【붙임 Global Ph.D Fellowship 신청서류 양식】

Documents to be submitted for 2011 Global Ph.D. Fellowship Program

No.	Documents	Guidelines
1	Cover of Application (Form A101)	○ Fill out the web form
2	Introduction of Applicant (Form 2)	○ Fill out the web form
3	Academic Plan and Research Proposal (Form 3)	○ Fill out the web form
4	Academic Transcripts (Form 4)	○ Fill out the web form ○ University transcript (including a certified copy of the official transcript) must be scanned and uploaded onto the NRF system
5	Research Achievements (Form 5)	○ Fill out the web form ※ supporting documents must be submitted through the NRF system
6	Reason for choosing the University(Form 7)	○ Fill out the web form

※ Go to http://ernd.nrf.re.kr for online application submission.

- First, sign up for membership on the Korean Researcher Information website (www.kri.go.kr) and change status to researcher.
- Then, log on to http://ernd.nrf.re.kr with the KRI ID.

※Personally identifiable information including applicant name, university and advisor should not be exposed on the documents (Otherwise, the applicant shall be immediately disqualified from the process.)

※ Additional documents to be submitted

- **For Applicant**: Academic transcript(Undergraduate), Certificate of Enrollment (Must be scanned and uploaded onto the NRF system)
- **For Recommenders**: Letters of Recommendation (from 2 people)

【Form 1】

Cover of Applicant

※ *Fill out the web form*

【Form 2】

Introduction of Applicant

1. Personal Background

● I am a Positive Intelligence

Whenever I encounter difficulties in my life, I don't feel frustrated. Instead, I say to myself, "That's ok. It will be well. Just try it." Surprisingly, after reciting these words, I feel calm and comfortable and finish the work successfully. I believe this is power of positivity, and with this attitude I can do anything. My graduate school life is not an exception in this case. Sometimes, an experiment does not show great results and may even be poorer than previous methods. However, I think this is part of the process of success, not failure, and I try again and again. Finally I overcome and achieve great results. During my doctorate program, I will keep my positive mindset and continue with my work.

● I believe that talent is the desire to practice and that it's attitude that counts

After finishing my military service, I knew nothing whatsoever about my major or English. In my first mid-term examination, I almost got the lowest score in class. It shocked me, because it was the first time to be second to last in the class. I took time for self-examination and I decided to study harder. After that day, I got up at 5 am every morning and studied until the library closed, from Monday to Sunday. I even memorized all the materials in the textbook for better understanding. I also read English magazines, including Harvard Business Review, Times and the Economist. And every week I memorized one article and recorded a video clip to practice English presentations. Starting in 2009, I recorded about 100 video clips and uploaded them to my blog [1]. This effort paid off, and I got a high score in my major and won prizes in English speech contests. As recently as last year, I was selected as one of the excellent students in 2011 by Brain Korea 21.

● I believe in TEAM, Together Everyone Achieves More

In modern society, we face more complicated and complex problems than previous years. A person's time and power is limited, so solving problems alone is hard. Sometimes it is even impossible. However, if we believe others and work together, we can solve our problems and bring about good results. I engraved these words into my mind, so that I can always prefer working with others. Through teamwork, we can exchange advice and are encouraged by each other. As a result, I finished many team projects and won many prizes in competitions.

Fig. 1. Achievements.

2. Purpose going on the doctor's course

(A) (B) (C)

Fig. 2. (A) Development of cryptography library, (B) Hosting the international conference, (C) Promoting world class security laboratory.

● **Development of cryptography library for technology transfer**

During my master's degree, I developed many cryptography libraries over sensor networks which included HIGHT, HUMMINGBIRD1, HUMMINGBIRD2, and Elliptic Curve Cryptography. I want to combine my previous implementations and develop a much more sophisticated design and technique than previous results. The results will improve the speed and size of cryptography technology.

The cryptography library will be used for various purposes. In an industrial field, it can be directly applied to applications and products, so that technology can contribute to our country as technology transfer to industrial area and secure our network environments. In education, my research results and methods can be used as a study and as a foundation for future research.

● **Hosting international conference**

I participated in the CHES2011, ASIACRYPT2011, ICISC2011, and INDOCRYPT2011 conferences last year. During the conferences, I felt that international conferences are fantastic and important events for experts in the field. Many renowned scholars, professors, and students working in the security sector gather together and share knowledge and experiences efficiently within a short period of time. I thought that if we host a famous international conference, it will draw international attention and improve the security field significantly in our country. My professor, many research collaborators, and I have proposed hosting CHES2014 in Busan. I have confidence that we can hold a CHES conference in the near future, if we devote our time to security research.

● **Promote world class security laboratory**

My laboratory was started four years ago. From the first year, my professor and laboratory members conducted a lot of research on a wide range of security fields including the security of ZigBee, Smart Grids, electronic vehicles, and DASH7. We had great results and achievements. If we continue to make progress in the security field, our laboratory will become renowned throughout the world. However, Korea still does not show strength in the field of security. I am eager to improve security technology in Korea. To succeed in this endeavor, I will complete my research and projects, collaborate with other laboratories, and pass on know-how to junior students in my school.

