Journal of KIIT. Vol. 24, No. 2, pp. 121-126, Feb. 28, 2026. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2026.24.2.121

다채널 IIoT 환경을 위한 인터리브 ASCON-128 하드웨어 구현

문 상 국*

Interleaved ASCON-128 Hardware Implementation for Multi-Channel IIoT Environments

Sangook Moon*

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (No. RS-2022-00144000)

요 약

산업용 사물인터넷 환경에서는 다수의 센서 채널에서 수집되는 데이터의 기밀성과 무결성을 실시간으로 보장해야 한다. 본 논문에서는 2024년 NIST 경량 암호 표준으로 선정된 ASCON-128을 기반으로, 다채널 IIoT 환경을 위한 인터리브 하드웨어 아키텍처를 제안한다. 제안하는 시스템은 시분할 다중화 방식을 적용하여 단일 ASCON 코어로 10개의 센서 채널을 처리한다. 하드웨어 스케줄러가 라운드로빈 방식으로 채널을 선택하고, 채널별 320비트 상태를 BRAM에 저장하여 1-2 클럭 사이클 내에 무지연 컨텍스트 스위칭을 수행한다. 또한 채널 ID와 샘플 카운터를 결합한 Per-Sample Nonce 모드를 도입하여 각 센서 샘플에 고유한 nonce를 부여함으로써 재전송 공격을 방지한다. DE1-SoC에서 구현한 결과, NIST SP 800-232 공식 KAT 테스트 벡터 168개에서 100% 일치를 확인하였다. 10채널 구성에서 1,847 ALM과 4개의 BRAM 메모리 블록을 사용하여 70.42 MHz 동작 주파수에서 225 Mbps의 총 처리량을 달성하였으며, 이는 채널별 전용 코어 방식 대비 약 84%의 리소스 절감 효과에 해당한다.

Abstract

In Industrial Internet of Things environments, ensuring real-time confidentiality and integrity of data collected from multiple sensor channels is essential. This paper proposes an interleaved hardware architecture for multi-channel IIoT environments based on ASCON-128, which was selected as the NIST lightweight cryptography standard in 2024. The proposed system employs time-division multiplexing to process 10 sensor channels using a single ASCON core. A hardware scheduler selects channels in round-robin fashion, storing each channel's 320-bit state in BRAM to achieve zero-overhead context switching within 1-2 clock cycles. Additionally, Per-Sample Nonce mode is introduced, combining channel ID and sample counter to assign unique nonces to each sensor sample, thereby preventing replay attacks. Implementation on DE1-SoC achieved 100% compliance with all 168 official NIST SP 800-232 KAT test vectors. The 10-channel configuration utilizes 1,847 ALMs and 4 BRAM memory blocks, achieving 225 Mbps total throughput at 70.42 MHz operating frequency, representing approximately 84% resource reduction compared to the dedicated-core-per-channel approach.

Keywords

ASCON, lightweight cryptography, AEAD, FPGA, IIoT, time-division multiplexing

* 목원대학교 전기전자공학과
- ORCID: https://orcid.org/0000-0002-0290-1887

· Received: Jan. 21, 2026, Revised: Feb. 10, 2026, Accepted: Feb. 13, 2026
· Corresponding Author: Sangook Moon
Dept. of Electrical and Electronic Engineering
800 Seo-gu Doanbuk-ro, Daejeon, Korea
Tel.: +82-42-829-7637, Email: smoon@mokwon.ac.kr

