Journal of KIIT. Vol. 23, No. 11, pp. 195-205, Nov. 30, 2025. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2025.23.11.195

블록체인 기반 영지식 증명과 트랜잭션 믹서를 이용한 개인정보 보호 시스템

윤영준*, 정현준**

Blockchain-based Privacy Protection System using ZK-Proof and Transaction Mixer

Youngjoon Yoon*, Hyunjun Jung**

요 약

최근 블록체인 기반 자격 증명 시스템이 활발히 연구되며, 개인정보의 안전한 저장과 검증에 대한 관심이 증가하고 있다. 그러나 블록체인은 트랜잭션이 모두 공개되는 특성상, 저장된 정보뿐 아니라 정보를 주고받는 주체 간 관계까지 노출되는 한계가 있다. 이러한 구조는 신뢰성과 무결성을 제공하는 동시에 민감 정보의 추적 및 분석 가능성으로 프라이버시 침해 우려를 낳는다. 이에 본 논문은 영지식 증명과 트랜잭션 믹서를 결합한 개인정보 보호 시스템을 제안한다. 사용자가 블록체인에 민감 정보를 등록하되, 내용은 노출되지 않고 진위만 증명되며, 거래 경로 또한 은닉된다. 이를 통해 개인정보의 내용과 관계 모두를 보호하는 인증 구조를 구현하고자 한다. 제안 시스템은 기존 zk-SNARK 단독 적용 시스템 대비 향상된 프라이버시 보호 성능을 제공한다.

Abstract

Blockchain-based credential systems are being actively studied, with increasing interest in the secure storage and verification of personal information. However, due to the transparent nature of blockchain, not only the stored data but also the relationships between transacting parties can be exposed. While such structure ensures trust and integrity, it raises privacy concerns by enabling the tracking and analysis of sensitive data. This paper proposes a personal data protection system that combines ZK-Proof and transaction mixer. Users can register sensitive data on the blockchain without disclosing its content while proving its validity, and the transaction path is also concealed. The proposed system provides enhanced privacy protection compared to existing systems that use only zk-SNARK without a transaction mixer.

Keywords
zero-knowledge proof, groth16, blockchain, ethereum, IPFS, transaction mixer

* 국립군산대학교 소프트웨어학과 학사과정
- ORCID: https://orcid.org/0009-0005-1617-8393
** 국립군산대학교 소프트웨어학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0002-6717-1395

· Received: Aug. 13, 2025, Revised: Sep. 29, 2025, Accepted: Oct. 02, 2025
· Corresponding Author: Hyunjun Jung
Dept. of Software at Kunsan National University, 558, Daehak-ro, Kunsan-si, Jeollabuk-do, Republic of Korea
Tel.: +82-63-469-8917, Email: junghj85@kunsan.ac.kr

Ⅰ. 서 론

2024년 IBM 데이터 유출 비용 보고서에 따르면 전 세계 데이터 유출 사고 한 건의 평균 비용은 약 488만 달러로 전년 대비 증가했으며, 특히 고객 개인 식별 정보(PII, Personally Identifiable Information)가 관련된 사건 비중과 비용이 가장 큰 것으로 보고됐다[1]. 이는 데이터 유출의 재정적 위험이 지속적으로 확대되고 있음을 의미하며, 기업·기관 개인정보 보호 대책이 필수임을 시사한다.

블록체인 기술은 신뢰성과 무결성을 제공하지만, 모든 트랜잭션이 공개되고 기록이 영구 보존된다는 특성 때문에 프라이버시 측면에서 도전 과제를 낳는다. 특히 DID(Decentralized Identifier)와 VC (Verifiable Credential) 기반 시스템에서는 데이터 내용뿐 아니라 “누가 누구에게 어떤 요청을 보냈는가”와 같은 관계 정보까지 남아 사용자의 행위가 추적될 위험이 존재한다. W3C(World Wide Web Consortium)의 VC 표준 논의에서도 상관관계 최소화와 제3자에 의한 링크 불가가 중요한 원칙으로 다뤄진다[2]. 기존에는 데이터 자체를 암호화하거나 오프체인에 보관해 내용 노출 억제에 집중해 왔다. 그러나 트랜잭션 타임스탬프, 수수료 패턴, 주소 재사용, 이벤트 로그와 같은 행위 기반 메타데이터는 온체인에 남아 그래프 클러스터링과 타이밍 분석을 통해 주체 간 관계가 유추될 여지가 크다.

동일 지갑에서 반복적으로 증명이 제출되면 요청자 - 응답자 간 통신 패턴이 강화되고, 단일 경로로만 증명이 전파되면 네트워크 관찰자가 라우팅을 역추적할 위험도 존재한다[3]. 따라서 내용 은닉만으로는 충분하지 않으며, 제출 경로와 상호작용 자체의 비연계성을 함께 보장해야 한다.

본 연구는 이러한 한계를 해소하기 위해 영지식 증명(ZKP, Zero-Knowledge Proof)과 트랜잭션 믹싱을 결합한 개인정보 보호 시스템을 제안한다. 블록체인은 무결성과 검증 가능성을, 영지식 증명은 민감한 원본을 공개하지 않고도 조건 충족을 입증하는 능력을 제공한다. 예를 들면, 사용자는 생년월일을 밝히지 않고도 “성인”임을 증명할 수 있다[4].

한편 믹서는 다수 사용자의 트랜잭션을 결합·재배치해 발신자와 수신자 사이의 직접 연결 고리를 제거함으로써 온체인 행위 추적을 어렵게 한다. CoinJoin 류의 절차처럼 입력과 출력을 동일 크기 집합으로 묶고 교환하면 링크 가능성은 급격히 낮아진다[5]. 나아가 본 시스템은 제출된 증명마다 재사용 불가능한 nullifier를 생성·검사하여 이중 제출을 방지하고, 검증자는 증명의 진위를 온체인에서 확인하되 원본 데이터나 제출자의 지갑 주소는 알 수 없다. 증명은 공개 신호만 온체인에 남기며, 원본 속성은 체인 밖에서 분리 보관된다.

제안 시스템은 세 가지 축으로 구성된다. 첫째, 지갑·발급자·검증자·블록체인 네트워크·믹서 간 상호작용을 정의한다. 둘째, 사용자가 개인정보를 암호화·저장해 검증용 식별자를 준비한다. 셋째, 검증 과정에서 영지식 증명과 믹싱을 결합해 관계 노출을 차단한다.

