

실시간 IIoT 이상 탐지를 위한 다채널 자원 최적화 하드웨어 Welford 엔진

문 상 국*

Resource-Optimized Multi-Channel Welford Engine for Real-Time IIoT Anomaly Detection on FPGA

Sangook Moon*

요 약

산업용 사물인터넷 게이트웨이는 데이터가 암호화되어 전송되기 전에 다수의 센서 채널에 대한 실시간 통계 이상 탐지를 요구한다. 소프트웨어 기반 분산 계산은 부동소수점 드리프트와 운영체제 스케줄링 지터에 취약하고, 2-패스 통계는 과도한 온칩 메모리를 소모한다. 본 논문은 Welford의 온라인 평균·분산 알고리즘을 자원 최적화 하드웨어로 구현하여 Intel Cyclone V 시스템 온 칩의 ASCON-128 인증 암호화 파이프라인 앞단에 배치한다. 각 채널은 고정소수점 단일-패스 갱신과 제곱근이 없는 3σ 규칙을 시프트·덧셈만으로 평가하여 탐지 경로에서 나눗셈기와 제곱근 유닛을 제거한다. 32-사이클 반복형 나눗셈기와 채널당 단일 공유 곱셈기를 통해 10채널 엔진은 약 2,500개의 로직 엘리먼트와 30개의 디지털 신호처리 블록으로 70 MHz 이상에서 동작하며, 채널 간 지터 없이 초당 약 599,000 항목을 기준 소프트웨어와 비트 단위로 일치하며 처리한다.

Abstract

Industrial Internet-of-Things gateways increasingly need on-the-fly statistical anomaly detection across many sensor channels before raw data is encrypted. Software running-variance computations suffer from floating-point drift and operating-system scheduling jitter, while two-pass statistics demand prohibitive on-chip memory. This paper presents a resource-optimized hardware implementation of Welford's online mean-and-variance algorithm, placed upstream of an ASCON-128 authenticated-encryption pipeline on an Intel Cyclone V system-on-chip. Each channel uses a single-pass fixed-point update and a square-root-free 3σ rule evaluated by shift-and-add, with no divider or square-root unit in the detection path. A 32-cycle iterative divider and one shared multiplier per channel let the ten-channel engine fit in about 2,500 logic elements and 30 digital signal processing blocks, run above 70 MHz, and sustain 599,000 entries per second with zero jitter, matching a software reference bit-exactly.

Keywords

anomaly detection, fixed-point arithmetic, Welford algorithm, FPGA, ASCON, IIoT gateway

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

• Received: Jun. 15, 2026, Revised: Jul. 28, 2026, Accepted: Jul. 31, 2026
• Corresponding Author: Sangook Moon
Dept. of Electrical and Electronic Engineering, Mokwon University,
88 Doan-buk-ro, Seo-gu, Daejeon 35349, Korea
Tel.: +82-42-829-7637, Email: smoon@mokwon.ac.kr

I. 서 론

산업용 사물인터넷(IIoT) 게이트웨이는 수십 개의 센서 채널로부터 데이터를 집계하여 결정론적 타이밍 요구사항을 갖는 상위 시스템으로 전달한다[1]. 데이터는 게이트웨이를 떠나기 전 인증 암호화 봉투로 감싸지므로, 모든 인라인 상태 모니터링과 이상치 탐지는 암호화 단계 이전에 동일한 표본 단위 지연 예산 내에서 이루어져야 한다. 이때 유용한 정합성 검사가 채널별 실시간 평균·분산으로, 계산 비용이 거의 없으면서도 단순한 3σ 검정만으로 센서 결합·스파이크·고착(Stuck-at) 상태를 하위 전과 이전에 노출시킨다.

