
# LIGHTWEIGHT TRUSTED ID-BASED SIGNCRYPTION SCHEME FOR WIRELESS SENSOR NETWORKS

Zhimin Li, Xin Xu, Zexiang Fan
School of Computer Engineering
Huaihai Institute of Technology, Canwu Road 59
Lianyungang, China, 222005
Emails: {lizhimin1981, xinxu, zx.fan}@gmail.com

***Submitted: Aug.3, 2012*** ***Accepted: Sep.3, 2012*** ***Published: Dec.1, 2012***

***Abstract - Wireless sensor networks (WSN) are usually deployed in hostile environments, which having a wide variety of malicious attacks. As various applications of WSN have been proposed, security has become one of the big research challenges dan is receiving increasing attention. In order to insure the security of communication in wireless sensor networks, we proposed a new ID-based signcryption scheme using bilinear pairing. Under the computational Diffie-Hellman assumption, the security of the scheme is proved under the Random Oracle Model. This scheme can be used by the sensor nodes that with low power, less storage space and low computation ability. It is concluded that the proposed lightweight scheme satisfies the security requirements of WSN.***

**Index terms*:* WSN, ID-based signcryption, provably secure, bilinear pairing.**

# I. INTRODUCTION

Wireless sensor network (WSN) is a new network structure which consists of small nodes also called motes. These motes can be used to monitor physical or environmental conditions around them such as temperature, sound, vibration etc, process data, and communicate through wireless links [1]. In WSN, wireless sensors communicate each other by using of a radio link. WSNs are widely used these days and are very popular in research for use of embedded systems in our daily life. WSNs are used in applications involving monitoring, tracking, or controlling such as habitat monitoring, robotic toys, battlefield monitoring, packet insertion [2, 3], traffic monitoring, object tracking and nuclear reactor control.

Usually, we protect message confidentiality by using encryption program, and use digital signature technology to prevent messages from being forged. Compared to the using of the above two techniques, Zheng [4] proposed the signcryption technology which is more applicable to resource-constrained networks. Signcryption scheme is a cryptographic primitive that provides both these properties together in an efficient way. Adi Shamir [5] introduced the concept of identity based cryptography. The idea of identity based cryptography is to enable a user to use any arbitrary string (such as name, Identity number, Email address, etc.) as his public key. Identity based cryptography serves as an efficient alternative to Public Key Infrastructure (PKI) based systems. ID-based signcryption was first studied by Malone-Lee et al. [6]. ID-based cryptography does not require public key authentication, it has a higher efficiency of computing and communications, and more suitable. Formally, some ID-based signcryption algorithms are designed for WSN security communications [7-12]. The results show that the ID-based signcryption technology plays an important role to improve the safety and efficiency of WSN.

In order to further improve the safety and efficiency of the WSN communication, this paper designs a provably secure signcryption algorithm based on the Identity, the computation and transmission costs of the algorithm is small, which can better meet the needs of the WSN that having fixed topology, distributed management, and resource-constrained environment.

The rest of the paper is organized as follows. Section 2 reviews some definitions and security modes. Our proposed scheme is described in Section 3. The security of our scheme is analyzed in Section 4. Section 5 gives the conclusion.

## II. PRELIMINARIES

In this section, we review some background knowledge including the bilinear pairing and Diffie-Hellman problem. We also provide the generic mode and security notions necessary to build our signcryption scheme in this section. We refer the reader to [13-15] for a discussion of how to build a concrete instance using supersingular curves and compute the bilinear map.

a. Bilinear pairings and Diffie-Hellman problem

We briefly review the bilinear pairing. Let $G_1$ denote an additive group of prime order p and G2 be a multiplicative group of the same prime order. Let $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ be a bilinear mapping with the following properties:

(1) Bilinear: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$, for all $P, Q \in G_1$, and $a, b \in$ $^{*}_{q}$.

(2) Non-degenerate: $\hat{e}(Q, R) \neq 1$, for some $Q, R \in G_1$.

