IoT 블록체인 시스템에서 PRESENT 알고리즘의 적용 및 성능 분석

이은지[1], 박희동[2*]
[1]나사렛대학교 IT인공지능학부 학생, [2]나사렛대학교 IT인공지능학부 교수

Application and Performance Analysis of the PRESENT Algorithm in IoT Blockchain Systems

Eun-Ji Lee[1], Hee-Dong Park[2*]
[1]Student, School of IT & Artificial Intelligence, Korea Nazarene University
[2]Professor, School of IT & Artificial Intelligence, Korea Nazarene University

요 약 사물인터넷 환경에서 블록체인 기반의 데이터 보안 기술이 중요해지는 가운데, 본 연구는 자원이 제한된 IoT 블록체인 시스템에 적합한 경량 암호화 알고리즘으로 PRESENT를 제안하고 그 성능을 분석한다. IoT 블록체인 시스템에서 PRESENT 알고리즘의 적용 가능성 및 성능을 평가하기 위하여 대표적인 경량 암호와 알고리즘인 SIMON과 성능을 비교하였다. 이를 위해 두 알고리즘을 동일한 이더리움 기반 블록체인 시스템에 각각 적용한 후 암복호화 속도, 전력 소비량, 가스 사용량을 정량적으로 비교하였다. 실험 결과, SIMON은 빠른 처리 속도를 보였으나 PRESENT는 전력 소비와 가스 사용 측면에서 더 뛰어난 효율을 나타냈다. 따라서 PRESENT가 연산 및 전력 자원이 제한적인 IoT 블록체인 환경에 보다 적합한 경량 암호화 솔루션임을 확인할 수 있었다.

주제어 : 경량 암호화, 사물인터넷 보안, 블록체인, SIMON, PRESENT

Abstract As blockchain-based data security technology becomes increasingly important in the Internet of Things (IoT) environment, this study proposes PRESENT as a lightweight encryption algorithm suitable for resource-constrained IoT blockchain systems and analyzes its performance. To evaluate the applicability and performance of the PRESENT algorithm in IoT blockchain systems, we compared its performance with that of SIMON, a representative lightweight cryptographic algorithm. To this end, we applied both algorithms to the same Ethereum-based blockchain system and quantitatively compared their encryption/decryption speed, power consumption, and gas usage. Experimental results showed that while SIMON demonstrated faster processing speed, PRESENT showed superior efficiency in terms of power consumption and gas usage. Therefore, it was confirmed that PRESENT is a lightweight encryption solution more suitable for IoT blockchain environments with limited computational and power resources.

Key Words : Lightweight Cryptography, IoT Security, Blockchain, SIMON, PRESENT

본 연구성과물은 2025년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2017R1D1A3B06035024).
본 연구는 2025년도 나사렛대학교 교내연구비 지원으로 이루어졌음.
*교신저자 : 박희동(hdpark@kornu.ac.kr)
접수일 2025년 10월 30일 수정일 2025년 11월 27일 심사완료일 2025년 12월 09일

1. 서론

최근 디지털 기술이 산업 전반에 걸쳐 융합되면서 다양한 물리적 대상이 네트워크에 연결되는 사물인터넷 환경이 빠르게 확산되고 있다. 센서 기반의 디바이스들은 대기오염, 온습도, 위치, 생체 신호 등 각종 정보를 실시간으로 수집하고 전송하며, 이로 인해 방대한 양의 데이터가 끊임없이 생성된다. 이러한 데이터는 단순한 정보 이상의 의미를 가진다. 실제 산업 현장이나 의료 시스템, 스마트시티와 같은 복잡한 인프라에서는 데이터의 신뢰성이 곧 시스템의 안정성과 직결되며, 정보의 변조, 유실, 혹은 도난은 막대한 사회적·경제적 피해로 이어질 수 있다.

