4-2010

Practical ID-based encryption for wireless sensor network

Cheng-Kang CHU
Singapore Management University

Joseph K. LIU
Institute for Infocomm Research

Jianying ZHOU
Institute for Infocomm Research

Feng BAO
Institute for Infocomm Research

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

DOI: https://doi.org/10.1145/1755688.1755734

Citation

CHU, Cheng-Kang; LIU, Joseph K.; ZHOU, Jianying; BAO, Feng; and DENG, Robert H.. Practical ID-based encryption for wireless sensor network. (2010). *ASIACCS '10: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, April 13-16, Beijing*. 337-340. Research Collection School Of Information Systems.
Available at: https://ink.library.smu.edu.sg/sis_research/635

Practical ID-based Encryption for Wireless Sensor Network[*]

Cheng-Kang Chu
Singapore Management University
ckchu@smu.edu.sg

Joseph K. Liu
Institute for Infocomm Research
ksliu@i2r.a-star.edu.sg

Jianying Zhou
Institute for Infocomm Research
jyzhou@i2r.a-star.edu.sg

Feng Bao
Institute for Infocomm Research
baofeng@i2r.a-star.edu.sg

Robert H. Deng
Singapore Management University
robertdeng@smu.edu.sg

ABSTRACT

In this paper, we propose a new practical identity-based encryption scheme which is suitable for wireless sensor network (WSN). We call it *Receiver-Bounded Online/Offline Identity-based Encryption* (RB-OOIBE). It splits the encryption process into two parts – the offline and the online part. In the offline part, all heavy computations are done without the knowledge of the receiver's identity and the plaintext message. In the online stage, only light computations such as modular operation and symmetric key encryption are required, together with the receiver's identity and the plaintext message. Moreover, since each offline ciphertext can be re-used for the same receiver, the number of offline ciphertexts the encrypter holds only confines the number of receivers instead of the number of messages to be encrypted. In this way, a sensor node (with limited computation power and limited storage) in WSN can send encrypted data easily: A few offline ciphertexts can be computed in the manufacturing stage while the online part is light enough for the sensor to process.

We propose an efficient construction for this new notion. The scheme can be proven selective-ID CCA secure in the standard model. Compared to previous online/offline identity-based encryption schemes, our scheme is exempt from a high storage requirement, which is proportional to the number of messages to be sent. The improvement is very significant if many messages are sent to few receivers.

1. INTRODUCTION

A wireless sensor network (WSN) is a wireless network composed of a large number of sensor nodes. In WSNs the scarcest resource is energy. For this reason, algorithmic research in WSN mostly focuses on the study and design of energy aware algorithms for data computation. This problem becomes harder in the case of security, as most of the security algorithms are quite heavy. Although symmetric cryptography maybe one of the approaches to solve the problem due to their small computation requirement, key distribution matter becomes another side effect. Recently, researchers are trying to apply assymmetric cryptography into WSN environment. Solutions include using online/offline algorithms and stateful public key encryption schemes.

ONLINE/OFFLINE ALGORITHM. "Online/offline" cryptographic algorithm was first introduced by Even, Goldreich and Micali [8], in the context of digital signature. Under this paradigm, the signing process can be divided into two phases. The first phase is called *offline* phase which is executed prior to the arrival of a message and the second phase is called *online* phase which is performed after knowing the message. The online phase should be very fast and require only very light computation, such as integer multiplication or hashing. Other heavier computation such as exponentiation should be avoided in the online phase. This is the basic characteristic of online/offline schemes. In this way, online/offline schemes are particularly useful for low-power devices such as smartcard or wireless sensor applications. Those heavy computations are done in the offline phase which can be carried out by other powerful devices, or even pre-computed by the manufacturers in the setup stage.

In parallel to online/offline signatures [15, 11, 6, 10], the first online/offline encryption scheme was proposed by Guo, Mu and Chen [9]. Similar to online/offline signature schemes, all heavy computations are done in the offline phase, without knowing the message to be encrypted. In the online phase, only light computations are executed with the knowledge of the plaintext. Nevertheless, there is a slight difference in the definition between online/offline signature and encryption schemes. Let us take a look on the following example. If we split the encryption process in the same way as the signing process, it is trivial to separate some standard encryption, such as ElGamal encryption scheme. In an ElGamal encryption scheme, the sender first computes $c_1 = g^r, c_1' = y^r$ for some randomly generated r where y is the public key of the

[*] This is the full version of [7]

receiver. This can be considered as the offline phase, as the message is still yet unknown. After knowing the message, the sender computes $c_2 = m \cdot c_1'$. As this part only requires a multiplication, it can be considered as the online part. The ciphertext is (c_1, c_2). However, it is only suitable for the situation where the sender knows the recipient of the encrypted message in the offline phase, since the offline phase requires the knowledge of the public key of the recipient. We are not interested in this scenario. Instead, we consider a notion that allows the knowledge of the recipient is yet unknown in the offline phase. [9] uses this definition for their scheme, in the context of identity-based encryption.

The above online/offline encryption (where the knowledge of the recipient is unknown in the offline phase) seems useful in many scenarios. However, it may not be practical enough to be used in WSN. As the offline information cannot be re-used, to encrypt *every* message one needs to execute the offline encryption process once. For example, if a sensor node needs to send 1000 encrypted data to the base station during its lifetime, it needs to store 1000 pieces of offline information first. Due to limited storage capacity inside a sensor node, it may not be practical. We call such encryption as *message-bounded* online/offline encryption (or OOIBE for short).

