Computer Security 및 Cryptography 위한 진화론적 계산의 적용 소개

경북대학교 전준철 · 김기원 · 임재열 · 윤희정* · 유기영**

1. 서 론

20세기 후반과 21세기를 들어서면서 정보통신 기술의 발전과 인터넷 기반의 정보통신 인프라의 확장으로 사람들 사이나 시스템 사이의 정보교환이 상상을 할 수 없을 정도로 엄청나게 많이 이루어지고 있다. 이로 인해 인간의 삶의 모습이 빠르게 변하고 삶의 질이 더욱 풍요롭게 되고 있다. 그러나 인간 생활에 있어 정보가 중요한 자원되어가고, 정보소통이 많으면 많을수록 사람의 사생활을 침해하거나 정보의 오·남용과 허가 받지 않은 불법적인 사용자에 의한 정보시스템을 파괴 그리고 불건전한 정보의 유통 등 여러 가지 문제점이 발생되었고 앞으로 더욱 심화될 것이다.

이런 문제점들을 해결하기 위해서 정보보호의 중요성이 인식되어지면서 정보보호 기술에 관한 연구가 이루어져 왔고, 앞으로 더 많은 연구가 요구되고 있다. 그 동안 정보보호를 위한 기본 메카니즘을 제공하는 암호 기술과 컴퓨터나 네트워크의 보안을 위한 컴퓨터 시스템 보호 기술에 대한 연구가 이루어져 왔다.

1990년대부터 인공지능 분야에서 발전되어 왔던 진화론적 계산(evolutionary computation) 기술들(genetic algorithm, genetic algorithm, simulated annealing, etc)이 컴퓨터 보안 분야인 네트워크/호스트 보안과 cryptography 분야에서 꾸준히 각광을 받으면서 연구되어 지고 있다. 최근 몇 년 동안에 진화론적 계산의 이점을 기반으로 하는 많은 알고리즘들이 제안되고 있다[1]. 예를 들어, 암호화 primitives(의사 난수 생성기, 해쉬 함수, S-box 및 대칭키 암호 시스템, 암호 시스템의 연산기)의 설계와 암호 해독(cryptanalysis) 그리고 암호화 프로토콜까지 많은 분야에 걸쳐 방법들이 제안되어 오고 있다. 이런 최근의 성공들의 결과로, 진화론적 계산 기술들은 컴퓨터 보안을 연구하는 연구자로부터 많은 관심을 끌고 있다. 본문에서는 정보보호 기술에 진화론적 계산 기술들이 적용되어 연구되어진 사례별로 소개한다.

2. 진화론적 계산의 적용 사례

이 절에서는 진화론적 계산 기술 중에서 유전자 알고리즘이나 simulated annealing과 같은 휴리스틱 방법이 적용되는 대칭키 암호 시스템의 암호 해독 분야를 소개하고, 그 다음에 주로 셀룰라 오토마타를 이용하여 암호학적 primitive들 설계하는 분야를 소개한다.

2.1 고전적 암호 시스템의 해독 및 미해결 문제

진화론적 계산에 관한 많은 연구들이 고전적 암호 시스템의 암호 해독 분야에서 지속적으로 연구되어 왔다. 이러한 연구들은 Peleg와 Rosenfeld에 의해서 시작되었고, Hunter와 McKenzie, Carroll과 Martin 그리고 King과 Bahler에 의해 지속적으로 연구되어졌다[2-5]. King[6]은 polyalphabetic 치환 암호에 대한 첫 번째 공격을 보였다. 그 후에 그의 아이디어는 Clark과 Dawson에 의해 병렬 유전자 알고리즘으로 확장되고, 개선되었다[7]. 오늘날에 많은 연구자들에게 직접적으로 영향을 미친 연구로 Spillman 등은 단순 치환(simple substitution)과 전치 암호(transposition ciphers)의 암호 해독에 처음으로 유전자 알고리즘을 제안하였다[8]. Forsyth과 Safavi-Naini은 같은 문제를 해결하는데 simulated annealing 기술을 제안하였다[9].

