천공 Reed-Muller 부호를 기반으로 한 McEliece 암호 시스템

이위직°, 노종선, 김영식*

서울대학교 전기정보공학부 뉴미디어 통신공동연구소, 조선대학교 정보통신공학과*

Punctured Reed-Muller Code-Based McEliece Cryptosystem

Wijik Lee°, Jong-Seon No, Young-Sik Kim*

Department of Electrical and Computer Engineering, INMC, Seoul National University, Department of Information and Communication Engineering, Chosun University*

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

요 약

본 논문에서는 천공 Reed-Muller (RM) 부호를 기반으로 한 McEliece 암호 시스템을 제안하였다. 기존의 RM 부호를 기반으로 한 McEliece 암호 시스템은 Minder-Shokrollahi 공격과 이를 개선한 Chizhov-Borodin 공격에 의해 비밀키를 노출하는 문제가 있었다. 하지만 천공 기법을 통해 이러한 공격들을 막을 수 있음을 증명하였다. 뿐만 아니라 공격을 피하기 위한 최소한의 천공 개수 및 천공 위치도 알아내었다.

1. 서론

McEliece 암호 시스템은 최근 양자 컴퓨터에 대한 연구가 진행되며 포스트 양자 암호로 주목을 받고 있다. 1987 년에 Goppa 부호를 기반으로 한 McEliece 암호 시스템이 제안되었다.

McEliece 암호 시스템의 단점으로는 공개키의 크기가 큰 것이고 이를 해결하기 위해 Goppa 부호 대신 GRS 부호 [2], 극부호 [3], Reed-Muller (RM) 부호 [4] 등을 이용한 암호 시스템이 제안되었다. 하지만 이들의 구조적 특성으로 인해 여러 공격에 의해 취약해졌다.

RM 부호는 많은 오류를 정정할 수 있어 키 사이즈 대비 보안성이 매우 높은 장점이 있지만 Minder-Shokrollahi 의 공격[5]과 이를 개선한 Chizhov-Borodin 공격[6]에 의해 비밀키가 노출되는 문제가 있었다.

본 논문에서는 천공 기법을 통해 RM 부호의 구조를 숨겨 두 공격을 막는 방법을 제안하였다. LDPC 를 기반으로 한 McEliece 의 암호 시스템에 천공 기법을 적용하는 시스템 [7]은 제안되었다. 하지만 이와 다르게 본 논문에서는 최소한의 천공 개수 및 천공 위치도 분석하였다.

2. 사전지식

A. RM 부호

RM 부호 $\mathrm{RM}(r,m)$은 차수가 r보다 작거나 같은 m 변수 Boolean 함수로 된 선형 부호이다.

정리 1. (Minder and Shokrollahi, 2007)

정수 m에 대해 다음식이 성립한다.

$$\mathrm{RM}(0,m) \subset \mathrm{RM}(1,m) \subset \cdots \subset \mathrm{RM}(m,m)$$

RM 부호의 부호 길이, 메시지 길이, 최소 거리는 다음과 같다.

$$n = 2^m, k = \sum_{i=0}^{r} \binom{m}{i}, d = 2^{m-r}.$$

B. RM 부호 기반 McEliece 암호 시스템

RM 부호 기반 McEliece 암호 시스템은 다음과 같다. G는 $\mathrm{RM}(r,m)$ 부호의 생성행렬이고 S는 $k \times k$ 정칙행렬, P는 $n \times n$ 전치행렬이다.

비밀키: S, G, P

공개키: $G' = SGP, t$

암호화: k비트 메시지 m에 대해

$c = mG' + e$를 수행

e는 오류 벡터이고 $\mathrm{wt}(e) = t$

복호화: 양변에 P^{-1}를 곱하면

$cP^{-1} = mSG + eP^{-1}$

복호알고리즘을 통해 오류 eP^{-1}를 고치고 mS값을 얻음. S^{-1}를 곱하여 m 복원.

C. RM 부호 McEliece 암호시스템 공격

C.1 Minder-Shokrollahi 의 공격

Minder-Shokrollahi 의 공격은 전치행렬 P를 찾는 공격이다. 부호 $C = \mathrm{RM}(r,m)^{\sigma}$는 어떤 σ에 의해 전치된 부호라고 하자. 공격을 요약하면 다음과 같다.

1. C의 부호들 중 $\mathrm{RM}(r-1,m)^{\sigma}$에 속하는 부호들을 충분히 찾는다.

2. $\mathrm{RM}(1,m)^{\sigma}$를 찾을 때까지 되풀이한다.
3. $\mathrm{RM}(1,m)^{\tau\cdot\sigma} = \mathrm{RM}(1,m)$인 순열 τ를 찾는다.

C.2 Chizhov-Borodin 의 공격
Chizhov-Borodin 의 공격은 Minder-Shokrollahi 의 공격을 개선한 것이다. $\mathrm{RM}(r,m)$ 이 주어져 있을 때, $\mathrm{RM}(kr,m)$과 직교 부호인 $\mathrm{RM}(m-r-1,m)$을 다항식 시간 안에 구할 수 있다. 그러면 $\mathrm{RM}(kr+l(m-1),m)$ 도 다항식 시간 안에 구할 수 있고 $\mathrm{RM}(\gcd(r,m-1),m)$ 도 마찬가지이다. $\gcd(r,m-1)=1$이면 $\mathrm{RM}(1,m)$을 바로 구할 수 있다.

