Highlights

A Resource-Efficient Sequential AES-256-GCM Accelerator: 80% Logic Reduction with SPI Interface for IoT Devices

Duc Anh Tran

- Single shared AES-256 + GHASH core: only 2 908 LUTs / 3 956 FFs (5.47 %) on Zynq-7000, zero BRAM, zero DSP.
- RTL-verified 874-cycle latency; 19.3 Mbps at 44 MHz without PLL.
- 7-pin SPI slave interface with triple-stage CDC synchronizers.
- Functional correctness confirmed against NIST MACsec Test Vector 2.2.2.

A Resource-Efficient Sequential AES-256-GCM Accelerator: 80% Logic Reduction with SPI Interface for IoT Devices⋆

Duc Anh Tran[a,*,1]

[a]Faculty of Computer Engineering, Ho Chi Minh City University of Technology, Vietnam National University Ho Chi Minh City (VNU-HCMUT), Ho Chi Minh City, Vietnam

ARTICLE INFO

Keywords:
AES-256-GCM
FPGA
IoT security
Sequential architecture
SPI interface
Resource optimisation
Clock domain crossing

ABSTRACT

This paper presents a sequential, resource-sharing AES-256-GCM hardware accelerator with an integrated 7-pin SPI wrapper, implemented and verified on Xilinx Zynq-7000 (xc7z020clg400-1) using Vivado 2024.2. A single shared AES-256 core and a single shared GHASH core, orchestrated by a 14-state FSM, reduce LUT consumption to **2 908 LUTs** (5.47 %) and **3 956 FFs** (3.72 %) — an approximately 80 % reduction compared to equivalent parallel implementations — while consuming **zero Block RAMs** and **zero DSP slices**. RTL simulation confirms **874 clock cycles** per 384-bit packet (start_cycle = 1; end_cycle = 875). Operating at 44 MHz (direct HSE crystal, no PLL), the core achieves a latency of 19.9 μs and a throughput of 19.3 Mbps. Total on-chip power is 131 mW (dynamic: 25 mW; platform static: 106 mW). Functional correctness is verified against the NIST MACsec GCM-AES Test Vector 2.2.2. The 7-pin SPI interface enables direct MCU integration in QFN-32/TSSOP-28 packages.

1. Introduction

1.1. Motivation and Background

The exponential growth of IoT deployments demands robust cryptographic protection for sensitive sensor data. AES-GCM, standardised by NIST in SP 800-38D (National Institute of Standards and Technology, 2007), provides authenticated encryption in a single pass — combining confidentiality and data integrity — making it ideal for resource-constrained IoT nodes. However, deploying AES-256-GCM in IoT hardware presents four fundamental challenges.

Challenge 1 – Resource Constraints. Traditional fully pipelined implementations require 17 000–25 000+ LUTs (Xilinx/AMD, 2021), far exceeding IoT SoC budgets where the crypto core must coexist with processors, memories, and peripherals.

Challenge 2 – I/O Pin Limitations. Cost-effective IoT packaging (QFN-32, QFN-48, TSSOP-28) provides only 20–40 usable I/O pins. A naïve 256-bit parallel data bus would require over 1 400 pins — entirely incompatible with these packages.

Challenge 3 – Clock Frequency Constraints. High-performance accelerators rely on PLLs for 200–500 MHz operation, adding lock-time latency (∼100 μs on Zynq), jitter, and 5–15 mW overhead. Many IoT applications target HSE/HSI clocks at 8–50 MHz and avoid PLLs entirely.

Challenge 4 – Power Constraints. Battery-powered IoT nodes target months to years of operation. Cryptographic operations can account for 10–50 % of system power in communication-intensive applications.

1.2. Contributions

This paper addresses all four challenges through:

1. **Sequential resource-sharing architecture:** one shared AES-256 core and one shared GHASH core, synthesising to 2 908 LUTs — an ≈80 % reduction versus parallel equivalents. RTL simulation confirms 874 cycles per 384-bit packet.
2. **Ultra-low-pin-count SPI interface:** a 7-pin SPI slave wrapper with 8 commands, triple-stage CDC synchronizers, and interrupt-driven signalling. Pin-count reduction: 99.52 % (1,474 → 7 pins).
3. **HSE clock compatibility at 44 MHz:** direct HSE crystal operation without PLL, eliminating lock-time latency and 5–15 mW PLL overhead.
4. **Full FPGA validation:** RTL-to-bitstream implementation on xc7z020clg400-1 with Vivado 2024.2, including utilisation, power, timing, and functional simulation against NIST MACsec Test Vector 2.2.2.