한편 Bagnall, McKeown, Rayward-Smith들은 유전자 알고리즘을 사용하여 간소화된 버전이지만 고전적 암호 시스템의 정수인 ENIGMA에 대한 ciphertext-only attack를 제시하였다[10]. Millan, Clark 및 Dawson는 암호 시스템 설계에 많이 응용되는 부울 함수의 생성 모델을 제안하였는데, 이런 기술들이 암호학 분야뿐만 아니라 암호 해독 분야에도 도움이 됨을 보였다[11,12]. 많은 연구에서 보는 바와 같이 고전적 암호 시스템의 해독에 대한 진화론적 계산 기술로 암호 해독

* 학생회원
** 종신회원

이 쉽게 이루어졌다.

반면에 DES나 AES와 같은 현대 암호 시스템의 암호 해독을 진화론적 계산으로 해결하지 못하고 있다. 현재 대부분 깨어진 고전 암호 시스템들에서는 일반적으로 실제 키와 비슷한 키로 메시지를 암호하면 원래의 암호문에, 복호하면 원래의 평문에 비슷하게 각각 생성하는 성질을 가지는데, 이는 주어진 어떤 임의 메시지가 의미있는 영어와의 근접성 정도를 측정하는 fitness 함수를 정의하는데 많은 도움을 주는 반면에, 현대의 암호화 시스템들에서는 이런 성질을 가지지 않는다. 이러한 것들이 고전적 암호 시스템에서는 암호 해독하는데 성공한 이런 진화론적인 계산 기술들을 현대적 암호 시스템에 적용할 수 없는데 부족한 주요한 원인이다. 또한 현대 암호 시스템의 avalanche effect 특성 때문에 256비트 중에 255비트는 옳고 1 비트만이 틀린 키로 복호하여 구한 평문은 완벽하게 랜덤하게 보인다. confusion과 diffusion 성질이 구현된 현대 암호 시스템의 암호 해독에서는 새로운 진화론적 계산 기술에 대한 연구가 요구된다.

2.2 셀룰라 오토마타의 적용사례

진화론적 계산 기술이 정보보호의 여러 분야에 응용되는 대표적인 개념 중의 하나가 셀룰라 오토마타이다. John Von Neuman에 의해 처음으로 소개된 셀룰라 오토마타 (CA)는 복잡하고 물리적인 시스템의 시뮬레이션을 위해 적당한 모델로서 채택 되었다[13]. 셀룰라 오토마타(Cellular Automata, CA)는 규칙적으로 상호 연결된 많은 셀들로 구성 되어져 있는 유한 상태 머신 (Finite State Machine)이다. CA의 각 셀들은 상호 연결된 이웃의 현재 상태 값과 특별한 법칙에 따라 이산적 시간에 동시에 새로운 상태 값으로 갱신 되어진다. CA는 이웃 셀을 이용하여 셀을 갱신하기 위한 함수 즉 법칙과 자신을 포함 하여 셀을 갱신하는데 직접적으로 관여하는 이웃의 개수에 의해 이루어진다.

Wolfram이 처음으로 의사난수 생성과 블록 암호의 디자인에 셀룰라 오토마타의 사용을 제안하였다[14]. 얼마동안 셀룰라 오토마타의 암호 분야의 적용에 연구가 이루지지 않았다가 최근에 이 분야에 많은 논문들이 발표되었다. 특히, Slipper과 Tomassini는 셀룰라 프로그래밍(cellullar programming)이란 새로운 용어를 만들어내며, 논문을 발표했다[15]. 그리고 최근에는 Sheng-Uei와 Shu Zhang이 뛰어난 랜덤 성질을 가지는 생성기를 기반으로 의사난수 셀룰라 오토마타를 설계하였다[16]. 이 절에서는 보안 primitive 설계에 다양한 셀룰라 오토마타의 적용 예를 보인다.

2.2.1 의사 난수 생성기 (pseudo-random number generator) 설계

암호학적 응용에서 난수가 사용되는 예를 보면 대칭키 암호에서의 비밀키나 암호알고리즘 및 프로토콜의 초기값 생성, 공개키 암호의 비밀키/공개키 혹은 공개 파라미터 생성, 패스워드와 해쉬되는 salt, 각종 키 관리/인증 메커니즘에서의 세션키나 nonce 생성 등이 있다. 암호학에서 난수를 얘기할 때는 크게 순수난수(true random number)와 의사난수(pseudo-random number)로 나누어질 수 있으며, 전자는 주로 하드웨어적인 잡음원(반도체, 방사선 붕괴 등으로부터의 전자소음 혹은 열소음)을 증폭시켜 샘플링함으로써 얻어진다[17].

