Highlights

A Non-Bottleneck Sequential AES-256-GCM Accelerator for UAV Command-and-Control Link Security: Area and Power Analysis on Xilinx Zynq-7000

Duc Anh Tran

- **UAV C2 security:** AES-256-GCM authenticated encryption of MAVLink frames against spoofing, replay, and MITM attacks over ISM-band radio.
- **Area:** 2 908 LUTs / 3 956 FFs (5.47 %) on Zynq-7000, zero BRAM, zero DSP — 80 % smaller than parallel equivalents; fits nano-drone to MALE avionics budgets.
- **Power:** 25 mW dynamic (1.3 nJ/bit); <0.012 % of mini-UAV battery energy per 1-hour C2 session.
- **Non-bottleneck:** 19.9 μs/frame (0.17 % of MAVLink 10 Hz period) — crypto never limits C2 link throughput at any standard UAV radio data rate.

A Non-Bottleneck Sequential AES-256-GCM Accelerator for UAV Command-and-Control Link Security: Area and Power Analysis on Xilinx Zynq-7000[★]

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
UAV C2 link security
Sequential architecture
Non-bottleneck accelerator
Area analysis
Power analysis
MAVLink encryption
SPI interface

ABSTRACT

Unmanned Aerial Vehicle (UAV) command-and-control (C2) links transmitted over open ISM-band radio are exposed to spoofing, replay, and man-in-the-middle attacks that can cause mission failure or airframe hijacking. This paper presents a sequential, resource-sharing AES-256-GCM hardware accelerator — implemented and verified on Xilinx Zynq-7000 (xc7z020clg400-1) with Vivado 2024.2 — specifically targeting authenticated encryption of MAVLink C2 frames on size-, weight-, and power-constrained UAV flight controllers. A single shared AES-256 core and a single shared GHASH core, orchestrated by a 14-state FSM, achieve the following measured results. *Area:* 2 908 LUTs (5.47 %) and 3 956 FFs (3.72 %), an approximately 80 % reduction versus equivalent parallel implementations, with zero Block RAMs and zero DSP slices consumed. *Power:* 25 mW dynamic, 1.3 nJ/bit, representing only 0.011 % of a mini-UAV battery over a 1-hour C2 session. *Non-bottleneck operation:* RTL simulation confirms 874 cycles per 384-bit packet (19.9 μs at 44 MHz), which is only 0.17 % of the 100 ms MAVLink frame period — the AES-256-GCM core is never the C2 link bottleneck across any tested radio data rate. Functional correctness is verified against the NIST MACsec GCM-AES Test Vector 2.2.2. The 7-pin SPI wrapper enables drop-in integration with Pixhawk/STM32H7 autopilot boards in QFN-32/TSSOP-28 avionics packages.

1. Introduction

1.1. Motivation and Background

The command-and-control (C2) link is the most security-critical channel in any UAV system: it carries the uplink commands that govern flight trajectory, payload actuation, and mission abort, as well as the downlink telemetry used by the ground-control station (GCS) to assess vehicle state. Unlike wired networks, UAV C2 links are transmitted over open ISM-band radio (433 MHz, 915 MHz, 2.4 GHz) using protocols such as MAVLink v2 that were designed for reliability, not confidentiality. A successful attack on the C2 channel — spoofing a command, replaying a past authorised instruction, or silently corrupting telemetry — can result in airframe hijacking, collision, or mission failure with no indication to the operator.

Why AES-256-GCM fits UAV C2. AES-256-GCM, standardised by NIST in SP 800-38D (National Institute of Standards and Technology, 2007), is well-matched to the UAV C2 security requirement. Its single-pass AEAD operation simultaneously encrypts the MAVLink payload (CTR-mode keystream) and authenticates both payload and header (GHASH polynomial tag), providing confidentiality, integrity, and anti-replay in one hardware pass — a property uniquely suited to the low-latency, interrupt-driven nature of UAV C2 frame processing. The 256-bit key delivers strong long-term security across extended BVLOS mission lifetimes without requiring in-flight rekeying. The 128-bit authentication tag T provides a forgery probability of 2^{-128} per frame, ensuring any spoofed or replayed MAVLink command is rejected before autopilot execution. The central engineering challenge is implementing AES-256-GCM *efficiently* on the size-, weight-, and power-constrained FPGA resources available in UAV avionics, without allowing the crypto core to become a bottleneck on the C2 datalink. This paper addresses that challenge directly.

