International Journal of Cryptology Research 2(1): 15-25 (2010)

A *k*-Resilient Identity-Based Identification Scheme in the Standard Model

[1]Swee-Huay Heng and [2]Ji-Jian Chin
[1]Faculty of Information Science and Technology,
Multimedia University, Jalan Ayer Keroh Lama,
75450 Bukit Beruang, Melaka, Malaysia
[2]Faculty of Engineering, Multimedia University,
Persiaran Multimedia, 63000 Cyberjaya, Selangor, Malaysia
Email: [1]shheng@mmu.edu.my, [2]jjchin@mmu.edu.my

ABSTRACT

An identification scheme allows one party to prove himself or herself (the prover) to another party (the verifier) without revealing any information regarding his or her secret. The traditional public key cryptography setting utilizes certificates to bind a user with his public key, but certificate management has since become a problem on its own. An identity-based identification scheme does away with the certificate management problem by binding a user's public key to his or her identity string. In this paper, we present a k-resilient identity-based identification (IBI) scheme. We provide a reductionist proof of security approach to prove that our scheme is secure up to k-number of passive malicious attackers by assuming the discrete logarithm problem is intractable. Our proof of security is in the standard model – we do not assume that random oracles exist.

INTRODUCTION

An identification scheme allows one prover to identify itself to another party, the verifier. Shamir (1984) proposed the idea of identity-based cryptography, and in 2004, Neven *et al.* (2004) and Kurosawa and Heng (2004) formalized the notion of identity-based identification (IBI) schemes independently. To date, IBI schemes proposed are mostly based on transformations, and are provable secure in the random oracle model.

Introduced by Bellare and Rogaway (1993), the random oracle model is an idealistic model where random oracles are used to answer any queries from both honest and malicious parties alike. Random oracles will generate a random response to new queries and return previous responses to previous queries. However, since random oracles are purely theoretical and do not exist, in practice these oracles are usually replaced by hash functions.

Canetti *et al.* (1998) demonstrated that schemes proven secure in the random oracle model are insecure in the standard model. Therefore, while having at least a proof in the random oracle model is necessary for provable security, it would be better to construct a scheme that is provably secure without random oracles.

Kurosawa and Heng (2005) proposed the first identity-based identification (IBI) scheme in the standard model, followed by another scheme by the same authors (Kurosawa and Heng, 2006, 2008) which is secure against man-in-the-middle attack. Yang *et al.* (2008) generalized a framework for IBI construction in the random oracle model, with security only in the selective-ID model for standard model schemes. Chin *et al.* (2008) proposed an efficient IBI scheme with a direct proof of security instead of relying on transformations. In latest developments in the IBI area, Chin *et al.* (2009) formalized the security model for hierarchical IBI (HIBI) schemes and proposed the first concrete HIBI scheme, while Thorncharoensri *et al.* (2009) proposed the first non-stateless IBI scheme which is secure against concurrent reset attacks, the strongest security model for IBI proposed so far.

Our Contribution

In this paper, we propose a k-resilient IBI scheme based on Heng and Kurosawa's (2004, 2006) k-resilient identity-based encryption (IBE) scheme. We show our scheme to be secure against non-adaptive passive attacks for up to k-malicious users using the discrete logarithm problem, which is indeed a very desirable weak security assumption. Our proof of security is in the standard model, without relying on the existence of random oracles. The efficiency of our scheme is also competitive with previously proposed IBI schemes as it involves no pairings and performance is linear in proportion to the number of malicious users assumed to exist, k, while independent of the total number of users.

Following the argument of Heng and Kurosawa (2004, 2006), the limit of the number of malicious users is not a serious problem in the real world. It is not easy to corrupt a large number of users normally; therefore the size of the malicious coalition cannot be too large. Heng and Kurosawa (2004, 2006) recommends the size of $k = 100$ to be sufficient for their IBE scheme. This size should be applicable to our scheme as well.

PRELIMINARIES

The Discrete Logarithm Problem (DLP)

Let G be a finite cyclic group of order q and let g be a generator of G and $\beta \in G$. The DLP of $\log_g \beta$ is to find the unique integer a where $0 \le a \le q-1$, so that $\beta = g^a$. We say that the DLP is (t, ε)-hard in G if Pr[A solves DLP] $\le \varepsilon$ for any A that runs in time t.

