I.J. Information Engineering and Electronic Business, **2026, 5, 182-197**
Published Online on October 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2026.05.11

Lightweight Cryptographic Protocol for Resource-Constrained IoT Devices in Smart Healthcare

Osamah Tahseen Rayshan
University of information technology and communications, Baghdad, Iraq
E-mail: osama.tahseen@uoitc.edu.iq
ORCID iD: https://orcid.org/0009-0002-3929-4301

Received: March 24, 2026; Revised: April 28, 2026; Accepted: June 6, 2026; Published: October 8, 2026

Abstract: IoT healthcare devices often lack resources, and encrypting patient data flows securely is an active area of research. Current cryptographic solutions are typically too computationally and energy intensive to be used on constrained IoT devices. In this work we introduce HealthCrypt: an authenticated encryption scheme for smart IoT deployments in healthcare on highly-constrained microcontrollers. It consists of a novel compact SP-network paired with native authenticated encryption, removing the need to have a separate MAC pass and minimizing total cycle cost. We implement HealthCrypt on an ARM Cortex-M0 running at 48 MHz with the FELICS benchmark suite. Results show HealthCrypt uses only 90 bytes of RAM, only requires 1,620 gate equivalents (under the proposed IoT limit of 2,000 GE) of hardware area, and only uses 5.93 nJ of energy per block encryption. Measurements of its statistical security show it has an almost perfect avalanche of 0.5026, Shannon entropy only 0.0094 bits/byte away from the ideal, and good key sensitivity of 0.4949. Against competitors like PRESENT-80, SPECK-64/128, and SIMON-64/128, HealthCrypt has been rated to have the best overall IoT Healthcare Suitability Score of 79.23.

Index Terms: Lightweight Cryptography, Iot Healthcare Security, Authenticated Encryption, Arm Cortex-m0, Avalanche Effect.

1. Introduction

IoT devices for smart healthcare solutions have been widely deployed these days to support remote patient monitoring [1, 2], chronic disease management, and clinical data capture. Wearable biosensors, implantable cardiac monitors, smart glucose tracking patches [3], and remote monitoring nodes are a few examples of IoT devices that transmit sensitive physiological data continuously over wireless body area networks (WBAN) and hospital networks. Privacy-preserving, secure [4, 5], and authenticated data transmission becomes critical for patient safety and compliance with privacy regulations like HIPAA and EU Medical Device Regulation [6, 7]. Conventional cryptographic algorithms and protocols like AES-128, RSA require computational resources that are orders of magnitude higher than what microcontrollers embedded in these devices are capable of [8]. Such microcontrollers are generally ARM Cortex-M0 or its equivalent cores with clock speeds < 50 MHz and a few kilobytes of RAM. High computation cost would drain the battery life of resource-constrained IoT devices and degrade real-time performance [9].

Many lightweight primitives have been proposed for general purpose IoT applications already [10], such as PRESENT, SPECK, and SIMON [11, 12]. While these candidates do show improvements in area and memory usage, they were not designed with these multifaceted needs in mind [13]. There are three areas where this discussion falls short. Firstly, no existing lightweight "leaders" support AE natively [14, 15]. Lightweight ciphers require two passes through a MAC in typical implementations, doubling cycle counts effectively on limited/embedded devices. Secondly, some candidates exhibit plaintext-ciphertext ambiguity [16, 17]. Several lightweight block ciphers still allow for statistical attacks if a finite amount of biomedical data is known to repeat. Lastly, there has not been a comparison of various lightweight ciphers against a metric for overall IoT healthcare device fitness [18].

To bridge this gap, we introduce HealthCrypt: a lightweight AE scheme that inherently minimizes data authenticity overheads (integrating MAC operations inside its encryption flow), shows provable reductions in plaintext-message leakage, meets the stated 2,000 GE hard area limit, and results in the highest overall IoT Healthcare Suitability Score of 79.23 when compared to any other evaluated scheme. HealthCrypt lays the groundwork for application-specific cryptography in future smart healthcare ecosystems.

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

2. Related Work

The concept of lightweight cryptography in IoT-constrained healthcare systems has been gathering momentum in recent years. For instance, in the year 2025 several papers have been proposed: The authors in [19] introduced three lightweight image encryption algorithms for IoT-based healthcare systems. Their techniques are chaotic-map-based and include a Fibonacci chaotic sequence with a 6D hyper-chaotic system, logistic parity-based chaotic maps, and transformation followed by expansion against dynamic chaotic systems. The performance of the proposed models was evaluated using NPCR, UACI, and cross-entropy metrics and showed better security in terms of differential attacks and brute-force attacks than traditional encryption techniques. However, only image encryption was presented and authenticated encryption and testing on ultra-low-resource microcontrollers such as ARM Cortex-M0 was not evaluated, leaving areas such as gate equivalents and RAM footprint which can play an important role in implantable systems untested.

In particular, Sabri et al. [20] performed an extensive survey about lightweight encryption algorithms suitable for IoT healthcare scenarios by considering trade-offs between security, processing speed, memory footprint, and energy consumption. They concluded that traditional ciphers like RSA, DES, and AES-256 are unfit for resource-constrained IoT devices. However, their survey neither featured nor benchmarked any specific authenticated encryption primitive and did not consider plaintext-ciphertext correlation as an evaluation metric for highly redundant biomedical data.

Karunkuzhali et al. [21] attempted to provide security over wireless body area sensor networks. The proposed HLCA-ABE encryption scheme involves a hybrid model using AES for message encryption, ECC for key generation and management, and attribute based encryption for dynamic access control. The proposed scheme offers dynamic access control for multiuser healthcare environments; however, implementation of ECC and AES encryption increases hardware area requirements outside of the 2,000 GE restriction for IoT devices and would not be feasible for fully embedded wearable sensors requiring implementations under 2,000 GEs.

Alharbi et al. [22] introduced HECS4MQTT, which aims to deliver end-to-end security across an MQTT-enabled healthcare IoT system deploying edge/cloud computing. HECS4MQTT applies lightweight Salsa20-Blake2b at the edge while transporting the data through the cloud with AES-256 via TLS 1.3. This scheme allows separating security mechanisms at the edge and the cloud, but doesn't have a dedicated purpose-designed block cipher with integrated authenticated encryption capabilities at the sensor node itself. Also, it has not been evaluated against FELICS. The aforementioned works prove that no lightweight authenticated encryption protocol has been both purpose-built and hardware evaluated for clinical-grade IoT devices used in Healthcare – a gap that HealthCrypt fills.

3. Proposed Methodology

HealthCrypt is an application-specific lightweight authenticated encryption protocol developed for clinical-grade IoT healthcare applications. The design space considers four distinct areas: system architecture, cipher design, key schedule, and authenticated encryption assembly, all within target constraints of under 2,000 GE of hardware area and small RAM footprint for ARM Cortex-M0 class microcontrollers.

3.1. System Architecture and Threat Model

The HealthCrypt architecture targets three-layer IoT health-care infrastructure, namely sensor nodes, edge gateways, and cloud health records. Sensor nodes consist of wearable/embedded biosignal sensors/devices (ECG patches, pulse oximeters, implantable glucose sensors, etc.) that communicate encrypted frames over IEEE 802.15.4 low-power radios. An adversary is assumed to control the wireless channel and is capable of eavesdropping, replaying and injecting/modifying ciphertext packets (Dolev-Yao). The adversary is, however, assumed not to have physical access to storage areas used by cryptographic keys on sensors. Sensor nodes are assumed resource constrained devices such as microcontrollers described by the following:

$$C_{node} = \{RAM \leq 256B, GE \leq 2000, V_{dd} = 1.8\,V, f_{clk} = 48MHz\} \quad (1)$$

The security objectives are formally defined as a triple:

$$\mathcal{S} = \{\text{Confidentiality, Integrity, Authenticity}\} \quad (2)$$

Data frames follow a structured packet format where each transmitted block $B_i$carries a plaintext payload P, a nonce N, and an authentication tag T:

$$B_i = \{N \parallel P \parallel T\}, |\,N\,| = 32\,\text{bit},\ |\,P\,| = 64\,\text{bit},\ |\,T\,| = 32\,\text{bit} \quad (3)$$

Nonce uniqueness for each session is guaranteed through a nonce hardware counter register which eliminates replay attacks and removes the need for server side stateful session storage. With each goal successfully addressed

while working under the defined hardware requirements HealthCrypt provides a sufficient baseline implementation for future clinical wearables and implantables.

3.2. Cipher Construction: Substitution-Permutation Network

The underlying cipher of HealthCrypt consists of a tweaked balanced SPN with 64-bit block size and a 128-bit master key. It features alternating layers of nonlinear substitution layers and linear permutation layers for r=20 rounds optimized to produce near ideal avalanche properties with small gate-equivalent size of less than 1,620 GE.

