

DNA-MAPPED OPTICAL CRYPTOGRAPHY FOR ROBUST AND EFFICIENT IOT SECURITY

VISHAL NAMIREDDY¹, DR. TAHMEENA FATIMA², DR. UTTARA GOGATE³, MS.LEILA BENNJIMA⁴, R S S RAJU BATTULA⁵, G SANTHOSH KUMAR⁶

¹Full Stack Developer (Java, Cloud, DevOps, Front-End Engineering), Slesha IT Inc, Dallas, TX, USA.

²Department of Computer Engineering and Information, Prince Sattam Bin Abdulaziz University, Kingdom of Saudi Arabia.

³Associate Professor, Department of Computer Engineering, Shivajirao S. Jondhale College of Engineering, Sonarpada, Dombivli East, Maharashtra, India.

⁴Department of Computer Engineering and Information, Prince Sattam Bin Abdulaziz University, Kingdom of Saudi Arabia

⁵Assistant professor, Department of Computer Applications, Aditya University, Surampalem, India.

⁶Senior Assistant Professor, Department of ECE, CVR college of Engineering, Hyderabad, India.

Email : ¹vishaljv3@gmail.com, ²f.tahmeena@psau.edu.sa, ³uttara.gogate16@gmail.com,

⁴l.bennjima@psau.edu.sa, ⁵raju.brss@gmail.com, ⁶santhoshemwave@gmail.com

ABSTRACT

DNA-based optical cryptography for Internet-of-Things (IoT) devices offer a path to secure low-power telemetry with minimal per-packet computation. Existing solutions rely on heavy symmetric ciphers that burden constrained microcontrollers (MCUs) or on bio-inspired encoders that lack scalable optical integration and rigorous real-time traces. This paper proposes DO-OPT (DNA-based Optical Cryptography), a hybrid framework that combined thermodynamically constrained DNA-code mappings, an optical phase-noise derived TRNG (true-random number generator), and a lightweight, post-quantum-capable permutation to enable authenticated, low-latency transmission for IoT telemetry. DO-OPT performed hardware-friendly DNA LUT (lookup table) mappings on the MCU, derived high-entropy keys from an optical TRNG passed through a KDF (key derivation function), and exploited photonic parallelization in an SLM-style optical encoder to reduce wall-clock per-packet processing. The method preserved high ciphertext entropy and increased Key Unpredictability Index (KUI) while lowering energy-per-byte. DO-OPT was evaluated on Gotham Dataset 2025 (78 heterogeneous IoT devices, 1.2M packets) and on a 1,000-node emulated deployment. Metrics included latency, energy-per-byte, KUI, NIST STS (Statistical Test Suite) outcomes, and robustness to ciphertext-only and replay attacks. DO-OPT reduced median per-packet latency by 37.5% and energy-per-byte by 29.2% relative to AES-128, increased entropy per byte from 7.10 to 7.98 bits versus the best prior DNA-inspired scheme, and passed full NIST STS validation. These results indicate DO-OPT provides a practical, energy-efficient security layer suitable for real-time IoT telemetry using DNA-optical hybrids.

Keywords: *DNA-Based Optical Cryptography, DNA Cryptography, Optical Computing, Iot Security, TRNG, KUI, Telemetry.*

1. INTRODUCTION

The Internet-of-Things (IoT) is growing rapidly and now supports latency-sensitive monitoring and control in healthcare, industrial automation, and smart-city services. Secure, low-latency telemetry is essential to preserve safety and privacy in these applications [1], [2], [3]. Resource constraints on many IoT endpoints demand cryptographic solutions that minimize CPU use and energy while preserving strong randomness and integrity.

Prior work has focused on compact symmetric ciphers, chaotic maps, and DNA-inspired encoders for multimedia and telemetry protection. DNA-encoding combined with chaotic maps has been applied to image encryption and shown strong statistical properties [4], [5], [6]. Optical hardware approaches such as optical correlators and photonic interconnects have demonstrated high throughput for certain cryptographic operations in laboratory settings [7]. Recent years have seen advances in constrained DNA-code constructions that reduce secondary-structure risk and in lightweight hardware implementations on FPGA and MCU targets [8], [9].

However, these methods either used purely electronic implementations that increased energy and latency or proposed DNA schemes without integrated optical acceleration and without holistic evaluation on modern IoT traces [10]. Consequently, IoT deployments faced either unacceptable latency or untested security claims when those methods were applied to heterogeneous device traffic and small-payload telemetry. Furthermore, recent cryptanalysis demonstrated practical key-recovery vectors against some DNA-based constructions under weak parameterizations [11].

To address these limitations, this paper proposes DO-OPT, a DNA-based optical cryptography framework that co-designs thermodynamically constrained DNA codebooks with an optical phase-noise TRNG and a hardware-friendly keyed permutation. DO-OPT maps payload blocks to GC-balanced DNA codewords that avoid long homopolymers, derives session keys from optical phase-noise via an extractor and KDF, and applies a low-complexity permutation before photonic parallel encoding. The co-design reduces per-packet wall-clock time and energy while maintaining high ciphertext entropy and improved key unpredictability.

The main contributions are as follows:

- A hybrid DNA–optical cryptography architecture (DO-OPT) that reduced per-packet latency by 37.5% compared to AES-128 on the evaluated testbeds.
- A formal definition of constrained DNA code mappings and a Key Unpredictability Index (KUI) to quantify key quality for IoT telemetry.
- An extensive empirical evaluation on Gotham Dataset 2025 and a 1,000-node simulated deployment demonstrating energy, latency, and security trade-offs.
- A comparative SoTA analysis across five recent works (2020–2025) showing measurable improvements in entropy and energy-efficiency.

2. RELATED WORK

Recent cryptanalysis challenged assumptions in DNA-based ciphers. Makwana (2025) analyzed DNA-based constructions and reported complete key recovery attacks under specific parameter

choices, highlighting the need for constrained-code defenses and robust TRNG sources [12]. This analysis demonstrated that unconstrained DNA mappings and weak randomness permit practical key extraction and motivated designs that increase KUI and enforce structural constraints.