Ⅰ. 서 론

산업용 사물인터넷(IIoT, Industrial Internet of Things) 환경에서는 다수의 센서 노드가 실시간으로 데이터를 수집하고 전송하며, 이러한 데이터의 기밀성과 무결성 보장이 필수적이다. 스마트 팩토리, 에너지 관리 시스템, 원격 모니터링 등 IIoT 응용 분야에서 센서 데이터가 탈취되거나 변조될 경우 심각한 안전 문제와 경제적 손실이 발생할 수 있다[1]. 이러한 사이버 위협에 대응하기 위해 제로 트러스트 보안 모델[2]이나 AI 기반 사이버 범죄 탐지 기법[3] 등 다양한 보안 접근 방식이 연구되고 있다. 그러나 IIoT 엣지 디바이스는 제한된 연산 능력, 메모리, 전력 예산을 가지므로 기존의 AES-256이나 ChaCha20과 같은 범용 암호화 알고리즘을 적용하기 어려운 경우가 많다[4]. 이러한 자원 제약 환경에서의 암호화 요구를 해결하기 위해 NIST(미국 국립표준기술연구소)는 2019년부터 경량 암호(Lightweight cryptography) 표준화 프로젝트를 진행하였다[5]. 5년간의 평가 과정을 거쳐 2024년 ASCON이 최종 표준(SP 800-232)으로 선정되었으며[6], ASCON은 128비트 보안 수준을 제공하면서도 소프트웨어와 하드웨어 모두에서 우수한 효율성을 보여 IoT 환경에 적합한 것으로 평가받았다[7].

ASCON의 하드웨어 구현에 관한 연구는 활발히 진행되어 왔다. W. Diehl et al.[8]은 ASCON과 ACORN의 FPGA(Field Programmable Gate Array) 구현을 비교 분석하였고, S. Saha et al.[9]은 ASCON 하드웨어에서의 오류 검출 기법을 제안하였다. 그러나 기존 연구들은 대부분 단일 채널 암호화에 초점을 맞추고 있어, 다수의 센서 채널을 동시에 처리해야 하는 IIoT 게이트웨이 환경에는 직접 적용하기 어렵다. 채널별로 독립된 암호화 코어를 배치하는 방식은 하드웨어 리소스 사용량이 채널 수에 비례하여 증가하므로 비효율적이다.

본 논문에서는 다채널 IIoT 환경에서 단일 ASCON-128 코어로 10개 이상의 센서 채널을 효율적으로 처리할 수 있는 인터리브(Interleaved) 하드웨어 아키텍처를 제안한다. 제안하는 시스템은 시분할 다중화(TDM, Time-Division Multiplexing) 방식을 적용하여 라운드로빈 스케줄링으로 각 채널의 암호화 요청을 순차적으로 처리하며, 채널별 컨텍스트를 BRAM(Block Random Access Memory)에 저장하여 무지연(Zero-overhead) 컨텍스트 스위칭을 구현한다. 또한, 샘플별 고유 nonce를 동적으로 생성하는 Per-Sample Nonce 모드를 도입하여 재전송 공격(Replay attack)을 방지한다.

제안하는 아키텍처는 Intel Cyclone V SoC FPGA(DE1-SoC)에서 구현 및 검증하였다. NIST SP 800-232 공식 테스트 벡터 168개(암호화 84개, 복호화 84개)에 대해 100% 일치를 확인하였으며[10], 10채널 동시 동작 시 1847개의 ALM 사용과 70.42 MHz의 최대 동작 주파수를 달성하였다. 이는 채널별 전용 코어 방식 대비 약 84%의 리소스 절감 효과가 있다.

