

논문 2026-3-8 <http://dx.doi.org/10.29056/jsf.2026.09.08>

분산형 정보 공유를 위한 분산 키 생성 기반 임계값 프록시 재암호화 아키텍처

김현수*, 최창준*, 박경엽*, 신동명*†

Distributed Key Generation-Based Threshold Proxy Re-Encryption Architecture for Distributed Information Sharing

Hyun-Soo Kim*, Chang-Jun Choi*, Kyung-Yeob Park*, Dong-Myung Shin*†

요 약

기존 프록시 재암호화 기반 정보 공유 기술은 마스터 개인키가 특정 주체에 집중되는 단일 장애점 문제를 가진다. 본 논문은 분산 키 생성(Distributed Key Generation, DKG)과 임계값 프록시 재암호화(Threshold Proxy Re-Encryption, TPRE)를 결합한 분산형 정보 공유 아키텍처를 제안한다. 제안 구조에서 블록체인 노드들은 마스터 공개키를 공동으로 생성하며, 마스터 개인키는 어느 단일 메모리에도 완전한 형태로 존재하지 않는다. 데이터 소유자는 원본 데이터를 일회성 대칭키로 1회 암호화하고, 대칭키를 마스터 공개키로 캡슐화한다. 스마트 컨트랙트가 접근을 승인하면 각 노드는 개인키 조각과 수신자 공개키를 결합한 부분 재암호화 결과를 생성한다. 수신자는 임계값 이상의 부분 결과를 결합하여 자신의 개인키로 대칭키를 복원한다. 마지막으로 제안 구조가 기밀성, 가용성, 반신평 등의 보안 요구사항을 분석하고 만족 여부를 확인한다.

Abstract

Existing proxy re-encryption-based information sharing schemes suffer from a single point of failure, as the master private key is concentrated in a single entity. This paper proposes a distributed information sharing architecture that combines Distributed Key Generation (DKG) with Threshold Proxy Re-Encryption (TPRE). In the proposed architecture, blockchain nodes jointly generate the master public key, and the master private key never exists in complete form in any single memory. The data owner encrypts the original data once with a one-time symmetric key and encapsulates the key under the master public key. When a smart contract approves an access request, each node generates a partial re-encryption result by combining its private key share with the recipient's public key. The recipient combines a threshold number of partial results and recovers the symmetric key with its own private key. Finally, the proposed structure analyzes security requirements such as confidentiality, availability, and antitrust, and verifies whether they are satisfied.

한글키워드 : 분산 키 생성, 프록시 재암호화, 접근 제어, 정보 공유 제어, 블록체인

keywords : Distributed Key Generation, Proxy Re-Encryption, Access Control, Data Sharing Control, Blockchain

* 엘에스웨어(주) 소프트웨어연구소 연구개발본부

† 교신저자: 신동명(email: roland@lsware.co.kr)

접수일자: 2026.09.03. 심사완료: 2026.09.10.

게재확정: 2026.09.20.

1. 서론

공공기관 간 정보 교환, 기업 간 보안 문서 공유, 블록체인(Blockchain) 기반 데이터 접근 제어와 같은 다자 간 협업 환경에서는 참여 주체들이 서로 완전히 신뢰하지 않는다. 따라서 허가된 수신자만이 데이터를 복호화할 수 있도록 하는 공개키 기반 권한 검증 구조가 필요하다. 일반적인 정보 공유 구조에서는 원본 데이터를 대칭키로 암호화하고, 해당 대칭키에 대한 접근 권한을 공개키 기반 방식으로 제어한다. 그러나, 마스터 개인키 또는 재암호화 권한이 데이터 소유자의 단말기, 중앙 키 관리 서버, 단일 프록시 노드에 집중되는 경우가 존재한다. 비밀키가 특정 장치의 메모리에 완전한 형태로 존재하는 순간, 해당 지점은 전체 시스템의 단일 장애 지점(SPOF, Single Point of Failure)이 된다. 해당 지점이 침해되면 시스템의 기밀성과 접근 제어 신뢰성이 약화된다.

프록시 재암호화(PRE, Proxy Re-Encryption)는 이러한 문제를 완화하기 위해 제안된 대표적인 암호 기술이다[1, 2]. 프록시 재암호화 과정에서 프록시는 평문을 알지 못한 상태에서 데이터 소유자의 복호화 권한을 수신자에게 위임할 수 있다. 그러나, 단일 프록시 기반 구조에서는 프록시 장애, 권한 남용, 재암호화 키 노출 문제가 발생할 수 있다. 이를 개선한 임계값 프록시 재암호화(TPRE, Threshold Proxy Re-Encryption) 역시 상당수가 초기 설정 단계에서 마스터 개인키를 특정 주체가 생성한 뒤 조각으로 나누어 분배한다[3]. 따라서, 최초 키 생성 과정에는 여전히 단일 장애 지점이 존재한다.

이에 본 논문은 분산 키 생성과 임계값 프록시 재암호화를 결합한 분산형 정보 공유 아키텍처를 제안한다. 제안하는 기술은 블록체인 노드가 시스템 초기화 단계에서 마스터 공개키를 공동으로

생성한다. 마스터 개인키는 어느 단일 메모리에도 완전한 형태로 존재하지 않아, 단일 실체화에 따른 보안 위험이 완화된다. 또한, 수신자의 공개키를 부분 재암호화 과정에 결합하여, 전송 구간에서 연산 결과가 탈취되더라도 수신자 개인키 없이는 대칭키를 복원할 수 없도록 한다. 아울러 스마트 컨트랙트를 접근 요청, 권한 검증, 부분 결과 제출, 감사 로그 관리의 제어 평면으로 활용하여 정보 공유 과정의 투명성과 추적성을 확보한다.

2. 관련 연구

2.1 분산 키 생성

분산 키 생성(DKG, Distributed Key Generation)은 신뢰할 수 있는 단일 딜러 없이 복수의 참여 노드가 공동으로 공개키를 생성하는 암호 기법이다. 각 노드는 대응되는 개인키의 조각만을 보유한다. 전통적인 비밀 분산 방식에서는 신뢰된 딜러가 전체 비밀값을 생성한 뒤 이를 조각으로 나누어 참여자에게 배포한다[4]. 이때 사전에 정한 임계값 이상의 조각이 모였을 때만 원래의 비밀을 복원할 수 있다. 그러나 이 구조에서는 딜러에게 전체 비밀값이 전달되어 단일 장애 지점이 될 수 있다.

