정 보 보 호 학 회 지
제 32 권 제1호, 2022. 2

양자내성 블록체인에 관한 기술적 동향

권 혁 동*, 심 민 주*, 임 세 진*, 강 예 준*, 서 화 정**

요 약

양자컴퓨터 개발이 가속화됨에 따라 기존 암호 기술이 기반하고 있는 수학적 난제가 실시간으로 해결될 수 있다는 문제점에 현실화되고 있다. RSA와 타원곡선 기반의 공개키 암호와 해시함수를 활용하여 만든 블록체인 역시 양자컴퓨터에 의해 해킹 가능성이 높아지고 있다. 블록체인 상에서 데이터 위·변조를 어렵게하기 위한 장치로 사용한 암호가 양자컴퓨터 상에서 동작하는 양자알고리즘에 의해 해킹된다면 블록체인으로 보호되고 있는 데이터들의 안전성은 보장받을 수 없다. 이를 해결하기 위한 하나의 방안으로 양자알고리즘에 의해서도 해킹되지 않는 양자내성을 가진 블록체인이 제안되었다. 이와 더불어 블록체인이 기존에 가지고 있던 정보에 대한 안전한 이전을 성립하기 위한 기술에 대한 연구도 활발히 진행되고 있다. 본 고에서는 양자 내성 블록체인과 이를 구현하기 위한 기술적 동향에 대해서 확인해 보도록 한다.

Ⅰ. 서 론

양자컴퓨터 개발이 가시화됨에 따라 기존 암호화 알고리즘의 안전성에 대한 의문이 산학연에서 제기되고 있다. 공개키 알고리즘 (RSA 그리고 ECC)은 Shor 알고리즘에 의해 polynomial 안에 기반 문제가 해결될 것으로 예상되며 해시함수 (SHA3 그리고 LSH)는 Grover 알고리즘에 의해 기존 암호 강도가 절반으로 줄어드는 보안 취약점이 나타날 것으로 예상된다 [1],[2]. 정보화 시대가 됨에 따라 암호는 사회 전반에 큰 영향을 미치고 있다.

최근들어 많은 관심을 받고 있는 비트코인과 같은 암호화폐는 블록체인에 기반하고 있다. 특히 블록체인은 탈중앙화된 네트워크 상에서 거래된 원장의 안전성을 보장하기 위한 방편으로 해시함수와 타원곡선 암호의 사용하고 있다[3]. 하지만 블록체인에서 사용하는 암호화 기술 역시 양자알고리즘에 대한 고려가 되지 못하였기 때문에 추후 양자컴퓨터의 도래에 따라 안전성이 훼손될 가능성을 내포하고 있다[4]. 예를들어 P2PK UTXO (Pay to Public Key Unspent Transaction Output)를 사용한 비트코인 거래는 출력에 공개키를 표시하는 특성이 있다. 이러한 트랜잭션이 브로드캐스트될 경우, QCA (Quantum-Capable Adversary)를 통해서 비밀키를 계산할 수 있기에 자금 유출 가능성이 생긴다[5].

위와 같은 보안 문제를 해결하기 위해 양자 내성을 가진 블록체인에 대한 연구가 활발히 진행되고 있다. 본 고에서는 양자 내성 암호와 이를 활용한 양자 내성 블록체인의 최신 연구 동향에 대해서 알아본다. 본 고의 구성은 다음과 같다. 2장에서는 양자 내성 암호에 대한 동향을 확인하며, 양자컴퓨터 시대에 안전한 암호 기술을 알아본다. 3장에서 양자 내성 블록체인에 대한 최신 연구를 확인한다. 4장에서 기존 블록체인을 양자 내성 블록체인 상으로 안전하게 이전하는 방안에 대해 확인한다. 마지막으로 5장에서 본 고의 결론을 내린다.

Ⅱ. 양자 내성 암호

양자 내성 암호 (Post-Quantum Cryptography, PQC)는 양자컴퓨터의 연산 능력으로 풀기 어려운 수학 문제에 기반한 새로운 암호 체계로 NIST를 중심으로 활발히 연구가 진행되고 있다. 본 고에서는 각각의 수학적 기반에 대해서 살펴보며, 기반 문제 별로 속한 암호 알고리즘에 대해서 확인한다. 양자 내성 블록체인은 양

본 연구는 2022년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2020R1F1A1048478).
* 한성대학교 IT융합공학부 (대학원생, korlethean@gmail.com, 대학원생, minjoos9797@gmail.com, 학부생, dlatpwls834@gmail.com, 학부생, etus1211@gmail.com)
** 한성대학교 IT융합공학부 (조교수, hwajeong84@gmail.com)

자 내성 암호의 전자서명을 주로 활용한다. 따라서 본 고에서는 NIST에서 진행 중인 양자 내성 암호 표준화 작업의 Round 3에서 발표된 후보군 중에서 전자서명 부분에 대해 보다 면밀히 확인해 보도록 한다.

2.1. 격자 기반 암호 (Lattice based Cryptography)

격자 기반 암호는 SVP (Shortest Vector Problem)와 CVP (Closest Vector Problem)의 수학적 난제에 기반을 두고 있는 암호로써 1996년 Miklos Ajtai에 의해 제안되었다[8]. SVP 문제는 격자 위에서 영점 0과 가장 가까우면서 0이 아닌 벡터를 다항 시간 안에 찾기 어렵다는 문제이며 CVP 문제는 격자 위에 벡터가 주어졌을 때, 해당 벡터와 가장 가까운 벡터를 구하기 어렵다는 문제이다. 격자 기반 암호는 위와 같은 수학적 난제에 기반하여 양자컴퓨터 환경에서도 안전하며 연산속도, 키 크기, 그리고 서명 크기 관점에서 높은 성능을 보여주고 있다. 이러한 장점으로 인해 NIST PQC 표준화 Round 3 평가 최종 후보군의 7개 알고리즘 중 5개의 알고리즘이 격자 기반 암호이다.

