one single thing. These systems have the particularity to involve trusted authorities called private key generators (PKGs) whose task is to compute users'private key from their identity information (users do not generate their key pairs themselves). Several practical identity based signature schemes (IBS) have been devised since 1984 ([9], [13]) but a satisfying identity based encryption scheme (IBE) only appeared in 2001 ([5]). It was devised by Boneh and Franklin and cleverly uses bilinear maps (the Weil or Tate pairing) over supersingular elliptic curves. Other identity based schemes using pairings were proposed after 2001 ([6],[27],[14],[8],[31]).

The concept of public key signcryption schemes was found by Zheng in 1997 ([33]). The idea of this kind of primitive is to perform encryption and signature in a single logical step in order to obtain confidentiality, integrity, authentication and non-repudiation more efficiently than the sign-then-encrypt approach. The drawback of this latter solution is to expand the final ciphertext's size (this could be impractical for low bandwidth networks) and increase the sender and receiver's computing time. Several efficient signcryption schemes have been proposed since 1997 ([32],[34],[35],[30],[29]) and a first example of formal security proof in a formal security model was published in 2002 ([2]). However, until 2002, none of these schemes were identity based. B. Lynn extended the Boneh-Franklin scheme to build an efficient authenticated IBE scheme ([18]) but his scheme does not have the non-repudiation property. The recipient of a ciphertext is the only entity to be able to check the ciphertext's origin and validity. J. Malone-Lee recently proposed a first method to achieve an identity based signcryption solution ([19]). In this paper, we describe a new scheme that is more secure and can be somewhat more efficient.

A. General scheme

Just like classical IBE systems, signcryption schemes are made of four algorithms which are the following.

Setup: given a security parameter k, the private key generator (PKG) generates the system's public parameters *params*.
Keygen: given an identity ID, the PKG computes the corresponding private key d_{ID} and transmits it to its owner in a secure way.
Signcrypt: to send a message m to Bob, Alice computes Signcrypt(m, d_{ID_a}, ID_b) to obtain the ciphertext σ.
Unsigncrypt: when Bob receives σ, he computes Unsigncrypt(σ, d_{ID_b}, ID_a) and obtains the clear text m or the symbol $\perp$ if σ was an invalid ciphertext between identities ID_a and ID_b.

For obvious consistency purposes, we of course require that if $\sigma =$ Signcrypt(m, d_{ID_a}, ID_b), then we have the relation $m =$ Unsigncrypt(σ, d_{ID_b}, ID_a).

B. Security notions

Malone-Lee ([19]) defines extended security notions for identity based signcryption schemes (IBSC). These notions are semantical security (i.e. indistinguishability against adaptive chosen cipher text attacks) and unforgeability against adaptive chosen messages attacks. Formally, we recall the following definitions.

Definition 1 *We say that an identity based signcryption scheme (IDSC) has the indistinguishability against adaptive chosen ciphertext attacks property (IND-IDSC-CCA) if no polynomially bounded adversary has a non-negligible advantage in the following game.*

1. *The challenger runs the Setup algorithm and sends the system parameters to the adversary.*

2. *The adversary $\mathcal{A}$ performs a polynomially bounded number of requests:*

- *Signcryption request:* $\mathcal{A}$ *produces two identities* ID_i, ID_j *and a plaintext* M. *The challenger computes* $d_{ID_i} =$ *Keygen*(ID_i) *and then Signcrypt*(m, d_{ID_i}, ID_j) *and sends the result to* $\mathcal{A}$.
- *Unsigncryption request:* $\mathcal{A}$ *produces two identities* ID_i *and* ID_j, *a ciphertext* σ. *The challenger generates the private key* $d_{ID_i} =$ *Keygen*(ID_i) *and sends the result of Unsigncrypt*(σ, d_{ID_j}, ID_i) *to* $\mathcal{A}$ *(this result can be the* $\perp$ *symbol if* σ *is an invalid ciphertext).*
- *Key extraction request:* $\mathcal{A}$ *produces an identity* ID *and receives the extracted private key* $d_{ID} =$ *Keygen*(ID).

