퍼블릭 블록체인 기반 SMPC 생체인증 시스템 제안

두지수[1], 강혁[2], 이근호[3*]
[1]백석대학교 컴퓨터공학부 학생, [2]고려대학교 영상정보처리협동과정, [3]백석대학교 컴퓨터공학부 교수

Proposal of SMPC Biometric Authentication System Based on Public Blockchain

Ji-Su Doo[1], Hyeok Kang[2], Keun-Ho Lee[3*]
[1]Student, Division of Computer Engineering, BaekSeok University
[2]Program in Visual Information Processing, Korea University
[3]Professor, Division of Computer Engineering, Baek-Seok University

요 약 4차 산업혁명의 영향으로 정형, 비정형 데이터를 수집 및 활용하는 방식이 발전됨에 따라 원치 않은 개인 정보 데이터도 수집되어 활용하고 있으며, 해커들은 정보탈취를 위해 다양한 공격을 시도하고 있다. 그럼에 따라 정보보호에 대한 중요성이 증가 되어 여러 보호 기법들이 등장하게 되었고 그 중 생체인증 기법의 보안성을 강화하기 위해 블록체인의 탈중앙화 기법과 다양한 알고리즘들을 활용한 연구가 많이 진행되었다. 본 논문에서는 분산 인증 시스템인 SMPC를 퍼블릭 블록체인 생체인증 시스템에 활용함으로써 사용자가 퍼블릭 블록체인 안에서 더욱 안전한 생체인증 방식으로 자신의 데이터를 보호할 수 있고 인증된 정보로 서명을 통해 블록체인 안에서 이용할 수 있도록 하는 퍼블릭 블록체인 생체인증 시스템을 제안하였다.

주제어 : 블록체인, 생체인증, SMPC, 퍼블릭, 동형 암호화

Abstract As the method of collecting and utilizing structured and unstructured data develops due to the influence of the Fourth Industrial Revolution, unwanted personal information data is also being collected and utilized, and hackers are attempting various attacks to steal information. As a result, the importance of information protection has increased, and various protection techniques have emerged, among which many studies have been conducted using decentralized techniques of blockchain and various algorithms to strengthen the security of biometric authentication techniques. This paper proposed a public blockchain biometric authentication system that allows users to protect their data in a safer biometric authentication method in the public blockchain and use it in the blockchain through signature with authenticated information.

Key Words : Blockchain, Biometric Authentication, SMPC, Public, Homomorphic Encryption

1. 서론

4차 산업혁명의 영향으로 다양한 데이터들을 수집하고 수집된 정형, 비정형 데이터를 활용하는 방식이 발전됨에 따라 원치 않은 개인정보 데이터도 수집되어 활용하고 있으며, 해커들은 정보탈취를 위해 랜섬웨어, 바이러스, 웜 같은 다양한 공격을 시도하고 있다. 그럼에 따라 정보 유출을 막기 위한 정보보호의 중요도가 증가하

*본 논문은 2020년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (NRF-2020R1I1A3069008)
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2023년 02월 21일 수정일 2023년 3월 23일 심사완료일 2023년 3월 29일

여 정보보호 방법의 하나인 신원을 인증할 수 있는 인증 기술에 대한 중요성이 증가하게 되었으며 인증기술은 비밀번호와 패턴 등을 사용하는 지식기반 인증기술에서 사용자의 신체 특성을 활용한 방법인 생체인증 기술이 등장하여 많은 사용자는 편리한 생체인증을 사용하였고 생체인증 기술 및 생체인증 정보 저장에 대한 중요성도 자연스럽게 증가하게 되었다. 그러나 기존 생체인증 기술의 문제점이라고 할 수 있는 생체인증 정보가 중앙 서버에 집중되어 있어 악의적인 공격으로 인해 보안성이 취약해질 수 있다는 문제를 시스템적인 보안 체계를 블록체인 기술의 탈 중앙화 기법을 통해 보완하였으며 최근에는 블록체인에 다양한 알고리즘을 적용하여 기존 기술의 보안성과 효율적인 측면을 더 높여주기도 한다. 그 예로 블록체인에 영지식 증명 중 하나인 zk-SNARK를 사용하거나 HASH 알고리즘, 스테가노그래피 등 여러 알고리즘을 활용하곤 한다. 본 논문에서는 분산 인증시스템인 SMPC를 블록체인 생체인증 시스템에 활용함으로써 퍼블릭 블록체인 생체인증 시스템에 대한 보안성을 향상하여 사용자가 더욱 안전한 생체인증 방식을 이용 할 수 있도록 시스템을 제안하고자 한다.

