Durandal 소개 : 양자 내성을 지닌 블록체인 전자서명 방식

김형주*, 김영식**, 이흥노**
GIST ITRC 블록체인 지능 융합 센터* / 리버밴스㈜**
hyeongju1994@gm.gist.ac.kr

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2021- 0- 00118, Development of decentralized consensus composition technology for large- scale nodes) and This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program(IITP- 2021- 0- 01835) supervised by the IITP(Institute of Information & Communications Technology Planning & Evaluation)

블록체인은 암호학 기술에 의존하여 중앙 기관의 개입 없이 상호간의 거래를 가능하게 한다. 이는 반대로 생각하면 암호 기술에 취약점이 생기면 블록체인 전체에 큰 악영향을 미치게 될 것이다. 현재까지는 블록체인에서 쓰이는 해시(Hash) 함수나 전자서명에 쓰이는 RSA, ECDSA, 등의 암호시스템을 다항시간 내에 깰 수 있는 효율적인 알고리즘이 존재하지 않는다.

하지만 양자컴퓨터가 나오면 상황이 달라진다. 전자서명에서 쓰이는 RSA 암호의 경우 쇼어 알고리즘(Shor algorithm)에 의해 매우 쉽게 깨지게 됨이 증명되었다[1]. 따라서 여러 기관에서는 기존의 암호시스템을 대체할 양자 후 암호에 대한 연구를 진행 중이다.

블록체인에서는 높은 트랜잭션 처리율(TPS)이 블록체인의 성능을 결정짓는 중요한 요소가 된다. 따라서 작은 키 사이즈로 빠르면서도 양자내성을 갖는 전자서명 알고리즘에 대한 연구가 필요하다.
이를 만족하는 암호시스템 중 하나로, Durandal [2]은 아직까지 양자컴퓨터로 효율적인 공격 알고리즘이 존재하지 않는 부호이론기반(code- based) 문제로 고안되었다.

일반적으로 부호이론에 입각한 전자서명에는 hash- and- sign 방식과 Fiat- Shamir 변환을 통한 인증 두 가지 방식이 있다. 후자의 경우는 큰 키 사이즈가 요구되어 블록체인에 적용하기 어렵다. 전자의 경우는 Hamming metric을 이용한 CFS 서명과 Durandal과 같은 rank metric을 이용한 RankSign 서명이 있다. Durandal은 Lyubashevsky의 격자기반(Lattice- based)을 변형으로 만든 RSL(Rank Support Learning) 기반의 전자서명 기법으로 비교적 작은 키 사이즈로 빠른 서명 및 증명이 가능한 장점을 가지고 있다. 아래 표는 Durandal에서 키 생성, 서명, 검증 단계의 알고리즘을 요약한 것이다. (서명단계에서 μ는 message)

키 생성 (q,k,m,n,l,l')

유한체 $\mathbb{F}_{q^m}$ 내에서 $(n-k)\times n$ 행렬 H 와 각각 임의의 l 개의 벡터 s_i 와 l' 개의 벡터 s'_i 를 만들어 $t_i = Hs_i^T, t'_i = Hs'^T_i$ 를 계산한 뒤, 다음과 같은 공개키와 비밀키를 생성한다.

공개키 = $(H, t_1,\cdots,t_l, t'_1,\cdots,t'_{l'})$

비밀키 = $(s_1,\cdots,s_l, s'_1,\cdots s'_{l'})$

Output : 공개키, 비밀키

서명 (μ,S,S') - S는 모든 s_i의 집합

r,w,d 차원의 임의의 부분공간 E,W,F 에서 임의의 y 벡터를 공간 $(W+EF)^n$ 에서 선택하여 $x = Hy^T$ 와 $c = Hash(x,F,\mu)$를 계산한다.

EF 의 부분공간 U 로부터 $Supp(z)\subset W+U$ 를 만족하는 $z = y+cS'+pS$ 를 계산한다. 이때 p 는 $p=(p_1,\cdots,p_{lk})\in F$ 이며 다음의 원소를 갖는다.

$p_i = \sum_{l=1}^{d} p_{il} f_l$ 여기서 $f_1,\cdots,f_d$ 는 F 의 기저이다.

Output : (z,F,c,p)

검증 (μ,z,F,c,p,H,T,T')

$\|zv\| \le rd+w-\lambda$ 임을 확인

$Hash(Hz^T - T'c^T + Tp^T, F, \mu) = c$ 임을 확인

Output : True or False

위 알고리즘을 Intel® Core™ i5- 7600 CPU @ 3.50GHz 환경에서 고정된 파라미터 m= 263, n= 226, k= 113, l= 4, l'= 1, q= 2, d= 7, r= 7, λ = 14 로 실험한 결과 평균 키 생성 시간 4.3ms, 서명 시간 17.8ms, 검증 시간 10ms로 블록체인에 적용하기에 문제 없는 성능을 보였다.

참고문헌

[1] Shor, P. W., Proceedings of the 35th Symposium on Foundations of Computer Science, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, California), pp. 124–134, 1994.

[2] Nicolas Aragon, Olivier Blazy, Philippe Gaborit, Adrien Hauteville, and Gilles Z´emor, Durandal: a rank metric based signature scheme. IACR Cryptology ePrint Archive, 2018.