$\mathcal{A}$ *can present its requests adaptively: every request may depend on the answer to the previous ones.*

3. $\mathcal{A}$ *chooses two plaintexts* $M_0, M_1 \in \mathcal{M}$ *and two identities* ID_A *and* ID_B *on which he wishes to be challenged. He cannot have asked the private key corresponding to* ID_A *nor* ID_B *in the first stage.*
4. *The challenger takes a bit* $b \in_R \{0, 1\}$ *and computes* $C =$ *Signcrypt*(M_b, d_{ID_A}, ID_B) *which is sent to* $\mathcal{A}$.
5. $\mathcal{A}$ *asks again a polynomially bounded number of requests just like in the first stage. This time, he cannot make a key extraction request on* ID_A *nor* ID_B *and he cannot ask the plaintext corresponding to* C.
6. *Finally,* $\mathcal{A}$ *produces a bit* b' *and wins the game if* $b' = b$.

The adversary's advantage is defined to be

$$Adv(\mathcal{A}) := \left|2P[b' = b] - 1\right|.$$

Definition 2 *An identity based signcryption scheme (IDSC) is said to be secure against an existential forgery for adaptive chosen messages attacks (EF-IDSC-ACMA) if no polynomially bounded adversary has a non-negligible advantage in the following game.*

1. *The challenger runs the Setup algorithm with a security parameter* k *and gives the system parameters to the adversary.*
2. *The adversary* $\mathcal{A}$ *performs a polynomially bounded number of requests just like in the previous definition.*
3. *Finally,* $\mathcal{A}$ *produces a new triple* (σ^*, ID_A, ID_B) *(i.e. a triple that was not produced by the signcryption oracle), where the private key of* ID_A *was not asked to the key extraction oracle and wins the game if the result of Unsigncrypt*$(\sigma^*, d_{ID_B}, ID_A)$ *is not the* $\perp$ *symbol.*

The adversary's advantage is simply its probability of victory.

In this definition, the adversary is allowed to ask the private key corresponding to the identity ID_B for which the ciphertext he produces must be valid. This condition is necessary to obtain the non-repudiation property and to prevent a dishonest recipient to send a ciphertext to himself on Alice's behalf and to try to convince a third party that Alice was the sender.

C. Preliminaries

We consider two groups $\mathbb{G}_1$ (additive) and $\mathbb{G}_2$ (multiplicative) of the same prime order q. We need bilinear maps $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ satisfying the following properties:

1. Bilinearity: $\forall\ P, Q \in \mathbb{G}_1,\ \forall\ a, b \in \mathbb{F}_q^*$, we have $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.
2. Non-degeneracy: for any point $P \in \mathbb{G}_1$, $\hat{e}(P, Q) = 1$ for all $Q \in \mathbb{G}_1$ iff $P = \mathcal{O}$.
3. Computability: there exists an efficient algorithm to compute $\hat{e}(P, Q)\ \forall\ P, Q \in \mathbb{G}_1$.

The modified Weil pairing ([5]) and the Tate pairing ([12]) are admissible applications. $\mathbb{G}_1$ is a cyclic subgroup of the additive group of points of a supersingular elliptic curve $E(\mathbb{F}_p)$ over a finite field. $\mathbb{G}_2$ is a cyclic subgroup of the multiplicative group associated to a finite extension of $\mathbb{F}_p$. The security of the schemes described here relies on the hardness of the following problems.

Definition 3 *Given two groups* $\mathbb{G}_1$ *and* $\mathbb{G}_2$ *of the same prime order* q, *a bilinear map* $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ *and a generator* P *of* $\mathbb{G}_1$, *the* ***Bilinear Diffie-Hellman problem*** *(BDHP) in* ($\mathbb{G}_1$,$\mathbb{G}_2$,$\hat{e}$) *is to compute* $\hat{e}(P, P)^{abc}$ *given* (P, aP, bP, cP).