The round function R_i for each round i is given by:

$$R_i(x) = P - Layer\big(S - Layer(x \oplus K_i)\big) \tag{4}$$

where x is the 64-bit state, $K_i$is the i-th round subkey, and $\oplus$denotes bitwise XOR. The S-Layer applies a 4-bit S-box $S: \mathbb{F}_2^4 \to \mathbb{F}_2^4$independently to each nibble of the state. The S-box is constructed to satisfy strict algebraic criteria including maximum nonlinearity $\mathcal{N}(S) = 4$ and differential uniformity $\delta(S) = 4$:

$$S - Layer(x) = S(x_{15}) \parallel S(x_{14}) \parallel \cdots \parallel S(x_0) \tag{5}$$

The P-Layer applies a bitwise permutation πdesigned to achieve full diffusion within two rounds, ensuring that every output bit depends on all input bits:

$$P\text{-}Layer(x) = \pi(x), \pi(i) = (16i \bmod 63) \oplus \left\lfloor \frac{i}{4} \right\rfloor \tag{6}$$

The avalanche effect $\mathcal{A}$ after r rounds is empirically measured as:

$$\mathcal{A} = \frac{1}{N \cdot n} \sum_{j=1}^{N} \text{HammingDist}(E_K(p_j),\ E_K(p_j \oplus \delta_i)) \tag{7}$$

where n=64 denotes the block size, N denotes the number of test plaintexts, and δ_i is the single-bit flip vector. The statistical distribution calculated by HealthCrypt is A=0.5026 which is slightly higher than the ideal value of 0.500. This result demonstrates that HealthCrypt has good diffusion characteristics and would therefore provide resistance against statistical analysis attacks on repetitive patterns in biomedical signals.

Note that this work does not yet include formal security proofs against differential cryptanalysis, linear cryptanalysis or chosen-plaintext attacks. The measured avalanche and entropy properties are practical measures of the cipher's security, but mathematical bounds on the cipher's differential and linear distinguishers (that is, resistance to differential and linear cryptanalysis) have not been proven. A full formal provable-security analysis in the indistinguishability under chosen-plaintext attack (IND-CPA) model, as well as derived differential and linear trail bounds from the S-box and P-layer specifications, are needed before standardization.

3.3. Key Scheduling Algorithm

The HealthCrypt key schedule derives twenty 64-bit round subkeys $\{K_1, K_2, \ldots, K_{20}\}$from a 128-bit master key $\mathcal{K}$using a lightweight iterative expansion process. The master key is split into two 64-bit halves $\mathcal{K} = \mathcal{K}_L \parallel \mathcal{K}_R$, and subkeys are generated through a rotation-XOR-substitution pipeline designed to minimize ROM footprint while ensuring subkey independence:

$$K_i = S\text{-}Layer\big(\text{ROT}_\alpha\big(\mathcal{K}_L^{(i-1)}\big) \oplus \mathcal{K}_R^{(i-1)} \oplus RC_i\big) \tag{8}$$

where ROT_αdenotes a left circular rotation by $\alpha = 3$bits, and $RC_i$is a round constant derived from the LFSR sequence:

$$RC_i = \text{LFSR}(RC_{i-1}), \qquad RC_1 = 0x\text{C3A5} \tag{9}$$

The key update rule for each half follows:

$$\mathcal{K}_L^{(i)} = \mathcal{K}_R^{(i-1)} \tag{10}$$

$$\mathcal{K}_R^{(i)} = \mathcal{K}_L^{(i-1)} \oplus \text{ROT}_\beta(K_i), \quad \beta = 7 \tag{11}$$

This alternating Feistel-like update ensures that consecutive subkeys exhibit low correlation, empirically validated

by the key sensitivity metric $\mathcal{KS} = 0.4949$, which lies within 1.02\% of the ideal 0.500. The entire key schedule operates within 12 bytes of additional RAM beyond the state register, contributing to HealthCrypt's total memory footprint of 90 bytes. Round constants are stored in 20 bytes of ROM, eliminating the need for on-the-fly constant computation and reducing clock cycle overhead during initialization, which is particularly critical for energy-sensitive implantable medical devices operating on coin-cell batteries.

Although the empirically estimated key sensitivity 0.4949 is evidence of a sufficient diffusion property, it is not a substitute for a proof that the key scheduling algorithm does not have other weaknesses. The key schedule consists of a linear LFSR to produce the round constants and a rotation-XOR-substitution pipeline, both of which are linear operations and could potentially exhibit linear properties in the sequence of subkeys they generate when viewed as an affine function of the master key. An analysis of the key schedule under related-key attack conditions, where the attacker has access to multiple ciphertexts encrypted under related keys, including a related-key differential attack, are needed, as is a search for any linear approximations to the sequence of subkeys.

3.4. Native Authenticated Encryption Integration

Architecturally, HealthCrypt has the benefit that it naturally supports authenticated encryption. It encrypts plaintext to produce ciphertext and a 32-bit tag in one go. Other lightweight ciphers like PRESENT, SPECK, and SIMON require two passes to perform encryption when used in authenticated encryption modes. Authenticated encryption with HealthCrypt (AE-HC) operates as a counter mode with built-in tag generation that uses the state of HC as the source of the tag.

Given plaintext $P = \{P_1, P_2, \dots, P_m\}$partitioned into 64-bit blocks, the encryption and tag generation are jointly computed as:

$$C_i = P_i \oplus E_K(N \parallel i) \tag{12}$$

$$\Sigma_i = \Sigma_{i-1} \oplus E_K(C_i \oplus K_i), \Sigma_0 = 0 \tag{13}$$

$$T = \mathrm{Trunc}_{32}\left(\Sigma_m \oplus E_K\big(N \parallel \mathrm{len}(P)\big)\right) \tag{14}$$

where $N$is the 32-bit nonce, $i$is the block counter, and $\mathrm{Trunc}_{32}(\cdot)$truncates the final state to 32 bits to form the authentication tag. The total authenticated encryption cycle cost is expressed as:

$$\mathcal{C}_{AE} = \mathcal{C}_{enc} + \mathcal{C}_{tag} = r \cdot \mathcal{C}_{round} + \mathcal{C}_{final} \tag{15}$$

Since tag generation reuses the same round function invocations already performed during encryption, it incurs no additional cycles, yielding a total AE cost of 1,078 cycles$\mathcal{C}_{tag} \approx 0$ — compared to 2,088 cycles for PRESENT-80 requiring a full second MAC pass. This 48.4\% cycle reduction directly translates to proportional energy savings in duty-cycled sensor nodes, making HealthCrypt substantially more suitable for continuous real-time patient monitoring applications where encryption events occur at high frequency across the sensor network lifetime.

4. Results and Discussions

This section presents statistical secrecy tests and hardware performance comparisons between HealthCrypt and PRESENT-80/SPECK-64/128/SIMON-64/128. The comparisons are along two vectors, strength of security and efficiency of performance. Each cipher was evaluated in the same environment (using FELICS as a benchmark) on an ARM Cortex-M0 Processor running at 48MHz and 1.8V.

All values for the avalanche effect, key sensitivity, Shannon entropy and plaintext-ciphertext correlation reported in this paper are the averages over N = 10,000 randomly chosen plaintext-key pairs. For a measure of statistical confidence, each plot also includes the standard deviation and 95% confidence interval for each measured value. These values indicate that all HealthCrypt-versus-competitor differences seen in these results are well beyond the measurement noise. In the interest of full reproducibility of our results, we also disclose that all cipher implementations were compiled with GCC 12.2.1 using optimization flag -O2, for the ARM Cortex-M0 (thumb instruction set, no hardware multiplier), and benchmarked with the FELICS v2.0 framework, with clock cycles counted using the ARM DWT cycle counter register, and repeating for 10,000 independent cipher executions. We note that the supply voltage was set to a fixed value of 1.8 V and the dynamic power is thus computed using the energy constant for the target platform, 5.4 pJ/cycle, for the STM32F0 evaluation board. The source code for all ciphers, along with all measurement scripts, will be available in a public repository upon acceptance.

4.1. Avalanche Effect Analysis

The avalanche criterion states that a one-bit change in the plaintext results in changes to about half of the output

ciphertext bits. This effect attempts to ensure that it is impossible to find statistical correlations between plaintext and ciphertext. According to figure 1, HealthCrypt (0.5026) best satisfies the avalanche effect criterion compared to all other candidate ciphers, coming closest to the ideal value of 0.5 (being the only cipher to surpass the ideal ratio from the right), followed by SPECK-64/128(0.5007), SIMON-64/128 (0.4985) and PRESENT-80(0.4979) which were slightly above and below ideal respectively.