본 시스템은 기존 zk-SNARK 단독 적용 시스템이 제공해 온 선택적 속성 검증과 제3자 의존 축소의 장점을 계승하면서, 트랜잭션 믹싱을 결합해 행위 추적성을 구조적으로 약화시킨다. 또한 Ethereum 및 IPFS를 활용한 DID 시스템의 실증 결과처럼, 사용자는 원본 데이터 공개 없이 “특정 조건을 만족”한다는 사실만으로 신뢰를 확보할 수 있으며[6], W3C Verifiable Credentials 데이터 모델을 준수해 최소 정보 공개와 사용자 통제권을 구현한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 개인정보 보호와 블록체인 및 영지식 증명, 믹싱 관련 관련 연구를 정리한다. Ⅲ장에서는 제안 시스템을 설명하는데, 전체 아키텍처와 주요 프로세스, 스마트 컨트랙트 주요 함수, 트랜잭션 믹서를 통한 프라이버시 보호를 순차적으로 기술한다. Ⅳ장에서는 ZK 증명 및 믹싱 결과를 제시하고, Ⅴ장에서는 결론 및 향후 과제를 정리한다.

Ⅱ. 관련 연구

이 장에서는 블록체인 기반 개인정보 보호 시스템 연구에 대한 동향을 설명한다.

2.1 신뢰성 있는 경력 증명을 위한 블록체인 기반 디지털 배지 프레임워크 설계

S. Jeong and H. Jung[7]은 신뢰성 있는 경력 검증을 위해 프라이빗 블록체인과 디지털 배지를 결합한 프레임워크를 설계하였다. 프라이빗 체인을 전제로 배지(NFT, Non-Fungible Token) 발급·조회 흐름과 구성요소를 제시하고, 검증 정보를 블록체인에 기록해 위변조를 방지하며 검증 시간을 단축하는 기대효과를 논의한다. 그러나 설계 중심으로 정량 실험과 공개 체인 상호운용·선택적 공개가 미흡하고, 행위 메타데이터 보호도 다루지 않는다. 평가 항목은 카테고리 비교·절차 제시에 머물러 수치 기반 검증이 부재하다. 또한 사용자 선택적 속성 제시나 ZK 연계는 논의되지 않는다. 본 논문은 온체인에서 ZK-Proof와 믹서를 통합해 내용 은닉과 링크 불가를 동시에 달성하는 방향으로 공백을 메운다. 아울러 운영 가이드라인을 제시한다.

2.2 영지식 증명을 활용한 블록체인 기반 개인정보 관리 기법

J. Lee et al.[8]는 zk-SNARK를 이용한 블록체인 기반 개인정보 관리 기법을 제안하였다. 개인정보 저장·제출·검증 알고리즘과 변수 정의를 제시하고, 신뢰기관 관여를 최소화한 verifiable computing 구조를 설명한다. 구성은 CRS(Common Reference String) 기반 증명 생성과 검증 절차, 참여자 역할을 수학적으로 기술하고 가정들을 열거한다. 그러나 권한 통제된 허가형 블록체인 환경과 신뢰 당사자를 전제하고, 링크 불가·행위 메타데이터 보호는 고려하지 않는다. 또한 온체인 검증 비용·성능에 대한 수치 평가가 부재하다. 본 논문은 퍼블릭 이더리움에서 Groth16 검증과 nullifier, 믹서를 결합해 재사용 방지와 관계 은닉을 실험 수치로 입증한다. 제시 수준은 개념적 시연에 가깝다.

2.3 Decentralization of Identity using Ethereum and IPFS

S. Lohar et al.[9]는 Ethereum과 IPFS를 결합한 분산 신원 관리에서 DID 생성, 속성 저장, ZK 기반 연령 확인을 제안한다. VC/SSI(Self-Sovereign Identity) 원칙을 준수하며 생년월일 노출 없이 '18세 이상'만을 증명하는 시나리오를 제시한다. 계층적 아키텍처와 스마트컨트랙트 흐름을 설명하고, 결과 및 분석 섹션에서 체계의 타당성을 논의한다. 그러나 메타데이터 노출과 관계 링크 불가, 믹싱·nullifier 기반 재사용 방지는 다루지 않으며, 성능 수치나 가스·지연 평가가 부족하다. DID-CID 연계를 활용하나 상호운용과 확장성 검증은 제한적이다. 이에 본 논문은 퍼블릭 체인에서 ZK-Proof와 믹서를 통합해 지갑 개수, 방어율 수치, 증명 생성 시간, 가스비(Wei), 각 지표에 대한 효율성 트렌드 파악 등 지표로 효과를 입증한다.

III. 블록체인 기반 영지식 증명과 트랜잭션 믹서를 이용한 개인정보 보호 시스템

이 장에서는 논문에서 제안하는 시스템의 전체 구조와 각 기능의 흐름에 대하여 설명한다.

3.1 전체 아키텍처

본 시스템은 그림 1과 같이 발급자 서비스, IPFS, 클라이언트 레이어, ZK-증명 모듈, 프라이버시 링 믹서, 이더리움 스마트 컨트랙트군, 네트워크 인프라로 구성된다. 네트워크 인프라는 P2P(Peer-to-Peer) 합의·블록 전파를 처리해 서버 없이 동작한다. 사용자는 발급자 서비스에서 DID·VC를 받은 뒤 클라이언트에서 개인정보를 암호화해 IPFS에 저장해 CID를 얻는다. CID·VC는 ZK-증명 모듈로 전달돼 Circom 회로와 Groth16 프로버를 거쳐 증명을 생성해 공개 신호와 함께 Verifier 컨트랙트에 제출된다. Verifier 컨트랙트는 검증자 요청에 유효성을 판별한 뒤 이벤트를 배포한다. 검증이 통과되면 Mixer 컨트랙트가 링 서명 기반 혼합 트랜잭션을 작성해 브로드캐스트하고 Registry 컨트랙트는 사용자가 속성을 최초 등록 시 DID-CID 매핑과 nullifier 사용 여부를 기록해 이중 제출을 차단한다. 원본 PII는 체인 밖에 저장돼 프라이버시를 지키며, 인터페이스 표준화로 VC 스키마와 믹싱 알고리즘 확장 가능하며, 감사 로그는 CID-해시 연결로 추적성을 강화한다.

