Puncturing, insertion, 그리고 shortening 을 이용한 McEliece 암호 시스템

이위직, 노종선
서울대학교

leewj422@ccl.snu.ac.kr, jsno@snu.ac.kr

McEliece cryptosystem using puncturing, insertion, and shortening

Wijik Lee, Jong-Seon No
Seoul National Univ.

요 약

본 논문은 puncturing, insertion, 그리고 shortening 을 이용한 McEliece 암호 시스템을 제안하였다. 이 암호시스템에서는 McEliece 공개키 암호시스템에서 선형부호생성행렬을 비선형생성행렬로 만들 수 있으며 이 경우 안전성이 높아지는 것을 확인할 수 있었다.

Ⅰ. 서 론

McEliece 암호 시스템은 최근 양자 컴퓨터에 대한 연구가 진행되며 포스트 양자 암호로 주목을 받고 있다. 1987 년에 McEliece 암호 시스템[1]이 제안되었으며 이는 오류 정정부호를 기반으로 하였다.

McEliece 암호 시스템의 단점으로는 키의 크기가 크다는 단점을 가지고 있다. 따라서 계속 키의 크기를 줄이려는 연구가 진행되어 왔고 이 중에서는 자기동형군을 이용하거나 준순환 부호를 사용하는 연구[2]가 진행되었다. 최근에는 MDPC 부호에 준순환 구조를 적용해서 안전성을 높이는 연구[3]도 제안되었다.

McEliece 는 생성행렬을 선형 오류 정정부호인 Goppa 부호를 사용하였다. Goppa 부호 대신 GRS, QC-LDPC, Reed-Muller[4]-[6]등을 이용한 암호 시스템이 연구되기도 하였지만 이들의 구조적 특성으로 인해 여러 공격에 의해 깨지기도 하였다.

McEliece 암호시스템을 공격하는 방법으로는 information set decoding[1]이 제안되었다. 하지만 계산량이 매우 높아서 이를 줄이는 알고리즘이 계속 제안되었다. Stern[7]은 낮은 무게 벡터를 찾는 알고리즘을 통해 계산량을 줄였으며 이 알고리즘이 Canteaut-Chabaud[8] 그리고 May, Meurer, Thomae[9]에 의해 개선되어왔다.

본논문에서는 puncturing, insertion, 그리고 shortening 을 이용한 새로운 McEliece 암호 시스템을 제안하였다.

Ⅱ. 사전 지식

A. McEliece 암호 시스템

McEliece 암호 시스템은 다음과 같다. 여기서 G 는 $[n,k,2t+1]$ Goppa 부호의 생성행렬이고 S 는 $k\times k$ 정칙행렬, P는 $n\times n$ 전치행렬이다.

비밀키: S,G,P
공개키: $G'=SGP,t$
암호화: k비트 메시지 $\boldsymbol{m}$에 대해
$\boldsymbol{c}=\boldsymbol{m}G'+\boldsymbol{e}$를 수행
$\boldsymbol{e}$는 오류 벡터이고 $\mathrm{wt}(\boldsymbol{e})=t$
복호화: 양변에 P^{-1}를 곱하면
$\boldsymbol{c}P^{-1}=\boldsymbol{m}SG+\boldsymbol{e}P^{-1}$
복호 알고리즘을 이용하여 오류 $\boldsymbol{e}P^{-1}$를 고치고 $\boldsymbol{m}S$값을 얻음.
$\boldsymbol{m}S(S^{-1})$를 계산하여 $\boldsymbol{m}$을 복원

B. McEliece 암호 시스템에 대한 공격

B.1 Information set decoding 공격

Information set decoding 공격은 G' 에서 오류가 없는 k 개의 위치를 이용한 공격이다. $\boldsymbol{e}$ 에서 오류가 없는 위치에 해당하는 G' 의 $k\times k$ 부분행렬 G'_k 을 선택하면 평문 $m=c_k{G'_k}^{-1}$ 을 복원할 수 있다. 부분행렬을 잘 선택할 확률은 다음과 같다.

$$\frac{\binom{n-t}{k}}{\binom{n}{k}}$$

그리고 여기에 역행렬을 구할 때 필요한 계산량까지 고려하였을 때 총 계산량은 약 2^{80}이다.

