Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.4, Aug. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.4.675

연산을 검증하기 위한 영지식 증명 프로토콜의 기법 및 응용 사례 분석*

주 찬 양,[1†] 이 현 범,[1] 정 희 원,[2] 서 재 홍[3‡]
[1,2,3]한양대학교 수학과 (대학원생, 박사후 연구원, 교수)

Analysis of Zero-Knowledge Protocols for Verifiable Computation and Its Applications*

Chanyang Ju,[1†] Hyeonbum Lee,[1] Heewon Chung,[2] Jae Hong Seo[3‡]
[1,2,3]Dept. of Mathematics, Hanyang University (Graduate student, Postdoctoral researcher, Professor)

요 약

최근 개인정보 보호법이 개정되고 개인정보에 대한 이목이 더해짐에 따라 각 기업들은 고객의 신원정보를 확인해야하는 의무(Know Your Costomer, 이하 KYC)와 동시에 이 정보를 개인정보보호법에 위반되지 않도록 처리 및 관리(개인정보보호법)를 해야 하는 의무를 가진다. 이러한 문제점을 해결할 수 있는 기술 중 하나는 영지식 증명(Zero-Knowledge Proof, 이하 ZKP)이다. ZKP를 사용하면 직접적으로 신원정보를 노출시키지 않으면서 해당 신원에 대한 검증이 가능하여 기업의 입장에서 신원정보 확인의 의무를 다함과 동시에 개인정보 관리에 대한 부담을 덜 수 있다. ZKP는 이 이외에도 많은 응용에 적용될 수 있는 기술로 본 논문에서는 현재 활발하게 연구되고 있는 ZKP기법 및 그 응용 사례를 분석하고 현실적인 모델에서의 ZKP의 적용을 위한 연구 방향을 제시한다.

ABSTRACT

According to the recent revision of Privacy Policy and the emerging importance of personal information, cooperations must verify customer identity (Know Your Costomer, KYC) while processing and managing this information so that it does not violate the Privacy Policy. One of the solution of this problem is zero-knowledge proof (ZKP). The use of the ZKP enables to verify the identity without exposing the identity information directly, thereby reducing the burden on the management of personal information while fulfilling the obligation of the cooperations to verify the identity. The ZKP could be employed to many other applications. In this paper, we analyze the ZKP technique and its applications currently being actively studied.

Keywords: Zero-Knowledge Proofs, Polynomial Commitment, Transparency, zk-SNARKs, STARKs

I. 서 론

최근 4차 산업혁명의 핵심 기술 분야로 분류되는 인공지능과 블록체인 산업의 비약적인 발전과 함께 방대한 양의 데이터의 활용이 필수적인 상황이 되면서 데이터가 최고의 가치로 인정받는 시대가 도래 하고 있다. 그러나 그 이면에 발생하는 개인정보의 가공 및 처리 등의 과정 중에 발생할 수 있는 개인정보

Received(05. 12. 2021), Accepted(06. 04. 2021)
* 이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(2020R1C1C1A01006 96812)
† 주저자, chanyangju@hanyang.ac.kr
‡ 교신저자, jaehongseo@hanyang.ac.kr(Corresponding author)

침해 등의 위협으로 인해 많은 기업들은 원활한 응용 서비스제공을 위한 '효율성'과 적절한 '안전성'을 모두 달성할 수 있는 데이터 활용방안에 주목하고 있다. 이 때 적용 가능한 중요한 암호 기법 중 하나는 ZKP로 최근 이와 관련한 이론적 연구들이 매우 활발하게 이루어지고 있다.

ZKP가 응용될 수 있는 예로 사용자의 나이에 대해 인증을 할 때 기존 서비스의 경우 신분증을 제시함으로써 나이를 인증 받을 수 있다. 하지만 신분증에는 나이 뿐 아니라 성별, 생년월일 등 기타 추가적인 신원 정보가 포함되어 있어 불필요한 정보까지 모두 공개해야 하지만 ZKP를 사용해 다른 신원 정보를 밝히지 않고 나이에 대해 인증이 가능하다. 또 다른 활용 예로 블록체인이 있다. 비트코인이나 이더리움과 같은 블록체인은 누구나 거래 내역을 검증할 수 있어야 하기 때문에 거래에 포함된 발신자, 수신자, 거래 금액 등은 모두 공개가 되어야 하고, 이로 인하여 비트코인을 사용하는 모든 사용자의 계좌를 추적할 수 있다. 하지만 블록체인에 ZKP를 적용한다면 거래의 세부 내역을 숨기면서도 누구나 거래 내역을 검증할 수 있도록 만들 수 있고, 이로 인하여 사용자의 프라이버시를 보존할 수 있다.

ZKP를 활용하는 예제에 따라 ZKP에 요구 되는 성질에는 차이가 있다. 예를 들어 클라우드 서비스나 블록체인과 같이 통신의 참여자가 다수인 상황에서는 참여자와 서버 간 통신 횟수가 성능에 직접적으로 영향을 미치기 때문에 통신 횟수를 최소화 하는 것이 중요하다. 그렇기 때문에 클라우드 서비스나 블록체인에 ZKP를 효과적으로 활용하기 위해서는 증명을 생성할 때 참여자 간 혹은 참여자와 서버 간 통신을 최소화시키는 것이 중요하다. 또한, 일반적으로 블록체인에서는 신뢰할 수 있는 주체를 가정하지 않기 때문에 신뢰할 수 있는 제3자가 초기 설정 단계에 참여하지 않더라도 안전한 증명을 설계 할 수 있는 지 여부가 중요하게 여겨진다[3,4,18].

하지만 신뢰할 수 있는 제3자를 가정하고 ZKP 알고리즘을 설계하는 경우에 대한 안정성 위협과 발생하는 제약 상황을 보완하기 위한 연구로 한번만 신뢰 가능한 방법으로 초기설정을 하고 업데이트하는 방법이 있다[1,12].

최근 양자컴퓨터의 발전으로 인해 양자내성암호가 많은 관심을 받고 있다. ZKP 알고리즘에서도 이를 고려하여 양자내성의 성질을 가지는 ZKP 알고리즘을 설계하는 연구는 중요하게 연구되고 있는 주제 중 하나이다[7].

본 논문에서는 각 응용에 필요한 성질 및 성능에 따른 분류 기준과 그 기준에 따른 최근 연구 결과 및 ZKP의 응용을 분석하며 다음과 같은 구성을 갖는다. 2장에서 ZKP에 대한 정의 및 성질에 대하여 정리하고 3장에서는 ZKP의 각 성질 및 성능을 나누는 기준에 대해 분석한다. 4장에서는 최근 연구결과들에 대한 분석을 진행하며 5장에서는 구체적인 응용 및 향후 연구 과제에 대해 기술하고 결론짓는다.

II. ZKP 개요

ZKP란 Zero-Knowledge Proof의 약자로 증명자(prover)가 자신이 알고 있는 비밀정보(witness)를 공개하지 않으면서, 해당 비밀정보를 알고 있음을 검증자(verifier)에게 증명하는 프로토콜이다[20].

