Malaysian Journal of Mathematical Sciences 7(S): 73-85 (2013)
Special Issue: The 3rd International Conference on Cryptology & Computer Security 2012 (CRYPTOLOGY2012)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

Security Upgrade for a K-Resilient Identity-Based Identification Scheme in the Standard Model

[1*]Ji-Jian Chin and [2]Swee-Huay Heng

[1]Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia

[2]Faculty of Information Science and Technology,
Multimedia University, Melaka, Malaysia

E-mail: jjchin@mmu.edu.my and shheng@mmu.edu.my

*Corresponding author

ABSTRACT

In 2010, Heng and Chin (2010) proposed an identity-based identification (IBI) scheme in the standard model which was resilient to a coalition of attackers conspiring together to break the scheme. They argued that the scheme was desirable due to its proof in the standard model, which is still rare in existing literature. Also desirable was that the proposed scheme was designed without bilinear pairings, which costs greatly in terms of operation costs, thereby allowing the scheme to run more efficiently. However, the proof of security for the proposed scheme was only against impersonation under passive attacks, where the adversary is only allowed to eavesdrop on conversations between honest parties during the identification protocol. In this paper, we upgrade the security proof to prove that the scheme is also secure against impersonation under active and concurrent attacks, showing that the scheme is still secure even if the adversary is to interact with honest parties during the attack.

Keywords: Identity-based identification (IBI), identification protocol, security.

1. INTRODUCTION

An identification scheme allows an entity to prove its identity (prover) to another entity (verifier) in order to gain access to certain resources. In traditional public key cryptography, an identification scheme required the use of certificates in order to bind a user’s identity to his random public key. This gave rise to the certificate management problem as managing certificates can prove to be a daunting task in a system with a large amount of users.

Shamir (1984) proposed the idea of identity-based cryptography, utilizing a user's identity-string to generate his public/private key pairs instead, therefore doing away with certificates. While the problem of key escrow still existed because the Private Key Generator (PKG) who generates the public/private key pairs knew all the secrets involved, the idea still is a desirable one because it solved the certificate management problem.

However, identity-based identification (IBI) schemes were only introduced and had their security rigorously mathematically defined in 2004 by Bellare *et al.* (2004) and Kurosawa and Heng (2004) independently. The former proposed transformations that would transform traditional public key identification schemes into IBI schemes while the latter proposed a transformation from traditional signature schemes into IBI schemes. Both papers utilized security proofs assuming the existence of random oracles.

Bellare and Rogaway (1993) introduced the idealistic model where random oracles exist to model security proofs where there are no practical functions to provide sufficient mathematical properties that satisfy the proof of security. A random oracle produces a bitstring of infinite length that can be truncated to a desired length, and is open to access by all parties, honest and malicious alike.

Canetti *et al.* (1998) however shown that given certain conditions, a scheme proven secure in the random oracle model may not be secure once these random oracles are replaced by real-life hash functions. Therefore, while all cryptographic schemes should have at least a basic proof of security in the random oracle model, it would be better if the proof of security was given in the standard model.

1.1 Recent Developments in IBI

The first IBI schemes in the standard model was introduced by Kurosawa and Heng (2005), followed by a an IBI scheme secure against man-in-the-middle attack by the same authors in Kurosawa and Heng (2006, 2008). Yang *et al.* (2007) provided a frame work for IBI construction in the random oracle model, with security for standard model schemes provided in the selective-ID model, a weaker setting where the attacker must first identify the target to be attacked before commencing with the training phase of the simulation.

Meanwhile, Chin *et al.* (2008) proposed an IBI scheme based on direct proof of security, instead of transformations from conventional identification and signature schemes as previously proposed in Bellare *et al.* (2004) and Heng and Kurosawa (2004). The same authors also formalized the security model for hierarchical IBI (HIBI) schemes in Chin *et al.* (2009) and proposed the first concrete HIBI scheme in the random oracle model. Subsequently, Thorncharoensri *et al.* (2009) proposed the first non-stateless IBI scheme secure against concurrent reset attacks, achieving the highest level of security so far, but relying on a new variant of the q-Strong Diffie-Hellman (q-SDH) assumption, the 2-SDH assumption. In the area of code-based cryptography, Cayrel *et al.* (2009) and El Yousfi (2011) have proposed code-based IBI schemes instead of number-theoretical ones.