(3) Computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in G_1$.

The security of our scheme relies on the hardness of the following problems.

**Definition 1.** Let $(G_1, +)$ be a cyclic additive group generated by $P$, the computational Diffie-Hellman (CDH) problem in $G_1$ is to compute $abP$ given $aP$, $bP$.

**Definition 2.** Given two groups $G_1$ and $G_2$ of the same prime order $p$, a bilinear mapping $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ and a generator $P$ of $G_1$, the computational bilinear Diffie-Hellman (CBDH) problem in $(G_1, G_2, \hat{e})$ is to compute $\hat{e}(P, P)^{abc}$, given $(P, aP, bP, cP)$.

b. Outline of ID-based signcryption

An ID-based signcryption scheme consists of the following four probabilistic polynomial time (*PPT*) algorithms:

***Setup:*** Given a security parameter $1^K$, private key generator (PKG) uses this algorithm to generate *Params* the global public parameters and master secret key $S$ and a corresponding public key $P_{pub}$.

***Extract:*** Given an identity ID, the PKG computes the corresponding private key $K_{ID}$ and transmits it to its owner in a secure way.

***Signcrypt:*** To send a message $m$ to Bob, Alice obtains the ciphertext $\sigma$ by computing $Signcrypt(m, K_{Alice}, ID_{Bob})$.

***Unsigncrypt:*** When Bob receives $\sigma$, he computes $Unsigncrypt(\sigma, ID_{Alice}, K_{Bob})$ and obtains the plaintext $m$ or value "invalid" if $\sigma$ is an invalid ciphertext between identities $ID_{Alice}$ and $ID_{Bob}$.

c. Security notions

Malone-Lee [3] defined the security notions for ID-based signcryption schemes. These notions are indistinguishability of ID-based signcryption against adaptive chosen ciphertext attacks and unforgeability of ID-based signcryption against adaptive chosen messages attacks.

**Definition 3:** An ID-based signcryption scheme is said to be indistinguishable against adaptive chosen ciphertext attacks (IND-IDSC-CCA2) if no polynomially bounded adversary has non-negligible advantage in the following game:

**Setup:** The challenger C runs the *Setup* algorithm with a security parameter $1^K$ and obtains public parameters *Params* and the master private key *S*. C sends *Params* to the adversary A and keeps *S* secret.

**Phase I:** The adversary A performs a polynomially bounded number of queries to C. The queries made by A may be adaptive, i.e. current query may depend on the answers to the previous queries. The various oracles and the queries made to these oracles are defined below:

(1) *Key extraction queries:* A produces an identity $ID_i$ and receives the private key $K_i$.

(2) *Signcryption queries:* A produces two identities $ID_i$, $ID_j$ and a plaintext $m$. C computes $K_i$ and generates the signcryption $\sigma$ of the message $m$ using $K_i$ following the signcryption scheme and sends $\sigma$ to A.

(3) *Unsigncryption queries:* A produces the sender identity $ID_i$, the receiver identity $ID_j$ and the signcryption $\sigma$ as input to this algorithm and requests the unsigncryption of $\sigma$. C generates the private key $K_j$ and performs the unsigncryption of $\sigma$ using $K_j$ and sends the result to A. The result of unsigncryption will be "invalid" if $\sigma$ is not a valid signcryption. It returns the message $m$ if $\sigma$ is a valid signcryption.

**Challenge:** A chooses two plaintexts, $m_0$ and $m_1$ of equal length, the sender identity $ID_i$, the

receiver identity $ID_j$ and submits them to C. However, A should not have queried the private key corresponding to $ID_i$ in Phase I. C now chooses $b \in )$,1} and computes $\sigma = Signcrypt(m_b, K_i, ID_j)$ and sends $\sigma$ to A.