STATEFUL PUBLIC KEY ENCRYPTION. Bellare et al. [2] proposed a method to significantly speed-up the public key encryption (PKE) by simply allowing a sender to maintain a “state” that is re-used across different encryptions. This new type of PKE is called *stateful PKE*. This can greatly reduce the computation cost for the sender if it wants to encrypt messages many times. Moreover, if the sender stores some more information with respect to the receiver's public key, it may not need any more exponential computation for encrypting to this receiver. As an efficient construction, Bellare et al. presented a stateful PKE scheme based on the Diffie-Hellman assumption. Stateful encryption can be used in WSNs [1] to reduce the computation cost of sensor nodes, compared with normal public key encryption.

Although stateful public key encryption reduces the computation cost a lot, the encrypter still needs to perform heavy computation at least once for each receiver. That limits the flexibility of its usage. In WSN environment, sometimes a sensor node may need to send data to different recipients, say, different base stations. Thus stateful public key encryption is not yet a perfect solution.

IDENTITY-BASED CRYPTOSYSTEM. Identity-Based (ID-Based) Cryptosystem, introduced by Shamir [14], eliminates the necessity for checking the validity of certificates in traditional public key infrastructure (PKI). In an ID-based cryptosystem, public key of each user is easily computable from an arbitrary string corresponding to this user's identity (e.g. an email address, a telephone number, etc.). Using its master key, a private key generator (PKG) then computes a private key for each user. This property avoids the requirement of using certificates and associates implicitly a public key (i.e. user identity) to each user within the system. One only needs to know the recipient's identity in order to send an encrypted message to him. It avoids the complicated and costly certificate (chain) verification for the authentication purpose. In contrast, the traditional PKI needs an additional certification verification process, which is equivalent to the computation of *two* signature verifications. Identity-based system is particularly suitable for power constrained devices such as sensor nodes or smartcards. The absence of certificate eliminates the costly certificate verification process. In addition, when there is a new node added to the network, other nodes do not need to have its certificate verified in order to communicate in a secure and authenticated way. This can greatly reduce communication overhead and computation cost.

Both two message-bounded online/offline encryption schemes proposed by [9] are in identity-based setting. The first scheme requires 7 pairing operations in the decryption stage. It is proven secure in the selective-ID model. While for the second scheme, it is secure in the full security model, though the ciphertext is very large (more than 4700 bits). Recently Liu and Zhou [12] proposed another efficient OOIBE scheme. The ciphertext is just 1248 bits. However, their scheme can be only proven secure in the random oracle model. For stateful public key encryption, there is only one identity-based solution [13] which is also proven secure in the random oracle model only.

1.1 Receiver-Bounded Online/Offline Identity-Based Encryption

Receiver-Bounded Online/Offline Identity-Based Encryption (RB-OOIBE) is a practical encryption solution on wireless sensor nodes. It allows a sensor node to encrypt data with *low computation power* and *low precomputation storage*. Briefly, the data sender prepares a small number of offline ciphertexts first, say, n. Since computing offline ciphertexts doesn't require the receiver's identity, it can be executed in the manufacturing stage. Then the data sender can enjoy light encryption process on unlimited messages for up to n receivers. In other words, as long as there are less than n receivers, the data sender can avoid all heavy computations.

RB-OOIBE gets rid of the shortcomings of online/offline and stateful encryption. Unlike message-bounded online/offline encryption, it doesn't need to prepare a large amount of offline ciphertexts (one for each encryption). An offline ciphertext is dedicated to a receiver instead of a message to be encrypted. Unlike stateful encryption, the sender of RB-OOIBE doesn't need any heavy computation when he encrypts messages for up to n different receivers.

RB-OOIBE is most suitable for WSNs. In the WSN environment, sensitive data are collected and encrypted by a low-power and low-storage sensor node, and then are sent back to one of several connected base stations. In general, lots of sensing data will be sent to the same base station (receiver). The sensor node may store up to n pieces of offline part information in the manufacturing stage, so that it can send unlimited encrypted data to n different base stations without any further heavy computation, while these base station identities can be unknown to the manufacturer.

COMPARED WITH HYBRID CRYPTOSYSTEMS. A hybrid cryptosystem consists of a public key (or identity-based) cryptosystem and a symmetric key cryptosystem. The sender first encrypts a symmetric key using the receiver's public key (or identity) and sends it to the receiver so that they can communicate with each other via the symmetric key cryptosystem. We can see that using hybrid cryptosystems, the sender has to perform a *full* public key encryption procedure before communicating to each receiver. Even the sender uses OOIBE to encrypt messages, the receiver is not stateless – it has to keep a key for each sender. Therefore, hybrid cryptosystems are not suitable for a large scale network where 1) a low-power device has to send data to multiple recipients; 2) a stateless device has to receive data from many other parties.

1.2 Contribution

In this paper, we propose a new notion of *Receiver-Bounded Online/Offline Identity-Based Encryption* (RB-OOIBE). We provide an efficient construction which can be proven selective-ID CCA secure in the standard model. The advantage of our schemes over previous OOIBE schemes is very clear if a sender sends multiple messages to one recipient. Our scheme re-uses most of the previous information including the offline pre-computed data. Only a small offline ciphertext has to be stored on the sensor node. In contrast, other OOIBE schemes require a number of offline information which is proportional to the number of messages to be encrypted. The difference is significant if there are lots of messages to be sent by a sender.

Even for encrypting one message, our scheme is more efficient than all OOIBE schemes in the literature. There were only three schemes proposed: two of them were proposed by Guo, Mu and Chen in [9]. We use GMC-1 and GMC-2 to denote them respectively. The remaining scheme was proposed by Liu and Zhou [12]. We use LZ to denote it. When compared to GMC-1 (selective-ID security) and GMC-2 (full security), our scheme enjoys over 50% improvement in storage cost and ciphertext size. Even if we compare our schemes with LZ (which is proven secure only in the random oracle model), our scheme also gains efficiency improvement in storage cost and online computation cost.

