정 보 보 호 학 회 지
제 33 권 제2호, 2023. 4

양자내성 전자서명의 블록체인 적용에 관한 연구동향

김 한 결*, 위 다 빈*, 박 명 서**

요 약

양자 컴퓨터의 기술이 발전됨에 따라 Shor 알고리즘과 Grover 알고리즘을 통해 기존의 공개키, 대칭키 및 해시 암호체계에 위협을 줄 수 있다. RSA 및 ECC 암호체계는 Shor 알고리즘에 의해 다항시간 내에 해독이 가능해진다. 이러한 보안 위협의 증가로 양자내성의 성질을 지닌 양자내성암호가 주목받고 있으며 양자내성 전자서명을 블록체인의 전자서명에 적용하기 위한 다양한 연구가 진행되고 있다. 본 논문에서는 양자내성암호를 블록체인의 전자서명에 적용하는 연구동향에 대해 설명한다.

Ⅰ. 서 론

양자컴퓨터의 발전은 기존의 암호체계에 막대한 영향을 준다. 기존의 컴퓨터는 비트 단위로 연산을 수행하는 데 반해 양자컴퓨터는 양자역학의 원리를 이용한 양자비트라고 불리는 양자 단위를 사용한다. 양자비트는 0과 1뿐만 아니라 이들의 중간값인 중첩상태를 가질 수 있는데 이를 통해 복잡한 연산을 더 빠르게 수행할 수 있다. 이렇게 발전된 양자컴퓨터의 뛰어난 연산량을 통해 암호 알고리즘에서 사용한 키를 해독할 수 있다. 특히, 소인수 분해와 이산 대수 문제의 어려움에 안전성을 기반을 두고 있는 공개키 알고리즘인 RSA와 ECC (ECC, Elliptic Curve Cryptography)는 양자 컴퓨터가 상용화되면 Shor 알고리즘으로 인해 충분한 안전성을 제공하지 못한다. 이러한 보안 위협을 극복하기 위해 양자내성의 성질을 가진 양자내성암호가 발전하고 있다. 양자내성암호 도입을 통해 양자 컴퓨터로 인한 기존의 암호체계를 위협하는 문제를 극복할 수 있다.

블록체인(Blockchain)은 분산된 네트워크에서 발생하는 모든 거래내역을 공유하는 탈중앙화된 거래처리 기술로써, 무결성 및 안정성을 보장하기 위해 해시함수와 전자서명의 암호화 기술을 사용한다. 그러나 이러한 블록체인의 암호화 기술 역시 양자컴퓨터의 발전으로 보안 위협을 받게 된다. 이를 위해 양자내성암호를 블록체인에 적용하는 다양한 연구가 진행되고 있다. 본 고에서는 블록체인에 양자내성전자서명을 적용한 연구 동향을 소개한다. 2장에서는 양자내성암호를 알아본다. 3장에서는 양자내성암호를 이용한 전자서명 알고리즘을 살펴본다. 4장에서는 양자내성전자서명을 블록체인에 적용하기 위한 연구를 알아본다. 마지막으로 5장에서 결론을 내린다.

Ⅱ. 양자내성암호

양자내성암호는 양자컴퓨터 기술에 대응하기 위해 개발된 암호화 기술이다. 양자컴퓨터에서는 기존의 암호화 방식에서 사용되는 공개키 암호화 방식이 취약해진다. 이는 양자컴퓨터의 빠른 연산속도로 대규모 연산을 수행할 수 있기 때문이다. 양자내성암호는 이러한 문제를 해결하기 위해 개발되었다. 불확실성 원리를 이용한 암호화 방식을 가지고 있는 양자내성암호는 양자컴퓨터의 빠른 연산속도에 대해서도 안전하게 사용할 수 있다. 현재 미국 국립표준기술연구소(NIST, National Institute of Standards and Technology)를 중심으로 활발한 연구가 진행되고 있다. NIST의 Round 3 최종후보 전자서명 알고리즘에는 CRYSTALS-DILITHIUM과 FALCON, RAINBOW이 있다[1].

양자내성암호는 기반하는 수학적 난제에 따라 격자 기반, 해시 기반, 다변수 기반, 코드 기반, 아이소제니 기반으로 나뉜다.