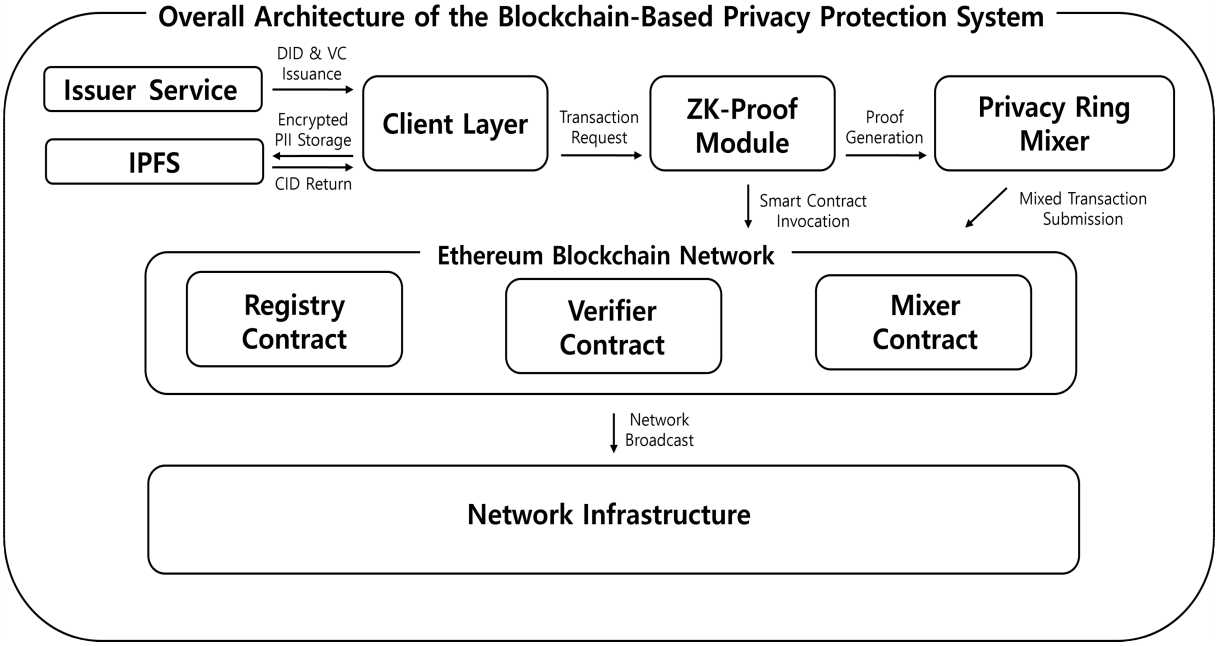

그림 1. 블록체인 기반 영지식 증명과 트랜잭션 믹서를 이용한 개인정보 보호 시스템 전체 아키텍처
Fig. 1. Overall architecture of the blockchain-based privacy protection system using zk-proof and transaction mixer

3.2 개인정보 등록 프로세스

사용자가 신원 정보를 생성·암호화하여 분산 저장하고, 이후 검증 요청에 대응할 수 있도록 준비하는 단계이다. 그림 2의 과정은 발급자, 사용자 지갑, IPFS, 트랜잭션 믹서, 스마트 컨트랙트, 블록체인 네트워크 간의 상호작용으로 구성된다. 우선 발급자는 사용자 기반의 키 쌍, DID, VC, Access Log 구조 등을 포함한 초기 지갑을 생성하여 사용자에게 전달한다. 사용자는 자신의 공개키를 기반으로 DID Document를 구성하고, 여기에 DID, VC, 공개키 등의 정보를 포함하여 하나의 사용자 정보 블록을 생성한다. 생성된 사용자 정보 블록은 사용자의 공개키로 암호화되며, 이름, 생년월일, 사진 등의 데이터는 IPFS에 저장된다. 이때 생성된 CID는 해당 정보의 고유 주소 역할을 하며, 이 또한 외부에서 직접 접근할 수 없도록 암호화되어 보호된다. 또한, 해당 CID는 이후 모든 검증 과정에서 참조 포인터 역할을 하여 데이터 일관성과 신뢰성을 유지한다.

이후 사용자는 해당 정보에 기반한 nullifier hash를 생성한 뒤, 이를 지갑에서 Mixer로 증명자의 정체와 제출 흐름을 은닉하여 스마트 컨트랙트에 제출하며, 스마트 컨트랙트는 이후에 증명 및 참조할 수 있도록 nullifier hash, CID hash, DID hash 등을 블록체인에 기록한다. 특히 지갑은 스마트 컨트랙트가 emit한 이벤트를 수신하되, 해당 이벤트에는 제출자의 주소나 식별자가 포함되지 않도록 설계되며, 지갑은 이벤트 내 nullifier 값을 자체적으로 보유한 리스트와 비교함으로써 자신이 제출한 증명 여부를 로컬에서만 판단한다. 이 과정은 외부에 데이터를 유출하지 않으며, 익명성을 보장하는 내에서 안전한 Access Log 인덱싱을 실현한다.

사용자의 지갑 내 Access Log 구성 요소로는 nullifier, CID, VC, 트랜잭션 등의 hash와 블록 번호, 타임스탬프 등이다. 이 메타데이터는 온체인 상태의 무결성 대응 관계를 확보하고, 추후 검증 요청에 대해 빠르고 정확한 참조가 가능하도록 지원한다.

이 구조는 사용자의 식별 정보와 검증 이력을 분리함으로써 프라이버시 보호와 무결성 보장을 동시에 실현하며, 개인정보의 등록, 참조, 증명 가능성, 비식별성, 위변조 방지 등의 요구사항을 포괄적으로 충족하는 설계로 기능한다.