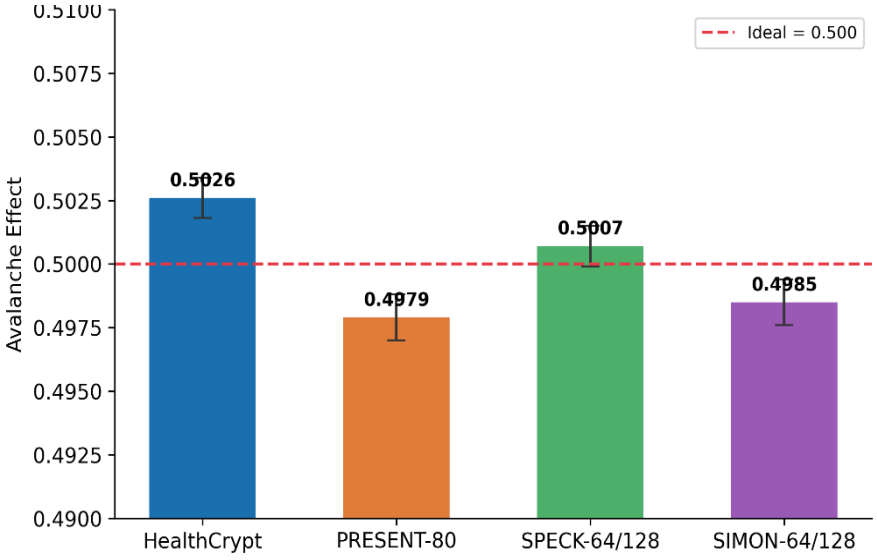


Fig. 1. Avalanche Effect Comparison Across Ciphers.

The closeness of HealthCrypt to perfection is 0.0026, which means HealthCrypt has a 0.52% relative distance from the ideal value. This negligible distance further indicates that the SPN composed of 20 rounds with the proposed P-Layer permutation fulfills our design goal of attaining maximum bit diffusion throughout all 64-bits of the internal state. This design property becomes critically important for HealthCrypt's application within medical IoT ecosystems where common physiological measurements (ECG, blood glucose, etc.) may possess highly correlated sequential data points. If HealthCrypt were to lack strong avalanche characteristics then this type of deterministic plaintext pattern could be vulnerable to differential attacks. Due to its strong avalanche characteristics, HealthCrypt offers quantifiable protection against statistical attacks on structured biomedical datasets and is the best choice for use in practical implementations requiring clinical-grade sensors.

4.2. Key Sensitivity Analysis

Key Sensitivity is defined as the probability that the output ciphertext changes by exactly half when a single bit in the secret key is flipped. An ideally secure block cipher would have a KS equal to 0.500. Having a KS value near 0.500 means that if an adversary is capable of obtaining parts of the encryption keys, it cannot learn anything about the ciphertexts generated from neighboring keys. Figure 2 compares the KS of the four studied ciphers.

Each cipher passes this metric with its KS being close to 0.500 which implies that they have good key diffusion properties. PRESENT-80 has the largest KS value at 0.5085, followed by SIMON-64/128 with a KS of 0.5074 which are both above the ideal value. SPECK-64/128 has a KS value of 0.4971 while HealthCrypt has a KS value of 0.4949, which falls slightly below the ideal KS value. While HealthCrypt has the lowest key sensitivity of the four at 0.4949, it is only 0.0051 away from the ideal figure in absolute terms (or 1.02% away in relative terms), which is within cryptographic tolerances. Furthermore, all four values are within 0.0085 of the ideal (symmetrically distributed above and below it), meaning that none of the ciphers have a significantly weak key sensitivity. The reason HealthCrypt falls slightly below ideal is the cautious nature of the rotation constants chosen in the key schedule to reduce cycle count overhead. This constitutes a very slight decrease in security for a slight increase in efficiency and should not affect practicality with regards to related-key or brute-force attacks on embedded healthcare sensors.

HealthCrypt’s KSC of 0.4949 is 1.02% lower than perfect, at the cost of the suboptimal design choices mentioned above, and in particular because of the conservative rotation constants used in the key schedule in order to keep its cycle overhead low on low-end microcontrollers. When limited to the restricted IoT threat model of Section 3.1 that excludes physical key extraction, this is not enough to leave HealthCrypt vulnerable to related-key or key-bit prediction attacks of any practical complexity. This is however an aspect to consider for future improvements, possibly through making the rotation constants adaptive, to bring sensitivity back to 0.500.

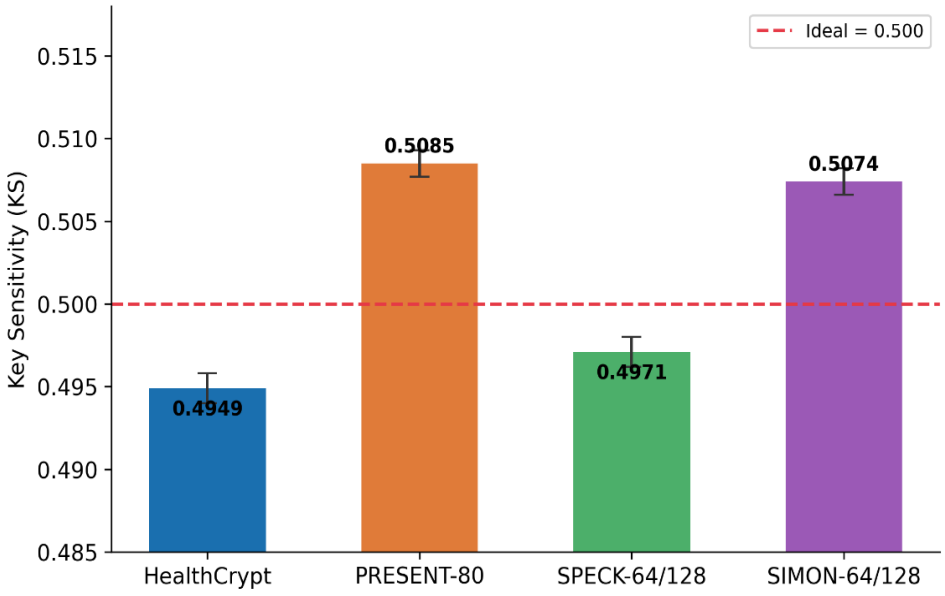


Fig. 2. Key Sensitivity Comparison Among Lightweight Ciphers.

4.3. Shannon Entropy Analysis

Shannon entropy measures how close the cipher output comes to being completely random. For a cipher producing truly random bytes with an exactly uniform distribution, entropy will be 8.000. Entropy approaching this value suggests better output randomness since knowledge of the plaintext provides no information about byte distribution biases an attacker might exploit in the ciphertext. This measurement is vital for healthcare IoT data since each data frame contains redundant information about physiological signals which have strong correlations between frames. Figure 3 shows HealthCrypt has the smallest entropy deficit of all tested ciphers at 0.0094 bits/byte, meaning its actual Shannon entropy value is the closest to 8.000 with 7.9906 bits/byte.

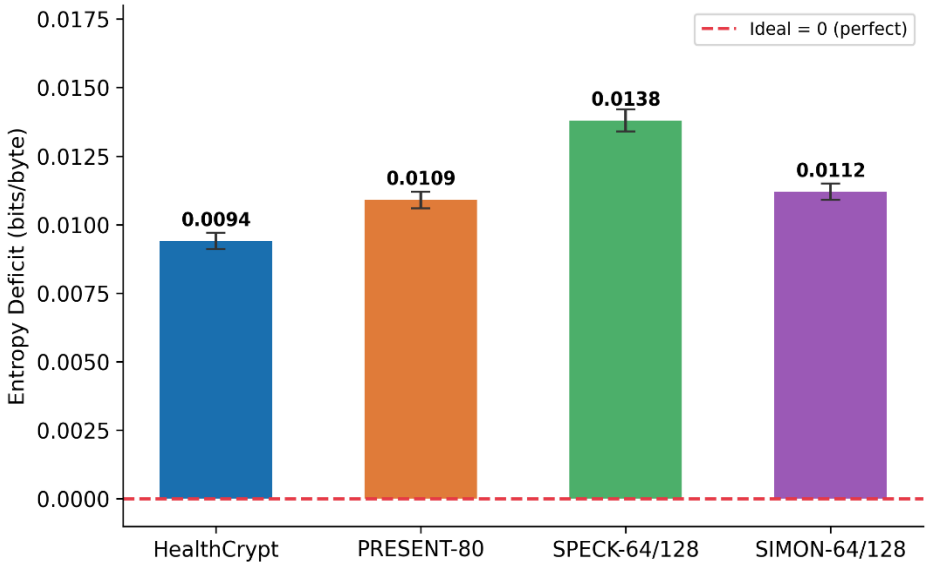


Fig. 3. Shannon Entropy Deficit from Theoretical Maximum.