격자 기반 양자내성암호는 격자이론을 기반으로 한

* 강남대학교 소프트웨어응용학부 (학부생, biequal@kangnam.ac.kr, 학부생, dbwe@kangnam.ac.kr)
** 강남대학교 ICT융합공학부 (조교수, pms91@kangnam.ac.kr)

다. 여기서, 격자는 벡터 공간에서 생성된 규칙적인 모양을 가지는 모임으로, 이산적인 수학적 구조이다. 격자기반암호는 NP-완전 문제를 해결할 수 있는 능력과 함께 양자컴퓨터에 대한 내성을 제공한다. 대표적인 격자 기반 양자내성암호는 FALCON과 CRYSTALS-DILITHIUM, NTRU, SABER, CRYSTALS-KYBER, Rlizard이 있다.

해시 기반 양자내성암호는 해시함수의 충돌 저항성 문제에 기반하고 있다. 해시함수 기반 암호는 그로버 알고리즘에 의해 보안성이 감소되지만, 단순히 긴 길이의 해시 출력을 사용하는 것으로 안전성을 유지할 수 있다. 또한, 빠르고 정량적 보안 수준을 계산할 수 있으며, 안전성도 증명된 상태라는 것이 강점으로 작용한다. 대표적인 해시기반 양자내성암호는 SPHINCS+와 XMSS가 있다.

다변수 기반 양자내성암호는 유한체 상에서 계산하는 다변수함수 문제의 어려움에 기반하는 암호 시스템이다. 다변수 기반은 안전성과 연산 효율성을 위해 주로 이차함수를 사용한다. 암호화와 복호화가 다항식의 계산이기 때문에 전력 분석의 부채널 공격에 안전하다는 장점이 있지만, 긴 키 길이로 인해 주로 서명 기법에 사용된다. 대표적인 다변수 기반 양자내성암호로는 RAINBOW, GeMMS, HiMQ가 있다.

코드 기반 양자내성암호는 오류정정 부호 기술을 이용하여 구현된다. 오류정정 부호는 데이터의 전송 및 저장 중에 발생할 수 있는 오류를 검출하거나 복원하는데 사용된다. 대표적인 코드 기반 양자내성암호의 종류로는 McEliece, HQC, BIKE가 있다.

아이소제니 기반 양자내성암호는 ECC 기반 암호와 같이 유한체 상의 연산을 기반으로 하지만, 타원곡선 대신 이차형식을 이용한 아이소제니 매핑 함수를 사용한다. 아이소제니 매핑 함수는 두 개의 타원곡선을 연결하는 함수이며 이를 통해 보안성을 제공한다. 대표적인 종류로는 SIDH, SIKE가 있다.

Ⅲ. 양자내성암호의 전자서명

3.1. FALCON

FALCON은 Fast Fourier Lattice-based Compact Signatures over NTRU의 줄임말로써, GPV Framework, NTRU, fast Fourier 샘플링이 융합된 형태의 양자 컴퓨터로부터 내성을 가진 양자내성암호 및 전자서명 알고리즘이다[2]. NTRU (N-Th degree Truncated Polynomial Ring Units)와 FFT (Fast Fourier Transform)를 기반으로 하여 기존의 RSA 및 ECDSA와 같은 서명 알고리즘과 다르게 양자 컴퓨터의 공격에 대한 내성을 가지며 대규모 다항식을 효율적으로 처리할 수 있다.

FALCON은 키 생성 단계에서 NTRU 방정식을 푼 후 FALCON tree를 해결한다. 마지막 단계에서는 LDL 트리의 리프를 정규화하여 FALCON tree로 변환한다. 결과적으로 개인키 sk에 래핑되고 해당 공개키 pk는 $h = gf^{-1} \bmod q$로 대응되는 공개키와 함께 제공된다. 서명 생성 단계에서는 먼저 메시지 m과 $saltr$에서 해시값 $c \in Zq[x]/(\Phi)$을 계산하고, 이를 이용해 비밀키 f, g, F, G를 사용하여 짧은 값 $s1$, $s2$를 계산한다. 서명 검증 과정에서는 공개키 $pk = h$, 메시지 m, 서명 $sig = (r,s)$ 및 허용 범위 '⌊β2⌋'가 주어지면 검증자는 pk를 사용하여 sig가 이후에 지정된 메시지 m에 대한 유효한 서명인지 확인한다.

