사물인터넷융복합논문지 Vol. 12, No. 4, pp. 45-51, 2026 https://doi.org/10.20465/KIOTS.2026.12.4.045

분산 시스템에서 분산 신원 증명과 영지식 증명을 활용한 프라이버시 보호 다중 인증 기법

홍성혁*
백석대학교 첨단IT학부 교수

Privacy-Preserving Multi-Factor Authentication Using Decentralized Identity and Zero-Knowledge Proof for Distributed Systems

Sunghyuck Hong*
Professor, Division of Advanced IT, Baekseok University

요 약 본 논문은 분산 신원 증명(DID)과 영지식 증명(ZKP)을 통합한 프라이버시 보호 다중 인증 프레임워크 DID-ZKP-MFA를 제안한다. DID 기반 신원 등록, ZKP 선택적 공개, 동적 challenge-response를 결합하고 Pedersen commitment, fuzzy extractor 및 Groth16 회로를 적용하였다. 22,450개 제약 조건의 프로토타입을 100회 측정한 결과 모바일 종단간 인증 시간은 평균 164.8ms이고 세션당 통신량은 1,428바이트였다. 제안 방식은 인증정보 노출을 줄이지만 고정 DID 환경의 완전한 세션 비연결성을 위해 pairwise DID 또는 세션별 가명 식별자가 필요하다.

주제어 : 분산 신원 증명, 다중 인증, 영지식 증명, 프라이버시 보호 인증, 블록체인, 사물인터넷

Abstract This paper proposes DID-ZKP-MFA, a privacy-preserving multi-factor authentication framework integrating decentralized identity and zero-knowledge proofs. The protocol combines DID-based registration, ZKP-based selective disclosure, and dynamic challenge-response. Its security is analyzed using Pedersen commitments, fuzzy extractors, Groth16, and the UC framework. In 100 prototype runs, mobile end-to-end authentication averaged 164.8 ms with 1,428 bytes per session. The design protects credentials and proof transcripts; identifier-level unlinkability additionally requires pairwise DIDs or session-specific pseudonyms.

Key Words : decentralized identity, MFA, zero-knowledge proof, privacy-preserving authentication, blockchain, IoT

1. 서론

디지털 서비스의 확산과 함께 사용자 자격증명 탈취, 피싱 및 서버 침해에 대응할 수 있는 강력한 인증 메커니즘의 필요성이 증가하고 있다. 기존 아이디·패스워드 방식은 단일 자격증명에 의존하므로 하나의 비밀정보가 노출될 경우 전체 인증이 무력화될 수 있다.

IoT·모바일·클라우드 서비스가 연계되는 분산 환경에서는 서비스마다 분리된 자격증명 저장소를 운영하지 않으면서도 검증에 필요한 최소 정보만 공개하는 인증 구조가 요구된다.

블록체인 기반 분산 신원 증명(DID)[1, 2]은 분산 원장에 신원 주장을 등록함으로써 중앙화 문제를 해결하고, 검증 중 신뢰할 수 있는 제3자의 필요성을 제거한다.

이 연구는 2026학년도 백석대학교 대학연구비 지원에 의하여 이루어졌음.
*교신저자 : 홍성혁(shong@bu.ac.kr)
접수일 2026년 06월 04일 수정일 2026년 08월 15일 심사완료일 2026년 08월 18일

W3C는 2022년 DID 명세를 표준화하여 상호운용 가능한 자기 주권 신원 시스템의 기반을 마련하였다. 그러나 기존 DID 기반 인증 기법은 검증 단계에서 생체 정보 등 자격증명 내용을 평문으로 전송하여 비연결성 위반 문제를 야기한다.

주요 기여로는 (1) 세 단계 인증 프레임워크 제안, (2) UC 프레임워크 기반 공식 보안 증명, (3) 22,450개 제약조건의 ZKP 회로 설계·구현, (4) 데스크톱·모바일 프로토타입 평가, (5) 기존 5개 기법과의 8가지 보안 속성 비교 분석이 있다.

