View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Directory of Open Access Journals

Sensors & Transducers, Vol. 157, Issue 10, October 2013, pp. 121-128

Sensors & Transducers

© 2013 by IFSA

http://www.sensorsportal.com

# An Efficient Multi-PKG Online/Offline Identity-Based Encryption Scheme for Wireless Sensor Network

**[1] Jianting NING, [2] Xinchun YIN, [1] Yebin XU**

[1] Department of Computer Science and Engineering, Yangzhou University, Yangzhou 225127, Jiangsu Province, P. R. China

[2] State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, Jiangsu Province, P. R. China

E-mail: jelly408385909@163.com, xybyzu@163.com

*Received: 11 July 2013 /Accepted: 25 September 2013 /Published: 31 October 2013*

**Abstract:** In this paper, we divide large-scale resource-constrained WSN nodes into several domains, split cryptographic operations into heavy operations and the fast lightweight operations, and present an efficient multi-PKG online/offline identity-based encryption scheme for multi-domain WSN. Most heavy computations such as pairing or exponentiation are done in the offline phase for pre-computation without the receiver's identity or the knowledge of the plaintext. Most fast lightweight operations are done in the online phase, together with the plaintext and the receiver's identity. The online encryption is extremely efficient and easy to be implemented on sensor node. We prove the security of our new scheme in the random oracle model. Compared with the existing schemes, our new scheme is more secure and efficient, which is suitable for multi-domain WSN. C*opyright © 2013 IFSA.*

**Keywords:** Identity-based encryption, Multi-PKG, Online/offline, Random oracle model, Wireless Sensor Network (WSN).

## 1. Introduction

Recently, as one of the core technologies of the Internet of things, wireless sensor network (WSN) is attracting more and more research interests because of its wide applications such as military operations, scientific explorations and so on. WSN are composed of a large number of low-power, low-cost, and multi-functional sensor nodes that communicate at short distances through wireless links. For distributed in the open environment which is exposed to the adversary, sensor nodes face different types of malicious attacks, such as communication monitor, sybil attack, wormhole attacks, sinkhole attacks and so on. To provide security, communication among nodes should be encrypted and authenticated. As traditional encryption scheme can not satisfy the security requirements of WSN due to the limited energy and weak computation capability of sensor nodes, it is extremely urgent to design efficient and applicable encryption scheme for WSN.

The current solution to the problem of establishing security in WSN premises is around symmetric cryptosystems, and a couple of symmetric-key based solutions have been proposed during the past few years. Eschenauer and Gligor [1] proposed a basic random key pre-distribution scheme (Random Key Pre-distribution, RKP). Based on the Eschenauer-Gligor scheme, Chan etc. [2] proposed a q-composite scheme based on the basic random key pre-distribution model. Perrig etc. [3] presented a suite of security building blocks SPINS optimized for resource constrained environments and wireless

communication. SPINS have two secure building blocks: SNEP and μTESLA. Later on, a series of schemes were proposed to provide efficient broadcast authentication mechanisms for WSN based on SPINS [4-8]. Lee etc. [9] studied three aspects of WSN security encryption algorithms modes of operation for block ciphers and message authentication algorithms. Claude etc. [10] proposed a simple and provably secure encryption scheme that allows efficient additive aggregation of encrypted data. Only one modular addition was necessary for ciphertext aggregation. Yang etc. [11] analyzed a chaos block cipher for wireless sensor network, and found that there is a fatal flaw in its security because the number of rounds was too small and the calculation precision of round function was too short. Guo etc. [12] proposed a novel chaotic map based block cryptosystem.

However, due to the limitation on memory and energy, these techniques are not able to achieve a perfect connectivity, scalability and resilience for large-scale sensor networks. The use of Public Key Cryptography (PKC) would eliminate the above problem. Employing PKC for WSN provides simple solutions, good scalability and strong security resilience, when compared to symmetric-key based solutions. Because of its asymmetry property, sensors do not need to preload the pre-distributed keys. Any two sensors can establish a secure channel between themselves, thus the capture of some sensors will not affect the security of others.

Identity-based Cryptography, first introduced by Shamir [13], eliminates the need for checking the validity of certificates in traditional public key infrastructure (PKI). In an identity-based cryptography, 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, and etc.). Using its master key, the private key generator (PKG) then computes a private key for each user. This property avoids the requirement of using digital certificates, which eliminates the costly certificate verification process and the storage of the lengthy certificate, is particularly suitable for WSN. Boneh etc. [14-16] introduced efficient identity-based encryption scheme and generic signature scheme, and proved their safety in the random oracle model and selective-ID model. Waters [17] proposed an efficient identity-based encryption without random oracles. Gentry' IBE [18] showed an improvement over Waters' IBE scheme [17] without random oracles in terms of the size of public master parameters and security reduction.