Note that we don't need to care about selective-ID security here. Usually, there are at most hundreds of base stations in a wireless sensor network. That means we only need hundreds of identities in the system. The simulator can guess the attacking identity in advance, and this will not loosen the security reduction too much in practice.

The rest of the paper is organized as follow. Some mathematical and security definitions are presented in Section 2. Our proposed scheme is given in Section 3. In Section 4 we give a performance comparison with previous schemes and we conclude the paper in Section 5.

2. DEFINITION

In this section we briefly describe the assumptions and definitions of our construction.

2.1 Bilinear Group

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic groups of prime order p. Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be a map with the following properties:

- Bilinear: for all $g_1, g_2 \in \mathbb{G}$ and $a, b \in \mathbb{Z}$, $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.
- Non-degenerate: for some $g \in \mathbb{G}$, $e(g, g) \neq 1$.

We say that $\mathbb{G}$ is a bilinear group if the group operations in $\mathbb{G}$ and $\mathbb{G}_T$, and the bilinear map are efficiently computable.

2.2 Complexity Assumption

Our construction is based on the decision Bilinear Diffie-Hellman (BDH) assumption [5, 3]. the decision BDH problem in $\mathbb{G}$ is that given a tuple $g, g^a, g^b, g^c \in \mathbb{G}$ and an element $Z \in \mathbb{G}_T$, decide if $Z = e(g, g)^{abc}$.

Definition 1. The decision BDH assumption holds in $\mathbb{G}$ if no polynomial time algorithm $\mathcal{A}$ has non-negligible advantage in solving the Decisional BDH problem. More precisely, we define the advantage of $\mathcal{A}$ in distinguishing two distributions as

$$\mathsf{Adv}^{\mathrm{BDH}}_{\mathcal{A},\mathbb{G}}(\lambda) = |\Pr[\mathcal{A}(1^\lambda, g, g^a, g^b, g^c, e(g,g)^{abc}) = 1] - \Pr[\mathcal{A}(1^\lambda, g, g^a, g^b, g^c, R) = 1]|,$$

where $R \in_R \mathbb{G}_T$ and the size of group $\mathbb{G}$ depends on the security parameter λ. The decision BDH assumption holds in $\mathbb{G}$ if $\mathsf{Adv}^{\mathrm{BDH}}_{\mathbb{G}}(\lambda) = max_{\mathcal{A}}\{\mathsf{Adv}^{\mathrm{BDH}}_{\mathcal{A},\mathbb{G}}(\lambda)\}$ is negligible for any adversary $\mathcal{A}$.

2.3 Building Block

We introduce three building blocks used in our schemes:

- an IND-CCA secure symmetric encryption scheme.

  The IND-CCA security of a symmetric encryption scheme SE=(SEnc, SDec) with key length k is captured by defining the advantage of an adversary $\mathcal{A}$ as

  $$\mathsf{Adv}^{\mathrm{CCA}}_{\mathcal{A},\mathsf{SE}}(\lambda) = 2 \cdot \Pr[\beta' = \beta : K \in_R \{0,1\}^k; \beta \in_R \{0,1\}; \beta' \leftarrow \mathcal{A}^{\mathsf{SEnc}_K, \mathsf{SDec}_K, \mathsf{Chal}_{K,\beta}}(1^\lambda)] - 1.$$

  In the above, $\mathsf{Chal}_{K,\beta}(m_0, m_1)$ returns $\mathsf{SEnc}_K(m_\beta)$. Moreover, $\mathcal{A}$ is allowed to issue only one query to the Chal oracle, and is not allowed to query SDec_K on the ciphertext returned by it. The symmetric encryption scheme is IND-CCA secure if $\mathsf{Adv}^{\mathrm{CCA}}_{\mathsf{SE}}(\lambda) = max_{\mathcal{A}}\{\mathsf{Adv}^{\mathrm{CCA}}_{\mathcal{A},\mathsf{SE}}(\lambda)\}$ is negligible for any adversary $\mathcal{A}$.

- a collision-resistant hash function.

  A hash function $H : \{0,1\}^* \to \mathbb{Z}_p$ is collision-resistant if no polynomial time adversary $\mathcal{A}$ has non-negligible advantage in finding collisions on it. More precisely, we define the advantage of $\mathcal{A}$ as

  $$\mathsf{Adv}^{\mathrm{COL}}_{\mathcal{A},H}(\lambda) = \Pr[H(x_1) = H(x_2) \wedge x_1 \neq x_2 : (x_1, x_2) \leftarrow \mathcal{A}(1^\lambda)],$$

  where the size of group $\mathbb{Z}_p$ depends on the security parameter λ. The hash function is collision-resistent if $\mathsf{Adv}^{\mathrm{COL}}_{H}(\lambda) = max_{\mathcal{A}}\{\mathsf{Adv}^{\mathrm{COL}}_{\mathcal{A},H}(\lambda)\}$ is negligible for any adversary $\mathcal{A}$.

- a secure key derivation function.

  A key derivation function $D : \mathbb{G}_T \to \{0,1\}^k$ on a random input outputs a k-bit string which is computationally indistinguishable from a random string. We define the advantage of an adversary $\mathcal{A}$ in distinguishing two distributions as

$$\mathsf{Adv}_{\mathcal{A},D}^{KDF}(\lambda) = \Pr[\mathcal{A}(1^\lambda, D(x)) = 1] - \Pr[\mathcal{A}(1^\lambda, r) = 1]$$

where $x \in \mathbb{G}_T, r \in_R \{0,1\}^k$ and λ is the security parameter determining k. So the key derivation function is *KDF-secure* if $\mathsf{Adv}_D^{KDF}(\lambda) = max_{\mathcal{A}}\{\mathsf{Adv}_{\mathcal{A},D}^{KDF}(\lambda)\}$ is negligible for any adversary $\mathcal{A}$.