분산 키 생성은 이러한 문제를 해결하기 위해 참여 노드들의 상호 통신을 통해 공동의 공개키를 형성한다[5, 6]. 대응되는 마스터 개인키는 단일 장치에서 재구성되지 않는다. 각 노드는 자신이 보유한 개인키 조각만으로 부분 연산에 참여하며, 임계값 미만의 조각만으로는 전체 비밀값에 대한 어떠한 추가 정보도 얻을 수 없다. 다만 분산 키 생성이 모든 위협을 방어하는 것은 아니다. 임계값 이상의 노드가 장기간 공모하거나 개인키 조각이 누적적으로 노출되는 경우에는 주기적 키 조각 갱신, 검증 가능한 비밀 분산, 악의적

노드 탐지 등의 보호 장치가 결합되어야 한다[7].

이에 본 논문에서는 프로세스 전 과정에서 비밀값이 노출되지 않으며, 임계값 프록시 재암호화 기술을 활용하여 기존의 단일 장애 지점 문제를 해결하기 위한 구조를 제안한다.

2.2 프록시 재암호화

프록시 재암호화는 제3자인 프록시가 평문을 알지 못한 채 암호문을 변환하는 공개키 암호 기법이다. 프록시는 특정 사용자의 공개키로 암호화된 암호문을 다른 사용자의 공개키 기반 암호문으로 변환한다. 데이터 소유자는 수신자 수가 증가하더라도 원본 데이터를 수신자별로 반복 암호화할 필요가 없다. 이러한 특성으로 인해 클라우드 스토리지, 콘텐츠 배포 등 다양한 환경에서 동적 권한 위임 기술로 활용된다[8]. 그러나 단일 프록시 구조에서는 프록시 장애 시 권한 위임 절차가 중단될 수 있다. 또한, 프록시가 악의적으로 동작하거나 재암호화 키가 노출되면 권한 오용이 발생할 수 있으며, 연산이 한 지점에 집중되어 성능 병목과 보안 문제가 함께 발생한다.

2.3 임계값 프록시 재암호화

임계값 프록시 재암호화는 재암호화 연산을 여러 노드로 분산하여 단일 프록시 구조의 권한 집중 문제를 완화한다[9]. 각 노드는 자신의 개인키 조각 또는 재암호화 권한 조각을 이용하여 부분 재암호화 결과를 생성한다. 최종 복호화 권한 위임은 임계값 이상의 부분 결과가 수집되어야 완료된다. 이 방식은 일부 노드 장애에 대한 가용성을 제공하고, 임계값 미만 노드의 담합을 방어할 수 있어 다자 간 정보 공유 환경에 적합하다. 그러나 임계값 프록시 재암호화의 보안성은 초기 키 생성 방식에 크게 의존한다. 마스터 개인키를 특정 주체가 생성한 뒤 조각으로 나누어 배포하는 경우, 최초 키 생성 시점에는 전체 개

인키가 단일 주체에게 노출된다.

일반적인 프록시 재암호화와 임계값 프록시 재암호화에서는 데이터 소유자가 자신의 개인키와 수신자 공개키로 재암호화 키 $rk_{\{A \rightarrow B\}}$ 를 생성하여 프록시에 전달한다. 반면, 본 논문의 구조에서는 캡슐이 소유자 개인키가 아닌 공동 생성된 마스터 공개키로 만들어지므로 소유자가 재암호화 키를 생성할 수 없고, 대신 각 노드가 자신의 마스터 개인키 조각과 수신자 공개키로 재암호화 키 조각을 생성한다. 즉, 재암호화 키 생성 권한이 소유자로부터 노드 집합으로 이동하며, 그 대가로 소유자는 위임 시점에 온라인 상태일 필요가 없고 재암호화 키 자체도 어느 한 곳에 완전한 형태로 존재하지 않는다. 이에 본 논문은 이러한 한계를 해결하기 위해 임계값 프록시 재암호화에 분산 키 생성을 결합한 기술을 제안한다.

2.4 조건부 및 조건은닉 프록시 재암호화

조건부 프록시 재암호화는 속성, 시간, 문맥 등 특정 조건을 추가하여, 조건을 만족하는 경우에만 재암호화가 가능하도록 확장한 구조이다. 그러나 다수의 스킴에서 조건 값이 암호문 또는 재암호화 키에 평문에 가까운 형태로 포함되어, 프록시나 제3자가 조건 구조를 추론할 수 있다. 이를 보완하기 위해 조건의 구체적인 값을 외부에서 파악할 수 없도록 하는 조건은닉 프록시 재암호화가 제안되었다[10].

최근 연구에서는 조건은닉 프록시 재암호화에 Shamir 비밀 분산 기법을 결합하였다[11]. 해당 연구는 속성과 문맥 정보를 해시한 조건 스칼라 값을 암호문 지수부에 은닉하고, 서버 비밀값을 조각 형태로 다수의 프록시 노드에 분산 보관한다. 재암호화 연산은 사용자 비밀 조각과 서버 비밀 조각이 결합될 때에만 수행된다. 이를 통해 단일 프록시 노드가 탈취되더라도 평문과 조건이

노출되지 않는 반신뢰 구조를 달성하였다.

다만, 이 구조에서 비밀 분산은 권한 위임 연산 자체를 임계값화하기보다, 서버 비밀값의 분산 보관과 연산 보조에 활용된다. 또한, 서버 비밀값의 최초 생성과 분배는 여전히 단일 주체가 수행하므로, 생성 시점에는 전체 비밀값이 하나의 메모리에 실체화된다. 이처럼 임계값 방식과 조건은닉 방식 모두 초기 키 생성 단계의 단일 장애 지점 문제를 공유한다.

이에 본 논문은 임계값 프록시 재암호화에 분산 키 생성을 결합하여, 마스터 개인키가 생성 시점부터 어디에도 실체화되지 않는 구조를 제안한다. 접근 정책의 검증은 조건 은닉 대신 스마트 컨트랙트 계층에서 수행하며, 암호 계층은 키의 단일 실체화 제거에 집중한다.

2.5 블록체인 기반 접근 통제

블록체인은 접근 요청, 권한 승인, 데이터 등록, 부분 재암호화 결과 제출 이력을 변조하기 어려운 형태로 기록할 수 있다. 스마트 컨트랙트는 코드화된 접근 제어 정책을 바탕으로 요청을 검증하고, 승인된 요청에 한해서만 후속 절차를 수행하도록 제어하며 그 이력을 남긴다. 이러한 특성은 분산형 정보 공유 환경에서 투명성과 감사 가능성을 제공한다[12]. 그러나 블록체인 자체가 데이터의 기밀성을 보장하는 것은 아니다. 따라서 블록체인 상에 평문 데이터나 대칭키를 직접 저장해서는 안 되며, 블록체인은 오직 접근 제어와 감사를 위한 제어 평면으로만 활용되어야 한다. 실제 데이터의 기밀성은 암호학적 캡슐화, 임계값 부분 재암호화, 수신자 개인키 기반의 복호화 과정을 통해 독립적으로 보장해야 한다.