1.2 Our Contribution

In [10], the authors proposed a k-resilient IBI scheme based on Heng and Kurosawa (2004, 2006), k-resilient identity-based encryption scheme. However, they only achieved security against passive attacks for up to k-malicious users using the Discrete Logarithm problem in the standard model.

The k-resilient IBI scheme is a desirable scheme because it has a natural proof of security in the standard model, and also offers competitive runtime efficiency due to the fact that it does not rely on bilinear pairings, as all other IBI schemes provably secure in the standard model currently available in literature do. Bilinear pairings are the costliest of all operational expenses, and doing without pairings improves the speed of the identification protocol.

However, Heng and Chin (2010) left the open question of whether the same scheme is secure against active and concurrent attackers. In this paper, we show that the answer to that question is a positive one.

2. PRELIMINARIES

In this section, we introduce some descriptions of preliminaries that are used in our k-resilient IBI construction and proof.

2.1. The One-More Discrete Logarithm Problem (OMDLP)

The OMDLP was first introduced in Bellare *et al.* (2003) and Bellare and Palacio (2002). Let G be a finite cyclic group of order q and let g be a generator of G. An adversary is given a challenge oracle, CHALL, that produces a random group element $W_i \in G$ when queried and a discrete logarithm oracle, DLOG, which provides the discrete logarithm $w_i \in Z_q$ corresponding to the query W_i where $g^{w_i} = W_i$. The adversary wins if after making i queries to the challenge oracle, the adversary is able to output solutions to all i challenges with only $i - 1$ queries to the discrete logarithm oracle, meaning it has to solve at least one instance of the discrete logarithm problem without relying on the discrete log oracle.

2.2. Formal Definition of IBI

An IBI scheme consists of four probabilistic polynomial time algorithms (Setup S, Extract E, Prove P and Verify V)

Setup(S). S on input of the security parameter 1^k, publishes the master public key mpk and keeps the master secret key msk to itself.

Extract(E). E on input of the public identity ID and msk, returns the corresponding user private key usk.

Identification Protocol (canonical interaction between P and V). P receives mpk, ID and usk as input while V receives mpk and ID. The two will then run a canonical 3-step interactive protocol which upon completion V will decide to accept or reject P. The interactive protocol consists of the following steps:

Commitment. P sends a commitment CMT to V.

Challenge. V sends a randomly chosen challenge CHA.

Response. P returns a response RSP which V will evaluate and then choose to accept or reject.

2.3 Security Model for IBI

The goal of an impersonator towards an IBI scheme is impersonation. An impersonator succeeds if after interacting with the verifier with public identity ID and is accepted with non-negligible probability.

We describe three types of adversaries for IBI schemes:

Passive Attacker. The passive adversary eavesdrops on conversations between an honest prover and verifier to extract information.

Active Attacker. The active adversary interacts with honest provers sequentially as a cheating verifier several times to extract information before attempting impersonation.

Concurrent Attacker. This is a special type of active adversary where it can interact with multiple provers at the same time.

The difference between IBI security and that of conventional identification schemes is that 1) instead of a random public key, an impersonator can freely choose a public identity ID to impersonate and 2) we assume the impersonator has compromised and therefore already possessed the private keys of several honest users. This allows the impersonator to obtain private keys of any honest users of his choice (thereby corrupting them) besides the one being attacked. The impersonation attack between an impersonator and the challenger is described as a two-phased game as follows:

Setup. The challenger takes in the security parameter and runs *setup*. The resulting system parameters are given to the impersonator while the master secret is kept to itself.

Phase 1. In this phase, the impersonator can issue Extract queries to the challenger. The challenger responds by running the Extract algorithm to generate and returns the private key to the impersonator. The queries may be asked adaptively. The capabilities of the impersonator differ in terms of passive attacks, where only conversation transcript queries are allowed, and active and concurrent attacks where it can request to interact with the challenger as a cheating verifier instead.

Phase 2. Finally, the impersonator outputs a challenge identity which it wishes to impersonate. The challenge identity must have not been queried before in Phase 1. The impersonator now acts as a cheating prover to convince the verifier based on information gathered in Phase 1 and wins the game if it is successful.