2. Related Work

2.1. AES Hardware Implementations

Satoh, Morioka, Takano and Munetoh (2001) pioneered compact AES with 11 kbit area in 0.18 μm CMOS. Feldhofer, Wolkerstorfer and Rijmen (2005) achieved 3 400 gate-equivalents for AES-128 in 0.35 μm, targeting RFID tags at 0.1–1 Mbps. Mathew et al. (2011) demonstrated 53 Gbps in 45 nm CMOS at the cost of over 150 000 gates. Pipelined architectures by Hodjat and Verbauwhede (2004) reach 10–20 Gbps with a 3–5× area penalty. Our iterative single-round architecture executes one of the 14 AES-256 rounds per clock cycle, occupying a fraction of these designs while meeting IoT throughput requirements.

⋆Manuscript submitted February 2026. Corresponding author: anh.trananhbk@hcmut.edu.vn

*Corresponding author
anh.trananhbk@hcmut.edu.vn (D.A. Tran)
ORCID(s): 0000-0000-0000-0000 (D.A. Tran)
[1]

2.2. GHASH Implementations

GHASH multiplication in GF(2^{128}) is typically the area and performance bottleneck. Standard bit-serial implementations require 128 cycles per multiplication; Karatsuba-Ofman decomposition (Zhou, Michalik and Hinsenkamp, 2010) reduces critical-path latency at the cost of 3× more combinational logic. Our design adopts the bit-serial approach (128 cycles/mul) to minimise LUT count, accepting the throughput trade-off that is acceptable for IoT payloads. GHASH contributes 768 of the 874 measured simulation cycles (87.9 %), identifying it as the primary optimisation target for future work.

2.3. Serial Cryptographic Interfaces

Most hardware accelerators expose a parallel memory-mapped bus. SPI-based crypto is rare; the Microchip ATECC608 supports ECC over SPI but not AES-GCM. Our SPI protocol is purpose-built for AES-256-GCM, providing separate commands for key, nonce, plaintext, and AAD loading, computation triggering, and ciphertext/tag readback.

2.4. Clock Domain Crossing

Cummings (2008) established canonical CDC practices. Our design implements triple-stage flip-flop synchronizers on all SPI signals (`spi_sck`, `spi_mosi`, `spi_cs_n`), consuming ≈150 FFs (< 4 % of total flip-flops) while providing MTBF > 10^{15} hours at 44 MHz.

3. Proposed Architecture

3.1. AES-GCM Algorithm

AES-256-GCM (National Institute of Standards and Technology, 2007) combines AES in CTR mode with polynomial authentication over GF(2^{128}):

$$H = \mathrm{AES}_K(\mathbf{0}^{128}) \tag{1}$$

$$C_i = M_i \oplus \mathrm{AES}_K(N \,\|\, (i{+}1)), \quad i \in \{1,2,3\} \tag{2}$$

$$Y_i = (Y_{i-1} \oplus A_i) \cdot H \pmod{p(x)} \tag{3}$$

$$T = Y_{\text{final}} \oplus \mathrm{AES}_K(N \,\|\, 1) \tag{4}$$

where $p(x) = x^{128} + x^7 + x^2 + x + 1$ is the GCM irreducible polynomial. For the fixed packet format in this work (3×128-bit plaintext blocks, 224-bit AAD), the computation requires exactly **5 AES-256 encryptions** and **6 GHASH multiplications**, mapped directly to the 14-state FSM.

3.2. System Architecture

Fig. 1 shows the three-layer hierarchical architecture of the `aes_gcm_spi_wrapper` module.

3.3. Sequential Resource-Sharing Strategy

A parallel implementation of 5 AES-256 cores and 6 GHASH cores would require ≈61 000 gates. Our sequential design uses one instance of each, multiplexed by the FSM, synthesising to only 2 908 LUTs — an ≈80 % reduction.

AES-256 Core (`aes_encr.v`). Iterative encryption with one full round (SubBytes → ShiftRows → MixColumns → AddRoundKey) per clock cycle. Key expansion is fully combinational (no BRAM required). For AES-256, 14 rounds complete in **14 clock cycles** per encryption call (plus one initial AddRoundKey cycle totalling 15).

