사물인터넷융복합논문지 Vol. 9, No. 5, pp. 73-78, 2023 https://doi.org/10.20465/KIOTS.2023.9.5.073

이더리움 블록체인 기반 부인봉쇄 바이오메트릭 서명 기법

윤성현*
백석대학교 컴퓨터공학부 교수

The Ethereum Blockchain based Undeniable Biometric Signature Scheme

Sunghyun Yun*
Professor, Division of Computer Engineering, Baekseok University

요 약 PKI(Public Key Infrastructure)는 인터넷 서비스에 대한 법적 구속력을 강화하는 데 사용된다. PKI 인증서는 사용자 공개키를 법적으로 인증한 것으로 정부가 지정한 신뢰할 수 있는 인증기관에서 발행된다. 따라서 사용자는 인증서 기반으로 법적 구속력을 갖는 서명을 생성할 수 있다. 바이오메트릭 데이터는 사람마다 고유하기 때문에 바이오메트릭 인증은 PKI 도움 없이 법적으로 자신의 신분을 증명할 수 있다. 소셜미디어와 같은 인터넷 서비스 가입은 지역적 제약을 받지 않기 때문에 PKI 기반의 인터넷 서비스를 구현하는 것은 쉽지 않다. 블록체인은 네트워크에 참여하는 사용자들의 합의로 수정 및 삭제할 수 없는 데이터를 저장하는 기술로 신뢰할 수 있는 제 3자의 도움이 필요하지 않다. 본 연구에서는 이더리움 스마트 계약 기반의 부인봉쇄 바이오메트릭 서명 기법을 제안한다. 제안한 방법은 바이오메트릭 템플릿 등록, 부인봉쇄 서명 생성 및 검증 단계로 구성된다. 부인봉쇄 서명은 서명자의 도움 없이는 서명을 검증할 수 없다. 서명자는 도전-응답 방식의 검증 프로토콜을 이용하여 원하는 검증자에게만 서명의 정당성을 확인시켜준다. 제안한 방법은 엘가말 서명 기법을 변형하여 다중서명 기법으로 확장될 수 있고 블록체인 기반 인터넷 서비스의 신뢰성을 높일 수 있다.

주제어 : 블록체인, 부인봉쇄 서명, 바이오메트릭 인증, 바이오메트릭 서명, 스마트계약

Abstract PKI(Public Key Infrastructure) is used to enforce legal binding forces to the Internet services. The PKI certificate is the legal certification of the user's public key and is issued by the trustworthy CA(Certificate Authority) designated by the government. Therefore, users can create legally binding signatures based on PKI certificates. Because biometric data is unique to each person, biometric authentication can legally prove one's identity without the help of PKI system. As users participating in Internet services such as social media are not subject to regional restrictions, thus it is not easy to implement Internet services based on PKI. Blockchain is a technology that stores data that cannot be modified or deleted, and does not require the help of a trusted third party. The block to add is determined by consensus of users participating in the blockchain network. In this study, we propose the undeniable biometric signature scheme based on Ethereum smart contracts. The proposed scheme consists of biometric template registration, undeniable signature generation, and verification protocolss. The Undeniable signature cannot be verified without the help of the signer. The signer uses a challenge-response protocol to show the legitimacy of the signature only to the desired verifier. The proposed scheme can be extended to a multi-signature scheme by modifying the El-Gamal signature scheme and can increase the reliability of blockchain-based Internet services.

Key Words : Blockchain, Undeniable Signature, Biometric Authentication, Biometric Signature, Smart Contract

*본 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(2018R1D1A3B07050180)
*교신저자 : 윤성현(shcrpt@gmail.com)
접수일 2023년 9월 2일 수정일 2023년 10월 12일 심사완료일 2023년 10월 15일

1. 서론

일반적으로 인터넷 서비스에서 사용자 인증은 패스워드 기반으로 이루어진다. 패스워드 기반 인증은 사용하기 쉽고 경제적이다. 단점은 다른 사람에게 자신의 아이디와 패스워드를 빌려줄 수 있다는 것이다[1,2].

