IDENTITY-BASED SIGNCRYPTION WITHOUT RANDOM ORACLES

Shivaramakrishnan Narayan, Parampalli Udaya and Peter Hyun-Jeen Lee
Department of Computer Science and Software Engineering
University of Melbourne, Victoria - 3010, Australia

Keywords: Identity based Cryptography, Bilinear Maps, Signcryption, Standard Model.

Abstract: The use of signcryption for secure and authenticated data communication was realized in 1997, following which numerous signcryptions have been presented which are provably secure in the random oracle proof methodology. In this paper, we present an identity-based signcryption provably secure in the standard model. Our scheme relies on the intractability of two well studied problems, the decisional bilinear Diffie-Hellman and the computational Diffie-Hellman. We achieve the security reduction of our scheme for the properties message confidentiality and unforgeability without relying on random oracles.

1 INTRODUCTION

A generic approach to achieve message authentication and confidentiality is by signing and encrypting the message sequentially. Apparently, this generic approach is a part of folkfore and commonly used by practioners. Initially, this way of achieving both authenticity and confidentiality was presented by Stallings (Stallings, 1999) with respect to symmetric key cryptography. In public key context, Zheng proposed a new primitive known as signcryption to achieve message confidentiality and authenticity simultaneously at a (computational and communicational) cost less than the generic approach (Zheng, 1997). Since the revival of identity-based cryptography in 2001 several identity-based signcryptions have been proposed. In this paper, we present an identity-based signcryption in the standard model.

The importance of security proof was realized in the early 90's. Since then a cryptographic scheme and its property is evaluated based on the proof outlining the reduction of the scheme to its underlying mathematical hard problem. Most of the identity-based signcryptions defined in the literature (Libert and Quisquater, 2003; McCullagh and Barreto, 2004; Libert and Quisquater, 2004; Malone-Lee, 2002; Chen and Malone-Lee, 2004; Yuen and Wei, 2004; Boyen, 2003; Barreto et al., 2005) are proved secure in a practice oriented proof methodology introduced by Bellare and Rogaway in 1993. This proving technique is known as the "Random Oracle Model" (Bellare and Rogaway, 1993). Although a stronger proof model namely the "Standard Model" was known to the community, efficient schemes in the standard model were not constructed due to the difficulty in presenting the security reduction.

Identity-based Encryption in Standard Model. The first efficient identity-based encryption provably secure without random oracles was defined by Boneh and Boyen (Boneh and Boyen, 2004) in 2004. Although the scheme was proved secure in a slightly weaker notion in which an adversary has to commit to a public identity (challenge identity used in the attack game) in advance. Following the result of Boneh and Boyen, Waters defined the first identity-based encryption which is fully secure without random oracles (Waters, 2005). His work was inspired by the hierarchical encryption scheme presented by Boneh and Boyen (Boneh-Boyen presented two encryption schemes in (Boneh and Boyen, 2004)). The way identity is mapped to a public key in Waters encryption scheme is based on a collison-resistant function given by Boneh and Boyen in (Boneh and Boyen, 2004). The Waters scheme is based on strong, well-studied problem namely decisional bilinear Diffie-Hellman. Recently, a practical identity-based encryption in the standard model with compact public parameter length was presented in the paper (Gentry, 2006). But, the scheme is based on a strong assumption known as augumented bilinear Diffie-Hellman exponent problem.

Narayan S., Udaya P. and Hyun-Jeen Lee P. (2008).
IDENTITY-BASED SIGNCRYPTION WITHOUT RANDOM ORACLES.
In *Proceedings of the International Conference on Security and Cryptography*, pages 342-347
DOI: 10.5220/0001929603420347

Identity-based Signature in Standard Model. One can construct simple IBS schemes by using ordinary signature scheme in the standard model by attaching a certificate containing the public key of the signer. Many such simple schemes have been mentioned in the literature, for example see (Gentry and Silverberg, 2002; Kiltz et al., 2005; Dodis et al., 2003). However these signatures have disadvantages from two counts: they are computationally expensive (two sign verifications) and secondly, they have a large signature space (need to include the public key of the signer and two signatures (one by the signer and the other by the certifier)). The first direct construction of efficient ID-based signature in the standard model was presented by Paterson and Schuldt (Paterson and Schuldt, 2006). The signature is based on the hierarchical extension of Waters encryption scheme (Waters, 2005). This methodology of converting a 2-level hierarchical Identity-Based Encryption (HIBE) to an IBS scheme was first presented by Gentry and Silverberg (Gentry and Silverberg, 2002).

