RM 부호 기반 전자서명 시스템

이위직, 노종선, 김영식*
서울대학교 뉴미디어통신공동연구소, *조선대학교

leewj422@ccl.snu.ac.kr, jsno@snu.ac.kr, *iamyskim@Chosun.ac.kr

RM Code-based signature scheme

Lee Wijik, No Jong-Seon, Kim Young-Sik*
Seoul National Univ. INMC, *Chosen Univ.

요 약

본 논문은 shortened and lengthened RM 부호 기반 전자서명 시스템을 제안하였다. 기존의 부호 기반 전자서명 시스템인 Courtois, Finiasz, Sendrier (CFS) 전자서명 시스템을 개선하였다. CFS 전자서명 시스템으로는 복호화 과정이 포함된 서명 과정에서 오랜 시간이 걸리는 단점이 있는데 RM 부호를 이용해서 서명 시간을 줄이고 Shortening 과 lengthening 기법을 통해 RM 부호의 안전성을 확보하였다.

Ⅰ. 서 론

최근 양자 컴퓨터의 출현으로 기존의 전통적인 암호인 RSA 암호, 타원곡선 암호 등의 암호 시스템은 모두 취약성이 드러났다. 양자 컴퓨터의 공격으로부터 안전한 포스트 양자 암호 시스템에 대한 연구가 진행되고 있다. 이 중 하나인 McEliece 암호 시스템 [1]과 Niderreiter 암호 시스템 [3]은 통신 기술의 채널 코딩을 기반으로 한 부호 기반 암호 시스템이다. 부호 기반 암호 시스템은 양자 컴퓨터의 공격에 취약하지 않아서 최근 포스트 양자 암호의 후보로 대두되고 있다.

부호를 기반으로 한 암호 시스템 뿐 아니라 전자 서명 시스템도 활발히 연구가 되고 있다. 그 중에 하나로 나온 것이 Courtois, Finiasz, Sendrier (CFS) 전자 서명 [3]이다. CFS 전자 서명은 McEliece 암호 시스템과 동치인 부호를 기반으로 한 Niederreiter 암호 시스템 [2]을 활용한 것이다. 하지만 CFS 전자 서명은 서명 과정에 오랜 시간이 걸리는 단점이 있다. 서명이 될 메시지가 복호 가능해야 하는데 그 확률이 매우 낮으므로 복호가 가능할 때까지 계속 반복해야하기 때문이다.

부호를 기반으로 한 전자서명은 CFS 전자서명 이외에도 Kabatianskii, Krouk, Smeets (KKS) 전자서명 [4] 이 있다. 하지만 이 서명은 Otmani 와 Tillich [5]의 공격에 취약한 것으로 드러났다.

본논문에서는 CFS 전자 서명의 단점을 개선한 새로운 shortened and lengthened RM 부호 기반 전자서명 시스템을 제안하였다. RM 부호는 closest coset decoding 이 가능하여 오류 정정 한계인 t보다 큰 부호에 대해서도 가장 가까운 부호로 decoding 할 수 있다. t에 대한 제약이 없다면 복호 가능할 확률이 매우 높아져 서명 과정에 걸리는 시간을 줄일 수 있다.

하지만 한 가지 문제로 RM 부호를 기반으로 암호 시스템은 Minder-Shokrollahi[6] 공격, Chizhov-Boroding[7] 공격에 취약하다. 이를 개선하기 위해 RM 부호 생성행렬의 puncturing 과 insertion[8]에 대응되는 패리티 검사행렬의 shortening 과 lengthening 을 동시에 적용하여 두 공격으로부터 안전성을 확보하였다.

Ⅱ. 사전 지식

A. CFS 전자서명

CFS 전자서명은 키 생성, 전자서명, 확인 총 3 단계로 나뉘어진다.

키 생성

H: 패리티 검사 행렬
S: 스크램블링 행렬
P: 순열 행렬
γ: 복호 알고리즘
공개키 $H' = SHP$
비밀키 S, H, P

전자서명

$i \leftarrow i + 1$
$s_i = S^{-1}h(h(m)|i)$가 복호 가능한 최소의 i를 찾음. 복호 가능할 때 $s = s_i$
$HPz^T = s$를 만족하는 z계산
서명은 (m, z, i)가 됨

확인

z의 해밍 무게가 t보다 작은지 확인
$s' = H'z^T$와 $s = h(h(m)|i)$를 각각 계산
$s' = s$일치하면 서명이 맞음.

CFS 전자서명 알고리즘의 문제점으로는 서명이 될 메시

지가 복호 가능해야 하는 것이다. H를 Goppa 부호의 패리티 검사 행렬이라고 가정할 때, 신드롬에 해당하는 서명이 될 메시지인 $Q^{-1}h(h(m)|i)$가 복호 가능할 확률은 $1/t!$정도 이다. t가 10 으로 일 때 성공할 확률이 대략 2^{-11}으로 확률이 매우 낮아서 서명하는데 시간이 매우 오래 걸림.

