面向医疗物联网的轻量级多层密码框架设计与验证

欧阳毅
赣南科技学院 信息工程学院，江西 赣州 341000
DOI: 10.61369/TACS.2026060035

摘　　要： 可穿戴传感器、植入式监护仪与远程监测平台等医疗 IoT 终端的规模化接入，使密码方案不得不在强安全与严苛资源约束之间寻找新的折中。AES-256 与 RSA-2048 在此类场景下并不适用——其计算开销、内存占用与功耗均超出受限节点所能承受的范围。基于此，本文构建了一种面向医疗 IoT 的多层轻量级密码框架，由优化 PRESENT-80 分组密码、ASCON-128 认证加密、CP-ABE 访问控制与 ECDH 密钥交换四层组件构成，覆盖机密性、完整性、属性化访问控制与会话密钥协商。基于 PhysioNet 真实生理数据的 Python 仿真实验显示：完整加解密流水线平均延迟分别为 202.95 μs 与 202.40 μs，可满足低延迟医疗 IoT 场景的部署需求。

关 键 词： 医疗 IoT；IoT 安全；轻量级加密；资源受限设备

Design and Verification of a Lightweight Multi-layer Cryptographic Framework for Medical Internet of Things

Ouyang Yi
School of Information Engineering, Gannan University of Science and Technology, Ganzhou, Jiangxi 341000

Abstract: The large-scale deployment of medical IoT endpoints—wearable sensors, implantable monitors, and remote monitoring platforms—forces cryptographic design to negotiate a new trade-off between strong security and severe resource constraints.AES-256 and RSA-2048 are ill-suited to such settings, as their computational overhead, memory footprint, and power draw exceed what constrained nodes can sustain.To this end, this paper builds a multi-layer lightweight cryptographic framework for medical IoT, composed of an optimized PRESENT-80 block cipher, ASCON-128 authenticated encryption, CP-ABE access control, and ECDH key exchange, covering confidentiality, integrity, attribute-based access control, and session-key agreement.Python-based simulations on real physiological data from PhysioNet show that the average end-to-end encryption and decryption latencies of the proposed pipeline are 202.95 μs and 202.40 μs, respectively, meeting the deployment requirements of latency-sensitive medical IoT scenarios.

Keywords: medical IoT; IoT security; lightweight cryptography; resource-constrained devices

引言

医疗 IoT 正在改写临床数据的产生与流转方式。可穿戴及植入式终端持续采集生理信号，并经由无线链路接入医院信息系统。据预测，至2030年全球医疗 IoT 市场规模将突破千亿美元量级，受保护健康信息（PHI）的产生节点也随之指数级增长[1]。然而，规模红利的背面是攻击面的同步扩张。RSA-2048 与 AES-256 在受限 MCU 上的硬件门数、能耗与栈占用均难以接受，致使大量在网终端要么“裸跑”，要么仅依赖 TLS 一层防护——前者完全失守，后者无法覆盖静态数据保护与细粒度授权两个关键环节。围绕这一矛盾，轻量级密码（lightweight cryptography）逐步形成独立分支。NIST 在2023年完成轻量级认证加密标准化，将 ASCON 选为获胜者；PRESENT-80则更早被纳入 ISO/IEC 29192-2:2012[2]。值得注意的是，标准化进展与工程落地之间仍存在断层：现有研究多停留在单一原语层面的优化，将多种轻量级原语组合成统一框架、并以真实医疗负载加以系统验证的工作并不多见。本文正是针对这一断层展开。

