Performance Comparison of Identity Based Encryption and Identity Based Signature

Arjun Kumar[1] and HoonJae Lee[2]

[1] *Dept. of Ubiquitous IT, Dongseo University, Busan, 617-716, Korea*
[2]*Dept. of Communication and Information Engg., Dongseo University, Busan*
a.kumar@iitg.ernet.in, hjlee@gdsu.dongseo.ac.kr

Abstract

Dependence on a public key infrastructure (PKI) is the prominent obstructer in the path of following a public key cryptography widespread, which is held together among various users. In order to ensure authenticated communication, encryption and signature key pair must be generated by each senders and receivers. Apart from this, request along with the proof of identity should also be submitted to the Certificate Authority (CA) and receive CA-Signed certificates, so that it can be used to authenticate one another and exchange encrypted message while limitations of this is that it consumes more time and is error-prone as well. So to get rid of this menace we need to explore few alternatives which will not ask about certificates for encryption and signature verification. Thus, we identify that identity based cryptography approach is one of the robust alternative feature. Using this Characteristic we will be able to overcome the complexity of a cryptography system to a greater extent by ignoring use of generating and managing user's certificates. Integer factorization, quadratic residue and bilinear pairing are the parameters on the basis of which we review the identity based cryptographic primitive. To make sure how it works several major proposals for identity based encryption schemes and identity based signature schemes has been explored along with their performance comparisons.

Keywords: *Identity based encryption, Identity based signature, Identity based cryptography*

1. Introduction

The concept of Identity based cryptography (IBC) was first introduced by Adi Shamir in 1984 [3]. Its primary innovation was its use of user identity attributes, such as email address, phone number, IP address instead of digital certificates for encryption and signature verification. This feature significantly reduces the complexity of a cryptography system by eliminating the need for generating and managing user certificates.

At the time Shamir published his proposal, which he had already determined a way of using the existing RSA function for identity based signature (IBS) scheme but had yet to solve the problem of identity based encryption (IBE). Most of the schemes proposed since 1984 [2, 4, 5, 6, 7] were unsatisfactory because they were too computational intensive and they required tamper resistant hardware or they were not secure if users colluded. Three IBE solutions were proposed in 2001 by Boneh and Franklin [1] as well as by Cocks [14] and Sakai-Kasahara [13] respectively. The Boneh-Franklin scheme has received much attention owing to the fact that it was the first IBE scheme to have a proof of security in an appropriate model. Boneh and Franklin used the bilinear pairing to realize IBE scheme, many IBE and IBS schemes based on the bilinear pairing have been constructed recently.

The purpose of this paper is not to provide full description of all the IBE and IBS schemes but to provide the performance comparison based on encryption algorithm and computational cost. In order to make the concept of given IBE and IBS schemes understandable for as many readers as possible, we have described schemes briefly so that readers could be encouraged to follow the given references for more details.

2. Definition of Identity Based Encryption

An identity based encryption scheme is specified by four probabilistic polynomial time algorithm: **Set-Up, Key-Gen, Encrypt and Decrypt**.

1) Set-up:- This algorithm takes as input a security parameter k and returns the system parameters PP together with the master secret key msk. The system parameter must include the description of the message space $\mathbb{M}$, the cipher text $\mathbb{C}$, the identity space $\mathcal{I}$ and the master public key. They are publicly known while the master secret key is known only to private key generator (PKG).

2) Key-Gen:- This algorithm takes as input a parameters PP together with identity $id \in \mathcal{I}$ and master secret key msk and outputs private key d_{id} using the master key. The identity *id* is used as public key while d_{id} is its corresponding private key.

3) Encrypt:- This algorithm takes as input an identity $id \in \mathcal{I}$, system parameters PP and message M and produces the output a ciphertext $C \in \mathbb{C}$.

4) Decrypt:- This takes as input system parameters PP, a ciphertext $C \in \mathbb{C}$, an identity *id* and corresponding private key d_{id} and returns the corresponding plaintext.

3. Security model for Identity Based Encryption Schemes

Security against adaptive chosen ciphertext attack is the acceptable notion of security for a public key encryption. This notion of security has been extended to the identity based setting by Boneh and Franklin [1]. This is termed as IND-ID-CCA model. The IND-ID-CCA model is described through the following game between the challenger $\mathcal{C}$ and the adversary $\mathcal{A}$..