2.1 ZKP의 입출력

[공통] 프로토콜에 따라서 증명자와 검증자는 CRS(Common Reference String)이라고 부르는 제 3자가 생성한 랜덤한 파라미터를 공통의 입력으로 가진다. 이때, CRS가 Uniform한 랜덤 소스로부터 생성가능하면 URS(Uniform Random String), 특정한 구조를 가지고 있는 경우는 SRS(Structured Random String)라고 한다.
[증명자] 증명의 대상이 되는 명제(statement)와 증거에 해당하는 비밀정보(witness)를 입력으로 가지고, 검증자와의 통신을 통해, 명제와 비밀정보의 관계를 증명하는 증명값(proof)을 만들어낸다.
[검증자] 검증자는 명제를 통신의 시작 시 입력으로 받고 프로토콜 마지막단계에서 명제와 비밀정보의 관계가 맞는지 증명자의 증명값을 통해 확인한다.

2.2 ZKP의 성질

[Completeness] 제시된 명제가 참이라면, 검증자는 프로토콜을 정상적으로 수행한 증명자가 제시한 명제가 참이라고 믿는다.
[Soundness] 제시된 명제가 거짓이라면, 검증자는 거짓 증명자가 제시한 명제를 믿지 않는다.
[Zero-Knowledge] 검증자는 명제의 참/거짓 이외의 어떠한 정보도 얻을 수 없다.

III. ZKP 기법 분류

3.1 Proofs vs Arguments

위에서는 구분하지 않고 영지식 '증명'이라는 용어를 사용하였으나 엄밀하게 증명이라는 것은 증명자의 계산 능력에 따라 proofs와 arguments로 구분될 수 있다. 계산 능력이 무한대인 증명자에 대한 soundness를 만족하면 proof라고 하고, 계산능력이 제한된 (보통은 다항식시간) 증명자에 대한 soundness를 만족하면 argument라고 부른다.

3.2 ZKP의 효율성 측정 기준에 따른 분류

3.2.1 복잡도 지표

증명자와 검증자의 계산 복잡도는 증명의 생성과 검증에 필요한 연산 횟수이며 통신 라운드 복잡도는 증명자와 검증자간의 통신 횟수, 커뮤니케이션(communication) 복잡도는 증명자와 검증자간 주고받는 메시지 크기를 의미하며 통신 횟수와 커뮤니케이션 횟수는 증명의 크기에 비례한다.

3.2.2 Interactive vs. Non-Interactive

NIZK(Non-Interactive ZKP)란, 증명자가 검증자에게 메시지를 한번만 전송하고, 그 이후에 추가적인 통신 없이 주어진 파라미터들로 메세지를 검증하는 ZKP이다. Interactive ZKP의 경우 프로토콜의 진행중 계속해서 증명자와 검증자가 통신을 유지하고 있어야 하지만 NIZK는 증명자의 메시지 전송 한번으로 추가적인 통신 상태를 유지할 필요 없다. Interactive ZKP에서 검증자의 역할이 랜덤한 값을 전송하는 것으로 제한된 것을 public coin 프로토콜이라고 하는데, public coin ZKP는 검증자가 선택하는 랜덤값을 랜덤이 필요한 시점까지 프로토콜 과정에서 주고받은 메시지에 대한 해시 값으로 대체함으로써 NIZK로 변환이 가능하고, 이런 기법을 Fiat-Shamir 변환이라고 부른다. 이는 증명자가 해시의 출력값을 임의로 조작할 수 없기 때문에 가능한 방법으로, 실제 대부분의 ZKP들은 public coin interactive ZKP로 설계하고 Fiat-Shamir 변환을 통해 NIZK 형태로 사용한다.

3.2.3 증명의 크기: Succinct Proofs

여러 응용에서 효율적으로 ZKP를 적용하기 위해서 증명자 및 검증자의 계산복잡도와 커뮤니케이션 복잡도를 중요하게 고려해야 한다. NIZK의 경우 커뮤니케이션 복잡도가 결국 증명의 크기가 되며, 증명의 크기와 검증시간이 증명하고자 하는 명제의 크기(circuit으로 표현할 때 circuit의 크기)보다 로그 이하로 작을 때 succinct하다는 표현 사용하며 Zero-Knowledge Succinct Non-interactive Argument of Knowledge를 줄여서 zk-SNARK라고 부른다.

3.3 초기설정에 따른 분류

대부분의 NIZK 프로토콜은 증명자와 검증자의 공통 입력인 CRS 없이는 달성할 수 없다는 것이 알려져 있다[22]. 2.1장에서 언급했듯이 CRS는 두가지고 분류되며, SRS는 생성과정에서 사용되는 비밀정보를 삭제하는 과정이 필요한데 가령, $g, g^{x}, g^{x^2}, \cdots$와 같이 지수들 간에 특정 구조가 있는 파라미터를 생성하기 위해 x를 생성하여 초기 설정을 거친다. x는 거짓증명을 생성하기 위한 트랩도어 역할을 하기 때문에 안전한 ZKP를 위해서는 해당 정보를 삭제해야하므로 신뢰할 수 있는 제3자가 정직한 방법으로 SRS를 생성해 준다는 가정이 필요하다.

SRS는 증명하고자 하는 명제의 특정한 형태에 적합하도록 생성해야 하면 non-universal, 증명하고자 하는 명제가 어떠한 형태이던 공통적으로 사용이 가능하면 universal하다고 한다.

CRS를 신뢰할 수 있는 제3자가 생성하면 신뢰가정이 필요한 초기 설정(trusted Setup)이라 하며, 생성자에 대한 별도의 신뢰과정이 필요 없는 경우에 투명한 초기 설정(transparent setup)이라고 부른다. URS의 경우 신뢰성 검증이 가능한 형태로 생성가능하기에 투명한 초기 설정으로 분류된다.

3.4 양자내성(Post-Quantum)여부에 따른 분류

다른 암호분야와 마찬가지로 ZKP에서도 양자내성을 가지는 프로토콜 설계는 중요한 연구 목표인데, 주로 대칭키 기반 혹은 격자기반으로 설계된 연구들이 다수로 격자 기반 프로토콜은 이론적인 연구들이 주를 이룬다[5]. 대칭키 기반의 프로토콜들은 실제

사용가능할 정도의 성능을 보이는 것들도 있으나 실제 사용하기에는 상대적인 성능이 떨어지며 아직 여러 가지 개선을 위한 연구들이 진행 중이다[7].

IV. ZKP 기법 연구 동향

ZKP는 1989년 Goldwasser, Micali, Rackoff 세명의 컴퓨터 과학자들에 의해 처음으로 소개 되었는데[20], 최근 ZKP에 대한 관심으로 이론 및 실제 응용에 대해 활발한 연구가 진행되고 있다. 이번 장에서는 어떠한 방법을 이용해서 ZKP의 효율적 설계를 위한 연구, 기존 연구들의 전반적인 흐름을 초기설정 단계에서 나타나는 차이점을 기준으로 기술하고, 가장 최신에 제안된 ZKP 기법들을 간략하게 비교한다.