바이오메트릭 데이터는 사람마다 고유하기 때문에 패스워드 인증과 마찬가지로 사용자 인증 수단으로 사용할 수 있다. 더불어 바이오메트릭 데이터는 신체의 일부분이기 때문에 사용하기 쉽고 패스워드 방식보다 안전한다[3].

바이오메트릭 기반 인증은 바이오메트릭 데이터를 스캔해야 하는 장비가 필요하기 때문에 대중화되지 못하고 시설 보안이 필요한 몇 몇 특정 기관에서 만 사용자 인증 용도로 사용되었다. 최근 출시되고 있는 대부분의 스마트폰은 지문, 얼굴 인식이 가능한 바이오메트릭 센서가 내장되어 있고 스마트폰 사용자들이 사용할 수 있는 다양한 바이오메트릭 인증 기반의 앱이 보급되고 있다 [4]. 스마트폰의 폭 넓은 보급으로 바이오메트릭 인증 기법의 대중화가 가능하게 되었다.

PKI는 인터넷 상에서 상거래 및 공공 서비스를 사용할 수 있도록 하기 위해서 필수적이다. 사용자 인증서를 발급하는 CA(Certificate Authority)는 전적으로 신뢰할 수 있는 기관으로 정부에서 지정한다. CA가 발급한 공개키 인증서는 법적 효력을 갖기 때문에, 인증서 기반으로 만든 디지털 서명은 법적 효력을 갖는다[1,5].

유투브, 페이스북 등과 같은 인터넷 기반의 소셜미디어 서비스 가입은 지역적 제한이 없다. 따라서 각 국가의 정부에서 관리하는 인증서 기반의 PKI 서비스는 글로벌 멤버를 대상으로 하는 인터넷 서비스에 적합하지 않다.

인터넷 커뮤니티 기반 서비스의 신뢰성을 높이기 위해서는 블록체인 기술과 바이오메트릭 인증 기술의 접목이 필수적이다. 블록체인 기술은 블록체인 네트워크에 참여하는 구성원들의 합의로 블록체인에 저장된 데이터를 삭제 및 수정할 수 없도록 하는 기술이다. 블록체인에 저장된 데이터는 블록체인 네트워크가 유지되는 동안 영구히 보존된다[6].

아이디 및 패스워드 기반 인증은 원격에서 로그인한 사용자가 실제 사용자인지 검증할 수 없는 단점이 있다. 따라서, 실제 사용자 확인이 필요한 인터넷 서비스에서 바이오메트릭 인증 기법의 적용은 필수적이다 [7].

본 연구에서는 블록체인 기반의 부인봉쇄 바이오메트릭 서명 기법을 제안한다. 제안한 기법은 바이오메트릭 템플릿 등록, 서명 생성 및 검증 단계로 구성된다.

제안한 기법에서 서명자는 블록체인 네트워크에 구현된 스마트계약 프로그램을 이용하여 서명을 생성하고 검증한다. 서명자의 바이오메트릭 템플릿, 공개키, 서명 및 검증 데이터는 블록체인에 저장되고 모든 사용자는 서명 사실과 결과에 대해서 부인할 수 없다.

2. 관련 연구

PKI는 국가가 지정한 공인인증기관에서 사용자의 공개키를 인증한 인증서를 발급해 주는 체계이다. 인증서 기반으로 디지털 계약을 서명하면 해당 계약은 법적 효력을 갖게 된다. 따라서, 법적 근거가 필요한 다양한 인터넷 서비스에서 사용된다.

단점은 법적 효력의 범위가 국내로 한정된다는 것이다. 퍼블릭 블록체인에 저장되는 데이터는 국가가 보증하는 것이 아니고 자동화된 블록체인 프로토콜에 의해서 데이터의 무결성이 보장된다[6].

블록체인에 저장된 데이터는 조작 및 삭제가 불가능한 특성을 갖는다. 특정 서비스를 위해서 블록체인에 저장된 스마트계약 프로그램은 모든 구성원들이 확인할 수 있고 해당 프로그램의 신뢰성을 판단할 수 있다[8].

따라서, 블록체인 기반 서비스는 국가에 종속되는 것이 아니고, 스마트계약 조건을 따르는 커뮤니티에 종속된다. 블록체인 기반 서비스는 지역적 제한이 없고 특정 서비스에 종속되는 다양한 신뢰 모델을 만들 수 있다[6,8].

