PQ-PoRR: 라운드로빈 기반 양자 내성 블록체인 합의 알고리즘

김원웅[1], 강예준[1], 김현지[2], 오유진[1], 서화정[3]
[1]한성대학교 IT융합공학과 석사과정
[2]한성대학교 전자컴퓨터공학과 박사과정
[3]한성대학교 융합보안학과 교수
dnjsdndeee@gmail.com, etus1211@gmail.com, khj1594012@gmail.com.
oyj0922@gmail.com, hwajeong84@gmail.com

PQ-PoRR: Post-Quantum Blockchain Consensus Algorithm with Round-Robin

Won-Woong Kim[1], Yea-Jun Kang[1], Hyun-Ji Kim[2],
Yu-Jin Oh[1], Hwa-Jeong Seo[3]
[1]Dept. of IT Convergence Engineering, Han-Sung University
[2]Dept. of Information Computer Engineering, Han-Sung University
[3]Dept. of Convergence Security, Han-Sung University

요 약

양자 컴퓨터의 발전과 쇼어 알고리즘을 통한 ECC(Eliptic Curve Cryptography)에 대한 다항 시간의 솔루션을 제공함으로써 블록체인의 안정성이 위협받고 있다. 본 논문에서는 Round-Robin을 기반으로 하는 알고리즘을 제안함으로써 블록 생성에 대한 공정성을 제공하며 양자 내성 전자 서명인 CRYSTALS-DIlithium을 적용함으로써 근미래에 다가올 양자 위험성에 대비하였다. TPS 측면에서는 DIlithium의 큰 키 크기와 큰 서명 크기에 의해 ECDSA에 비해 낮은 성능을 보여주었지만, Latency 측면에서는 더욱 높은 성능을 보여주며, 이는 실시간성이 중요한 IoT와 같은 분야에서 더욱 높은 효용성을 보여줌을 알 수 있다.

1. 서론

기존의 블록체인에는 주로 타원 곡선 암호 기반의 전자서명이 사용된다. 그러나 쇼어 알고리즘[1]과 양자 컴퓨터에 의해 근 미래에 타원 곡선 암호는 안전하지 않을 것이라 예상되고 있다. 따라서 본 논문에서는 양자 내성 전자서명인 CRYSTALS-Dilithium[2]을 적용한 PQ-PoRR(Post-Quantum Proof of Round-Robin)을 제안한다.

2. 관련 연구

2-1. 합의 알고리즘

블록체인은 분산 원장 기술이 적용된 Peer-to-Peer(P2P) 네트워크이다. 또한 중앙 기관이 존재하지 않아 모든 노드들이 동일한 원장을 소유하여 네트워크를 유지한다. 이에 따라 노드들의 동일한 의사결정을 내리기 위해 수행하는 것이 합의 알고리즘이다. 합의 알고리즘을 통해 데이터의 무결성을 보장할 수 있다.

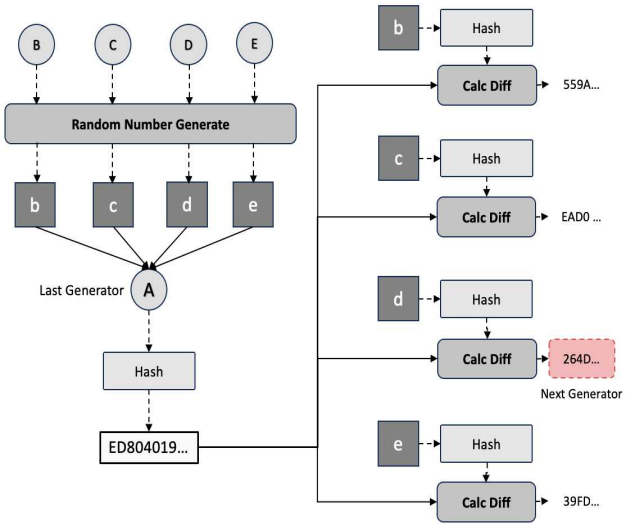
대표적인 합의 알고리즘은 비트코인의 PoW(Proof-of-Work), 이더리움의 PoS(Proof-of-Stake)[3], 기존의 PoS에 위임 기능을 추가한 DPoS(Delegated PoS)[4], TEE(Trusted Execution Environment)를 기반으로 한 PoL(Proof-of-Luck), PoET(Proof-of-Elapsed Time)[5]이 있다.