B.2 Stern 의 공격

Stern 의 공격은 information set decoding 의 한 종류이며 암호문 $c=\boldsymbol{m}G'+\boldsymbol{e}$ 는 부호들과의 거리가 t만큼 떨어져 있고 부호들 간에는 $2t+1$이상의 거리로 떨어져있다. 다음과 같은 새로운 행렬을 정의한다.

$$A=\begin{pmatrix} G' \\ c=\boldsymbol{m}G'+\boldsymbol{e} \end{pmatrix}.$$

새로운 부호 $\mathcal{A}$는 최소거리 t를 가지고 있고 최소 해밍 무게를 가지는 벡터는 $\boldsymbol{e}$이다. 따라서 $\mathcal{A}$의 최소 해밍 무게 벡터를 찾는 문제와 같다. Stern 은 선형부호행렬 G에 대해 최소 해밍 무게를 찾는 알고리즘을 제안하였다.

Stern 의 알고리즘을 통해 $\boldsymbol{e}$를 찾는데 필요한 계산량은 2^{66} 이며 이는 더욱 발전되어 최근에는 2^{36} 정도가 필요하다고 한다.

Ⅲ. 새로운 암호 시스템

A. 새로운 McEliece 암호 시스템

본논문에서는 puncturing, insertion, 그리고 shortening 을 이용한 새로운 McEliece 암호 시스템을 제안한다.

1) Shortening

$(k+s)\times(n+s)$ 크기의 생성행렬G를 shorten 해서 $k\times n$ 크기의 G_s 행렬을 생성한다. 생성행렬 G 의 부호는 임의로 선택할 수 있다.

$S: k\times k$ 정칙행렬, $P: n\times n$ 전치 행렬이라고 할 때

$G' = SG_sP.$

2) Puncturing 과 Insertion

G' 에 $\boldsymbol{c_1}, \boldsymbol{c_2}, \cdots, \boldsymbol{c_{s_P}}$의 열을 제거하고, s개의 $n\times 1$ 크기의 난수로 된 열 벡터 $\boldsymbol{a_1}, \boldsymbol{a_2}, \cdots, \boldsymbol{a_{s_I}}$을 추가하여 $k\times(n+s_I-s_P)$의 행렬 G'' 을 생성. G'' 에서 제거된 열 벡터들의 위치를 $L_P=\{m_1, m_2, \cdots, m_{s_P}\}$, 추가된 열 벡터들의 위치들을 $L_I=\{l_1, l_2, \cdots, l_{s_I}\}$, $1\le l_i\le n+s_I-s_P$라고 하자.

비밀키: S, G_s, P, L_P, L_I

공개키: G'', t

암호화: 메시지 $\boldsymbol{m}$에 대해서 $\boldsymbol{c}=\boldsymbol{m}\cdot G'' + \boldsymbol{e}$를 전송

복호화: 암호문 $\boldsymbol{c}$를 받았을 때, $\boldsymbol{c}$에서 집합 L의 원소에 해당하는 위치를 제거.
Erasure 복호화를 포함한 복호화 이후 P^{-1}, S^{-1}곱을 통해서 $\boldsymbol{m}$을 계산

B. 새로운 McEliece 암호시스템의 보안성

새로운 McEliece 암호시스템의 생성행렬은 shortening, puncturing 과 insertion 을 통해서 행렬의 크기를 임의로 조절할 수 있다. 따라서 행렬의 크기로 사용한 부호를 알아내어 공격하는 것은 없다. 따라서 공격방법은 information set decoding 이 된다.