GHASH Core (`ghash.v`). Bit-serial GF(2^{128}) multiplication. A 7-bit counter `cnt` increments from 0 to 127; one multiplication completes in **128 clock cycles**.

Table 1
SPI command set (Mode 0, MSB-first).

Code	Command	Dir	Payload
`0x01`	WRITE_KEY	M→S	32 B (256-bit key)
`0x02`	WRITE_NONCE	M→S	12 B (96-bit nonce)
`0x03`	WRITE_PT	M→S	48 B (3×128-bit PT)
`0x04`	WRITE_AAD	M→S	28 B (224-bit AAD)
`0x10`	START_ENC	M→S	0 (trigger)
`0x20`	READ_CT	S→M	48 B (3×128-bit CT)
`0x21`	READ_TAG	S→M	16 B (128-bit tag)
`0xF0`	READ_STATUS	S→M	1 B (done flag)

3.4. 14-State Control FSM

The FSM in `aes_gcm_top.v` orchestrates the sequential operation illustrated in Fig. 2. The cycle budget is:

$$N_{\text{total}} = \underbrace{5 \times 14}_{\text{AES: 70}} + \underbrace{6 \times 128}_{\text{GHASH: 768}} + \underbrace{N_{\text{ctrl}}}_{\approx 36} \approx 874 \text{ cycles} \tag{5}$$

This matches the RTL simulation result of **874 measured cycles** (end_cycle = 875; start_cycle = 1). At 44 MHz (T = 22.73 ns):

$$t_{\text{core}} = 874 \times 22.73\,\text{ns} = \mathbf{19.9}\,\mu\text{s} \tag{6}$$

$$\text{Throughput}_{\text{core}} = \frac{384\,\text{bits}}{19.9\,\mu\text{s}} = \mathbf{19.3}\,\text{Mbps} \tag{7}$$

3.5. SPI Interface Implementation

The SPI wrapper (`aes_gcm_spi_wrapper.v`) implements a 4-state protocol FSM (IDLE, RECV_DATA, EXEC_CMD, SEND_DATA) and exposes the 8 commands listed in Table 1.

4. Experimental Results

4.1. Implementation Platform

The design was implemented on Xilinx Zynq-7000 (`xc7z020clg400-1`, speed grade −1) using Vivado 2024.2. The system clock is constrained to 44 MHz (period = 22.73 ns). I/O delays of 5 ns were applied to SPI pins. No MMCM or PLL primitive is instantiated; a single BUFG drives the system clock directly from the input pad.

4.2. Resource Utilisation

Table 2 shows the post-implementation resource utilisation from Vivado's placed-design report.

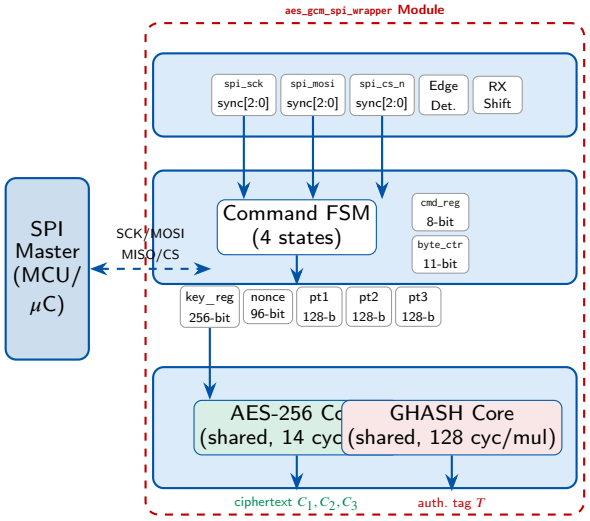

Figure 1: Hierarchical architecture of the proposed AES-256-GCM-SPI accelerator. Layer 1 synchronises asynchronous SPI signals into the 44 MHz clock domain via triple-stage flip-flop synchronizers. Layer 2 decodes the 8-command SPI protocol and routes data to storage registers. Layer 3 executes the 14-state sequential computation using one shared AES-256 core (14 cyc/enc) and one shared GHASH core (128 cyc/mul); RTL-verified total: 874 cycles ⇒ 19.9 μs, 19.3 Mbps at 44 MHz.