Set-Up: The challenger takes input as a security parameter k and run the **Set-Up** algorithm. It provides adversary with system parameters PP and keeps the master key msk to itself.

Phase 1: Adversary makes a finite number of queries where each query is one of the following two types:

a) Key-extraction Query (*id*):- The challenger responds by running algorithm **Extract** to generate the private key d_{id} of *id* and returns it to the adversary.

b) Decryption Query (*id*,C):- The challenger responds by running the algorithm **Extract** to generate the private key d_{id} of *id*. Then it runs algorithm **Decrypt** to decrypt the ciphertext C using the private key d_{id}. It sends the resulting plaintext to adversary.

$\mathcal{A}$ is allowed to make these queries adaptively, i.e., any query may depend on the previous queries as well as their answers.

Challenge: when $\mathcal{A}$ decides that phase 1 is complete, it fixes an identity *id** and two equal length message M_0, M_1 under the constraint that it has not asked for the private key of *id** or any prefix of *id**. The $\mathcal{C}$ chooses at random a bit $y \in \{0,1\}$ and obtains a ciphertext C* corresponding to the M_y .It returns C* as the challenge ciphertext to adversary $\mathcal{A}$.

Phase 2: $\mathcal{A}$ now issue additional queries just like Phase 1, with the restriction that it can not place a decryption query for the decryption of C* under *id**. All other queries are valid and $\mathcal{A}$ can issue these queries adaptively just like Phase 1. The $\mathcal{C}$ responds in Phase 1.

Guess: Adversary $\mathcal{A}$ outputs a guess y' of y and wins the game if $y= y'$.
The advantage for the adversary $\mathcal{A}$ is given as a function of the security parameter k as follows:

$$Adv_{\mathcal{A}}(k)= |Pr[y= y']-1/2| \qquad (1)$$

We say that an identity based scheme is semantically secure against an adaptive chosen ciphertext attack (IND-ID-CCA), if no polynomially bounded adversary $\mathcal{A}$ has non-negligible advantage against the challenger.

4. Identity Based Encryption Schemes

We introduce the four major identity based encryption schemes based on bilinear pairing and quadratic residues.

4.1. Boneh and Franklin's IBE

Boneh and Franklin [1] proposed the first efficient and secure identity based encryption scheme. This scheme is semantically secure against adaptive chosen ciphertext attack under the Bilinear Diffie-Hellman assumption in the random oracle model.

1) Set-up: Given k. Generate cyclic groups G_1 , G_2 of prime order p together with bilinear map $e\wedge : G_1 \times G_1 \to G_2$ corresponding to k; Pick a random generator $P \in G_1$.

(a)Pick a random $s \in Z_p{}^*$ and set $P_{pub} = sP$.

(b)Choose cryptographic hash function $H_1 : \{0,1\}^* \to G_1{}^*$, $H_2 : G_2 \to \{0,1\}^n$, $H_3 : \{0,1\}^n \times \{0,1\}^n \to Z_p{}^*$, $H_4 : \{0,1\}^n \to \{0,1\}^n$ for some integer n>0.The master key is s and the public parameters is PP= $\langle G_1, G_2, e\wedge, p, n, P, P_{pub}, H_1, H_2, H_3, H_4 \rangle$.

2) Extract: Given $id \in \{0,1\}^*$, PP and s, compute $Q_{id} = H_1(id)$ and set the private key $d_{id} = s\,Q_{id}$.

3) Encrypt: Given a plaintext $M \in \mathbb{M}$, PP and a public key *id*, compute $Q_{id} = H_1(id)$

(a)Pick a random $\sigma \in \{0,1\}^n$, compute $r = H_3(\sigma, M)$ and $g = e\wedge(P_{pub}, Q_{id})$

(b)Finally ciphertext $C = \langle rP, \sigma \oplus H_2(g^r), M \oplus H_4(\sigma) \rangle$.

4) Decrypt: Given a ciphertext $\langle U,V,W \rangle \in C$, d_{id} and PP,

(a)Compute $g' = e\wedge(U, d_{id})$, $\sigma = V \oplus H_2(g')$ and Compute $M = W \oplus H_4(\sigma)$

(b)Compute $r = H_3(\sigma, M)$ Verify whether U=rP; if not reject C; else output M.

4.2. Sakai and Kasahara's IBE

We describe the modified version of Sakai and Kasahara's IBE [8] which was introduced by Chen and Cheng in [15].