2-1. CRYSTALS-Dilithium

CRYSTALS-Dilithium은 NIST에서 선정한 표준 양자 내성 암호이다. 최단 벡터 문제에 기반을 한 격자기반암호이다. 보안 단계에 따라 Dilithium-2, 3, 5가 존재하며 보안 단계가 증가할 때 마다 공개키, 개인키 그리고 서명의 크기가 증가한다. Dilithium은 타 양자내성 전자서명 알고리즘들 중에 큰 키 크기와 서명 크기를 갖고 있지만 빠른 연산 속도를 제공한다는 특징이 있다.

3. PQ-PoRR

본 논문은 Round-Robin 방식을 통해 모든 노드들이 동일한 블록 생성 횟수를 가짐으로써 공평한 블록 생성 기회를 보장할 수 있다. 또한 양자 내성 전자서명인 CRYSTALS-Dilithium을 적용하였다. 이를 통해 잠재적인 양자 공격에 대한 보안성을 보장한다.



[그림 1] System Overview

3-1. 알고리즘

[그림 1]은 시스템의 전체적인 과정을 나타낸다. 우선 이전 라운드의 블록 생성자가 다른 노드들로부터 생성된 무작위 값을 수집한다. 그 후 수집한 무작위 값을 연접하여 해시 함수의 입력 값으로 사용하여 라운드 해시 값을 계산한다.. 다른 노드들은 자신의 무작위 값을 해시하여 라운드 해시와의 차이를 계산한다. 차이가 가장 적은 해시를 생성한 노드가 다음 라운드의 블록 생성자로 선택된다. 이 때 이전에 블록을 생성한 적이 있는 노드는 선택되지 않으며 모든 노드가 동일한 수의 블록을 생성하였을 때 블록 생성자로 선택될 수 있다.

4. 성능 평가

블록체인의 성능을 나타내기 위한 지표는 매우 다양하며 한 가지의 지표를 통해 성능을 나타내기 어려우며, 여러 가지 성능 지표들에 대한 연구들이 존재한다[6,7]. 본 논문은 이 중 대표적인 성능 지표인 TPS와 Latency에 대해 측정하였다.

4-1. 실험 환경

본 실험은 C++를 기반으로 구현하였으며 Dilithium-2를 적용하였다. 16GB RAM의 Intel i5-8295U CPU를 사용하여 Ubuntu 20.04.6 LTS 상에서 구현하였다. 또한 실제 블록체인 네트워크와 유사한 환경을 제공하기 위하여 오픈소스 네트워크 시뮬레이터인 NS-3를 사용하였다.

DIlithium을 적용하였을 때의 효용성을 증명하기 위하여 기존 블록체인에 주로 사용되는 ECDSA와의 비교 분석을 진행하였다. 또한 노드의 수를 변경함에 따라 나타나는 성능 차이를 측정하였다.

4-2. TPS (Transaction Per Second)

TPS는 초당 몇 개의 트랜잭션이 처리되었는가를 의미한다. 다시 말해, 초당 몇 개의 트랜잭션이 블록체인에 추가되었는지를 의미한다. TPS는 블록체인의 성능을 측정하기 위해 주요하게 고려되는 대상이지만, 탈중앙화와 확장성을 고려하지 않는다면 TPS를 극단적으로 증가시킬 수 있다. 그러나 그에 따른 중앙화 및 오버헤드 등의 문제가 발생한다.

