블록체인에서의 양자 내성 전자서명 연구 동향

김원웅*, 강예준*, 김현지*, 서화정**

*한성대학교 (대학원생)

**한성대학교 (교수)

Trends of Post-Quantum Digital Signature in Blockchain

Won-Woong Kim*, Yea-Jun Kang*, Hyun-Ji Kim*, Hwa-Jeong Seo**

*Hansung University(Graduate student)

**Hansung University(Professor)

요 약

최근 양자 컴퓨터의 급속한 발전으로 인하여 기존 블록체인의 보안성의 한계가 드러나고 있다. 양자 컴퓨터의 경우 Shor 알고리즘과 Grover 알고리즘을 통해 기존 블록체인의 보안성을 낮출 수 있으며, 보완되지 않을 경우 기존 네트워크의 사용자들의 개인정보가 무방비하게 노출될 수 있다. 이러한 문제를 해결하기 위한 단서를 제공하기 위하여 본 논문에서는 양자 내성 전자서명을 적용한 블록체인의 연구 사례에 대해 조사하였다.

I. 서론

최근 양자 컴퓨터의 급속한 발전으로 인해 기존의 블록체인 네트워크에서 트랜잭션을 검증하는 데에 사용되는 전자 서명 체계의 취약성이 드러나고 있다[1]. 양자 컴퓨터의 경우 현대 비대칭 암호에서 사용되는 유한 아벨 그룹에 대해 고전적인 수학적 난제 문제를 해결하기 위해 엄청난 속도 향상을 제공할 수 있다. 기존의 가장 많이 사용되는 전자서명 체계인 RSA와 ECDSA의 경우에도 유한 아벨 그룹 구조로 구성되어 있다. 결국 인수분해 및 이산 대수에서의 난제를 주기 찾기 범위로 줄일 수 있으며, 이러한 문제는 양자 컴퓨터에서 수행되는 푸리에 변환으로 해결할 수 있다. 또한 Shor 알고리즘[2]은 양자 푸리에 변환에 의해 인수분해 및 이산 대수 문제에 대하여 기하급수적인 속도 향상을 제공할 수 있다. Grover 알고리즘[3]의 경우에도 주로 사용되는 합의알고리즘인 PoW(Proof-of-Work)의 해시 충돌을 탐색하는 데에 사용될 수 있다. 또한 무작위 값 생성시간을 줄임으로써 체인을 빠르게 재구성하여 체인 재생성 공격이 가능해진다. 이로 인해 현재 대부분의 블록체인 시스템에 적용된 디지털 서명 알고리즘의 보안성이 문제가 되고 있으며, 사용자의 개인 정보 및 금전적인 피해가 존재할 것이다. 따라서 이러한 문제를 해결하기 위해 양자 내성 블록체인의 귀추가 주목되고 있으며, 본 논문에서는 양자 내성 전자서명 기법을 적용한 PQB(Post-Quantum Blockchain)의 연구 사례에 대하여 알아본다.

II. 관련 연구

블록체인이란 네트워크 내의 노드들이 p2p(peer-to-peer) 방식으로 통신하여, 동일한 원장을 노드들이 공유하는 분산 원장 네트워크를 말한다.[4] 원장은 네트워크 내에 발생하는 모든 거래를 말하며, 이는 블록에 포함되어 체인 형태로 묶여있다. 블록체인은 기존의 중앙 서버가 데

이터를 관리 방식과 다르게 탈중앙화되어 있어 네트워크 내의 노드들이 각각 원장을 소유하고 있다. 따라서 해커가 데이터를 위변조하고자 할 경우 네트워크 내의 과반수 노드들의 원장을 조작해야 한다. 이는 사실상 불가능하여, 네트워크에서 발생하는 거래의 무결성을 보장한다. 블록체인에서 블록을 공유하는 방식을 합의 알고리즘이라고 하며 다양한 합의 알고리즘이 존재한다. 대표적으로 비트코인에서의 작업 증명, 이더리움에서 사용하는 지분 증명 합의 알고리즘이 있다.

III. 연구 동향

3.1 [4]

해당 논문에서는 양자 컴퓨터와 전통적인 공격 기법에 대해 안전하다고 알려진 유한체 내에서의 2차 방정식 문제를 기반으로 하는 NP-hard 문제에 기반한 임계값 서명 스킴을 제안하였다. 기존의 임계값 서명의 경우 대부분 양자 컴퓨터의 공격에 대해 안전하지 않은 RSA 및 ECDSA를 사용하기 때문에 양자 내성 임계값 서명을 사용하는 것이 향후의 블록체인에 있어서 더 나은 선택으로써 작용한다. 또한 이러한 서명 스킴을 기반으로 하는 합의 알고리즘을 제안한다. 이때, 1.5개 이상의 노드가 양자 내성 임계값 서명을 기반으로 새로운 블록에 서명을 했을 경우에만 해당 블록을 생성할 수 있게 된다. 이러한 동작 과정은 PoW 및 PoET(Proof-of-Elapsed-Time) 등에 비해 양자 공격에 대해 안전하며 효율적이다. 최종적으로 이러한 합의 알고리즘을 기반으로 하는 블록체인 시스템을 설계한다.