2.4 Receiver-Bounded Online/Offline Identity-Based Encryption

A receiver-bounded online/offline identity-based encryption (RB-OOIBE) scheme consists of the following algorithms:

- **Setup**(1^λ): on input the security parameter 1^λ, output the public key $param$ and master secret key MK.
- **KeyGen**$(param, MK, id)$: on input the public parameter $param$, the master secret key MK and an identity id, output the secret key sk_{id}.
- **Off-Encrypt**$(param, st)$: on input the public parameter $param$ and a state table st, output the updated state table st.
- **On-Encrypt**$(param, id, m, st)$: on input the public parameter $param$, an identity id, a message m and a state table st, output the ciphertext C and the (updated) state table st, or '$\perp$'.
- **Decrypt**$(param, sk_{id}, C)$: on input the public parameter $param$, the secret key sk_{id}, a ciphertext C, output the plaintext m or '$\perp$'.

Note that the offline encryption should be performed by powerful devices in the offline phase. In the online phase, one can arbitrarily choose a pre-computed offline ciphertext from the state table and employ it in the online encryption. One offline ciphertext can be dedicated to one recipient only. The encrypter should maintain the state table for recording the usage of offline ciphertexts.

Now we define the CCA security for RB-OOIBE.

Definition 2. The chosen-ciphertext security of an RB-OOIBE scheme is defined by the following game with security parameter λ between an adversary $\mathcal{A}$ and a challenger.

1. Setup. Perform **Setup**(1^λ) to get $(param, MK)$ and give $param$ to $\mathcal{A}$.
2. Query phase 1. $\mathcal{A}$ may issue queries to the following oracles.
   (a) EXTRACT(id): return $sk_{id} \leftarrow$ **KeyGen**$(param, MK, id)$.
   (b) ENCRYPT(id, m): return the ciphertext C where $(C, st) \leftarrow$ **On-Encrypt**$(param, id, m, st)$, $st \leftarrow$ **Off-Encrypt**$(param, st)$ and st is the initially empty state table.
   (c) DECRYPT(id, C): return $m \leftarrow$ **Decrypt**$(param, sk_{id}, C)$, where $sk_{id} \leftarrow$ **KeyGen**$(param, MK, id)$.
3. Challenge. $\mathcal{A}$ presents (m_0, m_1). Return the challenge ciphertext C^* to $\mathcal{A}$ where

   $$(C^*, st) \leftarrow \textbf{On-Encrypt}(param, id, m_\beta, st), \beta \in_R \{0,1\}$$

   and $st \leftarrow$ **Off-Encrypt**$(param, st)$.
4. Query phase 2. $\mathcal{A}$ continues making queries as in Query phase 1, except that $\mathcal{A}$ can't issue C^* to the decryption oracle.
5. Guess. $\mathcal{A}$ outputs the guess $\beta' \in \{0,1\}$. We say $\mathcal{A}$ wins the game if $\beta' = \beta$.

The advantage of $\mathcal{A}$ for a scheme Π is defined as $\mathsf{Adv}_{\mathcal{A},\Pi}^{CCA}(\lambda) = |\Pr[\beta' = \beta] - \frac{1}{2}|$. An RB-OOIBE scheme is IND-ID-CCA-secure if $\mathsf{Adv}_{\Pi}^{CCA}(\lambda) = max_{\mathcal{A}}\{\mathsf{Adv}_{\mathcal{A},\Pi}^{CCA}(\lambda)\}$ is negligible for any adversary $\mathcal{A}$.

We also define a weaker model: selective-ID CCA security (IND-sID-CCA). The selective-ID security is defined in the same way as full CCA security except that $\mathcal{A}$ has to decide which id it wants to attack in the beginning of the game. As described before, the selective-ID is not so weak in case only hundreds of identities are used.

Note that our construction and all previous OOIBE schemes have to trust the offline ciphertext generator. That is, the ciphertexts sent by the sensor nodes can be always decrypted by the owner of them.

3. CONSTRUCTION

We introduce our main scheme Π in this section. The scheme is based on Boneh and Boyen's IBE [3].

- **Setup**(1^λ). Randomly generate a prime p, two groups $\mathbb{G}, \mathbb{G}_T$ of order p, a bilinear map e and generators $g, g_2, h_1, h_2 \in \mathbb{G}$. Compute $g_1 = g^\alpha$ where $\alpha \in_R \mathbb{Z}_p$. Choose a key derivation function $D : \mathbb{G}_T \to \{0,1\}^k$, where k is the block size of a symmetric key encryption SE=(SEnc,SDec), and a hash function $H : \{0,1\}^* \to \mathbb{Z}_p$. Output the public parameter and master secret key:

  $$param = (g, g_1, g_2, h_1, h_2, H, D), \quad MK = \alpha.$$

- **KeyGen**$(param, MK, id)$. Pick a random value $r \in \mathbb{Z}_p$. Compute the secret key for id as

  $$sk_{id} = (g_2^\alpha (g_1^{id} h_1)^r, g^r).$$

- **Off-Encrypt**$(param, st)$. Randomly choose $s, \hat{a}, \hat{b}, \hat{c} \in_R \mathbb{Z}_p$ and compute

  $$(c_1, c_2, c_3, c_4, c_5) = (e(g_1, g_2)^s, g^s, (g_1^{\hat{a}} h_1)^s, (g_1^{\hat{b}} h_2)^s, g_1^{\hat{c}s})$$

  and $K = D(c_1)$. Let $C' = (K, c_2, c_3, c_4, c_5, \hat{a}, \hat{b}, \hat{c}^{-1})$ be an offline ciphertext. Append $(*, C')$ to st.