FALCON 공식 사이트에서 제공하는 명세 및 벤치마크 결과는 [표 1]과 같다[3]. 이는 인텔 ®Core®i5-8259U, 2.3GHz, TurboBoost 비활성화 환경에서 측정되었다.

〔표 1〕 NIST Round3 FALCON 명세 및 벤치마크 결과

Name	FALCON-512	FALCON-1024
keygen (ms)	8.64	27.45
keygen (RAM)	14,336	28,672
sign (ms)	59,481,000	2,913,000
verify (ms)	27,933,000	13,650,000
pub size (kB)	0.897	1.793
sig size (kB)	0.666	1.280

3.2. CRYSTALS-DILITHIUM

CRYSTALS-DILITHIUM은 양자 내성을 가지는 양자 내성 암호 시스템으로, 전자서명에서 활용할 수 있으며 격자기반암호시스템에서 중요한 개념인 LWE (Learning With Error)를 기반으로 한다. LWE는 정수를 요소로 하는 벡터의 내적을 통해 암호화를 수행한다. 이를 풀기 위해서는 랜덤 벡터와 암호화된 벡터의 내적을 찾아야 하기 때문에 양자 컴퓨터에서 공격을

수행하더라도 현재 최선의 알고리즘보다 훨씬 많은 시간과 자원이 필요하다. 이러한 원리로 CRYSTALS-DILITHIUM 암호 시스템은 안전하고 빠르게 전자서명을 생성할 수 있다.

키 생성 단계에서는 R_q 링의 다항식으로 구성된 행렬 A를 생성하고, 무작위 비밀 키 벡터를 생성하여 공개키를 계산한다[4]. 이 체계에서 대수 연산은 모두 다항식 링 R_q에서 수행된다. 서명 생성 알고리즘은 계수가 전략적으로 설정된 ɣ1보다 작은 다항식 y의 마스킹 벡터 생성하고 이를 기반으로 서명을 생성한다. 서명 과정에서 거부 샘플링(rejection sampling)을 사용하여 비밀 키가 유출되지 않도록 한다. 서명 검증 과정에서 검증자는 먼저 $Az-ct$의 상위 비트가 되도록 w'_1를 계산한 다음 z의 모든 계수가 $\gamma_1-\beta$보다 작고 c가 메시지의 해시이고 w'_1이면 수락한다.

CRYSTALS-DILITHIUM는 매개변수에 따라 분류되며 공식 사이트에서 제공하는 명세는 [표 2]와 같다[5]. 매개변수에 따라 3가지 세트로 분류되었다.

〔표 2〕 NIST Round3 CRYSTALS-DILITHIUM 명세

Name	DILITHIUM2	DILITHIUM3	DILITHIUM5
pub size (kB)	1.312	1.952	2.592
sig size (kB)	2.420	3.293	4.595

3.3. SPHINCS+

SPHINCS+는 SPHINCS의 개정판으로 상태를 저장하지 않는 비저장해시(stateless hash) 기반 서명 프레임워크이며, 다중 타겟 공격 보호(multi-target attack protection), WOTS+ (Winternitz One-Time Signature) 공개키 압축, FORS (Forest Of Random Subsets) 등의 기술을 포함한다.

개인키에는 모든 WOTS+ 및 FORS 개인키 요소를 생성 시 사용되는 비밀 시드 (SK.seed)와 무작위 메시지 해시에 대한 무작위 값 생성 시 사용되는 PRF 키 (SK.prf) 가 포함되며, 공개키에는 최상위 계층에 있는 트리의 루트(HT 공개키)와 무작위로 균일하게 샘플링되는 공용 시드값 (PK.seed)이 포함된다[6]. 서명 생성 단계에서는 먼저 임의의 값 R이 의사 난수로 생성되고 다음으로 부분 메시지 다이제스트 tmp_md, 트리 인덱스 tmp_idx_tree,리프 인덱스 tmp_idx_leaf 로 구성된 메시지 다이제스트를 계산하는데 사용된다. 그 후 필요한 비트 수를 추출하여 실제 값 md, idx_tree 및 idx_leaf를 계산한다. 부분 메시지 다이제스트 md는 최하위 HT 계층에 있는 idx_tree-th XMSS 트리의 idx_leaf-th FORS 키 쌍으로 서명된다. FORS 키 쌍의 공개키는 HT를 사용하여 서명된다. 서명 검증 단계에서는 메시지 다이제스트 및 인덱스 재계산, 후보 FORS 공개키 계산 및 해당 공개키에서 HT 서명 확인의 절차를 따른다.