We say an IBI scheme is (t, q_I, ε) -secure under passive/ active/concurrent attacks if for any passive/active/concurrent impersonator I who runs in time, Pr $[I\ can\ impersonate] < \varepsilon$, where I can make at most q_I extract queries.

3. REVIEW OF THE K-RESILIENT IBI SCHEME

3.1 Construction

Setup: Define a group G of order q such that $p = 2q + 1$ and p is prime. Pick a random generator $g \epsilon G$ and a random k-degree polynomial $f(x) = \sum_{t=0}^{k} d_t \cdot x^t$ chosen over Z_q. The system parameters are publicized as $\langle g, D_0 = g^{d_0}, \ldots, D_k = g^{d_k} \rangle$. The master secret $f(x)$is kept as secret.

Extract. Given a public identity $ID \in Z_q$ (can be hashed using a hash function to desired length), compute $f_0 = f(ID)$ from the master key.
Identification Protocol: P and V do the following:

P chooses a random $r \in Z_q$, computes $x = g^r$and sends x to V.
V picks a random challenge $c \in Z_q$and sends to P.
P calculates $y = r + cf(ID)$and sends y as a response to V.
V accepts if $g^y = x \cdot \left(\prod_{t=0}^{k} D_t^{ID^t}\right)^c$

To verify the correctness of the identification protocol, we have:

$$g^y = g^{r+cf(ID)} = g^r\left(g^{f(ID)}\right)^c = g^r(g^{\sum_{t=0}^{k} d_t ID^t})^c = x.(\prod_{t=0}^{k} D_t^{ID^t})^c \quad (1)$$

3.2 Current Security

We obtain the current security for the k-resilient IBI scheme from Theorem 1 from Heng and Chin (2010).

Theorem 1. The k-resilient IBI scheme is (t, q_I, ε)-secure against impersonation under passive attacks (imp-pa) assuming the discrete log problem is (t', ε')-hard where: $\varepsilon \leq \sqrt{\frac{\varepsilon' n}{n-k}} + \frac{1}{q}$

4. THE SECURITY UPGRADE

In this section, we provide the new proof of security for the above k-resilient IBI scheme against impersonation under concurrent/ active attack (imp-aa/ca).

Theorem 2. The k-resilient IBI scheme is (t, q_I, ε)-secure against impersonation under active and concurrent attacks (imp-aa/ca) assuming the one-more discrete log problem is $(t", q_I, \varepsilon")$-hard where $\varepsilon \leq \sqrt{\frac{\varepsilon" n}{n-k}} + \frac{1}{q}$

Proof. Assume there exists an impersonator I who (t, q_I, ε)-breaks the k-resilient IBI scheme. Then we show that there is an algorithm M who $(t", q_I, \varepsilon")$-solves the OMDLP with the help of I. M will be given a group G, a generator $g \in G$, and access to oracles CHALL andDLog. M will then attempt to simulate a challenger for I as:

Setup: M begins Phase 1 by querying CHALL for the initial challenge, upon which M will be given $W_0 = g^{w_0} = g^{d_0}$. M first chooses k private keys $f_1, \ldots, f_k$at random to perform the following calculations for the system parameters $g^{d_1}, \ldots, g^{d_k}$. We have the following matrix equation:

$$\begin{bmatrix} f_1 \\ \vdots \\ f_k \end{bmatrix} = \begin{bmatrix} d_0 \\ \vdots \\ d_0 \end{bmatrix} + \begin{bmatrix} ID_1 & \cdots & ID_1^k \\ \vdots & \ddots & \vdots \\ ID_k & \cdots & ID_k^k \end{bmatrix} \begin{bmatrix} d_1 \\ \vdots \\ d_k \end{bmatrix} \tag{2}$$

with $V = \begin{bmatrix} ID_1 & \cdots & ID_1^k \\ \vdots & \ddots & \vdots \\ ID_k & \cdots & ID_k^k \end{bmatrix}$as a non-singular Vandermonde matrix with distinct elements $(ID_1, \ldots, ID_k)$. We then have $(d_1, \ldots, d_k)^T = V^{-1}(f_1 - d_0, \ldots, f_k - d_0)^T$.