**Phase II:** A is allowed to interact with C as in Phase-I with the following restrictions. A should not query the extract oracle for the private key corresponding to the receiver identity $ID_j$. A should not query the unsigncrypt oracle with ($\sigma$, $ID_i$, $ID_j$) as input, i.e. a query of the form $Unsigncrypt(\sigma, ID_i, ID_j)$ is not allowed.

**Guess:** Finally, A produces a bit *b'* and wins the game if *b'* = *b*. The advantage of A in the above game is defined by $Adv(A) = |2Pr(b' = b) - 1|$, where $Pr(b' = b)$ denotes the probability that *b'* = *b*.

Note that the adversary is allowed to make a key extraction query on identity $ID_i$ in the above definition. This condition corresponds to the stringent requirement of the insider security for confidentiality of signcryption. It also ensures the forward security of the scheme.

**Definition 4:** An ID-based signcryption scheme is said to be existentially unforgeable against adaptive chosen message attacks (EUF-CMA) if no polynomially bounded adversary has a non-negligible advantage in the following game.

**Setup:** The challenger C runs the Setup algorithm with security parameter $1^K$ and obtains public parameters *Params* and the master private key *S*. C sends *Params* to the adversary A and keeps *S* secret.

**Training Phase:** The adversary A performs a polynomially bounded number of queries adaptively as in Phase I of confidentiality game (IND-IDSC-CCA2).

**Forgery:** After a sufficient amount of training, A produces a signcryption ($\sigma$, $ID_i$, $ID_j$) to C. Here, A should not have queried the private key of $ID_i$ during the training phase and $\sigma$ is not the output of Signcrypt($m$, $ID_i$, $ID_j$) as input ($m=Unsigncrypt(\sigma, ID_i, ID_j)$ ). A wins the game, if $Unsigncrypt(\sigma, ID_i, ID_j)$ is valid.

The advantage of A is defined as the probability that it wins. Note that the adversary is allowed to make a key extraction query on the identity $ID_j$ in the above definition. This condition is considered to the stringent requirement of insider security for signcryption.

## III. ID-BASED SIGNCRYPTION SCHEME FOR WSN

In this section, we propose a new ID-based signcryption which can be efficient used in WSN. The following shows the details of our scheme.

**Setup:** Define $G_1$, $G_2$ and $\hat{e}$ as in previous section. Let $H_1$, $H_2$ and $H_3$ be three cryptographic hash functions where $H_1$: $\{0, 1\}^* \rightarrow G_1$, $H_2$: $\{0, 1\}^n \times G_1 \times G_2 \rightarrow \{0, 1\}^n$, $H_3$: $\{0, 1\}^n \times \{0, 1\}^n \times G_1 \rightarrow \{0, 1\}^n$. Let $P$ be a generator of $G_1$. PKG chooses a master secret key $S \in Z_q^*$, keeps $S$ secret and computes $P_{pub} = SP$. The system's public parameters *Params* are ($G_1$, $G_2$, $q$, $n$, $P$, $P_{pub}$, $\hat{e}$, $H_1$, $H_2$, $H_3$, $H_4$).

**Extract:** Given *Params*, to generate a secret key for a user with identity $ID \in \{0,1\}^n$, PKG computes $K_{ID} = SQ_{ID}$, where $Q_{ID} = H_1(ID)$.

**Signcrypt:** To send a message $m$ to user B with identity $ID_B$, user A with identity $ID_A$ follows the steps below.

(1) Choose $x \in Z_q^*$.

(2) Compute $U = xP$.

(3) Compute $\alpha = \hat{e}(P_2, Q_B)^x$.

(4) Compute $\beta = H_2(m, \alpha, U)$.

(5) Compute $C = m \oplus \beta$.

(6) Compute $r = H_3(C, U, \beta)$.

(7) Compute $V = xP_{pub} + rK_A$

The ciphertext is $\sigma = (c, U, V)$.

**Unsigncrypt:** When receiving $\sigma = (c, U, V)$, user B follows the steps below.

(1) Compute $\alpha = \hat{e}(U, K_B)$.

(2) Compute $\beta = H_2(m, \alpha, U)$.