Identity-based Signcryption in Standard Model. The construction of signcryption primitive poses two main problems. Firstly, the computational and space complexities of the primitive should be smaller than the combined complexities of encryption and signature. The space complexity is mainly responsible for the runtime communication cost which includes the amount of signcrypted data from a sender to a receiver. Secondly, the signcryption should admit formal proofs in strong security model. We describe such a strong model in Section 3.

In 2005, Yuen and Wei (Yuen and Wei, 2005) presented the first hierarchical signcryption in the standard model as an extension of their hierarchical signature construction. The security of their scheme is based on weaker notion called sample identity. This notion is weaker than the selective identity model, where the challenge identity is chosen by the adversary before the start of the game. The signcryption requires 7 pairings (1 pre-computable) and 9 exponentiations. Our goal is to present an efficient identity-based signcryption which is provably secure in the standard model where adversary can change challenge identity adaptively.

Signcryption is primarily useful in applications where secure and authenticated data transmission is necessary at a low computational and communicational cost. Another application where signcryptions are useful is in the area of key establishment protocols. In key establishment protocols authenticity and confidentiality need to be simultaneously satisfied for the exchanged keys and hence the signcryption meets this requirement perfectly. A basic signcryption is equivalent to a one-pass key exchange if the message block is viewed as the session key exchanged between the users. An interesting observation from (Gorantla et al., 2007) states that the security notions of the signcryption can be extended to key establishment protocols. The security of key exchange protocols is based on the indistinguishability of the keys by an adversary and this notion is analogous to the indistinguishability of ciphertext notion used in the signcryption security model. The authenticity of the key exchanged follows from the message confidentiality notion of the signcryption.

1.1 Our Contributions

Signcryption can be applied in two ways given a message, sign and encrypt the message or encrypt the message and sign. By following the latter approach we achieve public verifiability of the signature and the former way of signcryption results in a non-public verifiable signature. In this paper, we present a public verifiable identity-based signcryption in the standard model. Our construction is based on Waters encryption and our efficient identity-based signature. The security of the signcryption is based on two well studied hard problems namely, the decisional bilinear Diffie-Hellman and computational Diffie-Hellman. Our scheme is secure in the adaptive security notion defined in the Section 3. The scheme performs better than serially combining any known identity-based encryption and a signature in the standard model. We achieve reduction in the public parameter size, the signcryption size and the number of exponentiations. The efficiency results are presented in Table 1, Section 4.1. Further, it is to be noted that there is no gain in the number of pairing operations and the size of public parameter is same as in the Waters encryption scheme (Waters, 2005).

One of the disadvantages of schemes based on Waters hash is that the public parameters space is large. We have been able to reduce the public parameters space by half to that of Paterson-Schuldt scheme (Paterson and Schuldt, 2006). However, it should be pointed out that the public parameters are acquired only for the initialization of the scheme and does not affect runtime cost of signcrypted data. The initialization requirements can be easily accomplished in a desktop environment and thereby, the practicality of the scheme should not be affected.

1.2 Paper Outline

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

2 BACKGROUND

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

2.1 Bilinear Maps

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be multiplicative groups of prime order q. Let $\mathbb{Z}_q^*$ denote the set of all non-zero integers modulo prime q. A bilinear map is a map $\hat{e}:\mathbb{G}_1\times\mathbb{G}_1\rightarrow\mathbb{G}_2$, satisfying the following properties.

- $\hat{e}$ is bilinear, i.e. for all $g,g_1,g_2\in\mathbb{G}_1$ and $a,b\in\mathbb{Z}_q^*$, we have

(a) $\hat{e}(g,g_1\cdot g_2)=\hat{e}(g,g_1)\cdot\hat{e}(g,g_2)$.

(b) $\hat{e}(g^a,g_1^b)=\hat{e}(g,g_1)^{ab}=\hat{e}(g^b,g_1^a)$.

- $\hat{e}$ is non-degenerate, i.e. for $g\in\mathbb{G}_1/1$, $\hat{e}(g,g)\neq 1$.
- $\hat{e}$ is efficiently computable.