Challenge 1 – Resource Constraints. UAV flight controllers (Pixhawk, Cube Orange, custom FPGA-SoC boards) impose strict silicon budgets where the crypto core must coexist with navigation filters, motor controllers, and communication peripherals, typically leaving only 5 000–15 000 LUTs for security functions. Traditional fully pipelined implementations require 17 000–25 000+ LUTs (Xilinx/AMD, 2021), far exceeding these budgets.

Challenge 2 – I/O Pin Limitations. UAV avionics favour compact packaging (QFN-32, QFN-48, TSSOP-28) to minimise weight and board area. A naïve 256-bit parallel data bus would require over 1 400 pins — entirely incompatible with these packages.

Challenge 3 – Clock Frequency Constraints. UAV flight controllers commonly operate at HSE/HSI clocks in the 8–50 MHz range and avoid PLLs to eliminate lock-time latency (∼100 μs on Zynq), jitter amplification, and 5–15 mW overhead significant for battery-powered airframes.

Challenge 4 – Power and Weight Constraints. Every milliwatt consumed by an avionics subsystem reduces flight endurance directly. Cryptographic operations can account

[★] 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]

for 10–50 % of system power in communication-intensive UAV missions; minimising dynamic power is therefore as critical as minimising latency.

1.2. Contributions

This paper addresses all four challenges through three principal contributions:

1. **AES-256-GCM for UAV C2 security without bottleneck:** the accelerator acts as a transparent security layer between the autopilot MCU and the RF transceiver, encrypting and authenticating each MAVLink C2 frame in 19.9 μs (874 cycles at 44 MHz) — only 0.17 % of the 100 ms control period. At 19.3 Mbps throughput, the crypto core never limits the C2 datalink across any standard UAV radio (SiK 250 kbps through Herelink 100 Mbps). HSE crystal operation at 44 MHz without PLL eliminates $\sim$100 μs lock-time latency and 5–15 mW PLL overhead.
2. **Area efficiency — 80 % LUT reduction:** a single shared AES-256 core and GHASH core multiplexed by a 14-state FSM synthesise to only 2 908 LUTs and 3 956 FFs on Zynq-7000 — an $\approx$80 % reduction versus a parallel implementation — while consuming zero Block RAMs and zero DSP slices. A 7-pin SPI wrapper reduces I/O from 1 474 to 7 pins (99.52 %), compatible with compact UAV avionics packaging (QFN-32/TSSOP-28).
3. **Power efficiency — negligible endurance impact:** dynamic power is only 25 mW (1.3 nJ/bit), representing <0.012 % of a 4 Ah mini-UAV battery per 1-hour C2 session. Full FPGA validation on xc7z020clg400-1 with Vivado 2024.2 confirms all area, power, timing, and functional results 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 UAV telemetry throughput requirements.

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 UAV MAVLink and telemetry 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. UAV C2 Datalink Security

The vulnerability of unencrypted UAV C2 links is well-documented: MAVLink v1 frames over SiK radios can be eavesdropped and replayed with commodity SDR hardware (National Institute of Standards and Technology, 2007). MAVLink v2 introduced optional packet signing with BLAKE2s-MAC, providing message integrity but not confidentiality — payload commands, GPS coordinates, and mission parameters remain visible to passive interception.