3. 새로운 암호 시스템

정의
c를 C의 부호라고 하고 L을 인덱스 집합이라고 할 때, $\mathrm{proj}_L(c)$는 c에서 L의 위치에 해당하는 값들을 모은 서브 부호이다. 선형 부호 C에 대해서는 다음과 같다. $\mathrm{proj}_L(C) = \{\mathrm{proj}_L(c) | c \in C\}$
천공 RM 부호를 이용한 McEliece 암호 시스템은 다음과 같다.
1) 키생성
1-1) 천공
$C = \mathrm{RM}(r,m)$: $k \times n$ 생성행렬
해밍무게가 최소인 $x \in C$찾음
$\mathrm{proj}_{\mathrm{supp}(x)}(C)$중 해밍무게가 최소인 y찾음
$\mathrm{supp}(y) \subset L_D$를 만족하는 인덱스 집합 L_D선택
G에서 L_D에 해당하는 열을 제거하고 이를 G_D라고 정의.
1-2) S, P 생성
S: $k \times k$ 정칙행렬
P: $(n-|L_D|) \times (n-|L_D|)$ 전치행렬
비밀키: S, G, P, L_D
공개키: $G'_D = SG_DP, t' = \left\lfloor t - \frac{|L_D|}{2} \right\rfloor$
암호화: k비트 메시지 m에 대해
$c = mG'_D + e$를 수행
e는 오류 벡터이고 $\mathrm{wt}(e) = t'$
복호화: 양변에 P^{-1}를 곱하면
$cP^{-1} = mSG_D + eP^{-1}$
L_D에 해당하는 위치에 '?' 삽입 후
복호알고리즘을 통해 오류 eP^{-1}를 고치고 mS값을 얻음. S^{-1}를 곱하여 m 복원.

4. 새로운 암호시스템의 안전성

A. Minder-Shokrollahi 의 공격
다음 정리에 의해 Minder-Shokrollahi 의 공격을 막을 수 있다.
정리 1
RM 부호 $\mathrm{RM}(r,m)$에 대해 최소 $|L_D| = 2^{m-2r}$개의 열 삭제가 필요하다. 이 때, $C_{\mathrm{supp}(x)} \subsetneq C'_{\mathrm{supp}(x')}$가 성립한다.
$C_{\mathrm{supp}(x)} \subsetneq C'_{\mathrm{supp}(x')}$ 가 성립하면 공격에서 $\mathrm{RM}(r-1,m)$의 부호들을 찾을 수 없다. 따라서 공격을 막을 수 있다.
A. Chizhov-Borodin 의 공격
Chizhov-Borodin 의 공격은 RM 부호의 직교 부호는 RM 부호를 이용하였다. 천공 부호의 직교 부호는 단축 부호임을 이용한다. 따라서 천공 RM 부호의 직교 부호는 단축 RM 부호이고 단축에 의해 행이 삭제 되었고 이를 복원하는 것이 어려워 Chizhov-Borodin 의 공격을 막을 수 있다.

ACKNOWLEDGMENT

이 논문은 2017 년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (R-20170229-002941, IoT 및 클라우드 컴퓨팅을 위한 경량 포스트 양자 암호 시스템 연구)

5. 참고 문헌

[1] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," DSN Progress Report, vol. 44, pp. 114-116, 1978.
[2] V. M. Sidelnikov and S.O. Shestakov, "On insecurity of cryptosystems based on generalized Reed-Solomon codes," *Discrete Mathematics and Applications*, vol. 1, no. 4, pp. 439-444, 1992.
[3] S. R. Shrestha and Y.-S. Kim, "New McEliece cryptosystem based on polar codes as a candidate for post-quantum cryptography," in *Proc. ISCIT 2014*, Incheon, Korea, Sep 24-26, 2014, pp. 368-372.
[4] V. M. Sidelnikov, "A public-key cryptosystem based on binary Reed-Muller codes," *Discrete Mathematics and Applications*, vol. 4 no. 3, 1994.
[5] L. Minder and A. Shokrollahi, "Cryptanalysis of the Sidelnikov cryptosystem," in Proc *EUROCRYPT*, 2007, LNCS, vol. 4515, 2007, pp. 347-360.
[6] I. V. Chizhov and M. A. Borodin, "The failure of McEliece PKC based on Reed-Muller codes," *IACR Cryptology ePrint Archive*, Report 2013/287 (2013).
[7] M. Esmaeili, M. Dakhilalian, and T. A. Gulliver, "New secure channel coding scheme based on randomly punctured quasi-cyclic low-density parity check codes," *IET Commun.*, vol. 8, no. 14, pp. 2556-2562, Sep. 2014.
[8] V. M. Sidelnikov and A. S. Pershakov, "Decoding of Reed-Muller codes with a large number of errors," *Problems of Information Transmission*, Vol. 28, no. 3, pp. 269-282, Jan. 1993.
[9] P. Lee and E. Brickell, "An observation on the security of McEliece's public key cryptosystem," in *Proc. Advances in Cryptology-EUROCRYPT'88*, vol. 330, pp. 275-280, Springer Verlag (1989).
[10] E. C. Boyle and R. J. McEliece, "Asymptotic weight enumerators of randomly punctured, expurgated, and shortened code ensembles," in Proc. *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*, Sep. 2008, pp. 910-917.