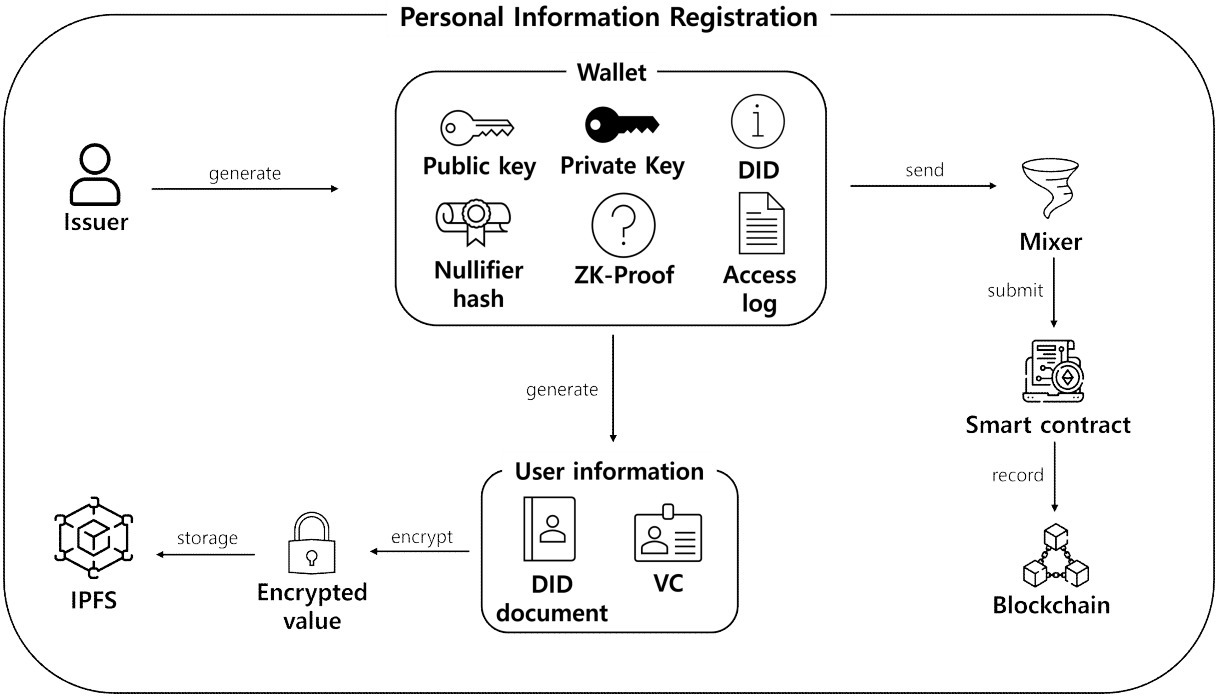

그림 2. 개인정보 등록 플로우차트
Fig. 2. Flowchart of personal information registration

3.3 검증자의 사용자 정보 조회 프로세스

기업 또는 기관이 사용자에게 속성 증명 또는 신원 정보 제공을 요청하고, 사용자가 이를 수락해 조건 기반 증명이나 VC 기반 응답을 생성·제출한다.

그림 3은 영지식 증명과 트랜잭션 믹서를 결합해 정보 내용뿐 아니라 요청자-사용자 간 관계까지 은닉하는 데 중점을 둔다. 검증자는 사용자에게 특정 속성 또는 신원 정보를 요청하며, 사용자는 수락 여부를 결정한다. 사용자가 수락하면 지갑은 DID, VC, 키 쌍 등으로 ZK-Proof와 nullifier hash를 생성한다.

ZK-Proof는 정보를 노출하지 않고 조건 충족을 증명하며, nullifier hash는 증명이 한 번만 사용되도록 하는 익명 토큰으로 작동한다. 증명은 검증자에 직접 전달되지 않고 먼저 믹서로 전송된다.

믹서는 해당 트랜잭션의 발신자·수신자 연결고리를 제거해 체인 추적 가능성을 차단한다. 이어 ZK-Proof와 nullifier hash를 스마트 컨트랙트에 제출한다. 스마트 컨트랙트는 온체인 정보로 증명 유효성을 검증하고, nullifier hash 중복 사용 여부를 확인한 후 블록체인에 증명 결과와 nullifier hash 상태를 기록한다. 이때 블록체인에는 조건 충족 여부만 남고, 실제 데이터나 발신자 정보는 기록되지 않는다.

검증자는 컨트랙트 출력을 통해 요청 성공 여부만 확인할 수 있다. 그러나 얼굴 사진 확인이 필요하면 IPFS 저장 사진을 복호화해 일회성 세션·엔드포인트로 1회 다운로드 가능한 형식으로 제공된다.

정보 접근은 Access Log로 로컬에 저장한다. Access Log에는 제출한 nullifier hash, 트랜잭션 해시, 블록 번호, 증명 종류 등이 포함되며, 외부에 게시되지 않고 지갑 내부에만 유지된다.

지갑은 컨트랙트 이벤트를 수신한 뒤 nullifier hash 리스트와 대조해 제출한 증명임을 식별하고 기록을 인덱싱한다. 이 과정은 사용자가 원하는 경우에만 검토·제시할 수 있게 설계된다. 이 구조는 DID 기반 인증 시스템의 한계였던 행위 추적성과 프라이버시 침해 문제를 해결하며, 온체인 데이터와 지갑 내 인덱스 간 무결성 연결을 유지한다. 또한 VC의 선택적 사용으로 보안 수준 조정이 가능해 사용자 주도적이고 비식별성을 보장하는 검증 구조를 제공한다.