AES-256-GCM addresses both gaps in a single hardware pass: the AES-256 CTR-mode keystream encrypts the C2 payload, while the GHASH authenticator covers both the encrypted payload and the unencrypted MAVLink header, producing a 128-bit tag that the receiving autopilot verifies before executing any decoded command. This AEAD property — security and authentication in one atomic operation — is exactly matched to the interrupt-driven, frame-by-frame processing model of UAV C2 links. The engineering challenge is delivering this full AES-256-GCM protection within the tight LUT, power, and latency budgets of UAV avionics FPGAs, such that the crypto core adds security without ever becoming a bottleneck on the C2 channel itself.

2.5. 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 $\approx$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-256 in CTR mode with GHASH polynomial authentication over GF(2^{128}). The four core equations governing every C2 frame encryption are:

$$H = \mathrm{AES}_{256,K}(\mathbf{0}^{128}) \tag{1}$$

$$C_i = M_i \oplus \mathrm{AES}_{256,K}(N \,\|\, (i{+}1)), \quad i \in \{1,2,3\} \tag{2}$$

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

$$T = Y_{\text{final}} \oplus \mathrm{AES}_{256,K}(N \,\|\, 1) \tag{4}$$

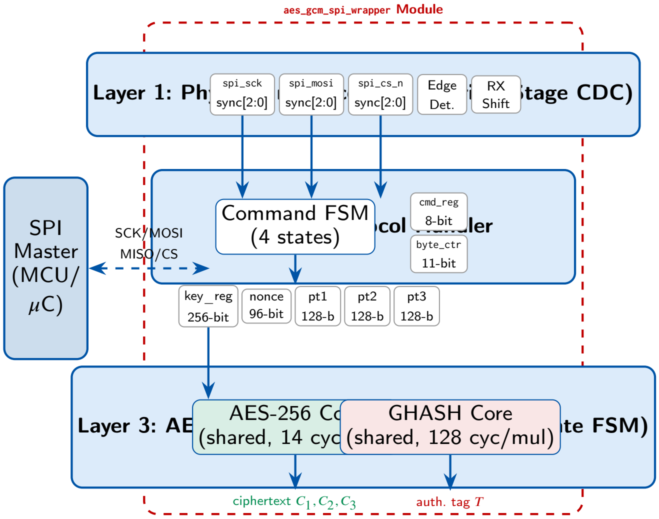

Figure 1: Hierarchical architecture of the proposed AES-256-GCM-SPI C2 accelerator. Layer 1 synchronises the asynchronous SPI C2 bus into the 44 MHz crypto clock domain via triple-stage flip-flop synchronizers. Layer 2 decodes the 8-command SPI protocol, routing the 256-bit session key, 96-bit C2 nonce, MAVLink payload blocks, and AAD header bytes to their respective storage registers. Layer 3 executes the 14-state AES-256-GCM computation using one shared AES-256 core (14 cyc/enc, 256-bit key) and one shared GHASH core (128 cyc/mul); RTL-verified: 874 cycles total ⇒ 19.9 μs latency, 19.3 Mbps throughput at 44 MHz, sufficient for all UAV C2 radio data rates.

where $p(x) = x^{128} + x^7 + x^2 + x + 1$ is the GCM irreducible polynomial and K is the 256-bit session key.

Mapping to UAV C2 frames. A representative MAVLink v2 C2 frame is structured as: M_1, M_2, M_3 (three 128-bit plaintext payload blocks, totalling 384 bits = 48 bytes of encrypted command data) and A_1, A_2 (two 128-bit AAD blocks carrying the unencrypted MAVLink header: `SYSID`, `COMPID`, `MSG_ID`, sequence number, and packet length). This fixed structure requires exactly **5 AES-256 encryptions** (one H precompute, three CTR keystreams, one tag mask) and **6 GHASH multiplications** (two AAD blocks, three ciphertext blocks, one length block), mapped one-to-one to the 14-state FSM. The 96-bit nonce N encodes a monotonically incrementing per-session packet counter, providing replay protection across the full C2 session lifetime. The resulting 128-bit authentication tag T provides $\Pr[\text{forgery}] = 2^{-128}$ per frame, ensuring any tampered or injected MAVLink command is rejected before autopilot execution.