4.1 PC(Polynomial Commitment) 설계 기법

PC는 ZKP를 설계가능하게 하는 하나의 암호학적 도구로, 다항식을 커밋하는 Com알고리즘, 커밋된 다항식을 확인하는 Open 알고리즘, 다항식의 커밋값과 특정한 점에 대한 함수값을 검증하는 Eval 알고리즘으로 구성되어있으며 이에 대한 개략적인 설명은 다음과 같다.

먼저, 증명자는 다항식을 공개하지 않기 위하여 다항식의 계수들을 랜덤 요소를 이용하여 Com 알고리즘을 수행하여 커밋을 한다. Eval 알고리즘은 다항식 f에 대해서 $f(x)=y$가 성립한다는 것을 커밋된 형태로 증명하는 알고리즘으로, 커밋값을 받은 검증자는 다항식이 정의된 공간상의 랜덤한 점을 고른 뒤 증명자와의 Eval 알고리즘을 수행한다. $\mathbb{F}_p[X]$에서 정의된 차수가 d보다 작은 서로 다른 두 다항식이 임의의 점에서 함숫값이 같을 확률이 d/p보다 작다는 Schwartz-Zippel Lemma에 의해 다항식의 계수가 정의되는 $\mathbb{F}_p$를 충분히 크게 정의하면 높은 확률로 증명자가 커밋해 둔 다항식과 동일한 다항식을 알고 있다는 것에 대한 검증이 된다. 또한 Com 알고리즘의 사용으로 직접적인 정보는 드러내지 않고 증명이 가능하므로 영지식성을 만족한다.

4.1.1 SRS를 사용하는 Kate PC

KZG10[2]에서 제안된 PC는 bilinear군들 $\mathbb{G}_1$, $\mathbb{G}_2$,$\mathbb{G}_T$의 페어링(Pairing) 연산 $e:\mathbb{G}_1\times\mathbb{G}_2\rightarrow\mathbb{G}_T$을 사용한다. Kate PC의 핵심 아이디어는 임의의 포인트 $\alpha\in\mathbb{F}_p$를 군의 생성자 $g\in\mathbb{G}_1$의 지수로 얹은 $\{g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^d}\}$를 CRS로 하여 다항식 $f(X)$를 $g^{f(\alpha)}$형태로 커밋한다. Eval 알고리즘은 특정한 포인트 $x\in\mathbb{F}_p$에 대해 $\frac{f(X)-f(x)}{X-x}$가 다항식이라는 성질과 bilinear 군의 성질을 이용하며 검증자는 3번의 페어링 연산을 통해 함숫값의 유효성을 검증한다. Kate PC의 장점은 검증자의 연산량이 다항식의 차수에 관계없는 상수크기라는 점이지만 CRS 생성시 사용한 α를 증명자가 알게 되면 거짓증명을 생성할 수 있으므로 초기 설정단계에 신뢰할 수 있는 제 3자에 대한 가정이 필요하다.

4.1.2 URS를 사용하는 DARK PC

URS를 사용하는 PC중 DARK PC[3]는 위수를 모르는 군을 활용한 PC이다. 위수를 모르는 군이란, 군의 위수에 대한 정보가 공개적으로 주어지지 않은 군으로 대표적인 예로 RSA 군과 class 군이 있다. 위수가 알려진 군들은 대수적 성질을 이용하여 군의 특정 원소의 n제곱근 값을 다항 시간 내에 구할 수 있다. 하지만 군의 위수를 알지 못하는 상태에서 임의의 원소의 n제곱근 값을 다항시간에 구하는 방법은 일반적으로 알려져 있지 않다. 즉, 위수를 모르는 군에서 임의의 군 원소에 대해 유리수 지수에 대한 연산이 어렵기 때문에 정수 지수연산만 수행 가능하다고 할 수 있다. DARK PC는 위수를 모르는 군에서 정수지수연산만 가능하다는 점과 주어진 정수에 대해서 q진법 표현방식이 유일하다는 점을 핵심 아이디어로 사용하며, 커밋과정은 다음과 같다.

주어진 다항식 $f(X)\in\mathbb{F}_p[X]$를 계수를 유지한 채로 변수만 정수 범위로 확장시켜 $\tilde{f}(X)\in\mathbb{F}[X]$를 만든 후 충분히 큰 정수 $q\in\mathbb{Z}$를 대입한 값 $\tilde{f}(q)$를 군 원소 $g\in\mathbb{G}$의 지수에 얹은 $g^{\tilde{f}(q)}$ 형태로 커밋한다. 앞에서 언급했던 q진법 표현방식의 유일성으로 동일한 커밋값을 가지는 다른 형태의 q진법 표현방식은 없을 것이고, 커밋 과정에서 랜덤 다항식을 추가하여 초기 다항식의 정보가 드러나지 않도록 설계할 수 있다. DARK에서 Eval 알고리즘은 차수가 d인 다항식을 두 부분으로 나누어 결합 후 새로 만들어진 차수가 $d/2$ 다항식에 대한 검증을 하는 과정을 마지막

에 상수다항식을 얻을 때까지 재귀적으로 수행하여 증명의 크기와 검증시간을 로그 크기로 줄였다.

DARK PC에서는 공통 파라미터로 위수를 모르는 군 $\mathbb{G}$와 원소 $g \in \mathbb{G}$, 충분히 큰 정수 q에 대한 정보들만 필요로 하므로 CRS의 크기가 다항식의 차수에 무관하게 항상 상수 크기를 갖는다. 또한 class 군을 사용할 경우, 군 생성과정에서 별다른 비밀정보를 사용하지 않기 때문에 투명한 초기 설정을 만족한다.

4.1.3 양자내성의 Virgo PC

충동 저항성을 가지는 해시함수(collision resistance hash function)가 블록 암호 기반으로 설계된 경우에는 파라미터 설정의 변경을 통해서 양자내성을 가지면서도 증명의 크기가 작은 커밋먼트 스킴의 설계가 가능해진다는 장점을 가지고 있다.

그러나 이러한 해시함수들의 경우 암호화된 상태에서 동형 연산의 성질을 가지지 못하기 때문에 커밋된 대상이 만족하는 성질을 보이는 것이 어렵다는 문제가 있다. 따라서 해당 커밋먼트 스킴을 활용하기 위해서는 해시로 커밋된 대상의 성질을 증명하는 추가적인 작업이 필요해진다.