본 논문에서의 블록체인 스마트 컨트랙트는 평문 데이터나 마스터 개인키를 보유하지 않고, 정책적·절차적 제어와 이력 관리만 담당한다.

3. 시스템 설계

본 장에서는 제안 기법이 적용되는 다자 간 정보 공유 환경에서 시스템 주요 구성요소와 상호작용 구조를 정의한다. 도입 단계에서는 고려해야 할 보안·운영 요구사항을 정리하여, 4장에서 제시하는 기술 설계의 전제 조건을 명확히 한다.

기존 정보 공유 기술은 데이터 소유자의 반복된 암호화 연산 경량화, 프록시 권한 분산, 블록체인 기반 접근 이력 관리 방향으로 발전했다. 그러나, 마스터 개인키 생성부터 복호화 권한 위임까지의 전체 과정을 분산형으로 설계하지 않으면 단일 장애 지점 문제 해결은 불가능하다. 이에 본 논문은 마스터 개인키 생성 단계부터 복호화 권한 위임 단계까지의 전 과정에서 키 실체화를 방지하는 통합 구조를 제안한다. 표 1은 중앙 키 관리 방식, 단일 프록시 재암호화 방식, 일반 임계값 프록시 재암호화 방식과 본 논문에서 제안하는 시스템을 비교한 표이다.

표 1. 기존 기술과의 비교
Table 1. Comparison with existing technologies

구분	중앙관리	단일 PRE	일반 TPPE	제안 시스템
마스터 개인키 생성	중앙 서버	소유자 단말	특정 주체 생성 후 분배	노드 공동 생성
개인키 보관 형태	키 보관	키 보관	조각 분산 (생성 시 노출)	조각 분산 (실체화 없음)
재암호화 수행 주체	해당 없음	단일 프록시	다수 노드	블록체인 노드
단일 장애점	키 관리 서버	프록시/소유자 단말	초기 키 생성 주체	제거
감사 가능성	로그 의존	제한적	제한적	온체인 기록

제안 시스템은 키 생성, 키 보관, 권한 위임, 이력 관리의 전 단계에서 단일 장애점을 제거하고 온체인 감사 기능을 결합한다는 점에서 기존

기술과 구별된다. 이러한 설계 방향은 이하 3.1절의 구성요소 정의와 3.2절의 시스템 요구사항에 반영된다.

3.1 시스템 설계 구성요소

본 논문에서 제안하는 시스템은 분산 환경에서 정보 공유 및 접근 제어를 지원하기 위해 그림 1과 같이 구성된다.

첫째, 데이터 소유자는 원본 데이터를 생성하거나 보유한 주체이다. 데이터 소유자는 원본 데이터를 일회성 대칭키로 암호화하여 외부 저장소에 업로드한다. 이후 해당 대칭키를 블록체인 노드들이 공동 생성한 마스터 공개키로 캡슐화하고, 저장 위치와 접근 정책을 스마트 컨트랙트에 등록한다.

둘째, 수신자는 공유된 데이터에 접근해야 하는 주체이다. 수신자는 자신의 공개키와 접근 요청 정보를 스마트 컨트랙트에 제출한다. 요청이

승인되면 블록체인 노드들이 생성한 부분 재암호화 결과를 수집하고, 자신의 개인키로 대칭키를 복원한다.

셋째, 블록체인 노드는 분산 키 생성과 부분 재암호화 연산에 참여하는 주체이다. 각 노드는 마스터 개인키 전체가 아니라 개인키 조각만 보유한다. 또한, 승인된 요청에 대해서만 자신의 개인키 조각과 수신자의 공개키를 이용하여 부분 재암호화 결과를 생성한다. 이러한 과정을 통해 어떤 단일 노드도 완전한 마스터 개인키를 확인할 수 없다.

넷째, 스마트 컨트랙트는 데이터 등록, 접근 정책 관리, 권한 요청 검증, 부분 결과 제출 기록, 감사 로그 관리를 담당한다. 스마트 컨트랙트에는 평문 데이터, 원본 대칭키, 마스터 개인키가 저장되지 않고, 정보 공유 절차의 정책적 제어와 이력만 기록한다.

다섯째, 외부 저장소는 암호화된 원본 데이터



그림 1. 제안 시스템 구성도
Fig. 1. Proposed System Architecture

를 저장하는 공간이다. 외부 저장소에는 원본 데이터와 대칭키가 저장되지 않는다. 따라서 저장소가 침해되더라도 공격자는 원본 데이터를 복호화할 수 없다.

이러한 구성요소는 '분산 키 생성 → 데이터 암호화 및 등록 → 접근 요청 및 권한 검증 → 임계값 부분 재암호화 → 부분 결과 결합 및 복호화'의 흐름으로 상호 연동된다. 각 단계는 최소 권한 원칙과 반신뢰 가정을 만족한다.

3.2 시스템 요구사항

본 논문의 제안 시스템은 다자 간 협업 환경에서의 사용을 목표로 한다. 따라서, 암호 연산의 안전성과 운영상 제약과 위협 모델을 포함하는 보안·가용성 요구사항을 충족해야 한다. 본 절에서는 이를 기밀성, 가용성, 반신뢰, 데이터 정합성 및 무결성, 권한 위임 강제성 및 감사 가능성의 다섯 관점으로 정리한다.

3.2.1 기밀성

시스템은 데이터 라이프사이클 전 구간에서 평문 데이터가 소유자와 허가된 수신자 외의 주체에게 노출되지 않도록 보장해야 한다. 원본 데이터의 암호화는 데이터 소유자의 로컬 환경에서만 수행된다. 외부 저장소에는 암호화된 데이터만, 블록체인에는 캡슐화된 대칭키와 메타데이터만 저장된다. 블록체인 노드는 부분 재암호화 과정에서 평문이나 대칭키에 접근하지 않고, 자신의 개인키 조각을 이용한 지수 연산과 페어링 연산만 수행해야 한다. 또한, 공격자가 블록체인에 기록된 접근 요청·승인 이력이나 부분 결과 제출 이력을 관찰하더라도 원본 데이터나 대칭키를 복원할 수 없어야 한다.