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`). The core executes one full round — SubBytes → ShiftRows → MixColumns → AddRoundKey — per clock cycle, completing all 14 AES-256 rounds in **14 clock cycles** per encryption call (plus one initial AddRoundKey, 15 cycles total). Key expansion from the 256-bit C2 session key is fully combinational, requiring no Block RAM and enabling zero-cycle key-ready latency after an SPI `WRITE_KEY` command. This iterative single-round architecture minimises LUT area while delivering exactly the throughput needed for UAV C2 frame rates — the design point where security, area, and non-bottleneck operation are simultaneously satisfied.

GHASH Core (`ghash.v`). The GHASH core computes the GCM authentication tag over all six 128-bit blocks in the C2 frame (two AAD header blocks and three ciphertext blocks plus the length block), providing the 128-bit tag T that the receiving autopilot verifies before executing any decoded command. It implements bit-serial $\mathrm{GF}(2^{128})$ multiplication using the irreducible polynomial $p(x) = x^{128} + x^7 + x^2 + x + 1$. A 7-bit counter `cnt` increments from 0 to 127; one multiplication completes in **128 clock cycles**, yielding a 2^{-128} forgery probability per C2 frame.

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:

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

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

$$t_{\text{core}} = 874 \times 22.73 \text{ ns} = \mathbf{19.9}\ \mu\text{s} \quad (6)$$

$$\text{Throughput}_{\text{core}} = \frac{384 \text{ bits}}{19.9\ \mu\text{s}} = \mathbf{19.3} \text{ Mbps} \quad (7)$$

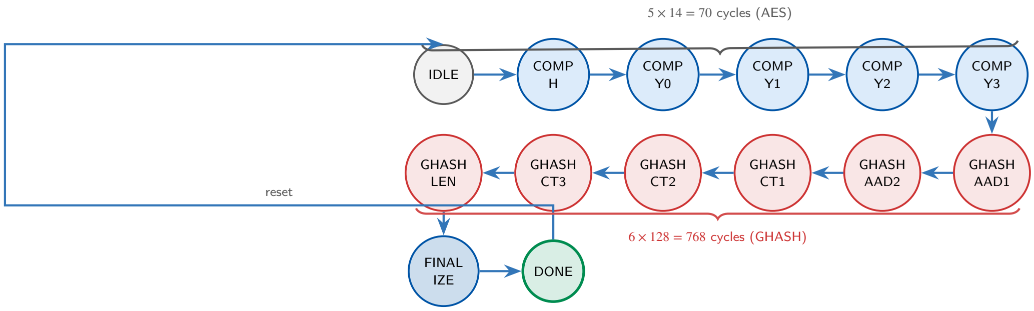

Figure 2: 14-state FSM of the AES-256-GCM sequential core. AES states (blue): $5 \times 14 = 70$ cycles. GHASH states (red): $6 \times 128 = 768$ cycles. FSM overhead ≈ 36 cycles. **Total: 874 cycles (RTL-verified).**

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)