그러나 IoT(Internet of Things) 장치는 물리적으로 소형이며, 대부분 저전력 MCU(Micro Controller Unit) 위에서 동작한다. 배터리 용량과 메모리, 연산 성능이 제한되어 있어, 일반적인 서버 환경에서 사용되는 보안 기술을 그대로 적용하는 데 어려움이 크다[1]. 특히 암호화는 보안의 핵심 요소임에도 불구하고, AES 같은 기존의 고전적 블록 암호 방식은 높은 연산 비용과 복잡한 구조를 갖고 있어 자원 제약이 큰 IoT 디바이스에 적용하기에는 실효성이 떨어진다. 이로 인해 경량화된 암호 알고리즘이 새로운 대안으로 주목받고 있다. 실제로 전력 소비와 연산 효율성 측면에서 경량 암호화 알고리즘은 기존 알고리즘 대비 IoT 환경에 더욱 적합하다는 실증 연구도 다수 보고되고 있다[2,3,4].

경량 암호화 알고리즘은 최소한의 연산 자원으로 최대한의 보안 효과를 달성할 수 있도록 설계된 암호 알고리즘이다. 경량 암호는 하드웨어 회로 면적을 줄이고 전력 소모를 최소화하는 방향으로 최적화되어 있으며, 실제로 소형 MCU 환경이나 RFID(Radio-Frequency Identification), 스마트 카드, 웨어러블 기기 등에서 활발히 활용되고 있다. 이러한 알고리즘들은 연산 구조, 키 스케줄 설계, 회로 구성 관점에서 다양한 방식으로 최적화되며, 이에 대한 구조적 분류 및 비교 분석 연구도 진행되고 있다[5]. 중요한 것은 경량 암호 알고리즘이 단순히 작고 빠르다는 특성만을 갖는 것이 아니라, 암호학적으로도 다양한 공격 시나리오에 대해 분석되어 어느 정도의 안전성을 확보하고 있다는 점이다[4,6].

이 가운데 SIMON과 PRESENT는 대표적인 경량 블록 암호화 알고리즘으로 널리 활용되고 있다. SIMON은 미국 국가안보국(NSA: National Security Agency)이 제안한 알고리즘으로 단순한 Feistel 구조와 낮은 하드웨어 복잡도를 특징으로 하며[7], PRESENT는 독일과 덴마크 연구진이 제안한 알고리즘으로 ISO/IEC 29192-2 국제 표준에 등재되어 있다[8]. 두 알고리즘 모두 IoT 기기 환경을 고려하여 설계되었으며, 적은 자원으로도 실용적인 보안 수준을 제공할 수 있는 구조적 특성을 갖고 있다. 특히 PRESENT는 약 1570 게이트 수준의 초소형 회로 면적과 우수한 전력 효율로 인해 센서 노드와 같은 저전력 시스템에 적합하다는 평가를 받고 있다[8,9].

한편, 최근에는 IoT 시스템에서 생성되는 데이터를 분산 저장하고 조작 불가능한 방식으로 관리하기 위한 기술로 블록체인이 주목받고 있다. 블록체인은 중앙 서버 없이 데이터를 여러 노드에 동일하게 분산 저장하고 각 트랜잭션을 체인 구조로 연결하여 불변성과 추적 가능성을 확보한다. 이러한 특성은 신뢰 기반이 취약한 IoT 환경에서 매우 유용하다.

하지만 블록체인을 실제 IoT 환경에 적용하려 할 때 또 다른 제약이 존재한다. 해시 연산, 디지털 서명, 블록 생성 등의 트랜잭션 처리 과정은 상당한 연산 자원과 전력을 요구하기 때문에 자원이 제한된 IoT 디바이스에서는 큰 부담으로 작용한다. 이와 관련하여 여러 연구에서는 IoT 시스템에서 블록체인 도입 시 에너지 소비가 주요 병목 요소로 작용하며, 이에 대한 최적화 필요성을 제기하고 있다[10]. 특히 이러한 시스템에서 데이터를 암호화할 때 고전적인 대칭키 기반 알고리즘을 사용할 경우 연산 효율성이 현저히 떨어질 수 있다. 따라서 IoT와 블록체인을 융합하는 구조에서는 연산 효율성과 전력 소비량을 동시에 고려한 암호 기술의 도입이 필수적이며[11], 이에 가장 부합하는 대안이 경량 암호화 알고리즘이다.