2.2 Admissible Collision-resistant Functions

Our scheme uses collision resistant function of the form $\{0,1\}^{n_u}\longrightarrow\mathbb{G}_1$, where n_u denotes the length of an identity and can constructed as given in (Waters, 2005). In addition, we use a target collision resistant function of the nature $\mathbb{G}_2\times\mathbb{G}_1\longrightarrow\mathbb{Z}_q^*$, this can be constructed using general cryptographic hash functions. To allow identities of arbitrary length, collision-resistant hash function, $H_1:\{0,1\}^*\longrightarrow\{0,1\}^{n_u}$ can be defined.

2.3 Identity-based Signcryption

An identity-based signcryption consists of the following four algorithms.

Set-up. Given a security parameter k, this algorithm generates the global public parameters *params* and the master secret. The private key generator keeps the master secret to itself and publishes the global public parameters *params*.

Extract. Given a user's identity ID, the algorithm generates the private key d_{ID} of ID using the master secret and *params*. The private key generator will use this algorithm to generate the private key of all the users participating in the scheme.

Signcrypt. Given a message M, a receiver's identity ID_R and the private key d_{ID_S} of a sender ID_S, this algorithm outputs a signcrypted text of the message M.

Unsigncrypt. Given a signcrypted text, public key of the sender ID_S and private key of the receiver d_{ID_R}, this algorithm outputs the message M if the signcrypted text is valid, else returns $\perp$.

2.4 Complexity Assumptions

2.4.1 Computational Diffie-Hellman Problem

Given $(g,g^a,g^b)\in\mathbb{G}_1$, where g is a generator of $\mathbb{G}_1$ and $a,b\in\mathbb{Z}_q^*$, the computational Diffie-Hellman problem is to compute g^{ab}.

2.4.2 Decisional Bilinear Diffie-Hellman (DBDH) Problem

Given $(g,g^a,g^b,g^c,Y)\in\mathbb{G}_1^4\times\mathbb{G}_2$, where g is a generator of $\mathbb{G}_1$, $Y\in\mathbb{G}_2$ and $a,b,c\in\mathbb{Z}_q^*$, the DBDH problem is to determine if $Y=\hat{e}(g,g)^{abc}$.

3 SECURITY NOTIONS FOR SIGNCRYPTION

The signcryption scheme we present is proved under the adaptive identity model for both indistinguishability and existential unforgeability attacks. A brief description of the game in given below.

3.0.1 Indistinguishability of Chosen Ciphertext

Definition 3.0.1. *We say that an Id-based signcryption scheme (IDSC) has the indistinguishability against adaptive identity chosen ciphertext attack property (IND-IDSC-CCA2), if no polynomially bounded adversary 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 Query: The adversary submits an identity ID to the challenger. The challenger runs the **Extract()** algorithm and responds with the private key of ID.
- Signcrypt Query: The adversary submits a sender identity, receiver identity and message to the challenger. The challenger runs the **Signcrypt()** algorithm and responds with the signcryption of the message consisting of the signature processed with private key of the sender, and encryption of the given message using public key of the receiver.
- Unsigncrypt Query: The adversary submits a sender identity, a receiver identity and a signcrypted text to the challenger. The challenger runs the **Unsigncrypt()** algorithm and returns the output.

Challenge. Once the adversary decides that Phase 1 is over, it presents two equal length messages M_0, M_1, sender's identity ID_1^* and a recipient identity ID_2^* on which it wishes to be challenged for which adversary did not ask the private key. The challenger chooses a random bit b and computes the signcryption of the message M_b and sends the signcrypted message to the adversary.

Phase 2. The adversary continues to probe the challenger with additional queries as in Phase 1. It is not allowed to extract the private key corresponding to the challenged identity ID_2^*.

Response. The adversary outputs a bit $b' \in \{0,1\}$ and wins the game if $b' = b$.

Definition 3.0.2. *An adversary (ε, Q_e, Q_s)-$\mathcal{A}$ against IND-IDSC-CCA2 exists if $\mathcal{A}$ that makes makes at most Q_e extract queries and Q_s signcryption queries has an advantage at least ε in the above game. A scheme is said to be (ε, Q_e, Q_s)-secure if no (ε, Q_e, Q_s)-adversary exists.*

3.0.2 Existential Unforgeability

Definition 3.0.3. *We say that an Id-based signcryption scheme (IDSC) has existential unforgeability property against adaptive identity chosen-message attack or (EUF-IDSC-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 in the above game.