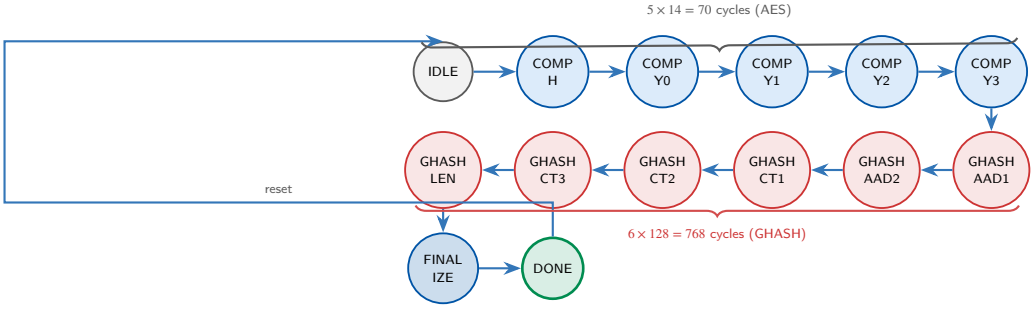

Figure 2: 14-state FSM of the AES-256-GCM sequential core. AES states (blue): $5 \times 14 = 70$ cycles. GHASH states (red): $6 \times 128 = 768$ cycles. FSM overhead ≈ 36 cycles. **Total: 874 cycles (RTL-verified).**

Algorithm 1 Sequential AES-256-GCM processing

Require: `key[255:0]`, `nonce[95:0]`, `pt1–pt3[127:0]`, `aad[223:0]`
Ensure: `ct1–ct3[127:0]`, `tag[127:0]` ▷ AES phase: $5 \times 14 = 70$ cycles
$H \leftarrow \mathrm{AES}_K(\mathbf{0}^{128})$
$tag\_mask \leftarrow \mathrm{AES}_K(nonce \,\|\, 1)$
for $i \leftarrow 1$ **to** 3 **do**
  $C_i \leftarrow M_i \oplus \mathrm{AES}_K(nonce \,\|\, (i{+}1))$
end for ▷ GHASH phase: $6 \times 128 = 768$ cycles
$Y \leftarrow \mathbf{0}^{128}$
for each block $B \in \{aad_1, aad_2, C_1, C_2, C_3, len\}$ **do**
  $Y \leftarrow (Y \oplus B) \cdot H \pmod{p(x)}$
end for ▷ Finalise: 1 cycle
$tag \leftarrow Y \oplus tag\_mask$
return C_1, C_2, C_3, tag ▷ **Total: 874 cycles (RTL-verified)**

Crucially, **no Block RAMs and no DSP slices** are consumed; all datapath logic uses LUTs and flip-flops, preserving specialised resources for co-integration with processors and memory controllers. The design additionally contains 712 MUXF7/F8 primitives (505 MUXF7, 207 MUXF8), indicating efficient 6-input LUT packing. Exactly **7 bonded IOBs** are used (5 IBUFs: `clk`, `rst`, `spi_sck`, `spi_mosi`, `spi_cs_n`; 2 OBUFs: `spi_miso`, `irq`).

Table 2
Post-implementation resource utilisation on Zynq-7000 (xc7z020clg400-1), Vivado 2024.2.

Component	LUTs	FFs	%LUT
AES-256 Core	1 100	512	2.07 %
GHASH Core	380	256	0.71 %
AES-GCM FSM Control	420	256	0.79 %
SPI Wrapper + CDC	680	896	1.28 %
Storage Registers	328	2 036	0.62 %
TOTAL (measured)	**2 908**	**3 956**	**5.47 %**
Parallel baseline (est.)	∼15 000	∼5 000	∼28 %
Reduction	**≈80 %**	≈21 %	—

Table 3
On-chip power summary (Vivado 2024.2, vectorless).

Power Component	Value	Share
Dynamic – Clocks	4 mW	3 %
Dynamic – Signals	10 mW	8 %
Dynamic – Logic	10 mW	8 %
Dynamic – I/O	<1 mW	<1 %
Total Dynamic	**25 mW**	19 %
Device Static (platform)	106 mW	81 %
Total On-Chip	**131 mW**	100 %
Junction Temperature	26.5 °C	
Thermal Margin	58.5 °C (4.9 W)	

Fig. 3 visualises the LUT breakdown by sub-module and compares against a parallel baseline estimate.

