JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 12 : 2865~2870 Dec. 2015

NP-complete 문제를 이용한 공개키 암호 시스템 개선

백재종*

An enhanced method using NP-complete problem in Public Key Cryptography System

Jaejong Baek*

Naval Information and Communication School, Jinhea, Changwon, Kyungnam 51691, Korea

요 약

최근 양자 컴퓨터가 개발되는 등 컴퓨팅 하드웨어의 성능이 발전하면서 단시간 내에 처리할 수 있는 정보의 양이 기하급수적으로 증가하고 있다. Koblitz-Fellows가 제안한 암호시스템은 생성할 수 있는 불변 다항식(invariant polynomial)의 개수가 충분하지 않아 특정 3-정규 그래프에서 완전지배집합(Perfect Dominating Set, PDS)을 찾는 문제가 NP-complete임을 보장할 수 없는 문제점이 발생한다. 본 논문에서는 이러한 취약점을 보완하기 위해 Koblitz-Fellows가 제안한 3-정규 그래프 상에서 완전지배집합을 이용하여 불변 다항식의 개수를 기하급수적으로 증가시킴으로 계산의 복잡도를 더욱 난해하게 하여 암호시스템의 취약점을 개선하도록 제안한다.

ABSTRACT

Recently, due to the hardware computing enhancement such as quantum computers , the amount of information that can be processed in a short period of time is growing exponentially. The cryptography system proposed by Koblitz and Fellows has a problem that it can not be guaranteed that the problem finding perfect dominating set is NP-complete in specific 3-regular graphs because the number of invariant polynomial can not be generated enough. In this paper, we propose an enhanced method to improve the vulnerability in 3-regular graph by generating plenty of invariant polynomials.

키워드 : 공개키, 암호시스템, 계산복잡도, 그래프

Key word : Publick-key, Cryptography-system, computing complexity, graph

Received 08 September 2015, **Revised** 21 September 2015, **Accepted** 05 October 2015

* **Corresponding Author** Jaejong Baek(E-mail:jjbaek35@gmail.com, Tel:+82-55-549-6750)
Naval Information and Communication School, Jinhea, Changwon, Kyungnam 51691, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.12.2865 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

양자컴퓨팅 기술은 현재의 컴퓨팅 능력으로 오랜 시간이 걸려 해결이 어려운 문제를 쉽고 빠르게 풀 수 있는 기술이다. 최근 D-Wave社의 양자컴퓨터가 2014년 2 월 7일자 Time지의 표지기사로 소개되는 등 10년 내 실용 가능한 양자컴퓨터의 등장이 전망되고 있다[1].

공개키 암호 알고리즘 RSA는 정수론의 인수분해에 기반을 두고 있으나 1995년 피터 쇼어는 소인수분해와 이산로그가 양자 컴퓨터상에서 다항 시간 내에 풀린다는 사실을 입증했다[2]. 그러나 P-NP 문제는 양자 컴퓨팅기술로도 여전히 풀기 어려운 문제로 남아있어 P-NP 문제를 이용해서 암호 시스템을 구축한다면, 향후 양자 컴퓨팅 기술이 보편화 되어도 안전한 암호 시스템으로 사용될 수 있을 것이다[3]. 본 논문에서는 1994년에 Koblitz와 Fellows가 [4]에서 제안한 완전지배집합(PDS)의 NP-complete 문제를 이용한 암호 시스템의 문제점을 살펴보고 이를 보완하는 암호 시스템을 제안한다. Koblitz와 Fellows가 제안한 방식은 3-정규 그래프에서 3-edge coloring map에 대한 불변식을 이용한 방식이다. 이 방식이 항상 풀기 어려운 문제가 아님을 확인하고, 항상 풀기 어려운 문제로 변경하여 그 문제점을 개선하는 것을 목적으로 한다.

Ⅱ. 관련 연구

2.1. Kobiltz-Fellows 암호시스템

배낭문제(Knapsack) 기반 공개키 암호시스템의 불완전함이 밝혀지면서 NP-complete 문제에 기반을 둔 조합이론은 암호학 시스템에서 적합하지 않다는 연구 결과가 제시되었다. 하지만 Fellows와 Kobiltz는 어려운 조합이론 문제들이 암호시스템에 적합하지 않다는 전제를 반박하고, NP(다항시간에 비결정적 알고리즘을 이용하여 풀 수 있는 문제의 집합) 문제들을 공개키 암호시스템의 기본으로 사용하는 아주 일반적인 방법을 소개했다. 현재까지는 공개키 암호시스템을 효율적으로 공격하는 방법에 대해서 알려지지 않았다.

