抗侧信道攻击对称算法的逐比特分析与功耗均衡防护

何乐生[1,2]，靳亚灿[1]，张孝蔚[1]，晋兵[1]
（1. 云南大学信息学院，云南 昆明 650091；2. 云南省高校物联网技术及应用重点实验室，云南 昆明 650091）

摘　要：物联网设备因计算与存储资源受限，数据安全需依赖轻量级加密算法，且只能工作在开放环境中，易受到侧信道攻击。为抵御该威胁，新一代的NIST轻量级加密算法ASCON采用了比特切片结构。针对比特切片结构，提出了一种高效的逐比特CPA攻击方法，通过密钥降维分解策略，使理论攻击复杂度降低至字节切片结构的$\frac{1}{2\,048}$，揭示了该新型结构存在的安全风险。为应对此攻击，进一步提出了功耗均衡S盒防御方案，通过恒定S盒操作的功耗来消除信息泄漏，实现了对逐比特攻击的有效防护。通过采用攻防协同的研究方法，验证了ASCON算法在逐比特攻击下的脆弱性，为物联网环境下ASCON算法的安全实现与攻击防护提供了实证参考。

关键词：物联网安全；抗侧信道攻击；逐比特攻击；ASCON算法
中图分类号：TP393.0
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025245

Bit-oriented analysis and power-equilibrated countermeasures for side-channel resistant symmetric cryptography

HE Lesheng[1,2], JIN Yacan[1], ZHANG Xiaowei[1], JIN Bing[1]
1. College of Information, Yunnan University, Kunming 650091, China
2. University Key Laboratory of Internet of Things Technology and Application of Yunnan Province, Kunming 650091, China

Abstract: Due to the limited computational and storage resources of Internet of things（IoT）devices, data security relies on lightweight cryptographic algorithms. However, since these devices are often operated in open environments, they are highly vulnerable to side-channel attacks. To resist such threats, the new National Institute of Standards and Technology (NIST) lightweight cryptography standard ASCON adopted a bit-sliced structure. Targeting this structure, an efficient bit-wise correlation power analysis (CPA) attack was proposed . By introducing a key dimension-reduction decomposition strategy, the theoretical attack complexity was reduced by $\frac{1}{2\,048}$ of the byte slice structure, thereby revealing potential security risks in this novel design. To counteract this attack, a power-equilibrated S-box defense scheme was proposed , which eliminated information leakage by ensuring constant power consumption in S-box operations, thus providing effective protection against bitwise attacks. Through an attack-defense co-design methodology, this work demonstrates the vulnerability of the ASCON algorithm under bitwise attacks and provides an empirical reference for the secure implementation and attack protection of the ASCON algorithm in the Internet of things environment.

Keywords: Internet of things security, Side-channel resistance, bitwise attack, ASCON algorithm

收稿日期：2025–10–23；修回日期：2025–12–08
通信作者：何乐生，31799693@qq.com
基金项目：国家自然科学基金资助项目（No.U1631121）
Foundation Item：The National Natural Science Foundation of China (No.U1631121)

0 引言

当今，在5G通信、嵌入式与云计算等前沿技术迅猛发展的推动下，物联网（IoT，Internet of things）技术已实现跨领域深度融合，全面赋能智能家居、智能交通以及智慧医疗等应用场景，改善了社会民生体验[1]。与此同时，智慧农业、工业物联网和智能电网等创新应用正持续重构传统产业模式，为生产力提升注入新动能。值得注意的是，这种爆发式发展也伴随着日益凸显的安全隐患[2]。当前物联网终端承载着个人生物特征、企业核心数据等敏感信息，在安全防护机制不完善的情况下，极易遭受数据窃取和身份冒用等多维度安全威胁[3-5]。物联网安全事关国家数字经济与公民信息权益，构建安全防护体系是数字基建的关键。

物联网设备部署广泛，同时物联网设备计算能力和存储空间有限，对于传统加密算法来讲，它们具有复杂的计算过程，需要更多的计算资源以及存储空间，导致物联网设备应用困难。为此，研究者提出了一系列轻量级加密算法，这类算法专用于资源受限的物联网设备，不仅可以降低功耗和内存占用，而且可以保证自身的安全性[6]。超轻量级分组密码（PRESENT）[7]、椭圆加密算法（ECC，elliptic curve cryptography）[8]与Chacha20[9]等轻量级加密算法，已广泛应用在物联网设备中。它们可以在资源受限的环境中运行，同时保证数据的安全性和机密性。将轻量级加密算法应用在物联网设备中，是目前确保物联网设备安全的主流方法[10-13]。