The ***Decisional Bilinear Diffie-Hellman problem*** *(DBDHP) is, given a tuple of points* (P, aP, bP, cP) *and an element* $h \in \mathbb{G}_2$, *to decide whether* $h = \hat{e}(P, P)^{abc}$ *or not.*

We define the advantage of a distinguisher against the DBDH problem like this

$$\begin{aligned} Adv(\mathcal{D}) = |&P_{a,b,c \in_R \mathbb{F}_q, h \in_R \mathbb{G}_2}[1 \leftarrow \mathcal{D}(aP, bP, cP, h)] \\ &- P_{a,b,c \in_R \mathbb{F}_q}[1 \leftarrow \mathcal{D}(aP, bP, cP, \hat{e}(P, P)^{abc})]|. \end{aligned}$$

The decisional problem is of course not harder than the computational one. However, no algorithm is known to be able to solve any of them so far.

II. The Malone-Lee signcryption scheme

In 2002, Malone-Lee described an identity based signcryption scheme ([19]) that was the result of a combination of the simplified Boneh-Franklin encryption scheme ([5]) with a signature that may be viewed as a variant of Hess's identity based signature ([14]). The ciphertexts produced by Malone-Lee's scheme are nearly a concatenation of a signature and a ciphertext (this approach is often called "encrypt-and-sign" in the literature) and only spares one scalar multiplication in $\mathbb{G}_1$ compared to the encrypt-and-sign approach. As a result of this approach, the scheme cannot achieve the semantical security. Indeed, as pointed out in [28], as soon as the signature on the plaintext is visible in the ciphertext, the scheme cannot be semantically secure because any attacker can simply verify the signature on plaintexts m_0 and m_1 produced during the game IND-IDSC-CCA and find out which one matches to the challenge ciphertext. Although, it can offer a reasonable security, the scheme is not semantically secure in its current version.

All systems resulting from the encrypt-and-sign approach have the same inherent weakness. It becomes clear that the universal verifiability feature of signcryption schemes can hamper their resistance to chosen-ciphertext attacks. Shin, Lee and Shin described in [28] how to solve this problem using a modified DSA-type signature. Malone-Lee and Mao also proposed in [20] a secure verifiable signcryption scheme based on RSA but both of these two schemes cannot support identity based public keys. We describe in the next section an identity based signcryption scheme that achieves both public verifiability and resistance to chosen-ciphertext attacks.

III. A NEW IDENTITY BASED SIGNCRYPTION SCHEME

In [35], Zheng showed how to use the SDSS1 and SDSS2[1] signatures schemes to build efficient signcryption schemes. He pointed out that his construction can use any shortened El Gamal based signature scheme or the Schnorr signature scheme to provide a signcryption solution. Unfortunately, his scheme does not offer the non-repudiation property and we have to use a modification of a construction due to Bao and Deng ([3]) to obtain it. We show that Hess's identity based signature [2] can also be used as a building block to obtain a provably secure identity based signcryption scheme for which the semantical security relies on the hardness of the DBDH problem.

A. Description of the scheme

Setup: given security parameters k and n, the PKG chooses the system parameters that include two groups $\mathbb{G}_1$, $\mathbb{G}_2$ of prime order q, a bilinear map $\hat{e}$ between these groups, a generator P of $\mathbb{G}_1$, a master secret $s \in_R \mathbb{F}_q^*$, and a public key $P_{pub} = sP \in \mathbb{G}_1$. It also chooses a secure symmetric cipher (E, D) and hash functions $H_1 : \{0,1\}^* \to \mathbb{G}_1$, $H_2 : \mathbb{G}_2 \to \{0,1\}^n$, and $H_3 : \{0,1\}^* \times \mathbb{G}_2 \to \mathbb{F}_q$. The public parameters are

$$\mathcal{P} := \{\mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub}, H_1, H_2, H_3\}.$$

Keygen: given an identity ID, the PKG computes the hash value $Q_{ID} = H_1(ID) \in \mathbb{G}_1$ and the corresponding private key $d_{ID} = sQ_{ID} \in \mathbb{G}_1$.