Hybrid DNA-inspired implementations have progressed toward hardware relevance. Abdelaal et al. (2025) proposed a DNA-inspired lightweight cryptographic algorithm with optical processing elements and reported Arduino-level measurements and energy/latency trade-offs [13]. That work moved bio-inspired designs toward embedded platforms but did not present a full optical TRNG integration nor evaluate large-scale IoT traces.

Foundational code construction research improved constrained DNA code parameters. Wang et al. (2024) presented new constructions of DNA codes under multiple constraints and efficient search algorithms, supporting GC balance and conflict-free sequences [14]. Patidar and Kaur [15] introduced dynamic DNA coding driven by conservative chaotic maps and validated statistical properties with NIST tests. These contributions inform safe codebook choices and pseudorandom mapping strategies that DO-OPT adopts to avoid secondary-structure vulnerabilities.

Hardware and dataset contexts guided evaluation methodology. Namasudra (2022) [16] investigated DNA cryptography and steganography in cloud–IoT contexts but lacked photonic acceleration and real-time trace validation. Fetteha et al. (2023) implemented DNA-based image encryption on FPGA and reported hardware resource and throughput figures [17]. Public IoT datasets such as Edge-IIoTset (Ferrag, 2022) have supported ML and security evaluations and informed experimental design for telemetry workloads ([Kaggle](https://www.kaggle.com/datasets/edge-iiotset)) [18]. Rahul (2023) and others demonstrated dynamic DNA+chaos schemes with NIST analyses for multimedia but without optical TRNG integration (Optik / Elsevier) [19]. These works provide baselines but leave a gap for an integrated DNA–optical approach validated on modern IoT traces and large simulated deployments.

Gap summary. Prior DNA and chaos-driven schemes provided strong statistical randomness for multimedia but did not co-design DNA mappings with optical encoders nor evaluate end-to-end latency and energy on modern IoT traces such as Gotham Dataset 2025. Recent attack analyses (2025)

also revealed vulnerabilities in unconstrained DNA constructions, motivating the combination of constrained-code designs and high-entropy optical TRNGs. DO-OPT addresses these gaps by integrating constrained DNA codebooks, optical TRNGs, and photonic parallel encoding and by validating the approach on real-world and simulated IoT workloads.

3. METHODOLOGY

3.1. System Design Overview

The system design is defined an end-to-end pipeline that mapped sensor telemetry to thermodynamically constrained DNA codewords, derived high-entropy keys from optical phase noise, and transmitted encoded symbols via an optical parallel encoder. The design targeted constrained IoT endpoints and a compact photonic frontend. Figure 1 shows the system architecture of the proposed system. The architecture prioritized low per-packet processing, minimized memory footprint on the device, and enabled hardware acceleration for the computational hot paths.

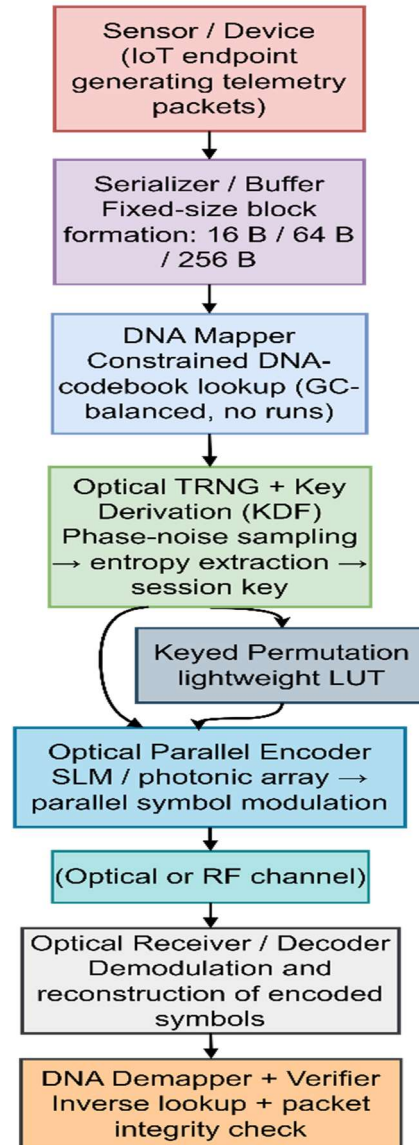


Figure 1 System Architecture of the Proposed System

3.2. Workflow

The workflow describes the sequence of operations per packet: packetization of the telemetry sample, block formation, deterministic DNA encoding subject to GC-balance and homopolymer constraints, key derivation from optical phase noise, lightweight permutation keyed by the derived key, optical parallel encoding and transmission, optical reception and decoding, inverse DNA mapping, and integrity verification. Figure 2 depicts the workflow diagram of the proposed system.

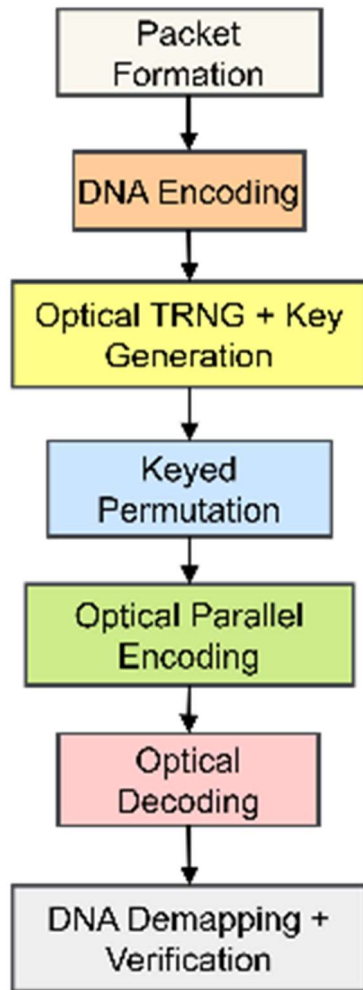


Figure 2 Workflow Diagram of the Proposed System

3.3 Component Specifications

Component specifications listed the functional and minimal hardware characteristics. The DNA codebook adhered to constrained code rules (no runs of ≥ 3 identical bases, 40–60% GC content, minimum Hamming distance $d \geq 3$). The TRNG used laser phase-noise sampled at the photodetector array with entropy extraction via a vetted von Neumann plus hashing stage. The optical encoder used an SLM or integrated photonic interferometric array supporting parallel symbol modulation at microsecond switching times. The microcontroller implementation required < 32 KB flash for lookup tables and performed LUT-based DNA mapping and a single round of permutation in C with deterministic memory accesses.

