높은 부호율을 갖는 Goppa 부호 기반 암호시스템 및 전자서명에서 열 추가 및 삭제 기법 적용

이위직, 노종선
서울대학교 뉴미디어통신공동연구소

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

Modification of high rate Goppa code-based cryptosystem and signature

Lee Wijik, No Jong-Seon
Seoul National Univ. INMC

요 약

본 논문은 열 추가 및 열 삭제 기법을 적용한 높은 부호율을 갖는 Goppa 부호 기반 암호시스템을 제안하였다. 기존에 높은 부호율을 갖는 Goppa 부호를 적용한 암호시스템은 취약성이 드러났다. 랜덤 부호와 스크램블링 및 순열 행렬에 뒤섞인 Goppa 부호는 서로 구분되지 않아야 하는데 이를 구분하는 알고리즘이 제안 되었다. 본 논문에서는 열 추가 및 열 삭제 기법을 통해 랜덤 행렬과의 구분을 피할 수 있음을 제시하였다.

Ⅰ. 서 론

McEliece 암호 시스템은 최근 양자 컴퓨터에 대한 연구가 진행되며 포스트 양자 암호로 주목을 받고있다. 1987 년에 Goppa 부호를 기반으로 한 생성행렬을 이용한 McEliece 암호 시스템이 제안되었다 [1]. 이후에 Niederrieter 에 의해 Goppa 부호의 패리티 행렬을 이용한 Niederrieter 암호 시스템이 제안되었다 [2]. 부호 기반의 암호 시스템은 제안 되었지만 전자 서명은 한동안 제안되지 않았다.

2001 년 Courtois, Finiasz, 그리고 Sendrier 에 의해 CFS 전자서명이 제안되었다 [3]. 하지만 CFS 전자서명은 서명 과정에 오랜 시간이 걸리는 단점이 있다. 서명이 될 메시지가 복호 가능해야 하는데 그 확률이 매우 낮으므로 복호가 가능할 때까지 계속 반복해야 하기 때문이다. 뿐만 아니라 CFS 전자서명에서 복호 가능할 확률은 $1/t!$ 에 비례하는데 확률을 높이기 위해서는 필연적으로 낮은 t값을 사용해야 하며 따라서 부호율이 매우 높아질 수 밖에 없다.

최근 높은 부호율을 갖는 Goppa 부호가 랜덤한 부호와 구분이 되는 문제가 제기 되었다 [4]. 랜덤 부호와 구분이 쉽게 되면 의미론적인 보안 existential unforgeability under adaptive chosen message attack 안전성 (EUF-CMA)을 달성할 수가 없다. 기존에는 EUF-CMA 보안성을 증명한 논문 [5]이 제안되었지만 EUF-CMA 안전성을 증명하는 과정에서 Goppa 부호가 랜덤 부호와 구분이 되지 않아야 한다는 가정을 필요로 했기 때문이다.

하지만 본 논문에서는 열 추가 및 열 삭제 기법을 높은 부호율을 갖는 Goppa 부호에 적용하여, 이 경우에는 랜덤 부호와 구분을 하는 알고리즘이 효과가 없음을 보였다. 따라서 CFS 전자서명도 EUF-CMA 안전성을 확보하였다. 전자서명뿐만 아니라 높은 부호율을 갖는 Goppa 부호를 McEliece 암호시스템에도 적용할 수 있게 되었다.

Ⅱ. 사전 지식

A. Goppa 부호

Goppa 부호는 Alternant 부호 군에 속하는 부호이다. 따라서 Alternant 부호의 parity matrix 로 정의할 수 있다.

정의 1. (Alternant 부호)

벡터 $x = (x_1, \cdots, x_n), y = (y_1, \cdots, y_n)$ 이 주어져 있을 때, $x, y \in \mathbb{F}_{q^m}^n$ alternant 부호 $A_r(x,y)$의 패리티 행렬은 다음과 같다.

$$V_r(x,y) = \begin{pmatrix} y_1 & \cdots & y_n \\ y_1x_1 & \cdots & y_nx_n \\ \vdots & \ddots & \vdots \\ y_1x_1^{r-1} & \cdots & y_nx_n^{r-1} \end{pmatrix}$$

이 때 Alternant 부호 $A_r(x,y)$의 정의는 다음과 같다.

$$\{c | c \in F^n, V_r(x,y)c^T = 0\}$$

정의 2. (Goppa 부호)

Goppa 부호 $G(x,\gamma)$는 연관된 다항식 $\gamma(z)=\sum_{i=0}^{r}\gamma_i x^i$과 함께 정의된다. 벡터 $x=(x_1,\cdots,x_n), y=(y_1,\cdots,y_n)$는 다음 조건을 만족한다. $\gamma(x_i)\neq 0$이고 $y_i=\gamma(x_i)^{-1}$이다. 이 때, Goppa 부호 $G(x,\gamma)=A_r(x,y)$이고 여기서 $A_r(x,y)$는 Alternant 부호이다.