- **On-Encrypt**$(param, id, m, st)$. Get C' from the entry $(id, C') \in st$. If there exists no such C', randomly pick an entry $(*, C')$ from st and replace it with (id, C'). If there is no free entry $(*, C')$ on st, return '$\perp$'. Let $C' = (K, c_2, c_3, c_4, c_5, \hat{a}, \hat{b}, \hat{c}^{-1})$. Compute

  $$\tilde{c}_1 = SEnc_K(m), \quad t_1 = \hat{c}^{-1}(id - \hat{a}) \quad \text{and} \quad t_2 = \hat{c}^{-1}(\sigma - \hat{b}),$$

  where $\sigma = H(c_2, c_3, c_4, c_5, t_1)$. Output the final ciphertext

  $$\begin{aligned} C &= (\tilde{c}_1, c_2, c_3, c_4, c_5, t_1, t_2) \\ &= (SEnc_K(m), g^s, (g_1^{\hat{a}} h_1)^s, (g_1^{\hat{b}} h_2)^s, g_1^{\hat{c}s}, \\ &\quad \hat{c}^{-1}(id - \hat{a}), \hat{c}^{-1}(\sigma - \hat{b})) \end{aligned}$$

  and the updated state table st.

- **Decrypt**$(Param, sk_{id}, C)$. Let $C = (\tilde{c}_1, c_2, c_3, c_4, c_5, t_1, t_2)$ and $sk_{id} = (d_1, d_2)$. Compute $\sigma = H(c_2, c_3, c_4, c_5, t_1)$. Check that

  $$e(c_4 c_5^{t_2}, g) \overset{?}{=} e(c_2, g_1^{\sigma} h_2).$$

  If the equation holds, output '$\perp$'. Otherwise, compute

  $$c_1 = e(c_2, d_1)/e(c_3 c_5^{t_1}, d_2) \quad \text{and} \quad K = D(c_1).$$

  Output the message

  $$m = SDec_K(\tilde{c}_1).$$

3.1 Security

We prove that the scheme is IND-sID-CCA secure.

Theorem 1. Our scheme Π is IND-sID-CCA-secure assuming the decision BDH assumption holds in $\mathbb{G}$, the symmetric encryption scheme SE=(SEnc,SDec) with block size k is IND-CCA secure, the hash function H is collision-resistant and the key derivation function $D : \mathbb{G}_T \to \{0,1\}^k$ is secure. More precisely, we have

$$\begin{aligned} \mathsf{Adv}_{\Pi_2}^{CCA}(\lambda) \le \mathsf{Adv}_{\mathbb{G}}^{DDH}(\lambda) + \mathsf{Adv}_{\mathsf{SE}}^{CCA}(\lambda) + \mathsf{Adv}_{D}^{KDF}(\lambda) \\ + \mathsf{Adv}_{H}^{COL}(\lambda) + \frac{q_D}{p} \end{aligned}$$

where λ is the security parameter and q_D is the maximum number of queries to the decryption oracle.

PROOF. Suppose there is an adversary $\mathcal{A}$ breaking Π with non-negligible advantage. Given a random decision BDH instance (g, g^a, g^b, g^c, Z), where Z is either $e(g, g)^{abc}$ or a random element of $\mathbb{G}_T$, we construct another algorithm $\mathcal{B}$ breaking the decision BDH as follows.

- **Init.** $\mathcal{A}$ chooses an identity $id^* \in \mathbb{Z}_p$ that it intends to attack.

- **Setup.** $\mathcal{B}$ sets $g_1 = g^a$, $g_2 = g^b$ and $g_3 = g^c$ and chooses a hash function $H : \{0,1\}^* \to \mathbb{Z}_p$ and a key derivation function $D : \mathbb{G}_T \to \{0,1\}^k$. It then picks random values $\lambda_1, \lambda_2 \in \mathbb{Z}_p$ and defines $h_1 = g_1^{-id^*} g^{\lambda_1}$ and $h_2 = g_1^{-\sigma^*} g^{\lambda_2}$, where $\sigma^* = H(g_3, g_3^{\lambda_1} g^{-k_{1,id^*} k_{3,id^*}}, g_3^{\lambda_2} g^{-k_{2,id^*} k_{3,id^*}}, g^{k_{3,id^*}}, k_{1,id^*})$ and $k_{1,id^*}, k_{2,id^*}, k_{3,id^*} \in_R \mathbb{Z}_p$. The parameter $(g, g_1, g_2, h_1, h_2, H, D)$ is then sent to $\mathcal{A}$. Since g, g_1, g_2 are randomly chosen, and h_1, h_2 are uniformly random, the distribution of the parameter is identical to that in the actual construction.

- **Query Phase 1.** $\mathcal{B}$ answers the following queries.

  1. Extract(id): for any $id \neq id^*$, $\mathcal{B}$ chooses a random value $r \in \mathbb{Z}_p$ and sets the private key for id as

     $$sk_{id} = (d_1, d_2) = (g_2^{\frac{-\lambda_1}{id - id^*}} (g_1^{id} h_1)^r, g_2^{\frac{-1}{id - id^*}} g^r).$$

     Let $\tilde{r} = r - b/(id - id^*)$, we can see that

     $$d_1 = g_2^{\frac{-\lambda_1}{id - id^*}} (g_1^{id} h_1)^r = g_2^{\frac{-\lambda_1}{id - id^*}} (g_1^{id - id^*} g^{\lambda_1})^r$$

     $$= g_2^a (g_1^{id - id^*} g^{\lambda_1})^{r - \frac{b}{id - id^*}} = g_2^a (g_1^{id} h_1)^{\tilde{r}};$$

     $$d_2 = g_2^{\frac{-1}{id - id^*}} g^r = g^{r - \frac{b}{id - id^*}} = g^{\tilde{r}}.$$

     Since $\tilde{r}$ is uniform in $\mathbb{Z}_p$, the key is correctly distributed.