Signcrypt: to send a message m to Bob, Alice follows the steps below

1. Compute $Q_{ID_B} = H_1(ID_B) \in \mathbb{G}_1$.
2. Choose $x \leftarrow_R \mathbb{F}_q^*$, and compute $k_1 = \hat{e}(P, P_{pub})^x$ and $k_2 = H_2(\hat{e}(P_{pub}, Q_{ID_B})^x)$.
3. Compute $c = E_{k_2}(m)$, $r = H_3(c, k_1)$ and $S = xP_{pub} - rd_{ID_A} \in \mathbb{G}_1$. The ciphertext is (c, r, S).

Unsigncrypt: when receiving $\sigma = (c, r, S)$, Bob performs the following tasks

1. Compute $Q_{ID_A} = H_1(ID_A) \in \mathbb{G}_1$
2. Compute $k_1 = \hat{e}(P, S)\hat{e}(P_{pub}, Q_{ID_A})^r$
3. Compute $\tau = \hat{e}(S, Q_{ID_B})\hat{e}(Q_{ID_A}, d_{ID_B})^r$ and $k_2 = H_2(\tau)$.
4. Recover $m = D_{k_2}(c)$ and accept σ if and only if $r = H_3(c, k_1)$.

The consistency is easy to verify by the bilinearity of the map. Indeed, we have $\hat{e}(P, S)\hat{e}(P_{pub}, Q_{ID_A})^r = \hat{e}(P, P_{pub})^x$ and $\hat{e}(S, Q_{ID_B})\hat{e}(Q_{ID_A}, d_{ID_B})^r = \hat{e}(P_{pub}, Q_{ID_B})^x$. Any third party (like firewalls as explained in [11]) can be convinced of the message's origin by recovering k_1 just like in step 1 above and checking if the condition $r = H(c, k_1)$ holds. The knowledge of the plaintext m is not required for the public verification of a message's origin. In order to convince someone that Alice is the sender of a particular plaintext m, the receiver just has to forward the ephemeral decryption key k_2 to the third party.

It is important to notice that replacing $r = H_3(c, k_1)$ by $r = H_3(m, k_1)$ would induce the same obstacle to the semantical security as in the Malone-Lee scheme (see [28]).

This scheme is as efficient as Malone-Lee's method (since the pairing $\hat{e}(P, P_{pub})$ does not depend on users or messages and can always be precomputed) and it can be slightly more efficient when users often have to communicate between each other (pairings $\hat{e}(P_{pub}, Q_{ID_B})$ and $\hat{e}(Q_{ID_A}, d_{ID_B})$ can be precomputed by the sender and the receiver once for all). In this case, the most expensive operations of the signcryption algorithm are two exponentiations in $\mathbb{G}_2$ and one computation of the type $aP + bQ \in \mathbb{G}_1$. The Unsigncrypt operation only requires two pairing evaluations and two exponentiations. When precomputing is done with the Malone-Lee scheme, we have a similar cost for the signcryption but we need three pairing evaluations for the unsigncryption. We can show that the new scheme achieves the semantical security.

B. Security

Theorem III.1 *In the random oracle model, we assume we have an IND-IDSC-CCA adversary called $\mathcal{A}$ that is able to distinguish ciphertexts during the game of definition 1 with an advantage ϵ when running in a time t and asking at most q_{H_1} identity hashing requests, at most q_R H_3 requests, q_R Signcrypt requests and q_U Unsigncrypt requests. Then, there exists a distinguisher $\mathcal{B}$ that can solve the Decisional Bilinear Diffie-Hellman problem in a time $O(t + (8q_R^2 + 4q_U)T_{\mathcal{E}})$ with an advantage*

$$Adv(\mathcal{B})^{DBDH(\mathbb{G}_1, P)} > 2(\epsilon - q_U/2^{k-1})/q_{H_1}^4$$

where $T_{\mathcal{E}}$ denotes the computation time of the bilinear map.

Proof. see the full paper ([17]).

It is possible to prove the semantical security under the weaker Bilinear Diffie-Hellman assumption by applying to the scheme the Fujisaki-Okamoto transformation ([10]) but as far as the decisional problem is believed to be hard, we think it is better to use the system in its original form.