The notion of online/offline digital signature was introduced by Even, Goldreich and Micali [19, 20]. With this notion, a signing process can be divided into two phases, the first phase is performed offline (before the message to be signed is given) and the second phase is performed online (after knowing the message). The online phase is typically very fast. Online/offline encryptions are particularly useful for low-power devices such as WSN. In parallel to online/offline signature, Guo etc. [21] first proposed an online/offline encryption by expanding the IBE of Boneh and Boyen [15] and Gentry [18]. Joseph K. Liu etc. [22] proposed an identity based online/offline encryption scheme which proved to be chosen ciphertext (CCA) secure in the random oracle model.

In this paper, we focus on the large-scale resource-constrained WSN, divide WSN nodes into several domains and present an efficient multi-PKG online/offline identity-based encryption scheme, which is suitable for multi-domain WSN.

The rest of this paper is organized as follows. The preliminaries including bilinear pairing and intractability assumption are introduced in Section 2. In Section 3, we describe the formal model of multi-PKG online/offline identity-based encryption. And in Section 4, we introduce the proposed multi-PKG online/offline identity-based encryption scheme. Section 5 gives the security analysis and the proof of confidentiality of the new scheme. Finally, Section 6 concludes the paper.

## 2. Preliminaries

### 2.1. Bilinear Pairing

We briefly describe the basic definition and properties of the bilinear pairings. Let $G_1$ be an additive cyclic group generated by $P$, with prime order $q$, and $G_2$ be a multiplicative cyclic group of the same order $q$, $q$ is a big prime number. Let $e$ be a bilinear map such that $e: G_1 \times G_1 \to G_2$ with the following properties:

1. Bilinearity: For all $U, V \in G$ and $a, b \in Z$, $e(aU, bV) = e(U, V)^{ab}$.

2. Non-degeneracy: $e(P, P) \neq 1$.

3. Computability: It is efficient to compute $e(U, V)$ for all $U, V \in G$.

### 2.2. Intractability Assumption

**Definition 1 *k*-Computation Diffie-Hellman Inverse Assumption (*k-CDHI*)**. The *k*-Computation Diffie-Hellman Inverse problem (*k-CDHIP*) is defined as follow: Given an additive group $G_1$ and a multiplicative group $G_2$, all with prime order $q$ and (*k* + *1*) tuples $(G, sG, s^2G, ..., s^kG)$, computing $(1/s)P$ is the *k*-Computation Diffie-Hellman Inverse problem. We say that the $(t, \varepsilon, k)$ -*CDHI* assumption holds in $(G_1, G_2)$ if no t-time algorithm has advantage at least $\varepsilon$ in solving the *k-CDHI* problem in $(G_1, G_2)$.

**Definition 2** ***k*-Bilinear Diffie-Hellman Inversion Assumption (*k-BDHI*)**. The k-Bilinear Diffie-Hellman Inversion Problem (*k-BDHIP*) is defined as follow: Given an additive group $G_1$ and a multiplicative group $G_2$, all with prime order $q$ and ($k$ + *1*) tuples $(G, sG, s^2G, ..., s^kG)$, computing $e(G,G)^{1/s} \in G_2$ is the k-Bilinear Diffie-Hellman Inversion problem. We say that the $(t, \varepsilon, k)$ *-BDHI* assumption holds in $(G_1, G_2)$ if no *t*-time algorithm has advantage at least $\varepsilon$ in solving the *k-BDHI* problem in $(G_1, G_2)$.

**Definition 3** ***k*-Bilinear Modified Diffie-Hellman Inversion Assumption (*k-BMDHI*)**. The *k*-Bilinear Modified Diffie-Hellman Inversion Problem (*k-BMDHIP*) is defined as follow: Given an additive group $G_1$ and a multiplicative group $G_2$, all with prime order $q$, $(P, yP, (x_1 + y)^{-1}P, ..., (x_k + y)^{-1}P) \in G_1^{k+2}$ for unknown $y \in Z_q^*$ and known $x_1, ...x_k \in Z_q^*$, computing $e(P,P)^{(y+x')^{-1}}$ for some $x' \notin \{x_1, ...x_k\}$ is the *k*-Bilinear Modified Diffie-Hellman Inversion problem. We say that the $(t, \varepsilon, k)$ *-BMDHI* assumption holds in $(G_1, G_2)$ if no *t*-time algorithm has advantage at least $\varepsilon$ in solving the *k-BMDHI* problem in $(G_1, G_2)$.

## 3. Formal Model of Multi-PKG Online/Offline Identity-Based Encryption

### 3.1. Bilinear Pairing

A generic multi-PKG online/offline identity-based encryption scheme consists of the following six algorithms.

**G-Setup** ($1^k$) → (*params*)**:** Given a security parameter $k$, the global trusted party generates global public parameters *params*.