NP-complete 문제 기반의 암호시스템을 공격하는 방법에는 내재된 조합이론 문제를 해결하는 것과 선형 대수 방법이 있다. 일반적으로 선형 대수 공격은 시간이 매우 오래 걸리는 비효율적인 방법이다. 내재된 조합이론 문제를 푸는 것이 어렵다는 것은 Brassard의 정리로 증명이 가능하다[5].

2.2. 지배집합(Dominating Set)

2.2.1. 지배집합 정의

그래프 $G=(V,E)$, $w\in V$의 닫힌 이웃집합 $N[w]$는 w와 인접한 G의 모든 꼭짓점들의 모임이다. $W\subset V$는 $\cup N[u]=V$일 때 G의 지배집합이다. W는 $N[u]\cup N[v]=0$ 일 때 완전하다.

2.2.2. 완전지배집합(Perfect Dominating Set)

지배집합 정의를 확장하여, 임의의 $v\in V$에 대해 $N[v]$가 오직 W의 한 원소만을 포함할 때 ($\forall u,v\, N[u]\cup N[v]=\varnothing \text{ and } u\neq v$), 이를 완전지배집합(Perfect Dominating Set, PDS)이라 한다.

2.2.3. 지배집합의 복잡도

$\delta(G)\geq 3$ ($\delta(G)$는 그래프 G의 최소 차수)인 일반적인 그래프에서 PDS를 구하는 문제는 NP-complete하다. 주어진 평면3-정규 그래프가 PDS를 갖는지를 판단하는 문제는 NP-complete하다. 3-정규 그래프는 그래프 G=(V, E)에서 V의 속하는 모든 꼭짓점의 차수가 3인 그래프를 의미한다. 주어진 평면3-정규 그래프가 4개의 PDS를 갖는 것과 이 3-정규 그래프가 K4-Covering 그래프라는 말은 동치이다. 따라서 주어진 평면 3-정규 그래프가 K4-Covering 그래프인지 판단하는 문제는 NP-complete이다.

Ⅲ. Koblitz-Fellows 암호시스템 및 문제점

3.1. Koblitz-Fellows 암호 시스템 개요

'갑'은 W를 PDS 3-정규-그래프($\delta(G)=\triangle(G)$)를 가지고, W는 비밀키로 감추고 G를 공개키로 공개한다. 또한 적당한 x,y,m을 가지고 $\sigma(x,y,m)$을 만들고 그것을 이루는 변수인 (x,y,m)은 공개한다. 여기서 W를 PDS 정규 그래프를 만드는 것은 쉽지만, 거

꾸로 G에서 W를 찾는 것은 NP-complete로 어려운 일방향 함수(one-way function)이다.

'갑'에게 메시지를 보내려는 '을'은 먼저 G에서 임의로 꼭짓점을 정하고, 다음 잡은 각 꼭짓점의 $N[v]$와 파라메타 (x, y, m)에 대한 불변식 수식들을 생성한다. 그리고 생성한 불변식 수식들을 곱하고 더해서 복잡한 다항식 P를 만들되 그 다항식이 변수 (x, y, m)에 의한 평가된 값이 자기가 '갑'에게 보내고 싶은 값 b (modulo m)가 되도록 한다. 이때 생성된 다항식 P는 중간에 도청 공격자가 P로부터 그 다항식을 이루는 불변식 수식들을 분해하기 어렵게 만들어야 한다. 이 다항식 P를 '갑'에게 보내고, '을'에게서 P를 받은 갑은 자신의 비밀키인 PDS W와 대체 노드 $\sigma(x, y, m)$을 사용하여 받은 다항식 P의 값을 구하여 '을'이 보낸 b의 값을 얻는다.

3.2. Koblitz-Fellows가 제안한 알고리즘의 문제점

Koblitz와 Fellows가 제안한 방법에서 이용하는 공개키는 3-정규 그래프 G이고 비밀키는 G의 PDS이다. 이들이 제안한 알고리즘의 문제점은 다음과 같다.