3. Reason for applying for fellowship

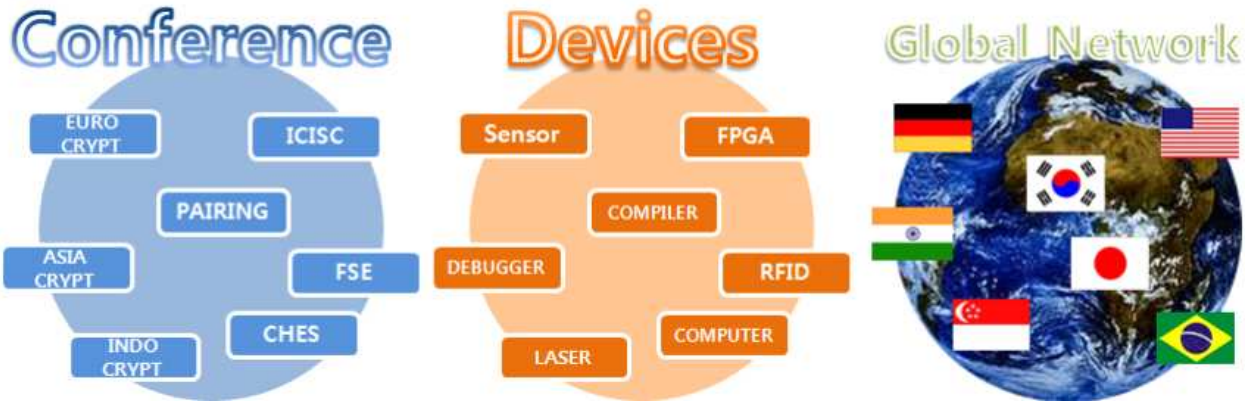

Fig. 3. Attendance at international security conferences, devices required for experiments, and global friend network.

● Attending conferences

While studying for my master's degree, I participated in seven international conferences and thirteen domestic conferences. These events gave me ideas and inspiration to study harder. If I have enough money for transportation, accommodation, registration, and living expenses, I want to attend as many conferences as possible. First, I will focus on international cryptography conferences. These conferences provide opportunities to communicate with renowned foreign scholars. This can be a chance for collaboration.

● Devices and software purchases

To test and simulate implementations, I need to have target board and simulation tools. The former consists of a sensor network mote for testing embedded microprocessors and field programmable gate arrays (FPGA) for implementing hardware design. The latter consists of simulation tools and compilers for embedded systems and hardware implementations. Both products are expensive because of their special purposes. Therefore, funds for experiment devices are needed for stable work in my field.

● Collaboration with foreign and domestic scholars

Today we can communicate with foreign and domestic scholars through the Internet and phone. However, meeting in person is a much effective way to share and collaborate on projects and research with others. Therefore, I want to invite foreign and domestic scholars to my laboratory as exchange scholars and visit their laboratories to work and study together.

4. References

[1] Presentation Homepage, *"http://moojukschool.blogspot.com"*

【Form 3】

Academic Plan & Research Proposal

1. Academic Plan

1. Reason and background for choosing the department and major

Fig. 1. Security crisis in computer systems

● **Critical condition of computer security**

Nowadays many cyber attacks are committed by malicious users. The methods have diverged and are getting complicated. The attacks, from hacking to physical attacks, threaten the financial and information safety of normal users. The hackers attack the vulnerabilities of computer system or security holes to obtain root permissions. Then the system can be used for malicious purposes. In the case of physical attacks, malicious users can access a system in person and conduct attacks more efficiently. After conducting physical attacks, the adversary can obtain a user's secrets, such as the information necessary to withdrawal money from a user's bank account.

● **Importance of computer security**

If we don't construct robust and secure computer systems, our national defense and many applications could be exposed to malicious attacks. A breach of national security could be catastrophic. First, all financial transactions will be shut down and accounts will be hacked. Second, national defense will collapse and North Korea could take military advantage. Third, our smart phone communications could be intercepted by an adversary. In short, our normal life cannot continue any more. For these reasons, security is an important factor for the individual and the nation.

● **Solution for computer security**

During my doctorate program, I will study computer security, especially the implementations of secure and efficient hardware and software. I will work to solve security problems and contribute to a robust and secure IT application environment by developing cryptography technology with tamper resistance.

2. Research advisor

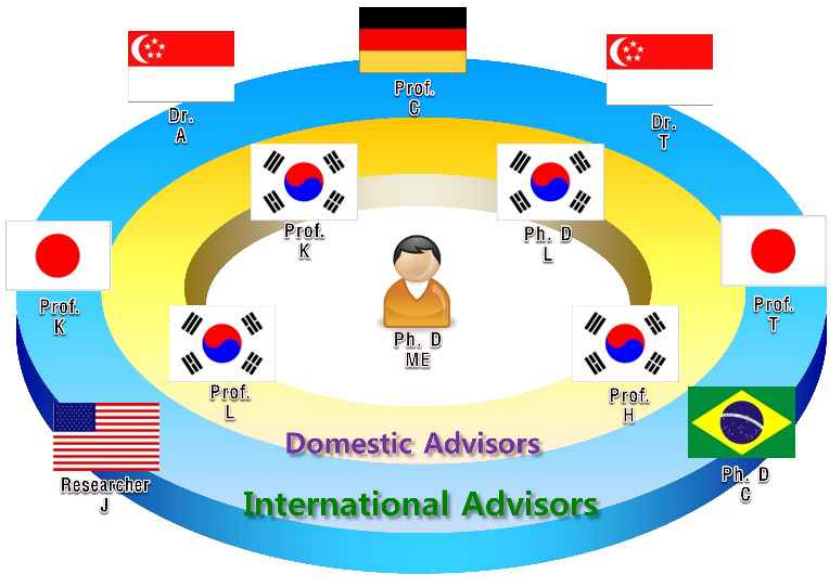

Fig. 2. Research advisor pool.