**D-Setup** (*params*) → ($P_x$, $s_x$)**:** Given the global public parameters *params*, each domain $PKG_x (x = 1,2,..., d)$ outputs a corresponding public key $P_x$ and a master private key $s_x$ (we suppose that there are $d$ domains). $P_x$ is made public while $s_x$ is kept secret by the $PKG$.

**Extract** ($1^k$, *params*, $s_x$, $ID$) → $D_{ID}$**:** Given an identity $ID$ in domain $PKG_x$, the $PKG_x$ executes this algorithm to generate the private key $D_{ID}$ corresponding to $ID$ and transmits $D_{ID}$ to the user with identity $ID$ via secure channel.

**Offline-Encrypt** ($1^k$, *params*) → $\phi$**:** To generate the offline share of the encryption, this algorithm is executed without the knowledge of message to be encrypted and the receiver of the encryption. The offline ciphertext is represented as $\phi$.

**Online-Encrypt** ($1^k$, $m$, $ID_A$, $\phi$) → $\bar{\phi}$**:** For encrypting a message $m$ to user with identity $ID_A$, any sender can run this algorithm to generate the encryption $\bar{\phi}$ of message $m$. This algorithm uses a new offline ciphertext $\phi$ and generates the full encryption $\bar{\phi}$.

**Decrypt** ($1^k$, *params*, $\bar{\phi}$, $ID_A$, $D_A$) → $m / \perp$**:** For decryption of $\bar{\phi}$, the receiver $ID_A$ uses his private key $D_A$ and run this algorithm to get back the message $m$ or $\perp$ which indicates the failure of decryption.

### 3.2. Bilinear Pairing

**Definition 1**. An multi-PKG identity-based online/offline encryption scheme is said to be indistinguishable against adaptive chosen ciphertext attacks (*IND-MPIDOOE-CCA*) if no polynomially bounded adversary has a non-negligible advantage in the following game.

**Setup:** The challenger $C$ runs the **G-Setup** and **D-Setup** algorithms with a security parameter $k$ and sends the system parameters and public keys $P_x (x = 1,2,..., d)$ to the adversary $A$.

**Phase I:** The adversary $A$ performs a polynomially bounded number of queries. These queries may be adaptive, i.e. current query may depend on the answers to the previous queries.

– **Key extraction queries (Oracle $O_{Extract}(ID)$):** $A$ chooses an identity $ID$ in domain $PKG_x$. $C$ computes $D_{ID}$ =**Extract(** $ID$**)** and sends $D_{ID}$ to $A$.

– **Decryption queries (Oracle $O_{Decrypt}(\bar{\phi}, ID_A)$**): $A$ submits a ciphertext $\bar{\phi}$ and a receiver identity $ID$ to the oracle for the result of **Decrypt(** $ID_A$ **,** $D_A$ **)**. $C$ generates the private key $D_A$ and sends the result of **Decrypt(** $ID_A$ , $D_A$ **)**. The result is made of a message if the decryption is successful. Otherwise, a symbol $\perp$ is returned for rejection.

**Challenge:** $A$ produces two plaintexts $m_0, m_1$ and the receiver identity $ID_R$ which $A$ wishes to be challenged. $A$ should not have queried for the private key corresponding to $ID_R$ in **Phase I**. $C$ chooses a random bit $b \in \{0,1\}$ and computes $\bar{\phi}$ = **Online-Encrypt (** $m$ **,** $ID_R$ **, Offline-Encrypt ()).** $\bar{\phi}$ is sent to $A$.

**Phase II:** $A$ is now allowed to get training as in **Phase–I**. $A$ makes a number of new queries as in Phase I with the restriction that it cannot query the decryption oracle and the extraction oracle.

**Guess:** At the end of the game, $A$ produces a bit $b'$ and wins the game if $b' = b$.

$A$ 's advantage is defined as $Adv(A) = |\Pr[b' = b] - 1/2|$, where $\Pr[b' = b]$ denotes the probability that $b' = b$.

## 4. The Proposed Multi-PKG Online/Offline Identity-Based Encryption Scheme

In this section, we aim at the features of WSN with constrained resources, and propose a new multi-PKG online/offline identity-based encryption scheme.

### 4.1. Description of the Proposed Encryption Scheme

Our scheme consists of the following five algorithms.

**G-Setup:** Given a security parameter $k$, let $G_1$ be an additive cyclic group generated by $P$, with prime order $q > 2^k$, and $G_2$ be a multiplicative cyclic group of the same order $q > 2^k$. Define $e$ as in previous section, and let $g = e(P,P)$. Let $M$ denotes the message space and $n_M = |M|$. Let $H_1 : \{0,1\}^* \to Z_q^*$, $H_2 : \{0,1\}^* \times G_1 \times G_2 \times G_2 \times G_2 \times G_2 \to Z_q^*$, $H_3 : \{0,1\}^* \to \{0,1\}^{n_M}$ be three cryptographic hash functions. The system parameters are $params = (G_1, G_2, q, P, g, M, H_1, H_2, H_3)$.