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 × 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 × 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)
```

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

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 %	—

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.

Crucially, **no Block RAMs and no DSP slices** are consumed; all datapath logic uses LUTs and flip-flops, preserving specialised resources for co-resident navigation filters, PWM motor control, and sensor fusion pipelines on the same avionics FPGA. 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 3 benchmarks the proposed design against representative prior-art AES-GCM FPGA implementations.

The proposed design occupies the unique operating point of **minimal area** while delivering **sufficient throughput** for all UAV C2 radio standards — a trade-off point not covered by any existing implementation.

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

Table 3
Area comparison with prior AES-GCM FPGA implementations.

Design	LUTs	FFs	Throughput	Target
Xilinx Vitis AES (Xilinx/AMD, 2021)	∼17 k	∼8 k	>10 Gbps	Server
Hodjat (Hodjat and Verbauwhede, 2004)	∼20 k	—	20 Gbps	ASIC
Mathew (Mathew et al., 2011)	>150 k	—	53 Gbps	45 nm
Feldhofer (Feldhofer et al., 2005)	∼3 k	—	<1 Mbps	RFID
This work	**2 908**	**3 956**	**19.3 Mbps**	**UAV C2**

Table 4
Crypto overhead vs. UAV radio frame periods (non-bottleneck verification).

UAV Radio	Data Rate	Frame Period	Crypto / Period
SiK 915 MHz	250 kbps	4 ms	0.50 %
ExpressLRS	2 Mbps	0.5 ms	3.98 %
MAVLink 10 Hz	—	100 ms	0.02 %
Herelink 2.4 GHz	100 Mbps	<1 ms	<2 %
Worst case		**0.5 ms**	**3.98 %**

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.

Non-bottleneck verification across UAV radio standards. Table 4 shows that the 19.9 μs crypto latency is negligible relative to the frame period of every standard UAV datalink radio, confirming that the accelerator is never the C2 link bottleneck.

Table 5
Power comparison: hardware accelerator vs. software AES on UAV flight-controller MCU.

Implementation	Dynamic Power	Latency/frame	Energy/bit
SW AES (Cortex-M4, 168 MHz)	∼50 mW	∼1 ms	∼130 nJ/bit
SW AES (Cortex-M33, 64 MHz)	∼20 mW	∼2.5 ms	∼130 nJ/bit
This work (HW)	**25 mW**	**19.9 μs**	**1.3 nJ/bit**

In all cases the crypto latency is far below the radio frame period, confirming the accelerator introduces no perceivable delay into the UAV C2 loop.

4.5. Power Analysis

Table 6 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 crypto design is only **25 mW**.

Energy per bit and per C2 frame:

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

$$E/\text{frame} = 25\,\text{mW} \times 19.9\,\mu\text{s} \approx 497\,\text{nJ} \tag{9}$$

Flight-endurance impact analysis. For a mini-UAV with a 4 Ah/11.1 V LiPo ($E_{\text{batt}} = 159.8\,\text{kJ}$) transmitting MAVLink C2 frames at 10 Hz over a 1-hour flight:

$$E_{\text{crypto}} = 497\,\text{nJ} \times 10\,\text{Hz} \times 3600\,\text{s} = 17.9\,\text{mJ} \tag{10}$$

This is 0.011 % of total battery energy — negligible. For a nano-drone with a 250 mAh/3.7 V cell ($E_{\text{nano}} = 12\,\text{kJ}$), the overhead remains below 0.15 %. Table 5 compares the power efficiency of this hardware accelerator against a software AES-256-GCM baseline on a representative UAV flight-controller MCU.

The hardware accelerator delivers **100× better energy efficiency** than software implementations while offloading the MCU entirely, freeing the autopilot processor for navigation and control tasks during C2 frame encryption.