게이트웨이에서는 두 가지 소프트웨어적 접근 모두 부적합하다. x 와 x^2 의 단순 누산기(Naïve accumulator)는 수백만 표본 후 정밀도를 잃고 $\mu \gg \sigma$ 에서 불안정하며, 2-패스 일괄 통계는 전체 윈도우를 온칩 메모리에 버퍼링해야 해 소형 SoC에서 수용 불가능하다. Welford의 단일-패스 정식화[2]는 두 합정을 모두 회피하지만, 실시간 리눅스로 포팅해도 부동소수점 드리프트가 남고, PREEMPT_RT를 적용해도 수십 마이크로초에 달하는 OS 스케줄러 꼬리 지연에 시달린다[3]. 결정론적 대안은 통계 계산을 하드웨어로 내리는 것으로, 고정소수점 연산이 비트 단위로 정확한 결과를, 동일한 유한상태기계(FSM)가 비트 단위로 정확한 타이밍을 주며, 이는 FPGA 보안·분석 가속기의 정립된 패턴이다[4].

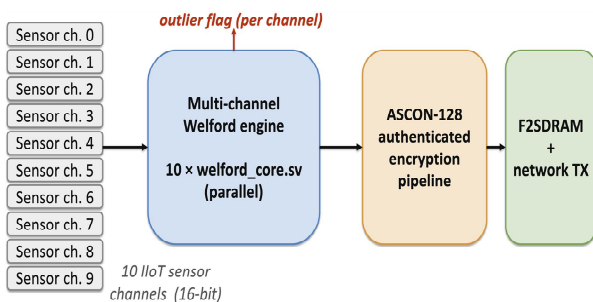


그림 1. IIoT 게이트웨이 내 Welford 엔진의 시스템 개요
Fig. 1. System overview – Welford engine in an IIoT gateway

본 논문은 바로 이 자리(Slot)를 목표로 하는 다 채널 하드웨어 Welford 엔진을 제안한다. 이 엔진은

Cyclone V SoC 상의 ASCON-128[5] 인증 암호화 파이프라인[6] 앞단에 위치하며 동일한 50 MHz 패브릭 클럭을 공유한다. 그림 1은 IIoT 게이트웨이 안에서 제안 엔진이 차지하는 전체 위치를 보여준다. 10개의 16비트 센서 채널이 다채널 Welford 엔진으로 들어가고, 채널별 이상치 플래그가 상위 계층으로 노출되며, 필터링된 데이터는 ASCON-128 인증 암호화 파이프라인을 거쳐 F2SDRAM 및 네트워크 송신으로 전달된다.

II. 관련 연구

엣지용 경량 인증 암호화에 관한 최근 FPGA 연구는 암호화 단계 자체에 집중되어 왔다. Koppuravuri et al.[7]은 보안 엣지 IoT 기기용 고정 리올 ASCON 아키텍처를, Trimberger와 Moore[4]는 FPGA 기반 보안 가속기의 광범위한 논거를 제시하였으며, 재구성 가능 모듈 기반 가속기 설계도 보고되었다[8]. 이들은 센서 입력을 이미 유효한 것으로 간주하고 처리율이 중요한 작업을 암호화 블록에 둔다. 반면 원시 스트림이 암호화 파이프라인에 들어가기 전, 결정론적 타이밍을 희생하지 않고 채널별 통계 정합성 검사를 수행하는 보안 문제는 주목받지 못했다. 기존 방안은 통계를 소프트웨어에 두어 부하 시 100 μ s를 넘는 꼬리-지연과 부동소수점 드리프트를 겪는다. 본 논문은 이를 하드웨어로 옮겨 10채널 시분할에서 중단간 114 사이클의 결정론적 지연과 지터 0을 유지한다. 소형 SoC에서 ASCON-AEAD128 코어와 나란히 동작하는 단일-패스 하드웨어 Welford 엔진은 알려진 바와는 IIoT 게이트웨이 맥락에서 보고된 바가 없으며, 본 논문이 그 간극을 메운다.