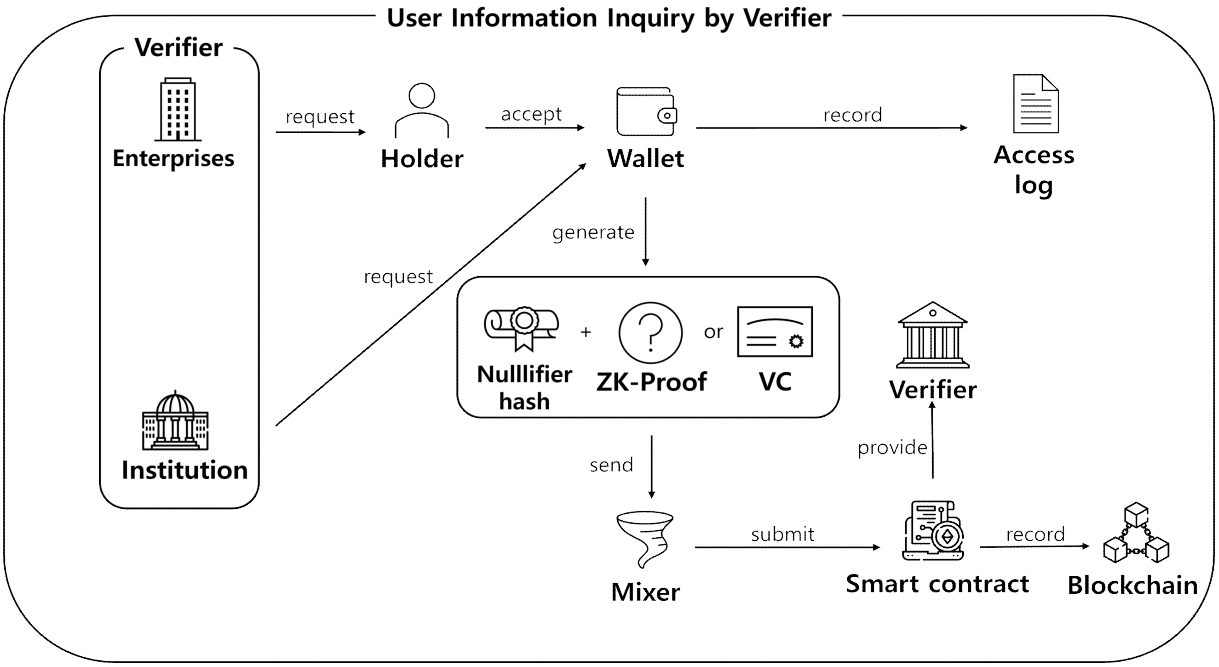

그림 3. 검증자의 사용자 정보 조회 플로우차트
Fig. 3. Flowchart of user information inquiry by verifier

3.4 스마트 컨트랙트 주요 함수

표 1의 코드는 snarkjs 도구를 사용해 자동 생성된 Verifier.sol의 스마트 컨트랙트 코드로, Groth16 방식의 zk-SNARK 증명을 온체인에서 검증하기 위한 구조를 담고 있다. 이 파일의 핵심 함수인 verifyProof는 생성된 세 개의 증명 요소(a, b, c)와 공개 입력을 받아 pairing 연산을 수행하며, 이를 통해 증명의 유효성을 판단한다. 내부적으로는 checkPairing, g1_mulAccC, checkField 등의 low-level 함수들이 계층적으로 호출되며, 이는 각각 필드 값의 유효성 검사, G1 그룹 상에서의 곱셈 누적 연산, pairing 조건의 만족 여부 판단이라는 역할을 수행한다. 특히 checkPairing 함수는 모든 pairing 결과가 일치하는지 검증하는 핵심 로직이며, g1_mulAccC는 누적된 곱연산을 효율적으로 처리해 불필요한 가스 소비를 줄인다. 이러한 로직은 EVM(Ethereum Virtual Machine) 상에서 inline assembly로 구현되어 있으며, 고정된 가스비 내에서 효율적으로 처리되도록 최적화되어 있다. Groth16 특유의 짧은 증명 크기와 빠른 검증 속도 덕분에 높은 신뢰성과 성능을 동시에 확보할 수 있다.

표 1. 영지식 증명 검증 함수
Table 1. Zero-knowledge proof verification functions

```
function verifyProof(
  uint[2] calldata _pA,
  uint[2][2] calldata _pB,
  uint[2] calldata _pC,
  uint[1] calldata _pubSignals
) public view returns (bool)

function checkPairing(
  pA, pB, pC, pubSignals, pMem
) -> isOk

function g1_mulAccC(pR, x, y, s)

function checkField(v)
```

표 2의 AgeVerifier 컨트랙트는 나이 증명을 수행하기 위해 Verifier.sol을 래핑한 컴포넌트다. 생성자에서 전달된 주소로 verifier 인스턴스를 설정하고, mapping(bytes32 => bool) public usedNullifiers를 통해 제출된 pi 증명의 nullifier 중복 여부를 추적한다. submitProof는 pi_a, pi_b, pi_c, public signal, nullifier를 받아 nullifier 미사용 여부를 require로 확인하고, verifier.verifyProof(view)로 on-chain 페어링 검증을 수행하며, 검증식의 결과를 판단한다. 검증 통과 시 null

ifier를 true로 기록하고, emit Verified (msg.sender,n)을 호출해 클라이언트가 indexed 로그를 통해 결과를 확인할 수 있도록 한다. 고정 길이 배열 시그니처는 ABI(Application Binary Interface) 안정성을 높이고, memory 사용으로 가스 소모를 줄였다. 또한 event 파라미터에 indexed를 적용해 로그 검색 효율을 높였으며, 오류 문구를 간결화해 revert 가스 비용을 최소화했다.

표 2. 나이 검증용 영지식 증명 컨트랙트 주요 함수
Table 2. Key functions of the age proof smart contract

```
contract AgeVerifier{
    Verifier public verifier;
    mapping(bytes32=>bool) public usedNullifiers;
    event Verified(address relayer,bytes32 n);
    constructor(address v){verifier=Verifier(v);}
    function submitProof(
        uint[2] memory a,uint[2][2] memory b,
        uint[2] memory c,uint[1] memory s,
        bytes32 n) public{
            require(!usedNullifiers[n],"Nullifier");
            require(verifier.verifyProof(a,b,c,s),"");
            usedNullifiers[n]=true;
            emit Verified(msg.sender,n);
}       }
```

3.5 트랜잭션 믹서를 통한 프라이버시 보호

트랜잭션 믹서를 활용하여 블록체인 상에서 트랜잭션 간의 링크성을 효과적으로 은닉하는 프라이버시 보호 방안을 제안한다. 기존 블록체인 시스템은 모든 트랜잭션의 입력과 출력이 공개되어, 외부 분석자가 송신자와 수신자 간의 관계를 추적할 수 있는 구조적 한계를 지닌다[10]. 이를 극복하기 위해 영지식 증명(ZK-Proof), 링 시그니처(Ring signature), 스텔스 주소(Stealth address)[11], 그리고 nullifier 구조를 통합한 Privacy Ring Mixer를 설계하였다.