한편 의사난수는 의사난수 생성기(pseudo-random number generator: PRNG)로부터 얻어지는 난수로, PRNG는 길이가 k인 순수한 랜덤 비트시퀀스가 주어졌을 때, 길이가 $l \gg k$인 랜덤한 것처럼 보이는 비트 시퀀스가 출력되는 결정적인(deterministic) 알고리즘이다. 이때 PRNG의 입력을 seed라 하고, 출력은 seed가 안전하게 보관되는 한 이론적으로 예측 불가함을 증명할 수 있어야 한다. 여기서 결정적(deterministic)이란 것은 같은 seed가 주어졌을 때, 항상 같은 출력을 생성하는 것을 의미한다 .

이런 seed를 입력으로 받아 해쉬 함수와 같은 일방향 함수를 이용하거나, 이산대수나 소인수분해와 같은 어려운 문제(intractable problem)를 가정하여 의사난수를 얻을 수 있다. 의사난수를 구하는 또 다른 방법으로 셀룰라 오토마타(Cellular Automata: CA)를 이용하는 방법이 있다. 셀룰러 오토마타는 인접한 셀과의 결합 논리로 서로 연결되어 있고 그 형태가 규칙적인 배열로 구성되기 때문에 의사난수를 효과적으로 생성할 수 있는 특성을 가지고 있다. 현재 1차원 또는 2차원 셀룰라 오토마타를 이용한 PRNG가 구현되었고, 프로그램 가능한 셀룰라 오토마타 (programmable cellular automata)나 셀룰라 프로그래밍 (cellular programming)을 이용한 PRNG의 연구도 계속되고 있다[15,18].

프로토콜에서의 nonce 사용이나, 블록암호에서 카운터모드의 IV 등 one-time pad의 성질을 지녀야 하는 난수를 생성하기 위해 PRNG를 사용할 때 진화연산이 이용될 수 있다. PRNG의 결정적 성질로 인해 의사난수를 생성할 때 마다 새로운 seed를 생성해 내야 한다. 따라서 한번 생성된 seed에 대해 유전자 알고리즘을 이용하거나 셀룰라 오토마타를 이용해 새로운 seed를 생성하는 것 보다 적은 비용으로 여러 개의 seed를 생성할 수 있다.

2.2.2 해쉬 함수의 설계

해쉬 함수란 임의의 길이의 비트 열을 입력으로 하여 고정된 길이의 비트 열을 출력하는 함수이다. 해쉬 함수는 서명 알고리즘과 결합하여 효과적으로 사용될 수 있다. 임의의 크기의 전문을 정해진 크기의 전문축약을 만들어 서명을 하게 함으로서 전체 전문의 무결성 및 서명을 동시에 수행하는 역할을 하게 된다. 일반적으로 해쉬 함수는 함수 h와 입력 x가 주어지면, $h(x)$를 계산하는 것이 쉬워야 한다[17].

암호학적으로는 안전한 해쉬 함수를 위해 다음과 같은 세가지 조건을 만족해야 한다. 첫째, 해쉬 값 y가 주어졌을때, $h(x)=y$를 만족하는 입력 x를 찾는 것이 계산상 불가능하여야 한다. 둘째, 입력 x와 출력 $h(x)$가 주어졌을때, $h(x)=h(x')$을 만족하는 입력 x'를 찾는 것은 계산상 불가능하여야 한다. 마지막으로, $h(x) = h(x')$을 만족하는 서로 다른 임의의 두 입력 쌍 x, x'을 찾는 것은 계산상 불가능하여야 한다. 셀룰라 오토마타는 유한상태 머신으로서 인접한 셀과의 결합 논리로 의사난수를 효과적으로 생성할 수 있는 특성을 가지고 있다. 이러한 특성을 이용하여 논문 [19]에서는 셀룰라 오토마타를 이용하여 해쉬 함수를 설계하였다.