2. 관련 연구

2.1 블록체인

블록체인(Blockchain)은 블록(Block)과 블록(Block)을 연결하는 방식이며 블록과 블록이 연결된 형태가 체인처럼 보인다고 하여 블록체인이라고 불린다. Satoshi Nakamoto가 비트코인(Bitcoin)을 개발하면서 블록체인 기술이 주목받기 시작하였고 Nakamoto가 작성한 논문을 통해 블록체인의 기술에 대한 전반적인 기반을 만들었다[1]. 해당 블록체인은 각 거래는 인정되는 광부(Miners)들에게 인정받은 거래만 등록되며 등록된 거래는 데이터 삭제 혹은 복구할 수 없다는 특성이 있는 지속성(Persistency)과 블록체인 합의 알고리즘 사용으로 중앙 기관(서버)을 통해서 검증되지 않게 되므로 중앙 서버 비용이 필요하지 않다는 탈중앙화(Decentralization), 블록체인에서 활용하여 만들어지는 각자 생성된 주소를 통해 거래하므로 자신의 신원이 노출되지 않는다는 익명성(Anonymity)이라는 세 가지 특성이 있다[2]. 이러한 특성은 많은 분야에서 보안성을 높여 줄 수 있는 블록체인과 접목하는 연구가 많이 등장하게 되었다[3, 4, 5].

2.2 생체인증

생체인증(Biometric Authentication)은 각 사람을 식별하고 식별된 결괏값을 기준으로 접근 제어를 가능하도록 개인이 가지고 있는 각각 고유한 신체적, 행동 특성 등을 활용하는 보안 기법이다[6]. 일반적인 생체인증에서 활용하는 데이터는 손가락에 있는 지문, 안면 인식, 홍채/망막 인식, 음성 인식이 있었으나 요즈음에는 일반적인 생체인증 데이터가 아닌 특이한 데이터도 활용하여 생체인식을 진행하기도 하는데, 정맥 인식[7], ECG(심장박동수)[8], 보행 분석[9]과 같이 기존에 생체인증으로 활용할 수 없었던 데이터도 생체인증에 활용할 수 있도록 연구되고 있으며 기존의 인증 시스템의 알고리즘을 다른 방식으로도 접근하여 보안성, 효율성 측면을 높이는 다중 팩터[10], ZKP[11] 등 여러 연구도 진행되고 있다.

2.3 SMPC

SMPC(Secure Multi-Party Computation)은 안전하게 분산 컴퓨팅 작업을 하는 것을 말한다[12, 13]. 즉, 자신의 데이터를 사용하여 여러 인원이 자신이 가지고 있는 정보를 공개하지 않고, 인증을 위해 공동으로 참여하여 각자 함수를 통해 계산하여 나온 값들을 모아서 해당 인증에 대한 결괏값을 자신이 가지고 있는 정보와 비교하여 인증하는 방식을 갖고 있다. SMPC는 어떤 참여자도 다른 참가자들로부터 정보를 받을 수 없으며 출력의 결괏값을 통해서만 얻을 수 있다는 개인 정보 보호 측면과 SMPC의 작업이 정확해야 한다는 정확성, 각 참여자는 독립적이라는 것을 알 수 있다.

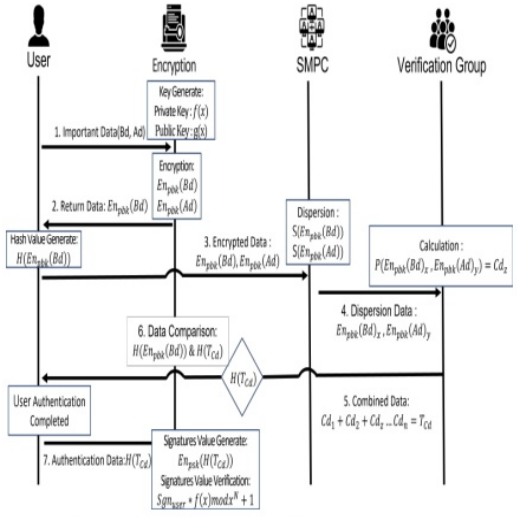
2.4 동형 암호화

동형 암호화(Homomorphic Encryption)는 데이터를 암호화하였을 때, 복호화를 진행하지 않고 암호화된 데이터에 대해 연산을 수행할 수 있는 암호화 기술이다. 동형 암호화는 덧셈만 혹은 곱셈만 연산할 수 있도록 제한되어 연산 수행이 가능한 부분적 동형 암호화(Partially Homomorphic Encryption)인 PHE와 덧셈과 곱셈과 같이 제한되지 않고 연산 수행이 가능한 완전한 동형 암호화(Fully Homomorphic Encryption)인 FHE[14, 15] 로 나누어진다. 그중에서 SMPC에 활용하기 위해서는 완전한 동형 암호화인 FHE 암호화 기법을 사용해야 한다.

