Classic McEliece의 Goppa Polynomial 생성에 관한 연구

김영효*, 김민지*, 전창열**, 김동찬***

*국민대학교(학부생), **국민대학교(대학원생), ***국민대학교(교수)

A Study on Goppa Polynomial Generation of Classic McEliece

Young Hyo Kim*, Minji Kim*, Chang Yeol Jeon**, Dong-Chan Kim***

*Kookmin University(UnderGraduate student)
**Kookmin University(Graduate student)
***Kookmin University(Professor)

요 약

미국 국립 표준 기술 연구소에서 주관한 양자 내성 암호 공모전 4라운드가 진행 중이다. Classic McEliece는 4라운드에 진출한 알고리듬이다. Classic McEliece는 Goppa 부호를 사용하며, Goppa 다항식으로 기약 다항식을 사용한다. 본 논문에서는 최소다항식 생성 알고리듬을 이용한 기약 다항식 생성 알고리듬을 소개하고, FLINT 라이브러리로 구현하여 측정한 시간과 알고리듬의 성공률을 제시한다.

I. 서론

미국 국립 표준 기술 연구소에서 주관한 양자 내성 암호 공모전이 진행 중이다. 현재 4라운드가 진행 중이고, 3라운드에서 4개의 알고리듬이 표준으로 채택되었으며, 4개의 알고리듬이 4라운드에 진출하였다. Classic McEliece는 양자 내성 암호 공모전 4라운드에 진출한 부호기반 암호이다.

Classic McEliece는 Goppa부호를 사용하는 부호기반 암호이다. 이때 Goppa부호를 생성하는 Goppa 다항식은 separable이어야 하는데 기약 다항식이 separable이기 때문에 기약 다항식을 사용한다. Classic McEliece에서는 기약 다항식을 생성하기 위한 알고리듬으로 최소다항식 생성 알고리듬을 사용한다[1].

본 논문에서는 최소다항식 생성을 이용한 기약 다항식 생성 알고리듬을 FLINT 라이브러리를 이용하여 구현하고, 연산시간을 측정한다[2]. 또한 생성하는 기약 다항식에 차수에 따른 알고리듬의 성공률을 확인한다.

논문의 구성은 다음과 같다. Ⅱ절에서는 본 논문에서 사용하는 기호를 정의한다. Ⅲ절에서는 최소다항식 생성 알고리듬을 소개한다. Ⅳ절에서는 FLINT 라이브러리를 이용하여 최소다항식 생성 알고리듬을 구현한 결과를 제시한다.

II. 기호

$\cdot m$	12 또는 13
$\cdot F_2$	2개의 원소를 갖는 유한체
$\cdot F_{2^m} = F_q$	원소의 개수가 $q(=2^m)$개인 유한체
$\cdot F_q[X]$	F_q의 원소를 계수로 하는 다항식 환
$\cdot F_q[X]/<k(X)> \cong F_{q^t}$	t차 기약 다항식 $k(X)$로 정의한 원소의 개수가 q^t개인 유한체
$\cdot a\|\|b$	두 비트열 a와 b의 연접
$\cdot d_i$	비트열 d의 i번째 비트

$\cdot d_{[i:j]}$	$d_{j-1}\|d_{j-2}\|\cdots\|d_i \in \{0,1\}^{j-i}$
$\cdot g \bmod f$	g를 f로 나눈 나머지
$\cdot \deg(f)$	다항식 f의 차수
$\cdot A_{m\times n}$	크기가 $m\times n$인 행렬
$\cdot \{A_{i,j}\}$	행렬 $A_{m\times n}$의 i행 j열 원소

III. 최소다항식 생성 알고리듬

Classic McEliece에서는 최소다항식을 생성하여 기약 다항식으로 사용한다. 최소다항식 생성 알고리듬의 유사부호는 알고리듬 1이다.