物联网设备安全面临诸多威胁。在众多攻击手段中，侧信道攻击（SCA，side-channel attack）是针对资源受限设备的重大安全隐患[14]。这类攻击利用设备在使用中产生的物理信息，窃取设备的加密密钥或其他敏感信息，这些信息看似无害，但攻击者可以通过分析这些信息，推断出设备内部的信息，威胁物联网设备安全。当前轻量级加密算法对侧信道攻击的防御能力有待加强，学术界应开展更深入的安全性评估与研究，提高算法的抗侧信道攻击能力，建立针对物联网场景的动态防护机制，从而确保这些算法在真实复杂的物联网环境中能够提供可靠的安全保障，维护系统的长期稳定运行。

为分析现有轻量级加密算法可能存在的安全威胁，本文选择ASCON算法作为研究对象，进行侧信道攻击。ASCON算法由奥地利格拉茨技术大学的团队设计[15]，本文只对ASCON-128（简称ASCON）展开讨论。该算法包含初始化、关联数据、明文/密文处理及终止化4个部分，这4个部分都包含核心单元全排列（permutation）过程，下文简称P过程。该算法已广泛应用于智能家居终端、工业传感器节点、可穿戴医疗设备等低功耗场景。同时，ASCON算法已入选NIST轻量级密码标准，其128 bit的安全强度和优秀的性能表现，能够在不增加硬件负担的前提下，为物联网终端设备提供安全保障。

为验证ASCON算法抵御侧信道攻击的能力，若干工作已对其展开评估和验证。文献[16]通过差分功耗分析（DPA，differential power analysis）的攻击方式，在采集到50 000条功耗曲线时，对前64 bit密钥攻击成功概率接近1，但是缺乏对真实硬件实现的深入评估，且未考虑任何防护措施，这使其结论的普适性受限，未能反映ASCON在带有防护的实际应用中的安全水平。文献[17]从理论层面分析了7轮置换的安全性，提出了一种能够在2^{123}次计算内恢复128 bit密钥的技术，虽然可以成功恢复初始密钥，但是时间成本太高，这决定了该方法在当前计算能力下尚不具备实用性，不构成现实威胁。文献[18]采用Cube攻击的思路，成功实现5~7轮算法的密钥恢复。此类攻击的根本局限性在于，其所依赖的数学结构会被标准算法的完整12轮设计彻底破坏；因此，攻击对实际使用的标准算法完全无效，所以其结论无法直接用于评估标准算法的安全性。文献[19]在随机数滥用的情况下，利用相关功耗分析（CPA）成功恢复了密钥的前64 bit；然而其攻击模型依赖于“随机数重用”这一特定的、协议设计中应极力避免的场景，这表明评估的是不安全实现所带来的风险，而非算法在规范使用下的内在鲁棒性。因此，学术界当前缺乏在标准、规范的操作条件下，实现对ASCON算法硬件发起高效且彻底的侧信道攻击能力的系统性评估，而这正是本文工作的切入点。

本文的主要工作如下。

1) 深入分析ASCON算法的比特切片结构，提出了一种逐比特侧信道攻击方法。该方法通过对攻击目标进行降维分解，将密钥猜测从字节级细化至比特级，显著降低了理论攻击复杂度，提升了密钥破解效率。

2) 针对该攻击所依赖的瞬态物理泄漏特性，设计了一种目标导向的有限冲激响应（FIR，finite impulse response）带通滤波器。该预处理方案通过精确匹配泄漏信号的频谱，实现了信噪比的最大化，为高效攻击提供了高质量的输入。

3) 为抵御高效威胁，本文提出了一种算法层面的功耗均衡S盒防御方案。该防御策略以极小的性能开销，换取了攻击成本数个数量级的提升。这证明了该攻防协同方案的有效性，为保障物联网设备安全提供了具有参考价值的解决方案。