具体而言，本文的工作可概括为以下三点。

(1) 设计并实现一个由四种互补密码组成的多层轻量级安全框架，覆盖加密、认证、访问控制与密钥协商；

(2) 基于纳秒级高精度计时器对医疗数据集进行全面的基准测试；

(3) 给出该框架在医疗 IoT 中的可部署性证据，并指出其代价对称性带来的工程意义。

一、相关工作与研究现状

传统密码原语与受限 IoT 硬件之间的不兼容已被反复印证。Ansari 等 [3] 以77篇同行评议文献为样本作系统综述，指出 RSA 与 AES-256在计算、内存与能耗三个维度均越过了轻量级硬件的边界；基于公钥基础设施的协议尤其受限，单次握手即可耗尽小型节点的能量预算。Kumar 等 [4] 为边缘 IoT 提出降轮 L-AES 与 ECC 的组合方案，将传统密码“瘦身”以适配资源受限场景。Goyal 等 [5] 在 UMC-90 nm 标准单元库上对 PRESENT、AES、ECDH、DH、RSA 五种算法作硬件实现并量化对比，结果显示 PRESENT 在面积与功耗上明显占优；PRESENT-128的时间复杂度约为 AES 的两倍，但仍是超资源受限节点的首选。

医疗场景下的算法选型同样有据可循。Sabri 等 [6] 在综述中梳理 了 AES-128、LEA、ASCON、GIFT、HIGHT、PRINCE 和 RC5 的性能，覆盖分组与密钥长度、加解密速度、吞吐与安全等级等维度。其结论可概括为两层：在带硬件加速的高敏感场景，AES-128、LEA、ASCON、GIFT 较为合适；中等敏感度的应用则可选 HIGHT 或 PRINCE。该工作同时提示，效率、安全性与资源消耗三者之间不存在“全能”的解，选型必须回到具体场景。需要补充的是，上述文献多以单算法基准为主，并未触及“多层组合”这一工程问题，这也是本文区别于既有工作的入手点。

二、轻量级密码框架设计

（一）框架设计目标与约束准则

结合文献 [3][5][6] 所归纳的医疗 IoT 约束，本框架确立四项核心设计原则：

(1) 最小内存占用：所有持久化数据结构须控制在64KB RAM 以内；

(2) 亚毫秒延迟：单次传感器读值的加解密须在1 ms 内完成，以避免影响典型医疗采样率下的实时生理监测；

(3) 多层安全保障：须同时提供机密性、完整性、身份认证和细粒度访问控制；

(4) 纵深防御：任意单一密码层被攻破均不应直接导致明文泄露。

（二）四层密码组件的协同架构

框架按数据流方向串联四个密码层。

1. PRESENT-80分组密码

原始传感器数据首先经 PRESENT-80加密。PRESENT-80是一种31轮替代 - 置换网络（SPN）结构的分组密码，分组长度为64 bit，密钥长度为80 bit。该算法已被纳入 ISO/IEC 29192-2:2012，硬件实现仅需约1570 GE[5]。

本实现引入四项关键优化：

（1）以 LRU 缓存策略保存轮密钥，复用相同主密钥下的扩展结果；

（2）向量化 S 盒代换层，以按位或操作累积半字节级置换结果，规避逐元素循环造成的对象分配开销；

（3）预计算256项的字节级 P 盒查找表 (LUT)，将原本64次比特迭代置换压缩为8次查表；

（4）预计算逆 S 盒 [7]，以 O(1) 数组索引替代原 O(n) 线性搜索。

2.ASCON-128认证加密

PRESENT 密文进入第二层。ASCON-128是 NIST 于2023年选定的轻量级认证加密标准，采用双工海绵（duplex sponge）结构，内部状态320 bit（5 个64 bit 字），可在单次扫描内同时提供机密性与完整性保护 [8]。本实现突破了原型仅支持8字节定长明文的限制，按 ISO/IEC 7816-4规则填充以处理任意长度负载；128 bit 标签与密文一并外发，解密侧据此判定数据是否被篡改。

3.CP-ABE 访问控制

第三层将 ASCON 密文包封装于 CP-ABE 之内。访问策略以 role 与 department 两个属性的 AND 合取式表示，并在 CP-ABE 对象实例化时一次性解析并缓存，避免每次解密重复执行字符串切分。该层强制仅当用户属性与策略完全匹配时（如某科室的授权医生）方能解封数据，对应到 HIPAA 法规即“最小必要”原则 [9]。