3.2.2 가용성

시스템은 긴급한 데이터 공유 요청이 빈번한

협업 환경의 특성을 고려하여, 언제든지 접근 요청과 권한 위임을 처리할 수 있어야 한다. 이를 위해 재암호화 연산은 다수의 블록체인 노드에 분산되어야 한다. 특정 노드에 장애가 발생하더라도 임계값 이상의 노드가 유지되는 한 권한 위임 서비스가 중단되지 않아야 한다. 데이터 소유자가 오프라인 상태이더라도, 사전에 등록된 캡슐과 접근 정책만으로 수신자의 요청을 처리할 수 있어야 한다. 아울러, 데이터 소유자는 수신자 수와 무관하게 원본 데이터를 1회만 암호화하도록 하여, 반복 암호화 부담이 발생하지 않아야 한다.

3.2.3 반신뢰

블록체인 노드는 시스템 운영상 필수적인 중개자이지만, 완전히 신뢰할 수 있는 주체로 가정하지 않는다. 본 논문의 기본 위협 모델은 이러한 반신뢰 노드이다. 즉, 노드는 프로토콜을 정직하게 수행하되 관찰 가능한 모든 값으로부터 비밀을 추론하려 시도하며, 임계값 미만의 노드는 서로 공모할 수 있다고 가정한다. 프로토콜을 위반하여 잘못된 값을 제출하는 악의적 노드는 기본 가정에 포함하지 않는다. 각 노드는 정해진 프로토콜을 정직하게 수행하되, 저장된 캡슐과 키 관련 정보로부터 평문이나 대칭키를 추론하려 할 수 있는 주체로 간주한다. 따라서 어떤 단일 노드도 자체적으로 복호 연산을 수행할 수 없어야 한다. 단일 노드가 탈취되더라도 마스터 개인키는 복구될 수 없어야 한다. 임계값 미만의 노드가 공모하더라도 유한체 기반 정보 이론적 안전성에 의해 마스터 개인키에 대한 유의미한 정보를 얻을 수 없어야 한다. 나아가, 초기 키 생성 단계에서도 어떠한 단일 주체가 전체 개인키를 알 수 없어야 한다는 점에서, 기존 임계값 방식보다 강화된 반신뢰 요구사항을 설정한다.

3.2.4 정합성 및 무결성

전송 및 저장 과정에서 캡슐의 구성요소나 부분 재암호화 결과가 변조될 경우, 해당 값으로는 정상적인 대칭키 복원이 불가능해야 한다. 반대로, 무결성이 유지된 캡슐만이 반드시 정확한 대칭키로 복원되어야 한다. 또한, 등록된 캡슐과 제출된 부분 결과의 식별자-해시-시각 정보를 블록 체인에 기록하여, 어떤 입력이 어떤 결과로 이어졌는지 사후에 대조·감사할 수 있어야 한다. 한편, 본 논문은 노드가 프로토콜을 준수하며 의도적으로 잘못된 결과를 제출하지 않는다는 반신뢰 가정을 전제로 한다. 따라서, 부분 결과의 정당성을 암호학적으로 별도 검증하는 기능은 본 연구의 요구사항에서 제외한다.

3.2.5 권한 위임 강제성 및 감사 가능성

접근 정책 검증은 스마트 컨트랙트 상에서 수행되어야 하며, 정책을 충족하지 못한 요청은 부분 재암호화 절차로 이어지지 않아야 한다. 단, 이는 정직한 노드들이 컨트랙트의 승인 결과에 따라 동작함을 전제로 하는 절차적 통제이며, 임계값 이상의 노드가 스마트 컨트랙트를 우회하여 악의적으로 담합하는 상황까지 암호학적으로 원천 차단하는 것은 아니다. 수신자는 캡슐만으로 대칭키를 복원할 수 없어야 하며, 임계값 이상의 부분 재암호화 결과를 수집해야만 복호화가 가능하다. 이때, 부분 재암호화 결과에는 수신자의 공개키 성분이 결합되어야 하므로, 전송 중 탈취되더라도 수신자의 개인키 없이는 대칭키 복원이 불가능하다. 마지막으로, 접근 요청, 권한 승인, 부분 결과 제출 등 시스템 내 주요 행위는 블록 체인에 기록되어 사후 추적성을 보장해야 한다.

4. 제안 기술

4.1 암호학적 설정

제안 암호 시스템은 256 비트 소수인 소수 위

수 q 를 가지는 쌍선형 사상 기반 군 위에서 동작한다. 이 환경에서 이산대수 문제와 판별 쌍선형 디피-헬만(Decisional Bilinear Diffie-Hellman, DBDH) 문제가 확률적 다항시간 공격자에게 어렵다고 가정하며, 이에 대한 증명은 5장에서 구체적으로 설명한다. 쌍선형 사상 위의 두 군을 각각 G_1 , G_2 목표 군을 G_T 라 하고 다음 식(1)과 같고, 쌍선형 사상 e 를 다음과 같이 정의한다. 이하 모든 지수 연산은 Z_q 상에서 수행된다.

$$e : G_1 \times G_2 \rightarrow G_T \quad (1)$$

여기서 $g_1 \in G_1$, $g_2 \in G_2$ 는 각 군의 생성자이며, 기준값 Z 는 다음 식(2)와 같이 정의한다.

$$Z = e(g_1, g_2) \quad (2)$$

수신자 B는 개인키 $b \in Z_q$ 를 보유하고, 이에 대응되는 공개키를 다음 식(3)과 같이 생성한다.

$$PK_B = (g_2)^b \quad (3)$$

제안 구조에서 마스터 개인키는 a 로 표현되나, a 는 어느 단일 블록체인 노드에도 완전한 형태로 존재하지 않는다. 각 노드는 a 의 조각에 해당하는 값을 보유한다. 임계값 이상의 부분 연산 결과가 모였을 때만 수신자에게 복호화 권한 위임이 가능하다. 본 논문에서 사용하는 주요 기호는 표 2와 같이 정의한다.

4.2 분산 키 생성 단계

시스템 초기화 단계에서는 중앙 키 관리 서버나 데이터 소유자에 의존하지 않고, 블록체인의 노드들이 공동으로 마스터 공개키를 생성한다. 분산 키 생성 프로토콜에서는 차수 $t-1$ 의 다항식 $f(x)$ 가 참여 노드들의 상호 작용을 통해 암묵적으로 형성된다.