격자 기반 암호를 구현하는 방법은 크게 LWE (Learning With Error)와 LWR (Learning With Rounding)기법이 있다. LWE 그리고 LWR 기법 모두 행렬식의 해를 찾기 어렵게 하기 위해 값을 왜곡하는 기법이다. 이때 LWE는 에러를 삽입하고 LWR은 반올림을 통해 결과값의 무작위성을 증가시킨다. LWE는 에러를 더하는 것으로 완성되지만, LWR은 결정론적으로 값이 계산되기 때문에 최적화 시 LWE보다 유리하다. Ring 상에서 LWE와 LWR을 구현함으로써, 연산속도를 높이고 키의 크기를 줄이는 기법도 연구되고 있다. 다만, Ring 상에서 LWE와 LWR을 구현할 경우, 기존 모델보다는 보안 안전성이 감소할 수 있다.

2.1.1. CRYSTALS-DILITHIUM

DILITHIUM은 SVP 문제에 기반하고 있으며 선택 메시지 공격 (Chosen Message Attacks, CMA)에 내성을 지닌다[9]. 제안 기법은 Fiat-Shamir with Aborts에 기반을 두었으며, 동일한 보안성을 가지는 격자 기반 암호 중 가장 작은 공개키와 서명 크기를 제공하고 있다는 장점이 있다. [표 1]에는 Dilithium의 공개키와 서명의 크기가 나타나 있다.

〔표 1〕 Dilithium의 서명 및 공개키 길이

비고	Dilithium 2	Dilithium 3	Dilithium 5
NIST 보안 레벨	2	3	5
공개키 크기 (바이트)	1,312	1,952	2,592
서명 크기 (바이트)	2,420	3,293	4,595

2.1.2 FALCON

Falcon은 Fast Fourier Lattice-based Compact Signatures over NTRU의 줄임말로, 격자기반 전자서명 알고리즘이다[10]. NTRU 격자상에서 Short Integer Solution (SIS) 문제가 효율적으로 풀리지 않는다는 가정에 기반을 두고 있으며, Gaussian sampler를 통해 비밀키가 유출되는 것을 방지한다. Falcon은 다른 격자기반 암호와 공개키 길이가 같은 경우, NTRU 격자를 통해 더 작은 서명 크기로 동일한 보안성을 확보하는 것을 가능하게 한다. 또한 Fast Fourier sampling을 사용함으로써 빠른 구현이 가능하며, 키 생성 알고리즘은 30KB 미만의 RAM을 사용하기에, 메모리 사용이 제한되는 소형 임베디드 장치에서도 키 생성이 가능하다. [표 2]에는 Falcon의 공개키와 서명의 크기가 나타나 있다.

〔표 2〕 FALCON의 서명 및 공개키 길이

비고	FALCON 512	FALCON 1024
NIST 보안 레벨	1	5
공개키 크기 (바이트)	897	1,793
서명 크기 (바이트)	666	1280

2.2. 다변수 다항식 기반 암호 (Multivariate based Cryptography)

다변수 다항식 문제 기반 암호는 1988년에 Matsumoto와 Imai에 의해 제안되었다. 이는 유한 필드 상에서 다변수 다항식 시스템의 해를 찾는 것이 어렵다

는 것에 기반한 암호화 알고리즘으로, 다른 암호 알고리즘에 비해 수학적 증명이 간단하다[11]. 다변수 다항식 기반 암호는 행렬 곱을 2개 혹은 3개의 레이어로 나누어서 연산을 수행하며 이 중 은닉 레이어를 앞 또는 뒤의 레이어와 결합하여 공격자가 이를 확인하기 어렵도록 하는 것에 기반한다. 행렬로 된 다항식의 해를 구하는 연산이기 때문에 특정한 인자들에 지속적으로 덧셈과 곱셈 연산을 취함으로써 결과 값을 도출 할 수 있게 하는 Gaussian Elimination 알고리즘을 활용하여 효과적인 계산이 가능하다. 다만 지금까지 다항식 기반 보안성에 대한 연구를 통해 보안 취약점이 많이 발견됨으로써 안전성에 대한 의문이 제기되고 있다[12]. 다변수 다항식 기반 암호는 서명 크기가 작고 연산 속도가 빠르지만, 키 크기가 크다는 단점이 있다.

2.2.1. RAINBOW

Rainbow는 UOV (Unbalanced Oil-Vinegar) 문제에 기반하고 있는 암호로써 이론적 보안강도는 무작위 다변수 다항식을 풀이하는 것이 NP-hard 문제에 속하는 것에 기반한다[13]. Rainbow는 다른 양자 내성 암호 알고리즘에 비해 상대적으로 짧은 서명 크기를 가진다. 또한 유한체 상에서의 간단한 연산으로 구성되어있어 빠른 속도의 서명 및 검증 알고리즘을 가진다는 장점이 있다. 반면에 공개키 크기는 다른 알고리즘 대비 매우 크다는 단점이 있다. 따라서 일반적인 상황에서는 효율적인 사용이 어렵다. 하지만 키 갱신이 자주 이루어지지 않아 키 공유가 자주 일어나지 않는다면, 효과적으로 활용될 수 있을 것으로 사료된다. [표 3]에는 Rainbow의 공개키와 서명의 크기가 나타나 있다.

〔표 3〕 Rainbow의 서명 및 공개키 길이

비고	GF(16),36,32,32	GF(256),68,32,48	GF(256),96,36,64
NIST 보안 레벨	1	3	5
공개키 크기 (바이트)	157.8	861.4	1,885.4
서명 크기 (바이트)	66	164	204

2.2.2. GeMSS

GeMSS는 다변수 다항식 기반 양자 내성 암호로서 빠른 검증이 가능하고 다른 양자 내성 암호 알고리즘에 비해 큰 공개키를 가지고 있다[14]. GeMSS는 QUARTZ의 가속화 버전임과 동시에 보안성을 강화하였다. 또한 NIST PQC 표준화에 GeMSS보다 작은 공개키를 가지고 큰 서명 크기를 가지는 DualModeMS가 함께 제시되었다. 현재는 GeMSS를 개선하여, 보안 매개 변수 선택에 대해 효율적인 라이브러리인 MQsoft를 제시한 상태이다. [표 4]에는 GeMSS의 공개키와 서명의 크기가 나타나 있다.