● Prof. K(Korea)
Security in hardware and sensor networks

● Prof. C(Germany)
Security in embedded applications

● Prof. K(Japan)
Cryptanalysis, Cryptography

● Prof. L(Korea)
Fast Software algorithms for cryptographic implementations

● Prof. H(korea)
Physical attacks against real world systems

● Prof. T(Japan)
Security in mobile and ad-hoc networks

● Dr. T(Singapore)
Fast software algorithms for cryptographic implementations

● Dr. A(Singapore)
Fast software algorithms for cryptographic implementations

● Ph.D. L(Korea)
Security in hardware and Countermeasure of physical attacks

● Ph.D. C(Brazil)
Fast software implementation for sensor networks

● Researcher. J(USA)
Sensor and ad-hoc network for DASH7

3. Academic objectives

● **Intensive research on security area**

While I was an undergraduate student, I studied a wide range of computer science including computer architecture, computer programming, data structure, and networking. However, as I started my master's degree, I have focused only on security, especially cryptography for hardware and software implementations. Now I am much more familiar with one specific area, and have became a security expert in cryptography. My knowledge of both basic computer science and cryptography go well together, and provide me with a strong academic background for my Ph.D. program. I will continue research along the lines of my previous security achievements and also challenge physical protection to provide tamper resistance.

● **Submission for renowned and famous journals**

I published papers in domestic journals with a low impact factor during my master's studies. This is a good method for a beginner to learn how to write papers. However, the papers have low practical use and research value. I will target famous and renowned journals and conferences including IACR and the IEEE computer society for future papers. This will introduce the excellence of my laboratory to the whole world, so I can have an opportunity to work with other scholars to get great results. To prepare for this, I will read many papers published in famous journals and choose research topics depending on the characteristics of conferences. In IACR conferences, the subjects are cryptanalysis, HASH functions, the software and hardware implementations of cryptography, public key cryptography, and pairing. There are a lot of subjects and topics, so I will choose a specific topic and focus on it.

● **Development of security solutions**

I implemented many cryptography techniques and methods but I didn't release security solutions, because I only partially implemented all the techniques due to a lack of time and knowledge. Nowadays, many cryptography libraries which use efficient computations are available on the Internet. During my doctorate studies, I will refine my techniques and methods to create a complete, efficient security solution. Also I will not study alone, but collaborate with leading laboratories for better results. Currently, Tinypbc has advanced cryptographic technology in sensor networks, and I am now in contact with a project member of the Tinypbc project [1]. In the future, I will collaborate with him to create an advanced cryptographic solution.

● **Practical Research**

During my master's studies, I focused on what I wanted to know and I was interested in, so I sometimes developed infeasible security protocols, including military security protocols. However, in my doctorate studies, I will focus more on practical research topics and what is necessary in our society. I think the most practical and necessary topic right now is a security library for hardware and software implementations of cryptography with tamper resistance. I want to contribute to my nation to repay it for its devotion and dedication to students.

4. References

[1] L. Oliveira, M. Scott, J. Lopez, and R. Dahab, *"TinyPBC: Pairings for Authenticated Identity-Based Non-Interactive Key Distribution in Sensor Networks,"* Fifth International Conference Networked Sensing Systems, pp. 173-180, June 2008.

2. Research Proposal

1. Research Title: Cryptographic Technology on Resource Constrained Environment

● Motivation and Research Background

Research on cryptography technology in a resource-constrained environment has been conducted all over the world for decades due to the growing demands of embedded systems and low-power devices. However, this research has not been conducted in Korea, so our technology is lagging behind that of countries such as France, India, China, and Brazil. For the wide range of IT applications including smart grids, vehicular networks (VANET), and national defense, secure and robust cryptography technology should be implemented using efficient and enhanced methods over resource constrained devices.

The research area includes hardware, software and tamper protection technology. In the case of hardware, small chip size and high throughput is required with complete security functions including public key, symmetric key cryptography, random number generator and hash function. In the software technology area, implementing the cryptography with small code size and low total clock per instructions (CPI) is needed. Tamper-protection technology protects chip modules against invasive and non-invasive attacks. Details follow.

a. Hardware Cryptography Implementation

To implement hardware cryptography, chip designers should follow implementation flow. Fig. 1. illustrates the detailed process. First, a chip programmer presents design ideas and specifications. Second, the design is described in verilog or VHDL and then verified. Next, the process diverges into two directions. The first flow is a Field Programmable Gate Array (FPGA), which is an integrated circuit designed to be configured by the customer or designer after manufacturing. The verified design can be downloaded to an FPGA chip. The second, Application Specific Integrated Circuit (ASIC), is an integrated circuit customized for a particular use, rather than intended for general-purpose use. In the case of ASIC, layout and chip fabrication processes are required to get results.