바이오메트릭 데이터는 사람마다 고유하고 사용자 신분 인증을 위한 수단으로 사용된다. 인터넷으로 로그인하는 서비스의 경우에 다른 사용자에게 아이디와 패스워드를 알려주어 대리 인증이 가능하다. 대리 인증의 위험을 최소화하기 위해서 바이오메트릭 인증 기법의 적용은 필수적이다.

바이오메트릭 인증은 먼저 스캐너를 이용하여 바이오메트릭 데이터를 수집하고 이미지 처리를 한다. 템플릿은 이미지로부터 추출한 특징점의 (x, y) 좌표와 방향을 가리키는 벡터로 구성된다. 관리 서버는 사용자의 바이오메트릭 템플릿을 DB에 등록한다. 서버는 사용자 인증 세션에서 사용자가 전송한 템플릿과 DB에 등록된 템플릿을 비교하여 확률적으로 이 사용자가 등록된 사용자와 맞는지 결정한다[3].

부인봉쇄 서명 기법은 서명자의 도움 없이는 서명을 검증할 수 없는 기법으로 D.Chaum이 처음으로 제안하였다[9]. 서명자가 자신이 원하는 사용자에게만 자신의

서명을 검증할 수 있도록 하는 것으로 서명자의 프라이버시를 보장할 수 있다.

제안한 기법은 부인봉쇄 특성을 만족하도록 기존의 엘가말 서명 기법 [10]을 변형한다. 부인봉쇄 서명 검증은 스마트계약에 구현된 도전-응답 프로토콜을 이용하여 서명자가 원하는 검증자에게만 서명의 정당성을 확인시켜 줄 수 있도록 서명자의 프라이버시를 보장한다.

3. 제안한 기법

제안한 기법은 바이오메트릭 템플릿 생성 및 등록, 부인봉쇄 서명 생성 및 검증 프로토콜로 구성된다.

정의 1. p는 매우 큰 소수로 GF(p)는 암호학적으로 안전한 유한체이고 g는 GF(p) 상에서 정의된 생성자이다[1,10].

가정 1. 블록체인 기반 바이오메트릭 서명 기법에 필요한 구성요소는 다음과 같다.

- BSigContract은 바이오메트릭 템플릿 등록, 부인봉쇄 서명 생성, 검증 서비스로 구성된 스마트계약이다.
- BSigContract 배포자의 공개키 pk_{bsc}와 개인키 sk_{bsc}는 다음과 같다.

  $sk_{bsc} < p$

  $$pk_{bsc} \equiv g^{sk_{bsc}} \bmod p$$
- 서명자 S는 자신의 바이오메트릭 템플릿, 공개키, 이더리움 네트워크의 EOA 주소를 블록체인에 등록한다. S는 바이오메트릭 인증에 성공하면 부인봉쇄 서명을 블록체인에 저장한다.
- 검증자 V는 BSigContract에 저장된 S의 서명을 검증하기 위해서 도전-응답 프로토콜에 참여한다.

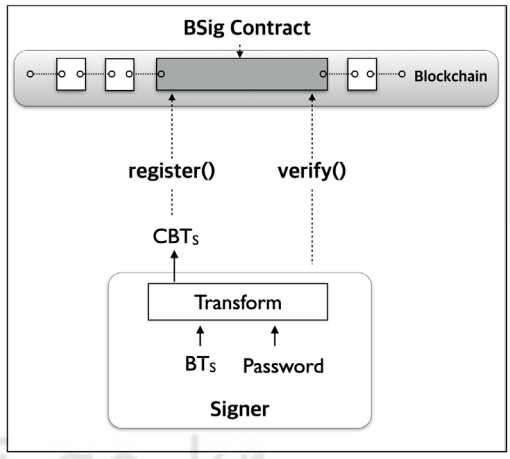
가정 2. BSigContract의 매핑 테이블은 다음과 같이 정의한다. CBT 타입은 사용자 바이오메트릭 템플릿을 정의한 포맷이라고 가정한다[11]. 공개키, 서명, 도전, 응답은 문자열로 저장하고 BigNumber 객체로 변환하여 사용한다[12].

```
struct SignerInfo = {
  address addr; // 서명자 주소
  string pkey; // 서명자 공개키
  CBT cbt; // 암호화된 바이오메트릭 템플릿
}
mapping (address => SignerInfo) RSigners[]

struct BUSig = {
  SignerInfo signer;
  bytes32 hash; // 256비트 해쉬값
  string R, BSIG; // 부인봉쇄 서명
}
mapping (UINT32 => BUSig) BSigs[]

struct VerifyBUSig {
  string busig; // BSigs 테이블에 있는 서명
  string challenge; // 검증자가 생성한 도전
  string response; // 서명자가 생성한 응답
}
mapping (UINT32 => VerifyBUSig) VerSigs[]
```