**D-Setup:** Each $PKG_x (x = 1,2,...,d)$ chooses the private key $s_x \in Z_q^*$ and computes the corresponding public key $P_x = s_x P$.

**Extract (** $ID_x$ **):** Given an identity $ID_x$ in domain $PKG_x$, the $PKG_x$ computes $q_x = H_1(ID_x)$, $D_x = 1/(q_x + s)P$. We suppose that $PKG_a$ keeps the private key $s_a$ and public key $P_a = s_a P$. Alice registers with $PKG_a$ and gets her private key $D_a = 1/(q_a + s)P$, where $q_a = H_1(ID_a)$. $PKG_b$ keeps the private key $s_b$ and public key $P_b = s_b P$. Bob registers with $PKG_b$ and gets his private key $D_b = 1/(q_b + s)P$, where $q_b = H_1(ID_b)$.

To send a message $m$ to Bob, Alice does the follows as showed below.

**Offline-Encrypt (** $params$ **):** $PKG_a$ randomly generates $x \in Z_q^*$ and computes: $u_a = H_1(x \| s_a)$, $U_a = u_a P$, $R = g^x$, $a = H_3(R)$, $T_1 = (u_a + s_a)^{-1} P$, $T_2 = u_a x P$. Outputs the offline ciphertext $\phi = (u_a, x, U_a, R, a, T_1, T_2)$.

**Online-Encrypt (** $m$ **,** $ID_a$ **,** $\phi$ **):** To encrypt a message $m$ for Bob, at the Online-Encrypt stage, Alice receives the offline ciphertext $\phi$ and computes: $t_1 = (u_a + s_a)(q_B + u_a) \bmod q$, $t_2 = H_2(m, u_a, R, T_1, T_2, t_1)x + u_a \bmod q$, $c = a \oplus m$, and outputs the ciphertext $\bar{\phi} = (U_a, T_1, T_2, t_1, t_2, c)$.

**Offline-Decrypt (** $\bar{\phi}$ **):** At the Offline-Decrypt stage, $PKG_b$ receives the ciphertext $\bar{\phi}$ and computes $Q = e(t_2 T_1 - U_a, P_b + U_a)$, outputs the offline decryptext $\tau = (Q, \bar{\phi})$.

**Online-Decrypt (** $\tau$ , $D_B$ **):** Bob receives the offline decryptext $\tau$ and computes: $R = e(x(T_1 t_1 + P_b) - T_2, D_B)$, $h = H_2(m, u_a, R, T_1, T_2, t_1)$ and $R^h$, accept the message $m = c \oplus H_3(R)$ if and only if the following equation holds: $R^h = Q$.

### 4.2. Implementation on WSN

We apply the above scheme to WSN, and propose a new framework of WSN, composed of a Base Station (BS), a small number of PKGs and numerous sensor nodes (SNs), as showed in Fig. 1. WSN is divided into several domains, WSN nodes determine how forming domains based on their location information or other criteria. And PKG is responsible for the offline phase in its domain, while the online phase is to be executed in the WSN node.

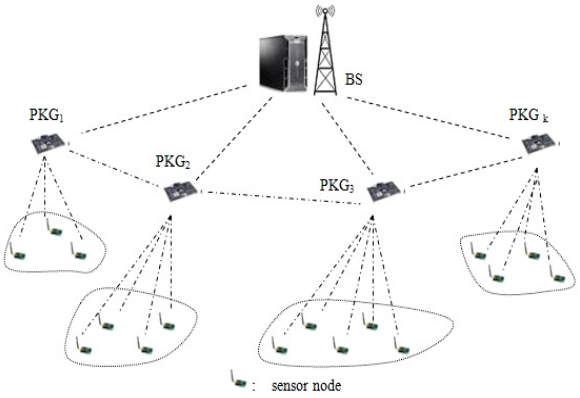


**Fig. 1.** The framework of WSN.

We assume that the system parameters $params$ are generated by the base station and are embedded in each sensor node when they are deployed. And the base station and PKGs are powerful enough to perform computationally intensive cryptographic operations, while the sensor nodes have limited resources in terms of memory, computation and battery power. We also assume that the private key of the base station is safely stored.

**G-Setup:** System randomly chooses a security parameter $k$, then the base station generates the system parameters are $params = (G_1, G_2, q, P, g, , M, H_1, H_2, H_3)$ as described in Section 4.

**D-Setup:** Each $PKG_x (x = 1,2,..., d)$ generates the private key $s_x \in Z_q^*$ and the corresponding public key $P_x = s_x P$.

We consider the communication between sensor node $SN_A$ from domain $A$ and sensor node $SN_B$ from domain $B$.