III. 시스템 모델 및 방법

3.1 Welford 온라인 갱신

표본 스트림 x_i 가 주어졌을 때, Welford 알고리즘[2][9]는 누적 표본 수 n , 평균 μ , 2차 모멘트 누산기 M_2 를 다음 점화식으로 유지한다.

$$n \leftarrow n + 1 \quad (1)$$

$$\delta = x - \mu \quad (2)$$

$$\mu \leftarrow \mu + \frac{\delta}{n} \quad (3)$$

$$M_2 \leftarrow M_2 + \delta \cdot (x - \mu') \quad (4)$$

여기서 불편(Unbiased) 분산은 $\sigma^2 = M_2 / (n - 1)$ 이다. 이 단일-패스 형식은 단순 Σx^2 누산기에서 발생하는 심각한 자릿수 손실(Catastrophic cancellation)를 회피하며 채널당 세 개의 상태 워드만 필요로 한다.

3.2 Q16.16 고정소수점 데이터패스

각 채널은 Q16.16 고정소수점(정수부 16비트·소수부 16비트의 32비트 형식) 데이터패스를 사용한다. 표본 입력은 부호 있는 Q16.16 표현범위($|x| < 2^{15}$) 내의 16비트 값으로 취급되며(대상 게이트웨이의 센서 표본이 이 범위에 든다), 평균은 32비트 부호 있는 레지스터에, 2차 모멘트 누산기 M_2 는 Q31.16 형식의 48비트 부호 있는 레지스터(저장값 = $M_2 \times 2^{16}$)에 유지한다. M_2 의 오버플로 한계는 $(n-1) \cdot \sigma^2 \cdot 2^{16} < 2^{47}$ 로, 실험 잡음 수준($\sigma \approx 2.89$)에서 약 2.6×10^8 표본까지 오버플로 없이 처리되어 정상 운용에 충분하며, 이를 넘는 장기 연속 운용은 reset_stats 스트로브로 채널 상태를 주기적으로 재설정한다. 모든 곱셈과 덧셈은 정수 연산이다. 이로써 엔진은 부동소수점 소프트웨어에서 얻기 어려운 두 가지 성질을 갖는다: (i) 표본당 지연이 피연산자 값에 무관하며, (ii) 하드웨어 결과가 Welford 점화식을 그대로 따르는 파이썬 참조 구현과 비트 단위로 정확히 일치한다(10^6 개 무작위 스트림 시뮬레이션으로 사전 확인).

3.3 반복형 비트-직렬 나눗셈기

사이클 단위 Welford 데이터패스에서 지배적인 비용은 식 (3)의 δ/n 을 산출하는 나눗셈기이다. 단순 조합형 부호 있는 32비트 나눗셈기는 Cyclone V에서 약 9,200 LE로 합성되며, 이는 단일 채널만으로도 DE1-SoC 패브릭의 거의 30%에 해당한다. 우리

는 이를 사이클당 몫(Quotient) 한 비트를 처리하면서 부분-나머지(Partial-remainder) 레지스터와 몫-시프트 레지스터를 유지하고 비교 경로에서 단일 32비트 감산기를 사용하는 반복형 비트-직렬 나눗셈기로 대체한다. 이 유닛은 한 번의 나눗셈을 32 사이클에 완료하고, 주변 FSM에 start/done 핸드셰이크를 노출하며, 채널당 약 250 LE로 합성된다. 나눗셈 경로의 처리율 비용(표본당 32 사이클)은 동일한 FSM 사이클이 공유 곱셈기의 순차화에 재사용되므로 상쇄된다.

3.4 FSM 구동 공유 곱셈기

식 (2)~(4)와 3.5절의 3σ 검정을 직접 구현하면 표본당 4회의 넓은(wide) 곱셈이 필요하다. 즉 M_2 갱신용 $\delta \cdot \delta_2$, 이상치 분사용 δ^2 , 비교식 좌변용 $(n-1) \cdot \delta^2$, 우변용 $9 \cdot M_2$ 이다. 채널당 4개의 병렬 곱셈기를 두면 수십 개의 DSP 블록을 소비하게 되어 10채널에서 결정적 제약이 된다.