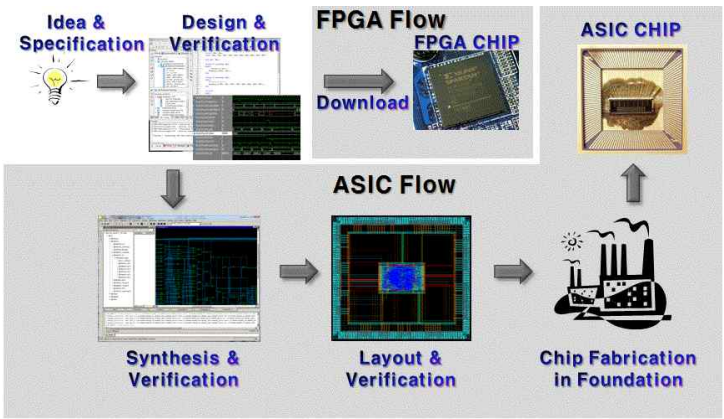

Fig. 1. Hardware implementation flow

b. Software Cryptography Implementation

For optimized software implementation, a programmer needs to follow the flow depicted in Fig. 2. First the programmer determines and specifies a cryptography algorithm. Second, it analyzes the features of a target board including an instruction set,

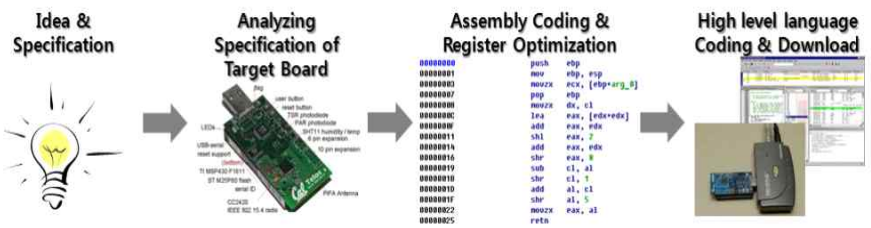

Fig. 2. Software implementation flow

general registers and word size. Third, critical operations such as arithmetic and bit operations are implemented in assembly code fully utilizing general registers. Lastly, assembly code is combined with high level languages and then downloaded to the target board.

c. Tamper Protection Technology

For tamper resistance technology, designers should combine two other technologies. The first method is additional logic protection including memory access protection and crypto-coprocessors. The second method is chip fabrication technology. In the process of fabrication, a designer can define the specification of a chip including layers and the size of transistors to block the attacks.

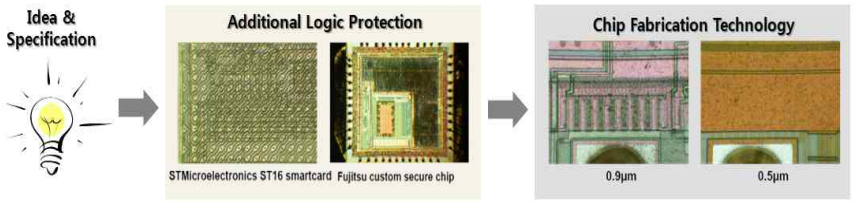

Fig. 3. Tamper protection implementation flow

● Project plan for Global Fellowship

During my doctorate program, I will conduct research on efficient hardware design for cryptography technology and upgrade my previous research results in software implementation of elliptic curve cryptography technology over embedded devices.

The technology will be applied to a wireless network environment, DASH7 standard [1], VANET, and smart grids. These results will contribute to creating secure and robust IT application environments.

The quantitative objectives are publishing **six SCI papers** and **twelve domestic journal papers** as a result of my research topic.

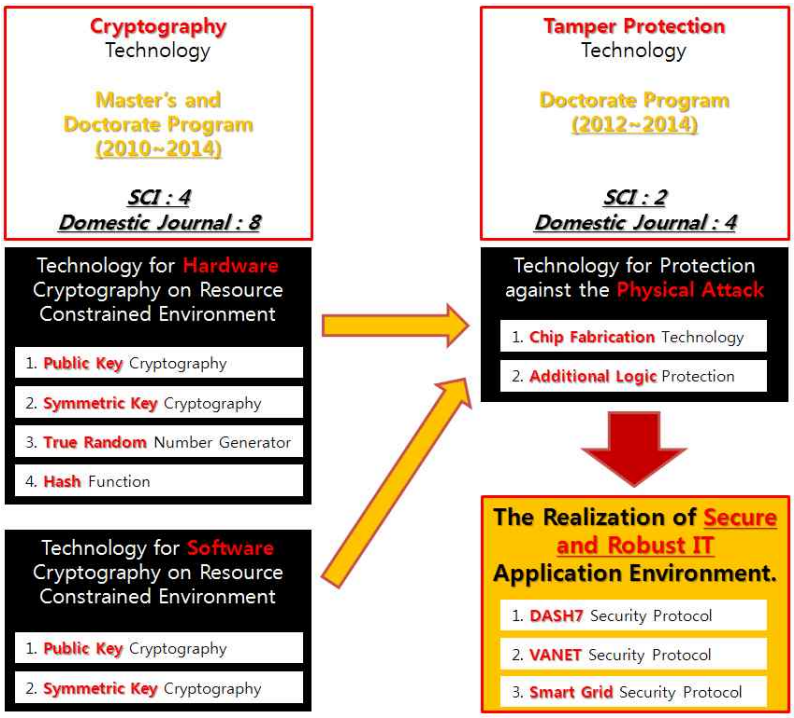

Fig. 4. Plan of master's and doctoral programs

2. Objective plan

● Hardware Cryptography on Resource Constrained Environment

Scalability together with interoperability represents one of the most critical requirements of cryptographic applications [2]. According to Tenca and Koc [3], scalability of an arithmetic unit is when "The unit can be used or replicated in order to generate long-precision results independently of the data path precision for which the unit was originally designed." Therefore, I will put effort to fulfill the requirements, conducting research.