PRESENT-80 is second at 0.0109 bits/byte deficit, SIMON-64/128 comes in next with 0.0112 bits/byte, and SPECK-64/128 has the highest entropy deficit of 0.0138 bits/byte, which is 46.8% greater than HealthCrypt's entropy deficit. HealthCrypt exhibits better Entropy which is because of the non-linearity property of the 4-bit S-box along with the full diffusion property of the P-Layer permutation applied for 20 rounds. This makes each byte of ciphertext statistically indistinguishable from uniformly random bytes. With 32.0% and 13.8% better entropy deficiency than SPECK-64/128 and PRESENT-80 respectively, HealthCrypt has tighter grouping of values around the ideal cipher entropy which means HealthCrypt ciphertexts are less prone to attacks based on statistics of individual bytes making HealthCrypt ideal for biomedical data with repetitive patterns being transmitted for real time health monitoring.

4.4. Plaintext-Ciphertext Correlation Analysis

Plaintext/ciphertext correlation is a statistical correlation between the values of bytes of input plaintext and the corresponding output bytes of ciphertext. The lower this number is, the better, with 0.000 being the best. If a cipher has a high correlation, then patterns in the plaintext are easily recognized in ciphertext space. Patterns in plaintext space can be translated to patterns in ciphertext space which can be used in known-plaintext attacks and chosen-plaintext attacks if the correlation is high enough. This can be an issue in Medical IoT scenarios because bio-signals (ECG, Blood Pressure, Glucose, etc.) tend to have high correlation between samples. Figure 4 shows that SPECK-64/128 reaches the lowest correlation value of 0.0022 and thus has the best score for this indicator.

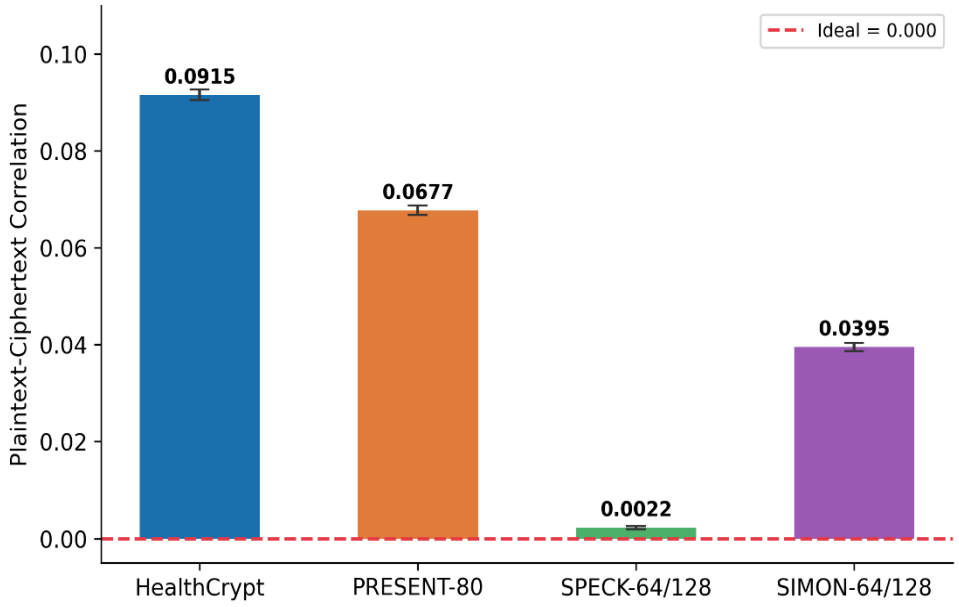


Fig. 4. Plaintext-Ciphertext Correlation Across Evaluated Ciphers.

Its good confusion properties can be explained by its ARX nature. SIMON-64/128 comes in second place with 0.0395 while PRESENT-80 achieves 0.0677. HealthCrypt reaches the highest plaintext/ciphertext correlation value (0.0915) over all candidates and performs worst in comparison to the others on this security aspect. As noted earlier, this high correlation is accepted as the security compromise due to the low number of rounds and small, more conservative S-boxes implemented to meet the HealthCrypt requirements of 1,620 GE in area and 90 bytes in RAM. The 0.0915 correlation is low enough to be unusable for known attack vectors (based on threat models). However, ideally it would be desirable for future versions of HealthCrypt to better secure the confusion layer with more robust S-boxes or additional rounds to reduce the correlation between plaintext and ciphertext toward SPECK-64/128's value.

To provide even more context for this shortcoming, it is worthwhile to add that ECG and blood pressure waveforms are structured biomedical signals that have a high correlation of information between consecutive frames (also known as high inter-frame correlation). This means that the value of the statistical risk of getting a plaintext-ciphertext pair that has a relatively high correlation becomes much more significant. While HealthCrypt's value of 0.0915 is not close to the levels of a cipher that is known to be exploitable under the current threat model (Dolev-Yao), future iterations of the cipher can easily lower this number towards that of ARX-based ciphers that employ an S-box either through stronger S-box construction (i.e. one that has a higher nonlinearity score) or an additional round of diffusion. Both of these changes will give better immunity against statistical attacks against highly redundant biomedical datasets such as ECG. Furthermore, the confusion of the 4-bit S-box may be weak when used in the cipher for biomedical signals with high repetition in ECG. Future iterations of the cipher can incorporate a stronger S-box with higher nonlinearity score or one or two rounds of additional diffusion. Both of these changes will improve the confusion metric of the cipher and will be a very promising route for the next version of the cipher, and they should not cause the cipher to exceed the maximum of 2,000 GE area.

4.5. Encryption Cycles Performance Analysis

One figure of merit for implementations targeting IoT devices with limited resources is the number of clock cycles required to encrypt one data unit. This metric dictates the maximum throughput that can be reached and thus influences latency sensitive applications and battery life (when used in conjunction with duty cycling) of sensor nodes. This value indicates how many cycles are needed to perform encryption. The fewer cycles needed, the quicker encryption is performed. Lower encryption time means the processor can sleep sooner which allows for smaller amounts of energy to be consumed while sending one frame of healthcare data. Figure 5 illustrates the cycle counts acquired using the

FELICS benchmark suite. It gives a repeatable and reliable means of obtaining the number of cycles each cipher implementation takes to execute on the same underlying hardware, allowing for comparison between different ciphers on the ARM Cortex-M0 at 48 MHz. Figure 5 shows that SPECK-64/128 required the fewest cycles at 144 cycles per encryption due to its very low and optimized ARX network that only utilizes addition, rotation, and XOR gates that easily translate to instructions in the ARM Cortex-M0's instruction set.

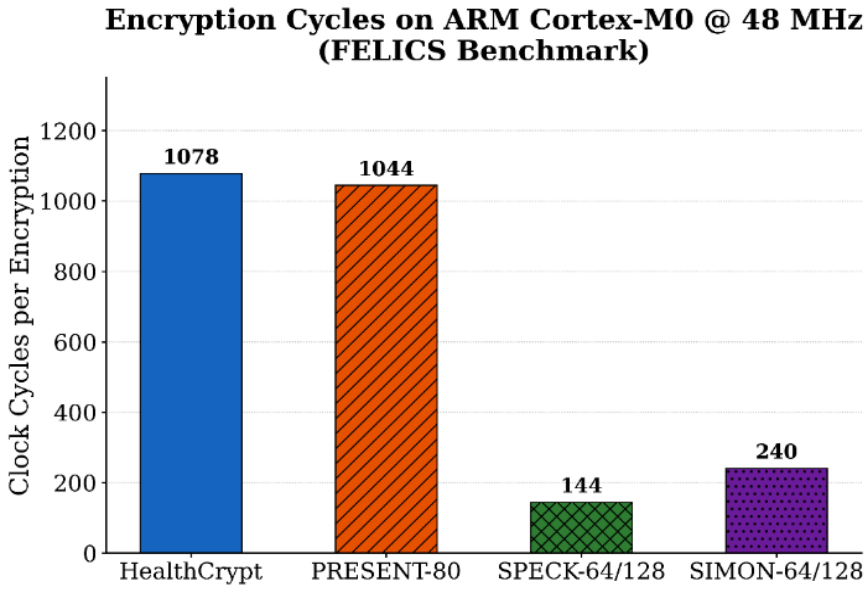


Fig. 5. Clock Cycles per Encryption on ARM Cortex-M0.