  2. Encrypt(id, m): for $id \neq id^*$, $\mathcal{B}$ chooses a fixed random value s for id, and computes the ciphertext as in the actual construction. For $id = id^*$, $\mathcal{B}$ computes the ciphertext as

     $$\tilde{c}_1 = SEnc_K(m), \quad c_2 = g_3, \quad c_3 = g_3^{\lambda_1} g^{-k_{1,id^*} k_{3,id^*}},$$

     $$c_4 = g_3^{\lambda_2} g^{-k_{2,id^*} k_{3,id^*}}, \quad c_5 = g^{k_{3,id^*}},$$

     $$t_1 = k_{1,id^*}, \quad t_2 = k_{2,id^*},$$

     where $k_{1,id^*}, k_{2,id^*}, k_{3,id^*}$ are chosen in **Setup** phase and $K = D(Z)$. We can see that if $Z = e(g, g)^{abc} = e(g_1, g_2)^c$, this is a valid encryption of m.

  3. Decrypt(id, C): let $C = (\tilde{c}_1, c_2, c_3, c_4, c_5, t_1, t_2)$. $\mathcal{B}$ first checks the validity of C as in the actual construction. If C doesn't pass the equation, $\mathcal{B}$ responses '$\perp$'. Otherwise, for $id \neq id^*$, $\mathcal{B}$ generates id's secret key as in Extract oracle, and then decrypts C. For $id = id^*$, $\mathcal{B}$ first computes $\sigma = H(c_2, c_3, c_4, c_5, t_1)$. Consider the following case:

     - $\sigma \neq \sigma^*$: $\mathcal{B}$ computes the private key for (id, σ) as

       $$\begin{aligned} &(d_1, d_2, d_3) \\ = \;& (g_2^{\frac{-\lambda_2}{\sigma - \sigma^*}} g^{\lambda_1 r_1} (g_1^{\sigma - \sigma^*} g^{\lambda_2})^{r_2}, g^{r_1}, g_2^{\frac{-1}{\sigma - \sigma^*}} g^{r_2}), \end{aligned}$$

       where $r_1, r_2 \in_R \mathbb{Z}_p$. We can see that when $\tilde{r}_2 = r_2 - b/(\sigma - \sigma^*)$, the private key is of the form:

       $$\begin{aligned} d_1 &= g_2^{\frac{-\lambda_2}{\sigma - \sigma^*}} g^{\lambda_1 r_1} (g_1^{\sigma - \sigma^*} g^{\lambda_2})^{r_2} \\ &= g_2^a g^{\lambda_1 r_1} (g_1^{\sigma - \sigma^*} g^{\lambda_2})^{r_2 - \frac{b}{\sigma - \sigma^*}} \\ &= g_2^a (g_1^{id} h_1)^{r_1} (g_1^{\sigma} h_2)^{\tilde{r}_2}, \\ d_2 &= g^{r_1}, d_3 = g^{\tilde{r}_2} \end{aligned}$$

       which is valid. Then $\mathcal{B}$ computes

       $$c_1 = e(c_2, d_1)/(e(c_3 c_5^{t_1}, d_2) e(c_4 c_5^{t_2}, d_3))$$

       and

       $$K = D(c_1),$$

       and outputs the message $m = SDec_K(\tilde{c}_1)$.

  - $\sigma = \sigma^*$: $\mathcal{B}$ computes $K = D(Z)$ and outputs the message $m = SDec_K(\tilde{c}_1)$. We can see that if $Z = e(g,g)^{abc} = e(g_1, g_2)^c$, m is correctly decrypted.

- **Challenge.** $\mathcal{A}$ outputs two messages m_0 and m_1. $\mathcal{B}$ randomly chooses a bit β and encrypts m_β under id^* as in Encrypt oracle.

- **Query Phase 2.** $\mathcal{A}$ makes key extraction, encryption and decryption queries, and $\mathcal{B}$ responds as in Query Phase 1.

- **Guess.** $\mathcal{A}$ outputs its guess β'. If $\beta' = \beta$, $\mathcal{B}$ outputs 0; otherwise, $\mathcal{B}$ outputs 1.

Analysis. Now we analyze the advantage of $\mathcal{B}$ in the above game. If $Z = e(g,g)^{abc}$, we have

$$\Pr[\mathcal{B}(1^\lambda, g, g^a, g^b, g^c, e(g,g)^{abc}) = 1] = \Pr[\beta' = \beta]. \quad (1)$$

We can see that all values responded by $\mathcal{B}$ for Extract and Encrypt queries have identical distribution to that in the actual construction. For Decrypt queries, if $id \neq id^*$, $\mathcal{B}$ just answers as in the actual construction. If $id = id^*$ but $\sigma \neq \sigma^*$, we have showed that the decryption key is in the right form and thus $\mathcal{B}$'s responses have right distribution. If $id = id^*$ and $\sigma = \sigma^*$, it means that $(c_2, c_3, c_4, c_5, t_1)$ is given by $\mathcal{B}$ except a negligible probability. So $K = D(Z) = D(e(g,g)^{abc}) = D(e(g_1, g_2)^c)$ is the correct key for $\tilde{c}_1$. $\mathcal{B}$ successfully simulates the game. Equation (1) holds.