<표 1> TPS of PoRR (N: the number of nodes)

N	ECDSA	Dilithium
2^1	2068.8	1366.1
2^2	692.3	277.5
2^3	293.9	163.1
2^4	136.7	55.9
2^5	61.5	16.8
2^6	26.2	4.7
2^7	9.3	1.1

<표 1>은 PoRR의 TPS를 나타낸다. 노드의 수가 증가함에 따라 더욱 많은 검증 과정을 거치게 되므로 TPS 성능이 감소함을 알 수 있다. 또한 TPS 측면에서 Dilithium을 적용하였을 때 ECDSA보다 낮은 성능을 보여준다. 그러나 Dilithium은 양자 내성을 보장할 수 있으며, Latency를 통해 낮아진 TPS와 같은 단점을 극복할 수 있다.

4-3. Latency

Latency는 트랜잭션이 네트워크에 나타나고 검증되기까지의 시간을 의미한다. 만약 Latency가 높다면 트랜잭션을 처리하는데에 많은 시간이 걸리는 것을 의미한다. 그러므로 높은 Latency는 블록체인의 성능 저하를 발생시킨다.

<표 2> Latency of PoRR (N: the number of nodes)

N	ECDSA	Dilithium
2^1	0.048	0.004
2^2	0.144	0.021
2^3	0.340	0.036
2^4	0.731	0.107
2^5	1.625	0.356
2^6	3.816	1.272
2^7	10.649	5.399

<표 2>는 PoRR의 Latency를 나타낸다. Latency는 TPS와 마찬가지로 노드가 증가함에 따라 성능이 감소하는 경향을 보인다. 그러나 Latency 측면에서 Dilithium을 적용하였을 때, ECDSA보다 높은 성능을 보여준다. 이는 Dilithium의 실행 속도가 ECDSA보다 빠르기 때문이다. TPS 측면에서는 ECDSA보다 낮은 성능을 보여주지만, Latency는 더 나은 성능을 보여준다. 다시 말해서, 제안 기법은 Latency가 ECDSA에 비해 낮기 때문에 실시간성이 중요한 IoT와 같은 분야에서는 더욱 높은 효용성을 보여준다.

5. 결론

본 논문에서는 공평한 블록 생성 기회를 제공해주며 양자 보안성을 지니고 있는 합의 알고리즘인 PQ-PoRR을 제안하였다. 공정성을 보장함으로써 PoW상에서의 ASIC (Application-Specific Integrated Circuit)과 같은 하드웨어를 사용하여 블록을 독점적으로 생성하는 문제를 해결할 수 있다. 또한 ECDSA를 적용하였을 때보다 TPS 측면에서는 낮은 성능을 보여주지만 양자 내성을 제공하기 위한 trade-off 관계이며, Latency 측면에서는 오히려 더욱 높은 성능을 보여줌으로써 IoT와 같은 분야에서 더욱 높은 효용성을 보여주는 것을 확인하였다.

6. 결론

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services, 50%) and this work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2022-0-00627, Development of Lightweight BIoT technology for Highly Constrained Devices, 50%).

참고문헌

[1] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete log- arithms on a quantum computer,” SIAM review, vol. 41, no. 2, pp. 303 - 332, 1999.

[2] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehl ´e, “Crystals-dilithium: A lattice-based digital signature scheme,” IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 238 - 268, 2018.

[3] G. Wood et al., “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum project yellow paper, vol. 151, no. 2014, pp. 1 - 32, 2014.

[4] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, “Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism,” IEEE Access, vol. 7, pp. 118541 - 118555, 2019.

[5] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, “On security analysis of proof-of-elapsed-time (poet),” in Stabilization, Safety, and Security of Distributed Systems: 19th International Symposium, SSS 2017, Boston, MA, USA, November 5 - 8, 2017, Proceedings 19, pp. 282 - 297, Springer, 2017.

[6] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, “A survey of blockchain consensus algorithms performance evaluation criteria,” Expert Systems with Appli- cations, vol. 154, p. 113385, 2020.

[7] M. Salimitari and M. Chatterjee, “A survey on consensus protocols in blockchain for iot networks,” arXiv preprint arXiv:1809.05613, 2018.