우리는 앞의 세 곱셈을 단일 32×32 부호 있는 곱셈기에 순차화한다. 상태기계가 구동하는 2-입력 멀티플렉서가 매 사이클의 피연산자 쌍을 선택한다. 즉 UPDATE_M2 상태는 (δ, δ_2) 를, OUTLIER_SQ 상태는 (δ, δ) 를, OUTLIER_MUL 상태는 $(\delta^2, n-1)$ 을 제시한다. 곱셈기 출력은 레지스터에 저장되어 M_2 에 누적되거나 우변과 비교된다. 네 번째 곱셈은 제공 없는 3σ 규칙에 의해 완전히 제거된다. 그 결과 채널당 곱셈기 수는 4개에서 1개로 줄어든다. 각 Q16.16 부호 있는 곱셈기는 약 3개의 Cyclone V 18×18 네이티브 DSP 블록에 매핑되므로, 10채널 엔진은 총 약 30개의 DSP를 소비한다.

3.5 제공 없는 3σ 규칙

교과서적인 3σ 검정 $|x - \mu| > 3\sigma$ 는 제공된 유닛을 요구한다. 양변을 제곱하고 $\sigma^2 = M_2 / (n-1)$ 을 교차곱하면 다음을 얻는다.

$$\delta^2 \cdot (n-1) > 9 \cdot M_2 \quad (5)$$

이 식에는 제공된 나눗셈도 없다. 좌변의 곱셈기는

공유 곱셈기 인스턴스이다. 우변의 곱셈기는 통상 네 번째 전용 곱셈기가 되겠지만, $9 = 8 + 1$ 이므로

$$9 \cdot M_2 = (M_2 \ll 3) + M_2 \quad (6)$$

이는 단일 시프트-덧셈이며 DSP 블록을 전혀 사용하지 않는다. 따라서 이상치 비교 경로 전체는 나눗셈기·제곱근·DSP가 없고 오직 덧셈, 시프트, 그리고 이미 존재하는 공유 곱셈기만으로 구성된다.

그림 2는 그 결과 얻어진 단일 채널 데이터패스를 보여준다. 입력 $x[n]$ 으로부터 $\delta = x - \mu$ 가 계산되고, 반복형 나눗셈기(32 사이클)가 δ/n 을 산출하여 평균을 갱신하며, $\delta_2 = x - \mu'$ 가 계산된다. 공유 곱셈기(채널당 1 DSP)가 $\delta \cdot \delta_2 \rightarrow \delta^2 \rightarrow \delta^2 \cdot (n-1)$ 을 순차적으로 수행하고, $M_2 \leftarrow M_2 + \delta \cdot \delta_2$ 로 갱신되며, 3σ 검정 $\delta^2 \cdot (n-1) > 9 \cdot M_2$ 가 이상치 플래그를 결정한다. 이 데이터패스는 IDLE에서 DONE까지 10-상태 FSM으로 구동되며, 첫 표본($n=1$)에서는 나눗셈기가 우회되고, $n \geq 2$ 부터는 모든 표본이 32-사이클 나눗셈기 지연을 온전히 치른다.