1) Set-up: Given a security parameter k. Generate three cyclic groups G_1, G_2, G_T of prime order p, an isomorphism ψ together with bilinear map $e\wedge : G_1 \times G_1 \rightarrow G_2$. Pick a random generator $P_2 \in G_2*$ and set $P_1 = \psi(P_2)$ then Pick a random $s \in Z_p^*$ and compute $P_{pub} = sP_1$

(a)Choose hash function $H_1 : \{0,1\}^* \rightarrow Z_p^*$, $H_2 : G_T \rightarrow \{0,1\}^n$, $H_3 : \{0,1\}^n \times \{0,1\}^n \rightarrow Z_p^*$, $H_4 : \{0,1\}^n \rightarrow \{0,1\}^n$ for some integer n>0. The master key is s and the public parameters is $PP = \langle G_1, G_2, G_T, P_1, P_2\ e\wedge, p, n, \psi, P_{pub}, H_1, H_2, H_3, H_4 \rangle$.

2) Extract: Given identity $id \in \{0,1\}^*$, PP and s, compute $Q_{id} = H_1(id)$ and set $d_{id} = (1/s + Q_{id})P_2$

3) Encrypt: Given $M \in \mathbb{M}$, PP and id, Compute $Q_{id} = H_1(id)P_1 + P_{pub}$ and set $g^r = e\wedge(P_1, P_2)^r$

(a)Pick a random $\sigma \in \{0,1\}^n$ and compute $r = H_3(\sigma, M)$

(b)Set the ciphertext $C = (rQ_{id}, \sigma \oplus H_2(g^r), M \oplus H_4(\sigma))$.

4) Decrypt: Given the ciphertext $C = (U,V,W) \in \mathbb{C}$, *id* and d_{id} Compute $g' = e\wedge(U, d_{id})$

(a)Compute $\sigma' = V \oplus H_2(g')$, $M' = W \oplus H_4(\sigma)$ and $r' = H_3(\sigma', M')$.

(b) If $U = r'(H_1(id)P_1 + P_{pub})$, output M' else reject C.

4.3. Cocks' IBE

This scheme encrypts a data bit by bit and it requires (log*n*) bits of ciphertext per bit as described in [14]. It does not provide the proof of security in a security model as strong as one we have discussed. This scheme is not efficient and possibly not secure as the other schemes.

4.4. Authenticated IBE

Lynn [9] introduced the Authenticated IBE by modifying the Boneh-Franklin scheme to achieve the message authentication at no additional computational cost. In fact, authenticated encryption is more efficient. Receiver verifies the identity of the sender and whether or not the message has been tempered with, thus removing the need for digital signatures when authentication is required. Authenticated Encryptis is faster than plain encrypt because there is one less exponentiation and no point multiplications.

5. Performance Comparison of IBE Schemes

We have discussed four identity based encryption schemes including Cocks-IBE but the performance of the Cocks-IBE is very slow. So for this reason, for evaluating Encrypt algorithm performance and computational cost we focus only on the pairing based identity-based cryptographic schemes which are widely used in practice.

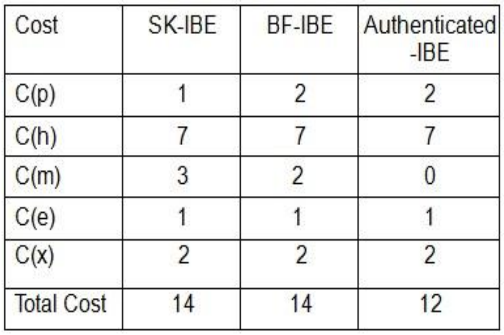
We note that exponentiation operation is equivalent to the point multiplication in elliptic curve cryptography (ECC) and multiplication is equivalent to the point addition in ECC. h- Chameleon hash operation is equivalent to one exponentiation. Notation used in this computation is as follows: P=Pairing operation, M=Modular multiplication, e=Exponentiation in G, m=Scalar or Point Multiplication in G, x=XOR operation, h= Hashing, $C(\theta)$=Computation cost of operation θ.