Lagrange Interpolation

Let q be a prime and $f(x)$ a polynomial of degree k in Z_q. Let $j_0,...,j_k$ be distinct elements in Z_q, and let $f_0 = f(j_0),...,f_k = f(j_k)$. Using Lagrange interpolation, we express the polynomial as $f(x) = \sum_{t=0}^{k} (f_t . \lambda_t(x))$, where $\lambda_t(x) = \prod_{0 \le i \ne t \le k} \frac{j_i - x}{j_i - j_t}$ for $t = 0,...,k$, are the Lagrange coefficients.

IBI Schemes Definition

An IBI scheme is specified by four polynomial-time algorithms (*SETUP, EXTRACT, PROVE and VERIFY). PROVE* and *VERIFY* interact with each other in the *IDENTIFICATION* protocol.

SETUP takes in the security parameter 1^λ and a number *k*, indicating the maximum number of malicious users, generates the initial system parameters, creates the master secret key. The master secret key will be kept secret while the system parameters will be publicized.
EXTRACT takes in the master secret key and a user ID and generates the user secret key.

IDENTIFICATION PROTOCOL. PROVE is run by the entity who wishes to prove itself to the verifier. It takes in the user secret key and sends the *commitment* to *VERIFY*, run by the verifier. *VERIFY* creates a random *challenge* and sends it to *PROVE. PROVE* then returns the *response* where VERIFY will return either accept or reject. *Commitment, challenge and response* steps form the 3-step canonical identification protocol.

Security Model for IBI

The goal of an adversary in the IBI model is impersonation. For non-adaptive setting, the adversary/impersonator has access to only a given set of corrupt user secret keys. For passive attack, the ability of the impersonator is to obtain valid transcripts of conversations between honest prover and verifier interactions. This ability can be described in a game played by a challenger *M* and an impersonator *I*.

M takes in the security parameter 1^{λ}, the number *k*, and runs *SETUP*. *M* passes the system parameters to *I* while keeping the master secret to itself. In Phase 1, *I* plays the role of the cheating prover and can issue queries in the form of extract queries to obtain corrupt user IDs and transcript queries to obtain valid conversations transcripts from *M*. These queries are interleaved and asked adaptively. We may assume *I* will not query the same ID that has been issued in extract queries in transcript queries. In Phase 2, *I* will output a challenge identity which was not queried before. This is the ID it wishes to attempt to impersonate. *I* then plays the role of the cheating prover to convince the verifier *M* to accept. *I* succeeds if *M* accepts.

We say that an IBI scheme is (t', q_I, ε')–secure under non-adaptive passive attack if for any non-adaptive passive impersonator *I* who runs in time t, $\Pr[I \text{ impersonates }] < \varepsilon$, where *I* can make at most q_I extract queries.

k-RESILIENT IDENTITY-BASED IDENTIFICATION SCHEME CONSTRUCTION

We show the construction of our *k*-resilient IBI scheme in the Table 1 below. The scheme is constructed using the underlying non-adaptive IND-CPA (indistinguishability against chosen plaintext attack) *k*-resilient IBE scheme (Heng & Kurosawa, 2004, 2006).

TABLE 1: *k*-Resilient IBI Scheme

SETUP	*EXTRACT*
Define a group G of order q such that $p = 2q+1$ and p is a prime. Pick a random generator $g \in G$. Pick a random k-degree polynomial $f(x) = \sum_{t=0}^{k} d_t x^t$ chosen over Z_q. Finally publicize $\langle g, g^{d_0}, ..., g^{d_k} \rangle$ as the system parameters and keep $f(x)$ as the master secret key.	Given a public identity $ID \in Z_q$, compute $f_{ID} = f(ID)$ from the PKG's master secret key. ID may be hashed from an arbitrary string to the desired length using a hash function.

