SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2015; **8**:3094–3098
Published online 10 February 2015 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1234

RESEARCH ARTICLE

On the security of a lightweight authentication and encryption scheme for mobile ad hoc network

Wun-She Yap[1]*, Joseph K. Liu[2], Syh-Yuan Tan[3] and Bok-Min Goi[1]

[1] Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Kuala Lumpur, Malaysia
[2] Infocomm Security Department, Institute for Infocomm Research, A*STAR, Singapore
[3] Faculty of Information Science and Technology, Multimedia University, Melaka, Malaysia

ABSTRACT

In 2011, Eissa, Razak and Ngadi proposed a lightweight authentication and encryption scheme to enhance the performance for mobile ad hoc network in Wireless Network, Vol. 17, No. 4, 2011. The main building block of such scheme is an identity-based encryption scheme. The scheme was proven secure in the random oracle model assuming the computational Diffie–Hellman assumption is hard. In this paper, we show that the proposed scheme is not even secure against chosen plaintext attack, which is the lowest acceptable level of security. In addition, we demonstrate the RSA parameter suggested by Eissa *et al.* to yield a better network performance is not appropriate under a wrong security assumption that each mobile node is totally trusted. Such short RSA parameter leads to a key recovery attack. Copyright © 2015 John Wiley & Sons, Ltd.

KEYWORDS
wireless network; security analysis; attack; encryption

***Correspondence**
Wun-She Yap, Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, KL Campus, Kuala Lumpur, Malaysia.
E-mail: yapws@utar.edu.my

1. INTRODUCTION

A mobile ad hoc network (MANET) is a temporary self-organized infrastructureless wireless network of mobile nodes. Mobile nodes may join or leave the network concurrently because of the nodes' mobility and the unreliability of wireless channels. The mobile nodes are normally the wireless devices such as smart phone, tablet, laptops and so on. MANET can be established on the fly by the mobile nodes without depending on any central authority that manages the keys and certificates.

Eissa *et al.* [1] proposed some cryptographic techniques to set up a secure MANET. More precisely, they proposed the use of identity-based encryption (IBE) scheme along with friendship concept in securing MANET. Aside from using bilinear pairing operations, they suggested to use a shorter RSA [2] parameter (i.e. RSA public key e, RSA private key D and RSA modulus N) in transferring encrypted messages between mobile nodes for the speed reason. Their idea was that it is not possible for an attacker to mount any existing RSA key attack if the RSA public key was pre-encrypted. However, this proposal does not solve the challenging issue in securing MANET because the proposed IBE scheme still rely on a trusted third party to boost the entire wireless network.

In this paper, we examine the security of Eissa, Razak & Ngadi proposed IBE scheme under a commonly recognized security model [3]. We show that their scheme is not even secure against chosen plaintext attack. In addition, we explain why shorter RSA parameter is useless in securing the MANET. More precisely, an insider which is one of the mobile nodes may recover the RSA private key through the factoring of short RSA modulus. It is not appropriate to assume that each mobile node is *totally* trusted.

Organization. We organize this paper as follows. We provide the preliminaries and background of mathematical hard problem, definition and security models of an IBE scheme in Section 2. Next, Eissa, Razak & Ngadi proposed IBE scheme and its proofs are briefly described in Section 3. Subsequently, we point out the flaws in their

Copyright © 2015 John Wiley & Sons, Ltd.

security proofs and the security weaknesses of their IBE scheme in Section 4. We explain how the inappropriate use of short RSA parameter leads to a key recovery attack in Section 5 before concluding the findings in Section 6.

2. PRELIMINARIES

In this section, we briefly discuss the related mathematical hard problem, definition and security models of an IBE scheme that are related to the security analysis later on. One can refer to [3] for more details.

2.1. Bilinear map

Let $P \in \mathbb{G}_1$ be the generator and $\mathbb{G}_1, \mathbb{G}_2$ be the two groups of prime order q. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a bilinear map, which satisfies the following properties:

(1) Bilinearity: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab} = \hat{e}(bP, aQ)$ for all $P, Q \in \mathbb{G}_1$ and all $a, b \in \mathbb{Z}_q^*$.
(2) Nondegeneracy: $\hat{e}(P, P)$ is a generator of $\mathbb{G}_2$.
(3) Computability: $\hat{e}(P, Q)$ is efficiently computable for any $P, Q \in \mathbb{G}_1$.