(3) Recover $m = C \oplus \beta$.

(4) Compute $r = H_3(C, U, \beta)$.

(5) Accept the message if and only if the equation holds, $\hat{e}(P, V) = \hat{e}(U, P_{pub})\hat{e}(P_{pub}, Q_A)^r$. Otherwise, output "Invalid".

## IV. SECURITY ANALYSIS

a. Correctness

The correctness can be easily verified by the following equations.

$$\hat{e}(P, V) = \hat{e}(P, xP_{pub} + rK_A) = \hat{e}(xP, P_{pub})\hat{e}(P, rK_A) = \hat{e}(U, P_{pub})\,\hat{e}(P, rSQ_A)$$
$$= \hat{e}(U, P_{pub})\,\hat{e}(SP, Q_A)^r = \hat{e}(U, P_{pub})\hat{e}(P_{pub}, Q_A)^r$$

b. Security

**Theorem 1 (Confidentiality).** If their exists an adversary called A that is able to break the IND-IDSC-CCA2 security with an advantage $\varepsilon$, then there exists a distinguisher C that can solve the CBDH problem with advantage $O(\varepsilon)$.

**Proof.** The interaction between A and C can be viewed as a game given in definition 3. Assume the distinguisher C is provided with a random instance ($P$, $aP$, $bP$, $cP$) of the CBDH problem. His goal is to compute $\hat{e}(P, P)^{abc}$. C will run A as a subroutine and act as A's challenger in the IND-IDSC-CCA2 game. During the game, A will consult C for answers to the random oracles $H_1$, $H_2$ and $H_3$. C maintains lists $L_1$, $L_2$, $L_3$ respectively in giving the responses to the queries. These answers are randomly generated, but to maintain the consistency and to avoid collision.

**Setup:** For having the game with A, C chooses $P_{pub} = aP$ and gives A the system parameters ($G_1$, $G_2$, $q$, $P$, $P_{pub}$). Note that $a$ is unknown to C, this value simulates the master secret key value for the PKG in the game.

**Phase I:** During phase I, A is allowed to access the various oracles provided by C. A can get sufficient training before generating the forgery. The various oracles provided by C to A during training are as follows.

• ***$H_1$* Oracle Queries ($\Omega_{H1}$):** When this oracle is queried with $ID_i$ by A, C responds as follows. C chooses a random number $i_0 \in \{1, 2, \ldots, q_{H1}\}$, where $q_{H1}$ is the maximum bounded number of allowed queries by A. At the $i_0$-th query, C answers by $H_1(ID_{i0}) = bP$, stores ($ID_i$, , $bP$) in list $L_1$. Otherwise, sets $Q_i = H_1(ID_i) = b_iP$, stores ($ID_i$, $b_i$, $Q_i$) in list $L_1$. C returns $Q_i$ to A.

• ***$H_2$* Oracle Queries** ($\Omega_{H2}$): When A makes a query with input ($m_i$, $\alpha_i$, $U_i$), C performs the following. If ($m_i$, $\alpha_i$, $U_i$, $\beta_i$) is available in list $L_2$, C returns $\beta_i$ to A. Otherwise, C picks $\beta \equiv Z_q^*$ satisfying no vector ($\cdot$, $\cdot$, $\cdot$, $\beta$) exists in $L_2$, stores ($m_i$, $\alpha_i$, $U_i$, $\beta$) in list $L_2$. Then, C returns $\beta$ to A.

• ***$H_3$* Oracle Queries ($\Omega_{H3}$):** On a ($C_i$, $U_i$, $\beta_i$) query, C checks whether there exists ($C_i$, $U_i$, $\beta_i$, $r_i$) in $L_3$ or not. If such a tuple is found, C answers $r_i$, otherwise he chooses $r \in Z_q^*$, returns it as an answer to the query and puts the tuple ($C_i$, $U_i$, $\beta_i$, $r$) into $L_3$.