Ⅱ. 관련 연구

2.1 ASCON 알고리즘

ASCON은 2024년 NIST SP 800-232로 표준화된 경량 인증 암호화(AEAD) 알고리즘이다[6]. ASCON-AEAD128은 128비트 키, 128비트 nonce, 128비트 인증 태그를 사용하며, 내부적으로 320비트 상태(State)를 기반으로 동작한다[7]. ASCON의 핵심은 스폰지(Sponge) 구조와 순열(Permutation) 함수 p이다. 순열 p는 5개의 64비트 워드로 구성된 320비트 상태에 대해 치환-순열 네트워크(SPN)를 적용한다. 초기화와 최종화 단계에서는 12라운드 순열(p^a)을, 데이터 처리 단계에서는 8라운드 순열(p^b)을 사용하여 보안성과 성능의 균형을 맞춘다. ASCON-AEAD128의 암호화 과정은 다음과 같다. (1) 초기화: IV, 키, nonce를 상태에 로드하고 p^a를 적용한다. (2) 연관 데이터(AD) 처리: AD를 128비트 블록 단위로 XOR하고 p^b를 적용한다. (3) 평문 암호화: 평문 블록을 XOR하여 암호문을 생성하고 p^b를 적용한다. (4) 최종화: 키를 XOR하고 p^a를 적용하여 128비트 인증 태그를 생성한다.

2.2 기존 ASCON 하드웨어 구현

ASCON의 FPGA 구현에 관한 연구는 CAESAR

경쟁 시기부터 활발히 진행되었다. W. Diehl et al.[8]은 ACORN과 ASCON의 FPGA 구현을 비교 분석하여, ASCON이 처리량(Throughput) 대비 면적 효율성에서 우수함을 보였다. 해당 연구에서 Xilinx Artix-7 FPGA 기준 ASCON은 약 2,000 LUT를 사용하여 1 Gbps 이상의 처리량을 달성하였다. S. Saha et al.[9]은 ASCON 하드웨어에서 부채널 공격에 대응하기 위한 오류 검출 기법을 제안하였다. 이 연구는 순열 연산에 패리티 검사를 추가하여 결함 주입 공격(Fault injection attack)을 탐지하는 방법을 FPGA에서 검증하였다. 그러나 기존 연구들은 공통적으로 단일 데이터 스트림의 암호화에 초점을 맞추고 있다. 다수의 독립적인 센서 채널을 처리해야 하는 IIoT 게이트웨이 환경에서는 채널별로 별도의 암호화 코어를 배치하거나, 소프트웨어에서 순차적으로 처리해야 하는 한계가 있다. 본 연구에서는 이러한 한계를 극복하기 위해 단일 코어에서 다채널을 시분할 처리하는 인터리브 아키텍처를 제안한다.

III. 제안 아키텍처

3.1 전체 시스템 구조

그림 1은 제안하는 다채널 인터리브 ASCON-128 시스템의 전체 구조를 보여준다. 시스템은 크게 하드웨어 스케줄러(HW scheduler), 인터리브 ASCON 엔진(ASCON interleaved), 그리고 ASCON 코어(ASCON core)로 구성된다. 10개의 센서 채널에서 수집된 데이터는 하드웨어 스케줄러를 통해 순차적으로 처리 요청이 접수된다. 스케줄러는 라운드로빈 방식으로 채널을 선택하고, 해당 채널의 컨텍스트를 로드하여 ASCON 엔진에 전달한다. 단일 ASCON 코어가 시분할 방식으로 모든 채널의 암호화를 처리하며, 완료된 암호문은 채널 ID와 함께 출력된다. 제안하는 TDM 방식은 채널별 전용 코어 방식과 비교하여 상당한 리소스 절감 효과를 제공한다. 전용 코어 방식에서 10채널을 처리하려면 10개의 독립적인 ASCON 코어가 필요하지만, 제안하는 구조에서는 단일 코어와 채널별 컨텍스트 저장용 BRAM만으로 동일한 기능을 수행한다. ASCON 순열 연산이 전체 하드웨어의 대부분을 차지하므로, 이를 공유함으로써 약 84%의 로직 리소스 절감이 가능하다. 또한, 각 모듈 간 인터페이스는 valid/ready 핸드셰이킹 프로토콜을 사용하여 백프레셔(Backpressure)를 지원하며, 이를 통해 처리 속도가 다른 채널들 간에도 데이터 손실 없이 안정적인 동작을 보장한다.