3. 제안 모델

기존의 SMPC를 활용한 블록체인의 경우 단일 블록체인 시스템으로 구성하지 않고 블록체인 시스템을 제외한 별도의 SMPC 네트워크 및 에그리게이터 컨소시엄을 이용한 방식이다. 그러나 본 논문에서는 퍼블릭 블록체인에서 별도의 서버나 블록체인이 필요 없는 SMPC를 이용한 생체인증 체계를 하나의 블록체인만으로 시스템이 가능하도록 설계하였다. 해당 시스템은 데이터를 동형 암호화 및 SMPC 알고리즘을 통해 데이터 보호에 대한 보안성을 보장하려고 하였으며 데이터 분산 처리 시스템인 SMPC를 선택적 방식으로 진행하여 방대한 생체인증에 대한 데이터를 직접 전송하는 것보다 전송 및 처리하는 비용과 시간을 줄이고 효율적으로 필요한 인증에 대해서만 진행한다는 장점을 가지며 더불어 등록된 데이터를 삭제하기 어려운 블록체인의 특징으로 인해 잊힐 권리를 가지지 못한다는 부분을 자신이 소유하고 있는 개인키를 파기함으로써 자신의 생체인증 데이터에 대한 접근을 방지할 수 있게 된다.

3.1 동작 시나리오



[Fig. 1] Authentication & Signatures Scenario

[Fig. 1]은 SMPC를 활용한 인증 및 서명 방법에 대한 시나리오를 도식화한 그림이며 아래 나열된 각 단계는 인증방식에 대한 상세 설명이다.

Step 1. 사용자는 중요 데이터 (Bd, Ad)를 생성된 공개키인 g(x)로 암호화를 진행한다.

Step 2. 암호화된 생체 데이터는 해시함수 $H(x)$를 거친 $H(En_{pbk}(Bd))$ 의 값을 사용자에게 돌려준다. 이 값은 인증데이터 비교에 활용한다.

Step 3. 암호화된 데이터인 $(En_{pbk}(Bd),\ En_{pbk}(Ad)$를 SMPC의 분산 알고리즘인 $S(x)$에 넣어 값을 계산한다.

Step 4. 분산된 $En_{pbk}(Bd)_x$와 $En_{pbk}(Ad)_y$의 값을 데이터 연산 함수인 $P(x,y)$에 넣어 각자 데이터를 계산하여 Cd_z의 값을 구한다.

Step 5. 각자 연산한 값들인 $Cd_{z_1}, Cd_{z_2}, \cdots Cd_{z_n}$을 더하여 연산한 값의 총합 계산 데이터인 T_{Cd}를 얻는다.

Step 6. 모은 연산 값인 T_{Cd}을 해시 한 결과인 $H(T_{Cd})$와 Step 2에서 사용자가 돌려받은 $H(En_{pbk}(Bd))$ 값과 같은지 비교한다.

Step 7. 데이터의 값이 같다면, 해시 처리된 모은 연산 값인 $H(T_{Cd})$을 개인키 $f(x)$로 서명을 진행하여 $En_{psk}(H(T_{Cd}))$ 서명 값 Sgn_{user}를 얻는다. 서명 검증(복호화)의 경우 공개키인 $g(x)$으로 $H(T_{Cd}) = Sgn_{user} * f(x) \bmod x^N + 1$ 수식을 통해 서명 검증을 진행 할 수 있다.

3.1.1 사용자 생체 데이터 등록

사용자는 먼저 자신의 생체 데이터를 자신의 블록체인에 등록해야 하며 본 논문의 동형 암호화에 사용되는 알고리즘은 Gentry의 FHE 방식을 활용하여 작성하였다 [16, 17].

