지혜콘텐츠 공동저작권 보호에 적합한 블록체인 기반 부인봉쇄 다중서명 기법

윤성현
백석대학교 컴퓨터공학부 교수

The Blockchain based Undeniable Multi-Signature Scheme for Protection of Multiple Authorship on Wisdom Contents

Sunghyun Yun
Professor, Division of Computer Engineering, BaekSeok University

요 약 지혜콘텐츠는 여러 사람들의 경험과 아이디어로 창작되고 지역 제한이 없는 인터넷 기반 소셜 플랫폼에서 소비된다. 기존의 저작권 등록 시스템은 전문 제작자를 대상으로 하고 있으며 그 효력은 해당 국가에 종속된다. 블록체인은 서비스에 종속적이고 P2P 네트워크를 구성하는 노드들의 합의에 의해서 수정 및 삭제할 수 없는 데이터가 저장된다. 본 논문에서는 소셜 플랫폼에서 사용되는 지혜콘텐츠의 공동저작권 보호에 적합한 블록체인 기반의 부인봉쇄 다중서명 기법을 제안한다. 제안한 기법은 공동저작자들의 공통키 생성, 다중서명 생성 및 검증 프로토콜로 구성된다. 부인봉쇄 서명은 서명자의 도움 없이는 서명을 검증할 수 없는 기법이다. 제안한 기법은 콘텐츠 구매 프로토콜에 적용되어 자동화된 수익분배를 가능하게 한다. 블록체인 기반 다중서명 검증을 통해서 모든 공동저작자들은 수익분배의 공정성을 부인할 수 없다.

주제어 : 블록체인, 저작권 보호, 다중 서명, 공동 저작권, 스마트계약

Abstract Wisdom Contents are created with experiences and ideas of multiple authors, and consumed in Internet based Social Network Services that are not subjected to regional restrictions. Existing copyright management systems are designed for the protection of professional authors' rights, and effective in domestic area. On the contrary, the blockchain protocol is subjected to the service and the block is added by the consensus of participating nodes. If the data is stored to the blockchain, it cannot be modified or deleted. In this paper, we propose the blockchain based undeniable multi-signature scheme for the protection of multiple authorship on Wizdom Contents. The proposed scheme is consisted of co-authors' common public key generation, multi-signature generation and verification protocols. In the undeniable signature scheme, the signature cannot be verified without help of the signer. The proposed scheme is best suited to the contents purchase protocol. All co-authors cannot deny the fairness of the automated profit distribution through the verification of multiple authorship on Wizdom Contents.

Key Words : Blockchain, Copyright Protection, Multi-Signature, Joint Copyright, Smart Contract

본 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(2018R1D1A3B07050180)
*교신저자 : 윤성현(shcrpt@gmail.com)
접수일 2021년 4월 15일 수정일 2021년 5월 22일 심사완료일 2021년 5월 26일

1. 서론

디지털 콘텐츠는 전문 저작자에 의해서 제작되는 전문 콘텐츠와 유투브, 블로그 등에 게시되는 일반인들의 창작 콘텐츠로 구분된다. 지혜콘텐츠는 일반인들의 경험과 아이디어로 만들어지는 창작 콘텐츠이다 [1].

공동 저작권은 여러 사람의 협업으로 만들어진 콘텐츠에 대한 공동 권리를 의미한다. 주저작자와 공동저작자의 권리는 기여도에 따라서 권리의 비율이 달라진다. 상용 콘텐츠일 경우에 이 비율은 수익 분배의 주요 지표가 된다 [1, 2].

전문 콘텐츠는 기존의 저작권 관리 시스템을 통해서 저작권을 등록하고 법적 분쟁이 발생하였을 경우에 법원을 통해서 이를 해결한다 [3]. 지혜 콘텐츠는 인터넷 기반의 소셜 커뮤니티에서 소비되는 일반인들이 만든 창작 콘텐츠이다. 인터넷 기반 소셜 플랫폼은 지역 제한이 없기 때문에 지혜 콘텐츠 저작권은 지역적 제한을 받지 않는다.