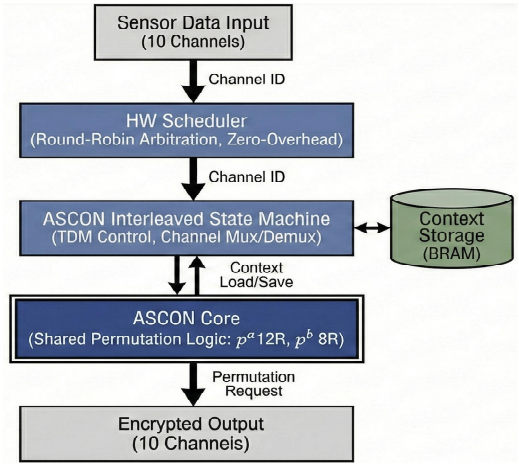

그림 1. 제안하는 ASCON-128 인터리브 시스템 아키텍처
Fig. 1. Proposed interleaved ASCON-128 system architecture

3.2 인터리브 ASCON 코어 설계

그림 2는 인터리브 ASCON 엔진의 상태 머신을 보여준다. 기본적인 ASCON-AEAD128 처리 흐름을 따르되, 채널 간 전환을 위한 컨텍스트 저장/복원 메커니즘을 추가하였다. 각 채널은 독립적인 320비트 ASCON 상태를 유지한다. 채널 전환 시 현재 상태를 BRAM에 저장하고, 다음 채널의 상태를 BRAM에서 로드한다. 이 과정은 포인터 기반으로 구현되어 1-2 클럭 사이클 내에 완료되며, 이를 무지연(Zero-overhead) 컨텍스트 스위칭이라 한다. 10개 채널을 위한 컨텍스트 저장에는 320비트 × 10채널 = 3,200비트의 BRAM이 사용된다.

ASCON 코어는 320비트 상태 레지스터와 순열 연산 유닛으로 구성된다. 320비트 상태는 5개의 64비트 워드(x0~x4)로 나뉘며, 순열 함수 p는 각 라운드에서 상수 덧셈(Addition of constants), S-box 치환(Substitution), 선형 확산(Linear diffusion) 연산을 순

차적으로 적용한다. 본 구현에서는 단일 라운드를 1 클럭 사이클에 처리하는 방식을 채택하여, 12라운드 순열(p^a)은 12 사이클, 8라운드 순열(p^b)은 8 사이클에 완료된다. 이러한 라운드 직렬화 방식은 완전 병렬화 대비 면적을 절감하면서도, IIoT 센서 데이터의 낮은 대역폭 요구사항을 충분히 만족하는 처리량을 제공한다.