표 2. 주요 기호 정의
Table 2. Notation

기 호	설 명
q	군 G_1, G_2, G_T 의 소수 위수
n	블록체인 노드 수
t	임계값
a	마스터 개인키 ($a = f(0)$)
a_1	블록체인 노드 P_1 개인키 조각
b, PK_b	수신자 B의 개인키와 공개키
m	일회성 대칭키
r	캡슐화에 사용되는 일회용 난수
λ_1	라그랑주 계수
W_1	노드 P_1 의 부분 재암호화 결과

마스터 개인키는 다음 식(4)와 같이 정의된다.

$$a = f(0) \quad (4)$$

그러나, 어느 단일 블록체인 노드도 a 전체를 알지 못하며, 각 블록체인 노드 P_1 은 자신의 개인키 조각만 보유하고 다음 식(5)와 같다.

$$a_1 = f(1) \quad (5)$$

마스터 공개키는 다음과 같이 목표 군 원소만으로 구성된다. 생성된 공개키는 블록체인 또는 스마트 컨트랙트에 등록되며, 데이터 암호화 시 대칭키 캡슐화에 사용되고 다음 식(6)과 같다.

$$MPK = Z^a \quad (6)$$

이때 $(g_2)^a$ 와 같이 마스터 개인키를 지수로 가지는 원천 군 원소를 공개해서는 안 된다. 임의의 관찰자가 캡슐의 C_1 과의 페어링 연산 $e(C_1, (g_2)^a) = Z^{ar}$ 을 통해 수신자 개인키 없이 대칭키를 복원할 수 있기 때문이다. 따라서 마스

터 공개키는 페어링의 입력으로 사용될 수 없는 목표 군 원소 Z^a 만으로 구성한다.

이 단계의 보안적 의미는 매우 크다. 기존 분산 키 생성 방식에서는 최초 키 생성 주체가 전체 개인키를 알 수 있지만, 제안 구조에서는 마스터 개인키가 네트워크의 수학적 관계 속에만 존재한다. 따라서 시스템 초기화 시점부터 단일 키 생성 주체에 대한 신뢰를 요구하지 않는다. 즉, 시스템에는 마스터 키 쌍을 생성하거나 관리하는 주체가 존재하지 않으며, 실물 값으로 존재하는 것은 공개키 MPK뿐이다. 각 노드의 개인키 조각 a_1 역시 노드 외부로 전송되거나 수집되지 않는다. 실제 구현에서는 Pedersen 방식 또는 Gennaro 등의 검증 가능한 분산 키 생성 프로토콜을 적용할 수 있다. 각 노드는 다항식 계수에 대한 공개 커밋 값을 게시하고, 다른 노드로부터 받은 조각이 커밋과 일치하는지 상호 검증한다. 검증에 실패한 조각은 이의 제기 절차를 통해 배제된다. 이를 통해 악의적 참여자가 잘못된 조각을 배포하여 키 생성을 방해하는 행위를 탐지하고 차단할 수 있다.

4.3 데이터 암호화 및 등록 단계

데이터 소유자는 원본 데이터를 일회성 대칭키 m 으로 암호화하고, 암호화된 데이터를 외부 저장소에 업로드한다. 실제 구현에서 m 은 데이터 암호화 키 또는 이를 유도하는 캡슐 값으로 사용할 수 있다. 이후 데이터 소유자는 일회용 난수 r 을 선택하고, 마스터 공개키를 이용하여 대칭키 m 을 다음같이 캡슐화한다. 이 때 수식으로는 다음 식(7)과 식(8)과 같이 표현한다.

$$C_1 = (g_1)^r \quad (7)$$

$$C_2 = m \cdot MPK^r = m \cdot Z^{ar} \quad (8)$$

최종 캡슐은 다음 식(9)와 같이 표현된다.

$$CT = (C_1, C_2) \quad (9)$$

데이터 소유자는 암호화 데이터의 저장 위치, 캡슐화된 대칭키, 접근 제어 정책, 데이터 식별자를 스마트 컨트랙트에 등록한다. 이때 원본 데이터와 대칭키는 어디에도 평문으로 저장되지 않는다. 이 구조에서 데이터 소유자는 수신자 수와 무관하게 원본 데이터를 한 번만 암호화하면 된다. 신규 수신자가 추가되더라도 원본 데이터를 다시 암호화하거나 수신자별 키를 관리할 필요가 없다. 이후의 복호화 권한 위임은 블록체인 노드의 부분 재암호화 절차를 통해 수행된다.

4.4 권한 검증 및 임계값 부분 재암호화 단계

수신자 B는 자신의 공개키 PK_B 와 접근 요청 정보를 스마트 컨트랙트에 제출한다. 스마트 컨트랙트는 등록된 접근 제어 정책에 따라 수신자의 자격을 검증한다. 접근 권한이 승인되면 승인 사실과 요청 식별자가 온체인에 기록되며, 각 노드는 이 승인 기록을 확인한 뒤 부분 재암호화를 수행한다. 이때, 컨트랙트가 노드에 요구하는 것은 개인키 조각의 제출이 아니라 부분 재암호화 연산의 수행이다. 이 단계는 기존 프록시 재암호화의 재암호화 키 생성 단계에 대응된다. 기존 방식에서는 소유자가 자신의 개인키와 수신자의 공개키로 단일 재암호화 키를 생성하지만, 본 논문에서는 마스터 개인키가 조각 형태로 존재하여 각 노드가 자신의 조각과 수신자의 공개키로 재암호화 키 조각을 생성한다. 각 블록체인 노드 P_1 은 자신의 개인키 조각 a_1 과 수신자 공개키 PK_B 를 이용하여 다음 식(10)과 같은 재암호화 키 조각을 생성한다.

$$rk_i = (PK_B)^{a_i} = (g_2)^{b \cdot f(i)} \quad (10)$$

이후 블록체인 노드는 원본 캡슐의 C_1 과 재암호화 키 조각 rk_i 에 대해 식 (11)의 페어링 연산을 수행하여 부분 재암호화 결과 W_i 을 생성한다.

$$W_i = e(C_1, rk_i) = e(g_1^r, (g_2)^{b \cdot f(i)}) = Z^{r \cdot b \cdot f(i)} \quad (11)$$

이 부분 결과는 단독으로 대칭키를 복원할 수 없다. 부분 결과에는 수신자 공개키 성분이 지수 형태로 반영되어 있다. 따라서, 공격자가 전송 구간에서 부분 결과를 탈취하더라도 수신자의 개인키 b 없이는 대칭키를 복원할 수 없다. 블록체인 노드는 자신의 개인키 조각을 외부로 노출하지 않으며, 내부 연산 결과만 제출한다. 스마트 컨트랙트는 제출 이력을 기록한다. 따라서, 프로토콜 어디에도 개인키 조각을 수집하여 마스터 개인키를 복원하는 절차가 존재하지 않는다. 향후 공개 검증 또는 비대화형 영지식 증명이 결합되면 각 노드의 부분 결과 정당성도 검증할 수 있다.