기존의 대표적인 합의 알고리즘인 PoW의 경우 새로운 트랜잭션을 확인하는 데에 있어 60분의 시간이 걸린다. 이에 근거하여, 전통적인 데이터 관리 기술인 데이터베이스에 비해 P2P 네트워크에서의 합의에 도달하는 것은 매우 복잡하며 비효율적이라는 것을 알 수 있다. 따라서 이러한 문제를 해결하기 위해 합의 알고리즘을 개선해야 한다. 이를 위해 해당 논문의 임계값 서명 기법은 양자 컴퓨터가 등장했을 때에도 안전하다고 여겨지는 유한체 내에서의 2차 방정식을 푸는 NP-hard 문제에 기반한 임계값 서명 방식을 제안하였다. 해당 서명 기법은 n명의 사용자 그룹 사이에서 사용되며 각 그룹에는 그룹 관리자가 존재한다. 그룹 관리자는 개인키를 생성하여 안전한 방식으로 n명의 사용자에게 개인키를 전송한다. 그 후, 그룹 관리자는 개인키를 기반으로 공개키를 생성한다. n명의 사용자 중 적어도 t명의 사용자가 메시지에 대해 서명할 경우 유효한 서명을 생성할 수 있다. 이 때 그룹 관리자만이 서명을 확인하여 누가 서명하였는지에 대해 확인 및 검증이 가능하다.

자세한 서명 스킴은 다음과 같다. 우선 노드 수를 n, n명의 노드들 중 메시지에 효율적으로 서명할 수 있는 노드 수를 t라고 나타낸다. 그룹 관리자는 R로 표현하며 개인키인 k_r을 관리한다. 이 때, k_r은 다항식 F와 선형 변환 L의 계수이며 랜덤하게 생성된다. F의 계수는 유한체 내의 다변식의 계수이고, L의 계수는 유한체 내의 매트릭스와 벡터를 위미한다. 관리자의 공개키는 개인키 k_r를 $\overline{F}= F \circ L$, $\overline{F_1}= F_1 \circ L_1$, $\cdots$, $\overline{F_n}= F_n \circ L_n$에 대입하여 생성된다. 이때 각 공개키는 $\overline{F}, \overline{F}_1, \cdots, \overline{F}_n$의 계수이다.

해당 논문의 블록체인 합의 알고리즘은 다음과 같다. 우선 m명의 관리자 노드를 선택한다. 그리고 네트워크를 m개의 그룹으로 나눈다. 각 관리자는 n명의 노드가 포함된 그룹을 관리한다. 그 중 랜덤하게 그룹을 하나 선출하고 새로운 블록을 생성하도록 한다. 리더 그룹의 관리자는 한 노드를 무작위로 선택하여 새로운 블록을 생성하도록 한다. 선택된 노드는 트랜잭션과 검증 정보를 포함하여 블록을 생성하고 관리자에게 해당 블록의 정보를 전송한다. 관리자는 받은 블록을 그룹 내의 노드들에게 전송하고 양자 내성 임계값 서명에 기반하여 서명하도록 한다. 1.5개 이상의 노드가 서명할 경우 블록은 유효하다고 판단된다. 블록을 생성하도록 선택되었던 노드는 자신의 체인에 블록을 추가하고 다음 블록 생성자를 선택하기 위한 난수값을 생성한다.

이러한 블록체인 시스템을 통하여 양자 내성을 만족할 수 있으며, 기존의 블록체인에 비해 효율적인 동작이 가능하다. 또한 그룹 관리자를

신뢰할 수 있는 정부 및 기관으로 선정할 수 있으며, 이러한 네트워크 내에서의 악의적인 블록을 생성하는 것을 매우 어렵게 만든다. 또한 개인키의 존재에 의해 관리자 없이 서명을 생성하는 것이 매우 어려워지므로 신뢰성이 증대된다. 또한 새로운 블록 생성 전에 관리자는 자신의 그룹의 노드들을 다른 그룹의 노드들과 교환하여 그룹을 선택하는 데에 있어 공평성을 보장할 수 있다.