2. 관련연구

2.1 블록체인 기반 인증

블록체인 기술은 신원 관리의 신뢰 앵커로서 광범위하게 연구되어 왔다. Mun[4]은 생체 정보와 OTP를 블록체인과 결합하여 재전송 공격에 대한 저항성을 개선하였으나, 생체 정보 템플릿을 해시 형태로 온체인에 저장하여 세션 간 상관 정보가 노출되는 문제가 있다. Kim 등[5]은 DID와 무작위 인증 방법·단말 선택을 결합한 MFA 기법을 제안하였으며, 본 연구는 이를 ZKP 기반 선택적 공개와 UC 보안 증명으로 확장한다.

Zhao 등[6]은 ZKP, 스마트 컨트랙트, 머클 해시 트리를 통합한 차량 인터넷용 블록체인 기반 크로스 도메인 인증 기법 CAIoV를 제안하였으나, 생체 인증 요소와 DID 기반 신원을 지원하지 않는다. Pathak 등[7]은 IoT용 블록체인 강화 ZKP 상호 인증 프로토콜 Z-PMA를 제안하여 인증 시간을 37% 단축하였다. Rivera 등[8]은 ZKP를 MFA와 제로 트러스트 아키텍처에 통합하였으나 생체 인증 요소와 공식 보안 증명이 부재하다.

2.2 분산 신원 증명 및 연구 공백

분산 식별자(DID)[1]는 중앙 등록 기관 없이 검증 가능한 분산 디지털 신원을 가능하게 한다. Bernabé Murcia 등[9]은 SSI와 ZKP를 결합한 제로 트러스트 다중 도메인 분산 신원 관리 솔루션을 제안하였고, He 등[10]은 BBS+ 서명과 동적 누산기 기반의 감독 가능·취소 가능 분산 신원 기법을 제안하였다. 기존 연구를 분석한 결과, DID 기반 자격증명·ZKP 기반 생체 정보 보호·UC 공식 증명을 동시에 달성한 기법은 존재하지 않는다.

〈Table 1〉 Security-property coverage of related studies

Study	DID	ZKP	Biometric	MFA	Formal proof	Unlinkability
Mun [4]	No	No	Yes	Yes	No	No
Kim et al. [5]	Yes	No	Yes	Yes	No	No
Zhao et al. [6]	No	Yes	No	No	No	Yes
Pathak et al. [7]	No	Yes	No	No	No	Yes
Rivera et al. [8]	Yes	Yes	No	Yes	No	Yes
He et al. [10]	Yes	Yes	No	No	No	Yes
Proposed	Yes	Yes	Yes	Yes	Yes	Conditional

3. 암호학적 기반

3.1 분산 식별자와 검증 가능 자격증명

DID는 did:method:identifier 형태의 URI이며, 각 DID는 공개 키, 인증 관계, 서비스 엔드포인트를 포함하는 DID 문서로 해석된다. 검증 가능 자격증명은 다음과 같이 정의된다:

VC = (id, issuer, subject, claims, expiry, σ_issuer) (정의 1)

여기서 σ_issuer = Sign(sk_issuer, H(id ‖ issuer ‖ subject ‖ claims ‖ expiry))이다. 검증 가능 프레젠테이션(VP)은 소유자가 하나 이상의 VC를 패키징하여 검증자에게 제출하는 구조이며, 기존 VP 제출에서는 모든 자격증명 내용이 검증자에게 노출되어 본 연구가 해결하고자 하는 프라이버시 유출 문제가 발생한다.

3.2 커밋먼트 스킴

커밋먼트 스킴 (Commit, Open)은 두 알고리즘으로 구성된다. Commit(m, r) → c는 메시지 m과 난수 r을 취하여 커밋먼트 c를 생성하고, Open(c, m, r) → {0,1}은 c가 (m,r)로부터 생성되었는지 검증한다. 안전한 커밋먼트 스킴은 다음 두 속성을 만족한다:

- 은닉성(Hiding): 임의의 m_0, m_1에 대해 $\{c : c \leftarrow Commit(m_0,r)\} \approx_c \{c : c \leftarrow Commit(m_1,r)\}$
- 결합성(Binding): $m \neq m'$이면서 Commit(m,r) = Commit(m',r')인 (m,r,m',r')을 찾기 계산적으로 불가능

본 논문에서는 소수 위수 타원 곡선 군에 대한 페더슨 커밋먼트를 사용한다:

$Commit(m,r) = mG + rH$ (수식 1)

여기서 G, H는 독립적인 생성원이다.