In public key cryptography, Elliptic Curve Cryptography (ECC) has a much shorter key-length than RSA. 1937-bit key size RSA has an equivalent security as a 190-bit key size ECC. Therefore, I will consider ECC as a research area. To optimize an ECC hardware

implementation, a scalable and unified architecture for arithmetic module including multiplication and inversion and deploying an array of word size processing units organized in a pipeline methods will be applied to hardware implementation.

In symmetric key cryptography, Data Encryption Standard (DES) consumes only about 6% of the logic resources of Advanced Encryption Standard (AES) and has a shorter critical path. However, optimized AES implementation requires only 3,400 gate equivalents and encrypts plain-text within 1,032 clock cycles [4]. Both have unique features so that they can be used for different purposes. The chip size and clock cycles are determined by substitution boxes (S-boxes). I will adjust the S-boxes and the arithmetic module to decrease the gate complexity of symmetric cryptography.

In a security module, TRNG is necessary to generate a random number for the initial vector and nonce. However, a random number with high entropy demands an analogy and a large circuit. To reduce chip size and replace the analogy of the digital circuit, I will present a novel approach to electronic circuit-based TRNG, which provides reasonable randomness and chip size using the metastablility characteristic [5].

Now, SHA3 is under competition for the next hash function. This coming August, NIST will announce the next HASH function. Many factors need to be considered including application scenarios, target technologies, and optimization goals. For the final round of the competition, I will compare SHA3 finalists to assist NIST with performance evaluation data on hardware platforms.

● **Software Cryptography on Resource Constrained Environment**

Various target boards equipped with 4, 8, 16 and 32-bit microprocessors are available for different applications. Each microprocessor has their own instruction sets, number of general purpose registers, and word length. For high performance and low power consumption, fully utilizing the capability of target boards is recommended.

In public key cryptography, the efficiency of the finite field arithmetic, especially field multiplication, determines overall efficiency. During my master's studies, I proposed efficient multiplication methods for reducing memory accesses. During my doctorate program, I will upgrade previous results in multiplication and expand them to other platforms. To optimize the implementation, I will analyze the specification of the target board including general purpose registers, instruction sets, and peripheral modules, and then utilize the capabilities and set the strategy for efficient computation flow.

In the case of symmetric key cryptography, arithmetic and bit operations are conducted with different word lengths. Depending on the word size of the platform, optimization methods diverge. If word size is longer than the length of the platform, it is divided into small blocks. Conversely, it can be combined with two or three blocks. In the process of permutation and substitution, a pre-computation method can reduce the clock cycles but increase code size. I will find an efficient design for both speed and size.

● **Protection against the Physical Attack**

Tamper-resistant microprocessors are used to store and process private or sensitive information. To prevent an adversary from deleting and modifying information, the chips are designed so that accesses to the memory and data are not available.

In the process of chip fabrication, planarization produces a chip smaller than 0.5 μm, and re-allocating building blocks obstructs tracing the data paths and covering multiple metal layers block direct access [6]. I will make physical attacks infeasible by adopting methods which complicate chip design and blocks access.

The second method is additional logic protection. Installing internal clocks and power supply pumps, memory access protection, and crypto-coprocessors can protect chips from attack. I will also study and upgrade previous techniques to propose more secure and robust countermeasures to attack.

3. Expected impact

My research area will contribute to both industrial and academic cryptography technology. The methods will be adapted to practical applications to make the environment secure and academic achievements derived from research experiments will improve previous work and be published in SCI indexed journals.

● **Secure and Robust IT Application Environment**

a. Establishment of DASH-7 Security Standard

The DASH7 standard is one of the promising wireless network standards[1] and our laboratory participates in the security aspect of the DASH7 project to define efficient public key-based key management and key distribution in order to make transmission data secure. I will apply my implementation results to the DASH7 to provide efficient computation on resource-constrained devices for software cryptography.

b. Secure and Robust Vehicular Network

Hardware implementing Elliptic Curve Cryptography is well used for VANET, through which the amount of sensitive and critical information is transmitted safely. If a malicious user intervenes and modulates the information, it will lead to car accidents. Currently, many vehicle companies are developing security modules for VANET to protect against adversaries. My research results, technology for hardware cryptography and tamper protection technology, can contribute to a secure and robust vehicular network.

c. Implementing End-to-End security for Smart Grid

Building end-to-end security is one of the important matters to implement smart grid technology. Currently, smart meters are installed in the home and are easily reachable. This exposes them to physical attacks. My research results related with tamper protection will protect smart meters from physical threats and optimized cryptographic implementation efficiently encrypt plain text which is useful for dense traffic networking environments.

4. References

[1] DASH7 Alliance Description, Available at "*http://www.dash7.org*".

[2] L. Batina, S. B. O¨ rs, B. Preneel, and J. Vandewalle. "*Hardware architectures for public key cryptography,*" Elsevier Science Integration the VLSI Journal, pp. 1-64, 2002.

[3] A. F. Tenca and C¸ . K. Ko¸c. "*A scalable architecture for Montgomery multiplication,*" Ches 1999, pp. 94-108, 1999.

[4] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "*A Survey of Light weight Cryptography Implementations,*" IEEE Design & Test of Computers, pp. 522-533, 2007.

[5] Majzoobi, M., Koushanfar, F., Devadas, S., "*FPGA-based True Random Number Generation using Circuit Metastability with Adaptive Feedback Control,*" CHES 2011, pp. 17-32, 2011.