기존 저작권 보호 시스템에서 저작권 등록 및 관리는 국가가 지정한 저작권 관리 위원회를 통해서 이루어지기 때문에, 관련 분쟁 발생 시 법원에서의 조정이 가능하다 [3]. 하지만 지혜콘텐츠는 인터넷 기반이기 때문에 기존 시스템을 이용하더라도 국외에서 발생하는 저작권 침해에 대해서는 보호받지 못한다.

따라서, 지혜콘텐츠 보호를 위해서는 기존 저작권 보호 시스템과 같이 법적 효력을 갖는 새로운 저작권 관리 플랫폼의 개발이 필수적이며 다음 요구사항을 만족해야 한다.

요구사항 1. 콘텐츠 저작권의 범위는 국가나 특정 지역에 제한되지 않고 관련 콘텐츠를 소비하는 인터넷 커뮤니티에 종속되어야 한다.

요구사항 2. 저작권료에 대한 수익 분배는 스마트계약에 따라서 자동으로 집행되고, 이에 대해서 저작자들은 그 공정성을 부인할 수 없어야 한다.

지역적 제한이 없는 지혜콘텐츠의 경우는 법원을 통한 분쟁 해결이 어렵기 때문에, 분쟁이 발생할 수 없도록 사전에 동의된 자동화된 계약 모델을 만들고 적용해야 한다. 커뮤니티 구성원이 이 계약 모델을 신뢰할 수 있으면 쟁의 조정을 위한 기존 법원의 역할을 대체할 수 있다. 따라서, 지혜콘텐츠를 위한 저작권 보호 모델에 블록체인 기술의 접목은 필수적이다.

본 논문에서는 지혜콘텐츠에 적합한 블록체인 기반의 부인봉쇄 다중서명 기법을 제안한다. 제안한 기법은 공동저작권 보호 및 수익분배 프로토콜에 적용될 수 있다.

공동저작권 등록 모듈은 공동저작자의 공통 공개키 생성, 다중서명 생성 및 검증 프로토콜로 구성된다. 다중서명 검증은 모든 서명자의 동의 없이는 서명 검증을 할 수 없는 All-or-Nothing 유형의 서명 검증 기법을 사용한다 [4, 5].

공동저작자는 지혜콘텐츠, 저작권 비율 등이 포함된 컨테이너 파일을 서명함으로써 해당 콘텐츠에 대한 공동권리를 갖게 된다. 블록체인의 특성상 한 번 등록된 공동저작권 데이터는 제 3자에 의한 위조 및 삭제가 불가능하다. 도전-응답 방식의 다중서명 검증은 모든 공동저작자들이 블록체인에 등록된 공동저작권에 대해서 부인할 수 없도록 한다.

수익분배 모듈에서는 블록체인에 저장된 각 저작자의 비율에 맞게 자동으로 수익을 분배한다. 스마트계약은 블록체인에 저장되기 때문에 계약 이행의 절차 및 결과를 누구나 확인할 수 있고, 스마트계약 코드를 조작 및 삭제하는 것은 불가능하다 [6, 7].

2. 관련 연구

PKI(Public Key Infrastructure)는 국가가 지정한 공인인증기관에서 사용자의 공개키를 인증한 인증서를 발급해 주는 체계이다 [8]. 인증서 기반으로 디지털 계약을 서명하면 해당 계약은 법적 효력을 갖게 된다. 따라서, 법적 근거가 필요한 다양한 인터넷 서비스에서 사용된다 [9]. 단점은 법적 효력의 범위가 국내로 한정된다는 것이다.

퍼블릭 블록체인에 저장되는 데이터는 국가가 보증하는 것이 아니고 자동화된 블록체인 프로토콜에 의해서 데이터의 무결성이 보장된다. 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.

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 [10].

현행법상 콘텐츠에 대한 저작권을 보호받기 위해서는 저작물을 '한국저작권관리위원회'에 등록해야 한다 [3].