① 지배집합 복잡도에 관한 정의에 의해서 일반적으로 3-정규 그래프에서 PDS를 구하는 문제는 NP-complete이다.
② 마찬가지로 지배집합 복잡도의 관한 정의에 의해 평면 3-정규 그래프가 PDS를 갖는지를 판단하는 문제는 NP-complete하다.
③ 주어진 평면 3-정규 그래프가 4개의 PDS를 갖는 것과 이 3-정규 그래프가 K4-Covering 그래프라는 말은 동치이다.
④ Koblitz-Fellows의 방법은 기본적으로 3-정규 그래프 G를 이용하며 공개키인 G와 비밀키인 PDS W를 갖는다. 여기서 G가 평면 그래프이며 4개의 PDS를 가질 수가 있는데 이것은 G가 K4-Covering 그래프라는 것과 동치이다.
⑤ 4에 의해 공개키 G가 K4-Covering 그래프일 가능성이 있다는 것이 도출되었다. G가 K4-Covering 그래프일 때 PDS를 찾는 것은 NP임이 확실히 밝혀져 있지 않기 때문에 보안상의 취약점이 나타날 가능성이 있다[2].

Ⅳ. 제안하는 암호 시스템

Koblitz와 Fellows가 제안한 암호 시스템의 문제점을 해결하고, 더 일반적인 범위에서 암호 시스템을 제안하려고 기존의 공개키를 3-정규 그래프에서 $\delta(G) \geq 3$인 랜덤 그래프로 변경한다. $\delta(G) \geq 3$인 일반적인 그래프에서 PDS를 구하는 문제는 NP-Complete하다. $\delta(G) \geq 3$인 일반적인 랜덤 그래프에서는 PDS를 구하는 문제가 항상 NP-Complete 하므로 항상 안전성을 보장할 수 있다.

4.1. 그래프 생성 방법

$S = \{j_1, j_2, ..., j_m\}$ 를 PDS라고 가정한다. 그리고 scheme $\sigma(a, b, m)$의 값인 a, b, m을 결정하고서, 이를 공개한다. m은 가능한 한 소수가 될수록 좋다. $\exists v \in S$, v에 대해 d(j)(차수 of j)를 지정해 주고, N(j)들을 그려준다. 이때, 위에서 결정한 σ을 이용하여 S에 속한 꼭짓점은 x, 그 꼭짓점의 이웃은 y로 값을 지정해 준다. $\forall v \in S$, v에 대해 d(v)만큼의 이웃들과 각각 연결되어 있을 것이고, 이런 m개의 성분(component)이 존재할 것이다.

$$C = \left\{ \begin{array}{l} \forall c_i, c_j \in C \wedge c_i \neq c_j \\ \wedge \ (\exists v_i \in S) \Rightarrow (v_i \in c_i) \wedge (v_i \notin c_j) \end{array} \right\} \quad (1)$$

$C = \{c_1, c_2, ..., c_m\}$와 같이 m개의 성분들이 생기게 된다. $\exists c_i, c_j \in C \ c_i \neq c_j$에 대해 c_i와 c_j 성분들을 연결된 상태로 만들어 줘야 한다. 이들을 연결하는 데는 4가지의 경우의 수가 존재한다. v_i, v_j는 $\{v_i \in c_i \wedge v_j \in c_j \wedge c_i \neq c_j\}$을 만족한다.

① $v_i \in S \wedge v_j \in S$

v_i와 v_j는 둘 다 PDS안에 들어 있으므로, 이 둘 사이에 변이 존재하게 되면 이 그래프에서 v_i와 v_j 둘 다 PDS에 들어갈 수는 없다. v_i와 v_j사이에 변이 존재하므로, $v_j \in N(v_i)$를 만족하게 된다. scheme $\sigma(a, b, m)$에 의해 v_i가 x를 갖게 되면 v_j는 y를 갖게 되고, v_i가 y를 갖게 되면 v_j는 x를 갖게 된다. 따라서

둘은 동시에 PDS에 들어갈 수 없다.

② $v_i \in S \wedge v_j \notin S$

v_i는 PDS안에 들어있고, v_j는 PDS안에 들어 있지 않다. 그러나 이 둘 사이에 변이 존재한다면 두 개의 성분들을 합친 그래프는 PDS를 갖지 않는다. 만약 둘 사이 변이 존재한다고 가정하면 $\exists v \in c_j \wedge v \in S$를 만족하는 v가 존재한다. v_i와 v_j사이에 변이 존재하므로 다음과 같다. 따라서 둘은 동시에 PDS에 들어갈 수 없다.

$$v_j \in N(v) \wedge v_i \in N(v_j) \wedge v, v_i \in S \qquad (2)$$

③ $v_i \notin S \wedge v_j \in S$

②의 경우와 마찬가지로 이 둘 사이에 변이 존재하면 안 된다.