Forge. The adversary chooses a sender's identity ID_1^*, receiver identity ID_2^* as the challenge identities and returns signature forgery Z on a message M.

Response. The adversary wins if $ID_i \neq ID_1^*$, $ID_1^* \neq ID_2^*$ and **Unsigncrypt**$(Z, M, ID_2^*) = \top$. The adversary should not have made extract query on ID_1^* and ID_2^*, and the forgery did not result from a query made to **Signcrypt** algorithm using (M, ID_1^*, ID_2^*).

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

Definition 3.0.4. *An adversary $\mathcal{A}$ is said to be an (ε, Q_e, Q_s)-forger of an IDSC scheme if $\mathcal{A}$ that makes at most Q_e extract queries and Q_s signcryption queries has an advantage at least ε in the above game. A scheme is said to be (ε, Q_e, Q_s)-secure if no (ε, Q_e, Q_s)-forger exists.*

4 NEW IDENTITY-BASED SIGNCRYPTION (IDSC) CONSTRUCTION

In this section, a new signcryption construction based on an efficient signature construction is presented.

Setup. The private key generator (PKG) chooses groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order q such that a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_2$ can be constructed and picks a generator g of $\mathbb{G}_1$. The PKG then selects a secret $s \in \mathbb{Z}_q^*$ randomly, computes $g_1 = g^s$ and picks $g_2 \in_R \mathbb{G}_1$. Further, PKG chooses $u', u'_m \in_R \mathbb{G}_1$ and a vector $\overrightarrow{U} = (u_i)$ of length n_u whose entries are random elements from $\mathbb{G}_1$.

Given an identity $\mathbf{u}$, $\mathcal{V} \subseteq \{1, ...n_u\}$ denotes the set of all i's such that $\mathbf{u}[i] = 1$, where $\mathbf{u}[i]$ is the ith bit of the identity string. The public key $g_{\mathbf{u}}$ is calculated as given below.

$$g_{\mathbf{u}} = u' \textstyle\prod_{i \in \mathcal{V}} u_i.$$

Given a string M'', $\mathcal{M} \subseteq \{1, ...n_{m'}\}$ (where $n_{m'} = n_u$) denotes the set of all j's such that $M''[j] = 1$ where, $M''[j]$ is the jth bit of the string. $g_{m''}$ is calculated as follows.

$$H_{m''} : \; g_{m''} = u'_m \textstyle\prod_{j \in \mathcal{M}} u_j.$$

In addition to H_u, the PKG selects another target-collision resistant function $H_m : \mathbb{G}_2 \times \mathbb{G}_1 \longrightarrow \mathbb{Z}_q^*$ to map the encrypted message.

The public parameters of the system are $params = \left(g, g_1, g_2, u', \vec{U}, H_u, H_m\right)$ and the master secret is g_2^s.

Extract. Given an identity ID, the private key d_{ID} is constructed as given below:

1. Choose $r_{ID} \in_R \mathbb{Z}_q^*$.
2. The private key is $d_{ID} = (g_2^s \cdot (g_{ID})^{r_{ID}},\ g^{r_{ID}})$ where, $g_{ID} = H_u(ID)$.

Signcrypt. Given a message M, a sender identity A and a receiver identity B, the signcryption on M is constructed as follows.

1. Select $t_1, t_2 \in_R \mathbb{Z}_q^*$.
2. Compute $C = \hat{e}(g_1,\ g_2)^{t_2} \cdot M$.
3. Compute $M' = H_m(C, W)$ where, $W = g^{r_A + t_1}$.
4. Let M'' be the binary representation of M', compute $H_{m'}$, $g_{M''} = u'_m \prod_{j \in \mathcal{M}} u_j$, where $\mathcal{M} \subseteq \{1, ...n_{m'}\}$ denotes the set of all j's such that $M''[j] = 1$, $M''[j]$ is the jth bit of the string.
5. Compute the value $Z = g_A^{t_1} (g_A g_{M''})^{M' t_2} \cdot g_2^s \cdot g_A^{r_A}$.
6. The resulting signcryption is: $\left(C, Z, U = g^{t_2}, V = g_B^{t_2}, W\right)$.