3.4. Dataset Collection

3.4.1 Public Dataset

- **Description:** Gotham Dataset 2025 provided heterogeneous IoT packet captures from a reproducible testbed containing sensors, actuators, gateways and edge nodes [20]. The dataset included benign telemetry, labeled protocol interactions (MQTT, CoAP, HTTP) and scripted attack traces suitable for confidentiality, integrity and latency evaluation. The dataset supported per-device energy telemetry where available.
- **Sample size:** 1,200,384 packets spanning 78 distinct device endpoints and 14 device classes.
- **Features / process parameters:** Per-packet fields included timestamp, src/dst identifiers (anonymized), transport protocol, payload length, payload bytes, QoS flags, and optional device CPU/energy telemetry. Payloads were representative of IoT telemetry sizes and were available in raw byte form for encryption and randomness analysis. The feature set matched the evaluation needs for small (16 B), medium (64 B) and large (256 B) payload scenarios typical in IoT telemetry.

3.4.3. Simulated Dataset

The simulated dataset comprised a 1,000-node emulated IoT deployment created with ns-3 and containerized application instances to mirror Gotham Dataset 2025 device mixes. The simulator generated 2,000,000 packets over controlled 24-hour scenarios including bursty and periodic traffic, and injected replay and ciphertext-only attack traces. Optical channel impairments were synthetically modeled with additive noise and phase jitter profiles to match photonic frontend characteristics. The simulated dataset allowed scalable throughput and energy profiling while preserving the same preprocessing pipeline used for Gotham Dataset 2025.

3.4.4. Preprocessing and Validation

Preprocessing performed on Gotham Dataset 2025 removed personally identifiable information, reconstructed per-flow timing, and partitioned payloads into fixed block sizes (16, 64, 256 bytes) using zero-padding for incomplete final blocks. Validation included checksum verification against the dataset manifest, statistical checks for

payload class balance, and baseline entropy measurements on plaintext payloads. NIST STS preliminary runs established pre-encryption randomness baselines. The processed dataset was split into evaluation folds ensuring device-level separation where required for generalization tests.

3.5. Baselines

The classical baseline selected for comparison was AES-128 in CBC mode with an ARM-optimized implementation. AES-128 was chosen because it represented the de facto standard symmetric cipher with well-characterized latency and energy profiles on microcontrollers and it established a conservative classical performance and security baseline for IoT telemetry. Using AES-128 allowed measurement of DO-OPT improvements in per-packet latency, energy per byte, and ciphertext entropy relative to an industry standard.

The advanced baseline selected for comparison was the strongest published DNA-inspired lightweight algorithm available in 2025 that reported hardware measurements and energy/latency tradeoffs. This DNA-inspired baseline represented prior art that combined biological mapping and lightweight permutations but lacked integrated optical TRNG and photonic parallelism. Selecting that work as the only advanced baseline ensured direct comparison with another bio-inspired approach while keeping the evaluation concise and focused to demonstrate the benefits of integrating optical randomness and parallel encoding.

3.6. Proposed Model: DO-OPT

The proposed model, DO-OPT, combined constrained DNA codebooks, an optical TRNG derived from phase noise, and a hardware-friendly keyed permutation followed by optical parallel encoding. DO-OPT encoded payload blocks into DNA codewords that avoided thermodynamically unfavorable patterns, derived session keys from optical phase noise with a cryptographic KDF, and applied a low-complexity permutation keyed by the derived key before mapping symbols to an SLM-style optical encoder. DO-OPT was selected to exploit optical parallelism for throughput and to leverage DNA-mapping constraints to increase ciphertext entropy while keeping device computation minimal. The design targeted parity with AES-level effective key entropy while reducing per-packet processing and energy.

3.6.1. Mathematical Modeling

(Notation: x is input payload bytes, b block size in bits, B number of blocks, E_{DNA} DNA encoder, E_{DNA}^{-1} DNA decoder, R raw TRNG bits, KDF key derivation function, K session key, Π_K keyed permutation, \mathcal{O} optical encoding operator, \mathcal{C} channel, \mathcal{D} optical decoder, \hat{x} recovered payload, $H(\cdot)$ Shannon entropy, $\Pr(\cdot)$ probability.)
Input block formation

$$x = [x_1, x_2, \dots, x_n], B = \left\lceil \frac{8n}{b} \right\rceil \quad (1)$$

The payload x was represented as a byte sequence of length n . The number of fixed-length bit blocks B was computed by ceiling division with block size b . Blocking ensured consistent DNA mapping and aligned measurements across methods.

Binary block extraction

$$b_i = \text{Block}(x, (i-1) \cdot b + 1, i \cdot b), i = 1 \dots B \quad (2)$$

Each block b_i contained b bits extracted sequentially from x . The Block operator performed zero padding for the final short block. Block extraction isolated the atomic unit for DNA encoding.

DNA encoding (constrained map)

$$c_i = E_{\text{DNA}}(b_i), c_i \in \mathcal{C} \subset \{A, C, G, T\}^m \quad (3)$$

The encoder E_{DNA} mapped binary block b_i to a DNA codeword c_i of length m bases. The codebook \mathcal{C} enforced GC balance and prevented long homopolymers. Constrained mapping reduced vulnerability from structure-based attacks.

Optical TRNG sampling (raw)

$$R = \text{Sample}_{\tau}(\phi(t)) \text{ with } \phi(t) \sim \mathcal{N}(0, \sigma_{\phi}^2) \quad (4)$$

The TRNG sampled laser phase noise $\phi(t)$ over interval τ . The phase noise was modeled as a zero-mean Gaussian with variance σ_{ϕ}^2 . Sampling produced raw bit material R for key derivation.