B.1 Information set decoding 공격

G''에서 오류가 포함되지 않는 열을 잘 선택할 확률은 다음과 같다.

$$\frac{1}{2}\sum_{t_2=0}^{t}\frac{\binom{s_I}{t-t_2}\binom{n-s_P}{t_2}}{\binom{n+s_I-s_P}{t}}\frac{\binom{n-t_2}{k}}{\binom{n+s_I-s_P}{k}}$$

난수 열 벡터도 정보를 포함하고 있기 때문에 선택을 해도 된다고 가정하였다. 다만, 난수 열 벡터로 인해 역행렬이 구해지지 않을 경우를 고려하여 1/2 정도를 곱하는 것으로 하였다. 이 경우 s_I, s_P 에 따라 값이 바뀌는데 두 값이 같다고 가정하면 기존의 information set decoding 의 보안성과 비슷한 것으로(2^{80}) 계산이 되었다.

B.2 Stern 의 공격

Stern 의 알고리즘의 입력 값은 최소 해밍무게를 찾고자 하는 행렬이다. 그리고 알고리즘 상에는 그 행렬의 기본 행연산을 통해 윗삼각행렬을 구하는 과정이 포함되어 있다. 생성행렬이 선형행렬이라면 부호 간의 기본 행연산을 하더라도 같은 부호가 나타나지만 새로운 암호시스템의 생성행렬은 난수 열 벡터가 포함이 되어있기 때문에 비선형행렬이다. 기본 행연산을 통해 계산된 새로운 행은 부호가 되지 않으며 최소 해밍무게를 찾을 수가 없게 된다.

Ⅵ. 결론

본논문에서는 기존의 암호시스템에 비해 보안성이 높은 puncturing, insertion, 그리고 shortening 을 이용한 McEliece 암호 시스템을 제안하였다. 이는 부호가 비선형인 성질을 통해 Stern 의 공격을 막을 수 있고, 행렬의 크기를 조절할 수 있어서 행렬크기로 부호의 종류를 알아내어 공격하는 것 또한 막을 수 있다.

추가로 부호의 종류를 알더라도 거기에 특화된 공격을 난수 열 벡터를 통해 막을 수 있는지에 대한 연구를 진행할 것이다.

참 고 문 헌

[1] R. J. McEliece “A public key cryptosystem based on algebraic coding theory,” DSN progress report, pp. 107-124, 1978.

[2] P. Goborit, “Shroter keys for code based cryptography,” in Proc. WCC, 2005, pp,81-91

[3] R. Misoczki et al. “MDPC-McEliece: New McEliece variants from moderate density parity-check codes,” in Proc IEEE ISIT, 2013, pp. 2069-2073.

[4] V. M. Sidelnikov and S. O. Shestakov, “On insecurity of cryptosystems based on generalized Reed-Solomon codes,” Discrete Math. Appl., vol. 1, no. 4, pp. 439-444, 1992.

[5] M. Baldi, M. Bodarato, F. chiaraluce, “A new analysis of the McEliece cryptosystem based on QC-LDPC codes,” Security Cryptography for Netw., pp. 246-262, 2008.

[6] V. M. Sidelnikov, “ A public-key cryptosystem based on Reed-Muller codes,” Discrete Math Appl., vol. 4, no. 3, pp.191-207, 1994

[7] J. Stern, “A method for finding codewords of small weight,” in Proc. Coding Theory and Appl., pp. 106-113, 1989

[8] A. Canteaut and F. Chabaud, “A new algorithm for finding minimum-weight words in a linear code: Application to McEliece’s cryptosystem and to narrow-sense BCH codes of length 511,” IEEE Trans. Inf. Theory, vol. 44 no. 1, pp. 367-378, 1998

[9] A. May, A. Meurer, and E. Thomae, “Decoding random linear codes in O(20.054n),” ASIACRYPT, vol. 7073, pp. 107-124, 2011.