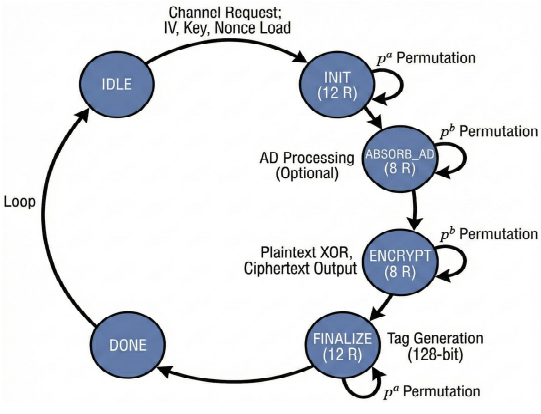

그림 2. 인터리브 ASCON 상태 머신
Fig. 2. Interleaved ASCON state machine diagram

3.3 Per-Sample Nonce 생성

ASCON-AEAD에서 동일한 키와 nonce 조합으로 다른 평문을 암호화하면 보안이 취약해진다. 특히 IIoT 환경에서는 센서 데이터가 주기적으로 생성되므로, 공격자가 암호문을 수집하여 재전송 공격(Replay attack)을 시도할 수 있다. 이를 방지하기 위해 본 연구에서는 Per-Sample Nonce 모드를 제안한다. 128비트 nonce를 상위 96비트는 base_nonce[127:32], 이후 16비트는 channel_id[15:0], 마지막 16비트는 sample_counter[15:0]로 구성하며, base_nonce는 세션 시작 시 설정되는 기본 nonce이고 channel_id는 채널 식별자 (0~9), sample_counter는 매 샘플마다 증가하는 채널별 샘플 카운터이다. 이 구조를 통해 각 센서 샘플은 고유한 nonce로 암호화되어, 동일한 평문이라도 매번 다른 암호문을 생성한다. 16비트 카운터는 채널당 65,536개의 샘플까지 고유성을 보장하며, 이후에는 base_nonce를 갱신하여 계속 운용할 수 있다.

IV. 구현 및 성능 평가

4.1 개발 환경

제안하는 인터리브 ASCON-128 시스템은 Terasic DE1-SoC 개발 보드에서 구현되었다[11]. DE1-SoC는 Intel Cyclone V SoC FPGA (5CSEMA5F31C6)를 탑재하고 있으며, 32,070개의 ALM(Adaptive Logic Module), 87개의 BRAM 메모리 블록, 듀얼코어 ARM Cortex-A9 HPS(Hard Processor System)를 제공한다[12]. 하드웨어 설계는 SystemVerilog로 작성하였으며, Intel Quartus Prime Lite 21.1을 사용하여 합성 및 배치배선을 수행하였다. ASCON 코어의 기능 검증을 위해 ModelSim을 활용한 시뮬레이션을 진행하였고, 실제 FPGA 보드에서 SignalTap Logic Analyzer를 통해 내부 신호를 모니터링하며 동작을 확인하였다. 소프트웨어 테스트벤치는 Python 3와 공식 ASCON 레퍼런스 구현을 활용하여 테스트 벡터를 생성하고 검증 결과를 비교하였다. HPS와 FPGA 간 통신은 Lightweight HPS-to-FPGA Bridge를 통한 메모리 맵 레지스터 접근 방식으로 구현하였다.

4.2 NIST KAT 검증

구현된 ASCON-128 코어의 정확성을 검증하기 위해 NIST SP 800-232에서 제공하는 공식 KAT (Known Answer Test) 벡터를 사용하였다[10]. KAT 검증은 암호화 84개, 복호화 84개로 총 168개의 테스트 케이스로 구성된다. 표 1은 KAT 검증에 사용된 테스트 벡터의 구성을 보여준다. 테스트 벡터는 연관 데이터(AD)와 평문(PT)의 길이를 0바이트부터 32바이트까지 다양하게 조합하여 경계 조건과 일반적인 사용 사례를 모두 검증한다.

검증 결과, 구현된 코어는 168개 전체 테스트 케이스에서 100% 일치를 달성하였다. 암호화 모드에서는 생성된 암호문과 인증 태그가 기대값과 정확히 일치하였고, 복호화 모드에서는 복원된 평문과 태그 검증 결과가 모두 정확하였다. 이를 통해 제안하는 구현이 NIST 표준을 정확히 준수함을 확인하였다.

표 1. NIST KAT 테스트 벡터 구성
Table 1. NIST KAT test vector configuration

Item	Range	Test count
AD Length	0-32 bytes	various combinations
PT Length	0-32 bytes	various combintations
Encryption	-	84
Decryption	-	84
Total		168

4.3 리소스 사용량

표 2는 제안하는 인터리브 ASCON-128 시스템의 FPGA 리소스 사용량을 보여준다.