17년, Ben-Sasson et al.[6] 에 의해 리드 솔로몬 부호(Reed-Solomon Code)를 활용하여 다항식이 특정한 차수 이하라는 검증을 할 수 있도록 하는 LDT(Low Degree Test) 프로토콜이 제안되었다. 리드 솔로몬 부호는 1960년에 개발된 오류 정정 부호의 한 종류로 주어진 파라미터 설정에 따라서 특정한 차수 미만으로 정의되는 유한체(finite field) 다항식이 가지는 값들에 대한 집합으로 기술될 수 있다. LDT 프로토콜은 이러한 성질을 이용해서 증명자가 특정한 차수 미만인 일변수 다항식에 대해서 다항식을 직접 공개하지는 않으면서 특정한 차수 조건을 만족한다는 것을 검증자가 확신할 수 있게 증명할 수 있는 상호 증명(interactive proof)이며 LDT 프로토콜을 활용하여 ZKP를 설계하는 기법으로 STARK[7], Virgo[14]등이 있다.

LDT 프로토콜에서 증명자는 차수가 작은 다항식 f가 정의된 공간에서 모든 값들에 대한 함숫값을 구해서 해당 값을 리프 노드(leaf node)로 하는 머클 트리의 머클 루트(root) 값을 커밋먼트로 검증자에게 전송한다. 검증자는 머클 루트 값을 받은 후 f의 임의의 함숫값을 증명자에게 요청하여 함숫값 $f(r)$과 초기에 커밋된 f의 값에 대한 증명을 받아 검증을 수행한다. 증명자의 커밋 과정은 여러 라운드에 걸쳐서 진행되는데, 각 라운드의 짝수, 홀수차수들의 다항식 f_e, f_o에 대해 $f(x) = f_e(x^2) + x f_o(x^2)$라고 두고, f_o앞의 변수 x에만 검증자의 랜덤값α를 대입하고, $f'(x) = f_e(x) + \alpha f_o(x)$에 대하여 다음 라운드를 진행한다. 그러면 최종적으로는 약 $\log(d)$번의 라운드를 통해 차수에 대한 검증이 가능하다.

이러한 LDT 프로토콜을 이용하면 해시함수로 다항식을 미리 커밋해 두고 해당 커밋먼트에 대한 증명 과정으로, 증명자는 검증자가 선택한 랜덤한 점에서의 값을 보내주고 사용된 다항식의 차수정보를 통해 악의적인 증명자는 높은 확률로 검증자의 검증을 통과할 수 없을 것이라는 보장이 가능한 PC의 설계가 가능[14]하며 해시함수를 활용하기 때문에 양자 내성의 성질을 갖게 된다.

4.2 초기 설정 단계의 가정에 따른 ZKP 설계 기법

4.2.1 SRS를 사용하는 신뢰할 수 있는 제3자에 대한 가정이 필요한 초기설정(Trusted Setup)

현재까지 가장 작은 크기의 증명을 생성하는 ZKP 기법은 2016년도 Groth[11]이 만든 방법으로, 증명하고자하는 관계를 2차 산술식으로 변형하여 증명값을 생성한다. 증명값의 크기는 그룹 원소 3개로 일정하지만, 타원곡선에서 페어링을 사용하기 때문에 신뢰가정이 필요한 SRS의 생성이 필요하다.

Zcash에서 거래의 정보를 숨기고 싶은 경우, 페어링 기반의 zk-SNARKs를 사용하고 있다. 만약 초기설정 단계에서 SRS을 생성하기 위해 사용된 트랩도어값을 공격자가 갖게 된다면, 거짓증명으로 거래를 위조하여 본인이 소유하고 있는 돈 이상을 사용하는 것이 가능할 수 있게 된다. 제3자가 SRS를 생성해 준다는 가정을 피하기 위해 다자간 연산(multi-party computation)을 활용[19]할 수도 있지만 이로 인해 생기는 파라미터들은 보이고자 하는 명제에 특화되어 만들어져서 ZKP가 활용되는 각각의 경우마다 새로운 초기설정이 필요하여 실제로 적용하기에는 효율성이 매우 떨어진다.

4.2.2 Universal SRS를 사용하는 ZKP 기법(Updatable Setup)

SRS를 사용하는 ZKP 기법의 한계점을 해결하기 위해 Universal SRS에 대한 연구들이 진행되고 있다. Universal SRS를 달성하기 위한 하나의 방법으로 초기 설정단계에서 한번만 신뢰할 수 있는 제3자를 가정하여 SRS를 군의 생성자의 지수에 $g^{x},g^{x^2},g^{x^3},...$과 같이 monomial들의 꼴이 되도록 생성한 뒤 그 이후에는 $g^{xy},g^{(xy)^2},g^{(xy)^3},...$등과 같은 형태로 업데이트 하는 방식으로 추가적인 신뢰성에 대한 가정 없이 사용가능한 방법이 알려져 있다[12]. Universal SRS를 생성해 두고 Kate PC를 사용하여 ZKP를 구성할 수 있으며 이러한 아이디어를 사용한 연구 결과들로 Sonic[16], PlonK[1] 등이 있다. Kate PC의 특징 중 하나가 다항식의 차수에 비례하지 않는 상수크기의 검증시간과 증명크기이며 아직까지 신뢰가정이 없이 상수크기의 검증시간과 증명크기를 달성한 ZKP가 없기 때문에 신뢰가정을 해야하는 번거로움이 있더라도 효율성이 중요시 되는 곳에서는 위에 소개된 ZKP들이 선호되곤 한다.

4.2.3 투명한 초기설정(Transparent Setup)

4.2.3.1 URS를 사용하는 ZKP 기법

투명한 초기설정이 가능한 Bulletproofs[4]라는 ZKP 기법은 Pedersen 커밋먼트를 사용하기 때문에 URS만을 필요로 하며 이산로그가 어렵다는 가정하에서 알려지지 않은 두 벡터의 내적관계를 이용해 범위 증명과 산술회로의 입출력 값에 대한 관계 증명이 가능하다. 주요 아이디어는 증명자가 Pedersen 커밋먼트를 활용하여 계속해서 압축된 형태의 커밋먼트를 검증자에게 전송하는데 각 전송마다 검증자의 랜덤 값에 따른 reduction과정을 거쳐서 검증자가 각 라운드에서 이전의 라운드에 사용된 커밋과 일치하는지에 대한 검증이 가능한 형태로 프로토콜이 진행된다. 재귀적인 reduction과정을 통해 증명의 크기가 보이고자 하는 관계의 크기에 로그정도로 줄어들지만, 검증자의 연산이 입력 길이에 선형으로 증가한다는 단점이 있다. 최근에 증명자나 검증자의 연산량은 동일하게 유지하면서 Bulletproofs 보다 더 작은 증명 크기를 갖는 Bulletproofs+[8]가 개발되었다. 복잡도는 로그에 비례하는 증명 크기를 갖지만 실제 실험 결과 현재까지 투명한 초기 설정으로 분류되는 증명기법들 중 가장 작은 증명 크기를 갖는 방법으로 투명한 초기 설정이 중요한 응용에서는 Bulletproofs+와 같은 기법을 사용할 수 있다[8].