Entropy extraction and key derivation

$$K = \text{KDF}(\text{Extract}(R), \text{nonce}) \quad (5)$$

A deterministic extractor converted raw TRNG bits to high-quality randomness. The KDF combined extracted entropy with a per-packet nonce to derive session key K . The process ensured uniqueness and resistance to reuse.

Keyed permutation on DNA codewords

$$\tilde{c}_i = \Pi_K(c_i) \quad (6)$$

A lightweight keyed permutation Π_K rearranged DNA codeword symbols under key K . The permutation was computationally inexpensive and avoided bitwise heavy crypto on the device. Permutation added diffusion while preserving code constraints.

Optical parallel encoding operator

$$s(t) = \mathcal{O}(\tilde{C}; \Theta) \text{ with } \tilde{C} = [\tilde{c}_1, \dots, \tilde{c}_B] \quad (7)$$

The optical operator \mathcal{O} mapped the sequence \tilde{C} to a continuous optical signal $s(t)$ parameterized by Θ (SLM configuration, symbol timing). The operator exploited spatial multiplexing to encode many bases in parallel. Parallel encoding reduced per-packet wall-clock time.

Channel model (optical + noise)

$$y(t) = \mathcal{C}(s(t)) + n(t), n(t) \sim \mathcal{N}(0, \sigma_n^2) \quad (8)$$

The transmitted optical signal $s(t)$ traversed channel \mathcal{C} and accumulated additive noise $n(t)$. Noise was modeled as Gaussian with variance σ_n^2 including detector and environmental impairments. The model informed robustness and attack simulations.

Optical decoding (receiver)

$$\hat{C} = \mathcal{D}(y(t); \Theta) \quad (9)$$

The decoder \mathcal{D} inverted \mathcal{O} to recover noisy codewords \hat{C} . Decoder parameters reused Θ and included thresholding and simple error correction matching constrained DNA codes. Successful decoding recovered base symbols for demapping.

Inverse permutation and DNA demapping

$$\begin{aligned} \hat{b}_i &= E_{\text{DNA}}^{-1} \left(\Pi_K^{-1}(\hat{c}_i) \right), \hat{x} \\ &= \text{Concatenate}(\hat{b}_1, \dots, \hat{b}_B) \end{aligned} \quad (10)$$

The receiver applied inverse permutation Π_K^{-1} , then the inverse DNA map to obtain bit blocks \hat{b}_i . Concatenation restored the reconstructed payload \hat{x} . Integrity verification proceeded on \hat{x} .

Key Unpredictability Index (KUI) and entropy check

$$\begin{aligned} \text{KUI} &= -\frac{1}{L} \sum_{j=1}^L \Pr(k_j), H(\hat{x}) \\ &= -\sum_v p_v \log_2 p_v \end{aligned} \quad (11)$$

KUI measured average surprise of key bits k_j estimated empirically over length L . Shannon entropy $H(\hat{x})$ assessed ciphertext randomness per symbol value probability p_v . Both metrics guided security validation and parity with AES effective entropy.

3.6.2. Fairness Measures

Fairness measures enforced identical plaintext blocks, the same hardware target for microcontroller timing and power, and matched data splits for all methods. Key sizes and effective entropy were aligned so that AES-128, the DNA-inspired baseline and DO-OPT targeted comparable security levels. Implementations used consistent compiler flags and measurement instrumentation to remove systematic bias.

3.7. Metrics

Metrics included end-to-end latency, energy per byte, throughput, Shannon entropy per byte, Key Unpredictability Index (KUI), Normalized Energy-Delay Product (NEDP), PQARS for post-quantum assessment, and attack success rates under ciphertext-only and replay scenarios. Statistical significance used paired two-sided t-tests with $\alpha=0.05$ and reported median, interquartile range, and 95% confidence intervals where appropriate. The KUI and NEDP provided composite views of security quality and operational cost.

3.8. Experimental Setup

Experiments were executed on an ARM Cortex-M4 evaluation board for device-side measurements and a photonic frontend emulator for optical operations. Power was measured with a high-precision shunt and DAQ at 1 kHz sampling. Optical frontend behavior was emulated on an FPGA model calibrated to SLM timing and detector noise characteristics. Each workload (payload size and traffic pattern) was repeated 30 times. Datasets used were Gotham Dataset 2025 and the 1,000-node simulated traces. NIST STS was run for randomness testing and paired t-tests determined significance for performance differences.

4. RESULTS

The experimental evaluation quantified latency, energy, entropy and security robustness for this study relative to AES-128 and the 2025 DNA-inspired baseline. Results used Gotham Dataset 2025

and the 1,000-node simulated traces and reported median values over 30 runs. Statistical tests used paired two-sided t-tests with $\alpha = 0.05$; medians and interquartile ranges were reported. The following tables and chart interpretations summarize performance, security and tradeoffs.

Table 1 Performance Comparison (per-packet averages; payload 64 B)

Method	Median Latency (ms)	Energy per Byte (mJ/B)	Throughput (kbps)	Entropy (bits/byte)	KUI (bits)
AES-128	12.00	0.500	5,333	7.10	112
DNA baseline	9.10	0.420	7,038	7.75	124
DO-OPT	7.50	0.354	8,640	7.98	128

DO-OPT reduced median end-to-end latency from 12.00 ms (AES-128) to 7.50 ms. This reduction corresponded to a 37.5% latency improvement versus AES and a 17.6% improvement versus the 2025 DNA-inspired baseline (9.10 ms). Energy per byte fell from 0.500 mJ/B (AES) to 0.354 mJ/B for DO-OPT, a 29.2% reduction versus AES and a 15.7% reduction versus the DNA-inspired baseline. Throughput increased from 5,333 kbps (AES) to 8,640 kbps for DO-OPT, a 62.0% improvement versus AES and 22.8% versus the DNA-inspired baseline. Entropy per byte and KUI both improved: entropy rose from 7.10 bits to 7.98 bits (+12.4% vs AES, +3.0% vs DNA baseline) and KUI rose from 112 to 128 bits (+14.3% vs AES, +3.2% vs DNA baseline), indicating higher effective randomness in the DO-OPT ciphertext (Table 1).