5.1. Performance Comparison on Encryption Algorithm and Computational Cost

Based on our observation we have observed that SK-IBE scheme has the better performance than other two schemes BF-IBE and Authenticated-IBE particularly in encryption. SK-IBE is faster than BF-IBE and Authenticated-IBE in two aspects. First, SK-IBE needs no pairing computation in Encrypt algorithm because $e\hat{}(P_1,P_2)$ can be pre-computed. Second, in the operation of mapping an identity to an element in G_1 or G_2 ,the map-to-point algorithm used by BF-IBE is not required because simple hash function is used in SK-IBE to maps an identifier to an element in Z_p^* .

We have evaluated the computational cost of the three schemes and have found that the computation cost of SK-IBE and the BF-IBE is same and the Authenticated-IBE cost is near about the SK-IBE and BF-IBE. As we know that in the Extract algorithm of BF-IBE and Authenticated-IBE, an identity string is mapped to a point on an elliptic curve and the corresponding private key is computed by multiplying the mapped point with the master key of public key generator (PKG) and Extract algorithm of SK-IBE requires much simpler hashing than the BF-IBE and Authenticated-IBE so the computational cost is reduced and therefore improves performance. It maps an identity string to an element $h \in Z_p^*$ instead of a point on an elliptic curve. The computational cost of SK-IBE, BF-IBE and Authenticated-IBE and performance graph of all the schemes has been given in Table 1 and Figure 1.

Table 1. Computational Cost



Cost	SK-IBE	BF-IBE	Authenticated -IBE
C(p)	1	2	2
C(h)	7	7	7
C(m)	3	2	0
C(e)	1	1	1
C(x)	2	2	2
Total Cost	14	14	12

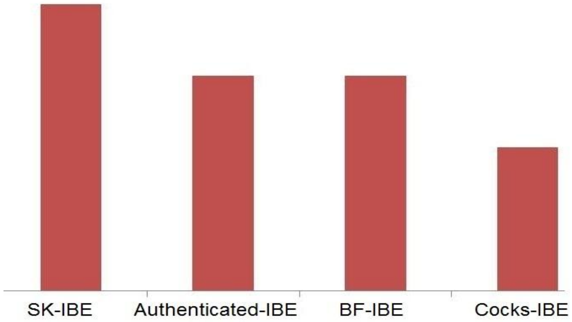


Figure 1. Performance Graph

6. Definition of Identity Based Signature

Identity based signature is the mirror image of the identity based encryption. It consists of the four algorithms **Set-up, Extract, Signature Generation and Signature verification.** In this scheme signer first obtain her private key associated with her identity and then she generates a signature for message and sends it to receiver. After receiving the signature and message the receiver checks the signature using the signer identity and PKG public key. If it is, he returns "*Accept*" otherwise he returns "*Reject*".

7. Security model for Identity Based Signature Scheme

Security against existential forgery under adaptively chosen message and id attack for an id–based signature scheme which consist of **Setup, Extract, Signature Generation and Signature Verification** algorithms is defined through the following game between a challenger $\mathscr{C}$ and adversary $\mathscr{A}$.

Set-Up: Challenger runs **Setup** algorithm and it provides adversary with system parameters PP while keeping the master key msk to itself. Adversary $\mathcal{A}$ issue the following queries as he wants:

a) Hash function query: Challenger computes the value of the hash for the requested inputs and sends the value to adversary.

b) Extract Query: Challenger responds by running algorithm **Extract** to generate the private key d_{id} of *id and returns it to the adversary.*

c) Sign Query: Given an identity id and message M, challenger responds by running algorithm **Signature Generation** to generate the signature of id.

Adversary $\mathcal{A}$ outputs (id,M,σ), where *id* is an identity, M is an message and σ is an signature such that *id* and (id,M) are not equal to the inputs of any **Extract** and **Sign queries** respectively. Adversary wins the game if σ is a valid signature of M for identity *id*.

Existential forgery under adaptively chosen message and *id* attack is the factor under which identity based signature scheme is secured if no polynomially bounded adversary has non-negligible advantage in this game.

8. Identity Based Signature Schemes

We introduce the major identity based signature schemes based on the integer factorization and bilinear pairing.

8.1. Shamir's Identity Based Signature

Shamir proposed the identity based signature scheme [3] in 1984 based on the integer factorization mechanism. The security of this scheme is based on the computational hardness of the integer factorization problem, i.e given a large positive integer, finding its prime factorization is computationally infeasible.

8.2. Hess's Identity Based Signature

Hess proposed the identity based signature scheme [10] in 2003. The security of this scheme was proved under CDHP assumption in the random oracle model.