3.3 퍼지 추출기

퍼지 추출기 (Gen, Rep)[11]는 생체 측정의 노이즈를 처리한다. Gen(b) → (K, P)는 생체 샘플 b를 입력으로 받아 키 K ∈ {0,1}^ℓ과 공개 보조 문자열 P를 출력한다. Rep(b', P) → K는 해밍 거리 δ 이내의 신선한 생체 샘플 b'와 P를 입력으로 동일한 키 K를 재현한다. 보안 보장은 다음과 같이 형식화된다:

∀b' : d_H(b', b) ≤ δ ⇒ Rep(b', P) = K (수식 2)

P가 주어진 경우에도 K가 균일 분포와 계산상 구별 불가능하다:

Δ(K ; U_ℓ | P) ≤ ε (수식 3)

여기서 Δ는 통계적 거리, U_ℓ은 균일 분포, ε은 무시 가능한 오류 확률이다. 본 기법에서는 이진화된 얼굴 임베딩에 대한 BCH 코드 기반 해밍 거리 보안 스케치를 사용하여 256비트 안정 키 K_bio와 공개 보조 문자열 P_bio를 생성한다.

3.4 zk-SNARK와 Groth16

관계 R = {(x, w) : C(x, w) = 1}에 대한 ZKP 시스템은 (Setup, Prove, Verify) 알고리즘의 튜플이며, 다음 세 속성을 만족한다:

- 완전성(Completeness): 임의의 (x,w)∈R에 대해

Pr[Verify(CRS, x, π)=1 | π ← Prove(CRS, x, w)] = 1 (수식 4)

- 건전성(Soundness): x ∉ L_R이면 임의의 PPT 공격자 A에 대해

Pr[Verify(CRS, x, A(CRS, x))=1] ≤ negl(λ) (수식 5)

- 영지식성(Zero-Knowledge): PPT 시뮬레이터 S가 존재하여

|Pr[D(π)=1] − Pr[D(S(CRS,x))=1]| ≤ negl(λ) (수식 6)

Groth16 구성[3]은 BN254 곡선에 대해 정확히 세 개의 군 원소(약 200바이트)의 증명을 생성하며, 검증은 세 번의 페어링 연산만을 요구한다. ZKP 회로 C(x,w)=1은 다음 네 제약 조건이 모두 만족될 때 성립한다:

Verify_pk_I (VC, σ_issuer) = 1 (수식 7)

Open(c_bio, K_bio, r) = 1 (수식 8)

d_H(K_bio, K_enroll) ≤ τ (수식 9)

H(sk_U ∥ ch ∥ tid) = resp (수식 10)

여기서 τ는 생체 매칭 임계값, H는 ZKP 친화적 해시 함수(Poseidon), c_bio는 DID 문서에 저장된 K_bio의 페더슨 커밋먼트이다.

3.5 UC 프레임워크

UC(Universal Composability) 프레임워크[12]는 실제 세계 프로토콜 실행과 이상적 기능 F를 비교하여 보안을 모델링한다. 프로토콜 Π가 F를 UC-실현한다는 것은, 모든 PPT 실제 세계 공격자 A에 대해 PPT 이상적 세계 시뮬레이터 S가 존재하여 모든 PPT 환경 Z에 대해 다음이 성립함을 의미한다:

|Pr[REAL_{Π,A,Z}=1] − Pr[IDEAL_{F,S,Z}=1]| ≤ negl(λ) (수식 11)

이상적 인증 기능 F_Auth는 (1) 검증자로부터 증명 요청을 수신하고, (2) 증명자가 주장된 DID에 발급된 유효한 VC를 보유하는지 조회하며, (3) 자격증명이 유효하고 생체 검증이 통과된 경우에만 검증자에게 ⊤을 출력하고, (4) 증명자의 속성, 생체 정보, 개인 키에 대한 어떠한 정보도 검증자에게 출력하지 않는다.

4. 제안 DID-ZKP-MFA 아키텍처

4.1 시스템 모델 및 위협 모델

제안 시스템은 (1) 신원 소유자 U, (2) 발급자 I, (3) 검증자 V, (4) DID 원장 L의 네 주체로 구성된다. 위협 모델: 원장 L은 변조 불가능하고 공개적으로 읽기 가능하다. 발급자 I는 자격증명을 올바르게 발급하지만 V와 공모할 수 있다. 검증자 V는 정직하지만 호기심이 있어 U에 관한 추가 정보를 학습하려 할 수 있다. 네트워크는 메시지를 도청·재전송·수정할 수 있는 Dolev-Yao 공격자에 의해 제어된다.