특히 경량 암호와 알고리즘 중 PRESENT는 CPU 성능, 메모리 용량, 배터리 전력 등 시스템 자원이 제한된 IoT 환경을 고려하여 설계된 경량 블록 암호화 알고리즘으로, 여러 연구에서 에너지 효율성 측면의 우수성이 보고된 바 있다[8,12,13]. 그러나 SIMON과 PRESENT가 실제 IoT 블록체인 시스템에서 어떤 성능 차이를 보이는지에 대한 실증적 분석은 아직 충분히 이루어지지 않았다.

따라서 본 연구는 SIMON과 PRESENT를 이더리움 블록체인 연동 구조에 실제로 적용한 후 암복호화 속도, 전력 소비량, 및 가스(Gas) 사용량을 정량적으로 비교 분석함으로써, 자원이 제한된 IoT 블록체인 시스템에 보다 적합한 경량 암호화 알고리즘을 실증적으로 검증하여 제안하고자 한다.

2. 관련 연구

사물인터넷 환경에서의 보안성 확보를 위해 경량 암호화 알고리즘의 적용에 대한 연구는 지속적으로 이루어져 왔다. 특히 제한된 연산 자원과 전력 환경에서도 높은 보안성과 효율성을 유지할 수 있는지에 대한 정량적 분석이 활발히 이루어지고 있다.

El-Hajj et al.은 Arduino UNO 및 Raspberry Pi 플랫폼에서 SIMON, PRESENT를 포함한 총 39개의 경량 블록 암호 알고리즘을 직접 구현하고, 암복호화 속도, ROM/RAM 점유율, 전력 소비, 에너지 효율 등을 기준으로 성능을 비교하였다[11]. 이 연구에서는 PRESENT가 SIMON과 비교하여 전력 소모와 메모리 효율 측면에서 우수한 결과를 보였으며, 전반적으로 두 알고리즘은 IoT 환경에서 모두 사용 가능한 수준의 처리 성능을 보유하고 있음을 확인하였다. 특히 PRESENT는 구조적 단순성과 더불어 에너지 효율성 면에서도 우위를 가지는 것으로 분석되었으며, 이는 소형 센서 노드 환경에서의 실용성을 뒷받침하는 근거로 제시되었다. 그러나 해당 연구는 로컬 임베디드 환경에 한정된 실험으로, 블록체인 연동 환경에서의 성능을 고려하지는 않았다.

Sharma, Joshi는 블록체인 기반의 의료 정보 시스템에 SIMON 알고리즘을 적용한 사례를 소개하였다[14]. Hyperledger Fabric 플랫폼 상에서 의료 데이터를 SIMON으로 암호화하여 블록체인에 안전하게 저장하는 구조를 설계하였으며, 이를 통해 블록체인과 경량 암호의 융합 가능성을 입증하였다. 다만 해당 연구는 암호 알고리즘의 처리 속도나 전력 소모 등 성능 지표에 대한 수치 기반 분석을 포함하지 않았다는 한계가 있다.

Fotovvat et al.은 IoT 센서 환경에서 AES, SPECK, SIMON, PRESENT 알고리즘을 대상으로 스루풋(Throughput), 암복호화 지연 시간, 전력 소비를 측정하여 비교하였다[15]. 그 결과 PRESENT는 SIMON과 유사한 수준의 처리 성능을 유지하면서도 낮은 전력 소모와 우수한 에너지 효율성을 보였으며, IoT 환경에서 높은 실용성을 확보할 수 있는 대안으로 평가되었다. 또한 PRESENT는 적은 회로 자원으로도 높은 효율을 달성하는 것으로 분석되어, 전력과 메모리 제약이 큰 디바이스에 보다 적합하다는 결론을 제시하였다. 그러나 해당 연구는 블록체인 연동 환경을 고려하지 않았으며, 각 알고리즘이 스마트 계약 실행 시 소비하는 가스량이나 블록체인 기반 시스템 내에서의 실제 성능 차이에 대해서는 다루지 않았다.