Ⅲ. 본문

A. 새로운 전자서명 시스템

본논문에서는 CFS 전자서명을 개선한 새로운 전자서명 시스템을 제안하였다. CFS 전자서명과 마찬가지로 키생성, 전자서명, 확인 3 단계로 이루어진다.

키 생성

H: RM(r,m)의 패리티 검사행렬 (systematic)
H_{sd}: RM(r,m)의 shortened and lengthened 행렬
S: 스크램블링 행렬
P: 순열 행렬
γ: Closest coset 복호 알고리즘
공개키 $H' = SH_{sd}P$
비밀키 S, H, H_{sd}, P

전자서명

1) Closest coset 찾기
$s_i = S^{-1}h(h(m)|i)$
$e'^T = Pe^T, s' = S^{-1}s_i$일 때, $He'^T = s'$를 만족하는 e'를 하나 계산. Closest coset decoding 을 통해 e^*를 구함.
$e^* = \gamma(e)$
2) Shortening 과 Lengthening
$He^{*T} = s'$가 만족.
이때 shortening, lengthening 된 부분을 알고 있으므로 그 부분만 수정하여 $H_{sd}e_{sd}^{*T} = s'$를 만족하는 e_{sd}^*를 구함.
만약 e_{sd}^*의 해밍 무게가 $2t$보다 크면
처음으로 돌아가서 i를 증가.
해밍 무게가 $2t$보다 작으면
서명 $\sigma = (m, e_{sd}^*, l)$를 보냄

확인

e_{sd}^*의 해밍 무게가 $2t$보다 작은지 확인.

$H'e_{sd}^{*T} = h(h(m)|l)$인지 확인

둘다 맞는 경우 서명이 맞음.

B. 새로운 전자서명 시스템에 대한 안전성

새로운 전자서명 시스템의 해밍 무게의 제한이 $2t$이므로 t 보다 큰 서명이 선택될 경우에는 보안성이 떨어지는 단점이 생긴다. 전자 서명에 대한 가장 큰 공격으로는 위조를 하는 공격이 있다. 공격자는 임의로 메시지 m과 l 을 정하고 거기에 대응하는 신드롬 값인 $s = h(h(m)|l)$을 구한다. 그리고 선형 방정식 $H'e_{sd}^{*T} = s$ 를 만족하는 e_{sd}^{*T}를 직접 계산한다. 만약 해밍 무게가 t보다 작은 e_{sd}^{*T}를 찾아야 한다면 이것은 신드롬 복호 문제인 NP-난해 문제를 풀어야 해서 불가능하지만 t보다 큰 e_{sd}^{*T}를 찾는 것은 불가능한 문제가 아니다. 따라서 H'의 준역행렬을 구하는 문제를 통해 확률적으로 e_{sd}^{*T}를 구할 수 있다. 만약 H의 파라미터 값이 $n = 1024, k = 386$라면 H의 준역행렬을 구하는데 대략 $386^3 = 2^{34}$정도의 계산이 필요하다. 하지만 준역행렬 연산을 통해 e_{sd}^{*T}를 구하더라도 새로운 무게 제약 조건인 $2t$를 넘는다면 계산을 다시 해야하므로 더 높은 계산복잡도를 가지게 될 것이다.

Ⅳ. 결론

본논문에서는 shortened and lengthened RM 부호를 기반으로 한 새로운 전자서명 시스템을 제안하였다. 기존의 CFS 전자서명에서 RM 부호의 closest 복호를 이용하여 서명이 될 메시지가 복호 가능할 확률을 높여서 서명에 오랜 시간이 걸리는 단점을 개선하였으며 shortened and lengthened 기법을 통해 RM 부호의 취약성을 개선하였다..

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] 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] G. Kabatianskii, E. Krouk, and B. Smeets, “A digital signaturescheme based on random error-correcting codes,” in *Proc. International conference on cryptography and coding,* 1997, pp. 161-167

[5] A. Otmani and J.-P. Tillich, “An efficient attack on all concrete KKS proposals,” in *Proc. PQCrypto*, 2011, pp. 98-116.

[6] L. Minder and A. Shokrollahi, “Cryptanalysis of the Sidelnikov cryptosystem,” in *Proc. EUROCRYPT 2007*, LNCS, no. 4515, pp. 347-360.

[7] I. V. Chizhov and M. A. Borodin, “The failure of McEliece PKC based on Reed-Muller codes,” *Prikl. Diskr. Mat. Suppl.*, no. 6, pp. 48-49, 2013.

[8] W. Lee, J.-S. No, and Y.-S. Kim, “Punctured Reed-Muller code-based McEliece cryptosystems,” *IET Commun.*, accepted in May, 2017.