믹서는 익명성 집합을 구성하고, 링 시그니처를 통해 송신자 신원을 은닉한다. 각 전송 시에는 스텔스 주소를 생성하여 수신자의 실제 지갑과의 연결고리를 차단하며, nullifier를 활용해 동일 증명의 재사용을 방지한다. 이러한 구조는 Circom 기반의 ZK 회로와 Solidity 스마트컨트랙트로 구현되며, 대규모 익명성 집합까지 확장 가능하다. 특히, 이 시스템은 트랜잭션의 내용뿐만 아니라 송수신자 간의 관계 자체를 체인 상에서 식별 불가능하게 하여, 기존 단일 트랜잭션 기반 시스템 대비 프라이버시 보호 수준을 크게 향상시킨다.

사용자는 자신의 프라이버시 요구 수준에 따라 익명성 집합의 크기를 유연하게 선택할 수 있어, 실질적 프라이버시-비용 균형을 달성할 수 있다. 이러한 설계는 시스템의 실용성과 확장성을 동시에 확보한다[12].

Ⅳ. 실험 및 평가

이 장에서는 논문에서 제안하는 연구에 사용된 기술 스택과 실험 과정 및 결과물에 대한 분석에 대해 다루고 설명한다. 실험 결과에 대한 분류는 영지식 증명과 트랜잭션 믹싱으로 나누어 설명한다.

4.1 실험 환경

표 3은 실험 환경으로 Ubuntu 22.04.4 환경에서 Node.js 18.20.8 및 Express 5.1.0을 사용하였다. 스마트 컨트랙트는 Solidity 0.8.20으로 작성하고 Truffle 5.11.5를 통해 컴파일 및 배포하였다. Circom 2.1.6과 Snarkjs 0.7.5로 Groth16 기반 zk-SNARK 증명을 생성하였으며, 증명 생성은 백엔드에서 자동화되었다. 트랜잭션 믹싱 실험은 Ethers.js 6.15.0과 Web3.js 4.16.0에서 실행되었고, 실험에 사용된 네트워크 환경은 Ethereum Sepolia와 MetaMask로 수행하였다.

표 3. 실험 환경
Table 3. Experimental environment

Operating system	WSL2 (Ubuntu 22.04.4)
Runtime	Node.js 18.20.8
Framework	Express 5.1.0
Compiler	Truffle 5.11.5
Smart contract	Solidity 0.8.20
Platform	Ethereum Sepolia
Wallet	MetaMask
Client API	Web3.js 4.16.0
	Ethers.js 6.15.0
ZK tool	Circom 2.1.6
	Snarkjs 0.7.5
ZK protocol	Groth16

4.2 사용자 입력 기반 zk-SNARK 증명 결과

표 4는 사용자의 입력값(나이 속성)에 대한 증명 결과를 나타낸다. Groth16 알고리즘은 증명 생성 시 회로 제약식의 1차, 2차, 3차 항에 해당하는 세 개의 곡선점 pi_a, pi_b, pi_c를 출력하며, 이 값들은 zk-SNARK의 핵심 산출물이다.

$$e(\pi_a, \pi_b) = e(\alpha, \beta) \times e(vk_y + \sum(public_i \times vk_{\gamma, ABC_i}), \gamma) \times e(\pi_c, \delta) \quad (1)$$

$public_i$는 회로가 외부에 노출하는 공개 신호로, 본 시스템에서는 "19세 이상" 조건을 나타낸다. vk_{γ, ABC_i}는 각 공개 입력에 대응하는 γ계수이며, vk_y는 공개 입력과 결합되는 전역 상수다. $e()$는 서로 다른 두 곡선 그룹의 점을 곱해 세 번째 그룹의 점을 도출하는 비선형 페어링 함수이다. 컨트랙트는 증명 검증 시, 회로 컴파일 과정에서 미리 생성된 검증키 $\alpha, \beta, \gamma, \delta$와 함께 π_a, π_b, π_c를 입력으로 받아 식 1의 페어링 등식이 성립하는지를 판단한다[13]. 이 등식이 성립하면 증명은 유효한 것으로 간주되며, 이를 통해 스마트컨트랙트는 사용자의 비공개 입력 없이도 “제출된 값이 회로 조건을 만족하는가?”를 판정할 수 있다. 이때 ‘public[0]’은 회로의 외부 출력으로, “19세 이상” 조건을 만족하면 1, 아니면 0으로 설정된다. protocol과 curve는 각각 사용된 SNARK 체계(Groth16)와 타원곡선 종류를 뜻하며, bn128은 이더리움이 네이티브로 지원하는 Barreto-Naehrig 128-bit 보안 곡선이다. 또한 nullifier는 회로 내부에서 Poseidon(secret ‖ salt) 해시로 생성된 32바이트 무작위 값으로, 동일 증명의 재사용을 방지하기 위해 스마트컨트랙트에 기록된다. 사용자는 이 nullifier와 함께 Poseidon(secret, nullifier) 형태의 커밋먼트를 Merkle Tree의 leaf로 제출해 증명이 특정 트리에 포함되었음을 입증하고 후속 증명에 활용할 수 있다. 이러한 구조는 pi_a, pi_b, pi_c가 수학적 정확성을, public이 논리 조건을, nullifier가 단일성과 익명성을 담당함으로써, 사용자는 개인 정보를 노출하지 않고도 조건 충족 여부만을 안전하게 증명할 수 있다.

표 4. 사용자 입력 기반 zk-SNARK 증명 결과
Table 4. zk-SNARK Proof Results Based on User Input


```
{
  "proof": {
        "pi_a": [
                "5455…", "1686…", "1"
              ],
        "pi_b": [
              [ "5412…", "1227…"  ],
              [ "2103…", "1535…"  ],
              [ "1", "0"  ]
              ],
        "pi_c": [
                "1935…", "2161…", "1"
              ],
        "protocol":  "groth16",
        "curve":  "bn128"
          },
  "public": [ "1"  ],
  "nullifier": "28602e56…"
}
```


4.3 Privacy Ring Mixer를 이용한 트랜잭션 믹싱 실험 결과

그림 4는 익명 집합 크기에 따른 프라이버시 방어율의 증가 패턴을 정량화한다. 2지갑 링에서 60%로 시작한 방어율은 지갑 수 증가와 함께 점진적으로 상승하여 50지갑에서 95%에 도달한다. 특히 n = 10 구간(66.4%)부터 실질적 보호 효과가 나타나며, n ≥ 25 구간에서는 증가율이 둔화되는 체감 효용 패턴을 보인다. 이는 Defense Rate = 60 + (n-2) × 0.8 공식으로 모델링되며, 계정 모델 기반 믹서에서도 링 크기 스케일링을 통한 선형적 프라이버시 향상이 가능함을 입증한다.