[1] Shortened Digital Signature Standard: these schemes were obtained by applying to DSS a method for shortening El Gamal based signatures

[2] The identity based signature scheme proposed by Hess at SAC 2002 is an adaptation of Schnorr's signature that uses the Tate pairing rather than exponentation as a group isomorphism. It is shown to be secure against existential forgery under adaptive chosen-messages attacks in the random oracle model.

The unforgeability against adaptive chosen messages attacks derives from the security of Hess's identity based signature scheme ([14]) under the computational Diffie-Hellman assumption. By arguments similar to those in [11], one can show that an attacker that is able to forge a signcrypted message must be able to forge a signature for a variant of Hess's signature.

IV. Conclusions

We have shown that Hess's signature can be used to build a new efficient identity based signcryption scheme that provides a better security than Malone-Lee's scheme. Both systems are more efficient than the approach consisting in combining the Boneh-Franklin encryption scheme with a signature. Our solution satisfies the semantical security notion under the Decisional Bilinear Diffie-Hellman assumption. Although, this is a stronger assumption than the difficulty of the computational bilinear problem, it seems to be a reasonable base for the security of cryptosystems.

A possible goal for future research would be to find hierarchical ID-based signcryption schemes that allow users of a system to receive signcrypted messages from senders who do not depend on the same authority.

Another interesting open question is the possible equivalence between the Decisional Bilinear Diffie-Hellman problem and the computational one.

We just gave here a basic description of our scheme. We refer to the full paper ([17]) for further details and the analysis of some other new schemes.

References

[1] J.H. An, Y. Dodis, T. Rabin, *On the security of joint signature and encryption*, Advances in Cryptology - Eurocrypt'02, LNCS 2332, Springer, pp. 83-107, 2002.

[2] J. Baek, R. Steinfeld, Y. Zheng, *Formal Proofs for the Security of Signcryption*, Proc. of PKC'02, LNCS 2274, Springer, pp. 81-98.

[3] F. Bao, R.H. Deng, *A signcryption scheme with signature directly verifiable by public key*, Proc. of PKC'98, LNCS 1431, Springer, pp. 55-59, 1998.

[4] M. Bellare, P. Rogaway, *Random oracles are practical: A paradigm for designing efficient protocols*, Proc. of the 1^{st} ACM Conference on Computer and Communications Secrurity, pp. 62-73, 1993.

[5] D. Boneh, M. Franklin, *Identity Based Encryption From the Weil Pairing*, Advances in Cryptology - Crypto'01, LNCS 2139, Springer, 2001.

[6] J.C. Cha, J.H. Cheon, *An Identity-Based Signature from Gap Diffie-Hellman Groups*, to appear in proceedings of PKC 2003. Springer Verlag, Lecture Notes in Computer Science series.

[7] C. Cocks, *An Identity Based Encryption Scheme Based on Quadratic Residues*, Proc. of Cryptography and Coding, LNCS 2260, Springer, pp. 360-363, 2001.

[8] R. Dupont, A. Enge, *Practical Non-Interactive Key Distribution Based on Pairings*, available at http://eprint.iacr.org/2002/136.

[9] A. Fiat, A. Shamir, *How to Prove Yourself: Practical Solutions to Identification and Signature Problems* , Advances in Cryptology - Crypto'86, LNCS 0263, Springer, pp. 186-194, 1986.

[10] E. Fujisaki, T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes", Advances in Cryptology - Crypto'99, LNCS 1666, Springer, pp.537-554, 1999.

[11] C. Gamage, J. Leiwo, Y. Zheng, *Encrypted message authentication by firewalls*, Proc. of PKC'99, LNCS 1560, Springer, pp. 69-81, 1999.

[12] K. Giuliani, *Attacks on the elliptic curve discrete logarithm problem*, Master thesis at University of Waterloo, 1999, available at http://citeseer.nj.nec.com/477524.html

[13] L. Guillou, J-J. Quisquater, *A "Paradoxical" Identity-Based Signature Scheme Resulting From Zero-Knowledge* , Advances in Cryptology - Crypto'88, LNCS 0403, Springer, pp. 216-231, 1988

[14] F. Hess, *Efficient identity based signature schemes based on pairings*, to appear in proceedings of SAC 2002. Springer Verlag, Lecture Notes in Computer Science series.