가정 3. BSigContract에서 바이오메트릭 템플릿 등록, 부인봉쇄 서명 생성 및 검증을 위한 함수는 다음과 같이 정의한다.

- register() : 서명자 템플릿 등록
- verify() : 서명자 템플릿 검증
- sign() : 서명자 확인 및 서명 생성
- challenge() : 검증자의 도전 값 생성
- response() : 서명자의 응답 생성
- verify_sig() : 서명 검증

3.1 바이오메트릭 템플릿 등록



[Fig. 1] Cancelable Biometric Template Registration

그림 1은 바이오메트릭 템플릿 등록 및 검증 단계를 보여준다.

단계 1: S는 자신의 바이오메트릭 데이터를 스캔하여 템플릿 BT_S를 생성한다.

단계 2: S는 랜덤하게 선택한 패스워드를 입력하여 BT_S를 변형한 취소가능한 템플릿 CBT_S를 생성한다. 바이오메트릭 데이터는 신체의 일부분으로 고유하기 때문에 블록체인에는 재발급할 수 있는 취소가능한 템플릿을 배포한다.

단계 3: S는 난수 RND를 생성하고 CBT_S 그리고 S의 이더리움 주소 $Addr_S$를 이용하여 다음과 같이 개인키 sk_S와 공개키 pk_S를 생성한다. H()는 해쉬함수이다.

sk_S = H(RND, CBT_S, $Addr_S$) 〈 p

$$pk_S \equiv g^{sk_S} \bmod p$$

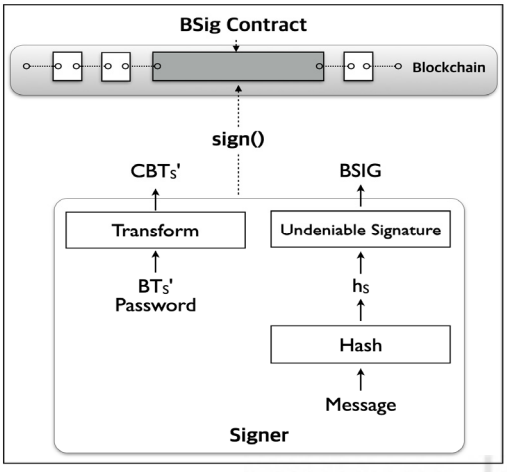
단계 4: S는 BSigContract의 공개키로 CBT_S를 암호화한다.

단계 5: S는 BSigContract의 register() 함수를 호출하여 S의 주소, S의공개키, 암호화된 CBT_S를 BSigContract으로 전송한다.

단계 6: BSigContract은 먼저 S의 이더리움 주소가 올바른지 검증한다. 검증에 실패하면 트랜잭션 발행 이전 상태로 복귀한다.

단계 7: BSigContract은 S의 공개키와 암호화된 CBT_S를 가정 2에서 정의한 RSigners 매핑테이블에 저장한다.

3.2 부인봉쇄 서명 생성



[Fig. 2] Undeniable Signature Generation

그림 2는 서명자가 sign() 함수를 호출한 경우에 부인봉쇄 서명을 생성하는 단계를 보여준다.