4.ECC 会话密钥交换与密钥管理

第四层承担会话密钥协商与主密钥维护。PRESENT-80所需的80 bit 会话密钥由 brainpoolP256r1椭圆曲线上的 ECDH 协商生成 [10]：双方计算共享秘密点后，对其 x 坐标作 SHA3-256哈希，截取前10字节即得80 bit 密钥。考虑到 ECC 标量乘是整个流水线中最昂贵的运算，本实现按对端公钥缓存其结果，重复会话不再付出二次代价。框架同时集成轻量级密钥管理模块，每隔3600 s 通过 os.urandom() 刷新主密钥，以为长期会话密钥派生提供前向安全。

三、软件实现与性能优化

（一）面向受限节点的软件级优化策略

本框架在各组件中核心优化如下：

(1) 轮密钥缓存

PRESENT 密钥扩展从80 bit 主密钥派生32个轮密钥，依次执行32次位旋转、S 盒代换与 XOR。引入 functools.lru_cache 后，每个唯一密钥的扩展过程仅计算一次。会话密钥相对稳定的医疗 IoT 典型负载下，后续调用降为 O(1) 字典查找，扩展开销几乎归零。

(2)LUT 加速 P 盒

PRESENT 置换层将64个输入比特映射至特定输出位置。基础实现每轮需迭代处理64个比特，31轮共计1984次比特级操作。本文优化方案预先构建字节级 P 盒查找表（LUT）：对8个字节位置的每一个，分别构造一张含256项的表，记录该字节所有可能取值对输出64 bit 字的贡献。运行时，置换过程被简化为8次查表与按位或运算，置换开销显著下降。

PRESENT 置换层将64个输入比特映射至特定输出位置，实现每轮64次比特操作、31轮共1984次。本文按字节粒度预构建 P 盒 LUT：对8个字节位置各建一张含256项的表，记录该字节所有取值对64 bit 输出字的贡献。运行时，置换被压缩为8次查表与

按位或，开销显著下降。

(3) 常数时间逆 S 盒

原始 PRESENT 解密通过 list.index 查找逆 S 盒值，每个半字节需 O(16) 线性扫描，每轮16次、31轮共计7936次扫描。改用预计算的 INV_SBOX 查找数组后，每次查找复杂度降至 O(1)，且不改变算法的安全属性。

(4) 流式 ASCON

原始 ASCON 实现仅处理恰好8字节的明文。本文实现支持任意长度数据，并采用 ISO/IEC 7816-4 填充方案，规避应用层分段引入的额外往返开销。

（二）实验数据集

基准测试使用 PhysioNet 公开的 BIDMC PPG and Respiration Dataset。该数据集包含 PPG、ECG 与阻抗呼吸波形（采样率 125 Hz）、心率 / 呼吸率 /SpO_2 等数值生命体征（采样率 1 Hz），以及专家标注的呼吸标记。为贴近商用医疗 IoT 终端的传输粒度，本文从中选取一位患者的三个 CSV 文件作为测试输入，将每条记录编码为定长 ASCII 串，不足8字节者以零填充，最终形成 8 字节二进制载荷。这一长度恰好落在商用医疗 IoT 设备每次采样4至16 字节的典型测量帧区间内。

四、实验评估与结果分析

实验在同一台计算机上完成，操作系统 Ubuntu 24（Linux），Python 3.12。计时采用 time.perf_counter_ns()，该单调时钟提供纳秒级时间戳且不受系统时钟调整影响，是 Python 内置精度最高的计时器。各组件正式测量前均经过缓存预热，随后以 N=1000 次迭代取均值。各组件实测结果见表 1。三点观察值得记录：其一，软件实现下 ASCON-128加密快于 PRESENT-80（95.03 μs vs 109.66 μs），与海绵结构的字级运算亲和性相符——PRESENT 多达 31 轮的位级置换在 Python 解释执行下放大了开销。其二，CP-ABE 策略层的额外开销几乎可忽略（加密 0.59 μs，解密 1.10 μs）。这一结果并非偶然，而是源于策略已在对象构造阶段被预解析并缓存，运行时仅余字典查找。其三，完整流水线的加解密耗时高度对称（202.95 μs vs 202.40 μs）。这一对称性看似工程细节，但对电池供电的医疗 IoT 设备而言并非小事。长期运行中，单向操作主导的方案会造成续航的系统性偏置，而对称代价意味着可预测的功耗模型。需要指出的是，上述数据由 Python 实现得出，其绝对量级会被解释执行成本放大；移植至 C 后，时间应进一步下降一个数量级以上。但在算法间的相对关系层面，本节结论仍具参考价值。