Let $(b_{t_1}, \ldots, b_{t_k})$ be the t^{th} row of V^{-1}, then we obtain $d_t = b_{t_1}(f_1 - d_0) + \cdots + b_{t_k}(f_k - d_0) = b_{t_1}f_1 + \cdots b_{t_k}f_k - (b_{t_1} + b_{t_k})d_0$. Upon which, we can then calculate

$$D_t = g^{d_t} = \frac{g^{b_{t_1}f_1 + \cdots + b_{t_k}f_k}}{W_0^{b_{t_1} + \cdots + b_{t_k}}} : t = 1,2, \ldots, k \tag{3}$$

Let $f'(x) = \sum_{t=1}^{k} f_t \lambda_t(x)$ and $f(x) = f'(x) + d_0 \lambda_0(x)$ where $\lambda_t(x)$, the Lagrange coefficients, are computed from $ID_0 = 0$ and $ID_1, \ldots, ID_k$. M does not know $w_0 = f_0$. M then passes the k private keys $f_1, \ldots, f_k$and the system parameters $\langle g, W_0, D_0, \ldots, D_k \rangle$ to I.

Identification Queries: In this phase, I plays the role of a cheating verifier requesting M to prove itself with ID_j . We can assume without a loss to generality that $ID_j \notin \{ID_1, \ldots, ID_k\}$.

Commitment: M queries CHALL for a random challenge W_m*, sets* $x = W_m$*and sends it to I.*

Challenge: I selects a random challenge $c_m \in Z_q$ *and sends it to M.*

Response: M queries DLog with $W_m W_0^{c_m} \left(\prod_{t=0}^{k} D_t^{ID_j^t}\right)^{c_m}$ *and sends the result* $y_m = log\ [W_m W_0^{c_m} \left(\prod_{t=1}^{k} D_t^{ID_j^t}\right)^{c_m}]$ *to I. M increases* m *by 1.*

Impersonation Phase: After some time, I outputs the challenge identity$ID^* \notin \{ID_1, \dots, ID_k\}$ that it wishes to impersonate, thus ending Phase 1. In Phase 2, I will now assume the role of the cheating prover trying to convince M to accept. M is then able to obtain two valid transcripts (x, c_1, y_1) and $(x, c_2, y_2)$by resetting I to the commitment phase after sending x. Based on the Reset Lemma proposed by [3], M can then extract two conversation transcripts with probability more than $(\varepsilon - \frac{1}{q})^2$. M extracts the secret w_0 by calculating $f(ID^*) = \frac{y_2 - y_1}{c_2 - c_1}$ and outputs the solution to the initial challenge by calculating

$$\begin{aligned}\frac{f(ID^*) - f'(ID^*)}{\lambda_0(ID^*)} &= \frac{\sum_{t=0}^{k} f_t \lambda_t(ID^*) - \sum_{t=0}^{k} f_t \lambda_t(ID^*)}{\lambda_0(ID^*)} \\ &= \frac{d_0 \lambda_0(ID^*)}{\lambda_0(ID^*)} = d_0 = w_0\end{aligned} \tag{4}$$

M then proceeds to calculate the solutions for the other challenges as

$$w_m = y_m - c_m(w_0 + \sum_{t=1}^{k} d_t ID_j^t) \tag{5}$$

where j corresponds to the identification queries for ID_j. This way, M solves all $m + 1$ challenges by making only m queries to the DLog oracle. This completes the description of the simulation.

Probability Study: We analyze the probability of M winning the game and solving the OMDLP with strictly less queries to DLog than CHALL. Firstly, we have $\Pr[M\ computes\ w_0 | \neg abort] \geq (\varepsilon - \frac{1}{q})^2$ by the Reset Lemma, accounting for the probability that M can extract $f(ID^*)$ from two valid transcripts. Therefore, the probability of M solving the OMDLP is given by

$$\begin{aligned}\Pr[M\ wins\ OMDLP] &= \Pr[M\ computes\ w_0 \wedge \neg abort] \\ &= \Pr\,[M\ computes\ w_0 | \neg abort] \Pr\,[\neg abort]\end{aligned} \tag{6}$$

$$\varepsilon" \geq (\varepsilon - \frac{1}{q})^2 \Pr\,[\neg abort] \tag{7}$$

Finally, we calculate $\Pr\,[\neg abort]$. M will not abort in Phase 1 since there are no adaptive extract queries. In Phase 2, the probability of M not aborting is if I outputs the challenge identity ID^* which it has not queried before. This is given by the probability $\frac{n-k}{n}$ where n is the total number of users. Putting them together, we have