〔표 4〕 GeMSS의 서명 및 공개키 길이

Category	GeMSS 128	GeMSS 192	GeMSS 256
NIST 보안 레벨	1	3	5
공개키 크기 (바이트)	352	1,237	375.21
서명 크기 (바이트)	258	411	576

2.3. 해시 기반 암호 (Hash based Cryptography)

해시 기반 암호는 Ralph Merkle에 의해 제안되었으며, 해시 함수의 충돌 저항 문제 (Collision Resistance)에 기반하고 있다[15]. 해시 기반 암호는 양자 알고리즘에 의해 보안성이 감소하게 되지만, 긴 해시 출력을 사용하는 것으로 안전성을 유지할 수 있다. 또한 해시 기반 암호는 해시 함수와 서명 알고리즘을 결합한 것으로 보안취약점이 발견된 부분을 모듈 형식으로 대체하여 대처를 유연하게 할 수 있다. 해시함수에 보안 취약점이 존재하는 경우, 포함된 해시 함수를 다른 해시 함수로 교체하는 것으로 보안성을 확보할 수 있다. 해시 함수 기반의 전자 서명에 대한 연구는 타원 곡선 암호보다 이전에 연구된 방식으로, 많은 공격으로부터 안전성을 유지하였다. 따라서 해시 함수 기반의 알고리즘 문제는 충분한 신뢰성을 가진다. 하지만 제한된 수의 서명만을 생성할 수 있다는 점과 서명 사이즈가 크다는 단점이 있다.

해시 기반 암호에 활용되는 서명 알고리즘에는 Lamport-Diffie OTS (One-Time-Signature)가 있다. 이

알고리즘은 비밀키인 서명키 (Signature Key)와 공개키인 인증키 (Verification Key) 쌍을 사전에 생성한다. 이후 서명키를 메시지에 따라 선택하여 상대방에게 전송하고, 상대방은 인증키 쌍을 확인하여 메시지 검증을 수행한다. 해당 기법은 키 크기가 크다는 문제점이 있어 이를 보완한 Winternitz OTS 알고리즘이 연구되었다. Winternitz OTS 메시지의 비트 값에 따라 연산 횟수를 조정한다. 이렇게 생성된 서명 값을 Merkle Tree 구조로 구성하여 검증한다. 또한 이는 블록체인에서 메시지를 검증하는 용도로도 활용되는 범용적인 알고리즘이다.

2.3.1. SPHINCS+

SPHINCS+ 알고리즘은 기존의 SPHINCS 서명 기법을 개선한 결과물로, Stateless 해시 기반의 전자서명 방식이며 ROM 기반의 보안 증명을 제시하고 있다[16]. Multi-target 공격에 대한 방어가 가능하고 Tree-less WOTS+ 수행 및 FORS (Forest of Random Subsets) key pair와 같은 최적화 기법을 통해 서명 크기를 대폭 감소시켰으며, Verifiable Index Selection 기능을 제공한다는 점에서 기존의 SPHINCS 서명 기법과 차별성이 있다. SPHINCS+는 SHAKE256, SHA-256, 그리고 Haraka를 기반으로 한다. SPHINCS+는 NIST PQC 표준화 Round 2를 기준으로 simple과 robust 버전으로 나누어서 발전하고 있다. Robust 버전은 보수적인 보안 강도에 기반을 두고 있다. [표 5]에는 SPHINCS+의 공개키와 서명의 크기가 나타나 있다.

〔표 5〕 SPHINCS+의 서명 및 공개키 길이

비고	SPHINCS+					
	128s	128f	192s	192f	256s	256f
NIST 보안 레벨	1	1	3	3	5	5
공개키 크기 (바이트)	32	32	48	48	64	64
서명 크기 (바이트)	7,856	17,088	16,224	35,664	29,792	49,856

2.4. 아이소제니 기반 암호 (Isogeny based Cryptography)

아이소제니 기반 암호는 2011년에 Luca De Feo와 Plut Jao에 의해 제안되었으며 Order가 같은 두 타원곡선 사이에 존재하는 아이소제니를 구하는 것이 NP-hard 문제임에 기반한다. 타원 곡선 상의 이산 로그 문제는 양자컴퓨터에서 쇼어 알고리즘(Shor's algorithm)을 통해 효율적으로 해결할 수 있지만, Supersingular Elliptic Curve의 동형성 문제는 현재까지 알려진 양자 공격 기법이 없다.

오랜 기간에 걸쳐 연구가 진행된 페어링과 타원곡선의 수학적 증명이 활용가능하다는 점에서 주목받고 있으며, 현재까지 연구가 활발하게 진행되고 있다[17]. 아이소제니 기반 암호는 다른 기반에 비해 키와 메시지가 합리적인 크기를 가진다는 장점을 가지고 있다. 다만 연산속도가 다른 기반에 비해 떨어지며 최신 암호인 만큼 보안성에 대한 충분한 암호 분석이 이루어지지 않았다는 한계점을 가지고 있다. 현재 아이소지니 기반 서명은 NIST 공모전에는 발표되지 않았지만 중국 양자내성암호 공모전의 SIAKE는 서명으로 활용이 가능하다.