알고리듬 1: 최소다항식을 이용한 기약 다항식 생성[3]
입력:$q(=2^m)$, $t\in N$
출력:$g(X)$: 유한체 F_q상의 t차 기약 다항식
1. $g(X)\leftarrow 0$
2. **while** $\deg(g(X))\neq t$ **do**
3. $d_{[16t:0]}\leftarrow$랜덤$16t$비트
4. **for** $j=0$ to $t-1$ **do**
5. $\beta_j \leftarrow d_{[16j+m:16j]}$
6. $\beta\leftarrow\beta_0+\beta_1X+\cdots+\beta_{t-1}X^{t-1}$
7. F_q상의 최소다항식 $g(X)$생성
8. **return** $g(X)$

최소다항식 $g(X)$생성 과정은 다음과 같다.

임의의 $\beta\in F_{q^t}\cong F_q[X]/<k(X)>$에 대한 t차 최소다항식 $g(X)$는 다음을 만족한다.

$$g(\beta)=g_0+g_1\beta+g_2\beta^2\cdots+g_t\beta^t=0.$$
$$(g_1,\cdots,g_t\in F_q)$$

이때 β는 유한체 $F_q[X]/<k(X)>\cong F_{q^t}$의 원소이므로 β의 거듭제곱 $\beta^i,(i=1,\cdots,t)$ 또한 F_{q^t}의 원소이다. β^i를 열벡터로 표현했을 때 $g(\beta)=0$를 다음과 같이 행렬식으로 표현 가능하다.

$$\begin{pmatrix}1\ \beta\ \beta^2\cdots\beta^t\end{pmatrix}\begin{pmatrix}g_0\\g_1\\\vdots\\g_t\end{pmatrix}=\begin{pmatrix}0\\0\\\vdots\\0\end{pmatrix}.$$

β의 거듭제곱 β^i의 계수를 다음과 같이 정의한다.

$$\beta^i=(\beta_0+\beta_1+\cdots+\beta_{t-1})^i \bmod k(X)$$
$$=\beta_0^{(i)}+\beta_1^{(i)}+\cdots+\beta_{t-1}^{(i)}.(\beta_0^{(i)},\cdots,\beta_{t-1}^{(i)}\in F_q, i=1,\cdots,t)$$

이를 이용하여 $g(\beta)=0$을 다음과 같이 행렬곱으로 표현할 수 있다.

$$\underbrace{\begin{pmatrix}1\beta_0^{(1)}\cdots\beta_0^{(t)}\\0\beta_1^{(1)}\cdots\beta_1^{(t)}\\\vdots\ \vdots\ \ddots\ \vdots\\0\beta_{t-1}^{(1)}\cdots\beta_{t-1}^{(t)}\end{pmatrix}}_{A}\begin{pmatrix}g_0\\g_1\\\vdots\\g_t\end{pmatrix}=\begin{pmatrix}0\\0\\\vdots\\0\end{pmatrix}.$$

위 식에서 $g_0,\cdots,g_t$값을 구하기 위해 행렬A를 기약 행사다리꼴로 변경한다. 행렬A가 표준형 행렬일 경우 다음과 같이 표현된다.

$$\begin{pmatrix}10\cdots0\ a_0\\01\cdots0\ a_1\\\vdots\vdots\ddots\vdots\ \vdots\\00\cdots1a_{t-1}\end{pmatrix}\begin{pmatrix}g_0\\g_1\\\vdots\\g_t\end{pmatrix}=\begin{pmatrix}0\\0\\\vdots\\0\end{pmatrix}.$$

위 행렬 곱을 전개하면 다음 연립방정식을 얻을 수 있다.

$$\begin{cases}g_0 & +a_0g_t & =0\\g_1 & +a_1g_t & =0\\ & \vdots & \\g_{t-1} & +a_{t-1}g_t & =0\end{cases}.$$

이때 g는 최소다항식이므로 $g_t=1$이다. 또한 이진 유한체 상의 연산이므로 다음을 얻을 수 있다.

$$\begin{cases}g_0 & = & a_0\\g_1 & = & a_1\\ & \vdots & \\g_{t-1} & = & a_{t-1}\end{cases}.$$

따라서 행렬A를 기약 행사다리꼴로 변경했을 때 표준형 행렬일 경우, β에 대한 t차 최소다항식을 생성할 수 있다. 이때 $t\geq 16$인 경우 99% 이상의 확률로 기약 다항식을 생성한다[1].