2.2.3 대칭기 암호화 시스템의 구현

대칭기 암호화 시스템의 구현을 위해서는 해쉬 함수와 달리 역원의 존재가 필수적이다. 이는 주어진 메시지를 암호한 후, 복호를 하기 위하여 필수적이다. 가역의 셀룰라 오토마타 (reversible CA)는 유한 상태에서 이러한 조건을 만족하는 가역 법칙을 제공한다. 이러한 가역법칙은 세 이웃 1차원 셀룰라 오토마타에서 단 6개만이 존재한다. 하지만, 두 개의 쌍으로 이루어진 가역의 셀룰라 오토마타의 클래스는 Wolfram[20]에 의해서 정의되어지고 Seredynski 등[21]에 의해 효과적인 대칭키 암호화 시스템의 구현을 위해 사용 되어지고 있다.

2.2.4 공개키 암호화 시스템에서의 연산기 설계

공개키 암호화 시스템에서 지수 연산은 가장 많은 연산시간을 요한다. 따라서, 모듈러 지수 연산의 속도에 따라 공개키 암호화 시스템의 효율성이 결정된다. 또한 지수연산은 곱셈의 반복에 의해 구해질 수 있기 때문에 많은 논문에서 셀룰라 오토마타와 프로그램 가능한 셀룰라 오토마타를 이용하여 효과적인 곱셈기를 구현하기 위한 논문들이 제시되고 있다. 논문 [22]에서 Choudhury등은 CA를 이용한 LSB 방식의 곱셈기를 제안하였으며, 논문[23]에서는 몽고메리 곱셈을 프로그램 가능한 셀룰라 오토마타를 사용하여 설계하였다.

2.2.5 암호화 프로토콜 설계

최근에 들어 셀룰라 오토마타의 역 연산 기능을 활용하여 암호화 프로토콜들 중에서 secret sharing 기법의 설계에 대한 연구가 제시되었다. 이는 Aloneso-Sanz 등[24]이 메모리 셀룰라 오토마타 (memory cellular automata)라는 개념을 도입하면서 시작되었다. 메모리 셀룰라 오토마타란 결정적인 법칙에 따라 모든 이산적인 시간에 변화되는 상태를 가지고 있는 유한개의 동일한 셀들로 이루어진 이산적인 동적 시스템을 말한다. secret sharing 기법은 비밀정보를 분산정보에 보호하고, 그 분산정보가 일정 개수 이상 모이면 원래의 비밀정보가 복원될 수 있으나, 그것보다 소수의 분산 정보로는 비밀정보를 완전하게 알 수 없다고 하는 부호화법이다.

Maranon[25]등은 최근에 2차원 메모리 셀룰러 오토마타(memory cellular automata)를 이용한 흑백, 그레이(gray) 그리고 컬러 이미지의 secret sharing 기법을 제안하였다. 제안한 기법은 설정단계(setup phase), 분배단계(sharing phase)와 복원단계(recovery phase)로 나눌 수 있다. 설정단계에서는 딜러(dealer)는 2차원 메모리 셀룰러 오토마타를 구성한다. 분배단계에서 딜러는 비밀 이미지(secret image) $C^{(0)}$을 분산정보에 보호화하기 위해 k-1개의 초기 배열, $C^{(1)}$, ... ,$C^{(k-1)}$을 의사 난수 생성기로 생성한다. 그리고, k개의 초기 배열들을 이용해 $(m+n-1)$번째 까지의 진화(evolution)를 시킨다. 딜러는 n명의 참가자 P_0, ..., P_{n-1}에게 마지막 n개의 배열 $C^{(m)}$, ... ,$C^{(m+n-1)}$을 각각 하나씩 분배한다. 복원단계에서는 n명이 가지고 있는 분산정보들 중에 연속된 k개의 분산정보들이 필요하다. 연속된 k개의 배열이 $C^{(m+a)}$, ... ,$C^{(m+a+k-1)}$, $0 \le a \le n-k$이라고 할 때, 메모리 셀룰라 오토마타 (inverse memory cellular automata)의 초기 배열을 $C^{(m+a+k-1)}$, ... ,$C^{(m+a)}$으로 설정한 뒤 $m+a$번의 역 메모리 셀룰라 오토마타를 진화시키면 비밀 이미지 $C^{(0)}$을 얻을 수 있다. 이러한 기법은 비밀 이미지와 각 참가자들이 가지는 분산 정보가 같은 크기이며, 복원 시 선명도의 손실(loss of resolution)이 없다.