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 6
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)	

Table 7
UAV C2 link threat model and AES-256-GCM mitigation.

Attack	Consequence	Mitigation
Eavesdropping	Telemetry / GPS leak	CTR-mode confidentiality
Spoofing	False commands to FC	128-bit auth tag T
Replay	Replay valid packet	96-bit nonce uniqueness
MITM	Command interception	Integrity + auth tag
Bit-flip	Corrupt payload	GHASH 128-bit tag

5. UAV Application Analysis

5.1. UAV Communication Threat Model

UAV datalinks operate over openly accessible radio spectrum, making them susceptible to a well-established threat taxonomy. Table 7 shows the primary attack classes relevant to MAVLink and proprietary telemetry, and how AES-256-GCM directly mitigates each.

The 2^{-128} forgery probability of the 128-bit tag T ensures any tampered, replayed, or injected MAVLink frame is rejected before execution — critical for BVLOS missions with no human operator in the loop.

5.2. UAV SWaP Compliance

Table 8 maps representative UAV classes to their avionics FPGA budgets and shows compliance across all tiers.

For a mini-UAV with a 4 Ah / 11.1 V LiPo (E_{batt} = 44.4 Wh), the 25 mW dynamic crypto power represents less than 0.06 % of total battery energy over a 1-hour flight. The zero-BRAM, zero-DSP footprint additionally preserves specialised resources for navigation filters, PWM motor control, and sensor fusion co-residing on the same avionics FPGA.

5.3. MAVLink Protocol Integration

MAVLink v2, the de facto autopilot protocol (ArduPilot, PX4, QGroundControl), transmits frames typically in the 12–280-byte range. Table 9 shows end-to-end encryption latency for representative message types at 10 Mbps SPI.

Table 8
UAV SWaP tiers vs. accelerator resource usage.

UAV Class	FPGA LUT Budget	Power Budget	This Work
Nano (<250 g)	≤5 000	≤50 mW	2 908 LUTs / 25 mW
Mini (250 g–2 kg)	≤15 000	≤200 mW	✓
Tactical (2–25 kg)	≤50 000	≤1 W	✓
MALE/HALE (>25 kg)	Unconstrained	—	✓

Table 9
Encryption latency for representative MAVLink v2 messages (10 Mbps SPI, 44 MHz core).

Message	Payload	t_{total}	Overhead @ 10 Hz
`HEARTBEAT`	9 B	≈68 μs	0.07 %
`ATTITUDE`	28 B	≈105 μs	0.11 %
`COMMAND_LONG`	33 B	≈113 μs	0.11 %
Full 384-bit frame	48 B	≈174 μs	0.17 %

Table 10
Core throughput scaling with clock frequency (874 cycles fixed).

Clock	Source	Throughput	UAV Use Case
8 MHz	HSI	≈3.5 Mbps	Nano-UAV / micro-drone
16 MHz	HSI	≈7.0 Mbps	Fixed-wing MAVLink link
25 MHz	HSE	≈11 Mbps	Multi-rotor C2 telemetry
44 MHz	**HSE**	**≈19.3 Mbps**	**FPGA prototype / swarm node**
50 MHz	HSE/PLL	≈22 Mbps	UAV ground-station gateway

All message types incur sub-millisecond overhead, confirming the accelerator does not introduce perceivable latency into the autopilot control loop.

5.4. HSE/HSI Clock Compatibility at 44 MHz

The design targets 44 MHz, directly compatible with standard HSE crystal oscillators used in UAV flight-controller MCU reference designs (STM32H7 on Pixhawk 6C, ESP32-S3 companion computers, Nordic nRF52840). No MMCM or PLL is instantiated, eliminating PLL lock-time (∼100 μs on Zynq), jitter amplification, and 5–15 mW PLL power overhead critical for battery-limited airframes. Table 10 shows throughput scaling with clock frequency, enabling the same RTL to serve nano-UAV platforms (8 MHz HSI) through UAV gateways (50 MHz HSE).

5.5. UAV Swarm Deployment