4.2.3.2 위수를 모르는 군(Unknown order group)을 사용하는 ZKP 기법

SuperSonic[3]은 위수를 모르는 군을 이용한 ZKP 기법이다. Sonic, PlonK에서 PC로 사용되는 Kate PC 대신 DARK PC를 사용한 ZKP 기법으로 Class 군을 이용한 DARK PC는 order를 알지 못해도 구성할 수 있는 class 군의 성질로 투명한 초기 설정으로 PC의 설계가 가능하다. DARK를 기반으로 사용하기 때문에 검증시간, 증명의 크기가 보이고자 하는 명제에 대응되는 회로 크기의 로그사이즈에 비례한다. 선형적인 검증시간을 가지는 Bulletproofs에 비해 검증시간이 짧은 것이 장점이지만 이때 사용되는 군의 원소 크기가 기존의 타원곡선군보다 크기 때문에 증명의 크기가 Bulletproofs에 비해 6배가량 크다[3]. 더 나아가 지수연산을 군의 위수를 모른 채 진행을 하므로 지수연산을 효율적으로 개선하기 어렵다는 단점이 있다. 프로토콜 내에서 검증자의 지수연산을 증명자에게 위탁하는 과정으로 인해 증명자의 연산량이 많이 소요된다.

4.3 투명한 초기설정이 가능한 ZKP 성능비교

본 논문에서 자세히 다루고 있는 투명한 초기설정 과정을 거치는 영지식 증명 중 URS를 사용하는 기법인 Bulletproofs, 위수를 모르는 군을 사용하는 Supersonic, 충돌저항성 해시를 기반으로 설계된 Virgo에 대한 성능을 [Table 1]에서 비교한다.

Bulletproofs는 입력길이에 대한 로그의 증명크기를 가지며 나머지 두 기법에 비해 증명의 크기가 작다는 장점이 있지만 검증자의 연산량은 입력 길이에 선형으로 비례한다. Supersonic은 검증시간과 증명크기 모두 로그크기로 작은 증명과 빠른 검증시간을 지녔다고 할 수 있다. 하지만 위수를 모르는 군에서의 지수연산이 무겁고, 증명자가 매우 큰 지수연산을 수행하기 때문에 동일한 복잡도를 가진 다른 ZKP와 비교했을 때 상대적으로 검증 및 증명 속도가 느리며 증명자의 연산량이 매우 크다. Virgo는

Table 1. Performance of Transparent ZKPs[3]
λ: a security parameter. n: the input length. $\mathbb{G}_U$, $\mathbb{G}_P$: an element of unknown order group and pairing group of order p each. H: the size of a hash output. E: exponentiation of in the groups.

	Supersonic	BPs	Virgo
Prover	$O(n\log n)$ E	$O(n)$ E	$O(\lambda n)$H
Verifier	$O(\log n)$ E	$O(n)$ E	$O(\lambda\log^2 n)$H
Proof	$O(\log n)\mathbb{G}_U$	$O(\log n)\mathbb{G}_P$	$O(\lambda\log^2 n)$H
$n=2^{20}$	10.1 KB	1.7 KB	271 KB

충돌저항성 해시 함수를 이용하여 양자내성을 지닌다. 해시연산이 지수연산에 비해 빠르기 때문에 검증시간도 빠르지만 안전성을 보장하기 위해서는 LDT 프로토콜의 반복적인 수행이 필요하여 복잡도 자체는 크게 개선되지 못하였다.

V. ZKP의 응용 사례 분석 및 활용방안

5.1 신원증명(Identification)

인터넷의 발전에 따라 온라인 상에서 기업이나 기관들이 제공하는 다양한 서비스를 제공 받기위해서 사용자는 개인, 회사, 자산 등의 여러 신원정보를 온라인에서 인증하고 신원 증명된 다수의 ID와 암호를 관리해야하는 어려움이 있다. 이에 구글, 페이스북, 네이버, 카카오 등의 국내외 대형 인터넷서비스 제공업체들이 타사 로그인에 ID와 기본정보를 제공하는 '오픈 아이디(open ID)' 서비스를 제공하고 있지만 특정 서비스에 개인 정보가 집중되면서 개인정보 유출시 발생할 수 있는 위협은 더욱 커졌다.

2018년 구글플러스 5200만 사용자의 개인정보 유출, 페이스북 5000만 명 개인정보의 해킹으로 인한 유출 사건, 2019년 업비트의 580억원에 이르는 가상 화폐 유출 사건 등 국내외 거대 유명 기업들의 빈번한 개인정보 유출사고가 기업에서도 개인정보 관리로 인해 어려움을 겪고 있다는 것을 암시해준다.

온라인상의 신원증명은 인터넷의 발전과 비대면 방식을 선호하는 사회적 양상에 따라 학문/산업 등 여러 분야에서 많은 관심을 받고 있지만 신원정보를 디지털화 하는 것은 프라이버시 침해 등 여러 문제에 노출되어 법적 문제가 발생할 수 있다. 따라서 개인정보를 보호하면서도 필요에 따라 성인 인증과 같이 특정한 나이 이상이라는 것에 대한 검증을 편리하게 할 수 있는 신원증명 방식의 도입이 필요하다.

분산신원증명을 사용하면 인증서의 발급 기관과 유효기간 및 인증하고자하는 정보만의 유효성 확인을 통해 신원을 검증하는 것이 가능하기 때문에 앞에서 언급한 프라이버시 문제를 해결할 수 있다. 또한 2020년 12월 10일 전자서명법 시행령[24]에 따른 공인인증서 폐지와 관련하여 공인인증서를 대체할 하나의 솔루션으로 분산신원증명에 대한 기업들의 관심이 높아지고 있다. 전 세계적으로 프라이버시를 보호할 수 있는 신원증명방식의 필요성은 중요하게 인식되고 있다. 이에 따라 표준화 방안이 활발히 진행중에 있으며 [Table 2]는 분산신원증명과 관련된 표준화 현황 및 주요 표준화 참여 기관들에 대해 간략히 정리한 표이다. W3C(World Wide Web Consortium)가 채택한 분산신원증명의 표준안에서는 검증 가능한 인증서 모델을 설계하기 위해서 적용할 수 있는 암호 기법으로 ZKP 적용을 명시[21]하고 있다. 이번 절에서는 관련한 분산신원증명의 표준안을 중심으로 ZKP의 활용 방안에 대해 분석한다.