SPHINCS+는 매개변수에 따라 분류되며 공식사이트에서 제공하는 스펙은 [표 3]와 같다[7]. [표 3]에는 매개변수에 대한 키 및 서명 크기가 나열되어있다.

〔표 3〕 NIST Round3 SPHINCS+ 명세

Name	public key size (kB)	secret key size (kB)	signature size (kB)
SPHINCS+-128s	0.032	0.064	7.856
SPHINCS+-128f	0.032	0.064	17.088
SPHINCS+-192s	0.048	0.096	16.224
SPHINCS+-192f	0.048	0.096	35.664
SPHINCS+-256s	0.064	0.128	29.792
SPHINCS+-256f	0.064	0.128	49.856

3.4. XMSS

XMSS (eXtended Merkle Signature Scheme)는 Merkle signature scheme을 기반으로하는 고정된 수의 메시지를 서명하는 알고리즘이다. XMSS는 OTS 방식으로서의 WOTS+를 포함하여 총 4가지의 암호화 기술을 사용한다. WOTS+의 사용하는 XMSS의 주요 장점은 사용된 해시함수의 충돌 저항성에 덜 의존하고 보안성을 높일 수 있다는 점이다[8].

XMSS 키 생성 단계에서는 높이가 h인 트리를 이용하여 키 쌍을 생성한다. 서명 생성 단계에서는 먼저

랜덤값 r, 사용될 WOTS+의 키 쌍의 인덱스(idx_sig), 그리고 공개키의 루트값을 키로 사용하여 랜덤화된 MD (message digest)를 계산한다. 그 후 인증경로를 계산한 뒤 마지막으로 개인키가 업데이트 된다. 서명 검증 단계에서는 먼저 랜덤값 r, 인덱스idx_sig, XMSS의 공개키의 루트와 message digest를 계산한다. 그 후 WOTS_pkFromSig를 사용한 WOTS+ 서명을 통해 사용된 WOTS+의 공개키인 pk_ots가 계산된다. 마지막으로 pk_ots는 L-트리를 사용하여 해당 리프를 계산하고, 리프는 인덱스 idx_sig 및 인증 경로 auth와 함께 트리의 대체 루트값을 계산한다. 결과적으로 계산된 루트값이 XMSS의 공개키와 일치할 경우 성공한다.

3.5. TESLA Family

TESLA Family는 2014년 Bai와 Galbraith의 서명 계획에서 시작되었으며 R-LWE (Ring Learning With Errors)문제에 기반한다. NIST Round 2에 진출한 qTESLA는 TESLA#의 발전된 버전이다.

3.5.1. TESLA#

TESLA#의 키 생성 단계에서는 보안 λ가 주어지면 확률적 키 생성 알고리즘 $(sk,pk)\leftarrow KeyGen(1^{\lambda})$로 표시되는 키 쌍 $(sk,pk)\in K$를 생성한다[9]. 여기서 공개키는 pk, 개인키는 sk라고 명명한다. 서명 생성 단계에서는 서명 키 sk와 메시지 $\mu\in M$를 입력하면, 확률적 서명 알고리즘은 $\sigma\leftarrow Sign(sk,\mu)$로 표시되는 서명 $\sigma\in S$를 출력한다. 서명 검증 단계에서는 확인 키 pk와 메시지 μ및 알려진 서명 $\sigma\in S$를 입력하면, 확인 알고리즘은 $b\leftarrow Verify(pk,\mu,\sigma)$로 표시되는 비트 $b\in\{0,1\}$을 반환한다. 여기서 알고리즘이 $b=1$이면 서명수락을 의미하고, 그렇지 않으면 서명거부를 의미한다.