④ $v_i \notin S \wedge v_j \notin S$

v_i와 v_j모두 PDS안에 들어있지 않으므로 이 둘 사이에 변이 존재한다고 해서 $G' = c_i \cup c_j$ 그래프가 기존의 PDS에 영향을 끼치지 않는다. 이렇게 모든 성분들을 연결시켜서 하나의 연결된 그래프 G를 얻을 수 있다. 따라서 $G := c_1 \cup c_2 \cup \ldots \cup c_m$이 되고, c_i와 c_j 사이엔 어떤 변이 존재할 수 있다. 비밀키 S를 감추고, 공개키 G 와 scheme $\sigma(a, b, m)$를 공개한다.

4.2. 불변 다항식 생성

$$P(x) = \sum i_j q_j \qquad (3)$$
$$(i_j \in F[G], q_j \in Inv[G])$$

위와 같은 방식으로 불변 다항식 P를 만들 수 있다. 위의 식에서 $Inv[G]$의 식을 생성하는 과정은 다음과 같다. 특별히 어떤 꼭짓점 j_1 대한 불변 다항식을 $d(j_1) = 3$이라고 가정하고, 이웃들을 각각 j_2, j_3, j_4라 하면, 다음과 같은 식 (4)가 성립한다.

$(\text{단}, i := constant)$

$$\begin{aligned} &i_1 j_1 + i_2 j_2 + i_3 j_3 + i_4 j_4 + i_{12} j_1 j_2 + i_{13} j_1 j_3 \\ &+ i_{14} j_1 j_4 + i_{23} j_2 j_3 + i_{24} j_2 j_4 + i_{34} j_3 j_4 + \\ &i_{123} j_1 j_2 j_3 + i_{124} j_1 j_2 j_4 + i_{134} j_1 j_3 j_4 + \\ &i_{234} j_2 j_3 j_4 + i_{1234} j_1 j_2 j_3 j_4 \end{aligned} \qquad (4)$$

$\sigma(a, b, m)$에 대해 PDS 에 속한 꼭짓점은 a, 그의 이웃들은 b의 값을 갖게 된다. j_1, j_2, j_3, j_4어느 것이 PDS에 속하는지 알 수 없으므로 각 꼭짓점에 모든 값을 대입 한다.

$$\begin{aligned} &i_1 a + i_2 b + i_3 b + i_4 b + i_{12} ab + i_{13} ab + \\ &i_{14} ab + i_{23} b^2 + i_{24} b^2 + i_{34} b^2 + i_{123} ab^2 + \\ &i_{124} ab^2 + i_{134} ab^2 + i_{234} b^3 + i_{1234} ab^3 \\ &= i_1 b + i_2 a + i_3 yb + i_4 yb + i_{12} ba + i_{13} b^2 + \\ &\quad i_{14} b^2 + i_{23} ab + i_{24} ab + i_{34} b^2 + i_{123} ab^2 + \\ &\quad i_{124} ab^2 + i_{134} b^3 + i_{234} ab^2 + i_{1234} ab^3 \\ &= i_1 b + i_2 b + i_3 a + i_4 b + i_{12} b^2 + i_{13} ba + \\ &\quad i_{14} b^2 + i_{23} ab + i_{24} b^2 + i_{34} ab + i_{123} ab^2 + \\ &\quad i_{124} b^3 + i_{134} ab^2 + i_{234} ab^2 + i_{1234} ab^3 \\ &= i_1 b + i_2 b + i_3 b + i_4 a + i_{12} b^2 + i_{13} b^2 + \\ &\quad i_{14} ab + i_{23} b^2 + i_{24} ab + i_{34} ab + i_{123} b^3 + \\ &\quad i_{124} ab^2 + i_{134} ab^2 + i_{234} ab^2 + i_{1234} ab^3 \end{aligned} \qquad (5)$$

식 (5)를 정리하면 다음과 같다.

$$\begin{cases} 1)\, i_1(a-b) + i_2(b-a) + i_{13}(ab-b^2) + \\ \quad i_{14}(ab-b^2) + i_{23}(b^2-ab) + \\ \quad i_{24}(b^2-ab) + i_{134}(ab^2-b^3) + \\ \quad i_{234}(b^3-ab^2) = 0 \\ \\ 2)\, i_2(a-b) + i_3(b-a) + i_{12}(ba-a^2) + \\ \quad i_{13}(b^2-ba) + i_{24}(ab-b^2) + \\ \quad i_{34}(b^2-ab) + i_{124}(ab^2-b^3) + \\ \quad i_{134}(b^3-ab^2) = 0 \\ \\ 3)\, i_3(a-b) + i_4(b-a) + ih_{13}(ba-b^2) + \\ \quad i_{14}(b^2-ab) + i_{23}(ab-b^2) + \\ \quad i_{24}(b^2-ab) + i_{123}(ab^2-b^3) + \\ \quad ih_{124}(b^3-ab^2) = 0 \end{cases} \qquad (6)$$