1　针对物联网设备的逐比特攻击方案设计

ASCON算法在设计时，因其采用了有利于硬件实现和掩码防护的比特切片结构，其核心的置换操作被分解为一系列独立的比特运算；然而这一设计也为侧信道攻击提供了独特的切入点，尽管每次比特运算产生的功耗或电磁泄漏极其微弱，但这种泄漏与特定的密钥比特和中间值存在着稳定的、可观测的统计相关性，这正是构筑CPA攻击的理论基石。对于ASCON这类采用比特切片技术的算法，运算的本质是将字节内的8 bit分散到不同的逻辑单元进行并行的比特运算。若采用逐字节攻击方式，就错误地假设8 bit的功耗是作为一个整体泄漏的。相反，本文设计的逐比特攻击直接针对单比特的运算进行建模，它与物理实现的操作是同构的。因此，逐比特攻击是针对此类密码最高效、最匹配的攻击方案。

1.1　逐比特攻击方案

本文方案的设计核心，是基于CPA方法，将ASCON算法S盒的攻击从字节维度彻底分解至比特维度。这一策略的理论依据，源于ASCON算法S盒独特的比特切片设计。不同攻击模型的S盒计算分解如图1所示。图1中，将320 bit的输入数据分为5个64 bit的数据，送入整个S盒进行运算，输出时重新组成320 bit的输出。两者在攻击时，都是采取分段攻击，先攻击前64 bit，再攻击后64 bit。逐字节攻击，是将64 bit分为8 B的计算单元，攻击者需在拥有256个可能值的空间中进行攻击。本文的逐比特攻击将64 bit密钥彻底分解为64个独立的比特数，攻击的计算单元是单比特数，攻击者的假设空间缩小到仅有2个可能值，之后将之前猜测的密钥加入新一轮的猜测中。

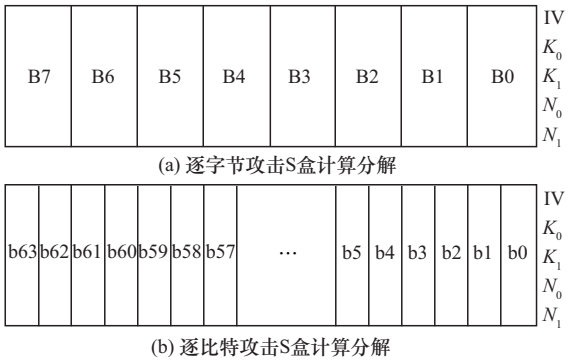


图1　不同攻击模型的S盒计算分解

为从物理层面探究逐比特攻击的内在机理，需进一步分析其泄漏源的物理特性。信噪比（SNR， signal-to-noise ratio）是量化在特定时间点上，与特定数据相关的功耗信号强度的关键指标。各中间值比特信噪比分析如图2所示。

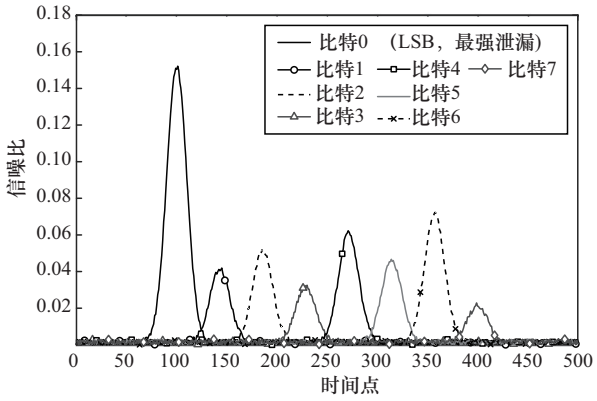


图2　各中间值比特信噪比分析

其中，S盒输出的8 bit，均存在可观测的SNR峰值，证实了逐比特泄漏是普遍存在的，但每个比特的泄漏强度差异显著。例如比特0的泄漏远高于其他比特位，是最薄弱的攻击点。尽管其他比特的泄漏较弱，但它们依然包含了与密钥相关的有效信息。这一物理层面的分析，为后续攻击策略的选择与优化提供了关键的理论依据。