2.2. Computational Diffie–Hellman assumption

Definition 2. *Let $P \in \mathbb{G}_1$ be the generator for the group $\mathbb{G}_1$ of order q. Given the values aP, bP, where $a, b \in \mathbb{Z}_q^*$ are chosen randomly, the computational Diffie–Hellman problem states that it is hard to compute the value abP.*

2.3. Definition of an identity-based encryption scheme

The notion of IBE was proposed by Shamir in 1984 [4] to rule out the certification in email systems. Every user in IBE has a public identity (ID), which is a meaningful string of any length. This ID can be viewed as an implicitly certified public key and rule out the authentication of public key. The users' private keys on the other hand are generated by a trusted party, namely, private key generator.

We now briefly review the definition of an IBE scheme by referring to [3]. An IBE scheme is an encryption scheme comprised of the following four algorithms:

(1) **Setup** takes a security parameter k to generate the system parameters, *params* and the *master-key*.
(2) **Extract** takes as input *params*, *master-key* and an $ID_i \in \{0,1\}^*$ for entity i. It returns a private key, D_i.
(3) **Encrypt** takes as input *params*, a message $m \in \mathcal{M}$ and a user identity ID_i. It returns a value $C \in \mathcal{C}$ as ciphertext.
(4) **Decrypt** takes as input *params*, $C \in \mathcal{C}$, ID_i and a private key D_i to recover a message $m \in \mathcal{M}$.

2.4. Security models of an identity-based encryption scheme

Chosen plaintext security and chosen ciphertext security are two standard security notions for public key encryption schemes. As an extension of public key encryption, IBE inherits the same security notions. For the details, one may refer to [3].

An IBE is secure against an adaptive chosen ciphertext attack (IND-ID-CCA) if no adversary $\mathcal{A}$ has a non-negligible advantage against the simulator in the security game as follows:

Setup. The simulator runs the Setup algorithm using the security parameter k. It provides the resulting system parameters, *params*, to adversary $\mathcal{A}$ and keep secret the master-key.

Phase 1. $\mathcal{A}$ can issue two types of queries as follows:

- Extraction query $\langle ID_i \rangle$. When queried, the simulator runs algorithm Extract and returns to $\mathcal{A}$ the private key, D_i.
- Decryption query $\langle ID_i, C_i \rangle$. When queried, the simulator checks if the private key, D_i (corresponding to the ID_i), exists. If D_i exists, the simulator runs algorithm Decrypt to decrypt the ciphertext C_i and sends to $\mathcal{A}$ the plaintext m_i. Else if D_i does not exist, the simulator runs algorithm Extract to generate ID_i before decryption.

Each query q_i may be asked adaptively such that it depends on the responses of previous queries.

Challenge. $\mathcal{A}$ declared the challenged ID and submits two chosen plaintexts $m_0, m_1 \in \mathcal{M}$ to the simulator. The only constraint on ID is that it does not appear in extraction query in Phase 1. The simulator randomly picks a bit $b \in \{0,1\}$ and returns $C = \text{Encrypt}(params, ID, m_b)$ to $\mathcal{A}$.

Phase 2. $\mathcal{A}$ can issue more queries $q_{j+1}, \ldots, q_k$, where q_i is one of:

- Extraction query $\langle ID_i \rangle$, where $ID_i \neq ID$. The simulator responds as in Phase 1.
- Decryption query $\langle ID_i, C_i \rangle$ where $\langle ID_i, C_i \rangle \neq \langle ID, C \rangle$. The simulator responds as in Phase 1.

These queries may be asked adaptively as in Phase 1.

Guess. Finally, $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$. If $b' = b$, $\mathcal{A}$ wins the game; otherwise, it fails.

Definition 3. *We say that an IBE scheme is IND-ID-CCA secure if for every adversary $\mathcal{A}$, the advantage in guessing the correct bit $b' = b$ is no better than random guessing:*

$$Adv_{IBE}^{IND-ID-CCA} < \frac{1}{2} + \epsilon$$

where ϵ is a negligible probability.