B. Goppa 부호와 랜덤 부호의 구분

G: $k\times n$ 생성행렬이고 암호시스템 및 전자서명에서 스크램블링 및 순열 행렬에 의해 뒤섞인 생성행렬이라고 가정 할 때 다음을 만족하는 Alternant 부호의 패리티 행렬 $V_r(x^*,y^*)$가 존재한다.

$$V_r(x^*,y^*)G^T=0, x^*=(X_1,\cdots,X_n), y^*=(Y_1,\cdots,Y_n)$$

G가 systematic 이라고 할 때, $(\mathrm{G}=(I_k|P), P=(p_{ij})$, 이고 이 때, i,j의 범위는 다음과 같이 주어진다. $1\le i\le k, k+1\le j\le n$)

$$\sum_{j=1}^{n} g_{i,j}Y_jX_j^e=0, \text{for } 1\le i\le k, 0\le e\le r-1$$

다음 식이 성립하므로

$$Y_iX_i^e=\sum_{j=k+1}^{n} p_{ij}\,Y_jX_j^e.$$

여기서 $Y_i(Y_iX_i^2)=(Y_iX_i)^2$이 항등식인 것을 적용하여 대입하면

$$\sum_{j=k+1}^{n} p_{ij}\,Y_j\sum_{j=k+1}^{n} p_{ij}\,Y_jX_j^2=\left(\sum_{j=k+1}^{n} p_{ij}\,Y_jX_j\right)^2$$

이 성립한다. 이 때, $Z_{jj'}=Y_jY_{j'}(X_{j'}^2+X_j^2)$라고 하면 다음 선형 시스템 $\mathcal{L}_p$를 얻을 수 있다.

$$\mathcal{L}_p=\begin{cases}\sum_{j=k+1}^{n-1}\sum_{j'>j}^{n} p_{1j}p_{ij}, Z_{jj'}=0\\ \vdots\\ \sum_{j=k+1}^{n-1}\sum_{j'>j}^{n} p_{kj}p_{ij}, Z_{jj'}=0\end{cases}$$

$\mathrm{Ker}(\mathcal{L}_p)$ 의 차원을 D 라고 할 때, D_{Goppa} 와 D_{Random} 값은 표 1[]과 같다. 높은 부호율일 경우에 r 은 작은 값을 가지며 이때 차원 D 의 값은 각각 $D_{\mathrm{Goppa}}=0$, $D_{\mathrm{Random}}>0$이다. 이 특성으로 Goppa 부호의 생성행렬과 랜덤 행렬을 구분할 수 있다.

Ⅲ. 본문

Goppa 부호와 랜덤 부호를 구분하는 알고리즘의 선형 시스템에서 $Z_{jj'}=Y_jY_{j'}(X_{j'}^2+X_j^2)$ 값이 변수로 쓰인다. 생성행렬 G 에서 i 번째 열을 삭제 후 추가하는 것은 p_{ij} 값을 모두 랜덤한 값 r_{ij} 로 대체하는 것과 같다. p_{ij} 이 바뀐다면 그 방정식에 포함된 모든 $Z_{jj'}$ 값들이 영향을 받게 되며 랜덤한 값들이 $Z_{jj'}$ 의 계수로 곱해진 것으로 볼 수 있다. 따라서 선형 시스템 $\mathcal{L}_p$ 는 선형 독립에 가깝게 되어 $\mathrm{Ker}(\mathcal{L}_p)$는 0 의 값을 가지게 된다. 따라서 랜덤 열 추가 및 삭제 기법으로 랜덤 부호와의 구분이 어려워지게 할 수 있다.

랜덤 부호와의 구분이 어려워지면 기존의 전자서명인 CFS 전자서명에서 의미론적인 보안 EUF-CMA 을 달성할 수 있다. 의미론적 보안을 증명하는 과정에서 Goppa 부호와 랜덤 부호를 구분할 수 없다는 가정을 다시 할 수 있게 되기 때문이다.

Table 1 $m=14$ 일 때 값 비교

r	D_{Random}	D_{Goppa}
10	0	5390
11	0	6776
12	0	8316
13	269	10010
14	2922	11858
15	5771	13860
16	8816	16016
17	12057	18564
18	15494	21294

Ⅳ. 결론

본 논문은 열 추가 및 열 삭제 기법을 적용한 높은 부호율을 갖는 Goppa 부호 기반 암호시스템을 제안하였다. 기존의 CFS 전자서명 시스템에서는 높은 부호율을 갖는 Goppa 부호를 기반으로 하는데, 높은 부호율을 갖는 Goppa 부호는 랜덤 부호와 구분하는 알고리즘이 있어 의미론적 보안 EUF-CMA 를 달성할 수가 없었다. 하지만 열 추가 및 열 삭제 기법으로 구분을 막게 되어 EUF-CMA 를 달성할 수 있게 되는 효과가 있다.

후속 연구로는 최적의 삭제 및 추가(대체)하는 열의 위치를 구하며, 최소한으로 대체 해야 하는 열의 개수를 수학적으로 구할 예정이다.

.

ACKNOWLEDGMENT

이 논문은 2016 년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (R-20160229-002941, IoT 및 클라우드 컴퓨팅을 위한 경량 포스트 양자 암호 시스템 연구)

참 고 문 헌

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

[2] H. Niederreiter, “Knapsack-type cryptosystems and algebraic coding theory,” *Problems of Contro.l and Information Theory*, vol 15, pp. 159-166

[3] N. T. Courtois, M. Finiasz, N. Sendrier, “How to achieve a McEliece-based digital signature scheme,” in *Proc. ASIACRYPT*, 2001, pp. 157-174

[4] J. C. Faugere *et al.*, “A distinguisher for high-rate McEliece cryptosystems,” IEEE *Trans. Inf. Theory*, vol. 59, no. 10, Oct 2013.

[5] L. Dallot, “Towards a concrete security proof of Courtois, Finiasz, and Sendrier signature scheme,” in *Proc. WEWoRC,* vol. 4945, 2007, pp. 65-77