逐字节攻击与逐比特攻击在搜索空间构造上存在本质区别。由图1可知，在S盒计算阶段，将16 B密钥分为前后各8 B，即图中的K_0与K_1。因此，攻击时进行分段攻击，同时将猜测得到恢复的密钥用于后续攻击。具体攻击思路是，逐字节攻击是针对前后8 B，每字节256种可能；逐比特攻击是针对64 bit，每比特2种可能。基于这一结构特性，可将2种方法的理论复杂度分别表示为

$$C_{\text{byte}} = n_b \cdot 2^8 \cdot 2^8 = 2^{19} \tag{1}$$

$$C_{\text{bit}} = n_b \cdot 2^1 \cdot 2^1 = 2^8 \tag{2}$$

其中，n_b为不同攻击方式下的最小分析单元，式(1)中n_b为8，式(2)中n_b为64。

二者的复杂度比值为

$$\frac{C_{\text{byte}}}{C_{\text{bit}}} = \frac{2^{19}}{2^8} = 2^{11} = 2\,048 \tag{3}$$

式(3)中“2 048”并非经验值，而是攻击算法结构与搜索空间规律推导得到的理论复杂度比。换言之，逐比特攻击通过将搜索维度由字节级降到比特级，有效减少了指数级的搜索空间，从而在理论上实现了复杂度的显著降低。本文逐比特攻击策略主要基于ASCON算法的S盒输出的比特级泄漏特征，此类攻击策略仅支持泄漏模型符合比特级相关性算法，对于AES、PRESENT等算法，使用逐字节攻击即可。

1.2　功耗采集与逐比特攻击

本文逐比特CPA攻击基于典型的嵌入式硬件平台，以STM32F030微控制器（MCU，microcontroller unit）作为目标板，在其上实现ASCON算法。将ASCON算法的攻击点选择在初始化阶段P过程第一轮的S盒输出，原因是，初始化阶段之前其他过程没有参与，即初始密钥没有扩散，因此初始化阶段是隔离单个密钥字节、实现低复杂度的最佳时间窗口。

功耗物理采集方案如图3所示，在MCU的供电引脚与主电源之间，串联一个低阻值的采样电阻R。此电阻足够小，不会影响MCU的正常工作，通过测量电阻两端电压，间接反映MCU内部瞬时功耗。串联电阻不需要修改芯片封装，保证攻击的隐蔽性和非侵入性，是侧信道攻击的有效方法。

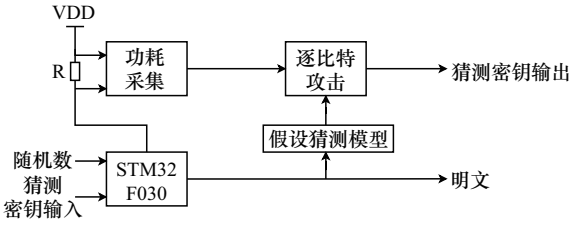


图3　功耗物理采集方案

逐比特CPA攻击包含以下几个步骤：首先，采集功耗曲线作为实际功耗；其次，对密钥进行猜测来模拟加密过程；接着，计算加密的中间值作为假设功耗；最后，计算实际功耗与假设功耗的相关性，以真实密钥与实际功耗具有最大相关性为理论，确定此刻的猜测密钥为正确密钥[20]。

物联网设备的功耗大小与逻辑门翻转次数相关，汉明重量模型（二进制数中1的个数）中，假设能量消耗与被处理数据中被置位的比特个数成正比，可以有效反映设备功耗变化。因此，使用汉明重量模型作为中间模型去衡量假设功耗，之后进行逐比特攻击。

具体攻击步骤如下。

1) 功耗曲线采集及模拟加密过程。计算机随机生成128 bit随机数，通过串口发送至加密设备，开始进行功耗曲线采集。对于每个假设的密钥比特值，通过模拟进入S盒参与运算，之后计算对应的假设功率消耗值，使用汉明重量模型模拟为假设功耗，映射关系如式(4)所示。

$$t_{d,j} = \text{HW}\left(S_{\text{box}}\left(\text{IV},K_0,K_1,N_0,N_1\right)\right) \tag{4}$$

其中，IV为定值，K_0为前64 bit假设密钥，K_1为后64 bit假设密钥，N_0为随机数的前64 bit，N_1为随机数的后64 bit，S_{box}是计算S盒的函数，HW是计算汉明重量的函数。