식(6) 연립 방정식을 풀면 다음과 같다.

$$\begin{cases} 1)\, i_1(b-a) = i_4(b-a) + i_{12}(ba-b^2) + \\ \quad i_{13}(ab-b^2) + i_{24}(b^2-ab) + i_{34}(b^2-ab) \\ \quad + i_{123}(ab^2-b^3) + i_{234}(b^3-ab^2) \\ \\ 2)\, i_2(b-a) = i_4(b-a) + i_{12}(ba-b^2) + \\ \quad i_{14}(b^2-ab) + i_{23}(ab-b^2) + i_{34}(b^2-ab) \\ \quad + i_{123}(ab^2-b^3) + i_{134}(b^3-ab^2) \\ \\ 3)\, i_3(b-a) = i_4(b-a) + i_{13}(ba-a^2) + \\ \quad i_{14}(b^2-ab) + i_{23}(ab-b^2) + i_{24}(b^2-ab) \\ \quad + i_{123}(ab^2-b^3) + i_{124}(b^3-ab^2) \end{cases} \tag{7}$$

$$\begin{aligned} &(b-a)(i_1+i_2+i_3) = 3i_4(b-a) + \\ &2i_{12}(ba-b^2) + 2i_{13}(ab-i^2) + \\ &2i_{14}(b^2-ab) + 2i_{23}(ab-i^2) + \\ &2i_{24}(b^2-ab) + 2i_{34}(b^2-ab) + \\ &3i_{123}(ab^2-b^3) + i_{124}(b^3-ab^2) + \\ &i_{134}(b^3-ab^2) + i_{234}(b^3-ab^2) \end{aligned}$$

i_1, i_2, i_3을 제외한 나머지 i값을 변수로 하는 방정식이 만들어 진다. i값을 $-1, 0, 1$만으로 한정했을 때, $O(3^{15})$만큼의 불변 다항식을 생성할 수 있다.

$$P(x) = \sum h_j q_j \tag{8}$$
$$(h_j \in F[G], q_j \in Inv[G])$$

식 (8)을 공격자가 불변 다항식으로 인수분해 하지 못하도록 하기 위해서는 가능한 불변식의 개수가 많을수록 좋다. 기존의 3-정규 그래프와 현재의 랜덤 그래프를 비교하여 평균적인 꼭짓점 수에 따른 평균적인 불변 다항식의 개수를 그래프로 나타내면 다음과 같다.(단, 꼭짓점의 개수는 100 로 한정)