3.5.2. qTESLA

qTESLA 전자서명 알고리즘의 키 생성 과정에서 공개 다항식 $a_1,\ldots,a_k$들은 PRF_1을 사용하여 확장된 $seed_a$를 통한 랜덤한 R_q에 의해 일관되게 생성된다. 이후 비밀 다항식 s가 가우시안 분포 D_σ를 통해 샘플링된다[10]. 공개키는 $seed_a$와 $t_i=a_is+e_i \bmod q$로, 비밀 키는 s, 비밀 오류 다항식 $e_1,\ldots,e_k$, $seed_a$, $seed_y$ 및 해시값으로 구성된다. 모든 시드는 PRF_1을 사용하여 사전 시드를 확장하여 생성된다. 서명 생성 단계에서는 서명 생성을 위해서는 먼저 다항식 $y\in R$가 무작위로 선택되어야 한다. 이를 위해 1로 초기화된 카운터를 nonce로 사용하고 임의의 문자열 $rand$를 seed로 사용한다. 다음으로, $seed_a$가 확장되어 다항식 $a_1,\ldots,a_k$를 생성한 다음 $i=1,\ldots,k$에 대한 다항식 $v_i=a_iy \bmod \pm q$를 계산하는 데 사용된다. 그 후 이 값은 각각 c의 0이 아닌 계수의 위치와 부호를 나타내는 두 개의 배열 pos 목록 및 의사 난수 생성 다항식 $c\in H_{n,h}$에 결정론적으로 매핑된다. 마지막으로 생성된 잠재적인 서명$(z\leftarrow sc+y,c')$이 거부 샘플링 이라고 하는 보안 감사까지 마치면 서명이 생성된다. 서명 검증 단계는 다음과 같다. 메시지 m, 서명 (z,c'), 그리고 공개키 pk를 입력받아 $\{pos_list,sign_list\}\leftarrow Enc(c')$를 계산하고, $seed_a$를 확장하여 $a_1,\ldots,a_k\in R_q$를 생성하고 $w_i=a_iz-b_ic$를 계산한다. 해시 기반 함수 H는 $[w_1]_M,\ldots,[w_k]_M$을 계산하고 $G(m)$과 $G(t_1,\ldots,t_k)$의 다이제스트와 함께 해시값을 계산한다. 이전 계산에서 생성된 비트 문자열이 서명 비트 문자열 c'과 일치하며 $z\in R_{[B-S]}$인 경우, 서명은 허용되고 그렇지 않으면 거부된다.

qTESLA의 공식 사이트에서 제공하는 명세는 [표 4]와 같다[11].

〔표 4〕 NIST Round2 qTESLA의 명세

Name	qTESLA-p-I	qTESLA-p-III
keygen	2,358.6	13,151.4
sign	2,299.0	5,212.3
verify	814.3	2,102.3

3.6. RAINBOW

RAINBOW는 Oil과 Vinegar의 원리를 기반으로 한 다변수 기반 서명 방식이다[12].

RAINBOW의 키 생성 단계에서 개인키는 다층 Oil과 Vinegar 시스템으로 구성된 중앙 맵 F 와 무작위

로 선택된 두 개의 가역적 아핀 선형 맵 L_1 및 L_2로 구성된다[13]. 공개키는 K의 필드 구조이며 구성된 맵 $\overline{F}=L_1 \circ F \circ L_2$의 $n-v_1$ 다항식 구성 요소이다. 서명 생성 단계에서는 임의 길이의 메시지에 서명하기 위해 해시 함수를 사용하여 메시지 다이제스트 Y'를 계산할 수 있다. 서명 검증 단계에서는 검증자는 메시지 해시 Y'를 계산하고 $\overline{F}(X')=Y'$를 확인하면 된다.

RAINBOW에서 제공하는 명세는 [표 5]과 같다[14]. 매개변수에 따라 세 가지 Level로 분류되어있다.