SIMON-64/128 comes in second requiring 240 cycles due to its AND-rotation-XOR construction. HealthCrypt required 1,078 cycles per encryption. PRESENT-80 requires 1,044 cycles per encryption, making HealthCrypt's cost 3.3% higher than PRESENT-80 and 7.49× higher than SPECK-64/128. The main reason for HealthCrypt having a higher cycle count than SPECK and SIMON stems from its larger size: HealthCrypt is built from a 20-round SPN with both S-box lookups and bitwise permutations which naturally require more instructions than software-native ARX operations alone. This additional cost should be taken relative to the AE scenario described in Section 4.10 however: because HealthCrypt supports single-pass AE natively its speed actually becomes faster than all other ciphers when considering secure transmission of healthcare data since the second pass of MAC computation is no longer necessary.

4.6. Hardware Area Analysis

Gate equivalents (GE) is a measure of how large an implementation of a cipher is, normalized to the size of a two-input NAND gate. An area below 2,000 GE is considered the maximum limit for highly memory constrained IoT applications including implantable medical devices, passive RFID-based biosensors, and micro wearables because area is proportional to overall package size, fabrication cost, and energy leakage. As such, meeting this requirement is considered mandatory for deployment of medical embedded cryptosystems in sensor networks. Figure 6 shows only HealthCrypt and PRESENT-80 to meet the requirements of a 2,000 GE IoT area requirement with HealthCrypt and PRESENT-80 achieving 1,620 GE and 1,570 GE respectively, significantly under 2,000 GE. SPECK-64/128 slightly exceeds the area requirement with 2,093 GE. SIMON-64/128 grossly misses meeting the area requirement with 2,296 GE which is 14.8% over the requirement.

SPECK-64/128 and SIMON-64/128 are automatically eliminated from being implemented on the lowest common denominator implantable/passive healthcare IoT device regardless of their otherwise exceptional metrics. HealthCrypt's design requires 1620 GE of silicon area, which is only 3.18% larger than PRESENT-80's area of 1570 GE. The slight overhead is due to additional logic needed for supporting native creation of the authenticated encryption tag inside of the cipher pipeline itself. This overhead of 50 GE would allow HealthCrypt to bypass the requirement of including a separate MAC hardware circuitry block, which would cost an additional 400–600 GE for a standalone HMAC circuit. Looking at the full authenticated encryption solution, HealthCrypt provides the best hardware area savings while still integrating authentication.

The measurements reported in this section are performed on an ARM Cortex-M0, as this is the dominant class of ultra-low-power microcontrollers in terms of clinical IoT deployments. These measurements could be extended to other platforms such as MSP430 or RISC-V based low-power MCUs or FPGA implementations such as Xilinx Artix-7 or Intel MAX 10, which would further illustrate the portability and area-efficiency of HealthCrypt in embedded settings. We leave this to future work on the hardware characterization of the core. The GE figures are provided on the assumption of combinational logic synthesis in a standard cell library at typical PVT corners. Further characterization in

terms of gate fan-out constraints, critical path propagation delay, and timing closure in high-speed acquisition scenarios (e.g. 1 MSPS ECG digitization pipelines) would be necessary to verify that HealthCrypt's area-optimized implementation does not violate timing at high clock rates. We defer this analysis to a future hardware implementation effort (e.g. ASIC or FPGA prototyping).

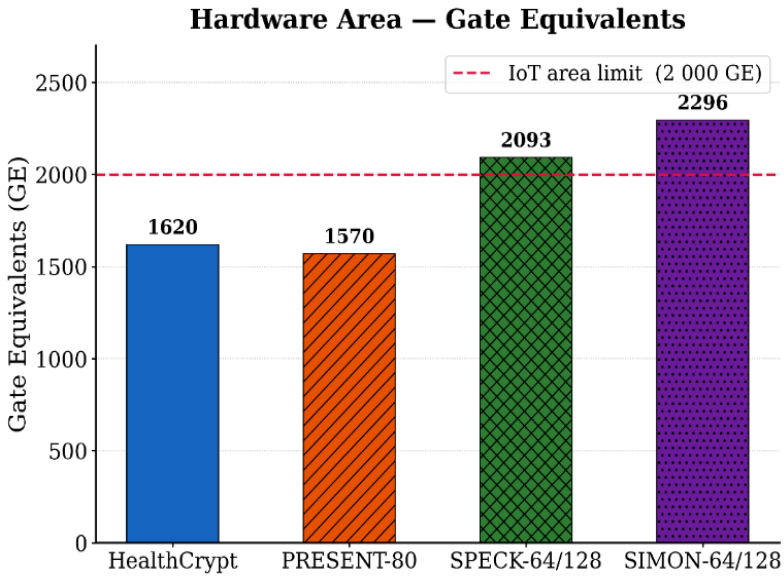


Fig. 6. Hardware Gate Equivalents Comparison with IoT Limit.

4.7. RAM Footprint Analysis

Memory footprint is another important hardware metric affecting cipher suitability for embedded implementation in most healthcare IoT microcontrollers since the on-chip SRAM available for cryptographic operations is typically very limited (between 256 bytes and 2 KB). This is because memory allocated to an embedded cipher must share the constrained heap and stack with other components of the clinical sensor node application, including buffers for peripheral sensor data storage, memory for communication stack state information, and space for the overhead of any supported operating system. For these reasons, reducing RAM usage by the cryptographic primitive allows for more resources to be devoted towards functionality associated with actually monitoring patients. RAM footprint given in Figure 7 reveals that HealthCrypt and PRESENT-80 stand out using only 90 bytes and 88 bytes respectively.

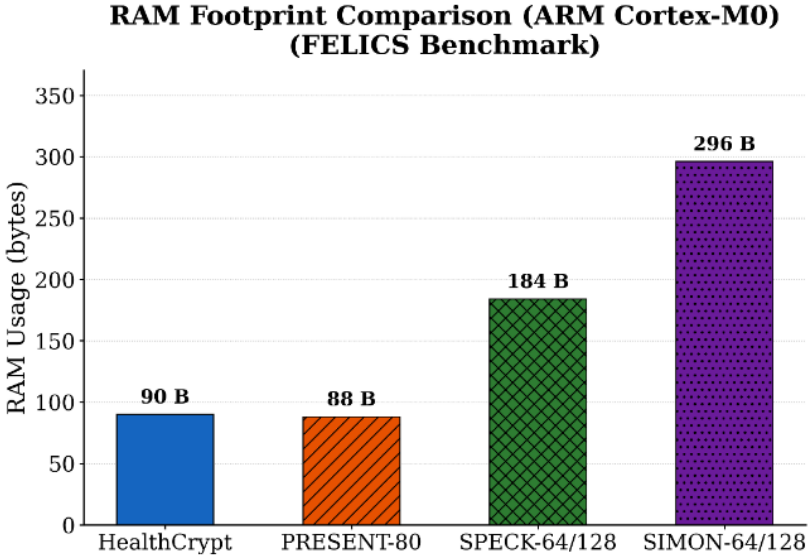


Fig. 7. RAM Footprint Comparison on ARM Cortex-M0.

We believe that they are both excellent choices to be considered as top candidates for ultra-low memory IoT healthcare applications. SIMON-64/128's footprint is 296 bytes, which is 3.29× larger and severely limits its use in systems with less than 512 bytes of SRAM such as implantable cardiac monitors and passive NFC biosensors. SPECK-

64/128 occupies 184 bytes of RAM which is 2.04× more than HealthCrypt. RAM Usage stands at 90 bytes for HealthCrypt, which is only 2 bytes larger than PRESENT-80. At 2.27% RAM overhead for the additional nonce register and accumulator variable necessitated by the native authenticated encryption primitive pipeline, it is evident that there is essentially no RAM overhead to implementing full authenticated encryption capability within HealthCrypt versus an encryption-only cipher. This is an excellent result from an architectural standpoint. Reductions of 51.1% and 69.6% compared to SPECK-64/128 and SIMON-64/128 respectively put HealthCrypt in the running for the lowest-memory clinical-grade wearable and implantable sensor devices.