2.5. 부호 기반 암호(Code based Cryptography)

부호 기반 암호는 네트워크 통신 중에 발생하는 노이즈를 제거하기 위해 사용되는 기술인 오류 정정 부호(Error Correction Code, ECC)로부터 개인키와 공개키를 생성하는 암호이다[6]. 사용자가 임의의 노이즈를 평문에 삽입함으로써 오직 사용자만 알 수 있는 방식으로 노이즈를 제거하여 평문을 확인할 수 있다. 노이즈를 제거하는 방법을 모르는 경우에는 평문을 확인할 수 없다. 부호 기반 암호는 효율적인 연산으로 인한 빠른 암호화 및 복호화가 가능하다는 장점이 있으나, 키 크기가 크다는 단점이 있다. 1978년도에 제안된 최초의 부호 기반 암호인 McEliece 알고리즘 상에서는 Goppa 부호가 사용된다. 선형 오류 정정 부호 중 하나인 Goppa 부호는 아직까지 취약점이 발견되지 않아 높은 보안성을 유지하고 있으며, McEliece는 현재까지도 활발히 사용되는 암호 중 하나이다[7]. 하지만 McEliece 암호는 Goppa 부호를 사용함으로써 공개키 크기가 크다는 단점이 있다. 따라서 공개키 크기를 합리적인 수준으로 줄이기 위

해 다양한 기법들이 연구되고 있다. Goppa 부호 외의 CRS, Gabidulin, Reed-Muller, 그리고 LDPC 등을 사용한 다른 부호 기반 암호는 보안 취약점이 발견되어서 사용되지 않는다. 현재 코드 기반 암호는 키교환 (Key Encapsulation Mechanism; KEM)에 집중하고 있으며 서명에 대한 기법은 NIST 표준화에서는 존재하지 않는다.

2.6. 영지식 기반 암호 (Zero-knowledge based Cryptography)

Picnic은 영지식 기반(Zero-knowledge Proof System)으로 설계된 양자 내성 암호로 대칭키 암호에 속하며, 정수론적 혹은 대수적 수학 문제에 기반을 두지 않은 구조로 관심을 받고 있다[18]. [표 6]에는 Picnic의 공개키와 서명의 크기가 나타나 있다.

〔표 6〕 Picnic의 서명 및 공개키 길이

비고	Picnic-FS		
NIST 보안 레벨	1	3	5
공개키 크기 (바이트)	32	48	64
서명 크기 (바이트)	32,838	74,134	128,176

Picnic 알고리즘은 해시 함수에 대한 Random Oracle 가정에 의존하고 있다. 또한 서명의 크기가 작은 LowMC 블록암호를 사용하여 안전성을 확보한다. 서명 생성과정에는 NIZK (NonInteractive Zero Knowledge) 증명 방식을 사용하고 있다. 현재까지 보안 취약점은 알려지지 않았으며, 키 교환 및 인증 알고리즘을 모두 사용한 최초의 TLS 연결을 하여 기존 프로토콜과의 호환성을 입증했다.

Ⅲ. 양자내성 블록체인

양자컴퓨터가 발전함에 따라서 양자 알고리즘에 대한 내성을 가지는 암호에 대한 관심이 높아지고 있다. 이와 더불어 핵심 4차 혁명 기술인 블록체인 상에서의 양자 내성을 만족하는 블록체인에 대한 요구도 함께 증가하고 있다. Bitcoin Post-Quantum[19]은 양자 내성 전자서명을 사용하는 것으로 기존 비트코인이 지니지 못한 양자 내성을 확보하기 위해 제안되었으며 Ethereum 3.0[20]은 zk-STARK (Zero-Knowledge Scalable Transparent ARguments of Knowledge)을 적용하고 있다. Corda[21]는 블록체인 컨소시엄 R3가 만든 분산원장 기술로, 양자 내성 암호 중 하나인 SPHINCS를 적용하기 위한 실험 및 연구를 진행하고 있다.

블록체인의 보안 안전성은 블록체인에 사용하는 암호 기술의 안전성에 기반하고 있다. 따라서 블록체인이 양자 내성을 가지기 위해서는 기존 암호를 양자 내성 암호를 전환하는 것이 필요하다. 하지만 양자 내성 암호를 블록체인에 적용하기 위해서는 양자 내성암호가 가지는 특성들이 블록체인 적용에 적합한지 먼저 고려해야 한다[22].

첫 번째로 키 크기가 작아야 한다. 기본적으로 블록체인은 정보를 안전하게 저장하는 데이터베이스의 일종이다. 따라서 데이터 이외에 다른 저장 공간을 효율적으로 줄여서 관리할 필요가 있다. 키 크기가 클수록 블록체인의 크기가 비대하게 증가하므로 저장 공간을 낭비하게 된다. 또한 키가 커질수록 키를 생성하는데 연산량이 커지기 때문에 빠른 블록 생성을 방해한다.

두 번째로 작은 서명 크기와 짧은 해시 길이이다. 블록체인의 헤더 데이터 중에는 사용자의 서명과 데이터 및 블록 해시 정보를 포함한 트랜잭션을 저장한다. 이때 서명의 크기가 커지고 해시 길이가 길어질수록 블록의 크기가 커진다. 따라서 서명의 크기를 줄이고 해시 길이를 짧게 해서 저장 공간을 효율적으로 사용할 수 있어야 한다.

세 번째는 빠른 연산 속도이다. 블록을 빠르게 생성하기 위해서는 트랜잭션 처리 속도가 빨라야 하며, 이는 연산 속도에 기반한다. 특히 블록체인은 자원이 한정된 환경 (Resource-constrained environment)에서도 원활한 동작을 지원하기 위해 낮은 연산 복잡도를 가질 필요가 있다.

네 번째는 낮은 연산 복잡도이다. 세 번째 조건에서 제시된 빠른 연산속도가 의미하는 단순히 암호 알고리즘의 연산이 간단하다는 것과는 다른 의미를 지닌다. 예컨대, ARM 프로세서 상에서 vector instruction을 사용한다면 연산을 병렬로 진행할 수 있기 때문에 다른 프로세서 상에서 연산할 때 보다 더 낮은 연산 복잡도를 지니게 된다. 즉, 낮은 연산 복잡도를 위해서는 하드웨어의 특성을 활용하여 효율성을 끌어올리는 것으로 생

각할 수 있다.

