블록체인 상의 키 교환 알고리즘 적용 사례

강예준*, 김원웅*, 김현지*, 서화정*†

*한성대학교 (대학원생)

*† 한성대학교 (교수)

Key Exchange Algorithm Application Case on Blockchain

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

*Hansung University(Graduate student)

*† Hansung University(Professor)

요 약

최근 블록체인은 다양한 분야에서 활용되고 있다. 하지만 블록체인의 특성 중 하나인 투명성으로 인해 프라이버시 보호 문제가 대두되고 있다. 이를 해결하고자 블록체인에 키 교환 알고리즘을 추가하여 개인 정보를 보호하려는 연구가 다수 진행되고 있다. 본 논문에서는 블록체인 상의 키 교환 알고리즘 적용 사례에 대해 살펴본다. 대표적으로 의료 데이터를 대칭키로 암호화하여 관리함으로써 프라이버시를 보호하였다. 또한 스마트시티와 교통 시스템에 적용된 블록체인 상에 키 교환 알고리즘을 활용하여 익명화하는 연구도 수행되었다. 하지만 추후 양자컴퓨터가 등장함에 따라, PQC로의 전환이 고려될 필요가 있다. PQC로 전환될 경우 속도 및 용량이 변화함에 따라 블록체인의 성능이 달라질 수 있으므로 이를 위한 다양한 연구가 수행되어야할 것으로 생각된다.

I. 서론

최근 다양한 분야에서 블록체인을 활용한 연구가 다수 진행되고 있다. 동시에 블록체인의 특성인 투명성으로 인한 프라이버시 보호 문제가 대두되고 있다. 이에 대한 대응책으로 블록체인 상에서 키 교환을 적용하려는 시도가 다수 이루어지고 있다. 본 논문에서는 블록체인 상의 키 교환을 적용함으로써 프라이버시를 보호한 사례에 대해 살펴본다.

II. 관련연구

1.1 블록체인

블록체인이란 모든 네트워크 참여자가 peer-to-peer 방식으로 연결되어, 원장을 모든 참여자가 공유함으로써 조작을 방지하는 분산 원장 네트워크이다[1]. 기존에는 서버가 데이터를 관리 및 저장을 수행하는 중앙 집중형 방식이다. 중앙 집중형의 문제점은 서버만이 데이터를 관리하기 때문에, 비용 문제 및 보안 문제가 발생할 수 있다. 비용 문제란 중앙 서버가 모든 데이터를 유지하고 관리하기 비용으로 클라이언트에게 수수료를 요구하는 것을 말한다. 보안 문제의 경우 해커의 공격 대상이 중앙 서버로 한정되어 있기 때문에, 단일 실패점 문제를 말한다. 하지만 블록체인은 모든 네트워크 참여자가 원장을 공유하여 제 3자인 중앙 서버가 존재하지 않는다. 따라서 해커가 데이터를 위조하기 위해서는 중앙 서버를 해킹하는 것이 아니라, 과반수의 네트워크 참여자가 가지고 있는 원장을 조작해야만 한다. 이는 사실상 불가능하여 데이터의 무결성을 보장한다. 블록체인의 종류로는 누구나 참여 가능한 퍼블릭 블록체인과, 허가받은 노드만이 참여 가능한 프라이빗 블록체인이 있다.

1.2 키 교환 알고리즘

키 교환 알고리즘이란 두 당사자가 안전하지 않은 채널에서 안전하게 동일한 대칭키를 공유하는 알고리즘이다. 대표적으로 이산 로그를 기반

으로 하는 Diffie-Hellman 알고리즘이 있다[2]. 하지만 Diffie-Hellman 알고리즘의 경우 중간자 공격에 취약하며, 상대방에 대한 인증 기능이 없다. 이에 대한 해결책으로 인증된 키 교환 알고리즘이 있다[3]. 이는 전자서명을 통해 상대방을 검증한 후에 키를 교환함으로써 중간자 공격을 예방할 수 있는 알고리즘이다.

III. 본론

본 논문에서는 블록체인 상의 키 교환 알고리즘을 적용한 사례에 대해 살펴본다. IEEE ICCT(International Conference on Communication Technology)'21에서는 의료 데이터를 보호하기 위해 블록체인 상에 키 캡슐화 메커니즘을 적용하여 프라이버시를 보호하는 기법을 제안하였다[4]. 의료 데이터는 일반적으로 중앙집중식으로 관리하는데, 이는 단일 장애점, 보안 문제, 비용 문제 등과 같은 문제점이 존재한다. 이러한 문제점을 해결하고자 최근 블록체인 기술을 의료 데이터를 저장 및 공유하기 위한 기술로써 블록체인을 활용하는 연구가 다수 진행중이다. 하지만 블록체인의 경우 투명성이라는 특징을 가지고 있어 개인 정보 유출 문제가 발생할 수 있다. 이를 방지하고자 [5]에서는 비대칭키를 통해 의료 데이터를 암호화하여 프라이버시를 보호하였다. 하지만 비대칭키의 특성상 비효율적이라는 문제점이 존재하였다. 이러한 문제점을 해결하고자 [4]에서는 블록체인에서의 키 캡슐화 메커니즘 기반의 의료 프라이버시 보호 기법을 제안하였다. 해당 논문에서는 먼저 의료 데이터를 대칭키를 통해 암호화한 후, 대칭키를 비대칭 암호화 알고리즘의 공개키를 통해 캡슐화한다. 그 후, 공개키와 암호화된 대칭 암호키를 스마트 컨트랙트에 저장한다. 만약 환자의 진료 기록이 필요할 경우, 비대칭키를 통해 암호화된 대칭키를 복호화하고 복호화된 대칭 비밀키를 이용하여 데이터를 복호화한다. 해당 기법을 통해 환자의 프라이버시를 보호할 수 있다. 실제 실험을 위해 대칭키를 SM4, SM2가 사용되었으며, 합의 알고리즘은 PBFT 합의 알고리즘을 사용하였다. 실험 결과 노드 수에 따라 처리량이 변동하지만, 키 캡슐화를 적용하였을 때의 TPS는 비대칭키를 적용하였을 때보다 낮았으며 대칭키를 적용하였을 때보다는 높았다.