Then we consider the case for $Z = R \in_R \mathbb{G}_T$. We have

$$\begin{array}{l}\Pr[\mathcal{B}(1^\lambda, g, g^a, g^b, g^c, R) = 1] \leq \\ \frac{1}{2} + \mathsf{Adv}_{\mathsf{SE}}^{CCA}(\lambda) + \mathsf{Adv}_{D}^{KDF}(\lambda) + \mathsf{Adv}_{H}^{COL}(\lambda) + \frac{q_D}{p}.\end{array} \quad (2)$$

We first define RejInv as an event that the decryption oracle rejects all invalid ciphertexts. The following equation holds.

$$\Pr[\beta' = \beta|\mathsf{RejInv}] \leq \frac{1}{2} + \mathsf{Adv}_{\mathsf{SE}}^{CCA}(\lambda) + \mathsf{Adv}_{D}^{KDF}(\lambda). \quad (3)$$

We can see that if the decryption oracle rejects all invalid ciphertexts, the distribution of β is independent from $\mathcal{A}$'s view under the assumption that SE is CCA-secure and D is KDF-secure. Moreover, we have the following equation.

$$\Pr[\neg\mathsf{RejInv}] \leq \mathsf{Adv}_{H}^{COL}(\lambda) + \frac{q_D}{p}. \quad (4)$$

If an invalid ciphertext $C = (\tilde{c}_1, c_2, c_3, c_4, c_5, t_1, t_2)$ passes the checking equation in **Decrypt**, $\mathcal{A}$ either

- finds collisions of H, or

- adjusts one of the values c_2, c_4, c_5 and t_1 so that the equation holds.

The probability that the former happens is bounded by the collision-resistent hash function H, where the probability that the latter happens is $1/p$. Considering that there are q_D decryption queries, Equation (4) holds.

Now from (3) and (4), we get Equation (2):

$$\begin{array}{rl} & \Pr[\beta' = \beta] \\ = & \Pr[\beta' = \beta|\mathsf{RejInv}] \Pr[\mathsf{RejInv}] \\ & + \Pr[\beta' = \beta|\neg\mathsf{RejInv}] \Pr[\neg\mathsf{RejInv}] \\ \leq & \Pr[\beta' = \beta|\mathsf{RejInv}] + \Pr[\neg\mathsf{RejInv}] \\ \leq & \frac{1}{2} + \mathsf{Adv}_{\mathsf{SE}}^{CCA}(\lambda) + \mathsf{Adv}_{D}^{KDF}(\lambda) + \mathsf{Adv}_{H}^{COL}(\lambda) + \frac{q_D}{p} \end{array}$$

Then by subtracting (1) from (2), we get the bound in the theorem statement. □

4. PERFORMANCE COMPARISON

There are only 3 existing online/offline IBE schemes, two of them are proposed by Guo, Mu and Chen in [9] and one of them is proposed by Liu and Zhou [12]. We use GMC-1, GMC-2 and LZ to denote them respectively. We also assume that $|\mathbb{G}| = 160$ bits, $|q| = 160$ bits, $|\mathbb{G}_T| = 1024$ bits and message space is 128 bits for the following comparison. Assume AES is used for the symmetric key encryption, where both the key size and ciphertext size are 128 bits. In order to make it CCA secure, we use another MAC function which adds further 80 bits to the ciphertext. For the online/offline signature scheme used in GMC-1, we adopt Boneh and Boyen's [4] construction which requires 320-bit offline, 320-bit online signatures and 320-bit public/private keys (by assuming some group elements can be shared between different keys).

Table 1 shows the comparison between our scheme and other OOIBE schemes, in the case of encrypting one single message. The differences can be summarized as follow:

1. When compared to the scheme in the full security model (GMC-2), both the offline storage and ciphertext size of our scheme are 4 times smaller than GMC-2. Again, as described before, selective-ID security is not really weak in our scenario.

2. When compared to the scheme in selective-ID model (GMC-1), both the offline storage and ciphertext size of our scheme are 2 times smaller than GMC-1. Even if we compare to the random oracle scheme (LZ), our scheme still achieves a smaller offline storage (2 times smaller).

3. In terms of computation requirement, we do not require any point addition operation (M operation) in the online encryption stage for both schemes. Modular computation (m_c operation) and symmetric key encryption (SE operation) are much faster than M operation. Thus the online encryption stages of our scheme is faster than GMC-1 and GMC-2.

4. We also note that schemes in the random oracle are usually more efficient than those in the standard model, due to the weaken security level. However, our scheme achieves similar or even outstanding performance over the random oracle scheme (LZ).

Figure 1 shows another comparison on offline storage. In this case, there are a number of messages to be sent to one receiver. It is very common in WSN for a sensor to send multiple messages to a base station. Since the offline computation and offline storage are independent of the number of

	GMC-1	GMC-2	LZ	Ours
Offline computation	$6E + 2ME$	$4E + 2ME$	$4E + 1ME$	$3E + 2ME$
Online computation	$1M + 2m_c$	$1M + 2m_c$	$3m_c$	$2m_c + SE$
Offline storage (bits)	2944	5056	2624	1248
Ciphertext length (bits)	2784	4736	1248	1168
Number of pairing for decryption	7	2	2	4
Security model	selective-ID	full	random oracle	selective-ID

Table 1: Comparison of computation cost and size for encrypting one message. E: point multiplication in $\mathbb{G}$ or exponentiation in $\mathbb{G}_T$; ME: multi-point multiplication in $\mathbb{G}$ (which costs about 1.3 times more than a single point multiplication); M: multiplication in $\mathbb{G}_T$; m_c: modular computation in $\mathbb{Z}_p$; and SE: the symmetric key encryption.