[6] Physical Attacks on Tamper Resistance: Progress and Lessons, Available at "*http://www.cl.cam.ac.uk/~sps32/ARO_2011.pdf*".

【Form 4】

Academic Transcript

※ *Fill out the web form*

【Form 5】

Major Research Achievements

1. Major research achievements

☐ Achievements : Performance Enhancement of TinyECC based on the Multiplication Optimizations

○ Summary

1. Abstract

In the paper, we present **multiplication techniques** for elliptic curve cryptography over a 16-bit processor, MSP430[1].

2. Primary Content & Summary

● Cached Operand

For multiplication we use three registers for results and three for pointers out of twelve general purpose registers. I used the remaining six registers for cached operands. The method reduces the number of memory accesses for operand allocation.

● Reordered Partial Products

To maximize the incremental addressing mode, the order of partial products is rearranged. Since the order of access to registers does not take additional overhead, the order of partial products can be changed without additional overhead.

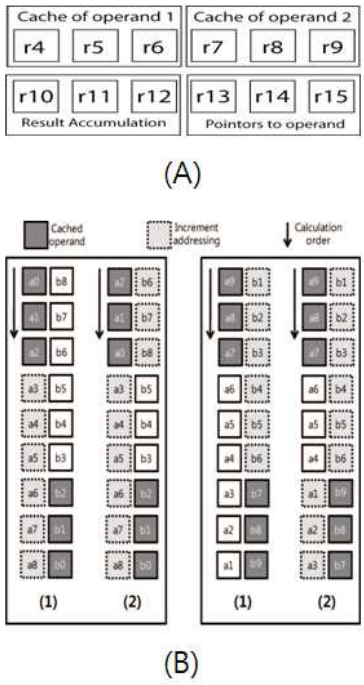

Fig. 1. (A) Cached Operand, (B) Reordered Partial Products, (1) and (2) are previous and proposed method

3. Evaluation

The proposed method shows that the latency of polynomial multiplication, which is the core operation of the ECC, is 6% smaller than previously known best results [2] by reducing the number of memory access.

4. Applicant's role and importance

As a lead author, I proposed a research paper about Multi-precision Multiplication and it was accepted in the **SCI-E journal** ***"Security and Communications Networks"***, which has an **impact factor** of **0.356**.

5. References

[1] Texas instruments, *"MSP430 Ultra-Low-Power Microcontroller,"* Texas Instruments, 2008.

[2] Conrado Porto Lopes Gouvêa, Julio López, *"Software Implementation of Pairing-Based Cryptography on Sensor Networks Using the MSP430 Microcontroller,"* Progress in Cryptology INDOCRYPT 2009, LNCS 5922, pp. 248-262, 2009.

□ Achievements : ZigBee Security For Home Automation Using Attribute-Based Cryptography.

○ Summary

1. Abstract

The paper presents Attribute Based Cryptography(ABC) for ZigBee networks.

2. Primary Content & Summary

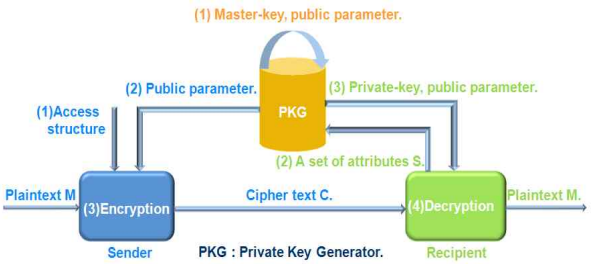

Fig. 1. Attribute-based encryption scheme

Fig. 2. Home automation using Attribute-based encryption

● **Attribute-Based Encryption(ABE)**

Attribute-based encryption encrypts and decrypts a cipher-text with access structures. The detailed working principle is depicted in Fig. 1.

● **Home automation using ABE**

The method provides strong features in home automation for the management of various electronic devices with a small number of keys. Fig. 2. shows an example of home automation using ABE.

3. Evaluation

Compared with ZigBee in terms of the number of keys, ABE reduces the number of keys to $O(n)$, and provides ease of managing the keys because a key is determined by each user's specific attributes. The feature is also useful to distribute the overhead of Trust center[2, 3].

4. Applicant's role and importance

As a lead author, I proposed a research paper about ZigBee Security For Home Automation and it was published at an IEEE conference, *"International Conference on Consumer Electronics(ICCE) 2011".*

5. References

[1]John Bethencourt, Amit Sahai and Brent Waters, *"Ciphertext-policy attribute-based encryption,"* In IEEE Symposium on Security and Privacy, pp 321-334, 2007.

[2]Son Thanh Nguyen and Chunming Rong, *"ZigBee Security Using Identity-Based Cryptography,"* Lecture Notes in Computer Science, Vol. 4610, pp. 3-12, Aug. 2007.

[3]Boneh, D., Franklin, M. *"Identity-based Encryption from the Weil Pairing,"* CRYPTO 2003. LNCS, vol.2729, pp. 382-398 Springer, Heidelberg, 2003.

□ Achievements : An Implementation Technique of Ultra-Light Block Cipher HIGHT over Sensor Network

○ Summary

1. Abstract

The paper presents efficient implementation techniques of HIGHT over a sensor network.

2. Primary Content & Summary

● Combining the correlated key pairs at a 16-bit scale

HIGHT cryptography is 8-bit based block cryptography [1]. Therefore, the master and white keys are 8 bits each. To implement efficiently over a 16-bit microprocessor, we combined key pairs, which had correlation with computing operations. Its relation is described in Table 1. Therefore, whenever computing operations, we can conduct two 8-bit operands at once.