S_{box}函数内部的猜测密钥输出如式(5)和式(6)所示。

$$y_1 = \text{IV}\hat{}K_0\hat{}K_1\hat{}N_0\hat{}N_1\hat{}(K_0\&K_1)\hat{}(K_0\&N_0)\hat{}(K_1\&N_0) \tag{5}$$

$$y_2 = K_0\hat{}K_1\hat{}N_1\hat{}(N_0\hat{}N_1)\hat{}1 \tag{6}$$

其中，y_1对应前64 bit输出密钥，y_2对应后64 bit密钥输出。

2) 将假设功耗与实际采集到的功耗曲线进行相关性分析。相关性分析方法通常使用皮尔逊相关系数来评估假设值与真实功耗曲线之间的匹配程度，相关系数如式(7)所示。对于每个假设的密钥值，计算实际功耗与假设功耗的相关性。理论上，正确的密钥字节值会导致较高的相关性，因为它与真实的功耗相匹配。

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i}-\bar{h}_i)(t_{d,j}-\bar{t}_j)}{\sqrt{\sum_{d=1}^{D}(h_{d,i}-\bar{h}_i)^2}\sqrt{\sum_{d=1}^{D}(t_{d,j}-\bar{t}_j)^2}} \tag{7}$$

其中，$h_{d,i}$和$t_{d,j}$分别是变量i、j的第d个值（$h_{d,i}$为实际值，$t_{d,j}$为假设值），$\bar{h}_i$和$\bar{t}_j$分别是变量i、j的样本均值（$\bar{h}_i$为实际均值，$\bar{t}_j$为假设均值）。

3) 通过对每个假设的密钥比特进行相关性分

析，选择相关性最高的假设值作为猜测的正确密钥比特，重复此过程，逐步恢复出更多的密钥比特，并利用已恢复的密钥信息简化后续的猜测过程。

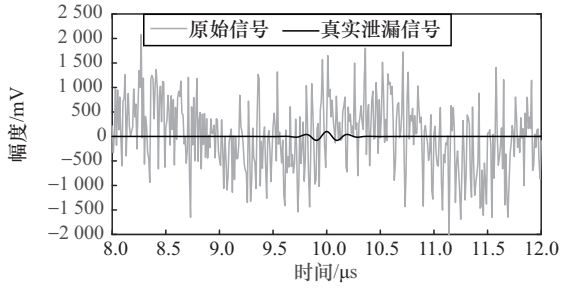
4) 最后，使用不同的随机数，重复前3个过程得到猜测密钥。将猜测得到的密钥值与真实密钥值对比，验证攻击是否成功。

1.3　功耗曲线预处理

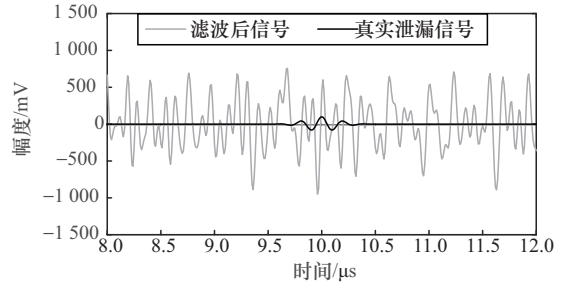
在逐比特攻击时，预处理是提升攻击效率的关键。对于本研究聚焦的逐比特攻击，其所依赖的物理泄漏在时域上表现为一个能量微弱、持续时间极短的瞬态脉冲信号。这一特性对预处理方案有着极高的要求。

常见的预处理方案使用一个线性的FIR低通滤波器，但其对本研究聚焦的、由单比特翻转引起的瞬态脉冲信号并非最优，通过对大量功耗曲线进行信号平均与频谱分析，发现与S盒单比特运算相关的泄漏能量信号并非集中在0 Hz附近，而是主要分布在1~15 MHz，其他频率范围内为噪声信号。因此，一个带通滤波器是匹配该泄漏模型的选择。

目标板工作频率为8 MHz，设置滤波器采样频率f_s为100 MHz，同时，设置截止频率f_c为16 MHz，所以归一化截止频率w_n为0.4。具体设计流程不再展开，最终计算得到滤波器阶数N=661，同时选用汉明窗进行设计。本方案设计的带通滤波器滤波效果前后如图4所示。



(a) 原始信号与瞬态泄漏



(b) 带通滤波效果

图4　带通滤波前后效果

图4(a)中真实泄漏信号（黑色实线）几乎淹没在噪声信号（灰色背景）中。而图4(b)中本方案的带通滤波通过滤除带外的高、低频噪声，实现了对泄漏信号的滤波，极大提升了信噪比，这一高质量的预处理，是后续成功实施高效CPA攻击的物理基础。