현행 저작권 등록 시스템은 등록신청, 등록심사, 등록 3단계로 진행된다. 저작권 등록을 위해 등록담당자가 필요하고, 저작권 등록 처리 기간이 길어서 시간적 제약이 따른다 [3]. 또한, 현행 시스템은 저작물 창작이 완료되어야만 등록이 가능하고, 추후 권리변동 발생 시 진정한 저작자가 누구인지 파악하는 데에 어려움이 있다 [11]. 블록체인 기반 저작권 관리의 선행 연구에서는 저작권관리위원회의 관리 독점 해소, 저작물 위·변조 방지가 핵심 기술로 제안되었다 [12]. 이 연구에서 저작권 등록·관리의 편의성 및 신뢰성은 확보할 수 있었지만 공동저작권 보호 및 수익분배 프로토콜로의 확장이 쉽지 않은 단점 또한 존재한다.

공동 저작권은 저작물에 대해서 여러 사람의 권리를 표현한 것이다. 디지털 다중서명 기법은 한 문서에 대해서 여러 사람이 서명하는 것으로 RSA 및 이산대수 문제에 근거한 많은 다중서명 기법이 제안되었다 [13]. 일반 다중서명 기법은 콘텐츠 거래 모델에서 판매자와 서명자의 공모 공격에 취약하기 때문에 서명자가 검증에 참여할 수 있는 부인봉쇄 서명 기법과 블록체인 기술의 적용이 필요하다 [5, 14].

기존 서버 기반 상거래 방식에서는 판매자가 판매 수량을 속이거나 또는 저작자와의 공모를 통해서 수익 분배를 조작하는 공격이 가능하다. 하지만 블록체인 기반으로 결제를 하게 되면, 저작자들의 다중서명 검증이 되어야 콘텐츠 거래가 이루어지고, 이 기록은 블록체인에 저장되기 때문에, 판매자의 부정을 최소화 할 수 있다.

본 논문에서는 공동저작자가 모두 동의해야만 서명 검증을 할 수 있는 블록체인 기반의 부인봉쇄 다중서명 기법을 제안한다. 저작권 보호 및 수익분배 모듈로 구성된 스마트계약 프로그램을 신뢰할 수 있으면, 제 3자의 도움 없이 저작권 분쟁을 최소화하고 공정한 수익 분배를 보장할 수 있다.

3. 제안한 모델

본 논문에서는 지혜콘텐츠 공동저작권 등록 및 검증에 적합한 부인봉쇄 다중서명 기법과 블록체인 기반의 자동화된 스마트계약 모델을 제안한다. 제안한 기법은 공동저작권 등록을 위한 공통키 생성, 다중서명 생성 및 검증 프로토콜 그리고 이를 적용한 수익분배 모델로 구성된다.

3.1 공동저작권 등록 및 검증 프로토콜

정의 1. GF(p)는 암호학적으로 안전한 유한체이고 g는 GF(p) 상에서 정의된 생성자로 위수 p-1을 갖는다 [15].

가정 1. 지혜콘텐츠에 대한 공동저작권 등록 및 검증 프로토콜에 필요한 구성요소는 다음과 같이 정의한다. 공동저작자의 수는 n+1 명이라고 가정한다.

- WizContents : 공동저작한 지혜콘텐츠
- WizContract : 저작권 등록, 검증, 수익분배 모듈로 구성된 스마트계약 [7, 14]
- A_0 : 주저작자
- $A_C = \{A_0, A_1, A_2, \ldots, A_n\}$: 공동저작자 그룹
- $sk_i < p$, i=[0..n] : A_i의 개인키
- $pk_i \equiv g^{sk_i} \bmod p$, i=[0..n] : A_i의 공개키
- V : 검증자
- vAddr : V의 EOA 주소

가정 2. WizContract의 매핑 테이블에 저장되는 지혜콘텐츠 공동저작권 및 저작자 정보는 다음과 같이 정의한다.

```
struct AuthorList = {
    address co_author[];
    uint sig[];
    uint share[];
}

struct WizContents = {
    byte32 h_c;
    uint R, Y;
    uint multi_sig;
    AuthorList author;
    address next;
}

struct VerifyMultisig {
    uint32 challenge;
    uint32 response;
    address next;
}

WizContents wizContents;
mapping (address => VerifyMultisig) vMulSig[];
```

가정 3. WizContract에서 지혜콘텐츠 등록, 검증 및 수익분배를 담당하는 함수는 다음과 같이 정의한다.