Chosen plaintext security (IND-ID-CPA) is a weaker notion of security for an encryption scheme. It is similar to chosen ciphertext security except that the adversary cannot ask any decryption queries.

3. EISSA AND COLLEAGUES' IDENTITY-BASED ENCRYPTION SCHEME

Because the focus of this paper is on the security of encryption mechanism, we omit some unrelated details such as the definition of elliptic curves and preauthentication process. We describe briefly Eissa, Razak & Ngadi IBE scheme [1] as follows:

Setup. Given a security parameter k, the algorithm works as follows:

- Step 1: Create two groups $\mathbb{G}_1, \mathbb{G}_2$ of order q and a bilinear map $\hat{e}$. Choose a random generator $P \in \mathbb{G}_1$.
- Step 2: Choose two secure hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1^*, H_2 : \mathbb{G}_2^* \rightarrow \{0,1\}^n$, where n is the size of the message space.

The system parameters are $params = \langle \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, H_1, H_2 \rangle$.

Extract. The algorithm works as follows:

- Step 1: Generate an identity key $Q_i = H_1(ID_i \| Time)$.
- Step 2: Generate the RSA parameters $RSA_i = \langle e_i, D_i, N_i \rangle$, where e_i denotes RSA public key, D_i denotes RSA private key and N_i denotes RSA modulus.
- Step 3: Publish $P_i = D_i P$.

Encrypt. Consider the scenario where the node $Node_i$ with ID_i wishes to send a ciphertext to the node $Node_j$ with ID_j. The algorithm is run by $Node_i$, and it works as follows:

- Step 1: Compute $g_{i,j} = \hat{e}\left(Q_j, P_j\right)^{D_i} \times \hat{e}\left(D_i Q_i, P_j\right)$, where $Q_j = H_1\left(ID_j \| Time\right)$ and $P_j = D_j P$.
- Step 2: Compute $c_{i,j} = e_i \oplus H_2\left(g_{i,j}\right)$.
- Step 3: Send the ciphertext $C = \left\langle N_i, c_{i,j} \right\rangle$ to $Node_j$.

Note that e_i is treated as the message to be encrypted in an encryption scheme.

Decrypt. Consider the scenario where $Node_j$ receives the ciphertext $C = \left\langle N_i, c_{i,j} \right\rangle$ from $Node_i$. The algorithm is run by $Node_j$ and it works as follows:

- Step 1: Compute $g_{j,i} = \hat{e}\left(Q_i, P_i\right)^{D_j} \times \hat{e}\left(D_j Q_j, P_i\right)$ where $P_i = D_i P$.
- Step 2: Recover $e_i = c_{i,j} \oplus H_2\left(g_{j,i}\right)$.

Thus, $Node_j$ knows $Node_i$'s RSA public key e_i and RSA modulus N_i. For future communications, $Node_j$ uses $Node_i$'s RSA public key to encrypt messages, while $Node_i$ uses his RSA private key D_i to decrypt ciphertexts. Because Eissa *et al.* proposed the use of shorter RSA keys, the time needed for both encryption and decryption will be much shorter [1]. The correctness of the previously mentioned IBE scheme can be verified easily as follows:

$$\begin{aligned}
& c_{i,j} \oplus H_2\left(g_{j,i}\right) \\
&= e_i \oplus H_2\left(g_{i,j}\right) \oplus H_2\left(\hat{e}\left(Q_i, P_i\right)^{D_j} \times \hat{e}\left(D_j Q_j, P_i\right)\right) \\
&= e_i \oplus H_2\left(g_{i,j}\right) \oplus H_2\left(\hat{e}\left(Q_i, D_i P\right)^{D_j} \times \hat{e}\left(D_j Q_j, D_i P\right)\right) \\
&= e_i \oplus H_2\left(g_{i,j}\right) \oplus H_2\left(\hat{e}\left(Q_i, D_j P\right)^{D_i} \times \hat{e}\left(Q_j, D_j P\right)^{D_i}\right) \\
&= e_i \oplus H_2\left(g_{i,j}\right) \oplus H_2\left(\hat{e}\left(D_i Q_i, P_j\right) \times \hat{e}\left(Q_j, P_j\right)^{D_i}\right) \\
&= e_i \oplus H_2\left(g_{i,j}\right) \oplus H_2\left(g_{i,j}\right) \\
&= e_i
\end{aligned}$$