단계 1: S는 메시지 m을 해쉬한다. p-1과 서로소인 임의의 난수 k를 선택하여 R_S를 만든다. H()는 해쉬 함수로 keccak256() 함수를 사용한다 [13].

h_S = H(m), gcd(k, p-1) = 1

$$R_S \equiv h_S^k \bmod p$$

단계 2: S는 sign() 함수를 호출하여 m에 대한 부인봉쇄 서명 BSIG를 생성한다. k와 p-1은 서로소이기 때문에 다음 서명식을 만족하는 sig가 존재한다 [14, 15].

$$k \cdot sig \equiv sk_S \cdot R_S - k \cdot h_S \bmod p-1$$

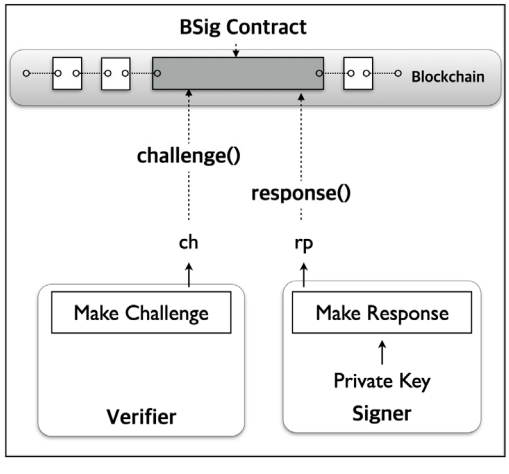
$$BSIG \equiv h_S + sig \bmod p-1$$

단계 3: S는 자신의 바이오메트릭 데이터를 스캔하고 템플릿 BT_S'을 생성한다. S는 패스워드와 함께 BT_S'을 템플릿 변형함수에 입력하여 CBT_S'을 생성한다.

단계 4: S는 그림 1의 verify() 함수를 호출하여 BSigContract에 등록된 S의 템플릿 CBT_S와 CBT_S'을 비교한다. 만약 검증에 실패하면 트랜잭션 발행 이전 상태로 복원한다.

단계 5: 바이오메트릭 인증에 성공하면 가정 2에서 정의한 BSigs 매핑테이블에 서명 BSIG를 저장한다.

3.3 부인봉쇄 서명 검증



[Fig. 3] Undeniable Signature Verification

그림 3은 부인봉쇄 서명 검증 단계를 보여준다. 검증자는 도전값을 생성하고 서명자는 이 도전값에 대한 응답을 생성한다.

단계 1: 검증자 V는 임의의 두 난수 (a, b)를 선택하여 challenge() 함수를 호출하여 다음과 같이 도전값 ch가 포함된 트랜잭션을 발행한다.

$$ch \equiv R_S^{BSIG \cdot a} \cdot pk_S^{R_S \cdot b} \bmod p$$

단계 2: ch는 VerSigs 매핑테이블에 저장된다. num_S는 부인봉쇄 서명이 저장된 BSigs 매핑테이블의 번호이다.

VerSigs[num_V].busig = num_S

VerSigs[num_V].challenge = ch

단계 3: S는 response() 함수를 호출하여 ch에 대한 응답 rp를 생성하고 다음과 같이 매핑테이블을 업데이트 한다.

$$rp \equiv ch^{sk_S^{-1}} \bmod p$$

VerSigs[num_V].response = rp

단계 4: V는 verify_sig() 함수를 호출하여 서명을 검증한다. verify_sig() 함수는 다음 검증식을 만족하면 True를 그렇지 않으면 False를 리턴 한다.

$$rp \equiv h_S^{R_S \cdot a} \cdot g^{R_S \cdot b} \bmod p$$

4. 안전성 분석

정리 1. 서명자는 블록체인 기반 부인봉쇄 서명에 대해서 부인할 수 없고 제 3자에 의한 대리 서명은 불가능하다.