4.5 부분 결과 결합 및 최종 복호화 단계

정상적인 부분 재암호화 결과가 임계값 이상 수집되면, 수신자 또는 결합 모듈은 해당 결과들을 하나로 결합한다. 수집된 블록체인 노드의 인덱스 집합을 S , 그 크기를 $|S| = t$ 라고 할 때, 각 노드에 대한 라그랑주 계수는 Z_q 상에서 다음 식 (12)와 같이 정의된다.

$$\lambda_i = \prod_{j \in S, j \neq i} (0 - j) / (i - j) \quad (12)$$

수집된 부분 결과는 다음 식(13)과 같이 결합된다. 라그랑주 보간 성질에 의해 지수부의 조각 합이 식(14)와 같이 마스터 개인키 a 로 재구성된다.

$$C^* = \prod_{i \in S} W_i^{\lambda_i} = Z^{r \cdot b \cdot \sum_{i \in S} f(i) \lambda_i} = Z^{rba} \quad (13)$$

$$\sum_{l \in S} f(l)\lambda_l = f(0) = a \quad (14)$$

수신자 B는 자신의 개인키 b 의 역원을 이용하여 다음 식(15)와 같이 값을 계산한다.

$$D = (C^*)^{b^{-1}} = Z^{ra} \quad (15)$$

마지막으로 수신자는 식(16)과 같이 데이터 소유자가 등록한 C_2 에서 D 를 제거하여 대칭키 m 을 복원한다.

$$C_2/D = (m \cdot Z^{ra})/Z^{ra} = m \quad (16)$$

이 과정은 마스터 개인키 a 를 복원하는 절차가 아니라는 점에 유의해야 한다. 라그랑주 결합은 개인키 조각이 아니라 부분 결과 W_1 에 대해 수행된다. 따라서, a 는 결합 결과의 지수 내부에서만 재구성될 뿐, 어떠한 주체도 a 의 값 자체를 획득하지 못한다. 또한, 결합 결과 C^* 의 지수에는 수신자 개인키 b 가 결합되어 있다. 결합을 수행하는 주체가 수신자가 아닌 별도의 결합 모듈 이더라도, 해당 주체는 Z^{ra} 나 대칭키에 대한 어떠한 정보도 얻을 수 없다. 수신자가 최종적으로 획득하는 것 역시 마스터 개인키가 아니라 대칭키 m 이다. 따라서, 수신자는 허가된 데이터에 대해서만 복호화 권한을 행사할 수 있다.

4.6 스마트 컨트랙트 설계

스마트 컨트랙트는 제안 아키텍처에서 접근 제어와 감사 기능을 담당하며, 주요 기능은 다음과 같다. 첫째, 데이터 등록 기능이다. 데이터 소유자는 암호화 데이터의 저장 위치, 캡슐화된 대칭키, 데이터 식별자, 접근 정책 식별자를 등록한다. 평문 데이터와 원본 대칭키는 등록하지 않는다. 둘째, 접근 요청 기능이다. 수신자가 공개키와 데이터 식별자를 제출하면 요청 시점, 요청자

식별자, 제출된 공개키가 기록된다. 셋째, 권한 검증 기능이다. 사전에 등록된 접근 정책에 따라 수신자의 접근 가능 여부를 판단한다. 정책은 수신자 신원, 역할, 기간, 데이터 범위, 소유자 승인 여부 등을 포함할 수 있다. 넷째, 부분 재암호화 제출 기능이다. 노드가 부분 결과를 제출하면 제출 노드, 요청 식별자, 제출 시점, 결과 해시, 검증 상태가 기록된다. 다섯째, 감사 로그 기능이다. 데이터 소유자와 운영자는 접근 요청·승인·거절과 부분 결과 제출 이력을 사후 확인하여 비정상 행위를 추적할 수 있다. 이상의 기능은 모두 정책 검증, 절차 제어, 이력 기록에 해당하며, 스마트 컨트랙트는 암호학적 기밀성이나 접근 통제를 직접 제공하지 않는다. 실제 기밀성은 분산 키 생성, 임계값 부분 재암호화, 수신자 개인키 기반 복호화 구조가 제공한다. 따라서, 컨트랙트의 승인 없이 임계값 이상의 노드가 담합하여 부분 결과를 생성하는 행위는 본 구조의 절차적 통제로는 방지되지 않는다.

5. 제안 기술 평가

5.1 기밀성

본 논문에서 제안하는 기법은 암호화 및 권한 위임 단계 전반에 걸쳐 강력한 데이터 기밀성을 보장한다. 원본 데이터는 데이터 소유자의 로컬 환경에서 일회성 대칭키로 암호화된다. 이후 외부 저장소에는 암호화된 데이터만이, 블록체인에는 캡슐화된 대칭키와 메타데이터만이 분리되어 저장된다. 결과적으로 공격자가 외부 저장소의 암호문을 탈취하거나 블록체인 상의 접근 이력을 관찰하더라도, 원본 데이터 및 대칭키를 복원하는 것은 불가능하다.

암호학적 관점에서 제안 구조의 기밀성은 판별 쌍선형 디피-헬만 가정에 근거한다[13]. 이 가정 하에 공격자가 관찰할 수 있는 공개값은 마스

터 공개키 Z^a , 캡슐 요소 g_1^r , 수신자 공개키 g_2^b 이다. 공격자가 필요로 하는 값은 쌍선형 디피-헬만 값이나, 이는 목표 군의 임의의 원소와 구별할 수 없으므로 공격자는 캡슐 $C_2 = m \cdot Z^r$ 로부터 대칭키 m 에 대한 어떠한 정보도 얻을 수 없다. 또한, 부분 재암호화 결과 $W_1 = Z^r \cdot b \cdot f(1)$ 역시 임계값 미만의 부분 집합만으로는 라그랑주 보간이 성립하지 않는다. 지수 부분에 수신자 개인키 b 가 결합되어 있으므로 수신자 이외의 주체는 이를 임의로 제거할 수도 없다. 마스터 개인키와 수신자 개인키는 철저히 분리되어 관리되므로, 어떠한 단일 주체도 완전한 비밀키에 접근할 수 없다. 결과적으로 저장소 탈취, 블록체인 관찰, 전송 구간 데이터 탈취 등 다양한 공격에 대해서도 데이터의 기밀성이 유지된다.