1) Set-up: PKG computes P_{pub}=s.P, where $s \in Z_q^*$ and master key is s. It chooses $H_1:\{0,1\}^* \rightarrow G_1$ and $H_2:\{0,1\} \times G_1 \rightarrow Z_q^*$. The system parameters are $\langle q, G_1, G_2, e\hat{}, P, P_{pub}, H_1, H_2 \rangle$.

2) Extract: Give *id*, PKG generates d_{id} for identity as d_{id} =s.Q_{id} , where Q_{id}= H_1 (*id*)

3) Signature Generation: To sign a message m, signer performs the following steps:

(a)Choose at random $P_1 \in G_1^*$, picks a integer at random $k \in Z_q^*$ and compute r= $e\hat{}(P_1,P)^k$

(b)Compute v=h(m,r), U=v d_{id}+k P_1 and Generate signature σ= (U,v)

4) Signature Verification: To verify signature σ=(U,v) on message m, user performs the following steps: Compute r= e^(U,P) $e\hat{}(Q_{id},- P_{pub})^v$, If v= h(m,r), return "*Accept*" otherwise "*Reject*"

8.3. Cha-Cheon's Identity Based Signature

This scheme is completely secure against existential forgery under adaptively chosen message and ID attack in the random oracle model assuming the hardness of CDHP. Signing phase of this scheme is very efficient as it does not require pairing operation as described in [11].

8.4. Barreto's Identity Based Signature

This scheme can benefits from the most efficient pairing calculation technique for a larger variety of elliptic curves than previous schemes as described in [12]. This identity based signature is faster and significantly more efficient at verification because its verification algorithm requires a single pairing calculation.

1) Set-up: The PKG specifies a groups (G_1, G_2,G_T) generated by $P\in G_2$,$T=\psi(P)\in G_1$, g= e^(P,T) and two hash function $H_1:\{0,1\}^*\rightarrow Z_q^*$, $H_2:\{0,1\}\times G_1\rightarrow Z_T^*$. The PKG then selects s at random and computes $P_{pub}=s.P\in G_2$. Finally PKG publish the description of Groups and hash functions H_1, and H_2 as well as PKG. PP=$\langle G_1, G_2, G_T$, e^ , T, g, P_{pub} , ψ, H_1, $H_2\rangle$.

2) Extract: Given identity *id*, the PKG generates a private key for identity, d_{id} =[1/(Q_{id} +s)]P.

3) Signature Generation: To sign a message m, signer performs the following steps:

(a)Choose a random $x\in Z_q^*$, compute $r=g^x$ and Set h= H_2 (m,r)$\in Z_q^*$.

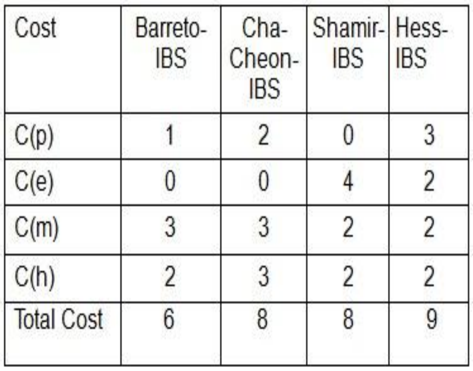
(b) Compute d=(x+h) d_{id} and Generate the signature on m is σ=(h,d)$\in Z_q^*\times G_1$

4) Signature Verification: A user verifies the signature as follows:
If h= H_2 (m, e^(d, Q_{id} P+ P_{pub})g^{-h}) then accept the signature otherwise reject.

9. Performance Comparison of IBS Schemes on Computational Cost

We have used the same notation as in section 5 to evaluate the computational cost of four identity based signature schemes and the result have been shown in Table 2 and Figure 2.