표 2. FPGA 리소스 사용량 비교
Table 2. FPGA resource utilization comparison

Configuration	ALM	BRAM	Fmax
Single channel	1,124	2	85.3 MHz
Proposed (10-ch TDM)	1,847	4	70.42 MHz
Dedicated core (10-ch))	~11,240*	20*	85.3 MHz

*Estimated (Single Channel × 10)

제안하는 10채널 인터리브 구조는 1,847 ALM을 사용하여 Cyclone V의 총 ALM 대비 약 5.8%의 사용률을 보인다. 이는 단일 채널 구현(1,124 ALM) 대비 약 64% 증가에 불과하며, 10개의 독립 코어를 배치하는 방식(약 11,240 ALM) 대비 약 84%의 리소스 절감 효과가 있다. 메모리 사용량은 4개의 BRAM 블록(총 40Kbit)으로, 10채널의 320비트 컨텍스트 저장(3,200비트)과 입출력 버퍼링에 사용된다. 최대 동작 주파수는 70.42 MHz로, 단일 채널 대비 약 17% 감소하였으나 채널 멀티플렉싱 로직의 추가로 인한 것이며, IIoT 센서 데이터 처리에는 충분하다.

4.4 성능 분석

표 3은 제안하는 구현과 기존 ASCON 하드웨어 연구를 비교한 결과이다. 공정한 비교를 위해 LUT 기반 리소스를 ALM으로 환산하였으며(1 ALM ≈ 2 LUT), 다채널 환경에서의 효율성을 평가하기 위해 채널당 리소스 사용량을 산출하였다.

표 3. ASCON 하드웨어 구현 비교.
Table 3. Comparison of hardware implementation of ASCON

Implement-ation	Resource	Fmax	Throughput	Channels	Resource/Ch
Diehl[8]	2,000	290	1,160	1	2,000
Saha[9]	2,847	185	740	1	2,847
Proposed	1,847	70.42	225	10	~185

W. Diehl et al.[8]의 구현은 Xilinx Artix-7에서 2,000 LUT를 사용하여 290 MHz에서 1,160 Mbps의 높은 처리량을 달성하였다. 그러나 이는 단일 채널 구현으로, 10채널 환경에서는 10배의 리소스(약 20,000 LUT)가 필요하다. S. Saha et al.[9]의 구현은 오류 검출 기능을 추가하여 2,847 LUT를 사용하며, 부채널 공격에 대한 내성을 제공하지만 역시 단일 채널만 지원한다. 제안하는 구현은 절대적인 처리량에서는 기존 연구보다 낮지만, 다채널 효율성 측면에서 우수성을 보인다. 채널당 리소스 사용량은 약 185 ALM(≈370 LUT)으로, W. Diehl et al.[8] 대비 약 81%, S. Saha et al.[9] 대비 약 87%의 리소스 절감 효과가 있다. 또한, IIoT 센서 환경에서 채널당 22.5 Mbps의 처리량은 일반적인 요구사항(수백 kbps)을 크게 상회하므로, 처리량 감소는 실용적 관점에서 문제가 되지 않는다. 결론적으로, 제안하는 인터리브 아키텍처는 다채널 IIoT 환경에서 리소스 효율성과 실용적 처리량의 균형을 달성하며, 단일 코어로 다수 채널을 처리해야 하는 자원 제약적 엣지 환경에 적합하다.

V. 결 론

본 논문에서는 다채널 IIoT 환경을 위한 인터리브 ASCON-128 하드웨어 아키텍처를 제안하였다. 제안하는 시스템은 시분할 다중화(TDM) 방식을 적용하여 단일 ASCON 코어로 10개의 센서 채널을 효율적으로 처리하며, BRAM 기반의 무지연 컨텍스트 스위칭을 통해 채널 간 전환 오버헤드를 최소화하였다. 또한, Per-Sample Nonce 모드를 도입하여 각 센서 샘플에 고유한 nonce를 부여함으로써 재전송 공격을 방지하였다. Intel Cyclone V SoC FPGA에서 구현한 결과, NIST SP 800-232 공식 KAT 168개 테

스트 케이스에서 100% 일치를 확인하여 표준 준수를 검증하였다. 리소스 측면에서 10채널 인터리브 구조는 1,847 ALM을 사용하여 채널별 전용 코어 방식 대비 약 84%의 리소스 절감 효과를 달성하였다. 성능 측면에서 70.42 MHz 동작 주파수에서 225 Mbps의 총 처리량을 제공하며, 이는 일반적인 IIoT 센서 데이터 요구사항을 충분히 만족한다. 향후 연구로는 채널 수 확장에 따른 성능 변화 분석, 부채널 공격 대응을 위한 마스킹 기법 적용, 그리고 ASCON-Hash를 활용한 무결성 검증 기능 통합을 계획하고 있다.