Table 2. Decentralized Identity Related Standardization

Name of institution	Logo	Contents of participation in standardization
World Wide Web Consortium	W3C	Formating of DID and ID management, Definition of verifiable credential formal, digital signature
Organization for the Advancement of Structured Information Standards	OASIS	Managing distributed key
Decentralized Identity Foundation	DIF	Interface of web browser, Mobile devices

5.1.1 분산신원(Decentralized Identity)

분산신원증명은 개인의 신원인증 및 자격증명을

특정한 중개기관 없이 수행하는 신원증명 방법이며 사용자가 서비스 제공기관에게 신원을 증명하고자 할 때 사용될 수 있다. 분산신원증명의 과정은 다음과 같다.[9,10,15] 사용자가 서비스 제공기관으로부터 개인 정보에 관한 인증을 요청 받으면 해당 내용을 인증해 줄 수 있는 기관에게 검증 가능한 증명서 발행을 요청한다. 발급기관은 사용자가 해당 권한을 가지고 있는지 여부를 확인 후 사용자에게 인증서를 발행하고 발행내역 사항을 검증 가능한 데이터 저장소에 발행기관의 서명(sign)과 함께 등록한다. 이후, 사용자는 발급받은 인증서에 대해 자신의 서명을 수행하여 검증 가능한 데이터 저장소에 이를 등록한다. 마지막으로 검증단계에서 ZKP가 사용되는데 ZKP스킴을 통해 검증자는 사용자가 제공한 증명서가 인증하고자하는 정보에 대한 증명서라는 것과 저장소에 서명한 비밀키(private key)가 사용자 소유임을 확인이 가능하므로 검증기관은 발행기관으로 부터의 증명서의 진위여부와 사용자가 해당 증명서의 소유권을 가지고 있음을 검증 가능하다.

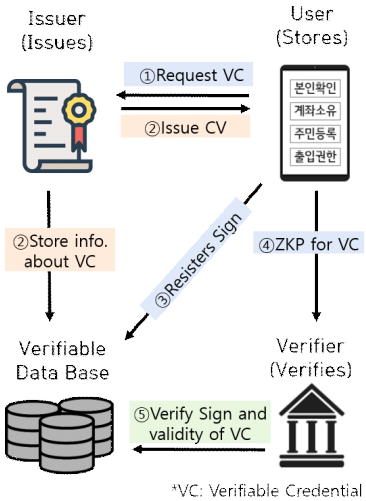

Fig. 1. Application of ZKP : Verifiable Credentials Data Model

5.1.2 분산신원증명을 위한 ZKP

분산신원증명에서 중개기관을 두고 개인정보를 보관하지 않으므로 데이터 프라이버시 측면에서 확연한 이점이 있다. 또한 검증 가능한 데이터 저장소로 블록체인구조를 활용하면 인증서 발급 내역들에 대한 무결성을 보장받을 수 있고 사용자는 한번만 인증서를 발급받고 그 이후에는 스스로가 ZKP로 자신의 신원을 인증하는 것이 가능해진다. 최근 ZKP연구 결과들은 흔히 증명자의 연산량이 충분하고 검증자의 연산량이 제한된 상황에서 설계되어 검증자의 연산량을 줄이고자 하는 목표를 중시한다. 하지만 위 와 같은 시나리오에서 사용자는 증명자가 되고 검증기관은 검증자가 되어 ZKP를 수행해야한다. 따라서 개인 사용자가 스마트폰과 같은 단말 기기에서도 빠르게 증명을 생성해 낼 수 있도록 증명자의 연산량이 적은 ZKP에 대한 연구가 이루어져야 한다. 또한 투명한 초기 설정으로 설계가 가능한 ZKP를 사용하는 것이 별도의 신뢰대상을 제거하고자 하던 원래의 취지와 부합할 것이므로 결국 투명한 초기 설정이 가능하고 증명자의 연산량이 적게 필요한 ZKP의 연구가 분산신원증명의 실용화를 가속화 시킬 수 있다.

5.2 딥러닝 (Deep Learning)

최근 컴퓨터의 연산 능력과 GPU를 이용한 병렬처리 기법 등의 발전으로 다량의 연산을 필요로 했던 인공지능의 한 분야인 딥러닝이 현실적으로 구현하고 실행할 수 있는 수준을 이루면서 크게 각광받고 있다. 거의 모든 학문에 딥러닝을 적용시킬 수 있을 정도로 딥러닝으로 해결할 수 있는 작업의 종류는 다양하지만 본 절에서는 그 중 비교적 간단한 작업에 속하는 이미지 분류를 위한 신경망 모델에 대해 서술하여 연산 검증에 대한 ZK에 초점을 맞추고자 한다.

이미지 분류를 위한 신경망에 대한 딥러닝은 구성된 모델의 파라미터를 찾는 트레이닝 과정과 찾은 파라미터에 대해서 실제 이미지 분류 작업을 수행하는 인퍼런스 과정으로 나뉜다. 이때 트레이닝과 인퍼런스 과정은 계산비용이 상당한데 높은 정확도의 이미지 분류를 잘 수행해 내는 모델을 찾기 위해서는 다량의 데이터에 대한 방대한 양의 반복연산이 필요한 트레이닝 과정을 거쳐야하므로 막대한 자원이 요구된다. 이를 위한 솔루션으로 정확도가 높게 트레이닝된 모델을 이용해서 인퍼런스를 수행해주는 클라우드의 위임연산이 가능하다. 그러한 서비스의 예로는 Amazon의 Amazon ML, Microsoft의 Azure ML, IBM의 Watson 그리고 Google의 Cloud ML등이 있으며 이들은 소유한 딥러닝 모델에 인퍼

런스 결과를 돌려주거나 딥러닝을 수행할 수 있는 저장 공간 및 연산환경을 제공해준다.

이러한 서비스를 이용할 때 사용자 입장에서는 서비스 제공업체가 제대로 된 트레이닝을 수행한 모델을 가지고 있는지, 사용자가 요청한 데이터를 입력으로해서 정상적인 인퍼런스 과정을 수행했는지에 대한 검증을 요구할 것이고 서비스 제공업체 입장에서는 자신들이 보유한 모델을 비공개로 유지하고 싶을 것이다. 이 때, 적용 가능한 암호학적 기법이 ZKP이며, 본 장에서 딥러닝 모델의 인퍼런스 과정에 대한 무결성을 안전하게 검증할 수 있는 ZKP를 위해 적용된 기존 기법들을 분석한다.

5.2.1 신경망 모델 연산의 무결성 증명

딥러닝 프라이버시를 다루는 기존 연구 중 인퍼런스에 대한 무결성을 위해 상호증명을 적용한 첫 번째 연구는 SafetyNet[23]이며, 클라우드 서버가 사용자를 위해 신경망 모델의 인퍼런스를 수행한 뒤 결과와 함께 모델에 대한 연산을 제대로 수행했음을 검증 가능한 증명을 제시하게 되고, 사용자는 결과에 대한 검증이 가능하다. 위임 연산을 위한 암호프로토콜을 신경망 모델에 대한 연산 검증에 곧 바로 적용하여 사용할 수 없는데, 그 이유는 크게 두 가지로 첫 번째 이유는 암호학적 기법들은 정수 상에서 설계되지만 신경망모델은 실수 상에서의 연산을 수행하기 때문이고, 두 번째는 임의의 연산 수행을 검증 가능한 암호 프로토콜의 효율적인 설계가 어렵기 때문이다. SafetyNet은 이전의 연구결과[17]를 따라서 이러한 한계점 들을 해결하며 그 대응은 다음과 같다.