Table 1. Relation of keys

MK	WK
(2, 0)	(6, 4)
(3, 1)	(7, 5)
(13, 12)	(1, 0)
(15, 14)	(3, 2)

● Pre-computed constant value

A constant used in HIGHT cryptography can be pre-computed to enhance speed of computation. However, as we compute a constant value in advance, it increases the size of memory consumption. Therefore, depending on applications we need to select strategies, speed first or memory first.

Table 2. Comparison of clock cycle on HIGHT implementation

Process	C code[2]	Proposed
Init	6360	950
Encryption	7730	2912
Decryption	7860	2912

3. Evaluation

Performance is evaluated in each process including initialization, encryption, and decryption. Our method significantly improved the speed of the operation. The detailed information is depicted in Table 2. Previous results implemented HIGHT cryptography in C code, so it demands high computational costs. To reduce the cost, I implemented the program in assembly code and adapted many techniques to implementations.

4. Applicant's role and importance

As a lead author, I proposed this research paper about the implementation technique of HIGHT over a sensor network, and I won an **excellence prize for superiority of paper** at the *"summer conference 2011"* supported by *"Korea Information and Communication Society."*

5. References

[1] Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bonseok Koo, Changhoon Lee, Donghoon Chang, Jaesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim, and Seongtaek Chee. *"HIGHT: A New Block Cipher Suitable for Low-Resource Device,"* CHES 2006, pp. 46-59, 2006.

[2] W. Liu, R. Luo, and H. Yang. *"Cryptography overhead evaluation and analysis for wireless sensor networks."* Communications and Mobile Computing, International Conference on, pp. 496-501, 2009.

No.	Classification (Research Paper/Patent)	Title	Journal Name/ Foreign or Domestic Patent	Role	Remarks · country (in case of foreign patent) · patent application/registration
1	Research Paper	Performance Enhancement of TinyECC based on the Multiplication Optimizations	Security and Communication Networks	Lead author	**SCI-E** Impact Factor: **0.356** **(2011. 12. Accepted)**
2	Research Paper	ZigBee Security For Home Automation Using Attribute-Based Cryptography	IEEE Consumer Electronic Society	Lead author	2011 IEEE International Conference on Consumer Electronics **(2011. 1. Published)**
3	Research Paper	An Implementation Technique of Ultra-Light Block Cipher HIGHT over Sensor Networks	Korea Information and Communication Society	Lead author	**First Prize** Summer conference **(2011. 7. Published)**

% Total number of published and accepted papers as a lead author from 2010 to 2012.

SCI-E : 1

IEEE conferences : 2

International conferences : 2

Domestic journals : 8

Domestic conferences : 11

2. Other research achievements

1. An Attribute-based Authentication Scheme for Electronic Money using Smart Cards

● **Primary Content :** Solution for problem of [1] and presenting attribute-based protocols.

● **Evaluation :** The protocol is more secure in terms of tracing and mutual authentication.

2. Speed Optimized Implementation of HUMMINGBIRD Cryptography for Sensor Network

● **Primary Content :** Providing optimization method on memory accesses.

● **Evaluation :** Enhancement of 20 % ~ 30 % in speed than [2].

3. Transmission Power Range-based Sybil Attack Detection Method over Wireless Sensor Networks

● **Primary Content :** Sybil attack detection measuring the range of RSSI.

● **Evaluation :** Improvement in accurate Sybil attack detection rate.

4. A Secure Mobile Message Authentication over VANET

● **Primary Content :** Location-based authentication protocol for VANET.

● **Evaluation :** Reducing the computation cost than [3].

5. ZigBee Security for Visitors in Home Automation using Attribute-based Proxy Re-encryption

● **Primary Content :** Empowering the authority for others in home automation.

● **Evaluation :** More features including re-encryption than [4].

● **References**

[1] H. W. Sim, S. J. Kim, *"An Authentication Scheme for Electronic Money with Anonymity and Traceability Using Smart Cards,"* Korea Minting & Security Printing Corporation (KOMSCO), 2010.

[2] D.Engels, X. Fan, G. Gong, H. Hu, and E. M. Smith, *"Hummingbird: Ultra-Lightweight Cryptography for Resource Constrained Devices,"* to appear in the Proceedings of The 14th International Conference on Financial Cryptography and Data Security-FC2010, Berlin, Germany: Springer-Verlag, pp. 5-18. 2010.

[3] SeockJae Jung, YoungJun Yoo, JungHa Paik, DongHoon Lee, *"Secure and Efficient V2V Message Authentication Scheme in Dense Vehicular Communication Networks,"* Korea Institute of Inforamtion Security & Cryptology, vol. 20, No. 4. pp. 41-52.

[4] Hwajeong Seo, CheolSoo Kim, Howon Kim, *"ZigBee Security For Home Automation Using Attribute-based Cryptography,"* IEEE International Conference on Consumer Electronics, pp 375-376, 2011.