[15] A. Joux, *A one round protocol for tripartite Diffie-Hellman*, Proc. of ANTS-IV, Lecture Notes in Computer Science vol. 1838, Springer, pp. 385-394, 2000.

[16] M.K. Lee, D.K. Kim, K. Park, *An Authenticated Encryption Scheme with Public Verifiability*, in 4^{th} Korea-Japan Joint Workshop on Algorithms and Computation, 2000.

[17] B. Libert, J-J. Quisquater, *New identity based signcryption schemes from pairings*, full versoin, available at http://eprint.iacr.org/2003/023/.

[18] B. Lynn, *Authenticated Identity-Based Encryption*, available at http://eprint.iacr.org/2002/072/.

[19] J. Malone-Lee, *Identity Based Signcryption*, available at http://eprint.iacr.org/2002/098/.

[20] J. Malone-Lee, W. Mao, *Two Birds one Stone: Signcryption using RSA*, to appear in proceedings of CT-RSA 2003. Springer Verlag, Lecture Notes in Computer Science series.

[21] A.J. Menezes, T. Okamoro, S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Trans. on Inf. Theory, vol. 39, pp. 1639-1646, 1993.

[22] K.G. Paterson, *ID-based signatures from pairings on elliptic curves*, available at http://eprint.iacr.org/2002/004/.

[23] D. Pointcheval, J. Stern, *Security proofs for signature schemes*, Advances in Cryptology - Eurocrypt'96, LNCS 1070, Springer, pp. 387-398, 1996.

[24] D. Pointcheval, J. Stern, *Security arguments for digital signatures and blind signatures*, Journal of Cryptology, vol. 13-Number 3, pp. 361-396, 2000.

[25] R. Sakai, K. Ohgishi, M. Kasahara, *Cryptosystems based on pairing*, In The 2000 Sympoium on Cryptography and Information Security, Okinawa, Japan, January 2000.

[26] A. Shamir, *Identity Based Cryptosystems and Signature Schemes*, Advances in Cryptology - Crypto' 84, LNCS 0196, Springer, 1984.

[27] N.P. Smart, *An identity based authenticated key agreement protocol based on the Weil pairing*, Electronic Letters, 38(13): 630-632, 2002.

[28] J-B. Shin, K. Lee, K. Shim, *New DSA-verifiable signcryption schemes*, to appear in proceedings of ICISC 2002. Springer Verlag, Lecture Notes in Computer Science series.

[29] R. Steinfeld, Y. Zheng, *A Signcryption Scheme Based on Integer Factorization*, Proc. of ISW'00, pp. 308-322, 2000.

[30] B.H. Yum, P.J. Lee, *New Signcryption Schemes Based on KCDSA*, Proc. of ICISC'01, LNCS 2288, Springer, pp. 305-317, 2001.

[31] F. Zhang, K. Kim, *ID-Based Blind Signature and Ring Signature from Pairings.* Advances in Cryptology - Asiacrypt'02, Lecture Notes in Computer Science vol. 2501, Y. Zheng ed., Springer-Verlag, 2002.

[32] Y. Zheng, H. Imai, *Efficient Signcryption Schemes On Elliptic Curves*, Proc. of IFIP/SEC'98, Chapman & Hall, 1998.

[33] Y. Zheng, *Digital Signcryption or How to Achieve Cost (Signature & Encryption) $\ll$ Cost (Signature) + Cost (Encryption)*, Advances in Cryptology - Crypto'97, LNCS 1294, Springer, pp. 165-179, 1997.

[34] Y. Zheng, *Identification, Signature and Signcryption using High Order Residues Modulo an RSA Composite*, Proc. of PKC'01, LNCS 1992, Springer, pp. 48-63, 2001.

[35] Y. Zheng, *Signcryption and its applications in efficient public key solutions*, Proc. of ISW'97, pp. 291-312, 1998.