첫 번째 문제의 해결방안으로 트레이닝 과정은 실수상의 연산들로 수행하고 이 과정을 통해 찾은 모델의 파라미터들에 충분히 큰 수를 곱하고 라운딩을 하여 정수 상에서 인퍼런스를 수행한다. 두 번째 문제의 해결방안으로 암호 프로토콜의 효율적인 설계가 가능한 산술연산으로 모델을 표현하는 방식을 채택한다. 모델 구성에 포함된 연산이 산술 연산으로 쉽게 표현하기 어려운 경우, 정확도를 크게 떨어뜨리지 않는 한에서 산술회로로 표현 가능한 다른 연산을 적용시킨다. 최종적으로 얻는 신경망 모델은 정수들 간의 산술연산으로 이루어지며 신경망에 데이터를 입력으로 할 때 연산들을 모두 행렬의 곱의 꼴로 표현하여 행렬 곱에 대한 위임 연산을 효율적으로 검증하는 프로토콜을 적용한다[13].

신경망 모델에서 수행되는 모든 연산들을 행렬로 표현 가능하다고 가정하자. 28x28크기의 이미지 데이터를 784x1형태의 벡터로 입력받고 배치의 크기는 b라고 하면 784xb의 행렬이 신경망의 입력이 된다. 입력 데이터에 5x5 컨볼루션 연산을 수행하는 연산은 [Fig 2]의 ①과 같은 행렬 곱으로 표현 할 수 있고 액티베이션으로 제곱 함수를 이용한다면 ② 산술연산만으로 관계를 나타낼 수 있다. 검증과정은 out에서 in 방향으로 진행되며 [Fig 2]의 경우에는 총 5단계를 거쳐서 행렬 곱 연산을 검증하게 된다.

이 때, 신경망의 인퍼런스 수행시 모델의 입력 크기 n, 입력 데이터와의 행렬 곱으로 표현되는 뉴런의 개수 k, 출력 크기 m에 대하여 증명 생성에 필요한 연산량, 검증시 소요되는 연산량과 증명의 크기 모두는 $O(nk+m)$에 비례하는 복잡도를 가지며 신경망의 인퍼런스에 대한 무결성 검증에 초점을 맞춘 첫 번째 연구 결과라는 것에 의의가 있으나, 신경망 연산의 중간 값 이외의 파라미터로 수행하게 되는 연산을 검증자가 직접 수행함으로써 검증시간이 늘어나며 검증자가 모델에 대한 파라미터를 알고 있다는 가정으로 인해 신경망 모델에 대한 프라이버시를 제공하지 못한다는 한계를 가지고 있다.

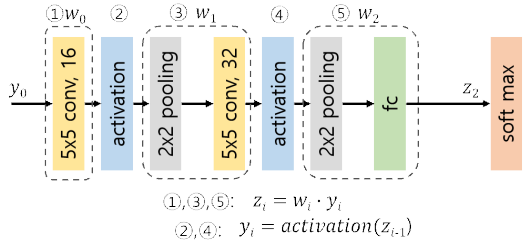

Fig. 2. SafetyNet for MNIST dataset

5.2.2 신경망 모델 연산의 ZKP

SafetyNet은 신경망 구조를 변형하는 방법을 택하여 암호학적 무결성 검증 프로토콜을 도입하였다. 이때 행렬에 대한 행과 열에 관한 정보를 입력으로 받아서 행렬의 각 성분에 대응시켜주는 다항식을 사용하였는데, 여기에 영지식성을 추가하는 가장 간단한 방법은 다음과 같다. 다항식에 대한 정보가 곧 신경망 모델의 파라미터 정보에 직결되므로 검증자가 다항식에 대한 정보를 얻을 수 없도록 하는 것을 목표로 영지식성을 만족하는 PC를 도입할 수 있다. 검

증자가 검증할 때 얻게 되는 다항식의 일부 정보들을 가리기 위한 랜덤 다항식 또한 PC를 이용해 미리 커밋해 두어 검증시 정보누출을 막을 수 있다. 여기서 도입하는 PC의 기반 가정들에 따라서 전체 프로토콜이 만족하게 되는 성질이 결정되므로 다양한 형태의 PC와 결합하여 각 응용 환경에 적합한 ZKP를 설계할 수 있을 것이다.

딥러닝은 현재 급격한 발전을 이루면서 막대한 양의 연구 결과들이 쏟아지고 있는 반면 딥러닝 모델에 대한 프라이버시와 무결성을 위한 연구는 상대적으로 연구가 활발하게 이루어지고 있지는 않은데, 향후 딥러닝이 실제 특정한 응용들에 대해 서비스화 되기 위해서 반드시 선행되어야 하는 연구 주제이다. 본 고에서 서술한 신경망 모델에 대한 연산 검증방법은 ZKP를 적용할 수 있도록 신경망 모델을 변형시킨 것이다. 그러나 추후 더 생각할 수 있는 연구 과제들로는 신경망 모델에서 사용되는 연산에 특화된 ZKP의 설계, 실수연산 검증에 특화된 ZKP 및 트레이닝 과정에 대한 효율적인 ZKP의 설계 등이 있으며 ZKP의 발전과 함께 더불어 발전 할 수 있는 핵심적인 응용 분야라 전망한다.

VI. 결 론

본 논문에서는 ZKP가 응용될 수 있는 각 상황마다 필요한 성질을 가지는 프로토콜의 설계를 위해 사용되는 설계기법들에 대해서 기술하며 연구의 진행 흐름 및 중요도를 파악할 수 있도록 하였다. 또한, ZKP의 중요한 빌딩블록으로 사용되는 PC의 일반적인 정의 및 그 원리에 대해서 분석을 하고 실제 제안된 구체적인 PC에 대해 다루었다. 여러 연구 결과들에서 보여주듯이 투명성을 만족하고 초기설정이 가능한 PC로 해당 성질을 만족하는 ZKP의 설계가 가능한데[3,4,12], 기존 PC의 성질을 정확하게 파악하고 그 성질을 분석하여 발전시키는 것이 더욱 향상된 ZKP 설계에 있어서 핵심적인 역할을 할 것으로 보여진다. 특히 향후 양자컴퓨터의 실용화를 대비, 양자내성을 지닌 효율적인 PC를 설계하는 연구가 필요하다.

세계적인 암호연구의 흐름에서 ZKP는 현재 전성기를 맞고 있다는 표현이 과하지 않을 만큼 그 이론적인 연구 뿐 아니라 분산신원증명, 검증 가능한 머신러닝 등 구체적이고 실질적인 응용을 위한 설계 및 그 개발 도구 등 다방면으로 수많은 연구들이 진행되고 있다.

현재 ZKP가 많은 관심을 받으면서 활발하게 연구가 진행되는 것은 ZKP가 다른 많은 응용에 활용될 수 있기 때문이기도 하지만 점점 더 데이터의 중요성이 강조되고 개인정보보호 관련 이슈들이 주목받게 된 결과이며, 앞으로는 더욱 다양한 분야의 업종의 많은 기업들이 ZKP에 관심을 가질 것이다. 연구 발전이 기대 되는 분야 인만큼 국내에서도 해당 분야에 대한 기초 연구에 대한 이해 및 관심이 필요하다.