PROVE		*VERIFY*
Pick $r \in Z_q$ and send $x = g^r$	$\xrightarrow{x}$	
	$\xleftarrow{c}$	Pick a random challenge $c \in Z_q$
Return $y = r + cf(ID)$ as response	$\xrightarrow{y}$	Accept if $g^y = x.(\prod_{t=0}^{k} g^{d_t ID^t})^c$

To show our scheme is complete, we present the following equation

$$g^y = g^{r+cf(ID)} \quad (1)$$

$$= g^r (g^{f(ID)})^c \quad (2)$$

$$= g^r (g^{\sum_{t=0}^{k} d_t ID^t})^c \quad (3)$$

$$= x.(\prod_{t=0}^{k} g^{d_t ID^t})^c \quad (4)$$

SCHEME ANALYSIS

Theorem 1. The *k*-resilient IBI scheme is (t', q_I, ε')–secure against non-adaptive passive attacks assuming the discrete logarithm problem is (t, ε)–hard where:

$$\varepsilon \leq \sqrt{\frac{\varepsilon' n}{n-k}} + \frac{1}{q} \quad (5)$$

Proof. Assume that the impersonator *I* successfully corrupts up to *k* users of its choice in the non-adaptive manner and hence obtains the *k* corresponding

private keys. We reserve indices 1 to k for corrupt users, and 0 for the challenge identity. In order to prove security, we assume there exists an impersonator I who can (t', q_I, ε')-break the IBI scheme. Then we show that there exists an algorithm M who can (t, ε)-solve the DLP. M takes in the description of group G and $(g, \beta = g^a = g^{d_0})$. M then simulates the challenger for I as follows:

1. *SETUP.* M first chooses k private keys $f_1, ..., f_k$ at random to perform the following calculations for the system parameters $g^{d_1}, ..., g^{d_k}$. If we write as the matrix equation:

$$\begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_k \end{bmatrix} = \begin{bmatrix} d_0 \\ d_0 \\ \vdots \\ d_0 \end{bmatrix} + \begin{bmatrix} ID_1 & ID_1^2 & \dots & ID_1^k \\ ID_2 & ID_2^2 & \dots & ID_2^k \\ \vdots & \vdots & \ddots & \vdots \\ ID_k & ID_k^2 & \dots & ID_k^k \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_k \end{bmatrix} \tag{6}$$

with $V = \begin{bmatrix} ID_1 & ID_1^2 & \dots & ID_1^k \\ ID_2 & ID_2^2 & \dots & ID_2^k \\ \vdots & \vdots & \ddots & \vdots \\ ID_k & ID_k^2 & \dots & ID_k^k \end{bmatrix}$ as a non-singular Vandermonde matrix and distinct elements $(ID_1, ..., ID_k)$, we then have

$$(d_1, ..., d_k)^T = V^{-1}(f_1 - d_0, ..., f_k - d_0)^T \tag{7}$$

Let $(b_{t_1}, ..., b_{t_k})$ be the t^{th} row of V^{-1} then

$$d_t = b_{t_1}(f_1 - d_0) + ... + b_{t_k}(f_k - d_k) = b_{t_1} f_1 + ... + b_{t_k} f_k - (b_{t_1} + b_{t_k}) d_0 \tag{8}$$

We can then calculate $g^{d_t} = \dfrac{g^{b_{t_1} f_1 + ... + b_{t_k} f_k}}{\beta^{b_{t_1} + ... + b_{t_k}}}$ where $t = 1, 2, ..., k$.

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 $ID_1, ..., ID_k$. Remember that M does not know $d_0 = f_0 = a$. M then passes the k private keys $f_1, ..., f_k$ and the system parameters $\langle g, \beta, g^{d_1}, ..., g^{d_k} \rangle$ to I.

2. *TRANSCRIPT QUERIES.* Whenever I makes a transcript query for ID_j, M randomly selects $y, c \in Z_q$, and returns the valid transcript

$$x = \left(\frac{g^{y}}{\left(\beta \cdot \prod_{t=1}^{k} g^{d_t ID_j^t} \right)^{c}} \right), c, y \tag{9}$$

3. *IMPERSONATION PHASE.* After some time, I outputs the challenge identity $ID^* \notin \{ID_1,..,ID_k\}$ that it wishes to impersonate. 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 Bellare and Palacio (2002), M can extract from two conversation transcripts with probability more than $\left(\varepsilon - \frac{1}{q}\right)^2$. M extracts the secret key by calculating $f(ID^*) = \frac{y_2 - y_1}{c_2 - c_1}$ and outputs the solution to the DLP by calculating $a = \frac{f(ID^*) - f'(ID^*)}{\lambda_0(ID^*)}$. This completes the description of the simulation.