이처럼 다양한 선행 연구들은 SIMON과 PRESENT 각각의 특징과 강점을 제시해왔지만, 이를 실제 블록체인 연동 환경에서 동일한 조건 하에 정량적으로 비교한 연구는 매우 드물다. 따라서 블록체인 시스템에 두 경량 암호화 알고리즘을 실제로 적용하여 두 알고리즘의 성능을 비교 평가할 필요가 있다.

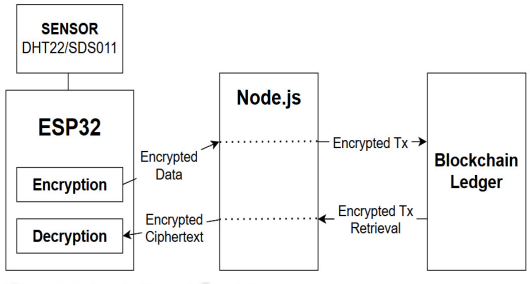
3. IoT 블록체인 암호화 시스템 구성

본 연구에서는 경량 암호화 알고리즘인 PRESENT와 SIMON의 성능을 블록체인 기반 IoT 환경에서 비교하기 위해 실제 하드웨어와 소프트웨어가 연동된 실험 시스템을 구축하였다. 해당 시스템은 암호화/복호화 연산, 블록체인 데이터 저장, 전력 측정 등의 과정을 포함한다.

3.1 IoT 블록체인 암호화 시스템 구성

본 연구에서는 경량 암호 알고리즘의 성능을 실제 IoT 블록체인 환경에서 검증하기 위해 센서 데이터의 암호화 및 복호화 전 과정을 블록체인 시스템과 연동한 실험 환경을 구성하였다. 전체 구조는 센서 모듈, ESP32 기반 암복호화 장치, 블록체인 네트워크, 그리고 트랜잭션 중계 서버로 구성되며, 암호화된 데이터를 블록체인에 저장하고 복호화하는 모든 과정이 실제 하드웨어에서 수행된다.

데이터 수집은 온습도(DHT22) 및 미세먼지(SDS011) 센서를 통해 이루어지며 수집된 데이터는 ESP32에서 경량 블록 암호 알고리즘을 이용해 암호화된다. 암호화된 데이터는 Node.js 서버를 통해 블록체인 네트워크로 전달되어 트랜잭션 형태로 저장된다. 이후 암호문을 블록체인에서 다시 조회하여 복호화 과정을 수행함으로써 전체 흐름이 하나의 폐쇄 루프로 구성된다.



[Fig. 1] Blockchain encryption system architecture

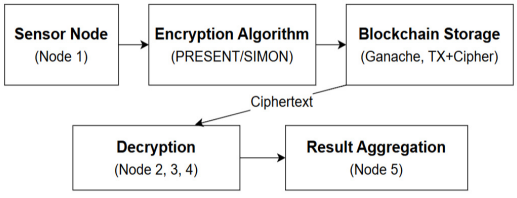
이러한 구조는 단일 장치 내 처리 방식이 아닌, 노드 간 기능을 분산시켜 구성함으로써 블록체인의 핵심 개념인 분산성과 무결성을 실제로 재현하였다. 이를 통해 블록체인 환경에서의 암복호화 처리 성능과 에너지 소비 특성을 보다 현실적으로 평가할 수 있도록 하였다.

[Fig. 1]은 이러한 블록체인 연동 암호화 시스템의 전체 구성을 도식화한 것이다. 센서로부터 수집된 데이터는 ESP32에서 암호화 처리되며, Node.js를 통해 블록체인에 기록된 후 다시 복호화 노드로 전송된다. 이 과정을 통해 각 단계에서의 성능 지표를 계측하고 비교할 수 있다.

3.2 실험 환경 및 성능 측정 방법

블록체인 기반 IoT 시스템 환경에서 경량 블록 암호 알고리즘의 성능을 정량적으로 비교하기 위해 다섯 개의 ESP32 모듈과 실시간 센서, 전력 측정 장치, 블록체인 네트워크 시뮬레이터, 그리고 트랜잭션 처리용 서버 환경을 구성하였다.