(증명) S는 자신만이 알고 있는 k 값을 이용하여 R_S을 생성하고 블록체인에 저장한다. 메시지 m은 암호학적으로 안전한 해쉬함수 H로 해쉬된다. S는 자신의 개인키로 서명 BSIG를 생성한다. S는 바이오메트릭 기반 인증을 하고 성공하면 BSIG를 매핑테이블에 저장한다. 서명 검증을 위해서 V는 도전 ch를 생성하고 S는 이에대한 응답 rp를 생성한다. 서명 검증식의 완전성은 다음과 같이 증명된다. Q.E.D.

$$\begin{aligned} rp &\equiv ch^{sk_S^{-1}} \\ &\equiv (R_S^{BSIG \cdot a} \cdot pk_S^{R_S \cdot b})^{sk_S^{-1}} \bmod p \\ &\equiv (h_S^{k \cdot (h_S + sig) \cdot a} \cdot g^{sk_S \cdot R_S \cdot b})^{sk_S^{-1}} \bmod p \\ &\equiv (h_S^{sk_S \cdot R_S \cdot a} \cdot g^{sk_S \cdot R_S \cdot b})^{sk_S^{-1}} \bmod p \\ &\equiv h_S^{R_S \cdot a} \cdot g^{R_S \cdot b} \bmod p \end{aligned}$$

정리 2. 서명자의 도움 없이는 부인봉쇄 서명을 검증할 수 없다.

(증명) 정리 1에서 서명자 S는 자신의 개인키를 이용하여 ch에 대한 응답 rp를 생성한다. 제 3자가 서명자 도움 없이 서명 검증을 할려면 서명자의 개인키를 구해야 한다. 정의 1에서 GF(p) 상에서 이산대수를 구하는 것은 계산상 불가능하기 때문에 제 3자는 응답 rp를 생성할 수 없다.

5. 결론

본 논문에서는 블록체인 기반의 바이오메트릭 부인봉쇄 서명 기법을 제안하였다. 제안한 기법은 바이오메트릭 템플릿 등록, 부인봉쇄 서명 생성 및 검증 프로토콜로 구성된다. 제안한 서명 기법은 바이오메트릭 인증에 성공한 서명자만 서명을 블록체인에 저장할 수 있기 때문에 대리 서명은 불가하다. 또한 서명자의 도움 없이는 서명 검증을 할 수 없는 부인봉쇄 서명의 특성과 도전-응답 프로토콜의 안전성을 분석하였다. 제안한 기법은 엘가말 서명식을 변형하여 여러 서명자가 참여하는 부인봉쇄 다중서명 기법으로 확장될 수 있고 전자투표 등 사용자 프라이버시와 공정성을 보장하는 응용에 적용될 수 있다.

REFERENCES

[1] M.Stamp, Information Security: Principles and Practice 2nd Edition, Wiley-Inerscience, 2011.

[2] S.Y.Kim, K.S.Jang and S.J.Lee, "Study on Password Security," Journal of Digital Forensics, No.8, pp.28-39, 2011.

[3] H.Li, K.Toh and L.Li, Advanced Topics in Biometrics, World Scientific, 2011.

[4] Apple Support, Use Touch ID on iPhone and iPad, https://support.apple.com/en-us/HT201371.

[5] Tepandi, "Wireless PKI Security and Mobile Voting," IEEE Computer, Vol.43, No.6, pp.54-60, 2010.

[6] A.M.Antonopoulos, G.Wood, Mastering Ethereum,

O'Reilly, 2019.

[7] S.H.Yun, "The USIM based Biometric Multi- Signature for Mobile Content Authentication," ICONI, pp.137-141, 2011..

[8] Wei-Meng Lee, Beginning Ethereum Smart Contracts Programming, Apress, 2023.

[9] D.Chaum, "Undeniable Signatures," Advances in Cryptology, Proceedings of CRYPTO'89, Springer-Verlag, pp.212-216, 1990.

[10] T.Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, vol.31, no.4, pp.469-472, 1985.

[11] ISO/IEC19794-1:2011, Information technology Biometric data interchange formats, 2023.

[12] https://docs.ethers.org/v5/api/utils/bignumber/#BigNumber--creating

[13] https://en.wikipedia.org/wiki/SHA-3

[14] https://en.wikipedia.org/wiki/Euclidean_algorithm

[15] David M. Burton, Elementary Number Theory 3rd Edition, Wm, C, Brown Publishers, 1994.

윤 성 현(Yun Sunghyun) [종신회원]

■ 1997년 2월 : 고려대학교 일반대학원 컴퓨터학과 (이학박사)
■ 1998년 3월 ~ 2002년 2월 : LG 전자 선임연구원
■ 2002년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 교수

〈관심분야〉
블록체인, 사물인터넷, DRM, 정보보호