$$\varepsilon" \geq (\varepsilon - \frac{1}{q})^2 (\frac{n-k}{n}) \tag{8}$$

$$\frac{\varepsilon" n}{n-k} \geq (\varepsilon - \frac{1}{q})^2 \tag{9}$$

$$\varepsilon \leq \sqrt{\frac{\varepsilon" n}{n-k}} + \frac{1}{q} \tag{10}$$

4.1 Efficiency Analysis

In this section, we review the efficiency analysis of the k-resilient IBI scheme and compare it against other IBI schemes currently in literature. It is to our discovery that some values can be pre-computed and thereby we revise the complexity costs based on this discovery. The efficiency of the k-resilient IBI scheme is given as in Table 1. We compare the efficiency of the k-resilient IBI scheme against other IBI schemes in the standard model in Table 2.

TABLE 1: Complexity cost for each algorithm in the proposed k-resilient IBI.

	Addition	Multiplication	Exponentiation
Setup	0	0	*k*
Extract	0	*k*	*k*
Prove	1	1	1
Verify	0	*k*+1	2*k*+2

TABLE 2: A Comparison with other IBI schemes in the standard model.

	Efficiency	Imp-pa	Imp-aa/ca	Reset Attacks
HKIBI05a[14]	6G,6E,4P	q-SDH	unknown	Insecure
HKIBI05b[14]	12G,12E,6P	q-SDH	q-SDH	Insecure
HKIBI06[15]	9G,11E,3P,1SOTSS	q-SDH	q-SDH	Insecure
CHG08[7]	(n+4)G,5E,3P	CDH	OMCDH	Insecure
TSY09[18]	16G,20E,2P	q-SDH	2-SDH	2-SDH
k-resilient IBI	(k+2)G,(2k+3)E	DLP	OMDLP	insecure

Legend: G: Group Operations, E: Exponentiations, P: Pairings, SOTSS: Strong One-Time Signature Scheme, imp-pa: passive attack, imp-aa/ca:active/concurrent attack, CDH: computational Diffie-Hellman assumption, OMCDH: one-more computational Diffie-Hellman assumption, q-SDH: q-strong Diffie-Hellman assumption, 2-SDH: 2-strong Diffie-Hellman assumption.

5. CONCLUSION

In this paper, we have provided an upgrade of security for the *k*-resilient IBI scheme. We showed that while the scheme is secure against impersonation under passive attacks previously, it is also provably secure against impersonation attacks under active and concurrent attacks. It is also the first IBI scheme without bilinear pairings.

However while the scheme is now secure against passive, active and concurrent attackers, we have yet to prove it secure against adaptive attackers who can query any identity of its choice. We pose an open problem to construct a k-resilient identity based identification scheme secure against attackers who can query user secrets adaptively.

ACKNOWLEDGMENT

The authors would like to thank the Fundamental Research Grant Scheme EP20100429004 and the Exploratory Research Grant Scheme EP20110815001 for sponsoring this research.

REFERENCES

Bellare, M., Namprempre, C. and Neven, G. 2004. *Security Proofs for Identity-Based Identification and Signature Schemes.* In Christian Cachin and Jan Camenisch (Eds.). Advances in Cryptology -

ASIACRYPT 2004, Springer-Verlag: Lecture Notes in Computer Science (LNCS), **3027**: 268-286.

Bellare, M., Namprempre, C., Pointcheval, D. and Semanko,M. The One-More-RSA-Inversion Problems and the Security of Chaums Blind Signature Scheme. *Journal of Cryptology*. **16**(2003): 185-215.

Bellare, M. and Palacio, A. 2002. *GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks*. In Moti Yung (Ed.). Advancesin Cryptology CRYPTO 2002, Springer-Verlag: Lecture Notesin Computer Science (LNCS), **2642**: 167-177.

Bellare, M. and Rogaway, P. 1993. Random Oracles are Practical: Paradigm for Designing Efficient Protocols. *Proceedings of the 1st ACM Conference on Computer and Communications Security CCS 1993*, USA: 6273.

Canetti,R., Goldreich, O and Halevi, S. 1998. The random oraclemodel, revisited. *30th ACM Symposium on Theory of Computing STOC 1998*, pp. 209-218. ACM Press.