3. 결 론

최근에 컴퓨터/네트워크 보안뿐만 아니라 여러 암호 분야에 인공지능 분야에서 발전되었던 진화론적 계산 기술의 적용에 관한 연구가 꾸준히 각광을 받고 있다. 본 글에서는 암호 분야에서 많은 관심의 대상인 진화론적 계산 기술의 적용 연구로 대칭키 암호 시스템의 암호해독, 의사 난수 생성기 설계, 고속 암호 알고리즘의 연산기 설계, 해쉬 함수의 설계, 그리고 암호화 프로토콜 설계 등 여러 분야의 연구 사례를 소개하였다. 이외에

도 여기서 언급하지 않았지만 계산상 어려운 문제에 기반한 공개 암호 시스템의 암호 해독 연구와 네트워크상의 침입 탐지 시스템에서의 진화론적 계산 기술의 적용에 대한 연구 사례도 있다. 정보보호 분야의 연구자들에게 이들 분야에 대한 연구에 동기를 부여할 것으로 기대한다.

참고문헌

[1] P. Isasi and J. C. Hernandez, "Introduction to the applications of evolutionary computation in computer security and crytography," *Computational Intelligence*, Vol. 20, No. 3, pp. 445-449, 2004

[2] S. Peleg and A. Rosenfeld, "Breaking substitution ciphers using a relaxation algorithm," *Communications of the ACM*, Vol. 22, No. 11, pp. 598-605, 1979.

[3] D. G. B. Hunter and A. R. Mckenzie, "Experiments with relaxation algorithms for breaking simple substitution ciphers," *The Computer Journal*, Vol. 26, No. 1, pp. 68-71, 1983.

[4] J. M. Carroll and S. Martin, "The automated cryptanalysis of substitution ciphers," *Cryptologia*, Vol. 10, No. 4, pp. 193-209, 1986.

[5] J. C. King and D. R. Bahler, "An implementation of probabilistic relaxation in the cryptanalysis of simple substitution ciphers," *Cryptologia*, Vol. 16, No. 3, pp. 215-225, 1992.

[6] J. C. King, "An algorithm for the complete cryptanalysis of periodic polyalphabetic substitution ciphers," *Cryptologia*, Vol. 18, No. 4, pp. 332-355, 1994.

[7] A. Clark and E. Dawson, "A parallel genetic algorithm for cryptanalysis of the polyalphabetic substitution cipher," *Cryptologia*, Vol. 21, No. 2, pp. 129-138, 1997.

[8] R. Spillma, M. Janssen, B. Nelson, and M. Kepner, "Use of a genetic algorithm in the cryptanalysis of simple substitution ciphers," *Cryptologia*, Vol. 17, No. 1, pp. 31-44, 1993.

[9] W. S. Forsyth, and R. Safavi-Naini, "Automated cryptanalysis of substitution ciphers," *Cryptologia*, Vol. 17, No. 4, pp. 407-418, 1993.

[10] A. J. Bagnall, G. P. McKeown, and V. J. Rayward-Smith, "The cryptanalysis of a three rotor machine using a genetic algorithm," *Proceedings of the 7th International Conference on Genetics Algorithms ICGA '97*, Morgan-Kaufmann, pp. 712-718, 1997.

[11] W. Millan et al., "New Concepts in Evolutionary Search for Boolean Functions in Cryptology," IEEE Proceedings, 2003.

[12] I. A. Clark et al. "Almost Boolean Functions: the Design of Boolean Functions by Spectral Inversion," IEEE Proceedings, 2003.

[13] J. Von Neumann, *The theory of self reproducing cellular automata*, University of Illinois Press, Urbana, Illinois, 1967.

[14] S. Wolfram, "Random sequence generation by cellular automata," *Advances in Applied Mathematics*, Vol. 7, No. 2, pp. 123-169, 1986.

[15] M. Sipper and M. Tomassini, "Generating parallel random number generators by cellular programming," *Int. J. Mod. Phys*, Vol. 7, No. 2, pp. 181-190, 1996.

[16] Sheng-Uei, and S. Zhang, "An evolutionary approach to the design of controllable cellular automata structure for random number generation," *IEEE Transactions on Evolutionary Computation*, Vol. 7, No. 1, pp. 23-36, 2003.