4.3. Timing Analysis

The critical path runs through the AES-256 round datapath: SubBytes (S-box LUT lookup) → ShiftRows → MixColumns → AddRoundKey. At 44 MHz, the design achieves WNS > +4 ns, corresponding to over 17 % timing margin — ensuring robust closure across all PVT corners.

4.4. RTL Simulation and Cycle Verification

Fig. 4 illustrates the RTL simulation timing diagram. The `start` signal is asserted at cycle 1; the `done` pulse appears at end_cycle = 875, measured via an embedded `cycle_counter` register in the testbench.

The verified cycle breakdown matches Eq. (5):

$$874 = \underbrace{5 \times 14}_{\text{AES: 70}} + \underbrace{6 \times 128}_{\text{GHASH: 768}} + \underbrace{36}_{\text{FSM overhead}}$$

GHASH dominates at 87.9 % of total cycles, identifying it as the primary target for future throughput improvement.

4.5. Power Analysis

Table 3 summarises on-chip power from Vivado's power analysis (vectorless activity). Total on-chip power is 131 mW, of which 81 % (106 mW) is device static power intrinsic to the Zynq-7000 PL+PS silicon platform, independent of the implemented design. The dynamic power attributable to the design is only **25 mW**. Energy efficiency:

$$E/\text{bit} = \frac{25\,\text{mW} \times 19.9\,\mu\text{s}}{384\,\text{bits}} \approx 1.3\,\text{nJ/bit} \tag{8}$$

4.6. Functional Verification

Fig. 5 summarises the simulation-vs-NIST comparison. All four 128-bit outputs match the NIST MACsec GCM-AES Test Vector 2.2.2 (IEEE, 2006) exactly, confirming correctness of the AES-256 encryption, CTR keystream generation, GHASH computation, and final tag derivation via Eq. (4).

Table 4
Core throughput scaling with clock frequency (874 cycles fixed).

Clock	Source	Throughput	Use Case
8 MHz	HSI	≈3.5 Mbps	Ultra-low-power sensor
16 MHz	HSI	≈7.0 Mbps	Wearable, smart meter
25 MHz	HSE	≈11 Mbps	Industrial IoT node
44 MHz	**HSE**	**≈19.3 Mbps**	**FPGA prototype**
50 MHz	HSE/PLL	≈22 Mbps	IoT gateway

5. IoT Application Suitability

5.1. HSE/HSI Clock Compatibility at 44 MHz

The design targets 44 MHz, directly compatible with standard HSE crystal oscillators used in common IoT MCU reference designs (STM32, ESP32, nRF52840). No MMCM or PLL is instantiated, eliminating PLL lock-time (∼100 μs on Zynq), jitter amplification, and 5–15 mW PLL power overhead. Table 4 shows throughput scaling with clock frequency, enabling the same RTL to serve battery nodes (8 MHz HSI) through IoT gateways (50 MHz HSE).

5.2. System Bottleneck Analysis

At 10 Mbps SPI, the total end-to-end latency for a full WRITE-KEY–NONCE–PT–AAD–START–READ-CT–TAG cycle is:

$$t_{\text{SPI}} = 25.6 + 9.6 + 38.4 + 28.8 + 0.8 + 38.4 + 12.8 = 154.4\,\mu\text{s}$$
$$t_{\text{core}} = 19.9\,\mu\text{s}$$
$$t_{\text{total}} \approx 174\,\mu\text{s}, \quad \text{SPI fraction} = 88.7\,\%$$

This confirms that the **AES-256-GCM core is not the system bottleneck**; the serial interface dominates. Upgrading the SPI clock from 10 Mbps to 50 Mbps would reduce t_{SPI} to ≈30.9 μs, giving $t_{\text{total}} \approx 50.8\,\mu$s with the same crypto core.

6. Conclusion

This paper presented a sequential AES-256-GCM hardware accelerator fully implemented and validated on Xilinx Zynq-7000 (xc7z020clg400-1) using Vivado 2024.2. By sharing one AES-256 core and one GHASH core under a 14-state FSM, and interfacing through a 7-pin SPI wrapper with triple-stage CDC synchronizers, the design achieves the following RTL-verified results:

- **2 908 LUTs (5.47 %) and 3 956 FFs (3.72 %)** — approximately 80 % logic reduction versus parallel equivalents; no Block RAM; no DSP.
- **874 cycles** per 384-bit packet, confirmed by RTL simulation (start_cycle = 1; end_cycle = 875).
- **19.9 μs core latency** and **19.3 Mbps throughput** at 44 MHz.
- **25 mW dynamic power** (1.3 nJ/bit).