**Extract ($ID_x$):** $SN_A$ registers with $PKG_a$ and gets its private key $D_a = 1/(q_a + s)P$, where $q_a = H_1(ID_a)$. $SN_B$ registers with $PKG_b$ and gets its private key $D_b = 1/(q_b + s)P$, where $q_b = H_1(ID_b)$.

To send a message $m$ to $SN_B$, $SN_A$ does the follows as showed below.

**Offline-Encrypt ($params$):** $PKG_a$ randomly generates $x \in Z_q^*$ and computes: $u_a = H_1(x \| s_a)$, $U_a = u_a P$, $R = g^x$, $a = H_3(R)$, $T_1 = (u_a + s_a)^{-1} P$, $T_2 = u_a x P$. Outputs the offline ciphertext $\phi = (u_a, x, U_a, R, a, T_1, T_2)$.

**Online-Encrypt ($m$, $ID_a$, $\phi$):** To encrypt a message $m$ for Bob, at the Online-Encrypt stage, $SN_A$ receives the offline ciphertext $\phi$ and computes: $t_1 = (u_a + s_a)(q_b + u_a) \bmod q$, $t_2 = H_2(m, u_a, R, T_1, T_2, t_1)x + u_a \bmod q$, $c = a \oplus m$, and outputs the ciphertext $\overline{\varphi} = (U_a, T_1, T_2, t_1, t_2, c)$.

**Offline-Decrypt ($\overline{\phi}$):** At the Offline-Decrypt stage, $PKG_b$ receives the ciphertext $\overline{\phi}$ and computes $Q = e(t_2 T_1 - U_a, P_b + U_a)$, outputs the offline decryptext $\tau = (Q, \overline{\phi})$.

**Online-Decrypt ($\tau$, $D_B$):** $SN_B$ receives the offline decryptext $\tau$ and computes: $R = e(x(T_1 t_1 + P_b) - T_2, D_B)$, $h = H_2(m, u_a, R, T_1, T_2, t_1)$ and $R^h$, accept the message $m = c \oplus H_3(R)$ if and only if the following equation holds: $R^h = Q$.

## 5. Analysis

### 5.1. Security Analysis

#### 5.1.1. Correctness

For the decrypt, we have

$$\begin{aligned} Left &= R^h \\ &= e(x(T_1 t_1 + P_b) - T_2, D_B)^h \\ &= e(x(\frac{1}{u_a + s_a} P \cdot (u_a + s_a)(q_b + u_a) \\ &\quad + s_b P) - u_a x P, \frac{1}{q_b + s_b} P)^h \\ &= e(x((q_b + u_a)P + s_b P) - u_a x P, \frac{1}{q_b + s_b} P)^h \\ &= e(x \cdot (q_b + s_b)P, \frac{1}{q_b + s_b} P)^h \\ &= e(xP, P)^h \\ &= g^{xh} \\ Right &= Q \\ &= e(t_2 T_1 - U_a, P_b + U_a) \\ &= e((H_2 x + u_a)(u_a + s_a)^{-1} P - u_a P, \\ &\quad s_b P + u_a P) \\ &= e((H_2 x + u_a)P - u_a P, P) \\ &= e(hxP, P) \\ &= g^{hx} \end{aligned}$$

Since $Left = Right$, correctness is confirmed.

### 5.1.2. Proof of Confidentiality of the New Scheme

**Theorem 1.** Assume that an *IND-MPIDOOE-CCA* adversary $A$ making $q_{H_i}$ queries to hash oracles $H_i(i=1,2,3)$, $q_E$ key extraction queries and $q_D$ decryption queries, has an advantage $\varepsilon$ against the proposed scheme. Then, there is a simulator $B$ running in polynomial time that solves the k-Bilinear Modified Diffie-Hellman Inversion Problem (*k-BMDHIP*) with an advantage

$$\varepsilon' \geq \varepsilon \cdot \frac{1}{q_{H_1}(q_{H_2}+q_{H_3})} \cdot (1-\frac{q_D}{2^k}).$$

**Proof:** We follow the proof technique from [23]. Suppose $B$ is given a random instance of the *k-BMDHIP* $(P, yP, (x_1+y)^{-1}P, ..., (x_k+y)^{-1}P)$, and aims to find $e(P,P)^{(y+x')^{-1}}$, for a random $x' \notin \{x_1, ..., x_k\}$. $B$ simulates the system with the various oracles $O_{H_1}, O_{H_2}, O_{H_3}, O_{\text{Extract}}, O_{Decrypt}$. $A$ is allowed to make polynomially bounded number of queries, adaptively to the oracles provided by $B$.

The game between $B$ and $A$ can be demonstrated by:

**Setup:** $B$ runs the **G-Setup** and **D-Setup** algorithms with a security parameter $k$ and sends the system parameters and public keys $P_x(x=1,2,...,d)$ to the adversary $A$.