〔표 5〕 NIST Round 3 RAINBOW 명세

Name	RAINBOW Level I	RAINBOW Level III	RAINBOW Level V
public key size (kB)	157.8	861.4	1,885.4
private key size (kB)	101.2	611.3	1,375.7
signature size (kB)	0.066	0.164	0.204

Ⅳ. 블록체인의 양자내성 전자서명 적용 연구

블록체인은 분산된 데이터를 안전하게 저장하고 관리할 수 있는 기술이다. 현재 의료, 금융 등 다양한 분야에서 사용되며 높은 보안성 및 투명성을 제공하여 암호화폐에서도 활용되고 있다. 이러한 블록체인 기술에 양자내성암호의 전자서명을 적용시키는 다양한 연구가 진행되고 있다.

4.1. 블록체인 체계에 양자내성전자서명 적용

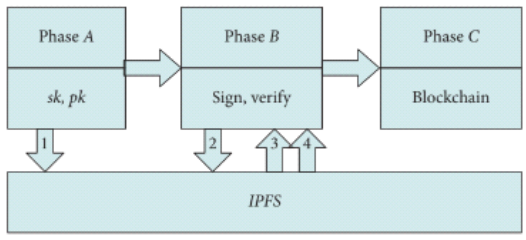
NIST PQC 3 Round 전자서명 중에서 어느 알고리즘이 블록체인에 가장 적합한지에 대한 연구가 진행되었다[15]. 해당 연구에 따르면 적합성을 평가하기 위해 키와 서명의 크기, 연산 속도, 에너지 소비량을 비교해야 하며, 이러한 부분을 고려하였을 때 FALCON이 블록체인에 가장 적합한 알고리즘이다. CRYSTALS-DILITHIUM의 경우 연산 속도가 다른 알고리즘보다 20배 이상 더 빠르다. 그러나 고속화 연구를 통해 극복할 수 있는 연산속도와는 다르게 매개변수는 보안 수준에 직접적인 영향을 주어 크기를 줄이는 것이 힘들며, 블록체인의 매 트랜잭션마다 사용되어 저장용량에 영향을 줄 수 있기 때문에 종합적으로 평가하였을 때 블록체인의 전자서명에서는 FALCON이 CRYSTALS-DILITHIUM보다 적합하다.

PQB (Post-Quantum Blockchain) 기반의 안전한 암호화폐 체계를 제안하는 연구가 진행되었다[16]. 새로운 격자 기반의 전자서명 기법이 제안되었고, 제안된 서명 기법을 블록체인과 결합하여 생성된 PQB 구성을 통해 해당 연구만의 암호화폐 설계 체계를 제공하였다.

양자내성암호를 기존의 블록체인에 그대로 도입했을 때 발생하는 공개키 및 서명의 크기나 서명검증 시간증가 등의 문제를 해결하기 위해 새로운 트랜잭션 구조와 프로토콜이 제안되었다[17]. 비대한 공개키와 서명 크기를 가진 전자서명 알고리즘을 고정된 크기로 감소시켜 저장하는 방식을 제안한다. 결과적으로 블록체인의 양자 내성 전자서명 호환성을 증대시키고, 전체적인 블록체인의 크기를 감소시킬 수 있었다.

블록체인에서 기존의 타원 곡선 기반의 전자서명을 격자 기반인 qTESLA 전자서명으로 대체하는 연구를 진행되었다[18]. 해당 연구에서는 qTESLA의 공개키 및 서명의 크기가 매우 크다는 단점을 극복하기 위해 공개키와 서명을 IPFS 네트워크에 저장하여 블록 용량 문제를 해결하였다. 제안된 qTESLA 기반의 시스템 아키텍처는 [그림 1]과 같다. 여기서, sk는 개인키, pk는 공개키를 나타낸다. 1과 2는 업로드 프로세스이고3과 4는 다운로드 프로세스이다.