2　功耗均衡S盒防御方案

为保障物联网终端的数据安全，降低侧信道攻击中信息泄漏的风险，必须设计有效的防御机制。针对ASCON算法在物联网设备上进行比特运算时，数据总线上出现的中间值与功耗相关联导致的侧信道信息泄漏问题，本文提出一种基于均衡查找表的S盒实现方案。该方案在不改变原加密逻辑和结果的前提下通过算法级修改，均衡S盒操作的功耗，从而抵御逐比特功耗攻击。

传统的CPA攻击，其基础在于设备的功耗与正在处理的数据的汉明重量存在线性关系。攻击者可以通过精确测量设备在处理不同数据时的功耗数据，计算出数据总线上中间值的汉明重量，以此达到破解密钥的目的。

本方案的核心思想是“均衡化”而非“随机化”功耗。通过构建一个特殊的S盒查找表，使无论S盒的输入为何值，CPU在执行查表操作后从数据总线上读取的输出值的汉明重量永远是一个固定值。这样一来，功耗与输入数据之间的关联性被彻底切断，攻击者无法通过测量功耗来获取任何关于中间值的有效信息，从而使攻击失效。功耗均衡S盒防御算法如算法1所示。

算法1　功耗均衡S盒防御算法

输入　状态S、轮常量C

输出　临时变量t

1) BALANCED_$S_{\text{box}}[x]$ =

$((\sim S(x)\&0\text{x}1\text{F}) \ll 5)|(S(x)\&0\text{x}1\text{F})$

2) $s[2] \leftarrow s[2] \oplus C$

3) $s[0] \leftarrow s[2] \oplus s[4]$

4) $s[4] \leftarrow s[4] \oplus s[3]$

5) $s[2] \leftarrow s[2] \oplus s[1]$

6) $t = 0$

7) for j = 0 :63 do

8) input$\leftarrow$ $(\text{bit}(s[0],i),\cdots,\text{bit}(s[4],i))$

9) lookup$\leftarrow$ BALANCED_$S_{\text{box}}[\text{input}]$

10) $y \leftarrow$ lookup & 0x1F

11)　　for j = 0 :4 do

12)　　$t[i][j] \leftarrow \mathrm{bit}(y,j)$

13)　　end for

14)end for

15) $t[1] \leftarrow t[1] \oplus t[0]$

16) $t[0] \leftarrow t[0] \oplus t[4]$

17) $t[3] \leftarrow t[3] \oplus t[2]$

18) $t[2] \leftarrow \sim t[2]$

19)return t

功耗均衡S盒的关键在于对ASCON原有的5 bit输入、5 bit输出进行逻辑扩展。将原本布尔代数实现S盒的方式，改为查表法实现，但将原5 bit的S盒扩展为一个新的10 bit的S盒，新S盒由原S盒与完全反向S盒组成，当5 bit的输入进行新的S盒计算时，该结构保证了每次输出的汉明重量恒为5。加密需要进行S盒变换时，程序将输入D作为地址索引，从新的S盒读取对应10 bit输出，这一操作会将一个汉明重量恒为5的数据加载到CPU的数据总线和寄存器中，读取完成后，程序保留前5bit进行后续加密，将后5 bit输出丢弃。可见，无论S盒的输入D为多少，产生的功耗始终是一个常数，使基于汉明重量模型的逐比特攻击彻底失效。该方法同样对其他利用数据依赖性功耗差异的侧信道攻击具有良好的防御效果。

3　实验结果与分析

采集功耗曲线时，示波器采样频率为20 MHz，明文A和关联数据P的值随机产生，将它们均设置为64 bit，密钥K设置为128 bit。随机数N通过随机函数生成，并将此随机数记录，随后进行功耗采集，每条曲线包含4 800个采样点。