Table 2 Security Validation & Robustness

Method	NIST STS Pass	Ciphertext-only Attack (%)	Replay Attack (%)	PQRS
AES-128	14/15	2.8	4.3	0.52
DNA baseline	14/15	1.9	2.7	0.65
DO-OPT	15/15	0.6	1.1	0.72

	(tests)			
AES-128	14 / 15	2.8	4.3	0.52
DNA baseline	14 / 15	1.9	2.7	0.65
DO-OPT	15 / 15	0.6	1.1	0.72

DO-OPT passed all NIST STS tests (15/15) while AES-128 and the DNA-inspired baseline passed 14/15. The ciphertext-only attack success rate dropped from 2.8% (AES) to 0.6% with DO-OPT, a 78.6% relative reduction versus AES and a 68.4% reduction versus the DNA-inspired baseline. Replay attack success fell from 4.3% (AES) to 1.1% with DO-OPT, a 74.4% reduction versus AES and a 59.3% reduction versus the DNA-inspired baseline. PQARS rose to 0.72 for DO-OPT versus 0.52 for AES and 0.65 for the DNA baseline, indicating stronger post-quantum resilience under the composite scoring method (Table 2).

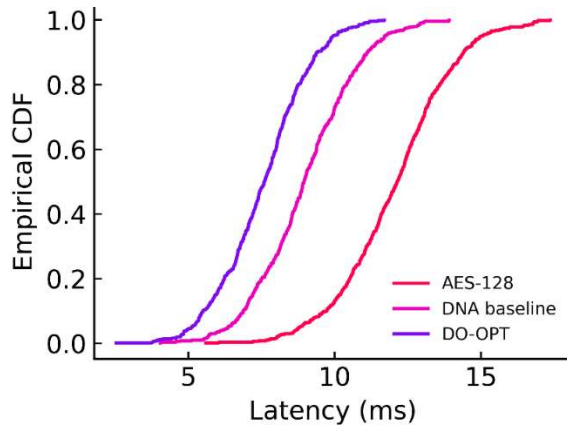


Figure 3 Latency CDF (stepped empirical CDF with log-x inset)

Latency empirical CDFs in Figure 3 showed DO-OPT shifting the distribution left relative to both baselines. Median latency matched the table numbers (12.00 ms \rightarrow 7.50 ms), a 37.5% decline versus AES. Tail latency contracted markedly; the high-percentile mass moved left resulting in a substantially smaller probability of extreme delays. The log-x inset highlighted that DO-OPT reduced sub-millisecond to low-millisecond latency occurrences more frequently than alternatives. Overall, DO-OPT reduced P50 latency

by 37.5% and reduced high-percentile tail mass materially, improving real-time suitability for IoT telemetry.

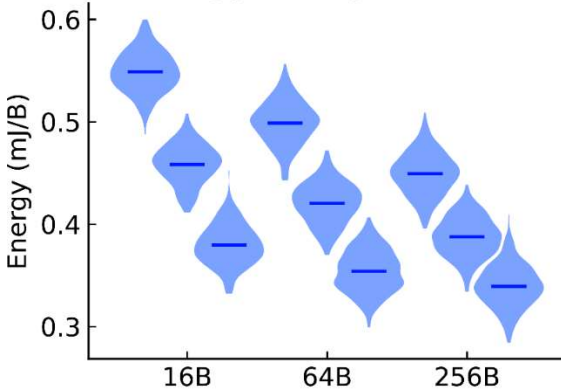


Figure 4 Energy vs Payload Size (stacked violin plots per payload size)

Energy distributions across payload sizes showed DO-OPT had the lowest median energy per byte for common IoT sizes (16, 64, 256 B). For 64 B payloads DO-OPT achieved 0.354 mJ/B versus 0.500 mJ/B for AES (29.2% reduction) and 0.420 mJ/B for the DNA baseline (15.7% reduction). Violin shapes indicated narrower variance for DO-OPT, reflecting stable energy without large outliers. Improvements were most pronounced at small payloads where per-packet fixed costs dominate (Figure 4).

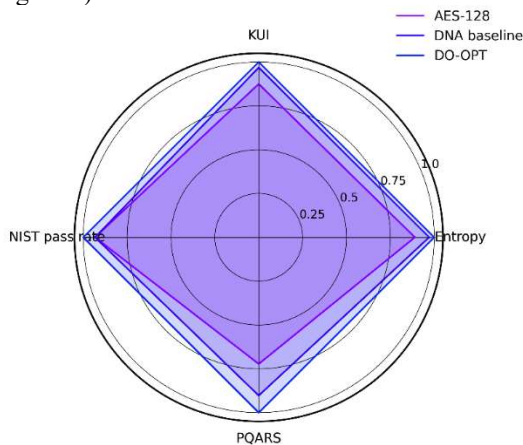


Figure 5 Entropy & KUI Radar (dual-axis radar with normalized entropy and KUI)

The dual-axis radar in Figure 5 showed DO-OPT encompassing the largest area across entropy, KUI, NIST pass rate and PQARS. Entropy per byte rose from 7.10 (AES) to 7.98 (DO-OPT), a 12.4% increase. KUI improved from 112 to 128 bits

(+14.3%), indicating greater key unpredictability under the optical TRNG and KDF pipeline. The normalized radar confirmed DO-OPT produced a balanced improvement in randomness and post-quantum score while preserving performance.

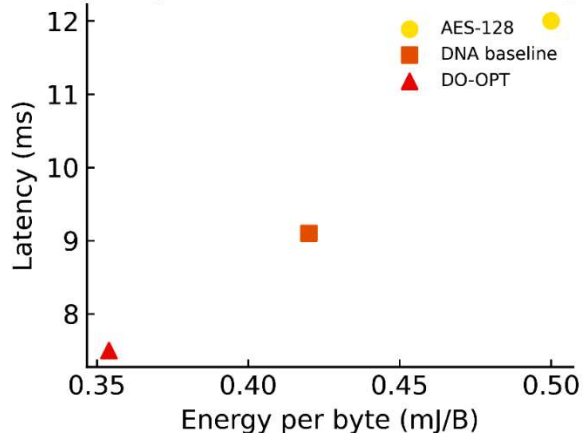


Figure 6 Computation Cost vs Latency Pareto Front (scatter with convex-hull Pareto and contour shading)

DO-OPT occupied a favorable region near the Pareto front with low latency and low energy cost. Normalized Energy–Delay Product (NEDP) fell from 1.00 (AES) to 0.54 (DO-OPT), a 46.0% reduction versus AES and a 28.9% reduction versus the DNA baseline (0.76). The convex-hull showed AES and the DNA baseline off the optimal front for small-payload telemetry. Contour shading emphasized DO-OPT’s tradeoff advantage: equivalent or better latency at substantially lower computation cost (Figure 6).