References

[1] International Electrotechnical Commission, "IEC 62443: Security for Industrial Automation and Control Systems", IEC, 2018.

[2] J. Y. Lee, B. H. Choi, S. Jang, and S. H. Chun, "A Study on the Deployment Strategy of Zero Trust Security Model Based on Human-Centered Security Design", J. of IIBC, Vol. 24, No. 4, pp. 1-7, Aug. 2024. https://doi.org/10.7236/JIIBC.2024.24.4.1.

[3] J. Son and J. Song, "A Study on Cybercrime Detection Using Explainable AI Technique", J. of IIBC, Vol. 25, No. 2, pp. 243-249, Apr. 2025. https://doi.org/10.7236/JIIBC.2025.25.2.243.

[4] H. S. Jeon and S. G. Lee, "Analysis and Implementation of Encryption Algorithm for Security of Remote Update of IoT Healthcare Devices", Journal of KIIT, Vol. 19, No. 7, pp. 91-99, Jul. 2021. https://doi.org/10.14801/jkiit.2021.19.7.91.

[5] M. S. Turan, et al., "Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process", NIST IR 8369, Jul. 2021. https://doi.org/10.6028/NIST.IR.8369.

[6] NIST, "SP 800-232: Ascon-Based Lightweight Cryptography Standards", National Institute of Standards and Technology, Aug. 2024. https://doi.org/10.6028/NIST.SP.800-232.

[7] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2: Lightweight Authenticated Encryption and Hashing", Journal of Cryptology, Vol. 34, No. 3, pp. 1-42, Jul. 2021. https://doi.org/10.1007/s00145-021-09398-9.

[8] W. Diehl, F. Farahmand, A. Abdulgadir, J. P. Kaps, and K. Gaj, "Face-off between the CAESAR Lightweight Finalists: ACORN vs. Ascon", Proc. IEEE FPT 2018, Naha, Japan, pp. 330-333, Dec. 2018. https://doi.org/10.1109/FPT.2018.00068.

[9] S. Saha, A. Bag, D. Mukhopadhyay, and P. P. Chakrabarti, "Hardware Constructions for Error Detection in Lightweight Authenticated Cipher ASCON Benchmarked on FPGA", IEEE Trans. VLSI Syst., Vol. 30, No. 4, pp. 476-489, Apr. 2022. https://doi.org/10.1109/TVLSI.2021.3136093.

[10] NIST, "Lightweight Cryptography Standardization: KAT Test Vectors", NIST CSRC, 2024. https://csrc.nist.gov/projects/lightweight-cryptography.

[11] Terasic Technologies, "DE1-SoC User Manual", Terasic, 2014.

[12] Intel Corporation, "Cyclone V Hard Processor System Technical Reference Manual", Intel, 2020.

저자소개

문 상 국 (Sangook Moon)

1995년 2월 : 연세대학교 전자공학과(공학사)
1997년 2월 : 연세대학교 전자공학과(공학석사)
2002년 2월 : 연세대학교 전기전자공학부(공학박사)
2002년 2월 ~ 2004년 2월 : SK하이닉스 선임연구원
2004년 3월 ~ 현재 : 목원대학교 전기전자공학과 교수
관심분야 : 데이터 암호화, 마이크로프로세서, 디지털회로설계, IoT 임베디드시스템디지털회로설계, IoT 임베디드시스템