**Phase I:** To maintain the consistency of the oracle query responses and to avoid collision, $B$ maintains three lists $L_i(i=1,2,3)$ to store the responses given by $B$ to the corresponding oracles ( $O_{H_i}(i=1,2,3)$ ) queries. $A$ performs a polynomially bounded number of queries. These queries may be adaptive, i.e. current query may depend on the answers to the previous queries. $B$ simulates $A$'s queries as below.

(a) Random Oracle:

For oracle $O_{H_1}$ query, we assume that $H_1$ queries are distinct throughout the game, and $A$ will ask for $H_1(ID)$ before $ID$ is used in any key extraction query. $B$ selects a random index $v$. When $A$ makes the $v^{th}$ query on $ID_v$, $B$ decides to fix $ID_v$ as target identity for the challenge phase, and $B$ responds to $A$ as follows: If it is the $v^{th}$ query, then $B$ sets $q_v = x'$, returns $q_v$ as the response to the query and stores $(ID_v, q_v)$ in the list $L_1$; If it is other query, $B$ sets $q_t = x_t$ where $x_t$ is the value given in the instance of *k-BMDHIP*. And $B$ puts the pair $(ID_t, q_t)$ in the list $L_1$.

For oracle $O_{H_2}$ query on input $(m, u_a, R, T_1, T_2, t_1)$, $B$ returns the defined value $h$ if it exists in the list $L_2$, otherwise, $B$ responds to $A$ by choosing a random $h \in Z_q^*$ such that no entry $h$ does not exist in $L_2$ and adds the tuple $(m, u_a, R, T_1, T_2, t_1, h)$ into $L_2$.

For oracle $O_{H_3}$ query on input $R$, $B$ returns the defined value $a$ if it exists in the list $L_3$, otherwise, $B$ responds to $A$ by choosing a random $a \in Z_q^*$ such that no entry $a$ does not exist in $L_3$ and adds the pair $(R, a)$ into $L_3$.

(b) Oracle $O_{Extract}$ query: On input $ID_t$, $B$ aborts if $ID_v = ID_t$. Otherwise, $B$ recovers the corresponding pair $(ID_t, q_t)$ from the list $L_1$ and responds to $A$ with $\frac{1}{I_t + s_a} P$.

(c) Oracle $O_{Decrypt}$ query: On input a ciphertext $\bar{\phi}$ for identity $ID_t$, $B$ can directly decrypt the ciphertext if $ID_v \neq ID_t$, since $B$ knows the private key $D_t$ corresponding to $ID_t$. Otherwise, $B$ does not know the private key corresponding to $ID_t$, $B$ responses as below:

For each $(R, a) \in L_3$, computes $m = a \oplus c$, check $h \stackrel{?}{=} O_{H_2}(m, u_a, R, T_1, T_2, t_1)$ and $R \stackrel{?}{=} g^x$, if not true, proceed with the next tuple in $L_3$. Else, check $x(T_1 t_1 + P_b) - T_2 \stackrel{?}{=} x q_b P + x P_b$, if true, $B$ output $m$. If none of the tuples passes the checks described above, then return $\perp$ for rejection.

**Challenge:** $A$ produces two plaintexts $m_0, m_1$ and the receiver identity $ID_R$ which $A$ wishes to be challenged. $A$ should not have queried for the private key corresponding to $ID_R$ in **Phase I**. If $ID_R \neq ID_v$, $B$ aborts. Otherwise $B$ chooses a random bit $b \in \{0,1\}$ and does as follows: picks $\delta, t_1 \in_R Z_q^*$, $T_1 \in_R G_1$, computes $T_2 = x(T_1 t_1 + P_b) - (y+\delta)P$, randomly picks a $c$, return the challenge ciphertext $\bar{\phi}' = (T_1, T_2, t_1, c)$ to $A$.

**Phase II:** $A$ is now allowed to get training as in **Phase I**. $A$ makes a number of new queries as in Phase I with the restriction that it cannot query the decryption oracle and the extraction oracle. $A$ runs the decryption algorithm $R = e(x(T_1 t_1 + P_b) - T_2, D_R) = e((y+\delta)P, D_R)$, thus $R^{(y+\delta)^{-1}}$ equal to $e(P, D_R) = e(P, D_v)$. $A$ should have queried the oracle $O_{H_2}$ or $O_{H_3}$ with $R$ as input to check $\bar{\phi}'$ is valid or not. Hence, one of the entries in list $L_2$ or $L_3$ will contain the value $R$, the solution to the *k-BMDHI* problem.

**Guess:** At the end of the game, $A$ produces a bit $b'$. $B$ fetches a random entry $(m, u_a, R, T_1, T_2, t_1)$ or $(R, \cdot)$ from the lists $L_2$ or $L_3$.

**Lemma 1.** If $B$ does not terminate the simulation game, $A$ can not distinguish between the simulation and the real world.