UnSigncrypt. Given a signcryption (C, Z, U, V, W) on message M, the unsigncryption steps are as follows:

1. Obtain the private key d_B.
2. Compute $M = C \cdot \frac{\hat{e}(g^{r_B},\ V)}{\hat{e}(g_2^s \cdot (g_B)^{r_B},\ U)}$.
3. Compute $M' = H_m(C, W)$.
4. Let M'' be the binary representation of M', compute $H_{m'}$, $g_{M''} = u'_m \prod_{j \in \mathcal{M}} u_j$, where $\mathcal{M} \subseteq \{1, ...n_{m'}\}$ denotes the set of all j's such that $M''[j] = 1$, $M''[j]$ is the jth bit of the message string.
5. Accept M if,
$$\hat{e}(Z, g) = \hat{e}(g_1, g_2)\ \hat{e}(W, g_A)\ \hat{e}(U, (g_{M''} g_A)^{M'}).$$

4.1 Efficiency of IDSC

Table 1 gives a comparison of the computations involved in our IDSC with respect to a generic signcryption derivable using Waters encryption (Waters, 2005) and the signature presented by Paterson and Schuldt (Paterson and Schuldt, 2006). In addition to the computations, the signcryption size and the public parameter size are mentioned. In case of the ciphertext space, there is a reduction of one element over $\mathbb{G}_1$. But again, due to the fact that $W = g^{r_A + t_1}$ can be fixed, a user needs to send this value only to a new receiver. This would further reduce the ciphertext space by one element over $\mathbb{G}_1$. The public parameter size is $\mathbb{G}_1^4 \times \mathbb{G}_1^{n_u}$.

The parameters n_u and n_m in Table 1 denotes the length of an identity and a message respectively.

5 SECURITY PROOFS

In this section, security results of IDSC against (ε, Q_e, Q_s)-IND-IDSC-CCA2 and (ε, Q_e, Q_s)-EUF-IDSC-CMA attacks explained in Section 3 are presented. The proofs will appear in an extended paper.

The use of collision resistant function H_m presents the necessity of including the probability of collisions which can affect the output of the attack game.

Theorem 5.0.1. *Let H_m be a target collision resistant hash function used in our signcryption and $\mathbf{Adv}_{TCR,\mathcal{H}}^{hash-tcr}(k)$ denote the advantage of an adversary $\mathcal{H}$ against the collision resistance of H_m. If there exists an adversary (ε, Q_e, Q_s)-$\mathcal{A}$ making at most Q_e extract queries and Q_s signcryption queries that succeeds against the IND-IDSC-CCA2 security of IDSC with a probability ε, then there exists a challenger $\mathcal{B}$ running in polynomial time that solves the DBDH problem with a probability ε' at least*

$$\frac{1}{16(n_u+1)(Q_e+Q_s)}(1 - \mathbf{Adv}_{TCR,\mathcal{H}}^{hash-tcr}(k)).$$

Theorem 5.0.2. *Let H_m be a target collision resistant hash function used in our signcryption scheme and $\mathbf{Adv}_{TCR,\mathcal{H}}^{hash-tcr}(k)$ denote the advantage of an adversary $\mathcal{H}$ against the collision resistance of H_m. If there is an (ε, Q_e, Q_s)-adversary $\mathcal{A}$ making at most Q_e extract queries and Q_s signcryption queries that succeeds against the EUF-IDSC-CMA security of IDSC with a probability ε, then there exists a challenger $\mathcal{B}$ running in polynomial time that solves the CDH problem with a probability ε' at least*

$$\frac{\varepsilon}{4(Q_e+Q_s)^2(n_u+1)}(1 - \mathbf{Adv}_{TCR,\mathcal{H}}^{hash-tcr}(k)).$$

6 CONCLUSIONS

In this paper, we presented an efficient and fully secure identity-based signcryption in the standard model. The scheme presented is proved secure in a well-defined adaptive identity chosen ciphertext and chosen message attack security notions. The scheme performs better than sequentially combining any known identity-based encryption and a signature in the standard model. We achieve reduction in the

Table 1: Efficiency of IDSC.