WCMC(Wireless Communications and Mobile Computing)'22에서는 블록체인 기반의 스마트시티를 위한 인증된 키 교환 프로토콜(DAKE)을 제안하였다[6]. 스마트시티의 특성상 참여자가 분산되어 있고 서로 신뢰할 수 없는 환경이다. 이러한 스마트시티의 특성을 고려하여 해당 논문에서는 인증된 키 교환 프로토콜을 활용하였다. 키 교환 과정에서 만족하고자하는 보안 속성 (Static secrecy, Perfect forward secrecy, Implicit authenticity, Explicit authenticity, Identity protection, Deniability)에 따라 여러 버전의 DAKE가 있다. 이는 모두 키 교환 프로토콜이며 해당 논문에서는 ElGamal 암호화 알고리즘(128byte~384byte)을 사용하여 세션키를 암호화하였다. 이더리움 네트워크에서 실험한 결과, DAKE1이 보안 속성을 가장 적게 만족하지만 속도가 가장 빠르며, DAKE5로 갈 수록 더 높은 보안 속성을 가지지만 키 교환에 더 오랜 시간이 소요된다. 해당 연구는 여러 종류의 보안 속성을 만족하는 스마트시티를 설계하는데에 적용될 수 있다.

IEEE T-ITS(Transactions on Intelligent Transportation Systems)'22에서는 블록체인 기반의 스마트 교통 시스템 상에서 익명의 참가자들 간의 인증된 키 교환 방식을 제안하였다[7]. 스마트 교통 시스템에는 차량, 도로변 장치 등의 여러 엔티티가 존재한다. 이들 간의 안전한 통신을 위해서는 익명의 엔티티 간의 인증된 키 교환 과정이 필요하다. 이를 위해 ECDH를 사용하였으며, 이렇게 생성된 세션키를 사용하면 클라우드 서버와 도로변 장치 및 차량간에 트래픽 정보를 안전하게 전송할 수 있다. PUF(Physical unclonable function)와 함께 해시 함수, 비트 배타적 논리합(XOR) 연산자, 타원 곡선 암호(ECC) 및 대칭 암호화/복호화로 구성된 초경량 암호 기술을 사용하였으며 이로 인해 통신 및 계산 오버헤드가 감소하였다.

IV. 결론

본 논문에서는 블록체인에서 발생할 수 있는 프라이버시 보호 문제를 예방하기 위해 키 교환 알고리즘을 적용한 사례들을 살펴보았다. 다양한 분야에서 키 교환 알고리즘이 적용되고 있으며, 일반적으로 공개키를 사용하였을 때보다 성능이 향상되었다. 하지만 추후 양자 컴퓨터가 등장함에 따라, 기존 키 교환 알고리즘을 PQC(Post Quantum Cryptography)로의 전환이 필요할 수 있다. PQC로 전환할 경우 속도 및 용량이 변화함에 따라 블록체인의 성능이 달라질 수 있으므로 이를 위한 다양한 연구가 수행되어야 할 것으로 생각된다.

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] March, 2002.Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized business review (2008): 21260.

[2] Diffie, Whitfield, and Martin E. Hellman. "New directions in cryptography." Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman. 2022. 365-390.

[3] Boyko, Victor, Philip MacKenzie, and Sarvar Patel. "Provably secure password-authenticated key exchange using Diffie-Hellman." Cryptology ePrint Archive (2000).

[4] Chen, Yanchi, Haoxiang Luo, and Qing Bian. "A Privacy Protection Method Based on Key Encapsulation Mechanism in Medical Blockchain." 2021 IEEE 21st International Conference on Communication Technology (ICCT). IEEE, 2021.

[5] Wang RJ, Yu SZ, Li Y, et al., “Medical blockchain of privacy data sharing model based on ring signature,” Journal of University of Electronic Science and Technology of China, vol. 48(6), pp. 886-892, 2019.

[6] Wu, Qiong, et al. "DAKEs: Decentralized Authenticated Key Exchange Protocols via Blockchain for Smart City." Wireless Communications and Mobile Computing 2022 (2022).

[7] Badshah, Akhtar, et al. "AAKE-BIVT: Anonymous Authenticated Key Exchange Scheme for Blockchain-Enabled Internet of Vehicles in Smart Transportation." IEEE Transactions on Intelligent Transportation Systems (2022).