Hence, with probability $1/(q_{H_2} + q_{H_3})$, $\delta' = R^{(y+\delta)^{-1}} = e(P, D_v) = e(P, P)^{(q_v+s)^{-1}} = g^{(x'+s)^{-1}}$.

And $B$ output $(x', g^{(x'+s)^{-1}})$.

**Probability Analysis:** $B$ only aborts the *IND-MPIDOOE-CCA* game because one of the following independent events happen:

1. $E_1$: $A$ does not choose the target identity $ID_R$ as the receiver during the challenge.

2. $E_2$: $A$ queries the private key of the target identity $ID_R$.

3. $E_3$: $B$ rejects a valid ciphertext at some point of the game.

We have $\Pr[E_1] = 1 - 1/(q_{H_1} - q_{Extract})$, $\Pr[E_2] = q_{Extract}/q_{H_1}$, $\Pr[E_3] \le q_{Decrypt}/2^k$. And the probability that the random entry chosen by $B$ from the list $L_3$ becoming the solution to the *k-BMDHIP* is $1/(q_{H_2} + q_{H_3})$, therefore the probability of $B$ solving the *k-BMDHIP* is

$$\Pr[A(P, yP, (x_1+y)^{-1}P, ..., (x_k+y)^{-1}P) = e(P,P)^{(y+x')^{-1}} \mid y, x' \in Z_q^*, x' \notin \{x_1, ...x_k\}] = \varepsilon \cdot \Pr[\neg E_1 \wedge \neg E_2 \wedge \neg E_3] \ge \varepsilon \cdot \frac{1}{q_{H_1}(q_{H_2} + q_{H_3})} \cdot (1 - \frac{q_{Decrypt}}{2^k}).$$

Since $\varepsilon$ is non-negligible, the probability of $B$ solving *k-BMDHIP* is non-negligible. This clearly shows that no polynomially bounded adversary exists who can solve the *IND-MPIDOOE-CCA* security of the proposed scheme.

### 5.2. Comparison with Existing Schemes

The performance of our scheme is comparable to previous identity based online/offline encryption scheme [21, 22]. The comparison of Complexity is showed in the Table 1, which indicates that the proposed scheme in this paper is more efficient. We denote by *PM* the point multiplication in $G_1$ or $G_2$, *BP* the bilinear pairing in $G_1$ and $G_2$, *M* the modular computation in $Z_q^*$, *E* the exponentiation in $G_2$, FE the offline encrypt, NE the online encrypt, FD the offline decrypt, ND the online decrypt and SM the security model.

**Table 1.** Comparison of Complexity.

| | GMC-1[21] | GMC-2[21] | Liu[22] | Our |
|---|---|---|---|---|
| FE | *7SPM+1BP +1E* | *6SPM+1BP +1E* | *5SPM+1BP +1E* | *4SPM+1E* |
| NE | *1SPM+2M +1E* | *1SPM+2M +1E* | *3M+1E* | *2M+1E* |
| FD | — | — | — | *2BP* |
| ND | *4SPM+ 7BP +2E* | *4SPM+ 3BP +2E* | *4SPM+ 3BP +1E* | *1SPM+ 1BP +1E* |
| SM | selective ID | standard | random oracle | random oracle |

## 6. Conclusions

Identity based encryption schemes wherein the encryption is carried out in two phases namely, offline and online phase according to the complexity of the operations performed is known to be identity based online/offline encryption scheme. We focus on the large-scale resource-constrained WSN, divide WSN nodes into several domains and present an efficient multi-PKG online/offline identity-based encryption scheme for WSN. Most heavy computations such as exponentiation or pairing, if any, are done in the offline phase, and it does not require the knowledge of the plaintext or the receiver's identity. And we prove the security of the new scheme in the random oracle model.

## Acknowledgements

The authors would like to thank the reviewers for their detailed reviews and constructive comments, which have helped improve the quality of this paper. This work was supported in part by National High Technology Research and Development Program of China (863 Program) (2007AA0124487), National Natural Science Foundation of China (60473012), and Colleges and Universities of Jiangsu Province Plans to Graduate Research and Innovation (CXLX11_1008).

## References


[1]. L. Eschenauer, V. D. Gligor, A key-management scheme for distributed sensor networks, in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, Washinghton, ACM Press, 2002, pp. 41−47.

[2]. H. Chan, A. Perrig, D. Song, Random key predistribution schemes for sensor networks, in *Proceedings of the IEEE Symposium on Security and Privacy*, Berkeley, California, USA, 2003, pp. 197-213.

[3]. A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, D. E. Culler, SPINS: security protocols for sensor networks, *ACM Wireless Networks*, Vol. 8, Issue 5, 2002, pp. 521–534.

[4]. D. Liu, P. Ning, Multi-Level μTESLA: broadcast authentication for distributed sensor networks, *ACM Transactions on Embedded Computing Systems*, Vol. 3, Issue 4, 2004, pp. 800–836.