데이터 수집은 온습도 센서와 미세먼지 센서를 통해 이루어졌으며, 이들은 각각 Node 1에 연결되어 실시간 데이터를 생성하였다. 생성된 센서 데이터는 Node 1의 ESP32에서 경량 암호화 알고리즘을 사용하여 암호화된다. 암호화된 데이터는 Wi-Fi를 통해 Node.js 기반 서버로 전송되고 이 서버는 암호문을 Ganache 기반의 로컬 블록체인 네트워크에 트랜잭션 형태로 저장한다. 저장된 암호문은 이후 Node 2, 3, 4에서 복호화 처리를 수행하기 위해 블록체인에서 다시 조회되고, Node 5에서는 전체 복호화 결과를 수집 및 집계하는 역할을 담당한다. 이와 같은 다중 노드 기반 구성을 실제 분산 블록체인 환경에서의 데이터 흐름과 처리 과정을 충실히 재현하기 위함이다.



[Fig. 2] Flowchart of Blockchain Storage and Decryption Process for Encrypted Sensor Data

한편, 각 ESP32 노드의 전력 소비 측정은 INA219 전류 센서를 활용하여 수행되었으며, 알고리즘 수행 시간 및 전류 사용량을 동시에 기록함으로써 성능과 에너지 효율성 모두에 대한 분석이 가능하도록 하였다. Node 1에서 Node 5까지의 ESP32는 동일한 조건 하에 알고리즘을 실행하여 공정한 비교가 가능하도록 설계되었으며, 모든 연산은 Wi-Fi 통신 환경 하에서 비동기적으로 이루어졌다.

[Fig. 2]는 본 실험 시스템에서 각 노드가 수행하는 역할과 데이터 흐름을 시각화한 것으로, 센서 데이터의 암호화부터 블록체인 저장, 복호화 및 결과 집계에 이르기까지의 전체 처리를 보여준다. 경량 블록 암호 알고리즘인 SIMON과 PRESENT를 블록체인 연동 IoT 환경에 적용한 후, 실험을 통해 두 알고리즘의 성능을 암복호화 속도와 전력 소모량의 두 가지 지표로 비교하였다.

암복호화 속도 측정을 위해 각 ESP32 노드에서 암호화 또는 복호화 연산이 시작되기 직전과 종료된 직후의 시점을 millis() 함수를 사용해 기록하였다. 이를 통해 연산 수행에 소요된 시간을 밀리초(ms) 단위로 산출하였으며, 알고리즘별로 동일한 길이의 데이터를 대상으로 10회 반복 측정을 수행한 뒤 평균값을 계산해 비교하였다.

Node 1은 센서 데이터를 암호화한 뒤 서버 노드(Node 5)로 전송하고, Node 2, 3, 4는 이 암호문을 각각 독립적으로 수신하여 동일한 복호화 연산을 수행한 후 서버에 결과를 전달하였다. 이처럼 하나의 암호문에 대해 다수의 노드가 동시에 복호화를 수행함으로써 측정값의 분산을 줄이고 연산 성능에 대한 신뢰도 높은 평균값을 확보할 수 있도록 설계하였다. 이를 통해 두 알고리즘이 실시간 데이터 처리에 미치는 영향을 보다 정밀하게 정량 분석할 수 있었다.

4. 실험 결과 및 분석

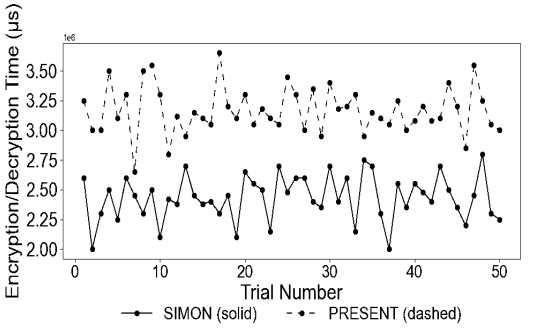
본 장에서는 제안한 실험 환경을 바탕으로 SIMON과 PRESENT 알고리즘을 적용하였을 때의 성능을 암복호화 속도, 전력 소모량, 및 가스량 측면에서 각각 비교 분석하였다. 특히, 가스량은 블록체인 자원 효율성 평가를 위해 중요한 성능 지표이다.