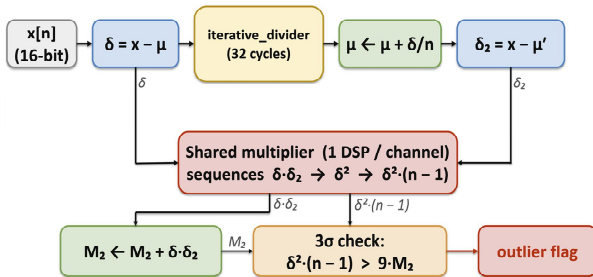


그림 2. Welford 코어 데이터패스 (단일 채널)
Fig. 2. Welford core datapath (single channel)

3.6 다채널 엔진 및 게이트웨이 통합

3.1~3.5절의 단일 채널 코어는 매개변수화된 SystemVerilog generate 구문으로 10회 복제된다. 채널별 출력(평균, M_2 , 표본 카운트, 이상치 플래그, ready)은 개별적으로 노출된다. 이상치 플래그는 또한 OR-축약 및 개수 집계되어, 상위 감독 계층에 1-사이클 “임의-이상치(Any-outlier)” 신호와 전체 이상치 카운트를 제공한다. 채널들은 상태를 공유하지 않으므로 한 센서의 결함이 다른 센서의 통계를 오

염시킬 수 없다.

통합 게이트웨이에서 각 Welford 출력은 ASCON-AEAD128 인증 암호화 파이프라인[5]의 해당 채널로 공급되며, 이는 엣지 IoT 기기용 경량 암호화에 관한 최근 FPGA 관행[7]을 따른다. 다만 Welford 엔진은 자기완결적(Self-contained)이어서 암호화 블록에 의존성이 없고, 두 모듈은 오직 채널별 data_valid / ready 핸드셰이크로만 통신한다.

IV. 결 과

4.1 FPGA 합성

엔진은 Terasic DE1-SoC 보드[10]의 Cyclone V 5CSEMA5F31C6 디바이스를 대상으로 Quartus Prime 21.1 Lite로 합성되었다. 표 1은 Welford 블록의 채널별 및 10채널 자원 예산을 요약한다.

표 1. Cyclone V 5CSEMA5F31C6 상 10채널 Welford 엔진의 자원 사용량

Table 1. Resource utilization of the ten-channel Welford engine on cyclone V 5CSEMA5F31C6

Item	Per channel	10 channels
LE	~250	~2,500
DSP	3	30
Latency	75 cyc	—
Fmax	—	> 70 MHz
Throughput	667k/s (calc.)	599k/s (meas.)

10채널 블록의 자원 사용량은 표 1과 같다. Welford 블록 단독의 Fmax는 70 MHz를 충분히 상회하여, 게이트웨이 상단으로부터 상속받은 50 MHz 패브릭 목표를 훨씬 넘어선다. 채널별 면적은 반복형 나눗셈기(약 250 LE)와 3-DSP 곱셈기 매크로 주변의 공유 곱셈기 제어부(약 80 LE)가 지배한다. 이상치 경로는 제공근 없는 3σ 규칙 덕분에 무시할 만한 면적만 기여한다.

두 최적화는 조합형 나눗셈기 약 9,200 LE를 250 LE로(약 97%), 곱셈기 4개를 1개로(75% DSP) 줄여, 표 1과 같이 10채널 합계가 Cyclone V(DE1-SoC)에 적합하게 들어맞는다.

4.2 지연시간, 처리량, 지터

표본당 Welford 지연은 10-상태 FSM을 순회한다. 8개 단일-사이클 연산 상태와, 반복형 나눗셈기 (DIVIDE_WAIT) 32 사이클, 파이프라인 레지스터 정착(Settling)에 약 35 사이클로, 합계 표본당 75 사이클이며 50 MHz에서 1.5 μ s이다.

엔진이 10개 채널 모두 활성화된 상태에서 TDM(Time-Division Multiplexing) 스케줄링으로 동작할 때, 센서 입력으로부터 암호화 출력까지의 중단 간 지연은 114 사이클로 결정론적이다(Welford 임계 경로 30 + 스케줄 2 + ASCON-128 78 + 출력 4 사이클). 채널 0의 연속 420,340개 표본에서 모든 표본이 정확히 114 사이클에 완료되었다(최소=최대=114, 지터=0). 32-사이클 나눗셈기는 하위 ASCON과 병렬로 동작하므로 임계 경로를 연장하지 않는다. 10개 채널 전체의 지속 처리율은 100 Mbit 이더넷 링크에서 초당 약 599,000 항목(측정 599,348 / 이론 600,000, 효율 99.9%)에 도달하고, 채널 분배는 완전 균등 대비 0.01% 이내이며 수신 항목의 100%가 정상 복호화되었다.