5.2 가용성

제안 기법은 긴급 데이터 공유 상황을 고려하여 장애 상황에서도 서비스가 지속되도록 설계되었다. 재암호화 연산은 단일 프록시가 아닌 다수의 블록체인 노드로 분산된다. 일부 노드에 장애가 발생하더라도 임계값 이상의 노드가 유지되면 부분 재암호화와 권한 위임이 가능하다. 데이터 소유자는 원본 데이터를 한 번만 암호화하므로, 수신자가 추가되더라도 재암호화나 재업로드가 필요 없다. 신규 수신자에 대한 권한 위임은 이미 등록된 캡슐에 대한 부분 재암호화만으로 수행된다. 따라서 데이터 소유자가 오프라인 상태여도 접근 요청 처리가 가능하다. 성능 관점에서 부분 재암호화는 노드당 지수 연산 1회와 페어링 연산 1회로 구성되며, 노드별 연산은 병렬로 수행된다. 전체 지연은 가장 느린 노드의 처리 시간에 의해 결정되고, 위임 비용은 임계값에 선형으로 증가한다.

5.3 반신뢰

제안 기법에서 마스터 개인키는 어느 단일 주체에서도 생성되거나 보관되지 않으며, 각 노드는 개인키 조각만 보유한다. 임계값 미만의 노드가 공모하더라도 마스터 개인키를 복원할 수 없다. 이는 특정 주체가 전체 개인키를 생성한 뒤 조각을 분배하는 기존 방식과 달리, 초기 키 생성 시점부터 단일 신뢰 주체를 요구하지 않는 강화된 반신뢰 특성이다. 부분 재암호화 단계에서 각 노드는 부분 연산 결과만 생성하며, 최종 복호화에 사용되는 지수 값에 단독으로 접근할 수 없다. 부분 결과에는 수신자 공개키 성분이 결합되어 있어, 노드가 부분 결과를 축적하더라도 수신자 개인키 없이는 대칭키를 복원할 수 없다. 라그랑주 결합 역시 개인키 조각이 아닌 부분 결과의 지수부에 대해 수행된다. 따라서 프로토콜 전 과정에 조각을 수집하거나 마스터 개인키를 복원하는 절차 자체가 존재하지 않으며, 결합 주체에게도 완전 신뢰가 요구되지 않는다. 그 결과 블록체인 노드는 암호문을 수신자용 권한 위임 형태로 변환하는 기능만 수행한다.

5.4 정합성 및 무결성

캡슐과 부분 재암호화 결과를 구성하는 값들은 일회용 난수, 개인키 조각, 수신자 개인키와 지수 관계로 연관되어 있다. 전송·저장 중 캡슐 구성 값이나 부분 결과가 변조되면 이 지수 관계가 깨져 결합 결과에서 정상적인 대칭키가 복원되지 않는다. 다만, 복호화 실패는 변조를 탐지하거나 무결성을 증명하는 수단이 아니며, 어느 값이 변조되었는지도 알려주지 않는다. 따라서, 제안 구조에서 무결성은 다음과 같이 확인한다.

첫째, 데이터 소유자는 캡슐과 암호화 데이터의 해시를 등록 시 스마트 컨트랙트에 기록하고, 수신자는 획득한 캡슐의 해시를 온체인 기록과 대조한다. 둘째, 각 노드는 부분 결과의 해시를

제출 시 기록하며, 결합 주체는 수신한 부분 결과의 해시를 기록과 대조하여 전송 구간 변조를 식별한다. 이 방식은 전송·저장 구간의 변조를 식별하지만, 노드가 처음부터 잘못된 부분 결과를 생성하여 제출하는 경우는 식별하지 못한다. 이는 3.2.3절의 반신뢰 가정 하에서는 발생하지 않는 상황이며, 악의적 노드까지 고려하려면 부분 결과의 정당성을 검증하는 공개 검증 또는 비대화형 영지식 증명이 필요하다(6장). 아울러 데이터 등록, 접근 요청, 권한 승인, 부분 결과 제출 이력이 시간순으로 기록되므로 동일 캡슐에 대한 비정상적 반복 요청이나 제출 누락과 같은 이상 행위를 사후 감사에서 식별할 수 있다.

5.5 권한 위임 강제성 및 감사 가능성

제안 구조에서 복호화 권한 위임은 스마트 컨트랙트의 정책 검증을 통과한 요청에 대해서만 개시된다. 접근 정책을 만족하지 않는 수신자가 공개키를 제출하면 스마트 컨트랙트가 요청을 거절하며, 정직한 노드는 승인 기록이 없는 요청에 대해 부분 재암호화 결과를 생성하지 않는다. 이 통제는 노드가 컨트랙트의 승인 결과를 따른다는 절차적 보장이며, 임계값 이상의 노드가 담합하여 컨트랙트를 우회하는 경우에는 성립하지 않는다. 승인된 요청도 단일 부분 결과만으로는 권한 위임이 완성되지 않는다. 임계값 이상의 부분 결과가 결합되어야만 수신자가 대칭키를 복원할 수 있다. 부분 결과의 지수부에는 수신자 공개키 성분이 결합되어 있으므로, 위임된 권한은 해당 수신자의 개인키에 종속되며 제3자에게 이전될 수 없다. 접근 요청, 권한 승인, 부분 결과 제출 등 주요 행위는 블록체인에 시간순으로 기록된다. 따라서 데이터 소유자는 누가 어떤 데이터에 접근을 요청하였고 어떤 노드가 참여하였는지 사후에 확인할 수 있다. 이는 애플리케이션 계층의

단순 접근 차단보다 강한 보안 보장을 제공한다.

6. 결 론

본 논문에서는 분산 키 생성과 임계값 프록시 재암호화를 결합한 분산형 정보 공유 아키텍처를 제안하였다. 제안 구조에서 마스터 개인키는 시스템 초기화 단계부터 권한 위임 단계까지 어느 단일 메모리에도 완전한 형태로 존재하지 않는다. 데이터 소유자는 원본 데이터를 일회성 대칭키로 1회만 암호화하여 캡슐화한다. 스마트 컨트랙트가 승인한 요청에 대해서만 블록체인 노드들이 개인키 조각과 수신자 공개키를 결합한 부분 재암호화 결과를 생성한다. 수신자는 임계값 이상의 부분 결과를 결합한 뒤 자신의 개인키로 대칭키를 복원한다. 이를 통해 제안 구조는 마스터 키의 생성·보관 단계에서 단일 장애점을 제거하고, 반신뢰 노드 가정 하에서 기밀성, 가용성, 반신뢰, 정합성 및 무결성, 권한 위임 강제성 및 감사 가능성의 다섯 요구사항을 구조적으로 만족함을 분석하였다. 제안 기법은 기관 간 민감 정보 공유, 기업 간 보안 문서 교환, 다자 간 데이터 협업 환경에 적용될 수 있다.