[5]. J. Drissi, Q. Gu, Localized broadcast authentication in large sensor networks, in *Proceedings of the International Conference on Networking and Services (ICNS' 2006)*, 2006, pp. 25–31.

[6]. K. Ren, W. Lou, K. Zeng, P. J. Moran, On broadcast authentication in wireless sensor networks, *IEEE Transactions on Wireless Communications*, Vol. 6, Issue 11, 2007, pp. 4136–4144.

[7]. P. Ning, A. Liu, W. Du, Mitigate DOS attacks against broadcast authentication in wireless sensor networks, *ACM Transactions on Sensor Networks*, Vol. 4, Issue 1, 2008, pp. 1–35.

[8]. K. Ren, S. Yu, W. Lou, Y. Zhang, Multi-user broadcast authentication in wireless sensor networks, *IEEE Transactions on Vehicular Technology*, 2009.

[9]. Jongdeog Lee, Krasimira Kapitanova, H. Son Sang, The price of security in wireless sensor networks, *Computer Networks*, Vol. 54, Issue 17, 2010, pp. 2967–2978.

[10]. Claude Castelluccia, C.-F. Chan Aldar, Einar Mykletun, Efficient and provably secure aggregation of encrypted data in wireless sensor networks, *ACM Transactions on Sensor Networks*, Vol. 5, Issue 3, 2009, pp. 1–36.

[11]. J. Y. Yang, D. Xiao, T. Xiang, Cryptanalysis of a chaos block cipher for wireless sensor network, *Communication Nonlinear Science Numerical Simulation*, Vol. 16, Issue 2, 2011, pp. 844–850.

[12]. X. Guo, J. Zhang, M. K. Khan, K. Alghathbar, Secure chaotic map based block cryptosystem with application to camera sensor networks, *Sensors*, Vol. 11, Issue 2, 2011, pp. 1607–1619.

[13]. A. Shamir, Identity-based cryptosystems and signature schemes, in G. R. Blakely, D. Chaum, (eds.) CRYPTO, Lecture Notes in Computer Science, Vol. 196, *Springer,* Heidelberg, 1985, pp. 47–53.

[14]. D. Boneh, M. K. Franklin, Identity-based encryption from the Weil pairing, in *CRYPTO 2001*, ed. by J. Kilian. Lecture notes in Computer Science, Vol. 2139, *Springer,* Berlin, 2001, pp. 213–229.

[15]. D. Boneh, X. Boyen, Efficient selective-ID secure identity based encryption without random oracles, in *EUROCRYPT 2004*, ed. by C. Cachin, J. Camenisch. Lecture Notes in Computer Science, Vol. 3027, *Springer*, Berlin, 2004, pp. 223–238.

[16]. D. Boneh, X. Boyen, Secure identity based encryption without random oracles, in Advances in Cryptology, Lecture notes in Computer Science, Vol. 3152, *Springer-Verlag*, Berlin, 2004, pp. 443-459.

[17]. B. Waters, Efficient identity-based encryption without random oracles, in Advances in Cryptology, Lecture notes in Computer Science, Vol. 3494, *Springer-Verlag*, Berlin, 2005, pp. 114-127.

[18]. C. Gentry, Practical identity-based encryption without random oracles, in Advances in Cryptology, Lecture Notes in Computer Sciences, Vol. 4004, *Springer-Verlag*, Berlin, 2006, pp. 445-464.

[19]. S. Even, O. Goldreich, S. Micali, Online/offline digital signatures, in G. Brassard, (ed.) Crypto, Lecture Notes in Computer Science, Vol. 435, *Springer*, Heidelberg, 1990, pp. 263–275.

[20]. S. Even, O. Goldreich, S. Micali, Online/offline digital signatures, *Journal of Cryptology*, Vol. 9, Issue 1, 1996, pp. 35–67.

[21]. Fuchun Guo, Yi Mu, Zhide Chen, Identity-based online/offline encryption, in *Financial Cryptography and Data Security, Lecture Notes in Computer Science*, Vol. 5143, 2008, pp. 247–261.

[22]. Joseph K. Liu, Jianying Zhou, An efficient identity-based online/offline encryption scheme, in Applied Cryptography and Network Security, *Lecture Notes in Computer Science,* Vol. S 5536, 2009, pp. 156–167.

[23] P. Barreto, B. Libert, N. McCullagh, J. Quisquater, Efficient and provably-secure identity-based signature and signcryption from bilinear maps, in: B. Roy, (ed.) *Advances in Cryptology – ASIACRYPT 2005*, *Lecture notes in Computer Science*, Vol. 3788, 2005, pp. 515–532.


2013 Copyright ©, International Frequency Sensor Association (IFSA). All rights reserved.
(http://www.sensorsportal.com)