A 단계에서 지갑의 서명 알고리즘에서 공개키와 개인키 쌍을 생성한다. pk는 해시 알고리즘을 통해 해당 계정의 주소를 생성하고, sk는 서명을 생성하는 데 사용된다. 해당 단계에서 공개키를 IPFS를 업로드 하고 해시 시퀀스를 얻는다. B 단계에서는 트랜잭션이 생성된다. 블록체인에서 트랜잭션 정보는 UTXO로 기록된다. C 단계에서 트랜잭션은 P2P 네트워크 구조를 통해 브로드캐스트되고 B 및 다른 마이너 노드의 검증



〔그림 1〕 qTESLA 기반의 시스템 아키텍처

〔표 6〕 공개키와 서명의 크기

System	qTESLA	qTELSA+IPFS
Public key (kB)	29.76	0.047
Sign (kB)	5.45	0.047

〔표 7〕 블록체인에서의 서명, 검증, 트랜잭션 시간 측정

System	qTESLA	qTELSA+IPFS
Transaction (ms)	33.7992995951315	105.081087620143
Sign (ms)	33.37018944616243	105.003335806339
Verification (ms)	179.651395134396	413.346856886305

을 기다린다. 트랜잭션을 수신한 마이너 노드는 IPFS 네트워크에서 공개키를 가져와 트랜잭션을 확인한다. [표 6]과 [표 7]은 IPFS를 도입하기 전과 후를 비교한 것이다. IPFS가 있는 블록체인 시스템은 IPFS가 없는 블록체인 시스템보다 더 효율적이다.

4.2. 암호화폐에 양자내성전자서명 적용

블록체인 기술의 양자 보안 위협에 대비하여 일부 연구자들은 기존 분산원장 기술을 수정하거나 새로운 솔루션을 제시한다[19]. 비트코인은 매개변수로 특정한 Koblitz 곡선인 secp256k1를 사용하는 ECDSA와 SHA-256을 사용하여 코인 및 자산 전송을 승인한다. 여기서 Koblitz 곡선은 효율성, 키 크기의 축소 및 보안 등 여러 가지 이점을 제공하지만, 양자 공격에 취약하다. 이를 극복하기 위해 BLAKE2와 SHA-3 함수를 사용하는 TESLA# 알고리즘을 기반으로 한 서명 체계가 제안되었다. 이더리움과 QRL에서 양자내성전자서명 적용이 제시되었다. 이더리움에서 민감한 산업용 데이터를 보호하면서 데이터를 공유할 사람을 업로더가 결정할 수 있는 프레임워크가 제안되었으며 해당 프레임워크는 ECDH (Elliptical-Curve Diffie-Hellman Key Exchange)와 SIDH 알고리즘을 사용한다. 두 알고리즘 중 SIDH가 양자 공격에 안전하며 양자 컴퓨팅 능력을 가진 공격자에 대한 보안을 보장하기 때문에 가장 적합한 방법이다. QRL은 전자서명 스키마의 암호 보안에 초점을 두어, 현재뿐만 아니라 미래 수십 년 동안도 클래식 및 양자 공격에 안전하도록 설계되었다. 따라서 secp256k1을 XMSS로 대체하였고, SHA-256 해시 함수를 사용한다. 이로 인해 196비트의 보안성을 제공하며 2164년까지 브루트 포스 공격에 대해 안전하다. 또한 QRL에서 사용되는 비대칭 하이퍼트리 서명 스키마는 체인 형태의 XMSS 트리로 구성된다. Corda는 매개변수로 특정한 NIST P-256 곡선인 secp256p1를 사용하는 ECDSA와 RSA와 같은 전통적인 공개키 서명 알고리즘을 지원한다. 하지만, 실험적인 수준에서 SPHINCS가 사용되어 양자 보안을 제공한다. 최근 BPQS 서명 방식이 제안되어 XMSS의 개선 버전을 형성하였다.

V. 결 론

본 고에서는 양자컴퓨터의 위협에 대응할 양자내성 전자서명의 블록체인 적용에 관한 연구 동향을 살펴보았다. 블록체인에서의 전자서명을 양자내성암호를 통해 구현함으로써 블록체인에서 양자내성을 가질 수 있다. 이때 양자내성암호의 스펙 및 매개변수를 적절하게 선택해야한다. 이후에도 지속적으로 관련 연구가 진행됨으로써 상용 솔루션에서도 양자내성암호를 적용한 사례가 증가할 것으로 기대된다.

참 고 문 헌

[1] Post-Quantum Cryptography | CSRC, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

[2] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, Zhenfei Zhang, “Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU”, falcon@ens.fr, 2020.