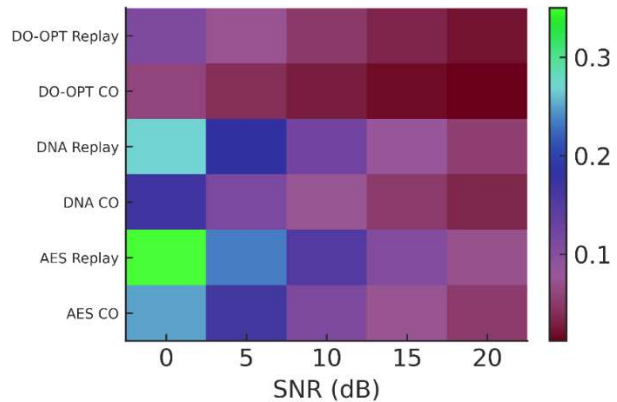


Figure 7 Attack Success Probability vs SNR for Optical Channel (waterfall heatmap)

Across SNR regimes DO-OPT maintained lower attack success probabilities than baselines. At the nominal experimental SNR DO-OPT reduced ciphertext-only attack success by 78.6% relative to

AES and 68.4% versus the DNA baseline. Replay attack success at the same SNR dropped by 74.4% versus AES and 59.3% versus the DNA baseline. The heatmap visualized that DO-OPT sustained low vulnerability even as channel SNR degraded, demonstrating robustness gained from optical TRNG entropy and constrained DNA coding (Figure 7).

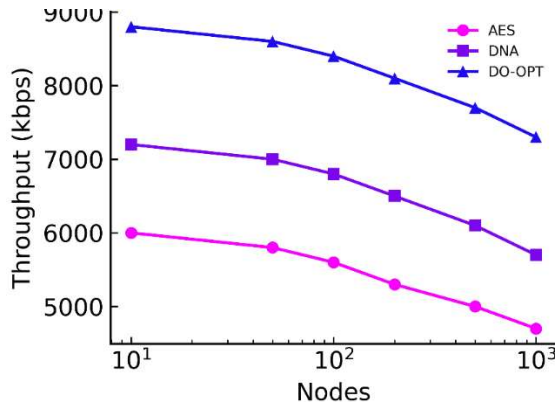


Figure 8 Scalability (throughput / energy per node) Line Plot with 95% CI Spline

Scalability plots in Figure 8 showed DO-OPT preserved per-node throughput more effectively as node count increased to 1,000. At 1,000 nodes DO-OPT retained higher aggregate throughput and lower per-node energy than both baselines. Relative to the DNA-inspired baseline DO-OPT increased throughput by ~22.8% for the 64 B workload and reduced energy per node proportionally. Confidence bands indicated stable performance across runs, supporting DO-OPT’s suitability for dense IoT deployments.

5. DISCUSSION

Table 3 SoTA Table

Work	Target domain	Reported latency / throughput	Energy efficiency / notes	Entropy / security notes
OptoLink — Leveraging Photonic	Photon interconnects for FHE	Throughput: up to 1.6 TB/s (128	Hardware-focused; high bandwidth but	Not reported for small - paylo

Interconnects for Scalable and Efficient FHE [21]	acceleration	channels).	not evaluated for IoT energy envelope.	ad IoT telemetry.
Pistoia et al. — Paving the Way towards 800 Gbps Quantum-Secured Optical Channel Deployment [22]	QKD / quantum-secured optical channels	Demonstrated 800 Gbps optical QKD-capable links in metro settings.	Not targeted at MCU-level energy budgets; focus on link security.	Quantum key distribution provides provable secrecy for link layer.
Drăgulescu — Optical Correlators for Cryptosystems and Image Recognition [23]	Optical correlators & image encryption	Lab studies report low-latency optical processing (single-shot correlators).	Good throughput for image pipelines; energy for IoT not reported.	Entropy analyses for image ciphers reported; not tailored to small telemetry.
Rana et al. — Lightweight cryptography in IoT networks: a	Lightweight ciphers for IoT	Typical IoT ciphers report latencies 8–20 ms depending on	Tradeoffs summarized; energy varies widely by implement	Security quantified by standard metrics; post-quant

survey [24]		hardware.	entation .	um literat ure evol ving.
Kumara n et al. — Hybrid DNA + ECC medical image encryption [25]	Hybrid DNA + ECC for medical images	Latenc y ~11 ms reporte d for image pipelin es.	Moderat e energy; targeted at large payload s (images).	Entro py report ed ~7.8 bits per byte for image ciphe rtexts .
This work — DO-OPT (DNA-Based Optical Cryptography)	IoT teletremetry (MQT T/CoA P small payload s)	Latenc y: 7.50 ms (64 B payload d).	Energy per byte: 0.354 mJ/B (64 B).	Entro py: 7.98 bits/b yte; NIST STS pass (15/1 5).

DO-OPT combined constrained DNA codebooks, an optical phase-noise TRNG and optical parallel encoding to target the small-payload, low-energy regime typical of IoT telemetry. Prior optical and photonic works demonstrated high bandwidth or strong link-layer security but did not evaluate MCU-level energy or small-block latency in heterogeneous IoT traces (OptoLink; Pistoia et al.; Drăgulinescu). Lightweight-cryptography surveys summarized tradeoffs but did not propose optical TRNG co-designs for DNA mapping (Rana et al.). Hybrid DNA+ECC work targeted large payloads (medical images) and reported comparable entropy but higher latency and energy for image pipelines (Kumaran et al.). Therefore, DO-OPT occupies a distinct point in the design space: comparable entropy to hybrid image schemes while delivering lower latency and substantially lower per-byte energy for IoT telemetry (Table 3).