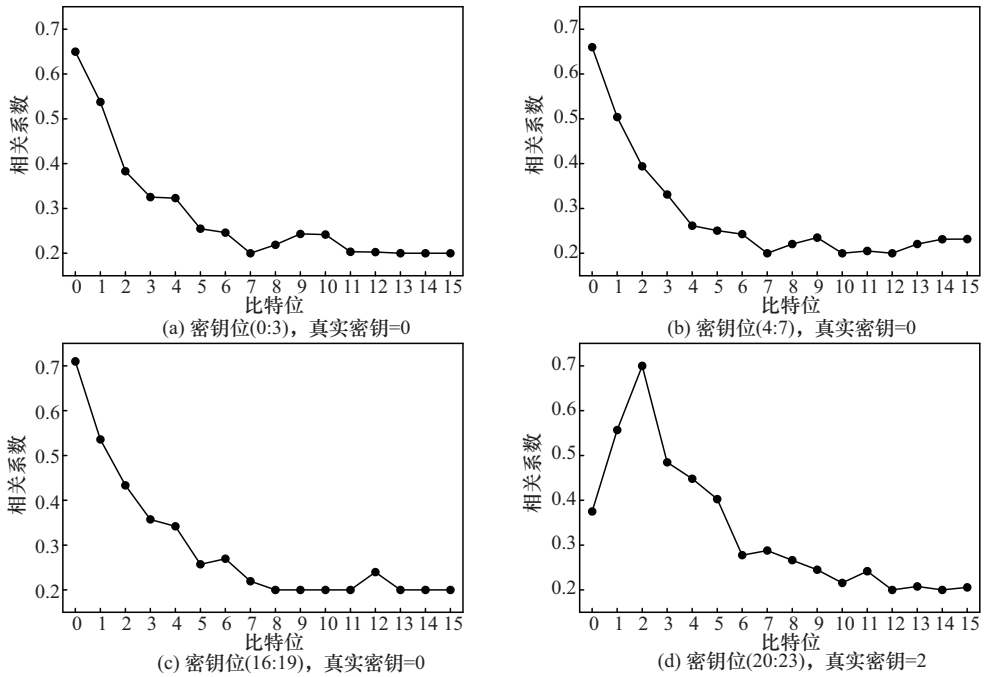
3.1　攻击结果

对ASCON算法执行逐比特攻击时，采集5 000条功耗曲线，进行1 000次逐比特攻击。在2 000条功耗曲线基础上，猜测密钥相关系数如图5所示。其中，相关系数曲线出现尖峰时，相关系数达到最大值，此时，密钥猜测正确。通过对ASCON实施逐比特攻击，最终成功恢复出114 bit初始密钥。

为评估整体攻击的成功率以及稳定性，在不同数量功耗曲线下分别进行1 000次攻击的成功率如表1所示。

表1　不同数量功耗曲线下1 000次攻击成功率

功耗曲线数量/条	攻击成功率
100	32.6%
200	55.3%
500	83.5%
1 000	93.6%
2 000	95.3%
3 000	97.0%



(a) 密钥位(0:3)，真实密钥=0　(b) 密钥位(4:7)，真实密钥=0

(c) 密钥位(16:19)，真实密钥=0　(d) 密钥位(20:23)，真实密钥=2

图5　猜测密钥相关系数

3.2　攻击结果评估

为全面、系统地评估本文方案的综合性能，需要验证内部逻辑的优越性，同时与先进的相关工作进行对比，主要在时间效率、最终效果和信息效率3个维度下，对本文方案进行了综合评估。攻击与预处理方案综合性能评估如图6所示。