表1 框架各组件实测执行时间（单位：μs)

算法	操作	平均耗时（单位：μs)
PRESENT-80	加密	109.66
PRESENT-80	解密	214.69
ASCON-128	加密	95.03
ASCON-128	解密	187.73
CP-ABE	加密	0.59
CP-ABE	解密	1.10
本文算法	加密	202.95
本文算法	解密	202.40

五、结论与展望

本文将 LUT 优化的 PRESENT-80、流式 ASCON-128、CP-ABE 与 ECDH 组合为一条面向医疗 IoT 的多层加密流水线，并在 PhysioNet 真实生理数据上完成了基准评估，端到端延迟约 202.95 μs。结果支持一个相对克制的结论：在受限 MCU 上构建多层防护并非必然以延迟为代价，前提是各层原语经过有针对性的工程优化。仍有若干工作未尽。其一，框架尚未引入抗量子密码，面对未来 CRQC 威胁需要在 PRESENT-80与 ECDH 两层做替换性研究；其二，本文的延迟数据来自 Python 仿真，跨平台尤其是 Cortex-M0/M4 等典型医疗 MCU 上的真实功耗与时序仍需实测；其三，CP-ABE 策略目前仅覆盖 role 与 department 一种合取式，更复杂的访问树及撤销机制留待后续研究。

参考文献

[1] Zarkia, M. N. H., & Usman, S. (2025). IoT Data Breaches and Privacy Issues in Healthcare System. Open International Journal of Informatics, 13(1), 41 - 55. https://doi.org/10.11113/oiji2025.13n1.327

[2] Gui B , Anton A A , Stngaciu C S ,et al.Securing IoT edge: a survey on lightweight cryptography, anonymous routing and communication protocol enhancements[J]. International Journal of Information Security, 2025, 24(3).DOI:10.1007/s10207-025-01071-7.

[3] Ansari S A, Ali S. A systematic review of lightweight cryptographic schemes for security and privacy in IoT[J]. Discover Computing, 2025, 28(1): 266.

[4] Kumar,Dingari.(2024).Lightweight Cryptographic Framework for Securing IoT Devices in Edge Environments.Journal of Information Systems Engineering and Management.9.199-208. 10.52783/jisem.v9i4s.11158.

[5] Goyal T K , Sahula V , Kumawat D .Energy Efficient Lightweight Cryptography Algorithms for IoT Devices[J].IETE Journal of Research, 2019:1-14.DOI:10.1080/03772063.2019.1670103.

[6] Sabri, O.; Al-Shargabi, B.; Abuarqoub, A.; Hakami, T.A. A Lightweight Encryption Method for IoT-Based Healthcare Applications: A Review and Future Prospects. IoT 2025, 6, 23. https://doi.org/10.3390/iot6020023

[7] Rana, M.; Mamun, Q.; Islam, R. P-Box Design in Lightweight Block Ciphers: Leveraging Nonlinear Feedback Shift Registers. InProceedings of the 2024 IEEE Wireless Communications and Networking Conference (WCNC), Dubai, United Arab Emirates,21-24 April 2024; pp. 1-8.

[8] Dobraunig C, Eichlseder M, Mendel F, et al. Ascon v1. 2: Lightweight authenticated encryption and hashing[J]. Journal of Cryptology, 2021, 34(3): 33.

[9] Zhang Y, Geng H, Su L, et al. A traceable and multi-authority CP-ABE scheme for IoT medical devices[J]. Computer Networks, 2025: 111754.

[10] Kumbhakar D, Adhikari S, Karforma S. CTEA: Chaos based tiny encryption algorithm using ECDH and TinkerBell map for data security in supply chain management[J]. Multimedia Tools and Applications, 2025, 84(13): 12371-12394

