체계적인 패리티 행렬을 이용한 부호 기반 전자서명 시스템

이위직, 노종선
서울대학교 뉴미디어통신공동연구소

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

Code-based signature scheme with systematic parity-check matrix

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

요 약

본 논문은 체계적인 패리티 (systematic parity check) 행렬을 이용한 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 매우 오랜 시간이 걸리는 단점이 있는데 복호화 과정을 단순화하고 서명이 될 메시지가 복호 가능할 확률을 높여 이를 해결하였다.

Ⅰ. 서 론

McEliece 암호 시스템 [1]은 통신 기술의 채널 코딩을 기반으로 한 부호 기반 암호 시스템이다. 최근 양자 컴퓨터에 대한 연구가 진행되며, 양자 컴퓨터가 개발된다면 기존의 RSA 암호나 타원 곡선 암호 등의 암호 시스템은 모두 취약해진다. 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 연구가 되고 있다. 그 중에 하나로 나온 것이 Courtois, Finiasz, Sendrier (CFS) 전자 서명 [2]이다. CFS 전자 서명은 McEliece 암호 시스템과 동치인 부호를 기반으로 한 Niederreiter 암호 시스템 [3]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 부호 기반 전자서명 시스템을 제안하였다. 기존의 CFS 전자서명에서 복호화 과정을 단순화 하였으며 서명이 될 메시지가 복호 가능할 가능성을 높여서 서명 과정에 걸리는 시간을 줄였다.

Ⅱ. 사전 지식

A. CFS 전자서명

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

키 생성

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

전자서명

$i \leftarrow i + 1$
$s_i = Q^{-1}h(h(m)|i)$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 메시지가 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. 복호화 알고리즘 대신 간단한 연산을 이용하는 알고리즘을 도입하고 z의 해밍무게가 t보다 큰 값을 이용하였다.

키 생성

$H = [R|I]$, R은 임의의 $(n-k) \times k$ 행렬, $I: (n-k) \times (n-k)$ 항등 행렬

Q: 스크램블링 행렬

P: 순열 행렬

공개키 $H' = QHP, w$

비밀키 Q, H, P

전자서명

메시지 m에 대해서 $m' = Q^{-1}h(m)$을 계산.(h는 해쉬함수)

H의 임의의 행렬 부분인 R의 열을 $r_1, r_2, \cdots, r_k$라고 하고 연산 $*$를 다음과 같이 정의

$$a * b = \sum_{i=1}^{n-k} c_i$$

$$c_i = \begin{cases} 1, & a_i = b_i = 1 \\ -1, & a_i = 1, b_i = 0 \\ 0, & \text{else} \end{cases}$$

$z' = (a|p)$라고 정의. z', a, p는 크기가 $n, k, n-k$인 벡터

$a \leftarrow 0, p \leftarrow m$

$i = 1$ 부터 k

  $r_i * m' \geq 2$이면

  $a_i \leftarrow 1 - a_i, p \leftarrow p + r_i$

  z'의 해밍 무게 $< w$ 가 되면 중단

서명은 $(P^{-1}z', m) = (s, m)$

확인

s의 해밍 무게가 w보다 작은 경우

$H's = m$이면 서명이 맞음

B. 새로운 전자서명 시스템에 대한 공격

해밍 무게가 t보다 큰 경우에는 보안성이 약간 떨어지는 단점이 생긴다. 전자 서명에 대한 가장 큰 공격으로는 위조를 하는 공격이 있다. 공격자는 임의로 메시지 m을 정하고 거기에 대응하는 신드롬 값인 $h(m)$을 구할 수 있다. 그리고 선형 방정식 $H'z = h(m)$을 만족하는 z를 직접 계산한다. 만약 해밍 무게가 t보다 작은 z를 찾아야 한다면 이것은 신드롬 복호 문제인 NP-난해 문제를 풀어야 해서 불가능하지만 t 보다 큰 z 를 찾는 것은 불가능한 문제가 아니다. 따라서 H'의 준역행렬을 구하는 문제를 통해 확률적으로 z를 구할 수 있다. 만약 H의 파라미터 값이 $n = 1000, k = 500$ 라면 H 의 역행렬을 구하는데 대략 $500^3 = 2^{27}$ 정도의 계산이 필요하다. 하지만 역행렬 연산을 통해 z를 구하더라도 새로운 무게 제약 조건인 w를 넘는다면 계산을 다시 해야하므로 더 높은 계산복잡도를 가지게 될 것이다.

Ⅳ. 결론

본논문에서는 부호를 기반으로 한 새로운 전자서명 시스템을 제안하였다. 기존의 CFS 전자서명에서 복호화 과정을 단순화하고 서명이 될 메시지가 복호 가능할 확률을 높여서 서명에 오랜 시간이 걸리는 단점을 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] N. T. Courtois, M. Finiasz, N. Sendrier, “How to achieve a McEliece-based digital signature scheme,” in *Proc. ASIACRYPT*, 2001, pp. 157-174

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

[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.