No.	Classification (Research Paper/Patent)	Title	Journal Name/ Foreign or Domestic Patent	Role	Remarks · country (in case of foreign patent) · patent application/registration
1	Research Paper	An Attribute-based Authentication Scheme for Electronic Money using Smart Cards	Korea Minting, Security Printing & ID Card Operating Corp.	Lead author	**4th Prize** Security paper contest **(2011. 12. Published)**
2	Research Paper	Speed Optimized Implementation of HUMMINGBIRD Cryptography for Sensor Network	The Korea Institute of Information and Communication Engineering	Lead author	**(2011. 12. Published)**
3	Research Paper	Transmission Power Range-based Sybil Attack Detection Method over Wireless Sensor Networks	The Korea Institute of Information and Communication Engineering	Lead author	**(2011. 12. Published)**
4	Research Paper	A Secure Mobile Message Authentication over VANET	Journal of the Korea Institute of maritime Information & Communication Sciences	Lead author	**(2011. 5. Published)**
5	Research Paper	ZIGBEE Security for Visitors in Home Automation using Attribute-based Proxy Re-encryption	IEEE Consumer Electronic Society	Lead author	The 15th IEEE International Symposium on Consumer Electronics **(2011. 6. Published)**

<Attachment> Supporting Documents

※ *Instructions* (delete instructions after completion)

- *Provide supporting documents for major and other research achievements in the order stated above*
- *Supporting documents must be provided for major research achievements*
  Example: Submission of a copy of a research paper (including a copy of the cover and table of contents of the academic journal or collection of dissertation the paper was published in. If it is an approved paper, provide an approval letter or a document that verifies its acceptance for publication)
- *Supporting documents must also be provided for other research achievements. However, if there are no supporting documents due to the nature of the research activity, explain the reason in the remark column. (If the reasons are considered unacceptable, they will not be taken into consideration.)*

【Form 6】

Reason for choosing the University

1. Reason for choosing the university

My university is one of the finest universities in the world. From cutting-edge experimental devices to renowned professors, my university provides high-quality educational resources to passionate students. Every year, many excellent papers are published in both foreign and domestic journals. These achievements motivate me to study hard. Also, my university has a beautiful campus. Whenever I commute to school, I enjoy the scenery and atmosphere of campus being full of energy.

Fig. 1. Strong features of my university

● **Professors**

In my department, many talented professors immerse themselves in research and education. Among them, two professors are experts in embedded systems and security fields. One professor's research topic is embedded systems. He has deep knowledge about the architecture of embedded systems and the principles they work by, which is useful to map out circuit architecture. Also, he is now managing the mesh network project. The project is closely related with my research topic, so I can get advice easily. Another professor here has worked in the security field for a long time so he knows the technology for cryptography on resource-constrained environments and has published many SCI indexed papers. He establishes security-related lectures in school and even invites many eminent speakers to give special lectures. Whenever I face difficulties of security principles and protocols, he kindly explains these concepts with clear examples. The passion and enthusiasm of these professors always lead students to great and fruitful results.

● **Courses**

In my Very Large Scale Integration (VLSI) class, I can cultivate the knowledge of hardware for implementing Field Programmable Gate Arrays (FPGAs) and simulating the performance character of hardware. I learn optimized hardware implementation and the characteristics of the hardware system. These techniques are useful to implement hardware cryptography. Second is embedded devices and the Linux operating system. The lecture helps me understand and utilize the unique characteristics of small and resource-constrained device and Linux-based embedded operating systems. With this knowledge, we can develop customized software and hardware. Third is about security. We learn about computer security from traditional to current cryptography. This lecture makes it easy for us to understand complicated theory and protocols.

● **Project and Research Topic of Laboratory**

From the beginning of the year, the laboratory has conducted nineteen projects with research organizations and government-affiliated organizations including NIMS, ETRI, KISA, NIPA, and MKE. The research area is a security issue such as sensor networks, low-power design, RFID, ASIC, FPGA, smart phones, NFC, WPAN, and smart grids. A wide range of interesting research topics motivate and inspire me with passion and enthusiasm.

● **Experiment devices**

To evaluate the results and assumption of the proposed methods, expensive experimental devices are needed. Especially, the security field demands many cutting-edge and sophisticated devices and tools such as sensor network devices, oscilloscopes, FPGAs, smart phones, and simulation and compilation tools. However, the laboratory already equipped sensor networks and hardware implementation environments for projects and research, and my university provides software programs including visual studio and office programs.

● **Online library**

Students get up-to-date technology and information from renowned and famous international and domestic journals. In campus, students have access to a number of journals free of charge. Therefore, students easily obtain knowledge from papers and patents.

● **Environment**

My university provides a pleasant working and learning environment. All classes have fully-equipped projectors, air conditioners, and sound systems for presentations and lectures. Using a projector, students and professors can deliver the presentations effectively, temperature is adjusted appropriately, and the sound system help students listen to voices clearly. Thanks to the environment, students can focus on their work and study.

● **English**

My university has an affiliated organization for English in which students take classes. During vacation, the organization provides additional high-quality English classes at a reasonable price. The English class is managed by native speakers. As a result, no students in the university feel fear when they encounter English classes and foreigners on the streets. Even in our major classes, many professors use English to meet the international level, and for foreign students. Various students from China, Japan, and India study together with Korean students, which is good to students for the better understanding of international society.

● **People and Collaboration**

I have studied for 6 years at my university. During this period, whenever I had trouble, many friends and professors advised and helped me out. This benevolence and kindness moved my mind and made me like colleagues and the school as well. In the department, many different laboratories collaborated with each other to fulfill the other's shortcomings. The efforts enhanced the efficiency and generated fruitful results. This is a good environment to lead students to becoming team players.

These are all about strong features of the university. I bet there is no university supporting student sincerely like my university, and that is the reason why I chose my university.