4. *PROBABILITY STUDY.* It remains to analyze the probability of M winning the game and solving the DLP. First off we have the probability that M can extract $f(ID^*)$ from two conversation transcripts as Pr[M computes $a \mid \neg$ abort] $\geq \left(\varepsilon - \frac{1}{q}\right)^2$ by the Reset Lemma. Upon extraction of $f(ID^*)$, M will then be able to compute a. Therefore the probability of M winning the game by solving the discrete logarithm is given by

Pr[M solves DLP]
$= \Pr[M \text{ computes } a \wedge \neg \text{abort}]$ (10)

$= \Pr[M \text{ computes } a \mid \neg \text{abort}] \Pr[\neg \text{abort}]$ (11)

$$\varepsilon' \geq \left(\varepsilon - \frac{1}{q} \right)^2 \Pr[\neg \text{abort}] \tag{12}$$

It remains to calculate Pr[¬ 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 probability is given by $\frac{n-k}{n}$, where n is the total number of users. Putting them together, we have the probability

$$\varepsilon' \geq \left(\varepsilon - \frac{1}{q}\right)^2 \left(\frac{n-k}{n}\right) \quad (13)$$

$$\frac{\varepsilon' n}{n-k} \geq \left(\varepsilon - \frac{1}{q}\right)^2 \quad (14)$$

$$\varepsilon \leq \sqrt{\frac{\varepsilon' n}{n-k}} + \frac{1}{q} \quad (15)$$

□

Efficiency Analysis

Our scheme uses no pairings, thus it is very efficient. Efficiency of our scheme is given by Table 2 below:

TABLE 2: Efficiency Analysis of *k*-Resilient IBI Scheme

	Addition	Multiplication	Exponentiation
Setup	0	k	$2k$
Extract	0	k	k
Prove	1	k+1	k+1
Verify	0	$2k$+2	$2k$+3

CONCLUSION

We presented a k-resilient identity-based identification scheme for security up to *k* number of malicious users in coalition. Our scheme is provably secure against non-adaptive passive attacks assuming the discrete logarithm problem is intractable. The proposed scheme is efficient as it utilizes no pairing operations. Work remains to be done to prove our scheme secure against adaptive passive/active/concurrent attacks, and if possible, extend to the concurrent reset setting or hierarchical setting.

ACKNOWLEDGEMENT

This research was supported by the Fundamental Research Grant Scheme (EP20100429004).

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

Bellare, M. and Rogaway, P. 1993. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. *Proceedings of the 1st ACM Conference on Computer and Communications Security – CCS 1993*, USA: 62–73.

Canetti, R., Goldreich, O. and Halevi, S. 1998. The Random Oracle Model, Revisited. *Proceedings of the 5th ACM Conference on Computer and Communications Security – CCS 1998*, USA: 209–218.

Chin, J.-J., Heng, S.-H. and Goi, B.-M. 2008. An Efficient and Provable Secure Identity-Based Identification Scheme in the Standard Model. In S.F. Mjølsnes, S. Mauw, and S.K. Katsikas (Eds.), *EuroPKI 2008*,. Springer-Verlag: Lecture Notes in Computer Science (LNCS), **5057**: 60-73.

Chin, J.-J., Heng, S.-H. and Goi, B.-M. 2008. 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.

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**: 67–80.

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 Feng Bao, 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, Marina L. Gavrilova, Vipin Kumar, Antonio Lagan`a, Heow Pueh Lee, Youngsong Mun, David Taniar, and Chih Jeng Kenneth Tan (Eds.)*, Computational Science and Its Applications – ICCSA 2005*, Springer-Verlag: Lecture Notes in Computer Science (LNCS), **3481**: 603–613

Kurosawa, K. and Heng, S.-H. 2006. The Power of Identification Schemes. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin (Eds.), *Public Key Cryptography – PKC 2006*, 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**: 47–53.

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**: 94–108.

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**: 307–322.