**Key extraction queries:** When A asks the secret key of user with identity $ID_i$, if $i = i_0$, then C fails and stops. Else, C computes $Q_i = \Omega_{H1}(ID_i)$, $K_i = aQ_i = b_iP_{pub}$. If ($ID_i$, ·, $Q_i$) does not exists in the list $L_1$, C stores it in $L_1$. Then C returns $K_i$ to A.

**Signcryption queries:** A queries a signcryption for a plaintext $m$ and identities $ID_i$ and $ID_j$. C has the following two cases to consider. Case1: $i \neq i_0$. C computes the private key $S_i$ corresponding to $ID_i$ by running the key extraction query algorithm. Then C answers the query by a call to Signcrypt($m$, $S_i$, $Q_j$). Case 2: $i = i_0$. C chooses $r, x \in Z_q^*$ and computes $U = xP - rQ_i$; $\alpha = \hat{e}(U, K_j)$; $V = xP_1$ (here, $K_j$ is derived from the key extraction algorithm). C runs the $H_2$ simulation algorithm to find $\beta = \Omega_{H2}(m, \alpha, U)$; $C = E_\alpha(m||\beta)$. C then checks if $L_3$ already contains a tuple ($C$, $U$, $\beta$, $r'$) with $r \neq r'$. In this case, C repeats the process with another random pair ($x$, $r$) until finding a tuple ($m$, $U$, $k$, $r$) whose first three elements do not appear in a tuple of the list $L_3$. When an appropriate pair ($x$, $r$) is found, the ciphertext ($c$, $U$, $V$) appears to be valid from A's viewpoint.

**Unsigncryption queries:** For an unsigncryption query, C has the following two cases to consider. Case 1: $j = i_0$. C always answers "invalid" to A. Case 2: $j \neq i_0$. C derives $K_j$ from the key extraction algorithm, then C computes $\alpha = \hat{e}(U, K_j)$; $\beta = \Omega_{H2}(m, \alpha, U)$; $m = C \oplus \beta$; $r = \Omega_{H3}(C, U, \beta)$. C checks if $\hat{e}(P, V) = \hat{e}(U, P_1)\hat{e}(P, Q_A)^r$ holds. If the equation does not hold, C rejects the ciphertext. Otherwise C returns $m$ to A.

**Challenge Phase:** At the end of Phase I interaction, A picks two messages ($m_0$, $m_1$) of equal length, the sender identity $ID_S$ and the receiver identity $ID_R$, and submits to C. On getting this, C checks whether $R = i_0$. If $R \neq i_0$, then we have the conclusion that C aborts. Otherwise, C chooses a random bit $t \in \{0,1\}$ and generates the signcryption value of $m$ as follows. C picks a random $x \in Z_q^*$, sets $U^* = aP$, computes $\beta^* = \Omega_{H2}(m_t, x, U^*)$; $C^* = m \oplus \beta^*$; $r^* = \Omega_{H3}(C^*, U^*, \beta^*)$; $V = daP + r^*\Omega_{Extract}(ID_i)$. C returns $\sigma^* = (U^*, V^*, C^*)$ as the challenge signcryption to A.

**Phase-II:** A interacts with $C$ as in Phase-I, but with the following restrictions that A should not query the private key of $ID_R$ and the unsigncryption of $\sigma^*$ with $ID_S$ as sender and $ID_R$. At the end of the interaction, A produces a bit $t'$ for which he believes the relation $\sigma^*$ = Signcrypt($m_{t'}$, $K_S$,

$ID_R$) holds. At this moment, if $t = t'$, $C$ outputs $h = \hat{e}(U^*, K_{i0}) = \hat{e}(aP, cbP) = \hat{e}(P, P)^{abc}$ as a solution of the CBDH problem, otherwise $C$ stops and outputs "failure".