PC - Denotes Pre-Computable			
	Waters Encryption	Kenny and Schuldt Signature	Our Signcryption*
Pairings	3(1PC)	4(1PC)	7(2PC)
$\mathbb{G}_1$ Exponentiations	2	3	3
$\mathbb{G}_2$ Exponentiations	1	-	1
Signcryption Size	$\mathbb{G}_2 \times \mathbb{G}_1^2$	$\mathbb{G}_1^3$	$\mathbb{G}_2 \times \mathbb{G}_1^4$
Public Parameter Size	$\mathbb{G}_1^4 \times \mathbb{G}_1^{n_u}$	$\mathbb{G}_1^5 \times \mathbb{G}_1^{n_u} \times \mathbb{G}_1^{n_m}$	$\mathbb{G}_1^4 \times \mathbb{G}_1^{n_u}$

public parameter size, signcryption size and exponentiations. One of the shortcomings of our scheme is its public parameter size. An open problem is to construct a signcryption with compact public parameter size.

REFERENCES

Barreto, P., Libert, B., McCullagh, N., and Quisquater, J. (2005). Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In *Advances in cryptology (ASIACRYPT 2005) (11th international conference on the theory and application of cryptology and information security)*, volume 3788, pages 515–532. Lecture notes in computer science, Springer, Berlin, ALLEMAGNE.

Bellare, M. and Rogaway, P. (1993). Random oracles are practical:a paradigm for designing efficient protocols. *First ACM Conference on Computer and Communications Security, ACM*, pages 62–72.

Boneh, D. and Boyen, X. (2004). Efficient selective-ID secure identity based encryption without random oracles. In *Advances in Cryptology EUROCRYPT 2004*, volume 3027, pages 223–238. Lecture Notes in Computer Science, Springer Berlin/Heidelberg.

Boyen, X. (2003). Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography. *In Proceedings of Crypto 2003*, 2729:383–399.

Chen, L. and Malone-Lee, J. (2004). Improved identity-based sincryption. *Cryptology ePrint Archive, Report 2004/114, 2004, http://eprint.iacr.org/2004/114/*.

Dodis, Y., Katz, J., Xu, S., and Yung, M. (2003). 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, pages 130–144. Lecture notes in computer science, Springer, Berlin, ALLEMAGNE.

Gentry, C. (2006). Practical identity-based encryption without random oracles. *In the Proceedings of Eurocrypt-06*, 4004:445–464.

Gentry, C. and Silverberg, A. (2002). Hierarchical ID-based cryptography,. In *Y. Zheng, editor, ASIACRYPT 2002*, volume 2501, pages 548–566. Lecture notes in computer science, Springer, Berlin, ALLEMAGNE.

Gorantla, M., Boyd, C., and Gonzalez, J. (2007). On the connection between signcryption and one-pass key establishment. In *Eleventh IMA International Conference on Cryptography and Coding*, *To appear*. Springer.

Kiltz, E., Mityagin, A., Panjwani, S., and Raghavan, B. (2005). Append-only signatures. In *L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, editors, ICALP*, volume 3580, pages 434–445. Lecture notes in computer science, Springer, Berlin, ALLEMAGNE.

Libert, B. and Quisquater, J. (2003). New identity-based signcryption schemes from pairings. *In IEEE Information Theory Workshop, 2003*, pages 155–158.

Libert, B. and Quisquater, J. (2004). Efficient signcryption with key privacy from gap Diffie-Hellman groups. In *In Public Key Cryptography - PKC 2004*, volume 2947, pages 187–200. Lecture Notes in Computer Science, Springer- Verlag.

Malone-Lee, J. (2002). Identity-based signcryption. *IACR eprint, report 2002/098*.

McCullagh, N. and Barreto, P. (2004). Efficient and forward-secure identity based signcryption. *Cryptology ePrint Archive, Report 2004/117*.

Paterson, K. and Schuldt, J. (2006). Efficient identity-based signatures secure in the standard model. *ACISP 2006*, 4058:207–222.

Stallings, W. (1999). *Cryptography and Network Security (2nd ed.): Principles and Practice*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA.

Waters, B. (2005). Efficient identity based encryption without random oracles. *In Advances in Cryptology-EUROCRYPT 2005*, 3494:114–127.

Yuen, T. and Wei, V. (2004). Fast and proven secure blind identity-based signcryption from pairings. *Cryptology ePrint Archive, Report 2004/121*.

Yuen, T. and Wei, V. (2005). Constant-size hierarchical identity-based signature/signcryption without random oracles. Cryptology ePrint Archive, Report 2005/412, http://eprint.iacr.org/.

Zheng, Y. (1997). Digital signcryption or how to achieve cost(signature & encryption) <<cost(signature) + cost(encryption). *In Advances in Cryptology - CRYPTO 97*, 1294.