마지막으로 낮은 에너지 소비가 필요하다. 일부 블록체인은 블록 생성 과정에서 많은 에너지를 소비하는 경우가 있다. 일례로 비트코인은 합의 프로토콜 과정에서 에너지 소비가 크다. 이와 같이, 에너지 소비가 클수록 효율적이지 못하기 때문에 에너지 소비량을 낮출 필요가 있다.

현재 양자 내성 블록체인에 대한 실용적인 활용 방안에 대한 연구가 활발히 진행되고 있다. 블록체인은 비트코인과 함께 성장한 만큼, 비트코인에 양자 내성 블록체인을 도입하고자 하는 연구가 활발히 진행되고 있다. 2019년 제안된 양자 내성 블록체인 비트코인[23]은 Tesla[24]를 사용하여 양자 내성을 확보하였다. RLWE (Ring-Learning With Errors)에 기반한 전자서명 알고리즘으로써 BLAKE2와 SHA-3 암호를 사용하고 있다. Tesla를 사용하는 것으로 기존 비트코인 블록체인의 ECDSA 과정에서 사용되는 Koblitz curve[25], secp256k1 curve, 및 SHA-256을 대체하여 양자 내성을 확보하였다. 이더리움에서는 ECDSA에 기반한 알고리즘 대신 다항식 다변수 기반인 Rainbow 전자서명을 통해 양자 내성을 확보하려는 연구가 진행되었다[26].

새로운 유형의 양자 내성 블록체인을 작성하거나 프레임워크를 구현하고자 하는 연구도 진행되고 있다.

〔표 7〕 다양한 서명의 성능 비교. w는 WOTS 체인의 길이

알고리즘	키생성	서명	검증
BPQS (w=4, SHA256)	0.569	0.08	0.10
BPQS (w=4, SHA384)	1.107	0.16	0.19
BPQS (w=16, SHA256)	0.872	0.19	0.20
BPQS (w=16, SHA384)	1.719	0.39	0.38
ECDSA secp256k1 (SHA256)	0.10	0.34	0.25
EdDSA Ed255519 (SHA512)	0.18	0.08	0.16
RSA3072 (SHA256)	561.1	5.39	0.17
SPHINCS-256 (SHA512)	0.69	144.5	1.76

BPQS (Blockchained Post-Quantum Signatures)는 기존 블록체인과 Merkle-tree 기반 서명 체계를 모티브로 한 양자 내성 블록체인이다[27].

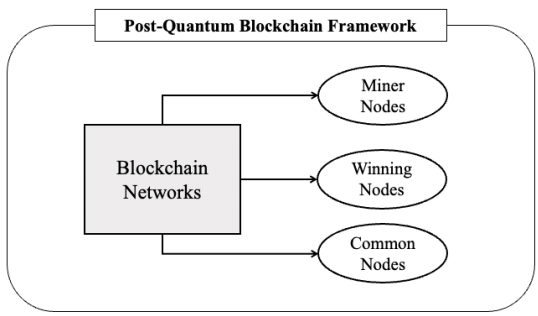
BPQS는 XMSS을 단순화한 형태로, 자체적으로 키 생성과 서명 생성 및 서명 검증에 드는 비용과 서명의 크기를 줄였다. 또한 필요에 따라 무제한으로 서명을 허용하는 폴백 메커니즘(fallback-mechanism)을 제공한다. [표 7]은 BPQS와 다른 알고리즘의 동작 시간을 밀리초 단위로 비교한 것이다.

블록체인에서 블록을 연결하는데 중요한 부분인 합의 알고리즘에 대한 양자 내성 관련한 연구도 활발히 진행되고 있다. IEEE DSC (Dependable and Secure Computing)'21에서는 채굴 난이도 조정 알고리즘인 DAA (Difficulty Adjustment Algorithm)를 사용한 새로운 PoW (Proof of Work) 합의 메커니즘을 제안하였다[28]. [그림 1]은 제안하는 PQB의 프레임워크의 구조이다.

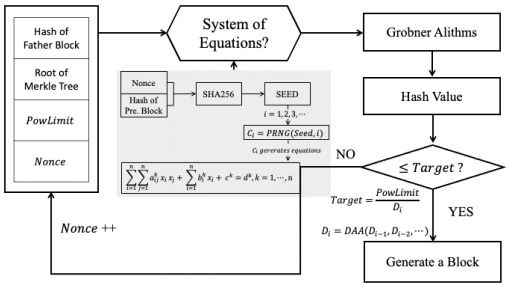
블록체인 네트워크는 채굴자 노드, 승자 노드, 일반 노드로 구성되며 이는 블록체인 시스템을 구축되는데 사용된다. 각각의 노드는 트랜잭션 요청에 대한 응답으로 트랜잭션 서비스 처리가 가능하며, 트랜잭션이 생성된 후에는 네트워크상으로 브로드캐스트 된다.

채굴자 노드는 트랜잭션을 수신할 수 있으며 승자 노드는 새로운 블록을 생성한다. 일반 노드는 확장 데이터를 처리한다. 해당 합의 알고리즘은 [그림 2]와 같이 동작한다.

작업 증명을 위해서는 비트코인의 PoW에서 사용되는 SHA-256을 대신하여 NP-hard 문제에 속하는 MQE (Multivariate Quadratic Equations)를 사용하여 양자 내성을 확보하였다. [그림 2]의 음영 부분이 MQE에 해당된다. 채굴자 노드는 MQE를 풀기 위해서 그뢰브너



〔그림 1〕 양자내성 블록체인 프레임워크



〔그림 2〕 PoW 모델의 워크플로우

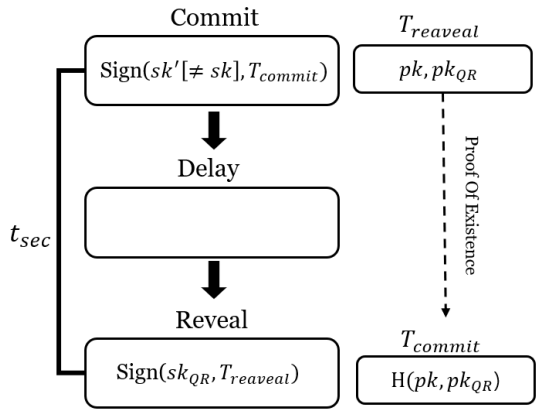
기저 (Gröbner basis)를 사용한다. 이후 유한체 상에서 MQE에 따라 작업 조건 증명이 가능한지 검증한다. 검증에 성공한다면 새로운 블록이 생성되며 채굴자 노드는 승자 노드가 된다. 이후 블록이 다른 노드로 브로드캐스트 된다.