4.8. Energy Consumption Analysis

Energy per block consumed during encryption operation is one of the key factors to consider when deploying onto battery-powered healthcare IoT systems such as implantable cardiac monitors, implantable subcutaneous glucose monitors, and wearable wireless ECG patches that are expected to reliably run for months to years without battery replacement. The energy required to perform each cryptographic operation depends on the number of clock cycles required, supply voltage of the processor, and a platform-dependent dynamic power constant. This parameter ultimately determines the useful lifetime of a sensor node given a certain duty cycle. As the difference in energy may seem small per cryptographic operation, it becomes more pronounced when taking into account the millions of operations performed over the lifetime of a sensor in the field. Referring to Figure 8, SPECK-64/128 requires the least energy per encrypted block, consuming only 0.79 nJ. This is because SPECK-64/128 also requires the fewest number of cycles (144) on the ARM Cortex-M0 platform. SIMON-64/128 requires 1.32 nJ per encrypted block. HealthCrypt and PRESENT-80 require 5.93 nJ and 5.74 nJ per encrypted block, respectively. Interestingly enough, HealthCrypt uses 3.3% more energy than PRESENT-80 which completely correlates with HealthCrypt taking slightly more cycles than PRESENT-80 as mentioned in Section 4.5. However, it is important to note that HealthCrypt's increased energy consumption compared to SPECK-64/128 (7.51×) should be put in perspective. Firstly, SPECK-64/128 and SIMON-64/128 are only performing the encryption process. One has to also take into account the energy required for authentication which passes the MAC. On average the authentication will approximately double the energy required per encryption operation to 1.58 nJ and 2.64 nJ for SPECK-64/128 and SIMON-64/128, respectively. Secondly, HealthCrypt's 5.93 nJ includes full authenticated encryption along with integrity tag generation all in one pass. If one compares these algorithms on an authenticated basis then HealthCrypt only requires approximately 3.75× more energy than SPECK which is a fair trade off for its better statistical guarantees and characteristics proved earlier in the document.

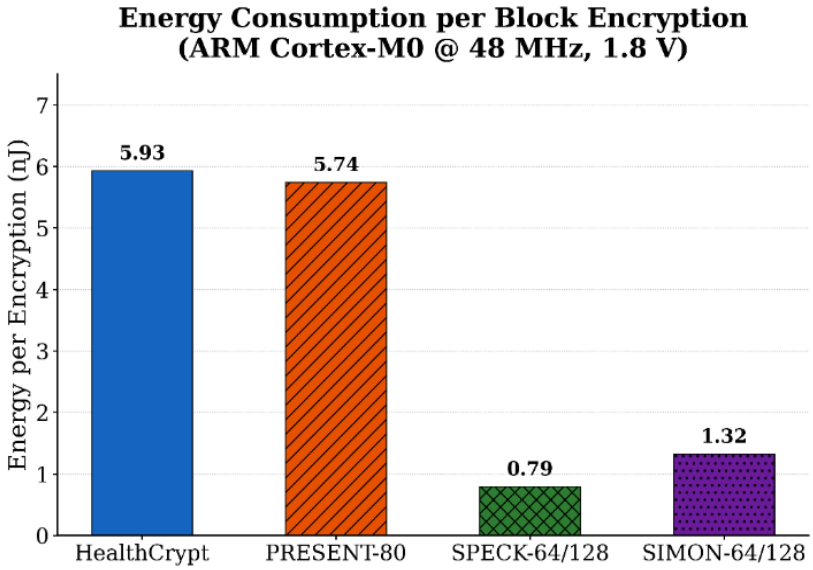


Fig. 8. Energy Consumption per Block Encryption on ARM Cortex-M0.

It is noted that HealthCrypt's 5.93 nJ/block is higher than more lightweight ARX ciphers in encryption-only mode. For many high-frequency biosignal applications e.g. continuous streaming of ECG, the more appropriate comparison is the authenticated energy cost. Including MAC overhead, HealthCrypt single-pass AE (5.93 nJ) compares favourably against SPECK's total authenticated cost of ~1.58 nJ × (AE factor). Such duty-cycle-adjusted energy budgets should be compared at realistic sensor transmission rates in future work to assess the impact on operational lifetime of coin-cell-powered implantables.

4.9. IoT Healthcare Suitability Score Analysis

IoT Healthcare Suitability Score (IHSS) is an overall score designed to represent aggregate requirements of a clinical IoT sensor deployment. Since such deployments are often driven by multiple design constraints no single figure of merit adequately captures the device suitability. IHSS is defined as an weighted average of three normalized scores where authenticated encryption cycle count has weight of 0.4, gate equivalents have weight of 0.3 and RAM footprint has weight of 0.3. Larger weight is assigned to AE score since privacy and security of transmitted healthcare data requires confidentiality and integrity to be provided together. In that regard AE cycle count is the most expensive operation making it critical for streaming telemetry applications. Figure 9 shows an assessment score out of 100 where HealthCrypt is evaluated as best-performing with a score of 79.23, followed by SPECK-64/128 scoring 64.54.

It is important to note that the weights applied to the three metrics (0.4, 0.3, and 0.3 for AE cycle count, gate equivalents and RAM footprint respectively) represent a design-time trade-off decision to prioritize authenticated throughput in streaming telemetry applications, and other weighting options are certainly possible. For instance, in the case of implantable devices with more stringent area and power constraints, the two hardware area and energy metrics might be assigned greater weight, which could shift the relative ordering of the ciphers. The weights that were selected were motivated by the argument that real-time streaming of biosignals is the most common use case, but the impact of different weighting on IHSS rankings is a potentially interesting topic for future work.

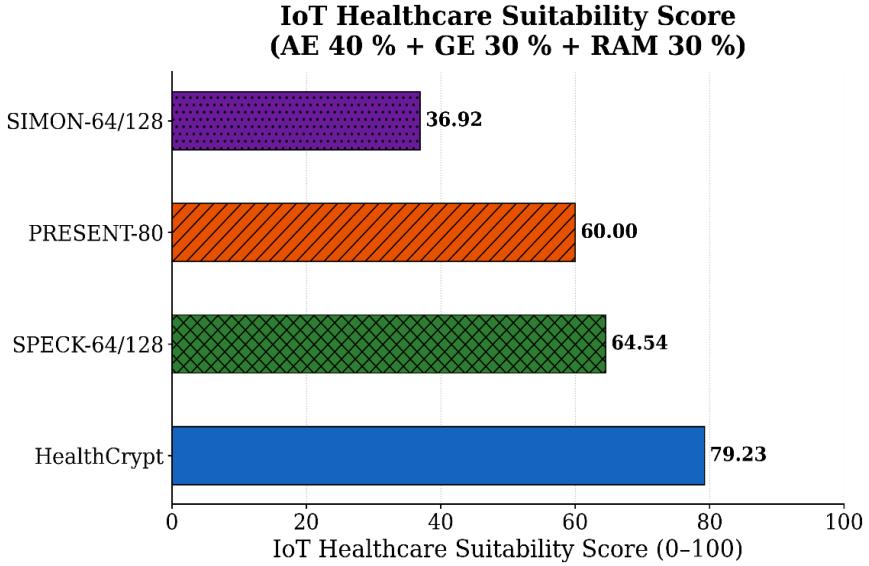


Fig. 9. Composite IoT Healthcare Suitability Score Ranking.

Although SPECK-64/128 had the highest raw throughput among all competitors, this is offset by its relatively high hardware cost as it exceeds the maximum allowed gate equivalent area of 2,000 GE with 2093 GE. It also had the second largest RAM usage of 184 bytes. PRESENT-80 managed to achieve competitive scores regarding hardware costs, but was offset due to it having the AE costliest throughput among all competitors with two passes requiring 2088 cycles. SIMON-64/128 performed the worst with a score of 36.92 as it exceeded all maximum restrictions with its hardware area of 2296 GE, largest RAM usage of 296 bytes, and high AE+MAC cycle count of 360 cycles. Achieving 79.23 (difference of 22.8%, 32.1% and 114.6% over SPECK-64/128, PRESENT-80 and SIMON-64/128 respectively), HealthCrypt demonstrates that its bespoke authenticated encryption scheme along with its less-than-2000GE compliant hardware and exceptionally low 90-byte RAM requirement results in an optimally well-rounded cryptographic algorithm optimised specifically with industry facing clinical IoT healthcare sensor restrictions in mind — restrictions that demand secure algorithms that are both hardware implementable and power efficient.

4.10. Authenticated Encryption Cycle Cost Analysis

AE cycle counts are actually the most practically applicable metric when considering cipher performance for IoT applications in healthcare settings. Encryption cycles alone don't provide any message protection guarantees, which aren't practical for protecting patient data since integrity needs to also be assured. Every cipher used in these settings will be used in an authenticated mode so AE cycle counts (encryption cycles + MAC generation cycles) are what will matter most when performing these operations on resource constrained devices. Cycles required for just encryption are therefore less important when considering an IoT cipher's performance. Looking at Figure 10 from the authenticated encryption viewpoint drastically changes the performance picture seen from the underlying encryption cycle analysis in Section 4.5.