4.2 1단계: 신원 등록

신원 등록 단계는 사용자의 생체 정보 템플릿과 DID 간의 암호학적 연결을 확립한다. 구체적 절차는 다음과 같다:

(단계 1) U는 키 쌍 (pk_U, sk_U) ← KeyGen(1^λ)을 생성하고 DID 문서를 원장 L에 등록한다:

DIDDoc = {pk_U, cbio, serviceEndpoint} (수식 12)

(단계 2) U는 생체 데이터 b를 캡처하고 퍼지 추출기로 안정 키를 도출한다:

(K_bio, P_bio) ← Gen(b) (수식 13)

(단계 3) 임시 난수 r에 대해 커밋먼트를 계산하여 발급자에게 전송한다:

c_bio = Commit(K_bio, r) = K_bio·G + r·H (수식 14)

(단계 4) 발급자 I는 신원 확인 후 서명된 VC를 발급한다:

σ_I = Sign(sk_I, H(DID_U ∥ claims)) (수식 15)

(단계 5) U는 (VC, K_bio, P_bio, r, sk_U)를 하드웨어 기반 신뢰 실행 환경(TEE)에 저장한다.

4.3 2단계: ZKP 기반 선택적 공개

검증자 V는 신선한 챌린지와 무작위 단말 식별자를 전송한다:

ch ← {0,1}^256, tid ← T (수식 16)

사용자 U는 신선한 생체 데이터를 캡처하고 퍼지 추출기를 실행한다:

K'_bio ← Rep(b', P_bio) (수식 17)

챌린지-응답 값을 계산한다:

resp = H(sk_U ∥ ch ∥ tid) (수식 18)

ZKP 공개 입력과 증인을 구성한다:

x = (DID_U, ch, tid, τ, c_bio, resp) (수식 19)

w = (K'_bio, r, sk_U, VC) (수식 20)

zk-SNARK 증명을 생성한다:

π ← Prove(CRS, x, w) (수식 21)

U는 (DID_U, x, π)만을 검증자에게 전달한다. 생체 키 K'_bio, 자격증명 내용, 커밋먼트 난수 r, 개인 키 sk_U는 전송되지 않는다.

4.4 3단계: 검증 및 서비스 접근

검증자 V는 원장 L에서 DID_U를 조회하여 pk_I와 c_bio를 포함한 DID 문서를 가져온다. 세 번의 페어링 연산으로 증명을 검증한다:

b ← Verify(CRS, x, π) (수식 22)

b=1이면 임시 세션 토큰을 발행한다:

tok = H(DID_U ∥ ch ∥ tid) (수식 23)

b=0이면 인증을 거부하며, 연속 3회 실패 시 단계적 인증을 시작하거나 계정을 일시 잠금할 수 있다.

4.5 ZKP 회로 설계

Groth16 회로 C는 Circom[13]으로 구현되며 네 개의 서브 회로로 구성된다. VC 서명 검증 서브 회로는 BabyJubjub 타원 곡선에 대한 EdDSA 서명을 검증하며 Poseidon 해시(57 제약 조건/호출)를 사용하여 3,457개의 산술 제약 조건을 요구한다. 퍼지 생체 매칭 서브 회로는 다음 해밍 거리 제약을 구현한다:

d_H(K'_bio, K_enroll) = Σ_i (K'_bio[i] XOR K_enroll[i]) ≤ τ (수식 24)

256비트 키와 임계값 τ=20에 대해 18,665개의 제약 조건을 요구한다.

〈Table 2〉 ZKP circuit constraint breakdown

Subcircuit	Constraints	Ratio (%)
VC signature verification	3,457	15.4
Biometric commitment opening	214	0.9
Fuzzy biometric matching	18,665	83.1
Challenge–response binding	114	0.5
Total	22,450	100.0

5. 보안 분석

5.1 보안 속성

제안 기법은 다음 8가지 보안·프라이버시 속성에 대해 분석된다: (P1) 인증 정확성, (P2) 건전성/사칭 저항성, (P3) 재전송 공격 저항성, (P4) 중간자 공격 저항성, (P5) 비연결성, (P6) 생체 정보 보호, (P7) 순방향 비밀성, (P8) 자격증명 프라이버시.