Ⅳ. 양자 내성 블록체인으로의 전환

양자 내성 암호 알고리즘에 대한 표준을 설계하는 것은 기존 블록체인을 양자 내성 블록체인으로 전이하기 위한 준비 단계라고 볼 수 있다. 양자 내성 블록체인이 설계되더라도, 기존 블록체인의 데이터를 양자 내성 블록체인으로 이전 (포크)하는 작업이 필요하다. 또한 블록체인 포크 이후에 발생할 수 있는 잠재적 결함과 고전(Classical) 공격에 대해서도 안전성을 확보해야 한다. 따라서 안전한 포크를 위해 기존 블록체인을 양자 내성으로 안전하게 전이하는 방법에 대한 연구가 활발히 진행되고 있다.

4.1. Commit-Delay-Reveal Protocol

비트코인이 개선되어 양자 내성 암호가 포함되어 업데이트된 경우라 할지라도 상당수의 유저들은 일반적인 트랜잭션 방식인 P2PKH (Pay-to-Public-Key-Hash)를 여전히 사용할 수 있다. 따라서 비트코인에 양자 내성 암호가 적용된 프로토콜이 배포되더라도 QCA (Quantum-Capable Adversary)에 취약하게 된다. 2018년 비트코인에서 사용되고 있는 서명 알고리즘인 ECDSA를 양자 내성 암호로 안전하게 전이하기 위한 CDR (Commit-Delay-Reveal 프로토콜이 제안되었다. CDR 프로토콜은 느리지만 안전하게 사용자를 양자 내



〔그림 3〕 Commit - delay - reveal 전환 스킴; (sk: 비밀키, QR: 양자 저항)

성 환경으로 전환할 수 있게 설계되었다. CDR 프로토콜로 전환이 완료된다면 기존 ECDSA는 더 이상 허용하지 않고, 클라이언트는 기존에 사용한 양자 내성 암호나 CDR 프로토콜을 통해 전환된 체계인 UTXO (Unspent Transaction Outputs)만을 사용할 수 있다. CDR 프로토콜의 메커니즘은 [그림 3]과 같다.

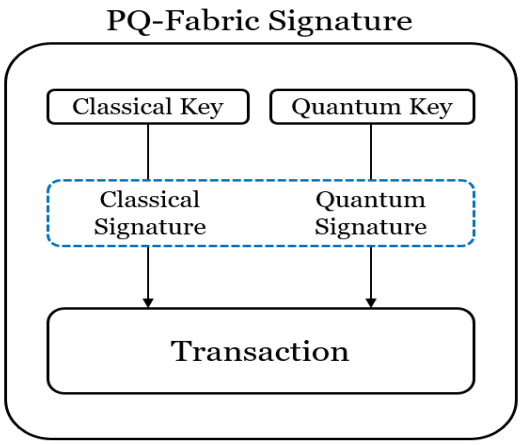
Commit 단계에서는 특정 지갑 주소 (pk, sk)에 트랜잭션을 보내기 위해, 사용자는 지갑 주소와 연결된 공개키 (pk)와 양자 내성 공개키(pkQR)의 해시 값을 공개한다.

Delay 단계는 해시 값 공개 이후, 프로토콜에서 지정한 시간만큼 대기한다. 대기 중에는 전자 지갑에서 자금 이동이 금지된다. 대기 시간이 길수록 블록체인 재구성이 실수 또는 고의로 발생하지 않으므로 자금을 보호할 수 있다. 지정된 기간에 대해서는 다양한 의견이 있지만 가장 많이 논의되고 있는 기간은 6개월이다.

Reveal 단계는 대기 시간이 흐른 다음 사용자는 공개키와 양자 내성 공개키를 사용하여 자신이 지갑의 소유자임을 증명한다. 이후 사용자는 자신이 원하는 지점으로 트랜잭션을 전송할 수 있다.

4.2. 실시간 마이그레이션

ICBC (IEEE International Conference on Blockchain and Cryptocurrency)'21에서는 고전 컴퓨터 공격과 양자컴퓨터 공격에 안전한 PQFabric이 제안되었다[29]. PQFabric은 암호내성 암호의 개발과 프로토타입을 제공하는 오픈소스 프로젝트인 OQS (Open



〔그림 4〕 PQ-Fabric 상의 하이브리드 서명 시스템 구조

Quantum Safe)에서 제공하는 라이브러리를 사용하였다[30]. 그리고 PQFabric은 양자컴퓨터 공격에 안전하지 않은 기존의 블록체인에서 양자 내성 블록체인으로 실시간 마이그레이션하는 것을 최초로 제시하였다.

PQFabric은 Classical key와 Quantum key라는 두 개의 키를 사용하여 기존 서명과 양자키를 사용한 서명을 하나의 형식에 묶어 두 가지 서명을 사용하는 하이브리드 전자 서명 체계를 사용하였다. [그림 4]는 PQFabric에서 사용되는 하이브리드 서명체계에 대한 구조도이다.

[표 8]은 블록체인에 적용된 암호 알고리즘별로 성능 평가를 수행한 것이다. 인증서 길이가 긴 암호 알고리즘에 대해서는 노드 충돌 등과 같은 문제가 발생하여 실행에 실패함을 확인할 수 있다. qTesla는 NIST 양자내성암호 대체 후보군은 아니지만, 포스트 퀀텀 하이퍼레저에 대한 최신 연구[31]에서 인증서의 크기가 너무 크지 않은 qTesla를 활용한 연구 결과를 PQFabric의 성능 평가에 포함시켰다.