이에 대한 유사부호는 알고리듬 2이다.

알고리듬 2: 최소다항식 생성 알고리듬
입력: $\beta, k(X) \in F_q[X] (\deg(\beta) = \deg(k(X) = t)$ 출력:$g(X)$: 유한체 F_q상의 t차 최소다항식 or failure 1. **for** $j = 0$ to t **do** 2. $\{A_{i,j}\} \leftarrow \beta_i^{(j)}$ $(i = 0, \cdots, t-1)$ 3. $A \leftarrow$기약 행사다리꼴(A) 4. **if** $\{A_{t-1,t-1}\} = 0$ **do** 5. **return** failure 6. **for** $j = 0$ to $t-1$ **do** 7. $g_j \leftarrow \{A_{j,t}\}$ 8. $g_t \leftarrow 1$ 9. **return** $g(X) = g_0 + g_1 X + \cdots + g_{t-1} X^{t-1} + X^t$

IV. 구현

최소다항식 생성 알고리듬을 FLINT 라이브러리를 이용하여 구현하였다.

4.1 시간 측정

알고리듬의 시간 측정 환경은 다음과 같다.

하드웨어	Mac book air, Apple M2, 8GB RAM
컴파일러	Apple clang 14.0.0 (-O2)
정수연산 라이브러리	FLINT 2.9.0

[표 1]은 Classic McEliece에서 제안한 파라미터와 t차 기약 다항식 생성 시 걸린 시간이다. $k(X)$는 유한체 $F_{2^m} = F_q$상의 원소를 계수로 하는 기약 다항식이다. t는 Goppa 다항식의 차수이다.

[표 1] Classic Mceliece 파라미터에 따른 기약 다항식 생성시간 (단위: ms/1회)

	m	t	$k(X)$	생성시간
Mceliece 348864	12	64	$X^{64} + X^3 + X + z$	11
Mceliece 460896	13	96	$X^{96} + X^{10} + X^9 + X^6 + 1$	35
Mceliece 6688128	13	128	$X^{128} + X^7 + X^2 + X + 1$	65
Mceliece 6960119	13	119	$X^{119} + X^8 + 1$	58

4.2 성공률 측정

최소다항식 생성 알고리듬 과정 중 행렬을 기약 행사다리꼴로 변환한다. 이때 변환한 행렬표준형 행렬임을 가정한다. 이 가정을 만족하지 않는 경우 최소다항식 생성 알고리듬은 실패한다.

[표 2]는 $t(\leq 16)$차 최소 다항식 생성알고리듬을 100,000회 실행했을 때의 성공률이다.

[표 2] t차 기약 다항식 생성 성공률

차수	성공률
$t = 2$	99.99%
$t = 3$	82.98%
$t = 4$	97.02%
$t = 5$	99.53%
$t = 6$	99.91%
$t = 7$	99.98%
$t \geq 8$	99.99%

V. 결론

논문에서는 Classic McEliece에서 사용하는 separable Goppa 다항식 생성을 위한 기약 다항식 생성 알고리듬을 소개하고 구현하였다. 구현한 알고리듬을 바탕으로 Classic McEliece의 파라미터에 따른 기약 다항식 생성 속도를 측정하고, 기약 다항식 차수에 따른 알고리듬 성공률을 확인하였다.

결과적으로 5차 이상의 기약 다항식을 생성할 때 99% 이상의 확률로 기약 다항식 생성에 성공함을 확인하였다.

ACKNOWLEDGEMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No.NRF-2021R1F1A1062305).

[참고문헌]

[1] CHOU, Tung, et al. Classic McEliece: conservative code-based cryptography, 10 October 2020. 2020.

[2] W. Hart, F. Johansson and S. Pancratz. FLINT: Fast Library for Number Theory, 2013. version 2.4.0, http://flintlib.org.

[3] 전창열; 최장혁; 김동찬. 유한체 상에서의 기약 다항식 생성에 관한 연구. *한국통신학회 학술대회논문집*, 2022, 1456-1457.