5.2 비공식 보안 논증

재전송 공격 저항성: 세션마다 신선한 챌린지 ch ← {0,1}^256을 사용한다. 이전 세션에서 캡처된 증명 π_old는 ch_new ≠ ch_old인 새 세션에서 공개 입력 x가 일치하지 않으므로 거부된다. 형식적으로 ch가 균일 분포에서 무작위로 샘플링되므로:

Pr[ch_new = ch_old] = 2^{-256} ≤ negl(λ) (수식 25)

중간자 공격 저항성: 무작위 단말 식별자 tid가 수식 10에서 챌린지-응답 검사를 통해 ZKP 공개 입력에 바인딩된다. tid' ≠ tid로 증명을 중계하는 공격자는 해시 함수 H의 충돌 저항성으로 인해 검증 실패를 초래한다:

Pr[H(sk_U∥ch∥tid')=resp] ≤ negl(λ) (수식 26)

증명·자격증명 비연결성: Groth16의 영지식 속성은 동일한 명제에 대한 증명 transcript가 증인의 생체 키·자격증명 속성·개인 키를 노출하지 않도록 보장한다. 그러나 기본 프로토콜의 공개 입력에 고정 DID_U가 포함되면 검증자는 동일한 DID_U를 기준으로 세션을 연결할 수 있다. 따라서 본 논문에서 비연결성은 (1) ZKP transcript와 비공개 자격증명 내용의 비연결성, 또는 (2) 서비스별 pairwise DID나 세션별 가명 식별자를 사용하는 확장 구성에서의 세션 비연결성을 의미한다. 고정 DID를 반복 공개하는 기본 구성은 식별자 수준의 완전한 비연결성을 제공하지 않는다.

생체 정보 보호: 원시 생체 정보 b와 키 K_bio는 전송되지 않으며, 공개되는 것은 c_bio = Commit(K_bio, r)뿐이다. 은닉성에 의해:

$$I(K_{bio} ; c_{bio}) = 0 \quad \text{(수식 27)}$$

여기서 I(·;·)는 상호 정보량이다.

5.3 UC 보안 정리

정리 1 (DID-ZKP-MFA의 조건부 UC-보안): Groth16의 지식 건전성과 영지식성[3], 페더슨 커밋먼트의 은닉성·결합성, 퍼지 추출기[11]의 보안, 서명 기법의 EUF-CMA 안전성 및 원장의 무결성을 가정하면, DID-ZKP-MFA는 (F_DID, F_ZKP, F_Ledger)-하이브리드 모델에서 이상적 인증 기능 F_Auth를 UC-실현한다. 이 정리는 인증 정확성·자격증명 프라이버시·재전송 저항성을 대상으로 하며, 식별자 수준의 비연결성은 pairwise DID 또는 세션별 가명 식별자를 추가로 가정한다.

증명 개요: H0를 실제 프로토콜 실행이라 하자. H1에서는 발급자 서명의 위조 성공 사건을 제거하며, EUF-CMA 안전성에 의해 H0와 H1의 차이는 무시 가능하다. H2에서는 페더슨 커밋먼트를 무작위 메시지의 커밋먼트로 교체하며 은닉성에 의해 구별 이점은 무시 가능하다. H3에서는 실제 Groth16 증명을 시뮬레이터가 생성한 증명으로 교체하며 영지식성에 의해 H2와 H3는 계산적으로 구별 불가능하다. 유효하지 않은 증인으로 검증을 통과하는 사건은 지식 건전성에 의해 무시 가능하다. 신선한 ch와 tid는 공개 입력에 결합되므로 이전 transcript의 재사용은 2^-256 이하의 확률을 제외하고 실패한다. 따라서 환경 Z가 실제 실행과 이상적 기능 F_Auth를 구별하는 이점은 각 가정의 무시 가능한 이점의 합으로 제한된다. 단, 고정 DID_U가 공개되는 경우 시뮬레이터도 동일한 공개 식별자를 노출하므로 본 정리는 식별자 수준의 비연결성을 주장하지 않는다.