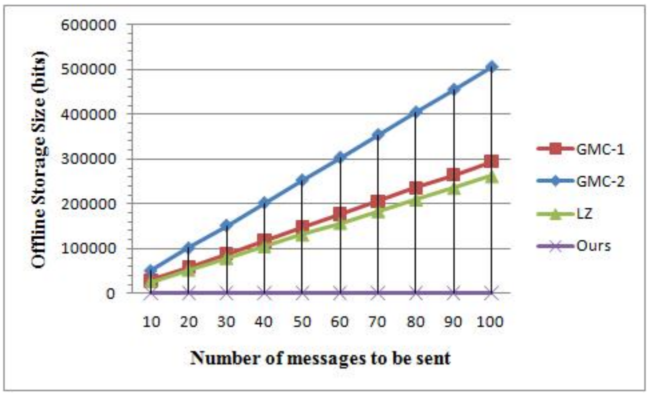

Figure 1: Offline storage size for different numbers of messages to be sent

messages to be encrypted in our schemes, the efficiency gain can be magnified when more messages will be sent, say, 100 messages. So when the number of receivers is limited, our schemes can achieve much better performance when compared to previous OOIBE schemes.

Again, even for encrypting one message, our scheme is more efficient than all OOIBE schemes in the literature. Therefore using RB-OOIBE to encrypt messages directly is better than using OOIBE schemes to encrypt a symmetric key and then using this symmetric key to encrypt messages.

5. CONCLUSION

In this paper, we have proposed a new notion called Receiver-Bounded Online/Offline ID-based Encryption. We also presented a concrete RB-OOIBE construction. The efficiency improvements of our scheme over previous schemes are very clear, especially in the case that many messages are encrypted for one receiver. In general, a wireless sensor node has three main limitations: energy, computation power and storage. For energy saving, our scheme provides the shortest ciphertext length compared to other OOIBE schemes. By the online/offline property, the sensor node doesn't need any heavy computation for encryption. Most importantly, RB-OOIBE saves lots of space required for offline ciphertexts. This makes our scheme really practical for wireless sensor nodes.

6. REFERENCES

[1] Joonsang Baek, Han Chiang Tan, Jianying Zhou, and Jun Wen Wong. Realizing Stateful Public Key Encryption in Wireless Sensor Network. In *Proceedings of The IFIP TC-11 23rd International Information Security Conference (SEC '08)*, pages 95–107. Springer, 2008.

[2] Mihir Bellare, Tadayoshi Kohno, and Victor Shoup. Stateful Public-key Cryptosystems: How to Encrypt with One 160-bit Exponentiation. In *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pages 380–389. ACM, 2006.

[3] Dan Boneh and Xavier Boyen. Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In *Proceedings of Advances in Cryptology - EUROCRYPT '04*, volume 3027 of *LNCS*, pages 223–238. Springer, 2004.

[4] Dan Boneh and Xavier Boyen. Short Signatures Without Random Oracles the SDH Assumption in Bilinear Groups. *Journal of Cryptology*, 21(2):149–177, 2008.

[5] Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. In *Proceedings of Advances in Cryptology - CRYPTO '01*, volume 2139 of *LNCS*, pages 213–229. Springer, 2001.

[6] Xiaofeng Chen, Fangguo Zhang, Willy Susilo, and Yi Mu. Efficient generic on-line/off-line signatures without key exposure. In *Proceedings of Applied Cryptography and Network Security 2007 (ACNS '07)*, volume 4521 of *LNCS*, pages 18–30. Springer, 2007.

[7] Cheng-Kang Chu, Joseph K. Liu, Jianying Zhou, Feng Bao, and Robert H. Deng. Practical ID-based Encryption for Wireless Sensor Network. To appear in ASIACCS '10, 2010.

[8] Shimon Even, Oded Goldreich, and Silvio Micali. On-line/off-line digital schemes. In *Proceedings of*

Advances in Cryptology - CRYPTO '89, volume 435 of *LNCS*, pages 263–275. Springer, 1989.

[9] Fuchun Guo, Yi Mu, and Zhide Chen. Identity-based online/offline encryption. In *Proceedings of Financial Cryptography and Data Security (FC '08)*, volume 5143 of *LNCS*, pages 247–261. Springer, 2008.

[10] Marc Joye. An efficient on-line/off-line signature scheme without random oracles. In *Proceedings of 7th International conference on Cryptology and Network Security (CANS '08)*, volume 5339 of *LNCS*, pages 98–107. Springer, 2008.

[11] Kaoru Kurosawa and Katja Schmidt-Samoa. New online/offline signature schemes without random oracles. In *Proceedings of the Public Key Cryptography (PKC '06)*, volume 3958 of *LNCS*, pages 330–346. Springer, 2006.

[12] Joseph K. Liu and Jianying Zhou. An efficient identity-based online/offline encryption scheme. In *Proceedings of Applied Cryptography and Network Security 2009 (ACNS '09)*, volume 5536 of *LNCS*, pages 156–167. Springer, 2009.

[13] Le Trieu Phong, Hiroto Matsuoka, and Wakaha Ogata. Stateful identity-based encryption scheme: faster encryption and decryption. In *Proceedings of the ACM Symposium on Information, Computer & Communication Security (ASIACCS '08)*, pages 381–388. ACM, 2008.

[14] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Proceedings of Advances in Cryptology - CRYPTO '84*, volume 196 of *LNCS*, pages 47–53. Springer, 1984.

[15] Adi Shamir and Yael Tauman. Improved online/offline signature schemes. In *Proceedings of Advances in Cryptology - CRYPTO '01*, volume 2139 of *LNCS*, pages 355–367. Springer, 2001.