골든 소프트웨어 참조와의 비트 단위 일치는 전체 17.6M 항목 검증 윈도우(약 30초 실시간)에 대해 성립하므로, 하드웨어는 알고리즘 명세 대비 어떠한 수치 드리프트도 도입하지 않는다.

4.3 보드 검증 이상 탐지

3 σ 이상치 규칙은 AXI Lightweight HPS-to-FPGA 브리지를 통해 표본을 주입함으로써 DE1-SoC에서 직접 검증되었으며, 내부 센서 생성기는 우회하였다. 기준 분포는 $1000 \pm 5(\sigma \approx 2.89)$ 의 균등 분포였다. 500-표본 위밍업 이후, 6가지 주입 크기(2.08 σ , 2.77 σ , 3.46 σ , 5.20 σ , 6.93 σ , 10.4 σ)를 각 100회 시행하고, 10,000-표본 거짓 양성 스윕과 500-표본 사후 회복 스윕을 수행하였다.

측정 결과, 설계 3 σ 컷오프 미만의 두 크기(2.08 σ , 2.77 σ)는 각각 0/100 탐지로 과탐지가 없었고, 컷오프 바로 위의 3.46 σ 는 36/100으로 경험적 잡음 바닥 부근에서의 강건한 임계 동작과 부합하며, 5.20 σ 이상의 모든 크기는 100/100 탐지를 보였다. 거짓

양성 스윕은 10,500개 정상 표본(10,000 + 500 회복)에서 0건을 기록하여 경험적 거짓 양성률은 1×10^{-4} 미만이다.

탐지 지연은 ± 100 (약 35 σ)에서 별도로 측정하였다. CSR 쓰기로부터 이상치 카운트 증가까지의 시간(AXI 브리지 왕복 및 1회 Welford 사이클 포함)은 10/10 시행에서 2 - 3 μ s였다.

4.4 소프트웨어와의 비교

동일한 Welford 점화식의 소프트웨어 기준선을 온보드 ARM Cortex-A9의 PREEMPT_RT 리눅스[3]에서 실행한 결과를 하드웨어 엔진과 표 2에 비교하였다. 소프트웨어는 단일 채널에서 유사한 평균 처리율에 도달하나 네트워크 부하 시 100 μ s를 초과하는 꼬리-지연과 장기 실행 시 부동소수점 드리프트를 나타내는 반면, 하드웨어 엔진은 모든 표본을 75 사이클에 처리하고 정수 명세와 비트 단위로 일치하며 지터가 없다. 이 결정론의 대가는 표 1의 적정 수준 면적 예산이다.

표 2. 하드웨어 Welford 엔진과 소프트웨어 참조 구현 비교

Table 2. Comparison of the hardware Welford engine and the software reference

Metric	This work	SW (ARM)
Result	bit-exact	reference
Latency	75 cyc	variable
Tail lat.	none	> 100 μ s
Jitter	0	present
FP drift	none	yes

V. 논의 및 결론

제안 엔진은 온라인 다채널 통계 선별을 매우 낮은 비용(10채널에 대해 소형 Cyclone V 로직 예산의 8% 미만)과 표본 단위 결정론적 지연으로 FPGA 게이트웨이에 추가할 수 있음을 보인다. 세 최적화(반복형 나눗셈기·공유 곱셈기·시프트-덧셈 3 σ 규칙)는 상호 보강적으로 면적과 결정론을 동시에 확보한다.