모든 실험은 동일한 하드웨어 및 통신 조건, 동일한 블록체인 네트워크 구조에서 수행되었으며, 측정값의 신뢰도를 높이기 위해 알고리즘당 50회의 반복 실험을 통해 신뢰도 높은 평균값을 산출하였다.

4.1 암복호화 속도 비교 분석

ESP32 보드에서 각 알고리즘의 암호화 및 복호화 소요 시간을 측정한 결과, SIMON이 PRESENT보다 평균적으로 약 22.7% 더 빠른 속도를 보이는 것으로 나타났다. 반복 측정을 통해 산출된 평균 소요 시간은 SIMON이 약 1.13μs, PRESENT는 약 1.46μs 수준으로 확인되었다.

이러한 차이는 알고리즘 구조에서 기인한 것으로 분석된다. SIMON은 Feistel 구조를 기반으로 하여 좌우 블록 분할 후 간단한 AND, XOR, Rotation 연산만을 반복적으로 수행하므로 연산 복잡도가 낮다. 반면 PRESENT는 SPN(Substitution-Permutation Network) 구조로 S-box와 Premutation 연산이 각 라운드마다 적용되며, 이는 메모리 접근 및 비트 재배열 비용을 유발하여 MCU 환경에서 성능 저하로 이어진다.



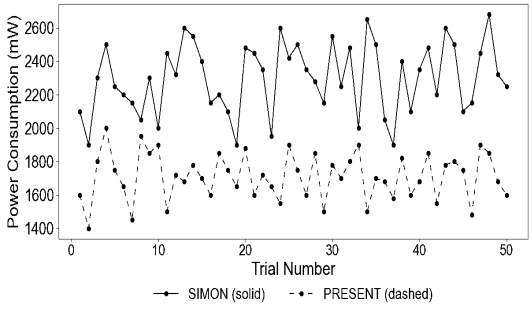
[Fig. 3] Comparison of Encryption/Decryption Time Between SIMON and PRESENT

4.2 전력 소모량 비교 분석

각 알고리즘을 반복적으로 수행하며 INA219 센서를 사용하여 평균 전류 소비를 측정한 결과, PRESENT가 SIMON보다 약 26.1% 더 낮은 전력을 소모하는 것으로 나타났다. 구체적으로 SIMON은 평균 95.3mW의 전력을 소모한 반면, PRESENT는 약 70.4mW로 측정되었다.

PRESENT는 국제표준화기구(ISO/IEC 29192-2)에 등재된 경량 블록 암호로 게이트 수가 약 2000GE 수준에 불과하며, 하드웨어 기반 최적화를 고려한 구조로 설계되어 있다. 이에 따라 소형 MCU 환경에서 높은 에너지 효율성을 제공하며, 연산 간 스위칭 활동이 적어 전류 피크를 효과적으로 억제할 수 있다.

반면 SIMON은 속도 중심으로 최적화된 구조로 인해 연산 반복에 따른 피크 전류가 발생하기 쉽고, 특히 Rotation 연산이 많아 소비 전력이 증가하는 경향을 보였다. 결과적으로 저전력 특성이 중요한 센서 네트워크나 배터리 기반 IoT 환경에서는 PRESENT가 더 적합한 알고리즘으로 평가된다.



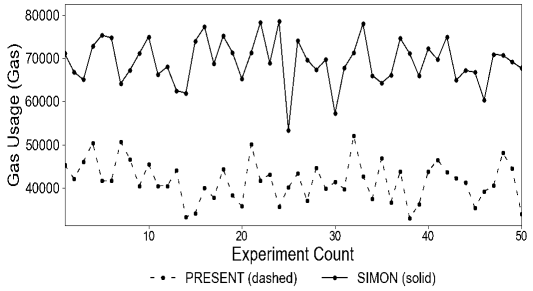
[Fig. 4] Comparison of Power Consumption Between SIMON and PRESENT

4.3 가스량 비교 분석

센서 데이터를 암호화한 후 블록체인에 전송하는 과정에서 발생하는 가스 소비량을 측정한 결과, PRESENT 알고리즘은 SIMON 대비 평균 약 35.6% 적은 가스를 소모하는 것으로 나타났다. 구체적으로, SIMON을 사용할 경우 평균 약 70,000 가스가 소모된 반면, PRESENT는 약 45,000 가스 수준으로 측정되었다.