Remark. *Note that there are likely typos in* [1]. *In their description of the Decrypt algorithm, one needs to apply a cryptographic hash operation (i.e. H_3) to recover e_i. It is obvious that such operation is redundant, else it will not satisfy the standard consistency constraint. Moreover, one should have an extra check when choosing the value of e_i in* [1] *to make sure the inverse of e_i exists (i.e. $d_i = e_i^{-1} \bmod \phi(N_{ID})$, where $\phi(N_{ID})$ is the Euler's totient function).*

4. ON THE SECURITY OF EISSA AND COLLEAGUES' IDENTITY-BASED ENCRYPTION SCHEME

Eissa *et al.* [1] emphasized that their proposed scheme does not need certificates implementation because it uses IBE concept to secure the RSA public key, which is treated as a message and is encrypted using an IBE scheme. Once the encrypted RSA public key is decrypted by the receiver, the key can be used as in conventional RSA public key scheme. The main idea in [1] is that the RSA keys can be used securely even the RSA keys are shorter than the keys involved in conventional RSA public key scheme. It is thus reasonable to examine Eissa, Razak and Ngadi IBE scheme using the notions of IND-ID-CCA and IND-ID-CPA described in Section 2.4.

4.1. On the security proofs of Eissa and colleagues' identity-based encryption scheme

To prove the security of their scheme, Eissa *et al.* [1] proposed a new security notion, namely, indistinguishability under chosen secret public key attack (IND-CSPKA).

Under the security model of IND-CSPKDA, two types of adversary had been defined in which Type 1 adversary's goal is to recover the encrypted RSA public key during the public key announcement phase, while Type 2 adversary's goal is to recover the encrypted message after the public key announcement phase.

Based on the security notion, three security claims have been made. First claim stated that the scheme can be used as an authentication scheme and is secure if the computational Diffie–Hellman problem is hard in the random oracle model. Second claim reported the security against Type 1 adversary, while the last claim described a generic proof of RSA encryption against the Type 2 adversary.

As stated in [1], Eissa *et al.* claimed that IND-CSPKA attack can be converted to IND-ID-CCA attack by replacing the RSA public keys with the messages. It is obvious that the so called new security notion of IND-CSPKA is equivalent to IND-ID-CCA.

There exists one fundamental flaw in the security proofs given by Eissa *et al.*, where no hard problems are linked with the security proofs. In order to prove that an encryption scheme is secure, one needs to show that if an adversary can win the games as stated in Section 2.4, then the adversary can also break the underlying hard problem. Since the hard problem is intractable, there is a proof by contradiction, and thus, such adversary does not exist in the real world. In the case where the hard problem is not linked to the scheme in the security game, one cannot claim that such scheme is provable secure. As a conclusion, the security of Eissa, Razak & Ngadi IBE scheme remains as an open question, which will be answered in the next subsection.

4.2. Chosen ciphertext attack

We now describe a chosen ciphertext attack against Eissa, Razak & Ngadi IBE scheme. Without loss of generality, we denote e_i with m_i. We assume the adversary $\mathcal{A}$ aims to attack $Node_i$ with ID_i. $\mathcal{A}$ can win the security game of IND-ID-CCA specified in the Subsection 2.4 as follows:

(1) $\mathcal{A}$ obtains $params = \langle \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, H_1, H_2 \rangle$, P_i, N_i and P_j from the simulator.
(2) **Challenge.** $\mathcal{A}$ submits two challenged plaintexts m_0, m_1 to the simulator. The simulator randomly chooses a bit $b \in \{0,1\}$ and returns the corresponding ciphertext $C = \langle N_i, c_b = m_b \oplus H_2(g_{i,j}) \rangle$ to $\mathcal{A}$, where $g_{i,j}$ involves $Node_i$ and $Node_j$.
(3) **Phase 2.** $\mathcal{A}$ asks the simulator a decryption query of $\langle ID_i, C' \rangle$, where $C' = \langle N_i, c'_b = c_b \oplus 1 \rangle$. The simulator then returns $c'_b \oplus H_2(g_{i,j})$ to $\mathcal{A}$.
(4) **Guess.** Note that $\mathcal{A}$ knows the value of $m_b \oplus 1$ because

$$\begin{aligned} c'_b \oplus H_2(g_{i,j}) &= c_b \oplus 1 \oplus H_2(g_{i,j}) \\ &= m_b \oplus H_2(g_{i,j}) \oplus 1 \oplus H_2(g_{i,j}) \\ &= m_b \oplus 1 \end{aligned}$$

Thus, $\mathcal{A}$ can easily determine the value b by comparing m_b with m_0 and m_1. $\mathcal{A}$ always wins the game with advantage $Adv_{IBE}^{IND\text{–}ID\text{–}CCA} = 1$.