Cayrel, P.-L., Gaborit, P.,Galindo, D. and Girault, M. 2009. Improved Identity-based Identification using Correcting Codes. *Computing Research Repository*, Vol (abs/0903.0069).

Chin, J. J., Heng, S. H. And Goi, B. M. 2008. *An Efficient and Provable Secure Identity-Based Identification Scheme inthe Standard Model*. In S.F. Mjlsnes, S. Mauw, and S.K. Katsikas(Eds.), Euro PKI 2008,. Springer-Verlag: Lecture Notesin Computer Science (LNCS), **5057**: 60-73.

Chin, J. J., Heng, S. H. And Goi, B. M. 2009. *HIBI: An Efficient and Provable Secure Hierarchical Identity-Based Identification Scheme*. In Dominik Slezak, Tai-Hoon Kim, Wai-Chi Fang, and Kirk. P. Arnett (Eds.), Security Technology SECTECH 2009, Springer- Verlag: Communications in Computer and Information Science (CCIS), **58**: 93-99.

El Yousfi, A. M., Cayrel, P. L. and Meziani, M. Improved Identity-based Identification and Signature Schemes using Quasi-Dyadic Goppa Codes. *Proceedings of ISA 2011* (to appearing LNCS).

Heng, S. H., Chin, J. J. 2010. A k-Resilient Identity-Based Identification Scheme in the Standard Model. *International Journal of Cryptology Research*. **2**(1): 15-25.

Heng, S. H. and Kurosawa, K. 2004. *k-Resilient Identity-Based Encryption Scheme in the Standard Model.* In Tatsuaki Okamoto (Eds.), Topics in Cryptology CT-RSA 2004, Springer-Verlag: Lecture Notes in Computer Science (LNCS), **2964**: 6780.

Heng, S. H. and Kurosawa, K. 2006. k-Resilient Identity-Based Encryption Scheme in the Standard Model. *IEICE Transactions on Fundamentals*. **E89-A**(1): 39-46.

Kurosawa, K. and Heng, S. H. 2004. *From Digital Signature to ID-based Identification/Signature*. In FengBao, Robert H.Deng, and Jianying Zhou (Eds.), Public Key Cryptography PKC 2004, Springer-Verlag: Lecture Notes in Computer Science (LNCS), **2947**: 248-261.

Kurosawa, K. and Heng, S. H. 2005. *Identity-Based Identification without Random Oracles*. In Osvaldo Gervasi, MarinaL. Gavrilova, Vipin Kumar, Antonio Lagan‘a, HeowPueh Lee,Youngsong Mun, David Taniar, and Chih Jeng Kenneth Tan (Eds.), Computational Science and Its Applications ICCSA2005, Springer-Verlag: Lecture Notes in Computer Science(LNCS), **3481**: 603-613.

Kurosawa, K. and Heng, S. H. 2006. *The Power of IdentificationSchemes*. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin (Eds.), Public Key Cryptography PKC2006, Springer-Verlag: Lecture Notes in Computer Science (LNCS), **3958**: 364-377.

Kurosawa, K. and Heng, S. H. 2008. The Power of Identification Schemes. *International Journal of Applied Cryptography (IJACT).* **1**(1): 60-69.

Shamir, A. 1984. *Identity Based Cryptosystems and Signature Scheme*. In G. R. Blakley, and David Chaum (Eds.), Advances in Cryptology - CRYPTO 1984, Springer-Verlag: Lecture Notes in Computer Science (LNCS), 196: 4753.

Thorncharoensri, P., Susilo, W. and Yi, M. 2009. *Identity- Based Identification Scheme Secure against CR Attacks without RO.* In Heong Youl Youm and Moti Yung (Eds.). The 11th Workshop on Information Security Applications WISA 2009, Springer-Verlag: Lecture Notes in Computer Science (LNCS), **5932**: 94108.

Yang, G., Chen, J., Wong, D. S., Deng, X. and Wang, D. 2007. *A More Natural Way to Construct ID-Based Identification Schemes*. In Jonathan Katz, Moti Yung (Eds.), Applied Cryptography and Network Security - ACNS 2007, Springer-Verlag: Lecture Notes in Computer Science (LNCS), **4521**: 30732.