**Probability Analysis:** The probability of success of C can be measured by analyzing the various events that happen during the simulation. Assume $q_{H1}$, $q_{H2}$, $q_{H3}$, $q_K$, $q_S$, $q_U$ are the maximum polynomial number of queries allowed to the oracles $\Omega_{H1}$, $\Omega_{H2}$, $\Omega_{H3}$, $\Omega_{H1}$, key extraction queries, signcryption queries and unsigncryption queries, respectively. The events in which C aborts the IND-IBSC-CCA2 game are list as follows. If A asked a key extraction query on $ID_{i0}$ during the first stage, C fails. The probability for $C$ not to fail in this event is $(q_{H_1} - \iota_K)/q_{H_1}$. Further, with a probability $1/(q_{H_1} - \iota_K)$, A chooses to be challenged using the receiver with identity $ID_{i0}$. Hence the probability that A's response is helpful to $C$ is $1/q_{H_1}$.

Taking into account all the probabilities that $C$ will not fail its simulation, the value of Adv(C) is calculated as follows, $\text{Adv(C)} = (\frac{(\varepsilon \vdash)}{2}(1 - \frac{q_U}{2^n}) - \frac{1}{2})(\frac{1}{q_{H_1}}) = \frac{\varepsilon\, 2^n - q_U) - q_U}{q_{H_1} 2^{n+}}$.

If the advantage $\varepsilon$ of A to break the IND-IDSCMP-CCA2 game non-negligible, the probability of C to solve CBDH problem is also non-negligible.

**Theorem 2 (Unforgeability).** If their exists an adversary called A that is able to break the EUF-CMA security with an advantage $\varepsilon$, then there exists a distinguisher C that can solve the CDH problem with advantage $O(\varepsilon)$.

**Proof.** The interaction between A and C can be viewed as a game given in definition 4. When C is provided with a random instance ($P$, $aP$, $bP$) of the CDH problem. C can use A as a subroutine and act as A's challenger in the EUF-CMA game to compute $abP$. During the game, A will consult C for answers to the random oracles $H_1$, $H_2$ and $H_3$. C maintains lists $L_1$, $L_2$, $L_3$ respectively in giving the responses to the queries. These answers are randomly generated, but to maintain the consistency and to avoid collision.

**Setup:** For having the game with A, C chooses $P_{pub} = aP$ and gives A the system parameters ($G_1$, $G_2$, $q$, $P$, $P_{pub}$). Note that $a$ is unknown to C, this value simulates the master secret key value for the PKG in the game.

**Training Phase:** During this phase, A is allowed to access the various oracles provided by C. A can get sufficient training before generating the forgery. The various oracles provided by C to A during training are similar to the oracles described in phase I of Theorem 1.

**Forgery Phase:** After getting sufficient training, A submits the signcryption ($ID_i$, $ID_j$, $\sigma$) with the following restrictions that A has not ever queried the private key of $ID_i$ and the unsigncryption of $\sigma$*. If $i = i_0$ and $\sigma$ is valid, $C$ does the following. C retrieves $r$ correspondingly from list $L3$, computes the value $abP = K_i = r^{-1}(V - xP_1)$, i.e., C obtains the solution to the CDH problem instance.

**Probability Analysis:** The probability of success of $C$ can be measured by analyzing the various events that happen during the simulation. Assume $q_{H1}$, $q_{H2}$, $q_{H3}$, $q_K$, $q_S$, $q_U$ are the maximum polynomial number of queries allowed to the oracles $\Omega_{H1}$, $\Omega_{H2}$, $\Omega_{H3}$, $\Omega_{H1}$, key extraction queries, signcryption queries and unsigncryption queries, respectively. The events in which C aborts the EUF-CMA game are list as follows. If A asked a key extraction query on $ID_{i0}$ during the first stage, C fails. The probability for $C$ not to fail in this event is $(q_{H_1} - \prime_K)/q_{H_1}$. Further, with a probability exactly $1/(q_{H_1} - \prime_K)$, A chooses to be challenged using the receiver with identity $ID_{i0}$. Hence the probability that A's response is helpful to $C$ is $1/q_{H_1}$. We have the conclusion that if A can win the EUF-CMA game with an advantage $\varepsilon$, the value of Adv(C) is calculated as Adv(C) = $\varepsilon_{,} q_{H_1}$. Then, if the advantage $\varepsilon$ of A to break the EUF-CMA game is non-negligible, the probability of C solving CDH problem is also non-negligible.