As a matter of fact, deterministic encryption schemes can never achieve the chosen ciphertext security. This is due to the lack of randomization in the encryption process. Thus, Eissa, Razak & Ngadi IBE scheme is not IND-ID-CCA secure.

4.3. Chosen plaintext attack

Because Eissa, Razak & Ngadi IBE scheme is not secure against a chosen ciphertext attack, a very natural question is whether it is secure against a chosen plaintext attack, which is a weaker attack than a chosen ciphertext attack. Under the security notion of IND-ID-CPA given in the Subsection 2.4, the adversary $\mathcal{A}$ does not have the access of decryption oracle as in the security notion of IND-ID-CCA.

It is obvious to spot the difference between Eissa, Razak and Ngadi IBE scheme [1] with the existing IBE schemes [3,4], where the private key generator's *master-key* is not involved in Eissa, Razak & Ngadi IBE scheme. Besides, it is weird that there exists another public parameter published by the nodes, namely D_iP. Because no certificate is involved, thus, one can always change this public parameter. For example, the adversary may intercept the original public parameter and block it from reaching other nodes within the same wireless network. To make things worse, the adversary may choose another value of D'_i and broadcast the new public parameter D'_iP by impersonating the targeted node $Node_i$.

We assume the adversary $\mathcal{A}$ aims to attack $Node_i$ with ID_i. Due to the earlier reasons, it is reasonable to assume that the adversary had modified the $Node_j$'s public parameter without being detected by the other nodes within the same wireless network. We assume the corrupted public parameter as $P'_j = D'_jP$, where D'_j is picked randomly by the adversary. Using the corrupted public parameter, $\mathcal{A}$ can win the security game of IND-ID-CPA as follows

(1) $\mathcal{A}$ obtains $params = \langle \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, H_1, H_2 \rangle$, P_i and N_i from the simulator.
(2) **Challenge.** $\mathcal{A}$ submits two challenged plaintexts m_0, m_1 to the simulator. The simulator randomly chooses a bit $b \in \{0,1\}$ and returns the ciphertext $C = \langle N_i, c_b = m_b \oplus H_2(g_{i,j}) \rangle$ to $\mathcal{A}$, where $g_{i,j} = \hat{e}\left(Q_j, P'_j\right)^{D_i} \times \hat{e}\left(D_iQ_i, P'_j\right)$.
(3) **Guess.** Because $\mathcal{A}$ knows the value of D'_j, m_b can be recovered as follows:

$$\begin{aligned} & c_b \oplus H_2(g_{j,i}) \\ &= m_b \oplus H_2(g_{i,j}) \oplus H_2\left(\hat{e}(Q_i, P_i)^{D'_j}\right. \end{aligned}$$

$$\times \hat{e}\left(D'_j Q_j, P_i\right)\Big)$$
$$= m_b \oplus H_2\left(g_{i,j}\right) \oplus H_2\left(\hat{e}(Q_i, D_i P)^{D'_j} \times \hat{e}\left(D'_j Q_j, D_i P\right)\right)$$
$$= m_b \oplus H_2\left(g_{i,j}\right) \oplus H_2\left(\hat{e}\left(Q_i, D'_j P\right)^{D_i} \times \hat{e}\left(Q_j, D'_j P\right)^{D_i}\right)$$
$$= m_b \oplus H_2\left(g_{i,j}\right) \oplus H_2\left(\hat{e}\left(D_i Q_i, P'_j\right) \times \hat{e}\left(Q_j, P'_j\right)^{D_i}\right)$$
$$= m_b \oplus H_2\left(g_{i,j}\right) \oplus H_2\left(g_{i,j}\right)$$
$$= m_b$$

Thus, $\mathcal{A}$ can easily determine the value b by comparing m_b with m_0 and m_1. $\mathcal{A}$ always wins the game with advantage $Adv_{IBE}^{IND\text{–}ID\text{–}CPA} = 1$.