$\epsilon(G) = \dfrac{1}{2|\,V(G)|} \sum_{v \in V(G)} d(v)$ 일 때,

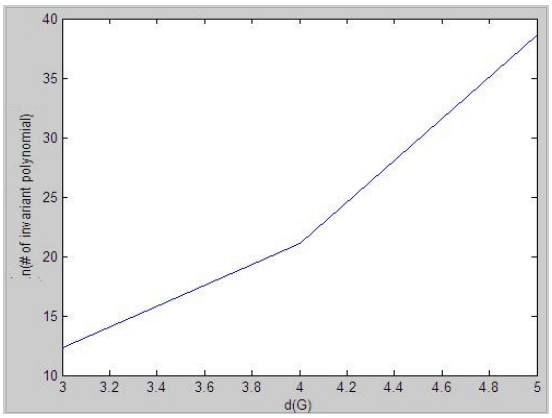

Fig. 1 # of invariant polynomial if $3 \le \epsilon(G) \le 5$

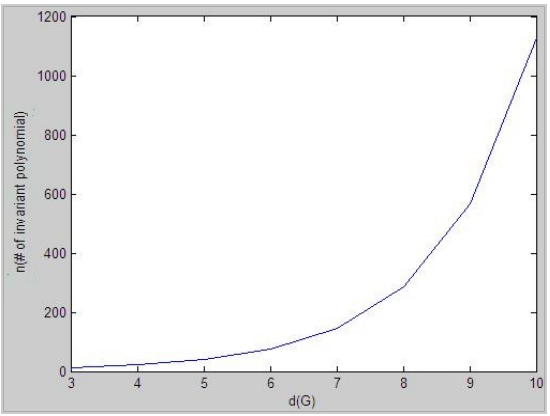

Fig. 2 # of invariant polynomial if $3 \le \epsilon(G) \le 10$

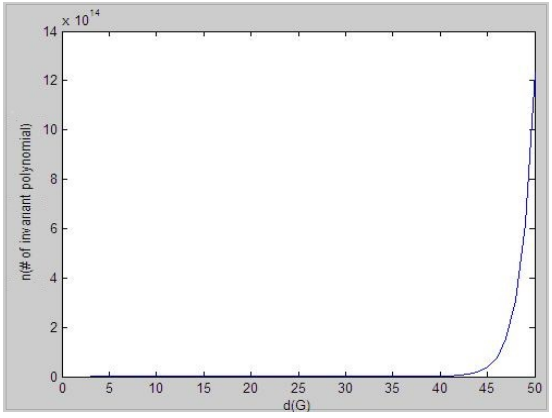

Fig. 3 # of invariant polynomial if $3 \le \epsilon(G) \le 50$

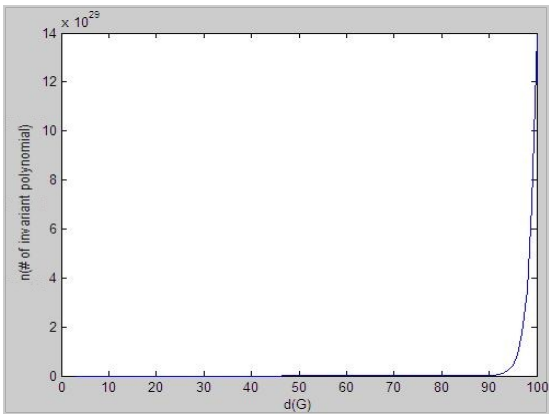

Fig. 4 # of invariant polynomial if $3 \leq \epsilon(G) \leq 100$

위의 그림에서 보는 바와 같이 불변 다항식의 개수는 그래프의 평균 차수의 수가 증가할 때마다 기하급수적으로 늘어나는 것을 볼 수 있다. 위의 그래프는 불변 다항식의 개수에 자연 상수의 log를 취한 값이므로 실제 개수는 그래프의 평균 차수에 따라 매우 큰 숫자로 증가할 것이다.

V. 결 론

본 논문에서는 Koblitz-Fellows가 제안한 암호시스템에서 생성할 수 있는 불변 다항식의 개수가 충분하지 않아 특정 3-정규 그래프에서 NP-complete임을 보장할 수 없는 문제점을 제시하였다. 이에 대한 해결방안으로 불변 다항식의 개수를 기하급수적으로 더 많이 생성하여 양자컴퓨팅과 같은 슈퍼 컴퓨팅 기술이 보편화 되어도 안전성을 보장하도록 개선하는 방안을 제안했다. 또한 공격자가 불변 다항식으로 인수분해 하지 못하도록 하기 위해서는 가능한 불변식의 개수가 많을수록 유리함을 확인하였다. 향후 양자 기술과 같은 컴퓨팅 능력이 급격히 발전함에 따라 현재 해결이 어려운 문제들이 쉽게 풀릴 수 있을 것이다. 따라서 암호시스템의 계산 복잡도를 높이는 것은 미래 암호체계에서 더욱 보완해야 할 사항으로 판단된다.

REFERENCES

[1] S.S. Park. et al, “Status of Quantum Information and Communication Technologies”, *ETRI*, 2015.

[2] Peter Shor, “*Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*”, 1995.

[3] Michael H. Freedman, “*P/NP, and the quantum field computer”, The National Academy of Sciences*, 1998.

[4] Fellows, Koblitz, “*Combinatorial cryptosystem Galore!*”, Contemporary Maths, 168, pp. 51-61, 1994.

[5] Brassard, G., “A note on the complexity of cryptology”, *IEEE Transactions on Information Theory IT-25*, pp. 232-233, 1979.

백재종(Jaejong Baek)

1996년 2월 한밭대학교 전자계산학과 공학사
2001년 2월 연세대학교 컴퓨터과학과 공학석사
2011년 8월 연세대학교 컴퓨터과학과 공학박사
1996년 ~ 현재 해군 정보통신학교 학부장
※관심분야 : 무선 보안, 네트워크 보안, 시스템보안, 사이버전, 역공학