블록 지연 시간은 ECDSA를 단독으로 사용하였을 때 49ms으로 가장 짧았고, 뒤이어 Falcon-Hybrid가 60ms로 짧은 지연시간을 나타내었다. 또한 지연시간이 짧을수록 처리량은 높아지는데 지연시간이 가장 짧은 ECDSA 단독 모델은 초당 2,084개의 트랜잭션을 처리할 수 있다.

결과적으로, PQFabric이 기존 Fabric보다 더 높은 지연 시간과 더 낮은 처리량을 갖지만, 양자 내성 서명 알고리즘에 따라 성능 저하는 발생되지 않았다. Hybrid Falcon-512의 경우, ECDSA 단독으로 사용하는 방식에 비해 트랜잭션 처리량이 떨어질 것으로 예상하였으나, [표 7]의 결과에 따르면 약 14% 가량 감소함을 확인하였다. 따라서 Hybrid Falcon-512에 추가적인 최적화 없이 사용 가능할 것으로 판단된다.

4.3. Lightweight Post-quantum Blockchain Transaction

SegWit은 블록체인을 확장할 때 사용되는 기법이다[32]. 하지만 트랜잭션 검증 데이터가 블록의 메모리를

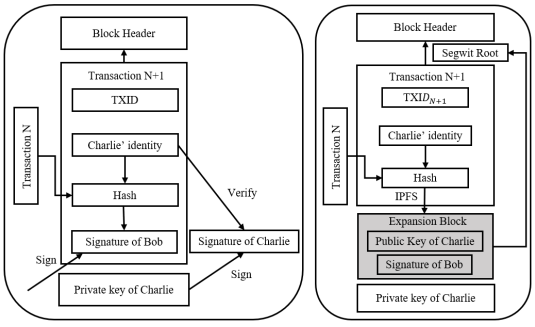
〔표 8〕 암호 알고리즘 별 성능 평가

알고리즘	3-Round 혹은 대체 암호군	서명 크기 (바이트)	성공	블록 지연시간 (밀리초)	초당 거래량
ECDSA	양자전 암호	818	o	49	2,084
Falcon-512	3-Round	2,988	o	60	1,788
Falcon-1024	3-Round	5,051	o	64	1,664
Dilithium-2	3-Round	5,263	o	68	1,545
Dilithium-3	3-Round	6,542	o	76	1,391
Dilithum-4	3-Round	7,830	o	85	1,268
qTesla-p-I	-	24,551	o	102	1,035
Picnic-L1-FS	대체 암호군	45,319	x	-	-
Rainbow-Ia-Cyclic-Compressed	3-Round	79,708	x	-	-
Rainbow-Ia-Classic	3-Round	202,741	x	-	-

차지한다는 단점을 갖고 있다. Lightweight Post-quantum Blockchain Transaction은 검증 데이터가 블록의 메모리가 아닌 블록 외부에 위치한 확장 블록으로 위치시키는 방법을 제안하여 트랜잭션을 경량화 시켰다. 이후 2019년도에 제안된 Rainbow 기반의 양자내성 전자서명 체계인 8-byte의 공개키를 갖는 ID-Rainbow[33]를 활용하였다.

[그림 5]는 기존 양자내성 암호 트랜잭션 솔루션과 제안하는 경량화한 트랜잭션을 비교한 그림이다. 사용자의 트랜잭션 데이터만 블록으로 패키징되어 있고, ID-Rainbow를 사용한 트랜잭션 처리방법과 다르게 검증 데이터를 외부 블록인 확장 블록으로 패키징 되어 있는 것을 확인할 수 있다.

검증 데이터가 블록의 외부에 따로 분리되어 있기 때문에 거래 데이터를 검증하기 위해서는 블록의 거래 데이터와 확장 블록의 검증 데이터가 대응되는 것을 확인해야 한다. 이를 위해 블록은 블록의 트랜잭션 데이터와 확장 블록의 검증 데이터 사이의 대응 관계를 [그림 5]의 오른쪽과 같이 IPFS를 사용하여 기록한다.



〔그림 5〕 (왼쪽) 블록체인 시스템 상에서 ID-Rainbow을 이용한 양자 내성 전환 솔루션; (오른쪽) 블록체인 시스템 상에서 IPSF 알고리즘을 사용한 경량 전환;

V. 결 론

본 고에서는 다가올 양자컴퓨터 시대에 대비하여 양자 내성 블록체인에 관한 동향에 대해 살펴보았다. 양자내성 블록체인은 기존 블록체인에 사용되는 암호 알고리즘을 양자 내성 암호로 변경하는 것으로 일차적으로 가능하다. 이와더불어 양자 내성 블록체인으로 기존 블록체인을 전환하는 과정도 면밀히 검토되어야 함을 확인할 수 있다. 이후로도 양자컴퓨터 상의 양자 알고리즘에 대응하기 위해서 양자 내성 암호와 양자 내성 블록체인에 대한 지속적인 연구가 필요할 것으로 사료된다.

참 고 문 헌

[1] D. J. Bernstein, and T. Lange, "Post-quantum cryptography," *Nature*, pp. 188-194, 2017.

[2] D. J. Bernstein, "Introduction to post-quantum cryptography," *Post-quantum cryptography, Springer*, pp. 1-14, 2009.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, 2008.

[4] M. C. Semmouni, A. Nitaj, and M. Belkasmi, "Bitcoin security with post quantum cryptography," *International Conference on Networked Systems*, pp. 281-288, June 2019.

[5] I. Stewart, D. Ilie, A. Zamyatin, S. Werner, M. F. Torshizi, and W. J. Knottenbelt, "Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack," *Royal Society open science*, 5(6), 2018.

[6] R. Overbeck, and N. Sendrier, "Code-based cryptography," *Post-quantum cryptography*, pp. 95-145, 2009.