본 논문에서는 아키텍처 설계 및 보안 요구사항 분석에 범위를 한정하였다. 향후에는 분산 키 생성, 대칭키 캡슐화, 부분 재암호화, 결합 및 복호화 단계별 연산 시간과 트랜잭션 비용을 노드 수와 임계값 조합별로 측정할 예정이다. 이를 통해 기존 PRE 및 TPPE 대비 오버헤드를 비교 평가한다. 또한, 저장소 탈취, 전송 구간 탈취, 임계값 미만 노드 담합, 변조된 부분 결과 제출 등 악성 시나리오에 대한 검증 실험을 수행한다. 아울러 비대화형 영지식 증명 기반 부분 결과 검증, 주기적 키 조각 갱신, 동적 노드 가입·탈퇴 대응, 수신자 권한 철회 기법을 연구하여 보다 강력한 블록체인 기반 정보 공유 플랫폼으로 발

전시키고자 한다.

본 연구는 문화체육관광부 및 한국콘텐츠진흥원 부설 한국문화기술기획평가원의 2026년도 문화기술 연구개발 사업으로 수행되었음 (과제명 : 한류콘텐츠 보호를 위한 국제공조 수사 협력 체계 기술 개발, 과제번호 : RS-2024-00439553, 기여율 : 100%)

참 고 문 헌

- [1] M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography", *Advances in Cryptology - EUROCRYPT '98* (LNCS 1403), Springer, pp.127-144, 1998, DOI : 10.1007/BFb0054122
- [2] K. O.-B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia, and J. Gao, "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain", *IEEE Systems Journal*, Vol. 16, No. 1, pp.1685-1696, 2022, DOI : 10.1109/JSYST.2021.3076759
- [3] W. Li, Z. Xie, S. Liu, Y. Zhou, and H. Zhang, "Controllable Access Control in Permissioned Blockchains via Controllable Threshold Proxy Re-Encryption", *IEEE Transactions on Information Forensics and Security*, Vol. 20, pp.9625-9640, 2025, DOI : 10.1109/TIFS.2025.3606185
- [4] A. Shamir, "How to Share a Secret", *Communications of the ACM*, Vol. 22, No. 11, pp.612-613, 1979, DOI : 10.1145/359168.359176
- [5] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Secure Distributed Key Generation for Discrete-Log Based Cryptosystems", *Advances in Cryptology - EUROCRYPT '99* (LNCS 1592), Springer, pp.295-310, 1999, DOI : 10.1007/3-540-48910-X_21
- [6] S. Das, T. Yurek, Z. Xiang, A. Miller, L. Kokoris-Kogias, and L. Ren, "Practical Asynchronous Distributed Key Generation", 2022 IEEE Symposium on Security and Privacy (SP), pp.2518-2534, 2022, DOI : 10.1109/SP46214.2022.9833584
- [7] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive Secret Sharing Or: How to Cope With Perpetual Leakage", *Advances in Cryptology - CRYPTO '95* (LNCS 963), Springer, pp.339-352, 1995, DOI : 10.1007/3-540-44750-4_27
- [8] A. Manzoor, A. Braeken, S. S. Kanhere, M. Ylianttila, and M. Liyanage, "Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain", *Journal of Network and Computer Applications*, Vol. 176, Article 102917, 2021, DOI : 10.1016/j.jnca.2020.102917
- [9] N. Andola, et al., "Proactive threshold-proxy re-encryption scheme for secure data sharing on cloud", *Journal of Supercomputing*, 79(13), pp.14117-14145, 2023, DOI : 10.1007/s11227-023-05221-3
- [10] Z. Hu, L. Ge, and J. Wang, "Conditional Proxy Pool Re-Encryption Scheme against Collusion Attacks", *Proceedings of the 2023 11th International Conference on Communications and Broadband Networking (ICCBN 2023)*, ACM, pp.18-23, 2023, DOI : 10.1145/3596871.3596875
- [11] K.-Y. Park, H.-S. Kim, C.-J. Choi, and D.-M. Shin, "LLM Embedding-based Attribute Recommendation and SSS Combined Condition Hiding Proxy Re-encryption Technique", *Journal of Korea Society of Software Assessment and Valuation*, Vol. 21, No. 4, pp.99-114, 2025, DOI : 10.29056/jsav.2025.12.09
- [12] S. Pal, A. Dorri, and R. Jurdak, "Blockchain for IoT Access Control: Recent Trends and Future Research Directions", *Journal of Network and Computer Applications*, Vol. 203, Article 103371, 2022, DOI : 10.1016/j.jnca.2022.103371
- [13] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing",

Advances in Cryptology - CRYPTO 2001
(LNCS 2139), Springer, pp.213-229, 2001,
DOI : 10.1007/3-540-44647-8_13



박경엽(Kyung-Yeob Park)

2019.02 : 서울과학기술대학교 컴퓨터공학과 석사
2019.01-현재 : 엘에스웨어(주) 소프트웨어연구소
연구개발본부 책임연구원
<주관심분야> 정보보호, IoT 보안, 블록체인,
빅데이터, 분산신원증명, 저작권 기술

저 자 소 개



김현수(Hyun-Soo Kim)

2019.02 : 단국대학교 소프트웨어학과 졸업
2023.08 : 숭실대학교 AI·SW융합학과 석사
2026.02 : 숭실대학교 AI·SW융합학과 박사수료
2019.01-현재 : 엘에스웨어(주) 소프트웨어연구소
연구개발본부 연구팀장
<주관심분야> 인공지능, 머신러닝, 컴퓨터
비전, 분산신원증명, 정보보호



최창준(Chang-Jun Choi)

2019.02 : 상명대학교 컴퓨터공학과 졸업
2021.08 : 세종대학교 정보보호학과 석사
2021.09-현재 : 엘에스웨어(주) 소프트웨어연구소
연구개발본부 책임연구원
<주관심분야> 정보보호, 블록체인, 네트워크 보안,
분산신원증명, 저작권 기술



신동명(Dong-Myung Shin)

2003.02 : 대전대학교 컴퓨터공학과 박사
2001-2006 : 한국정보보호진흥원(KISA)
응용기술팀 선임연구원
2006-2014 : 한국저작권위원회
저작권기술팀 팀장
2014-2016 : 한국스마트그리드사업단
보안인증팀 팀장
2016-현재 : 엘에스웨어(주) 소프트웨어연구소
연구개발본부 연구소장/전무이사
<주관심분야> 오픈소스 라이선스, 저작권 기술, 시스템/
네트워크 보안, SW 취약점 분석·감정, 블록체인