- register_author() : 공동저작자 등록
- register_contents() : wizContents 등록
- get_pubkey() : 공통 공개키 (R, Y) 리턴
- update_pubkey() : 공통 공개키 (R, Y) 업데이트
- sign_contents() : wizContents 서명
- gen_group_sig() : wizContents 다중서명 생성
- gen_challenge() : 검증자의 도전 값 생성
- gen_response() : 공동저작자의 응답 생성
- verify_multisig() : 다중서명 검증
- purchase_contents() : 콘텐츠 구매 및 대금 분배

단계 1: 공통 공개키 생성

단계 1.1: A_C는 wizContents에 대한 저작권 비율을 합의한다. A_0는 WizContract의 register_author() 함수를 호출하여 공동저작자의 주소와 저작권 비율을 다음과 같이 저장한다.

wizContents.author.co_author[i] = A_i의 주소

wizContents.author.share[i] = A_i의 지분

단계 1.2: A_0는 wizContents를 해쉬 한다. p-1과 서로소인 임의의 난수 k_0를 선택하여 R_0를 생성하고 자신의 공개키로 다음과 같이 Y_0를 만든다. H()는 해쉬 함수로 keccak256() 함수를 사용한다 [7].

hc = H(wizContents)

$$R_0 \equiv hc^{k_0} \bmod p \ , \ Y_0 \equiv g^{sk_0} \bmod p$$

단계 1.3: A_0는 WizContract의 register_contents() 함수를 호출하여 wizContents를 다음과 같이 초기화 한다.

wizContents.h_c = hc

wizContents.R = R_0, wizContents.Y = Y_0

wizContents.next = A_1의 주소

단계 1.4: A_i는(i=[1..n]) wizContents.next에 저장된 주소를 확인하고, 본인 순서이면 get_pubkey() 함수를 호출하여 (R, Y)를 가져온다.

R = wizContents.R, Y = wizContents.Y

단계 1.5: A_i는 다음과 같이 (R_i, Y_i)를 생성하고 update_pubkey() 함수를 호출하여 wizContents.R과 wizContents.Y를 업데이트 한다. update_pubkey() 함수는 wizContents.next를 다음 순번인 A_{i+1}의 주소로 업데이트 한다.

$$R_i \equiv R^{k_i} \bmod p, \ Y_i \equiv Y^{sk_i} \bmod p$$

wizContents.R = R, wizContents.Y = Y

wizContents.next = A_{i+1}의 주소

공동저작자 모두가 공통 공개키 생성에 참여하도록 단계 1.4와 단계 1.5를 반복한다. A_i가 마지막 저작자인 경우에 wizContents.next를 WizContract의 주소로 설정한다.

$$R \equiv hc^{\prod_{i=0}^{n} k_i} \bmod p, \ Y \equiv g^{\prod_{i=0}^{n} sk_i} \bmod p$$

wizContents.next = WizContract의 주소

get_pubkey() 함수와 update_pubkey() 함수는 wizContents.next에 저장된 주소에서만 접근할 수 있다. wizContents.next가 WizContract 주소를 가리키면 공통키 생성이 완료되었음을 의미하고, 해당 함수는 더 이상 실행되지 않도록 한다.

단계 2: 그룹 서명 생성

단계 2.1: A_i(i=[0..n])는 sign_contents() 함수를 호출하여 WizContents 저작권에 대한 부인봉쇄 서명을 한다. k_i와 p-1은 서로소이기 때문에 다음 서명식을 만족하는 sig_i가 존재한다 [10].

$$k_i \cdot sig_i \ \equiv \ sk_i \cdot R \ - \ k_i \cdot hc \bmod p-1$$

wizContents.author.sig[i] = sig_i

단계 2.2: A_0는 gen_group_sig() 함수를 호출하여 그룹서명 SIG를 생성한다. gen_group_sig() 함수는 단계 2.1에서 생성된 공동저작자의 서명이 모두 저장되어 있어야만 실행된다.