주목할 만한 두 가지 한계가 있다. 첫째, Welford 점화식은 통계적으로 비강건(Non-robust)하다. 매우

큰 단일 이상치 하나가 μ 와 M_2 를 영구적으로 오염시켜 후속 작은 이상치를 놓칠 수 있으며, 보드 테스트에서도 이를 확인하였다. 실제 배치에서는 절대-범위 가드 또는 Hampel 필터와 같은 강건 추정기를 보완 계층으로 함께 두어야 한다. 둘째, 48비트 M_2 레지스터와 32비트 Q16.16 평균 레지스터는 유한한 동작 범위를 부과한다. 고잡음에서 매우 긴 실행은 채널별 상태를 느린 타이머로 재설정해야 하며, 본 구현은 이미 `reset_stats` 스트로브를 통해 이를 지원한다.

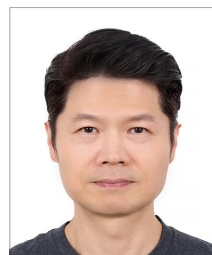
향후 연구는 결정론적 표본 단위 지연이 SoC 내 부편 아니라 네트워크를 통한 종단간에서도 보존되도록 엔진을 시간-민감 네트워킹(Time-sensitive networking) 전송으로 확장하고, 하드웨어 Welford를 매력적으로 만드는 비트 단위 정확 연산을 포기하지 않으면서 천천히 변하는 잡음 영역을 추적하는 적응형 α -곱셈기를 탐구할 것이다.

References

- [1] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions", IEEE Transactions on Industrial Informatics, Vol. 14, No. 11, pp. 4724-4734, Nov. 2018. <https://doi.org/10.1109/TII.2018.2852491>.
- [2] B. P. Welford, "Note on a method for calculating corrected sums of squares and products", Technometrics, Vol. 4, No. 3, pp. 419-420, Aug. 1962. <https://doi.org/10.1080/00401706.1962.10490022>.
- [3] F. Reghenzani, G. Massari, and W. Fornaciari, "The real-time Linux kernel: A survey on PREEMPT_RT", ACM Computing Surveys, Vol. 52, No. 1, pp. 1-36, Feb. 2020. <https://doi.org/10.1145/3297714>.
- [4] S. Trimberger and J. Moore, "FPGA security: Motivations, features, and applications", Proceedings of the IEEE, Vol. 102, No. 8, pp. 1248-1265, Aug. 2014. <https://doi.org/10.1109/JPROC.2014.2331672>.
- [5] National Institute of Standards and Technology, "Ascon-Based Lightweight Cryptography Standards", NIST SP 800-232, pp. 1-75, Aug. 2024. <https://doi.org/10.6028/NIST.SP.800-232>.
- [6] S. Moon, "Interleaved ASCON-128 Hardware Implementation for Multi-Channel IIoT Environments", Journal of KIIT, Vol. 24, No. 2, pp. 121-126, Feb. 2026. <https://doi.org/10.14801/jkiit.2026.24.2.121>.
- [7] A. Koppuravuri, H. Pasupuleti, S. Gvk, and J. Bapat, "A high throughput ASCON architecture for secure edge IoT devices", Proc. IEEE International Conference on VLSI Design (VLSID), Kolkata, India, Jan. 2024. <https://doi.org/10.1109/VLSID60093.2024.00087>.
- [8] H.-M. Lee, S.-H. Jeon, and S.-H. Ok, "An Implementation of a Reconfigurable Module-based CNN Accelerator", Journal of KIIT, Vol. 20, No. 4, pp. 69-79, Apr. 2022. <https://doi.org/10.14801/jkiit.2022.20.4.69>.
- [9] D. E. Knuth, "The Art of Computer Programming, Volume 2: Seminumerical Algorithms", 3rd ed., Addison-Wesley, pp. 232-233, 1997.
- [10] Terasic Technologies, "DE1-SoC User Manual", 2014. <https://www.terasic.com.tw/>. [accessed: Jul. 06, 2026]

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, IoT
임베디드시스템