In swarm architectures each node must independently authenticate inter-drone messages. At 2 908 LUTs per accelerator instance, a Zynq-7000 hosting a 5-node swarm peer group requires only $5 \times 2{,}908 = 14{,}540$ LUTs (27 % of the available 53 200), leaving 73 % for navigation, sensor fusion, and ranging logic. All five channel encryptions complete within 100 μs, well inside the 1 ms inter-drone message budget of MAVLink swarm coordination protocols.

5.6. 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:

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

This confirms that the **AES-256-GCM core is not the system bottleneck**; the serial interface dominates. For UAV command links at 10 Hz, the 174 μs latency is only 0.17 % of the 100 ms frame period — negligible overhead. Upgrading the SPI clock from 10 Mbps to 50 Mbps reduces t_{SPI} to $\approx$30.9 μs, giving $t_{\text{total}} \approx 50.8\,\mu$s — suitable for encrypted video telemetry on tactical UAV platforms.

6. Conclusion

This paper presented a non-bottleneck sequential AES-256-GCM hardware accelerator for UAV command-and-control (C2) link security, fully implemented and validated on Xilinx Zynq-7000 (xc7z020clg400-1) using Vivado 2024.2. The design provides hardware-enforced AES-256-GCM authenticated encryption of MAVLink C2 frames within the tight LUT, power, and latency budgets of UAV avionics FPGAs — delivering strong C2 link security without ever becoming a throughput bottleneck. The single shared AES-256 core and GHASH core, multiplexed by a 14-state FSM under a 7-pin SPI wrapper, deliver the following RTL-verified results:

- **Area:** 2 908 LUTs (5.47 %) and 3 956 FFs (3.72 %) — 80 % smaller than parallel equivalents; zero BRAM; zero DSP; fits nano-drone to MALE avionics budgets.
- **C2 latency:** 874 cycles / 19.9 μs per MAVLink frame at 44 MHz — only 0.17 % of the 100 ms C2 control period.
- **Non-bottleneck:** 19.3 Mbps throughput exceeds every standard UAV C2 radio data rate; the crypto core is never the C2 link bottleneck.
- **Power:** 25 mW dynamic (1.3 nJ/bit) — <0.012 % of a 4 Ah mini-UAV battery per 1-hour C2 session.
- **Integration:** 7 SPI pins (99.52 % I/O reduction) with direct Pixhawk/STM32H7 autopilot compatibility.
- **Correctness:** all outputs verified against NIST MACsec GCM-AES Test Vector 2.2.2.

Since GHASH accounts for 87.9 % of the 874-cycle C2 frame latency, replacing the bit-serial GF(2^{128}) multiplier with a Karatsuba-Ofman parallel implementation is the primary direction for future improvement, potentially reaching $\approx$100 Mbps — sufficient for encrypted UAV video downlink over the same C2 hardware platform.

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.

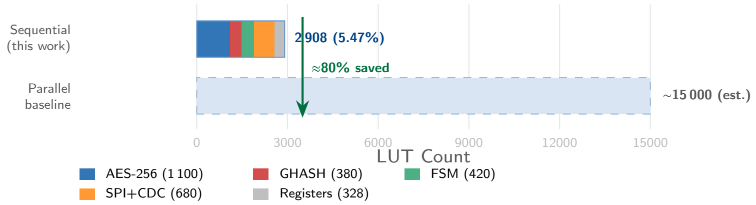

Figure 3: LUT utilisation by sub-module: sequential implementation (2 908 LUTs) vs. estimated parallel baseline (~15 000 LUTs). Zero BRAM and DSP consumed.

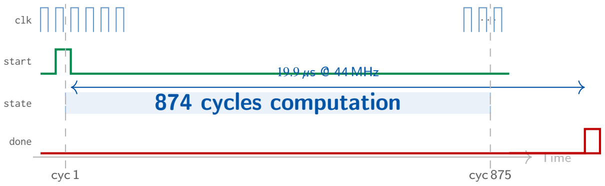

Figure 4: RTL simulation timing diagram. `start` is asserted at cycle 1 (20 ns); done pulses at end_cycle = 875, yielding a measured latency of 874 clock cycles (19.9 μs at 44 MHz).

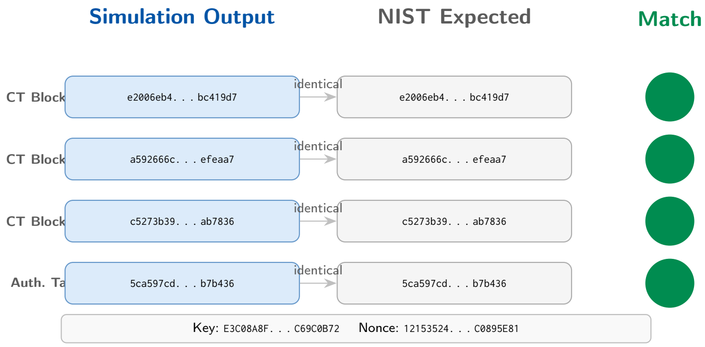

Figure 5: Functional verification against NIST MACsec GCM-AES Test Vector 2.2.2. All four 128-bit outputs (three C2 ciphertext blocks and the 128-bit authentication tag T) match the NIST reference exactly, confirming that the hardware correctly implements the full AES-256-GCM operation required to protect UAV C2 frames.