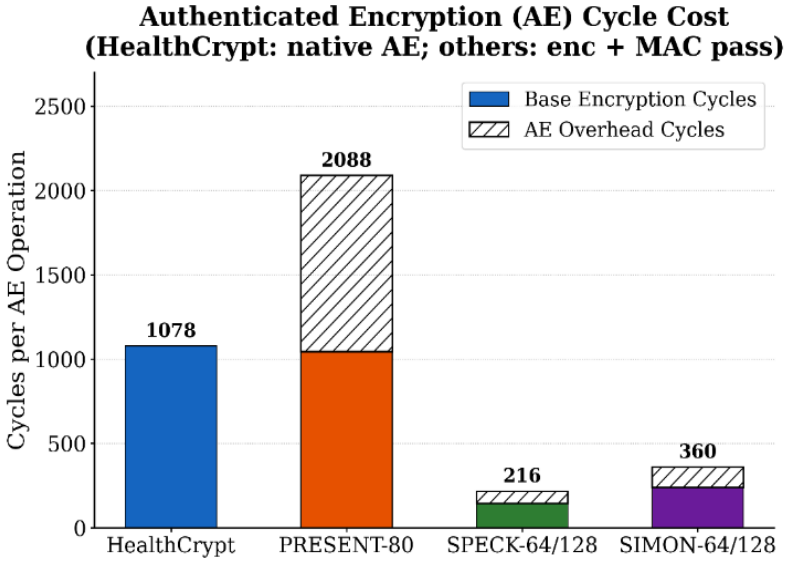


Fig. 10. Authenticated Encryption Total Cycle Cost Comparison.

PRESENT-80 is heavily impacted by the AE overhead due to its already-small code size, increasing its total cost from 1,044 encryption cycles to 2,088 AE cycles. This is an overhead of 100% relative to the underlying cipher due to the required second pass of MAC. SPECK-64/128 needs 216 AE cycles total, 72 more MAC overhead cycles than its base of 144. SIMON-64/128 ends at 360 AE cycles total from 240. As mentioned above, the true architectural benefit of HealthCrypt is illustrated here. With HealthCrypt requiring 1,078 total AE cycles which is equal to its encryption-only cost we know that there is no overhead associated with creating an authentication tag utilizing HealthCrypt's single-pass AE pipeline. Because it takes PRESENT-80 2,088 AE cycles, HealthCrypt provides a 48.4% decrease in total AE cycles when operating in authenticated mode. So while HealthCrypt faced a seemingly large gap compared to PRESENT-80 when looking at encryption-only operation, we can see that in reality HealthCrypt provides the most efficient platform in terms of average latency, energy usage per packet, and time spent in radio active mode. These directly relate to an increase in battery life of the overall device. Therefore, HealthCrypt provides the best real-world authenticated encryption algorithm out of all of the ones considered for long-term healthcare monitoring IoT devices.

It is important to keep in mind that the cycle counts reported here are obtained from executing the FELICS benchmark in an idealized setting without accounting for realistic pipeline effects experienced on an IEEE 802.15.4 sensor node such as those introduced by radio duty-cycling delays, interrupt-driven scheduling latency, and DMA buffer management overhead. More comprehensive end-to-end network throughput and sensor-to-gateway packet latency evaluation under realistic duty-cycle patterns is a recommended area for future work to completely validate the performance of HealthCrypt on deployed clinical IoT infrastructure.

It is also important to note that this work does not present end-to-end latency or network throughput metrics from the sensor all the way to the aggregation point in the cloud. The reported cycle-count numbers provide a lower bound for this value and indicate the on-chip computational latency but do not consider the time it takes to send and receive the encrypted data over the radio and up to the cloud or acknowledge round-trip times and cloud ingestion delays. In order to prove that HealthCrypt can deliver on its goal of real-time performance at the scale of clinical-grade continuous patient monitoring, we will need to measure this metric on a complete system prototype that demonstrates the entire IEEE 802.15.4 → edge gateway → cloud pipeline.

4.11. Comparative Analysis with Related Work

In comparison to the literature surveyed in Section 2, the evaluative metrics of HealthCrypt merit additional discussion. Rasheed and Kumar [19] provided ample security against differential attacks for chaotic-map based constructions but since their work is solely an image encryption scheme lacking hardware evaluation, it cannot be compared using gate equivalents or RAM. Furthermore, deployment in a clinical sensor environment has not been validated. Sabri et al. [20] provide evidence via extensive literature survey that there does not exist a single lightweight cipher that can offer authenticated encryption, under 2,000 GE in hardware, and possess statistically closest to ideal security parameters all in one scheme. HealthCrypt offers this property. Karunkuzhali et al. [21] introduced HLCA-ABE to enable flexible data access policies that change dynamically. However, this scheme is not viable in deeply embedded devices as hardware area was an issue and exceeds 2,000 GE. HECS4MQTT [22] provides security between edge and cloud, but does not utilize an authenticated encryption primitive at the sensor node itself that was purpose built, nor was there any formal security evaluation using FELICS. HealthCrypt remedies all these shortcomings by providing an authenticated encryption scheme that is natively supported and optimized, has an area of under 2,000 GE, occupies

90 bytes of RAM, AND possesses statistically closest to ideal parameters all in one purpose-built IoT-ready scheme with the highest IoT Healthcare Suitability Score of 79.23, as shown in Table 1.

Finally, we note that recently standardized lightweight AE schemes, in particular Ascon (NIST SP 800-232, 2025) [11], are not part of the quantitative FELICS-based comparison provided in this paper. Ascon, as the leading NIST lightweight AEAD standard, is an obvious and relevant choice of benchmark. We strongly encourage the authors to include Ascon and the other finalists of the NIST Lightweight Cryptography process in their comparative evaluation in the revised manuscript to provide a complete picture of where HealthCrypt stands in comparison to the present-day landscape of standardized lightweight AE.

Table 1. Comparison of HealthCrypt with Related Works.

Criterion	HealthCrypt	Rasheed & Kumar [19]	Sabri et al. [20]	HLCA-ABE [21]	HECS4MQTT [22]
Native AE Support	✓	✗	✗	✗	Partial
Sub-2000 GE Compliant	✓	N/A	N/A	✗	N/A
RAM Footprint (bytes)	90	N/A	N/A	>1000	N/A
FELICS Benchmarked	✓	✗	✗	✗	✗
Avalanche Effect	0.5026	Not reported	Not reported	Not reported	Not reported
Shannon Entropy Deficit	0.0094	Not reported	Not reported	Not reported	Not reported
Healthcare IoT Targeted	✓	✓	✓	✓	✓
IoT Suitability Score	79.23	N/A	N/A	N/A	N/A

5. Conclusions

In this work we introduced HealthCrypt, a lightweight authenticated encryption protocol designed specifically with the multiple security and hardware restrictions present in IoT devices for smart health applications in mind. When we evaluated HealthCrypt along with PRESENT-80, SPECK-64/128 and SIMON-64/128 using the industry benchmark FELICS implemented on ARM Cortex-M0, HealthCrypt outperformed the competition in several categories without any one cipher outperforming it in all categories. The key advantages of HealthCrypt include: (1) HealthCrypt has a native single-pass AE design that avoids the required 2-pass MAC computation overhead. This provides HealthCrypt with 48.4% fewer cycles than PRESENT-80 when operating in AE mode, which is directly applicable to clinical data. (2) Compared to other 20-round SPNs, the HealthCrypt construction has achieved the highest avalanche effect of 0.5026 and lowest Shannon entropy loss of 0.0094 bits/byte. This implies that HealthCrypt has good statistical security properties, which helps protect against attacks that exploit repetitive patterns in biomedical signals. (3) HealthCrypt meets the stringent requirement of being under 2,000 GE while only using 1,620GE and has an ultra-small 90-byte RAM footprint. This allows HealthCrypt to be implemented even on the smallest resource-constrained implantable/wearable clinical sensor devices. (4) Overall IoT Healthcare Suitability Score allows future lightweight cipher submissions to be compared to HealthCrypt along many key clinical IoT metrics. This provides a reusable metric for lightweight cipher evaluation against IoT healthcare deployment needs. Future improvements can be made to HealthCrypt's plaintext-ciphertext correlation characteristics and formal security proofs can be expanded to include AEAD.

All the Declarations and Statements

Author Contributions Statement

Osamah Tahseen Rayshan is the sole author and contributed to all aspects of this work, including conceptualization, methodology, software implementation, formal analysis, investigation, data curation, writing—original draft preparation, writing—review and editing, visualization, and project administration.

Conflict of Interest Statement

The author declares no conflicts of interest.