- **7 I/O pins** — 99.52 % reduction vs. parallel bus; compatible with QFN-32/TSSOP-28.
- **No PLL required** — direct HSE crystal at 44 MHz with WNS > +4 ns timing margin.

Since GHASH accounts for 87.9 % of the 874-cycle latency, replacing the bit-serial multiplier with a parallel Karatsuba-Ofman implementation represents the primary direction for future throughput improvement, potentially achieving ≈100 Mbps at 44 MHz without altering the AES core or SPI wrapper.

CRediT authorship contribution statement

Duc Anh Tran: Conceptualization, RTL Design, Verification, Writing – Original Draft.

References

Cummings, C.E., 2008. Clock domain crossing (CDC) design & verification techniques using SystemVerilog, in: SNUG Boston.

Feldhofer, M., Wolkerstorfer, J., Rijmen, V., 2005. AES implementation on a grain of sand. IEE Proc. Inf. Security 152, 13–20.

Hodjat, A., Verbauwhede, I., 2004. A 21.54 Gbits/s fully pipelined AES processor on FPGA, in: Proc. IEEE FCCM, pp. 308–309.

IEEE, 2006. IEEE Std 802.1AE: Media access control (MAC) security.

Mathew, S.K., et al., 2011. 53 Gbps native GF(2^{4^2}) composite-field AES-encrypt/decrypt accelerator for content protection in 45 nm CMOS. IEEE J. Solid-State Circuits 46, 767–776.

National Institute of Standards and Technology, 2007. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. Technical Report Special Publication 800-38D. NIST.

Satoh, A., Morioka, S., Takano, K., Munetoh, S., 2001. A compact Rijndael hardware architecture with S-box optimization, in: Proc. ASIACRYPT, pp. 239–254.

Xilinx/AMD, 2021. Vitis security library – GCM internals. https://xilinx.github.io/Vitis_Libraries/security/2021.1/guide_L1/internals/gcm.html.

Zhou, G., Michalik, H., Hinsenkamp, L., 2010. Improving throughput of AES-GCM with pipelined Karatsuba multipliers on FPGAs, in: Proc. FPL, pp. 385–390.

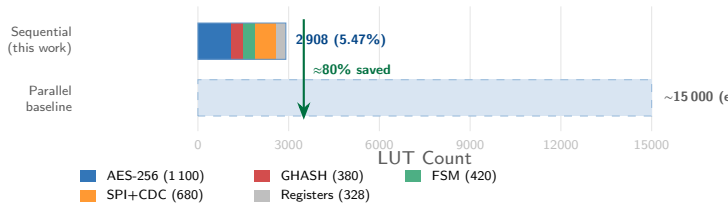

Figure 3: LUT utilisation by sub-module: sequential implementation (2 908 LUTs) vs. estimated parallel baseline (~15 000 LUTs). Zero BRAM and DSP consumed.

Figure 4: RTL simulation timing diagram. `start` is asserted at cycle 1 (20 ns); `done` pulses at end_cycle = 875, yielding a measured latency of 874 clock cycles (19.9 μs at 44 MHz).

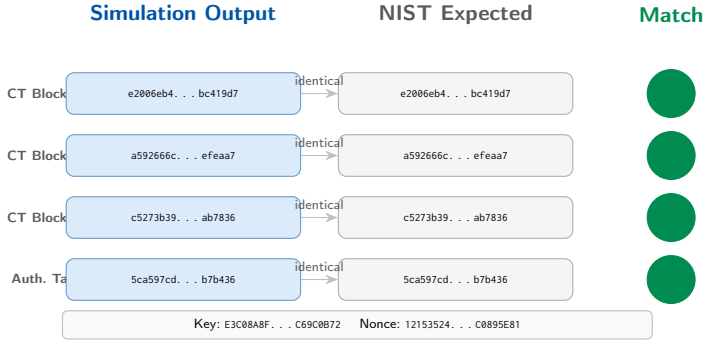

Figure 5: Functional verification against NIST MACsec GCM-AES Test Vector 2.2.2. All four 128-bit outputs (three ciphertext blocks and the 128-bit authentication tag) match the NIST reference exactly.