이러한 차이는 스마트 컨트랙트 내에서의 연산 구조 및 코드 구성의 차이에서 기인한 것으로 분석된다. SIMON은 구조적으로 단순한 Feistel 네트워크를 기반으로 하지만, 이를 Solidity 언어로 구현할 경우 반복적으로 발생하는 조건 분기와 비트 이동 연산으로 인해 연산 단위가 세분화되고, 코드 길이가 길어지는 경향이 있다. 이는 EVM(Ethereum Virtual Machine) 상에서 실행 시 가스 비용 증가의 원인으로 작용한다. 반면, PRESENT 알고리즘은 고정된 라운드 구조와 연산 흐름의 일관성으로 인해 코드 최적화가 용이하며, Solidity 내에서 상대적으로 간결하게 구현 가능하다. 결과적으로 EVM 상에서 연산 효율성이 높고 가스 소비가 적은 실행 구조를 갖추게 된다.

가스 사용량은 곧 트랜잭션 수수료로 직결되기 때문에 전력 및 비용 제약이 큰 IoT 기반 블록체인 응용 환경에서는 PRESENT가 보다 경제적이고 실용적인 대안이 될 수 있음을 시사한다.



[Fig. 5] Comparison of Gas Usage Between SIMON and PRESENT

5. 결론

본 연구는 IoT 환경에서 활용 가능한 경량 블록 암호 알고리즘인 SIMON과 PRESENT를 이더리움 기반 블록체인 시스템에 직접 구현하고, 동일한 조건 하에서 암복호화 속도, 전력 소비량, 가스 사용량을 정량적으로 측정하여 성능을 비교하였다. 이를 통해 각 알고리즘의 실제 활용 가능성과 환경 적합성을 평가하였다.

실험 결과, SIMON 알고리즘은 전반적으로 빠른 암복호화 속도를 보이며, 실시간 처리가 중요한 응용 시나리오에서 강점을 나타냈다. 반면, PRESENT는 낮은 전력 소비와 가스 사용량을 기록하며 에너지 자원이 제한적인 IoT 기기 환경에서 보다 유리한 특성을 보였다. 특히 Solidity 환경에서의 구현 복잡도, 조건 분기 수, 연산 단위 등의 차이가 EVM 상의 처리 효율성과 트랜잭션 비용에 영향을 미치는 것으로 분석되었다. 이는 단순히 암호 알고리즘의 이론적 특성만이 아니라, 이를 블록체인 상에서 어떻게 구현하는지에 따른 효율성 차이가 존재함을 시사한다.

본 연구는 블록체인 네트워크 상에서 실제로 암호 알고리즘을 적용하고 실험적으로 성능을 측정했다는 점에서 실증적 가치가 있다. 이를 통해 경량 암호화 기술이 IoT 기반 블록체인 응용에 있어 단순한 이론적 선택이 아닌 실제 구현 단계에서 성능과 자원 효율성에 미치는 영향을 보다 구체적으로 검증하였다.

향후에는 다양한 경량 암호 알고리즘과 블록체인 플랫폼을 대상으로 비교 범위를 확장하고 메모리 사용량, 코드 크기, 하드웨어 구현 복잡도 등의 종합적인 성능 지표를 고려하여 포괄적인 실험이 수행될 필요가 있다. 또한 보안성 평가를 포함한 후속 연구를 통해 알고리즘 선택의 신뢰성을 높이는 것도 중요한 과제로 제시된다.

REFERENCES

[1] Amrita, C.P.Ekwueme, I.H.Adam, and A.Dwivedi, “Lightweight Cryptography for Internet of Things: A Review,” *EAI Endorsed Transactions on Internet of Things*, Vol.10, 2024.