[3] Falcon, https://falcon-sign.info

[4] Shi Bai, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler and Damien Stehlé, “CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation,” Feb 2021.

[5] Dilithium, https://pq-crystals.org/dilithium/index.shtml

[6] Jean-Philippe Aumasson, Daniel J. Bernstein, Ward Beullens, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Andreas Hülsing, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, Bas Westerbaan, "SPHINCS+ Submission to the NIST post-quantum project, v.3," pp. 30-34, 2020

[7] Jean-Philippe Aumasson, Daniel J. Bernstein, Ward Beullens, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Andreas Hülsing, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, Bas Westerbaan, "SPHINCS+ Submission to the NIST post-quantum project, v.3.1," p. 57,2022

[8] A. Huelsing, TU Eindhoven, D. Butin, TU Darmstadt, S. Gazdag, genua GmbH, J. Rijneveld, A. Mohaisen, “XMSS: eXtended Merkle Signature Scheme,” pp. 25-32, 2018

[9] Paulo S. L. M. Barreto, Patrick Longa, Michael Naehrig, Jefferson E. Ricardini, and Gustavo Zanon, "Sharper Ring-LWE Signatures," p. 6, 2016

[10] Nina Bindel, Sedat Akleylek, Erdem Alkim, Paulo S. L. M. Barreto, Johannes Buchmann, Edward Eaton, Gus Gutoski, Juliane Kr¨amer, Patrick Longa, Harun Polat, Jefferson E. Ricardini, Gustavo Zanon, “Submission to NIST’s post-quantum project (2nd round): lattice-based digital signature scheme qTESLA”.

[11] qTESLA – Efficient and post-quantum secure lattice-based signature scheme, https://qtesla.org

[12] MIKAEL SJÖBERG, “Post-quantum algorithms for digital signing in Public Key Infrastructures,” pp. 24-25, 2017

[13] Jintai Ding and Dieter Schmidt, “Rainbow, a new multivariable polynomial signature scheme,” pp. 164-175. Springer, 2005.

[14] PQCRainbow, https://www.pqcrainbow.org/

[15] 서은영, 김영식, “양자 공격에 안전한 블록체인을 위한 요구사항 분석”, 한국통신학회 학술대회논문집, pp. 1449-1450, 2022.

[16] YU-LONG GAO, XIU-BO CHEN, YU-LING CHEN, YING SUN, XIN-XIN NIU, YI-XIAN YANG, “A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain,” IEEE Access, Volume 6, 2018.

[17] 김미연, 이준영, 윤기순, 염흥열 ,“블록체인의 양자 내성 전자서명 호환성을 증대하기 위한 트랜잭션 구조 제안”, Journal of The Korea Institute of Information Security & Crypology, pp. 87-100, 2020.

[18] Peijun Zhang , Lianhai Wang , Wei Wang , Kunlun Fu, and Jinpeng Wang, “A Blockchain System Based on Quantum-Resistant Digital Signature,” Hindawi Security and Communication Networks, Volume 2021.

[19] S. Brotsis, N. Kolokotronis1, K. Limniotis, "Towards Post-Quantum Blockchain Platforms," pp. 118-120, 2022

〈저자소개〉

김 한 결 (Hangyeol Kim)

학생회원

2019년 3월~현재 : 강남대학교 소프트웨어응용학부 재학

<관심분야> 정보보호, 디지털 포렌식

위 다 빈 (Dabin We)

학생회원

2019년 3월~현재 : 강남대학교 소프트웨어응용학부 재학

<관심분야> 정보보호, 디지털 포렌식

박 명 서 (Myungseo Park)

정회원

2013년 2월 : 국민대학교 수학과 졸업

2015년 2월 : 국민대학교 금융정보보안학과 석사

2014년 12월~2017년 2월 : 국가보안기술연구소 연구원

2021년 8월 : 국민대학교 금융정보보안학과 박사

2021년 9월~2022년 2월 : 국민대학교 금융정보보안학과 박사후연구원

2022년 3월~현재 : 강남대학교 ICT융합공학부 조교수

<관심분야> 정보보호, 디지털포렌식