5.4 보안 주장 범위와 한계

본 분석은 발급자 키, 사용자 단말의 TEE, 초기 CRS 생성과 허가형 원장의 합의 가정이 안전하다는 조건에 의존한다. 생체 퍼지 추출기의 실제 오류율과 템플릿 노화, 단말 탈취, 사이드채널, 발급자·검증자 공모에 의한 메타데이터 상관분석은 본 프로토타입 평가 범위에 포함되지 않는다. 또한 고정 DID를 공개하는 기본 구성에서는 검증자가 세션을 식별자 수준에서 연결할 수 있으므로, 강한 세션 비연결성이 필요한 응용에서는 pairwise DID, 주기적 DID 회전 또는 세션별 가명 식별자를 사용해야 한다.

〈Table 3〉 Detailed comparison of security properties

Scheme	P1	P2	P3	P4	P5	P6	P7	P8
Kim et al. [5]	Yes	Yes	Yes	Yes	No	No	No	No
Mun [4]	Yes	Yes	Yes	No	No	No	No	No
Pathak et al. [7]	Yes	Yes	Yes	Yes	Yes	No	No	No
Rivera et al. [8]	Yes	Yes	Yes	Yes	Yes	No	No	Yes
He et al. [10]	Yes	Yes	Yes	No	Yes	No	No	Yes
Proposed	Yes	Yes	Yes	Yes	Conditional	Yes	Yes	Yes

6. 성능 평가

6.1 구현 환경

Circom 2.0[13]과 SnarkJS 0.7을 사용하여 구현하였다. ZKP 회로는 BN254 곡선 위 Groth16 백엔드로 22,450개 R1CS 제약 조건으로 컴파일된다. DID 원장은 Hyperledger Fabric 2.5 기반이며, 생체 인식 모듈은 MobileNetV2 INT8 양자화 모델(128차원 임베딩, ~85ms)을 사용한다. 퍼지 추출기는 (256, 128, 20, 2^{-40})-보안 스케치를 사용한다. 실험 플랫폼: (a) 데스크톱: Intel Core i7-12700K @ 3.6GHz, 32GB DDR5, Ubuntu 22.04 LTS; (b) 모바일: Samsung Galaxy S22 (Snapdragon 8 Gen 1, 8GB), Android 13. 각 측정은 100회 반복한다.

6.2 계산 오버헤드

모바일 종단간 인증 시간 165ms는 사용자가 인지하기 어려운 임계값 500ms를 크게 하회한다. ZKP 증명 생성의 오버헤드 비율은 다음과 같이 계산된다:

$$r\_ZKP = t\_ZKP / t\_total = 41.9 / 164.8 \approx 25.4\% \quad \text{(수식 28)}$$

〈Table 4〉 Computation overhead of DID-ZKP-MFA (ms, mean ± standard deviation)

Phase	Desktop (ms)	Mobile (ms)	Execution
DID lookup	12.3±1.1	24.7±2.8	Client
ZKP proof generation	18.4±2.3	41.9±4.6	Client
ZKP verification	3.1±0.3	6.2±0.8	Server
Biometric recognition	85.0±12.0	91.7±14.3	Client
Fuzzy extractor	2.1±0.2	6.5±0.9	Client
Total (client)	117.8	164.8	-
Total (server)	15.4	30.9	-

6.3 통신 오버헤드 및 배터리

〈Table 5〉 Communication overhead per authentication session

Message	Size (bytes)	Direction
Challenge (ch, tid)	36	V → U
Authentication request (DID_U, x, π)	458	U → V
DID document	742	L → V
Accept/reject response	192	V → U
Total	1,428	-

배터리 측정 결과, 단일 인증 세션의 에너지 소모량은 약 1.8mJ이다. 일일 50회 인증 시 배터리 영향도:

$$E\_daily = 50 \times 1.8\ mJ = 90\ mJ \ll 20{,}000\ mJ \quad \text{(수식 29)}$$

6.4 기존 기법과의 종합 비교

〈Table 6〉 Qualitative comparison with existing authentication schemes

Scheme	Unlinkability	Biometric protection	Forward secrecy	MFA	DID	Evidence
Kim et al. [5]	No	No	No	Yes	Yes	Published description
Mun [4]	No	No	No	Yes	No	Published description
Pathak et al. [7]	Yes	No	No	No	No	Published description
Rivera et al. [8]	Yes	No	No	Yes	No	Published description
He et al. [10]	Yes	No	No	No	Yes	Published description
Proposed	Conditional	Yes	Yes	Yes	Yes	Sections 4–6

Table 6은 인용 문헌 [4], [5], [7], [8], [10]에 명시된 기능을 기준으로 저자가 재분류한 정성적 비교이다.