[7] B. Biswas, and N. Sendrier, "McEliece cryptosystem implementation: Theory and practice," *International Workshop on Post-Quantum Cryptography*, pp. 47-62, October 2008.

[8] M. Ajtai, "Generating hard instances of lattice problems," *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 99-108, 1996.

[9] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-dilithium: A lattice-based digital signature scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 238-268, 2018.

[10] P. A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang, "Falcon:

Fast-Fourier lattice-based compact signatures over NTRU," *Submission to the NIST's post-quantum cryptography standardization process*, 2018.

[11] T. Matsumoto, and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption," *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 419-453, 1988.

[12] V. Dubois, P. Fouque, A. Shamir and J. Stern, "Practical cryptanalysis of SFLASH," *Lecture Notes in Computer Science*, 4622, pp. 1–12, 2007.

[13] J. Ding, D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," *International conference on applied cryptography and network security*, pp. 164-175, 2005.

[14] A. Casanova, J. C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem, "GeMSS: a great multivariate short signature," *Diss. UPMC-Paris 6 Sorbonne Universités; INRIA Paris Research Centre*, 2017.

[15] J. Buchmann, E. Dahmen, and A. Hülsing, "XMSS-a practical forward secure signature scheme based on minimal security assumptions," *International Workshop on Post-Quantum Cryptography*, pp. 117-129, 2011.

[16] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, P. Schwabe, "The SPHINCS+ signature framework," *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019.

[17] D. Jao, and L. D. Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," *International Workshop on Post-Quantum Cryptography*, pp. 19-34, 2011.

[18] D. Kales, and G. Zaverucha, "Improving the performance of the picnic signature scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 154-188, 2020

[19] Bitcoin Post-Quantum, November, 2019. Available: https://bitcoinpq.org. [Online].

[20] Ethereum's Official Roadmap, November, 2019. Available: https://github.com/ethereum/wiki/wiki/Sharding-roadmap. [Online].

[21] Corda's Supported Security Suites, November, 2019. Available: https://docs.corda.net/cipher-suites.html. [Online].

[22] T. M. Fernández-Carames, and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE access*, 8, pp. 21091-21116, 2020.

[23] M. C. Semmouni, A. Nitaj, and M. Belkasmi, "Bitcoin security with post quantum cryptography," *International Conference on Networked Systems*, pp.281-288, June, 2019.

[24] P. S. L. M. Barreto, P. Longa, M. Naehrig, J. E. Ricardini, and G. Zanon, "Sharper ring-LWE signatures," *IACR Cryptol. ePrint Arch.*, November, 2016.

[25] T. Lange, "Koblitz curve cryptosystems," *Finite Fields and Their Applications*, 11(2), pp. 200-229, 2005.

[26] R. Shen, H. Xiang, X. Zhang, and B. Cai, "Application and implementation of multivariate public key cryptosystem in blockchain," *International Conference on Collaborative Computing: Networking*, Applications and Worksharing, pp. 419-428, August 2019.

[27] K. Chalkias, J. Brown, M. Hearn, T. Lillehagen, I. Nitto, and T. Schroeter, "Blockchained post-quantum signatures," *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE*, pp. 1196-1203, July 2018.

[28] J. Chen, W. Gan, M. Hu, and C. M. Chen, "On the Construction of a Post-Quantum Blockchain," *2021 IEEE Conference on Dependable and Secure Computing (DSC) IEEE*, pp. 1-8, 2021.

[29] A. Holcomb, G. Pereira, B. Das and M. Mosca,

"PQFabric: A Permissioned Blockchain Secure from Both classic and Quantum Attacks," *2021 IEEE International Conference on Blockchain and Cryptocurrency(ICBC)*, pp.1-9, 2021.

[30] D. Stebila and M. Mosca, "Post-quantum key exchange for the inter- net and the open quantum safe project," *International Conference on Selected Areas in Cryptography*, pp. 14-37, 2016.

[31] R. Campbell, "Transitioning to a Hyperledger Fabric Quantum-Resistant Classical Hybrid Public Key Infrastructure," *The Journal of The British Blockchain Association*, pp. 9902, July 2019.

[32] Segregated Witness for Bitcoin. Scaling Bitcoin Hong Kong, 2015. Available: https://prezi.com/lyghixkrguao/segregated-witness-anddeploying-it-for-bitcoin. [Online].

[33] J. Chen, J. Ling, J. Ning, and J. Ding, "Identity-based signature schemes for multivariate public key cryptosystems," *The Computer Journal*, 62(8), pp. 1132-1147, 2019.

〈저 자 소 개〉

권 혁 동 (HyeokDong Kwon)
정회원
2018년 2월 : 한성대학교 정보시스템공학과 졸업
2020년 2월 : 한성대학교 IT융합공학부 석사
2020년 3월~현재 : 한성대학교 정보컴퓨터공학과 박사과정
<관심분야> 정보보호, 암호구현

심 민 주 (MinJoo Sim)
정회원
2021년 2월 : 한성대학교 IT융합공학부 학사 졸업
2021년 3월~현재 : 한성대학교 IT융합공학부 석사과정
<관심분야> 암호구현, 정보보호

임 세 진 (SeJin Lim)
정회원
2018년 3월~현재 : 한성대학교 컴퓨터공학부 학사과정
<관심분야> 인공지능 보안, 정보보안

강 예 준 (YeaJun Kang)
정회원
2018년 3월~현재 : 한성대학교 컴퓨터공학부 학사과정
<관심분야> 블록체인, 인공지능 보안

서 화 정 (Hwajeong Seo)
종신회원
2010년 2월 : 부산대학교 컴퓨터공학과 졸업
2012년 2월 : 부산대학교 컴퓨터공학과 석사
2015년 4월~5월 : 싱가포르 난양공대 인턴쉽
2016년 2월 : 부산대학교 컴퓨터공학과 박사
2017년 3월 : 싱가포르 과학기술청 연구원
2017년 4월~현재 : 한성대학교 조교수
<관심분야> 블록체인, 인공지능 보안