[17] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press,

1997

[18] Sheng-Uei Guan and Shu Zhang, "An Evolutionary Approach to the Design of Controllable Cellular Automata Structure for Random Number Generation," *IEEE Transactions on evolutionary computation*, Vol. 7, No. 1, pp. 23-36, 2003.

[19] M. Mihaljevic, Y. Zheng, and H. Imai, "A Cellular Automata based Fast One-Way Hash Function Suitable for Hardware Implementation," *Public Key Cryptography - Proceedings of PKC'98, LNCS*, Vol. 1431, pp. 217-233, 1998.

[20] S. Wolfram, *A New Kind of Science*, Wolfram Media, pp. 435-441, 2002.

[21] F. Seredynski, P. Bouvry, and A. Y. Zomaya, "Cellular Programming and Symetric Key Cryptography Systems," *Genetic and Evolutionary Computation (GECCO), LNCS* 2724, Part II, pp. 1369-1381, 2003.

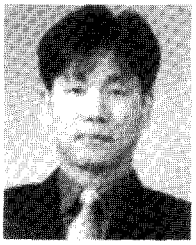
[22] P. Pal. Choudhury and R. Barua, "Cellular Automata Based VLSI Architecture for Computing Multiplication And Inverses In GF(2^m)," *IEEE 7th International Conference on VLSI Design*, pp. 279-282, 1994.

[23] J. C. Jeon and K. Y. Yoo, "Design of Montgomery Multiplication Architecture Based on Programmable Cellular Automata," *Computational Intelligence*, Vol. 20, No. 3, pp. 495-502, 2004.

[24] R. Alonso-Sanz, and M. Martin, "One-dimensional cellular automata with memory: patterns from a single site seed," *International Journal of Bifurcation and Chaos Applied Sciences and Engineering*, pp. 205-226, 2002.

[25] G. Alvarez Maranon, L. Hernandez Encinas, and A. Martin del Rey, "Sharing secret color images using cellular automata with memory," *arXiv.org e-Print*, CR/0312034, 2003.

전 준 철

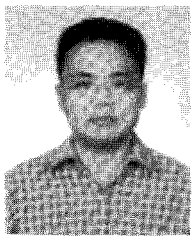


2000 국립 금오공과 대학교 공과대학 컴퓨터공학과(공학사)
2003 경북대학교 공과대학 대학원 컴퓨터공학과(공학석사)
2003~현재 경북대학교 공과대학 대학원 컴퓨터공학과(박사과정)
관심분야 : 암호연산, 암호화 프로토콜, 접근제어, 진화연산
E-mail : jcjeon33@infosec.knu.ac.kr

김 기 원

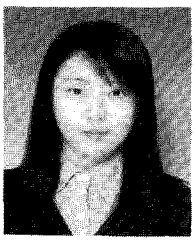
1999 경성대학교 이과대학 전산통계학과(이학사)
2001 경북대학교 공과대학 대학원 컴퓨터공학과(공학석사)
2001~현재 경북대학교 공과대학 대학원 컴퓨터공학과(박사과정)
관심분야 : 암호화 프로토콜, 정보보호, 진화연산
E-mail : nirvana@infosec.knu.ac.kr

임 재 열



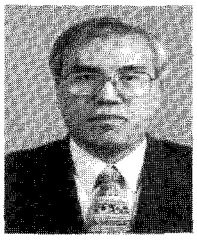
2003 경북대학교 공과대학 컴퓨터공학과(공학사)
2003~현재 경북대학교 공과대학 대학원 컴퓨터공학과(석사과정)
관심분야 : 암호화 프로토콜, 정보보호
E-mail : tenheat@infosec.knu.ac.kr

윤 희 정



2004 안동대학교 공과대학 정보통신공학과(공학사)
2004~현재 경북대학교 공과대학 대학원 컴퓨터공학과(석사과정)
관심분야 : 접근제어, 진화연산
E-mail : dude93@infosec.knu.ac.kr

유 기 영



1976 경북대학교 이과대학 수학교육과(이학사)
1978 한국 과학기술원 컴퓨터공학과(공학석사)
1992 New York Rensselaer Polytechnic Institute 컴퓨터과학과(이학박사)
1978~현재 경북대학교 공과대학 컴퓨터공학과 교수
관심분야 : 암호연산, 병렬처리, 암호화 프로토콜, 정보보호
E-mail : yook@knu.ac.kr