7. 결론

본 논문에서는 DID, ZKP, 생체 정보 보호 및 동적 챌린지-응답을 통합한 프라이버시 보호 다중 인증 프레임워크 DID-ZKP-MFA를 제안하였다. 제안 기법은 인증 정확성, 자격증명 프라이버시, 생체정보 비공개, 재전송 및 중간자 공격 저항성을 하나의 프로토콜에서 제공하며, pairwise DID 또는 세션별 가명 식별자를 사용할 때 식별자 수준의 세션 비연결성으로 확장할 수 있다.

핵심 기여로는 100회 반복 측정에서 모바일 종단간 인증 시간은 평균 164.8ms이고 세션당 통신량은 1,428 바이트로 확인되었다.

REFERENCES

[1] W3C, “Decentralized Identifiers (DIDs) v1.0,” W3C Recommendation, 2022.

[2] S.Goldwasser, S.Micali and C.Rackoff, “The knowledge complexity of interactive proof systems,” SIAM Journal on Computing, Vol.18, No.1, pp.186-208, 1989.

[3] J.Groth, “On the size of pairing-based non-interactive arguments,” Proceedings of EUROCRYPT 2016, pp.305-326, 2016.

[4] H.J.Mun, “Biometric information and OTP based authentication mechanism using blockchain,” Journal of Convergence for Information Technology, Vol.8, pp.85-90, 2018.

[5] S.Kim, H.J.Mun and S.Hong, “Multi-factor authentication with randomly selected authentication methods with DID on a random terminal,” Applied Sciences, Vol.12, No.5, Article 2301, 2022.

[6] F.Zhao et al., “A blockchain-based efficient cross-domain authentication scheme for Internet of Vehicles,” Computers, Materials & Continua, Vol.80, No.1, pp.567-585, 2024.

[7] S.Pathak, S.Dhanush and P.V.S.Rao, “Blockchain-enhanced ZKP-based privacy-preserving mutual authentication for IoT networks,” IEEE Access, Vol.12, pp.1-18, 2024.

[8] J.J.D.Rivera, A.Muhammad and W.C.Song, “Securing digital identity in the zero trust architecture: A blockchain approach to privacy-focused multi-factor authentication,” IEEE Open Journal of the Communications Society, Vol.5, pp.2792-2814, 2024.

[9] J.M.Bernabé Murcia et al., “Decentralised identity management for zero-trust multi-domain frameworks,” Future Generation Computer Systems, Vol.162, Article 107479, 2025.

[10] J.He, X.Ma, D.Zhang and F.Peng, “Supervised and revocable decentralized identity privacy protection scheme,” Security and Safety, Vol.3, Article 2024013,

2024.

[11] Y.Dodis, L.Reyzin and A.Smith, “Fuzzy extractors,” SIAM Journal on Computing, Vol.38, No.1, pp.97-139, 2008.

[12] R.Canetti, “Universally composable security,” Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science, pp.136-145, 2001.

[13] M.Belles-Muñoz et al., “Circom: A robust and scalable language for building ZK circuits,” IEEE Transactions on Dependable and Secure Computing, Vol.20, No.6, pp.4872-4882, 2023.

[14] A.Gabizon, Z.J.Williamson and O.Ciobotaru, “PLONK: Permutations over Lagrange-bases for oecumenical noninteractive arguments of knowledge,” IACR Cryptology ePrint Archive, Report 2019/953, 2019.

[15] D.Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete," Communications of the ACM, Vol.28, No.10, pp.1030-1044, 1985.

홍 성 혁(Sunghyuck Hong) [정회원]

- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2012년 3월 ~ 현재 : 백석대학교 첨단IT학부, IoT 전공 주임 교수

〈관심분야〉
자율주행, 객체인식, 딥러닝, 블록체인, 사물인터넷 보안