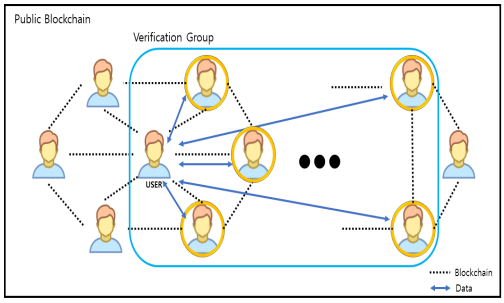
Step 1. 두 개의 큰 소수인 p와 q를 선택한 뒤 모듈로서 역할을 해줄 p와 두 소수의 곱인 N을 계산한다. 이후 모듈 N에 관한 두 개의 다항식인 $f(x)$ 와 $g(x)$을 선택한 동형 암호화로 공개키$g(x)$와 개인키$f(x)$를 만든다.

Step 2. 공개키$g(x)$을 활용하여 공개키 암호문인 $En_{pbk}(x)$을 아래의 수식을 이용하여 구한다.

$$En_{pbk}(x) = r(x) * g(x) + m * N \bmod x^N + 1$$

수식을 토대로 본 논문에서 중요 데이터로 분류된 생체 데이터 (Bd)는 $En_{pbk}(Bd)$으로 암호화가 된다.

Step 3. 암호화된 생체 데이터인 $En_{pbk}(Bd)$을 해시 함수를 통해 $H(En_{pbk}(Bd))$ 값으로 받아온 뒤, 해당 정보를 자신의 블록체인에 저장한다.



[Fig. 2] Biometric Authentication Request

3.1.2 다른 사용자로부터 인증요청을 받았을 경우

[Fig. 2]에서 노란색으로 표시된 것처럼 자신에게 생체인증을 요청한 사용자들을 특정하여 해당 사용자들을 인증그룹으로 지정한 뒤, 자신의 암호화된 생체 데이터 및 인증데이터를 SMPC를 이용하여 분산 전달한다.

Step 1. 사용자는 자신에게 인증요청을 한 사용자들을 특정하고 해당 사용자들을 자신의 인증그룹으로 지정한다.

Step 2. 해시값으로 저장된 $H(En_{pbk}(Bd))$ 의 해시값을 복호화하여 암호화된 자신의 생체 데이터인 $En_{pbk}(Bd)$을 얻는다.

Step 3. 인증 요청한 사용자들 일명 인증그룹에 SMPC의 비밀공유(Secret Sharing) 알고리즘인 $S(x)$을 사용하여 인증그룹 인원수인 n명만큼 아래의 수식으로 암호화된 데이터를 n개에 맞게 분산된 값을 얻는다 $S(En_{pbk}(Bd)) = En_{pbk}(Bd)_1 + En_{pbk}(Bd)_2 \cdots$ $\cdots En_{pbk}(Bd)_n$ 분산 처리된 값인 $En_{pdk}(Bd)_x$ 를 인증그룹 안의 각각의 사용자들에게 전달한다. 이때, x는 지정된 값이 아니며 인증그룹의 인원인 n명의 사람에게 값을 전달하기 위한 임의의 숫자이다.

Step 4. 인증요청 데이터인 Ad을 이전에 만들어둔 사용자의 공개키인 $g(x)$로 암호화를 진행한다. 암호화에 대한 수식은 아래의 수식을 만족한다. $En_{pbk}(x) = r(x)*g(x)+m*N \bmod x^N+1$ 인증요청 데이터 (Ad)는 $En_{pbk}(Ad)$로 암호화가 된다.

Step 5. 암호화된 인증요청 데이터 $En_{pbk}(Ad)$을 SMPC의 비밀공유 알고리즘인 $S(x)$을 사용하여 인증그룹의 인원수인 n명만큼 아래의 수식으로 암호화된 데이터를 n개에 맞게 분산처리하여 값을 얻는다. $S(En_{pbk}(Ad)) = En_{pbk}(Ad)_1 + En_{pbk}(Ad)_2 \cdots$ $\cdots En_{pbk}(Ad)_n$ 분산처리된 값인 $En_{pdk}(Ad)_y$ 을 인증그룹 안의 각각의 사용자들에게 전달한다. 이때 y는 지정된 값이 아니며 인증그룹의 인원인 n명의 사람에게 값을 전달하기 위한 임의의 숫자이다.

3.1.3 사용자 생체인증 및 서명

[Fig. 2]로 인해 인증그룹 내의 사용자들은 암호화된 생체 데이터와 인증요청 데이터를 분산되어서 전달받았다. 전달받은 데이터는 각 사용자의 연산을 통해 나온 연산 값을 공유하여 연산 값을 전부 더하고, 연산 값에 대한 검증을 진행하며, 검증이 완료되었을 때 참이라면 해당 값을 이용하여 디지털 서명 인증으로 이용할 수 있다.