[2] J.Soto-Cruz, E.Ruiz-Ibarra, J.Vázquez-Castillo, A.Espinoza-Ruiz, A.Castillo-Atoche, and J.Mass-Sanchez, “A Survey of Efficient Lightweight Cryptography for Power-Constrained Microcontrollers,” *Technologies*, Vol.13, No.1:3, 2025.

[3] P.S.Suryateja and K.VenkataRao, “A Survey on Lightweight Cryptographic Algorithms in IoT,” *Cybernetics and Information Technologies*, Vol.24, No.1, 2024.

[4] S.M.Al-Nofaie, S.Sharaf, and R.Molla, “Design Trends and Comparative Analysis of Lightweight Block Ciphers for IoTs,” *Applied Sciences*, Vol.15, No.14:7740, 2025.

[5] Y.Zhong and J.Gu, “Lightweight Block Ciphers for Resource-Constrained Environments: A Comprehensive Survey,” *Future Generation Computer Systems*, Vol.157, pp.288-302, 2024.

[6] J.Kaur, A.C.Canto, M.M.Kermani, and R.Azarderakhsh, “A Comprehensive Survey on the Implementations, Attacks, and Countermeasures of the Current NIST Lightweight Cryptography Standard,” arXiv preprint arXiv:2304.06222, 2023.

[7] R.Beaulieu, S.Treatman-Clark, D.Shors, B.Weeks, J.Smith and L.Wingers, “The SIMON and SPECK Lightweight Block Ciphers,” in Proceedings of *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp.1-6, 2015.

[8] A.Bogdanov, L.R.Knudsen, G.Leander, C.Paar, A.Y.Poschmann, M.J.B.Robshaw, Y.Seurin, and C.Vikkelsoe, “PRESENT: An Ultra-Lightweight Block Cipher,” *Lecture Notes in Computer Science*, Vol.4727, pp.450-466, 2007.

[9] M.Rana, Q.Mamun, and R.Islam, “Balancing Security and Efficiency: A Power Consumption Analysis of a Lightweight Block Cipher,” *Electronics*, Vol.13, No.21:4325, 2024.

[10] S.M.Habibullah, S.Alam, S.Ghosh, A.Dey, and A.De, “Blockchain-Based Energy Consumption Approaches in IoT,” *Scientific Reports*, Vol.14, No.1:28088, 2024.

[11] M.El-Hajj, H.Mousawi, and A.Fadlallah, “Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform,” *Future Internet*, Vol.15, No.2:54, 2023.

[12] B.Aslan, “Energy Consumption Analysis of ISO/IEC 29192-2 Standard Lightweight Ciphers,” *Applied Sciences*, Vol.15, No.7:3928, 2025.

[13] E.J.Lee and H.D.Park, “Performance Evaluation of Lightweight Cryptographic Algorithms for IoT Blockchain Networks,” in Proceedings of *2025 Digital Contents Society Conference*, pp.686-687, 2025.

[14] M.Sharma and R.Joshi, "Hyperledger Blockchain Enabled Secure Medical Record Management with Deep Learning-Based Diagnosis Model," *Complex & Intelligent Systems*, Vol.8, pp.625-640, 2022.

[15] A.Fotovvat, G.M.E.Rahman, S.S.Vedaei, and K.A.Wahid, "Comparative Performance Analysis of Lightweight Cryptography Algorithms for IoT Sensor Nodes," *IEEE Internet of Things Journal*, Vol.8, No.10, pp.8279-8290, 2021.

이 은 지(Eun-Ji Lee) [준회원]

■ 2022년 3월 ~ 현재 : 나사렛대학교 IT인공지능학부 (학사과정)

〈관심분야〉
사물인터넷, 정보보호, 블록체인

박 희 동(Hee-Dong Park) [정회원]

■ 1998년 2월 : 경북대학교 일반대학원 전자공학과 (공학석사)
■ 2005년 8월 : 경북대학교 일반대학원 전자공학과 (공학박사)
■ 1998년 3월 ~ 2007년 8월 : 포항대학교 컴퓨터응용계열 교수
■ 2007년 9월 ~ 현재 : 나사렛대학교 IT인공지능학부 교수

〈관심분야〉
사물인터넷, 모바일 컴퓨팅, 블록체인, 인공지능