sig_i = wizContents.author.sig[i], i=[0..n]

$$SIG \equiv \prod_{i=0}^{n} (hc + sig_i) \bmod p$$

단계 3: 그룹서명 검증

단계 3.1: V는 임의의 두 난수 (a, b)를 선택하여 gen_challenge() 함수를 호출한다. gen_challenge() 함수는 다음과 같이 ch를 생성한다.

$$ch \equiv R^{SIG \cdot a} \cdot Y^{R^n \cdot b} \bmod p$$

vMulSig[vAddr].challenge = ch

vMulSig[vAddr].next = A_0

단계 3.2: A_i(i=[0..n])는 ch에 대한 응답 rp_i를 생성하고 gen_response() 함수를 호출하여 다음과 같이 매핑 테이블을 업데이트 한다.

$$rp_0 \equiv ch^{sk_0^{-1}} \bmod p, \ A_0$$

$$rp_i \equiv rp_{i-1}^{sk_i^{-1}} \bmod p, \ A_i \ (i=[1..n])$$

vMulSig[vAddr].response = rp_i

vMulSig[vAddr].next = A_{i+1}

모든 저작자가 서명 검증에 참여하도록 단계 3.2를 반복한다. A_n은 vMulSig[vAddr].next를 WizContract의 주소로 설정한다.

$$rp_n \equiv ch^{sk_n^{-1}} \equiv ch^{\prod_{i=0}^{n} sk_i} \mod p$$

vMulSig[vAddr].response = rp_n

vMulSig[vAddr].next = WizContract의 주소

gen_response() 함수는 vMulSig[vAddr].next에 저장된 주소에서만 접근할 수 있다. vMulSig[vAddr].next가 WizContract 주소를 가리키면 응답 생성이 완료되었음을 의미하고, 해당 함수는 더 이상 실행되지 않는다.

단계 3.3: V는 verify_multisig() 함수를 호출하여 다중서명을 검증한다. verify_multisig() 함수는 다음 검증식을 만족하면 True를 그렇지 않으면 False를 리턴 한다.

rp = vMulSig[vAddr].response

$$rp \equiv hc^{R^n \cdot a} \cdot g^{R^n \cdot b} \mod p$$

3.2 콘텐츠 구매 및 수익 분배

단계 1: 구매자는 purchase_contents() 함수를 호출하여 콘텐츠 구매 대금을 WizContract으로 전송한다.

단계 2: purchase_contents() 함수는 구매자가 보낸 (a, b)를 이용하여 WizContents에 대한 공동저작권을 검증한다. 검증에 성공하면 단계 3을 진행하고, 그렇지 않으면 트랜잭션을 취소한다.

단계 3: WizContract은 WizContents.author에 등록된 지분에 맞게 구매 대금을 공동저작자에게 분배한다.

4. 안전성 분석

정리 1. 모든 공동저작자는 WizContents에 대한 다중서명과 지분에 대해서 부인할 수 없다.

(증명) A_i는 자신만이 알고 있는 k_i 값을 이용하여 공통 공개키 (R, Y)를 생성하고 블록체인에 저장한다. 단계 1.1과 단계 1.2에서 WizContents에 대한 저작권 정보와 지분은 해쉬되고, 단계 2.1에서 각 공동저작자는 자신의 개인키를 이용하여 WizContents 해쉬값에 대한 서명 sig_i를 생성한다. 단계 2.2에서 WizContract은 이를 조합하여 다중서명 SIG를 생성하고 블록체인에 등록한다. 단계 3.2에서 A_i는 순차적으로 ch에 대한 응답 rp를 만들어 낸다. 다중서명 검증에 성공하면 수정 및 삭제할 수 없는 블록체인의 특성 상 A_i는 WizContents 공동저작권과 지분에 대한 다중서명을 부인할 수 없다. 제안한 다중서명 검증식은 다음과 같이 증명된다.