Step 1. 인증그룹 내의 각 사용자는 기존에 가지고 있던 분산된 사용자의 데이터 값인 $En_{pdk}(Bd)_x$와 분산된 인증요청 데이터인 $En_{pdk}(Ad)_y$을 SMPC의 연산 함수인 $P(x,y)$에 값을 넣어 통해 계산을 진행한다. $P(En_{pdk}(Bd)_x, En_{pdk}(Ad)_y) = Cd_z$ 이때 z는 지정된 값이 아니며 인증그룹 내의 z번째를 의미하기 위한 임의의 값이다.

Step 2. 각 사용자는 각자 계산한 데이터의 연산 값인 Cd_z 을 공유하여 합산하고 최종 연산 값인 T_{Cd}을 얻어낸다. $Cd_1 + Cd_2 + Cd_z + \cdots Cd_n = T_{Cd}$

Step 3. 최종 연산 값인 T_{Cd}을 해시함수 $H(x)$를 통해 해시값으로 변환한 값 $H(T_{Cd})$을 인증받는 사용자의 블록체인에 있는 암호화된 생체 데이터 해시값 $H(En_{pbk}(Bd))$ 과 비교한다.

Step 4. 해시값이 같다면 인증결과는 참이므로, 해시 된 최종 연산 값 $H(T_{Cd})$을 인증받은 사용자의 개인키로 암호화하여 개인키 암호문인 $En_{psk}(x)$을 얻을 수 있으며, 해당 암호문을 서명으로 활용할 수 있다. $En_{psk}(H(T_{Cd})) = Sgn_{user}$

Step 5. 만들어진 디지털 서명은 인증그룹뿐 아니라, 해당 퍼블릭 블록체인 안에서 활용 가능하며 일정 시간이 지난 후에는 재인증이 필요하다.

Step 6. 만들어진 디지털 서명은 공개키를 사용하여 복호화를 진행할 수 있으며 복호화를 진행함으로써 서명이 누구의 인증인지 알아낼 수 있으며 블록체인의 무결성을 유지할 수 있으며 공개키$g(x)$와 N을 사용하여 복호화하는 수식은 아래와 같다.

$$H(T_{Cd}) = Sgn_{user} * f(x) \bmod x^N + 1$$

3.2 사용자 생체 데이터 접근 불가 요청

생체 데이터 삭제를 희망할 경우, 블록체인 특징 및 구조로 인해 생체 데이터를 삭제하는 것은 불가능에 가깝다. 그렇지만 삭제 대신 데이터에 대한 접근을 방지하는 방법으로 해당 사용자가 보유하고 있던 개인키를 삭제하여 암호화된 생체 데이터를 복호화하지 못하도록 하여 사용자의 잊힐 권리를 충족시키도록 한다. 그러나 사용자의 공개키는 아직 남아있으므로 서명의 경우 공개키로 복호화하여 서명한 사람이 누구인지 특정 할 수 있다.

3.3 기존 SMPC 블록체인과 비교

〈Table 1〉을 보면 기존 SMPC 블록체인의 경우 인증해주는 검증자들이 이미 지정되어 있으며 검증자들은 별도의 자원(서버 등)을 가지고 있거나 별도의 블록체인을 이용하여 효율성을 더 높이려 하였다. 그러나 본 논문에서는 퍼블릭 블록체인에서 사용자 간의 선택적 생체인증을 수행하여 유연한 인증방식 체계를 가질 수 있고 그로 인한 블록체인의 신뢰성과 안정성, 효율성이 높아지고 데이터 보안성과 검증 가능성이 보장되며 사용자의 생체 데이터는 공개키 삭제를 통해 잊힐 권리를 만족시킬 수 있다는 것이 본 논문에서 제안한 퍼블릭 블록체인 기반 SMPC 생체인증 시스템의 장점이다.