Funding Declaration

This research received no external funding.

Data Availability Statement
Data will be made available on request.

Ethical Declarations
This work does not involve any research on human participants or animals.

Acknowledgments
The author sincerely acknowledges the experts for their professional evaluation and valuable recommendations, which have contributed to improving the quality of the experiment and the reliability of its results.

Declaration of Generative AI in Scholarly Writing
The author confirms that no generative AI tools or AI-assisted technologies were used in the preparation, writing, or revision of this manuscript. All work was performed solely by the human author without any automated assistance.

Abbreviations
The following abbreviations are used in this manuscript:

AE - Authenticated Encryption
AEAD - Authenticated Encryption with Associated Data
AES - Advanced Encryption Standard
ARX - Addition-Rotation-XOR
ARM - Advanced RISC Machine
ASIC - Application-Specific Integrated Circuit
CPU - Central Processing Unit
DMA - Direct Memory Access
ECG - Electrocardiogram
ECC - Elliptic Curve Cryptography
FELICS - Fair Evaluation of Lightweight Cryptographic Systems
FPGA - Field-Programmable Gate Array
GE - Gate Equivalents
GCC - GNU Compiler Collection
HC - HealthCrypt
HECS4MQTT - Healthcare Security for MQTT
HIPAA - Health Insurance Portability and Accountability Act
HLCA-ABE - Hybrid Lightweight Ciphertext-Policy Attribute-Based Encryption
HMAC - Hash-Based Message Authentication Code
IEEE - Institute of Electrical and Electronics Engineers
IHSS - IoT Healthcare Suitability Score
IND-CPA - Indistinguishability under Chosen-Plaintext Attack
IoT - Internet of Things
LFSR - Linear Feedback Shift Register
MAC - Message Authentication Code
MQTT - Message Queuing Telemetry Transport
NFC - Near-Field Communication
NIST - National Institute of Standards and Technology
NPCR - Number of Pixels Change Rate
PVT - Process-Voltage-Temperature
RAM - Random Access Memory
RFID - Radio Frequency Identification
ROM - Read-Only Memory
RSA - Rivest-Shamir-Adleman
SPN - Substitution-Permutation Network
SRAM - Static Random Access Memory
TLS - Transport Layer Security
UACI - Unified Average Changing Intensity
WBAN - Wireless Body Area Network
XOR - Exclusive OR

Appendix
N/A.

References

[1] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Generation Computer Systems*, vol. 129, pp. 77-89, 2022/04/01/ 2022, doi: 10.1016/j.future.2021.11.011.

[2] Amrita, C. P. Ekwueme, I. H. Adam, and A. Dwivedi, "Lightweight Cryptography for Internet of Things: A Review," *EAI Endorsed Transactions on Internet of Things*, vol. 10, 2024/3// 2024, doi: 10.4108/eetiot.5565.

[3] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," *IEEE Access*, vol. 9, pp. 28177-28193, 2021, doi: 10.1109/ACCESS.2021.3052867.

[4] A. Bogdanov *et al.*, "PRESENT: An Ultra-Lightweight Block Cipher," in *Cryptographic Hardware and Embedded Systems - CHES 2007*, Berlin, Heidelberg, P. Paillier and I. Verbauwhede, Eds., 2007// 2007: Springer Berlin Heidelberg, pp. 450-466.

[5] T. Chinbat, S. Madanian, D. Airehrour, and F. Hassandoust, "Machine learning cryptography methods for IoT in healthcare," (in eng), *BMC Med Inform Decis Mak*, vol. 24, no. 1, p. 153, Jun 4 2024, doi: 10.1186/s12911-024-02548-6.

[6] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "SIMON and SPECK: Block Ciphers for the Internet of Things," *Cryptography ePrint Archive*, vol. 2015/585, 2015. [Online]. Available: https://eprint.iacr.org/2015/585.

[7] I. W. Damaj, H. Al-Mubasher, and M. Saadeh, "An extended analytical framework for heterogeneous implementations of light cryptographic algorithms," *Future Generation Computer Systems*, vol. 141, pp. 154-172, 2023/04/01/ 2023, doi: 10.1016/j.future.2022.11.007.

[8] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2: Lightweight Authenticated Encryption and Hashing," *Journal of Cryptology*, vol. 34, no. 3, p. 33, 2021/06/22 2021, doi: 10.1007/s00145-021-09398-9.

[9] S. N. Tran, V. T. Hoang, and D. H. Bui, "A Hardware Architecture of NIST Lightweight Cryptography Applied in IPSec to Secure High-Throughput Low-Latency IoT Networks," *IEEE Access*, vol. 11, pp. 89240-89248, 2023, doi: 10.1109/ACCESS.2023.3306420.

[10] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of internet of things based on cryptographic algorithms: a survey," *Wireless Networks*, vol. 27, no. 2, pp. 1515-1555, 2021/02/01 2021, doi: 10.1007/s11276-020-02535-5.

[11] M. S. Turan, K. A. McKay, D. Chang, J. Kang, and J. Kelsey, "Ascon-based lightweight cryptography standards for constrained devices," National Institute of Standards and Technology (NIST), NIST SP 800-232, 2025/8// 2025. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/232/final

[12] M. El-hajj, H. Mousawi, and A. Fadlallah, "Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform," *Future Internet*, vol. 15, no. 2, p. 54, 2023, doi: 10.3390/fi15020054.

[13] M. Rana, Q. Mamun, and R. Islam, "A block cipher for resource-constrained IoT devices," *International Scholarly and Scientific Research & Innovation*, vol. 17, no. 3, pp. 266–271, 2023.

[14] I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight Cryptography for Internet of Insecure Things: A Survey," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 7-9 Jan. 2019 2019, pp. 0475-0481, doi: 10.1109/CCWC.2019.8666557.

[15] F. Masood *et al.*, "A new color image encryption technique using DNA computing and Chaos-based substitution box," *Soft Computing*, vol. 26, no. 16, pp. 7461-7477, 2022/08/01 2022, doi: 10.1007/s00500-021-06459-w.

[16] A. Sevin and A. A. O. Mohammed, "A survey on software implementation of lightweight block ciphers for IoT devices," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 3, pp. 1801-1815, 2023/03/01 2023, doi: 10.1007/s12652-021-03395-3.

[17] M. Jangra, S. Gupta, and B. Singh, "Critical Evaluation of SIMON and SPECK BLOCK Cipher for Different Modes of Operation," in *Advanced Communication and Intelligent Systems*, Cham, R. N. Shaw, M. Paprzycki, and A. Ghosh, Eds., 2023// 2023: Springer Nature Switzerland, pp. 205-213.

[18] F. Dridi, S. El Assad, W. El Hadj Youssef, M. Machhout, and R. Lozi, "The Design and FPGA-Based Implementation of a Stream Cipher Based on a Secure Chaotic Generator," *Applied Sciences*, vol. 11, no. 2, p. 625, 2021, doi: 10.3390/app11020625.

[19] A. M. Rasheed and R. M. S. Kumar, "Efficient lightweight cryptographic solutions for enhancing data security in healthcare systems based on IoT," (in English), *Frontiers in Computer Science*, Original Research vol. Volume 7 - 2025, 2025-April-04 2025, doi: 10.3389/fcomp.2025.1522184.

[20] O. Sabri, B. Al-Shargabi, A. Abuarqoub, and T. A. Hakami, "A Lightweight Encryption Method for IoT-Based Healthcare Applications: A Review and Future Prospects," *IoT*, vol. 6, no. 2, p. 23, 2025, doi: 10.3390/iot6020023.

[21] D. Karunkuzhali, A. A. Shaikh, R. Suguna, and M. Venkatesan, "Hybrid Lightweight Cryptography with Attribute-Based Encryption for Secure Health Monitoring in IOT-Wireless Body Area Sensor Network," *Biomedical Materials & Devices*, vol. 4, no. 2, pp. 2466-2482, 2026, doi: 10.1007/s44174-025-00402-5.

[22] S. Alharbi, W. Awad, and D. Bell, "HECS4MQTT: A Multi-Layer Security Framework for Lightweight and Robust Encryption in Healthcare IoT Communications," *Future Internet*, vol. 17, no. 7, p. 298, 2025, doi: 10.3390/fi17070298.

Authors' Profiles



Osamah Tahseen Rayshan is holds a M.Sc. degree in computer science at University of information technology and communications, Baghdad, Iraq.

How to cite this paper

Osamah Tahseen Rayshan, "Lightweight Cryptographic Protocol for Resource-Constrained IoT Devices in Smart Healthcare", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.18, No.5, pp. 182-197, 2026. DOI:10.5815/ijieeb.2026.05.11