## V. CONCLUSIONS

In this paper, we have proposed a new ID-based signcryption scheme based on the bilinear pairings. Confidentiality, integrity, non-repudiation and authentication are the important requirements for many cryptographic applications. We discussed the security of the newly proposed scheme in the random oracle model in detail. The results are that our scheme satisfies the confidentiality, the unforgeability, and the public verfiability. Thus, we have the conclusion that our scheme is fit for using in wireless sensor networks.

## ACKNOWLEDGMENT

This work is sponsored by Item of Scientific Research Fund for Talents of Huaihai Institute of Technology (No.KQ10121), Research Fund of Huaihai Institute of Technology (No.KX10530).

## REFERENCES

[1] F. Amin, A. H. Jahangir, H. Rasi fard, "Analysis of Public-Key Cryptography for Wireless Sensor Networks Security," World Academy of Science, Engineering and Technology, 2008.

[2] J. Deng, R. Han, Shivakant Mishra, "Enhancing Base Station Security in Wireless Sensor Netowrks," University of Colorado, Department of Computer Science. Technical Report CU-US-951-03, 2003.

[3] P. Wide, "Human-based Sensing - Sensor Systems to Complement Human Perception", International Journal on Smart Sensing and Intelligent Systems, vol.1, No.1, pp.57-69, 2008.

[4] Y. Zheng, "Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)," Advances in Cryptology-CRYPTO'07, LNCS 4294, Springer, 2007, pp.165-179.

[5] A. Shamir, "Identity-based cryptosystems and signature schemes," Advances in Cryptology-CRYPTO' 84, LNCS 196, Springer, 1984, pp.47-53.

[6] J. Malone-Lee, "Identity based signcryption," Cryptology ePrint Archive. Report 2012/098, 2002, Available from: http://eprint.iacr.org/2012/098.

[7] J. K. Liu, J. Baek, J. Zhou, Y. Yang, J. Wong, "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network," Cryptology ePrint Archive. Report 2010/03, 2010, Available from: http://eprint.iacr.org/2010/03.

[8] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," IEEE Transactions on Wireless Communications, pp. 660–670, 2012.

[9] A. Boukerch, L. Xu, K. El-Khatib, "Trust-based security for wireless ad hoc and sensor networks," Computer Communication 30(11–12), pp. 2413–2427, 2007.

[10] K. Kifayat, M. Merabti, Q. Shi, D. Lewellyn-Jones, "An efficient algorithm to detect faulty reading in wireless sensor network using the concept of reputation," International Conference on Network and Service Security, pp. 1–5, 2009.

[11] P. Kamat, A. Baliga, W. Trappe, "An identity-based security framework for VANETs," VANET'06, Los Angeles, California, pp.94-95, 2006.

[12] H. Yussof, J. Wada and M. Ohka, “Analysis of Tactile Slippage Control Algorithm for Robotic Han Performing Grasp-Move-Twist Motions”, International Journal on Smart Sensing and Intelligent Systems, vol. 3, No. 3, 2010, pp. 359-375.

[13] S. D. Galbraith, “Supersingular curves in cryptography,” Advances in Cryptology-ASIACRYPT 2011, LNCS 4248, Springer, pp. 419-513, 2011.

[14] D. Boneh, B. Lynn, H. Shacham, “Short signatures from the Weil pairing,” Advances in Cryptology - ASIACRYPT 2011, LNCS 4448, Springer, pp. 514-532, 2011.

[15] A. Joux, “The Weil and Tate pairings as building blocks for public key cryptosystems,” Algorithm Number Theory, LNCS 2369, Springer, pp. 20-32, 2002.