〈Table 1〉 Performance comparison with Existing systems

	SMPC Blockchain	Proposed scheme
Security	O	O
Flexibility	X	O
Expensive	High	Low
Efficiency	O	O
Based System	Complex Network	Blockchain
Right to be forgotten	X	O

4. 결론

본 논문에서 제안하는 시스템은 누구나 블록체인에 접근하고 확인할 수 있는 단일 퍼블릭 블록체인만으로 생체인증을 안전하고 유연하게 진행할 수 있으며 자신의 개인키를 파기함으로써 블록체인에 등록된 자신의 생체 데이터의 접근을 막아 잊힐 권리를 만족할 수 있다는 것이다. 본 논문의 시스템을 활용하여 속도는 조금 느리지만 정확하고, 투명성이 요구되는 전자 선거나 공공데이터를 이용하는 시스템 등에 활용하여 정확하고, 투명하게 데이터를 관리할 수 있다. 향후 연구를 통해 본 논문에서 제시한 퍼블릭 블록체인 기반 SMPC 생체인증 시스템을 구축하고 시험해보며 시험결과를 토대로 해당 시스템의 효율성, 보안성 등을 분석하고자 한다.

REFERENCES

[1] Nakamoto. S, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[2] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), pp.557-564, 2017.

[3] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, Vol.4, pp.2292-2303, 2016.

[4] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," in IEEE Access, Vol.8, pp.21091-21116, 2020.

[5] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2016 2nd International Conference on Open and Big Data (OBD), pp.25-30, 2016.

[6] U. Uludag, S. Pankanti, S. Prabhakar and A. K. Jain, "Biometric cryptosystems: issues and challenges," in Proceedings of the IEEE, Vol.92, No.6, pp.948-960, 2004.

[7] R. Bhupal, K. L. Sanjana, N. K. Khaneja, P. Bhartiya, A. S. Bhat and S. B J, "Finger Vein Authentication System," 2021 International Conference on Computer Communication and Informatics (ICCCI), pp.1-7, 2021.

[8] S. Pouryayevali, S. Wahabi, S. Hari and D. Hatzinakos, "On establishing evaluation standards for ECG biometrics," 2014 IEEE International Conference on

Acoustics, Speech and Signal Processing (ICASSP), pp.3774-3778, 2014.

[9] Vijay Bhaskar Semwal, Manish Raj, G.C. Nandi, "Biometric gait identification based on a multilayer perceptron," Robotics and Autonomous Systems, Vol.65, pp.65-75, 2015.

[10] A. Mansour, M. Sadik and E. Sabir, "Multi-factor authentication based on multimodal biometrics (MFA-MB) for Cloud Computing," 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), pp.1-4, 2015.

[11] Y. C. Tsai, R. Tso, Z. -Y. Liu and K. Chen, "An Improved Non-Interactive Zero-Knowledge Range Proof for Decentralized Applications," 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), pp.129-134, 2019.

[12] Yuhan Yang, Lijun Wei, Jing Wu, Chengnian Long, "Block-SMPC: A Blockchain-based Secure Multi-party Computation for Privacy-Protected Data Sharing," In Proceedings of the 2020 The 2nd International Conference on Blockchain Technology (ICBCT'20), Association for Computing Machinery, pp.46–51, 2020.

[13] FengY, Bai T, Lu S, Tang X, Wu J, "SMPC Task Decomposition: A Theory for Accelerating Secure Multi-party Computation Task," 2023.

[14] Kristin E. Lauter, "Practical applications of homomorphic encryption," In Proceedings of the 2012 ACM Workshop on Cloud computing security workshop (CCSW '12), Association for Computing Machinery, pp.57–58, 2012.

[15] Ahmed El-Yahyaoui and Mohamed Dafir EC-Chrif El Kettani, "Fully homomorphic encryption: Searching over encrypted cloud data," In Proceedings of the 2nd international Conference on Big Data, Cloud and Applications (BDCA'17), Association for Computing Machinery, pp.1–5, 2017.

[16] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan, "(Leveled) Fully Homomorphic Encryption without Bootstrapping," ACM Trans. Comput, 2014.

[17] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. "(Leveled) fully homomorphic encryption without bootstrapping," In Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS '12). Association for Computing Machinery, pp.309–325, 2012.

두 지 수(Ji-Su Doo) [준회원]

- 2019년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 재학

〈관심분야〉
정보보안, 블록체인, 시스템보안

강 혁(Hyeok Kang) [종신회원]

- 2013년 3월 : 워싱턴대학교 컴퓨터학과
- 2020년 9월 ~ 현재 : 고려대학교 박사과정
- 2015년 3월 ~ 현재 : 백석대학교 컴퓨터공학부

〈관심분야〉
양자암호, 융합 보안, 생체 인증, 블록체인

이 근 호(Keun-Ho Lee) [종신회원]

- 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 기술전략팀 과장
- 2010년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 교수

〈관심분야〉
이동통신 보안, 융합보안, 개인정보보호, 블록체인