실험에서 관찰된 포화곡선 형태는 "공격자가 추가 외부 정보를 갖지 못한다"는 가정 하에서 지갑 간 독립성이 유지될 때의 이론적 한계를 반영한다. 또한 역익명화 확률 P_deanon = 1/n이 지갑 수에 반비례하여 감소하는 것은 Shannon의 정보 이론[14]과 일치하며, 엔트로피 증가에 따른 불확실성 확장 효과를 보여준다. ZK 증명 생성 시간과 가스 비용을 종합 고려할 때, 30-40지갑 구간이 방어율 향상과 운영 비용 사이의 최적 균형점으로 분석되며, 이는 중·대형 믹싱 풀의 연속 운영 전략이 가장 실용적임을 시사한다.

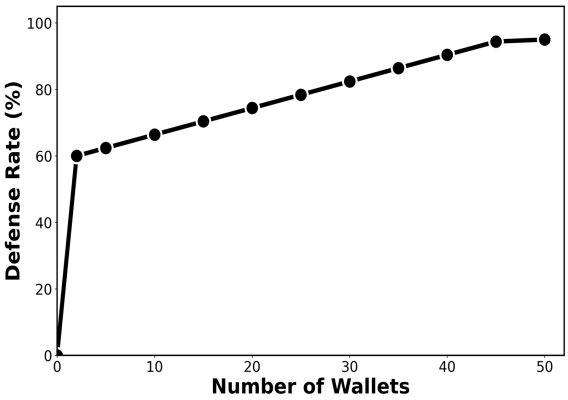

그림 4. 지갑 수에 따른 프라이버시 방어율
Fig. 4. Privacy defense rate by wallet count

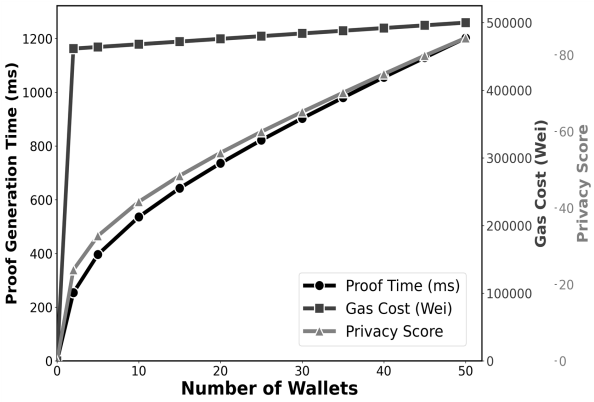

그림 5. 증명 시간 대비 가스비 효율성
Fig. 5. Proof time vs gas cost efficiency

그림 5는 증명 생성 시간, 가스비, 프라이버시 점수의 trade-off를 시각화한다. Privacy Score = min(40, n×0.8) + min(30, $\log_2$ (n)×5) + max(10, 30-gas/50000)는 링 크기, 엔트로피, 가스 효율성을 종합한다. 이 산정식의 가중치와 임계값은 실험 데이터와 Shannon 엔트로피 기반 불확실성 모델을 참고하여, 프라이버시·비용·성능 균형점을 반영하도록 설정하였다.

30회 반복 실험한 결과 Sepolia 테스트넷 기준, 평균적으로 증명 시간(흑색)은 254ms(2지갑, 송·수신 지갑만 포함)에서 1202ms(50지갑)까지 선형 증가하고, 가스 비용(진회색)은 461→500kWei로 완만히 상승한다. 프라이버시 스코어(회색)는 23.8점에서 84.4점까지 로그 곡선으로 증가한다.

Groth16 알고리즘의 O(n log n) 복잡도 특성으로 인해 지갑 수 증가 시 증명 시간이 점진적으로 증가하며, alt_bn128 곡선의 페어링 연산 비용이 가스비 상승 요인으로 작용한다. 특히 링 크기별 공개키 검증과 nullifier 생성 과정에서 Poseidon 해시 연산이 누적되어 전체 증명 시간에 기여한다.

시작 구간인 n = 2~10 구간에서는 증명 시간이 급증(254→536ms)하지만 프라이버시 스코어가 현저히 향상되며(23.8→41.6점), n ≥ 25부터는 증가율이 둔화된다. 이는 익명성 집합 크기에 따른 정보 이론적 엔트로피 한계와 일치하며, 체인 분석 공격에 대한 방어 효과가 포화 구간에 도달함을 의미한다. 30~40지갑 구간에서 증명 시간 903~1056ms, 가스 484~492kWei, 스코어 65~75점을 기록하여 성능 대비 효율성 균형점을 형성하며, 실용적 믹서 운영의 최적 파라미터를 제시한다.

Ⅴ. 결론 및 향후 과제

본 논문에서는 zk-SNARK 기반의 암호학적 증명 시스템과 Privacy Ring Mixer를 결합하여 블록체인 거래의 프라이버시를 강화하는 새로운 은닉 구조를 제안하였다. 제안된 기법은 거래 시 발신자와 수신자 간의 연계를 차단하여 거래 추적을 어렵게 만들고, 동시에 zk-SNARK 증명을 통해 거래의 무결성을 보장한다. 이러한 구조를 이더리움 기반 Sepolia 테스트넷에서 최대 50개의 지갑을 혼합한 환경으로 구현하여 그 효과를 검증하였다. 실험 결과 제안 기법은 실시간 처리 요구를 충족하면서도 거래 프라이버시를 향상시킬 수 있음을 확인하였다.

본 연구의 의의는 zk-SNARK의 암호학적 증명 능력과 링 믹서의 익명화 기법을 융합함으로써 기존 단일 기술 접근법의 한계를 극복했다는 점에 있다. 통합된 프라이버시 보호 기법을 통해 거래 은닉성과 프라이버시 방어율이 향상되었으며, 특히 기존의 한 가지 기술만 사용했을 때보다 약 15% 더 높은 프라이버시 방어율을 달성하면서도 가스 비용 증가는 3~5% 수준에 그쳤다. 이는 프라이버시 보호와 시스템 효율성 간 균형을 유지하면서도 강력한 익명성 보장을 제공할 수 있음을 의미한다. 아울러 실용적 프라이버시 보호 모델을 제시함으로써 블록체인 보안 연구 분야에 기여할 것으로 기대된다. 특히 프라이버시와 성능을 동시에 향상시킬 수 있는 새로운 해결책을 제시했다는 점에서 본 연구의 의의가 크다.