3.2 [5]

해당 논문에서는 우선 양자 컴퓨터의 급속한 발전으로 인해 발생하는 양자 공격에 대응하기 위하여 Shor 알고리즘 및 Grover 알고리즘을 기반으로 한 양자 컴퓨팅 공격에 대한 기존 블록체인 네트워크의 취약성과 몇 가지 양자 내성 기법에 대한 개요를 제공한다. 그 후, 블록체인 네트워크를 보호하는 데에 사용할 수 있는 새로운 격자 기반 서명 스킴을 제안하였다. 해당 스킴의 공개키 및 개인키는 루트키에서 RandBasis 알고리즘을 사용하는 Bonsai Trees 기술에 의해 생성된다. RandBasis 알고리즘과 ExtBasis 알고리즘을 결합하여 트랜잭션 메시지를 확인하기 위한 개인키를 생성한다. 이는 알고리즘 ExtBasis의 출력을 무작위화 하고 사용자 개인 정보의 보안을 향상시킬 수 있다. 또한 랜덤성을 보장할 뿐만 아니라 경량 지갑을 구성할 수 있게 된다. 제안 기법의 안정성을 SIS(Short Integer Solution)문제를 기반으로 하고 있으며, 임의의 오라클 모델에서 메시지가 위조되지 못하며 효율적이라는 것을 증명할 수 있다. 또한 공개키, 개인키 그리고 서명의 크기가 기존의 연구보다 작기 때문에 계산 복잡도를 줄이고 구현 효율성을 높일 수 있다.

3.3 [6]

해당 논문에서는 격자 기반의 전자 서명 기법을 제안하였다. 격자 기반 위임 알고리즘을 사용하여 임의의 값을 선택하여 개인키를 생성하고 사전 이미지 샘플링 알고리즘으로 메시지에 서명한다. 또한 이중 서명으로 정의되는 체계에서 첫 번째 서명과 마지막 서명을 설계하여 메시지와 서명 간의 상관관계를 줄이는 데에 사용한다. 또한 이러한 서명 방식을 블록체인과 결합하여 PQB를 구성하고 암호화폐 방식을 제안한다. 이를 통해 보안을 SIS 문제로 축소시키며, 양자 컴퓨팅 공격에 대한 저항성과 격자 SIS 가정 하에서 정확성과 위조 가능성을 만족한다. 또한 기존 서명에 비해 서명 및 개인키의 크기가 감소하므로 계산 복잡도를 줄일 수 있으며, 결론적으로 보다 안전하고 효율적인 암호화폐를 설계할 수 있게 된다.

해당 논문에서의 서명 알고리즘은 SetUp, KeyGen, Sign, Verify의 네 단계로 구성되어 있다. 우선 SetUp 단계에서는 보안 매개변수인 n을 입력하면 SetUp 알고리즘이 마스터 비밀키인 MK 및 공개 매개변수 PP를 출력한다. KeyGen 단계에서는 공개 매개변수 PP, 마스터 비밀키 MK 및 ID ms를 입력하면 ms에 해당하는 개인키 sk를 출력한다. Sign 알고리즘은 공개 매개변수 PP, 메시지 msg 및 사용자의 개인키 sk를 입력하면 서명 e를 출력한다. Verify 알고리즘은 공개 매개변수 PP, 서명 e, 메시지 msg 및 ID ms를 입력하였을 때, 서명 e가 유효하면 1, 그렇지 않으면 0을 출력한다.

IV. 결론

본 논문에서는 양자 내성 전자서명 기법을 적용한 PQB의 연구 사례에 대해 조사하였다. 양자 컴퓨터의 경우 Shor 알고리즘과 Grover 알고리즘을 통해 기존의 블록체인 네트워크의 보안성을 낮춰 사용자들에게 금전적인 피해 및 개인정보 탈취 등과 같은 문제를 일으킬 수 있게 된다. 이러한 문제를 해결하기 위해 양자 내성 전자 서명을 적용한 합의 알고리즘은 바람직한 해결책으로 검토될 수 있으며, 본 논문에서 조사한 연구 사례는 포스트 퀀텀 시대의 미래 PQB에 대한 연구를 하는 데에 있어 도움이 될 수 있다.

V. Acknowledgement

This work was partly 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 partly 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] Aggarwal, Divesh, et al. "Quantum attacks on Bitcoin, and how to protect against them." *arXiv preprint arXiv:1710.10377* (2017).

[2] Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." *SIAM review* 41.2 (1999): 303-332.

[3] Grover, Lov K. "A fast quantum mechanical algorithm for database search." *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. 1996.

[3] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." *Decentralized business review* (2008): 21260.

[5] Yi, Haibo, et al. "An efficient blockchain consensus algorithm based on post-quantum threshold signature." *Big Data Research* 26 (2021): 100268.

[6] Li, Chao-Yang, et al. "A new lattice-based signature scheme in post-quantum blockchain network." *IEEE Access* 7 (2018): 2026-2033.

[7] Yi, Haibo, et al. "An efficient blockchain consensus algorithm based on post-quantum threshold signature." *Big Data Research* 26 (2021): 100268.