Table 2. Computational Cost



Cost	Barreto-IBS	Cha-Cheon-IBS	Shamir-IBS	Hess-IBS
C(p)	1	2	0	3
C(e)	0	0	4	2
C(m)	3	3	2	2
C(h)	2	3	2	2
Total Cost	6	8	8	9

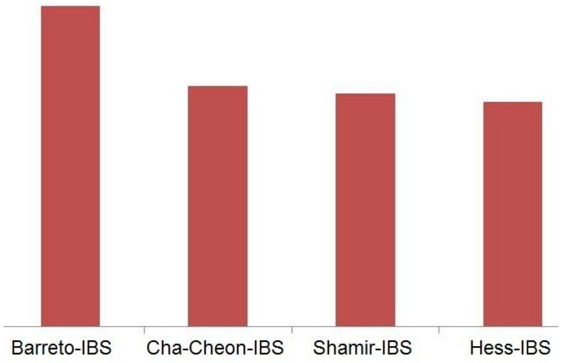


Figure 2. Performance Graph

10. Conclusions

We have evaluated the Encryption algorithm performance and computational costs of all four major IBE schemes. Moreover the computational costs of all four major Identity based signature schemes has also been evaluated. On light of this we have come to an conclusion that the schemes based on the bilinear map is much more secure and has high performance specially the one that is based on bilinear pairing having simpler hashing used in the Extract algorithm.

Acknowledgements

We thank Anu Kumari, Anshul Verma and Deepu Kumar for their contribution and sharing their insight in this work.

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2011-0023076) and 2012 ADD project.

References

[1] D. Boneh and M. Franklin, “Advance in Cryptology”, Proceedings of CRYPTO 01, **(2001)** August 19-23, California, USA.

[2] Y. Desmedt and J. -J. Quisquater, “Advance in Cryptology” Proceedings of CRYPTO 86, **(1986)** August 11-15, California, USA.

[3] A. Shamir, “Advance in Cryptology”, Proceedings of CRYPTO 84, **(1984)** August 19-22, California, USA.

[4] H. Tanaka, “Advance in Cryptology”, Proceedings of CRYPTO 87, **(1987)** August 16-20, California, USA.

[5] S. Tsuji and T. Itoh, IEEE Journal on Selected Areas in Communication, vol. 7, no. 4, **(1989)**.

[6] U. Maurer and Y. Yacobi, “Advance in Cryptology”, Proceedings of Eurocrypt 91, **(1991)** April 8-11, Brighton, UK.

[7] D. Huhnlein, M. Jacobson and D. Weber, “Selected Areas in Cryptography”, Proceedings of SAC 2000, **(2000)** August 14-15, Ontario, Canada.

[8] R. Sakai and M. Kasahara, Cryptology eprint Archieve.054 **(2003)**, http://eprint.iacr.org/2003/054.

[9] B. Lynn, Cryptology eprint Archieve.072 **(2002)**, http://eprint.iacr.org/2002/072.

[10] F. Hess, “Selected Areas in Cryptography”, Proceedings of 9th Annual International Workshop of SAC 2002, **(2002)** August 15-16, Newfoundland, Canada.

[11] J. Cha and J. H. Cheon, “Public Key Cryptography”, International Workshop on Practice and Theory on Public Key Cryptography, **(2003)** January 6-8, Florida, USA.

[12] M. Barreto, B. Libert, N. McCullagh and J. Quisquater, “Advance in Cryptology”, Proceeding of ASIACRYPT 2005, **(2005)** December 4-8, Chennai, India.

[13] R. Sakai, K. Ohgishi and M. Kasahara, “Cryptography and Information Security”, The 2001 Symposium on Cryptography and Information Security, **(2001)** January 23-26, Oiso, Japan.

[14] C. Cocks, “Cryptography and Coding”, Proceedings of the 8th IMA International Conference on Cryptography and Coding, **(2001)** December 17-19, Cirencester, UK.

[15] L. Chen, Z. Cheng, “Cryptography and Coding”, Proceedings of 10th IMA International Conference, **(2005)** December 19-21, Cirencester, UK.

Authors

Arjun Kumar

Arjun Kumar completed his B.Tech in Computer Science and Engineering from Indian Institute of Technology Guwahati, India in 2010. He is pursuing his master degree in Computer Science majoring Cryptography and Network Security at Dongseo University, Busan, South Korea. He has several research interests. Among which his prominent research interests are Cryptography, Cloud Computing Security and Secure Wireless Sensor Network.

HoonJae Lee

HoonJae Lee received his BS, MS, and PhD degrees in electronic engineering from Kyungpook National University, Daegu, Korea in 1985, 1987, and 1998, respectively. He is currently a professor in the School of Computer & Information Engineering at Dongseo University. From 1987 to till date, he was a research associate at the Agency for Defense Development (ADD). He has more than 150 national/international technical publications as well as about 50 patents. His current research interests include developing secure communication system, secure Wireless Sensor Network, and Side-Channel Attack.