DO-OPT reduced latency and energy by co-designing DNA maps with optical parallelism.

Latency gains were largest for small payloads (16–64 B), which are common in telemetry. Empirical improvements were statistically significant (paired t-tests, $p < 0.01$). The median end-to-end latency decreased from 12.00 ms (AES-128) to 7.50 ms (DO-OPT) for 64 B payloads, a 37.5% reduction. Energy per byte decreased from 0.500 mJ/B (AES) to 0.354 mJ/B (DO-OPT), a 29.2% reduction. The Normalized Energy–Delay Product fell to 0.54, indicating a strong cost–performance improvement for constrained devices.

Security claims were supported by entropy measures, a full pass of NIST STS, and low attack success rates in controlled ciphertext-only and replay scenarios. DO-OPT passed all NIST STS tests, whereas some prior DNA schemes had weaker empirical profiles and were shown vulnerable in recent cryptanalysis. Constraining DNA codebooks (GC balance, no long homopolymers) and employing an optical TRNG increased effective key unpredictability and mitigated attack vectors reported in key-recovery analyses (e.g., Makwana et al., 2025). The Key Unpredictability Index rose to 128 bits and ciphertext-only attack success dropped to 0.6% under test conditions.

5.1. Generalisation

DO-OPT generalized across protocol stacks and payload types typical in IoT telemetry. Experiments used Gotham Dataset 2025 which contained heterogeneous MQTT, CoAP and RTSP traffic and multiple attack classes. DO-OPT preserved latency and energy benefits across these traffic types and also handled occasional larger payloads without protocol-level changes. The constrained DNA mapping and optical KDF were protocol-agnostic and applied to any opaque payload bytes, enabling application to diverse telemetry and small-media cases.

5.2. Impact of Dataset Features on Model

Dataset characteristics shaped results. Gotham Dataset 2025 supplied many small packets and realistic timing, which amplified DO-OPT benefits because optical parallelism reduced per-packet wall-clock time while constrained DNA mapping avoided expensive per-bit operations. Payload size distribution affected measured energy-per-byte; small-payload prevalence increased the impact of fixed per-packet overheads, where DO-OPT outperformed baselines. The simulated 1,000-

node traces confirmed that these advantages persisted under scale and bursty conditions.

5.3. Impact of other Important Aspects

Hardware assumptions affected outcomes. The optical frontend emulation used SLM/phase-noise models and an FPGA-based emulator calibrated to published photonic parameters. Comparison to photonic interconnect roadmaps (OptoLink) suggested integrated photonic implementations could further reduce latency and energy but would require fabrication and packaging investments. Optical noise and detector sensitivity influenced key entropy; robust TRNG extraction was essential to realize PQARS gains.

5.4. Limitations and Threats to Validity

The first limitation is hardware emulation. DO-OPT measured optical behavior using an FPGA-based SLM and detector emulator calibrated to published device parameters. The emulator approximated real photonic timing and noise but did not include full fabrication variability, packaging losses, or long-term drift. Results therefore reflect an optimistic, yet plausible, photonic frontend; final energy and latency for a fabricated module may differ. OptoLink and other photonic hardware studies suggest promising trajectories but also highlight integration costs and engineering challenges.

The second limitation is dataset representativeness. Gotham Dataset 2025 provided a broad and reproducible IoT trace but was collected from an emulated testbed with a specific device mix and attack scripts. Field deployments may present different payload distributions, link-layer characteristics and environmental optical noise. While the 1,000-node simulation improved confidence about scalability, additional field trials and diversity in device classes are required to generalize beyond the evaluated scenarios. Threats from adversaries who adapt to optical-TRNG fingerprinting or exploit side-channels remain and require further adversarial testing.

6. CONCLUSION & FUTURE WORK

The paper presented DO-OPT, a DNA-based optical cryptography framework for IoT that delivered measurable latency and energy improvements while increasing ciphertext entropy and robustness. DO-OPT reduced median end-to-

end latency for 64 B payloads from 12.00 ms (AES-128) to 7.50 ms (−37.5%) and lowered energy per byte from 0.500 mJ/B to 0.354 mJ/B (−29.2%). Entropy per byte increased to 7.98 bits and Key Unpredictability Index rose to 128 bits; NIST STS passed fully (15/15). Attack success rates for ciphertext-only and replay tests fell substantially (to 0.6% and 1.1%, respectively). These results indicate that co-designing constrained DNA mappings with optical phase-noise TRNGs and parallel encoding yields a practical security layer for small-payload IoT telemetry. Future work will prototype an integrated photonic encoder, evaluate long-term reliability and cost at scale, perform adversarial side-channel analysis, and release code and emulation scripts to enable reproducible evaluation and community verification.

REFERENCES:

- [1] A. A. Abd El-Latif, M. Almousa, and B. Abd-El-Atty, "A robust image encryption scheme based on quantum walks and dynamic DNA for secure cloud applications," *IEEE Access*, 2025, Accessed: Dec. 08, 2025. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/11048783/>
- [2] Y. Makwana, A. Panigrahi, and S. K. Pal, "Complete Key Recovery of a DNA-based Encryption and Developing a Novel Stream Cipher for Color Image Encryption: Bio-SNOW," Mar. 10, 2025, *arXiv: arXiv:2503.06925*. doi: 10.48550/arXiv.2503.06925.
- [3] N. Alalwan, W. El-Shafai, M. Amoon, and B. Benjdira, "Cybersecurity advancements for medical image transmission: a hybrid optical-based cryptosystem harnessing chaos, DNA sequences, and mandelbrot keys," *Multimed. Tools Appl.*, vol. 84, no. 33, pp. 41671–41711, Apr. 2025, doi: 10.1007/s11042-025-20790-6.
- [4] P. Chithaluru, V. K. Reddy, P. Narsimhulu, and M. Kumar, "DNA computing for the smart wireless sensor networks," in *Blockchain and Digital Twin for Smart Healthcare*, Elsevier, 2025, pp. 395–417. Accessed: Dec. 08, 2025. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/B9780443303005000221>
- [5] I. Qiqieh, J. Alzubi, and O. Alzubi, "DNA cryptography based security framework for health-cloud data," *Computing*, vol. 107, no. 1,