$$rp \equiv ch^{\prod_{i=1}^{n} sk_i^{-1}} \equiv (R^{SIG \cdot a} \cdot Y^{R^n \cdot b})^{\prod_{i=1}^{n} sk_i^{-1}} \mod p$$

$$\equiv (hc^{\prod_{i=1}^{n} (k_i \cdot (hc + sig_i)) \cdot a} \cdot g^{\prod_{i=1}^{n} sk_i \cdot R^n \cdot b})^{\prod_{i=1}^{n} sk_i^{-1}} \mod p$$

$$\equiv (hc^{\prod_{i=1}^{n} (sk_i \cdot R) \cdot a} \cdot g^{\prod_{i=1}^{n} sk_i \cdot R^n \cdot b})^{\prod_{i=1}^{n} sk_i^{-1}} \mod p$$

$$\equiv hc^{R^n \cdot a} \cdot g^{R^n \cdot b} \mod p \quad \text{Q.E.D.}$$

정리 2. 판매자와 공동저작자는 WizContract 기반의 수익 분배 프로토콜을 조작할 수 없다.

(증명) 3.2절에서 WizContents를 구매하려면 WizContents에 대한 공동저작권 검증을 해야 한다. 다중서명 검증의 안전성은 정리 1과 같다. 판매자와 일부 저작자가 공모하여 특정 저작자를 제외하게 되면, 단계 3.3의 검증식을 만족할 수 없게 된다. 결국, 단계 3.3의 검증식을 만족하려면 제외된 저작자의 개인키 값을 알아야 하는데, GF(p) 상에서 이산대수를 구하는 것은 계산상 불가능하다 [15]. purchase_contents() 함수는 검증에 성공해야만 저작권 비율에 따라서 수익분배가 이루어지기 때문에 판매자와 일부 저작자의 공모 공격은 불가능하다. Q.E.D.

5. 결론

본 논문에서는 지혜콘텐츠 거래에 적합한 블록체인 기반의 부인봉쇄 다중서명 기법을 제안하였다. 제안한 기법은 공통키 생성, 다중서명 생성 및 검증 단계로 구성된다. 더불어, 제안한 서명 기법을 이용한 블록체인 기반의 콘텐츠 구매 프로토콜의 안전성을 분석하였다.

제안한 블록체인 기반의 WizContract 모델은 수정 및 삭제할 수 없는 스마트계약의 특성상 법원과 같은 제3자의 도움 없이 공정하게 공동저작권에 대한 수익 분배를 자동화 할 수 있다. 지역적 제한이 없는 소셜 플랫폼의 지혜 콘텐츠를 위한 공동저작권 보호 기법으로 적합하다.

REFERENCES

[1] Development of distribution and diffusion service technology through individual and Collective Intelligence to digital contents, ICT R&D program of MSIP/IITP 1st Year Annual Report, 2014.

[2] S. Yun et al., "The Method of Digital Copyright Authentication for Contents of Collective Intelligence", Journal of the Korea Convergence Society, 2015.

[3] Korea Copyright Commission. www.copyright.or.kr

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

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

[6] A.M.Antonopoulos, Mastering Bitcoin 2nd Edition, O'Reilly, 2017.

[7] K. Solorio, R. Kanna, D. H. Hoover, Hands-On Smart Contract Development, O'Reilly, 2019.

[8] KCAC, https://www.rootca.or.kr/kor/main.jsp

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

[10] Melanie Swan, Blockchain, O'Reilly, 2015.

[11] H. Yang, "Major issues related to copyright in the field of culture and arts Study on policy improvement measures", Korea Culture & Tourism Institute, pp.232-233, 2014.

[12] J. Hwang, H. Kim, "Blockchain-based Copyright Management System Capable of Registering Creative Ideas", Journal of Internet Computing and Services, 2019.

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

[14] A. M. Antonopoulos, G. Wood, Mastering Ethereum, O'Reilly, 2019.

[15] 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.

윤 성 현(Yun Sunghyun) [종신회원]

- 1997년 2월 : 고려대학교 일반대학원 컴퓨터학과 (이학박사)
- 1998년 3월 ~ 2002년 2월 : LG 전자 선임연구원
- 2002년 3월 ~ 현재 : 백석대학교 ICT학부 부교수

〈관심분야〉

블록체인, 사물인터넷, DRM, 정보보호