References

[1] A. Gabizon, Z.J. Williamson and O. Ciobotaru. "PlonK: permutations over Lagrange-bases for oecumenical noninteractive arguments of knowledge." IACR Cryptol. ePrint Arch, 2019, 953. Dec. 2019.

[2] A. Kate, G.M. Zaverucha and I. Goldberg, "Constant-size commitments to polynomials and their applications." Proceedings of the ASIACRYPT 2010, vol. 6477, pp. 177-194, Dec. 2010.

[3] B. Bünz, B. Fisch and A. Szepieniec "Transparent SNARKs from DARK compilers," Proceedings of the EUROCRYPT 2020. vol. 12105, pp. 677-706, May. 2020.

[4] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: short proofs for confidential transactions and more." Proceedings of the IEEE Symposium on Security and Privacy 2018, pp. 315-334, May. 2018.

[5] B. Libert, S. Ling, K. Nguyen and H. Wang, "Lattice-based zero-knowledge arguments for integer relations," Proceedings of the CRYPTO 2018, vol. 10992, pp. 700-732, Aug. 2018.

[6] E. Ben-Sasson, I. Bentov, Y. Horesh and M. Riabzev. "Fast Reed-Solomon interactive oracle proofs of proximity," In International Colloquium on Automata, Languages, and Programming 2018, vol. 107, pp. 14:1-14:17, Jul. 2018.

[7] E. Ben-sasson, I. Bentov, Y. Horesh

and M. Riabzev, “Scalable zero knowledge with no trusted setup,” Proceedings of the CRYPTO 2019, vol. 11694, pp. 701-732, Aug. 2019.
[8] H. Chung, K. Han, C. Ju, M. Kim and J.H. Seo, “Bulletproofs+: shorter proofs for privacy-enhanced distributed ledger,” IACR Cryptol. ePrint Arch, 2020, 735. May. 2020.
[9] J. Camenisch and A. Lysyanskaya, “Signature schemes and anonymous credentials from bilinear maps,” Proceedings of the CRYPTO 2004, vol.3152, pp. 56-72, Aug. 2004.
[10] J. Camenisch, M. Drijvers and A. Lehmann, “Anonymous attestation using the strong diffie hellman assumption revisited.” Proceedings of the International Conference on Trust and Trustworthy Computing 2016, vol.9824, pp. 1-20, Aug. 2016.
[11] J. Groth. “On the size of pairing-based non-interactive arguments.” Proceedings of the Eurocrypt 2016, vol. 9666, pp. 305-326, May. 2016.
[12] J. Groth, M. Kohlweiss, M. Maller, S. Meiklejohn and I. Miers, “Updatable and universal common reference strings with applications to zk-SNARKs,” Proceedings of the CRYPTO 2018, vol. 10993, pp. 698-728, Aug. 2018.
[13] J. Thaler, “Time-optimal interactive proofs for circuit evaluation.” Proceedings of the CRYPTO 2013, vol. 8043, pp. 71-89, Aug. 2013.
[14] J. Zhang, T. Xie, Y. Zhang, and D. Song, “Transparent polynomial delegation and its applications to zero knowledge proof” Proceedings of the IEEE Symposium on Security and Privacy 2020, pp. 859-876, May. 2020.
[15] M.H. Au, W. Susilo, Y. Mu, “Constant-size dynamic k-TAA.” Proceedings of the International Conference on Security and Cryptography for Networks 2006, vol. 4116, pp. 111-125, Sep. 2006.
[16] M. Maller, S. Bowe, M. Kohlweiss, and S. Meiklejohn. “Sonic: zero-knowledge SNARKs from linear-size universal and updatable structured reference strings,” Proceedings of the ACM SIGSAC Conference on Computer and Communications Security Association for Computing Machinery 2019, pp. 2111 - 2128, Nov. 2019
[17] R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter, M. Naehrig and J. Wernsing, “Cryptonets:applying neural networks to encrypted data with high throughput and accuracy.” Proceedings of the International Conference on Machine Learning 2016, vol. 48, pp. 201-210, Jun. 2016.
[18] R.S. Wahby, I. Tzialla, A. Shelat, J. Thaler and Walfish, M. “Doubly-efficient zkSNARKs without trusted setup,” Proceedings of the IEEE Symposium on Security and Privacy 2018, pp. 926-943, May. 2018.
[19] S. Bowe, A. Gabizon and I. Miers, “Scalable multi-party computation for zk-SNARK parameters in the random beacon model,” IACR Cryptol. ePrint Arch, 2017, 1050. Oct. 2017
[20] S. Goldwasser, S. Micali and C. Rackoff, "The knowledge complexity of interactive proof systems,“, Proceddings of the ACM Symposium on Theory of Computing, pp. 291-304, May 1985.
[21] W3C, “Decentralized Identifiers(DIDs)”, https://www.w3.org/TR/did-core/, Jun. 2021.
[22] Y. Oren, “On the cunning power of cheating verifiers: some observations about zero knowledge proofs,” Proceedings of the Symposium on Foundations of Computer Science 1987, pp. 462-471, Oct. 1987.
[23] Z. Ghodsi, T. Gu, and S. Garg,“ Safetynets: verifiable execution of deep neural networks on an untrusted cloud.” Proceedings of the Advances in Neural Information Processing Systems 2017, pp. 4672-4681, Jun. 2017.

[24] Presidential Decree No. 31222, "Enforcement Decree of the Electronic Signature Act[2020. 12. 10.]" https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%84%EC%9E%90%EC%84%9C%EB%AA%85%EB%B2%95%EC%8B%9C%ED%96%89%EB%A0%B9, Dec. 2020.

〈저자소개〉

주 찬 양 (Chanyang Ju) 종신회원
2018년 2월: 명지대학교 수학과 학사
2018년 2월~현재: 한양대학교 수학과 암호론 석·박사통합과정
〈관심분야〉 암호론, 검증 가능한 연산

이 현 범 (Hyeonbum Lee) 종신회원
2018년 2월: 한양대학교 수학과 학사
2020년 2월~현재: 한양대학교 수학과 암호론 석·박사통합과정
〈관심분야〉 암호론, 부호이론

정 희 원 (Heewon Chung) 종신회원
2010년 8월: 한국과학기술연구원(KAIST) 수학과 학사
2013년 8월: 서울대학교 수학과 암호론 석사
2017년 8월: 서울대학교 수학과 암호론 박사
2018년 2월~2019년 7월: KT 블록체인 센터
2019년 8월~2020년 2월: MEDIUM 암호연구팀
2020년 4월~현재: 한양대학교 Post-Doc
〈관심분야〉 암호론, 블록체인

서 재 홍 (Jae Hong Seo) 종신회원
2004년 2월: 고려대학교 수학과 학사
2011년 2월: 서울대학교 수학과 암호론 박사
2011년~2012년: NICT, Japan
2013년~2017년: 명지대학교 수학과 조교수
2018년~현재: 한양대학교 수학과 부교수
〈관심분야〉 암호론, 계산수론, 정보이론