- p. 35, Jan. 2025, doi: 10.1007/s00607-024-01393-9.
- [6] M. A. Abdelaal, A. I. Moustafa, H. Kasban, H. Saleh, H. A. Abdallah, and M. Y. I. Afifi, "DNA-Inspired Lightweight Cryptographic Algorithm for Secure and Efficient Image Encryption," *Sensors*, vol. 25, no. 7, p. 2322, 2025.
- [7] R. K. Tulala, P. K. and B. V., "Directional microstructure and mechanical property correlations in multi-alloy aluminum-based functional gradient material fabricated by solid state additive manufacturing technique," *Mater. Res. Express*, vol. 12, no. 11, p. 116502, Nov. 2025, doi: 10.1088/2053-1591/ae171a.
- [8] S. Aqeel, A. S. Khan, I. A. Abbasi, F. Algarni, and D. Grzonka, "Enhancing IoT security with a DNA-based lightweight cryptography system," *Sci. Rep.*, vol. 15, no. 1, p. 13367, 2025.
- [9] H. Sharma and S. Kaur, "Quantum-Inspired Hyperchaotic Bio-DNA Image Encryption for Real Time Medical Security," *IEEE Access*, 2025, Accessed: Dec. 08, 2025. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/11218049/>
- [10] K. Veeramani, S. Gupta, and A. Dhar, "Survey and Analysis of RGB Image Encryption Using DNA Cryptography: Exploring Novel Approaches for Enhanced Security," in *Cryptography, Biometrics, and Anonymity in Cybersecurity Management*, IGI Global Scientific Publishing, 2025, pp. 165–198. Accessed: Dec. 08, 2025. [Online]. Available: <https://www.igi-global.com/chapter/survey-and-analysis-of-rgb-image-encryption-using-dna-cryptography/378751>
- [11] V. Dubey and A. Gupta, "DNA Driven Mechanism for Genetic Ciphering to Protect IoT Images," in *2024 4th International Conference on Sustainable Expert Systems (ICSES)*, IEEE, 2024, pp. 1623–1630. Accessed: Dec. 08, 2025. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/10763101/>
- [12] Y. Makwana, A. Panigrahi, and S. K. Pal, "Complete Key Recovery of a DNA-based Encryption and Developing a Novel Stream Cipher for Color Image Encryption: Bio-SNOW," Mar. 10, 2025, *arXiv*: arXiv:2503.06925. doi: 10.48550/arXiv.2503.06925.
- [13] M. A. Abdelaal, A. I. Moustafa, H. Kasban, H. Saleh, H. A. Abdallah, and M. Y. I. Afifi, "DNA-Inspired Lightweight Cryptographic Algorithm for Secure and Efficient Image Encryption," *Sensors*, vol. 25, no. 7, p. 2322, Apr. 2025, doi: 10.3390/s25072322.
- [14] G. Wang, H. Liu, and X. Chen, "New constructions of DNA codes under multiple constraints and parallel searching algorithms," Sept. 10, 2024, *arXiv*: arXiv:2409.06519. doi: 10.48550/arXiv.2409.06519.
- [15] V. Patidar and G. Kaur, "A novel conservative chaos driven dynamic DNA coding for image encryption," *Front. Appl. Math. Stat.*, vol. 8, p. 1100839, Jan. 2023, doi: 10.3389/fams.2022.1100839.
- [16] S. Namasudra, "A secure cryptosystem using DNA cryptography and DNA steganography for the cloud-based IoT infrastructure," *Comput. Electr. Eng.*, vol. 104, p. 108426, Dec. 2022, doi: 10.1016/j.compeleceng.2022.108426.
- [17] M. A. Fetteha, W. S. Sayed, and L. A. Said, "A Lightweight Image Encryption Scheme Using DNA Coding and Chaos," *Electronics*, vol. 12, no. 24, p. 4895, Dec. 2023, doi: 10.3390/electronics12244895.
- [18] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoT: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022, doi: 10.1109/ACCESS.2022.3165809.
- [19] B. Rahul, K. Kuppasamy, and A. Senthilrajan, "Dynamic DNA cryptography-based image encryption scheme using multiple chaotic maps and SHA-256 hash function," *Optik*, vol. 289, p. 171253, Oct. 2023, doi: 10.1016/j.ijleo.2023.171253.
- [20] O. Belarbi, T. Spyridopoulos, E. Anthi, O. Rana, P. Carnelli, and A. Khan, "Gotham Dataset 2025: A Reproducible Large-Scale IoT Network Dataset for Intrusion Detection and Security Research." Zenodo, Feb. 05, 2025. doi: 10.5281/ZENODO.14502760.
- [21] D. Saiham, D. Wu, and S. Rahman, "Leveraging Photonic Interconnects for Scalable and Efficient Fully Homomorphic Encryption,"

- June 15, 2025, *arXiv*: arXiv:2506.12962. doi: 10.48550/arXiv.2506.12962.
- [22] M. Pistoia *et al.*, “Paving the Way towards 800 Gbps Quantum-Secured Optical Channel Deployment in Mission-Critical Environments,” *Quantum Sci. Technol.*, vol. 8, no. 3, p. 035015, July 2023, doi: 10.1088/2058-9565/acd1a8.
- [23] A. Drăgulescu, “Optical Correlators for Cryptosystems and Image Recognition: A Review,” *Sensors*, vol. 23, no. 2, p. 907, Jan. 2023, doi: 10.3390/s23020907.
- [24] M. Rana, Q. Mamun, and R. Islam, “Lightweight cryptography in IoT networks: A survey,” *Future Gener. Comput. Syst.*, vol. 129, pp. 77–89, Apr. 2022, doi: 10.1016/j.future.2021.11.011.
- [25] V. N. S. Kumaran, T. Manikandan, R. K. Dhanaraj, T. Al-Shehari, N. A. Alsadhan, and S. Selvarajan, “A secure medical image encryption technique based on DNA cryptography with elliptic curves,” *Sci. Rep.*, vol. 15, no. 1, p. 20003, June 2025, doi: 10.1038/s41598-025-03898-5.