One of the reason such chosen plaintext attack works against Eissa, Razak & Ngadi IBE scheme is due to the lack of binding between the *master-key* and the identity *ID*.

5. ON THE SECURITY OF SHORTER RSA KEYS

In this subsection, we comment several other security issues regarding the usage of shorter RSA parameter, $RSA = \langle e, D, N\rangle$. One of the wrong assumption made by Eissa *et al.* is that each mobile node is trusted, and thus, this gives rise to a malicious insider attack.

In [1], Eissa *et al.* proposed the usage of shorter RSA parameter to boost the network performance in which the time needed to encrypt message and decrypt ciphertext will be shorter. The idea is that shorter RSA key attacks cannot be done without the knowledge of the RSA public key e and the RSA modulus N. Thus, Eissa *et al.* encrypted the RSA public key e from being known by the untrusted nodes using their proposed IBE scheme. Moreover, when a new node joins the network, its RSA public key e should be validated by the other nodes using threshold cryptography. The new node needs to sign its RSA public key e using the knowledge of its RSA private key D and the service public key agreed by all other nodes.

At first glance, Eissa, Razak & Ngadi intuition sounds fine. However, one cannot guarantee that all the nodes which join the same network are trusted. To prevent untrusted nodes from joining the network, Eissa *et al.* proposed a preauthentication phase, which is a friendship voting system. If a number of neighbour nodes trust the new node, then the new node is allowed to join the network. Even if a preauthentication phase is included, the malicious node still can join the network by paying more cost, that is, to fake more number of nodes. Once the untrusted node joins the network, then it can recover all nodes' RSA private keys because it knows all nodes' RSA public keys and the short RSA modulus. To result a secure RSA cryptosystem, RSA key size should be at least 1024 bits; however, Eissa *et al.* proposed the use of 200 bits for N and 50 bits for e. According to [5], such 200-bit long N can be factored within seconds using hundreds of workstations and self-initializing quadratic sieve.

Because no certificate is involved in certifying the RSA public keys, the adversary can sign on behalf of any nodes by regenerating a new RSA parameter. Thus, the RSA public key's validation proposed by Eissa *et al.* is insecure too. Moreover, if the adversary can obtain such signature in validating the public key e, the adversary is still able to factor N and discover the RSA private key D even if the adversary does not know the RSA public key e. This can be done by launching a naive exhaustive search on 50-bit long e and check whether it is consistent with the signature.

6. CONCLUSION

In this paper, we revisited the lightweight authentication and encryption scheme proposed by Eissa *et al.* that is used to secure MANET. We showed that this IBE scheme is vulnerable to both chosen ciphertext and chosen plaintext attacks. Aside from this, we discussed the security weaknesses for using shorter RSA parameter in securing MANET, as well as in the authentication part. Most importantly, aside from being not secure, the idea of using IBE concept in securing MANET by Eissa *et al.* will never solve the challenging issue faced by MANET as IBE needs a trusted third party (which cannot be found in MANET) to boost the entire wireless network. We thus believe that this paper can tweak the misconceptions in an identity-based encryption scheme proposed by Eissa *et al.* [1] for securing MANET.

REFERENCES

1. Eissa T, Razak SA, Ngadi MDA. Towards providing a new lightweight authentication and encryption scheme for MANET. *Wireless Networks* 2011; **17**(4): 833–842.
2. Rivest R, Shamir A, Adleman L. A Method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* 1978; **21** (2): 120–126.
3. Boneh D, Franklin M. Identity based encryption from the Weil pairing. *SIAM Journal of Computing* 2003; **32**(3): 586–615.
4. Shamir A. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology — CRYPTO '84*, LNCS 0196. Springer-Verlag: Santa Barbara, California, USA, 1985; 47–53.
5. Milan J. Factoring Small to Medium Size Integers. An Experimental Comparison. INRIA, CNRS-00188645, version 3, 29 Jan 2010.

DOI: 10.1002/sec