실험을 통한 정량적 평가에서도 제안 기법의 성

능이 입증되었다. Sepolia 테스트넷에서 혼합 지갑 개수를 단계적으로 늘려가며 측정한 결과, 증명 생성 시간은 평균 약 1202ms에 불과했고 가스 비용도 최대 약 6.9×10^5 Wei 수준으로 나타나 실시간 처리에 무리가 없는 것으로 확인되었다. 또한 Privacy Score는 23.8점에서 최대 84.4점까지 상승하였으며 프라이버시 방어율은 최고 95%에 달해 익명성 향상을 수치로 입증하였다. 특히 약 30~40개의 지갑을 혼합하는 구간에서 시간 지연과 가스 비용 대비 프라이버시 향상의 효율이 가장 높아 해당 범위가 최적의 운영 조건으로 도출되었다. 이러한 실험 결과와 방어율 및 증명 시간에 대한 그래프 분석을 통해 제안 기법의 실용성과 높은 성능을 동시에 확인할 수 있었다.

향후 연구에서는 시스템의 효율성을 높이기 위하여 사용자 거래 특성에 따라 수수료를 탄력적으로 조정하는 동적 수수료 모델의 도입, 운영 환경에 맞춘 믹싱 풀 크기의 가변적 운영, 증명 데이터 크기 최적화를 통한 처리 효율 향상, OAuth 연동을 통한 외부 인증 통합 등의 개선 방안을 검토하고 있다. 이러한 기능 확장을 통해 제안 기법이 다양한 블록체인 환경에서 더욱 효율적으로 동작함으로써 실용성을 한층 강화할 수 있을 것으로 기대된다.

나아가 제안한 기법은 금융 사기 방지, 탈중앙화 신원관리(DID), 의료 정보 접근 통제, zk-email 등 다양한 실생활 분야에도 확장 및 응용이 가능하며, 이는 다양한 디지털 서비스에서 개인정보 보호를 강화하는 핵심 기술이 될 수 있음을 시사한다.

References

[1] IBM, "Cost of a Data Breach Report 2024", IBM, Jul. 2024. https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf. [accessed: May 15, 2025]

[2] W3C, "Verifiable Credentials Data Model 1.0", World Wide Web Consortium (W3C), May 2022. https://www.w3.org/TR/vc-data-model/. [accessed: May 15, 2025].

[3] L. Hendrickson, "The Impact of Blockchain on Data Privacy", Identity.com, Feb. 2025. https://www.identity.com/impact-of-blockchain-on-data-privacy/. [accessed: Aug. 11, 2025].

[4] Dock, "Zero-Knowledge Proofs: A Beginner's Guide", Jul. 2025. https://www.dock.io/post/zero-knowledge-proofs [accessed: Aug. 11, 2025].

[5] J. Li, C. Zhang, J. Zhang, and Y. Shao, "Research on Blockchain Transaction Privacy Protection Methods Based on Deep Learning", Future Internet, Vol. 16, No. 4, Mar. 2024. https://doi.org/10.3390/fi16040113.

[6] S. Lohar, S. D. Babar, and P. N. Mahalle, "A Self-Sovereign Identity Framework for Context-Aware De-Centralized Identifier Creation and Credential Verification", Engineered Science, Vol. 36, No. 1629, Jul. 2025. https://dx.doi.org/10.30919/es1629.

[7] S. Jeong and H. Jung, "Design of Blockchain based Digital Badge Framework for Reliable Career Verification", Journal of The Korea Institute of Information Technology, Vol. 20, No. 9, pp. 147-153, Sep. 2022. https://doi.org/10.14801/jkiit.2022.20.9.147.

[8] J. Lee, J. Hwang, H. Oh, and J. Kim, "Personal Information Management System with Blockchain Using zk-SNARK", Journal of The Korea Institute of Information Security & Cryptology, Vol. 29, No. 2, pp. 299-308, Apr. 2019. https://doi.org/10.13089/JKIISC.2019.29.2.299.

[9] S. Lohar, S. D. Babar, and P. N. Mahalle, "Decentralization of Identity using Ethereum and IPFS", Communications on Applied Nonlinear Analysis, Vol. 31, No. 4s, pp. 378-391, Jun. 2024. https://doi.org/10.52783/cana.v31.917.

[10] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Oct. 2008.

[11] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "P2P Mixing and Unlinkable Bitcoin Transactions", Network and Distributed System Security Symposium (NDSS), pp. 1-15, Feb. 2017. https://doi.org/10.14722/ndss.2017.23415.

[12] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of Clients in Bitcoin P2P Network", 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale Arizona USA, pp. 15-29, Nov. 2014. https://doi.org/10.1145/2660267.2660379.

[13] J. Groth, "On the Size of Pairing-Based Non-interactive Arguments", 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), Vienna, Austria, pp. 305-326, May. 2016. https://doi.org/10.1007/978-3-662-49896-5_11.

[14] C. E. Shannon, "A Mathematical Theory of Communication", Bell System Technical Journal, Vol. 27, No. 3, pp. 379-423, Jul. 1948. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

저자소개

윤 영 준 (Youngjoon Yoon)

2022년 3월 ~ 현재 : 국립군산대학교 소프트웨어학과 학사과정

관심분야 : LLM, 서버, 웹, 블록체인

정 현 준 (Hyunjun Jung)

2008년 3월 : 삼육대학교 컴퓨터과학과(공학사)

2010년 3월 : 숭실대학교 컴퓨터학과(공학석사)

2017년 9월 : 고려대학교 컴퓨터·전파통신공학과(공학박사)

2017년 8월 ~ 2020년 8월 : 광주과학기술원 블록체인인터넷경제연구센터 연구원

2021년 3월 ~ 현재 : 국립군산대학교 소프트웨어학과 교수

관심분야 : 블록체인, 데이터 사이언스, 센서 네트워크, 사물인터넷, 머신러닝