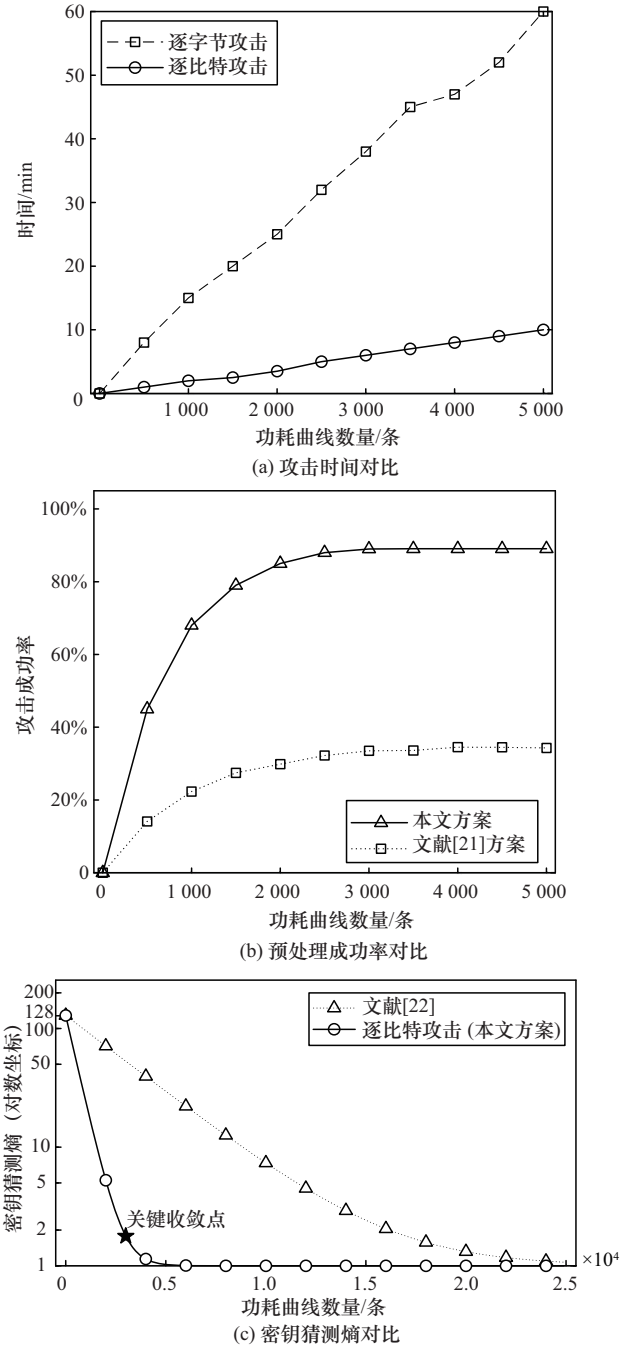


图6　攻击与预处理方案综合性能评估

图6(a)的时间对比直观地显示了本文方案核心攻击方法的优越性。图6(b)从最终攻击成果的维度，将本文方案的预处理技术与文献[21]进行了对比，本文方案在应用了目标导向的带通滤波器后，可达到近90%的成功率，显著超越了后者34.38%的水平，证明了本文预处理方案的先进性。图6(c)的密钥猜测熵对比，从信息效率层面揭示了本文方案攻击方法论的根本优势。文献[22]中的标准CPA攻击需要数万条功耗曲线才能使猜测熵收敛，而本文方案仅需3 000条即可实现同样目标。因此，经过综合性能评估，全面论证了本文攻击方案的高效性与先进性。

值得一提的是，近年来基于深度学习的侧信道攻击作为一种新兴技术同样备受关注。以文献[23]的工作为代表，这类攻击方案不需要精确的泄漏模型，更加灵活。为更加全面地评估本文方案的性能，与文献[23]攻击方案进行了比较，如表2所示。

表2　　本文方案与文献[23]方案对比

对比维度	文献[23]方案	本文方案
决策依据	神经网络	皮尔逊相关系数
所需曲线数量/条	100	3 000
攻击时间/s	<10	600
计算资源	CPU	CPU
密钥恢复位数	56	114

由表2可以看出，2种方案在技术路径和成本结构上存在显著差异。文献[23]方案需要大量的离线训练（约5万条迹线，数小时GPU时间），从而换取极快的攻击速度（秒级）。而本文方案不需要任何训练，直接进行攻击分析，虽然在线攻击耗时较长，但省去了高昂的训练成本。在关键的密钥恢复位数上，文献[23]选取了128 bit密钥中的64 bit片段作为攻击目标，实际仅恢复了56 bit密钥信息。相比之下，本文方案若仅针对其中64 bit密钥，可以恢复完整的64 bit。即使将方案应用在对128 bit密钥攻击时，也可以恢复其中的114 bit，在攻击的完整性和可靠性上远超对比方案。

3.3　防御评估

为全面、客观地评估本文功耗均衡S盒防御方案的有效性，本节在STM32F030上部署防御后的ASCON算法。之后，在目标板采集3 000条功耗曲线，并进行1 000次逐比特攻击后，对本文防御方案与文献[24]、文献[25]的掩码防御方案进行综合对比，效果如表3所示。

表3　本文方案与文献[24]、文献[25]防御效果对比

评估项目	无防御（基准）	本文方案	文献[24]	文献[25]
所需功耗曲线	3 000	3 000	10^6	10^4
攻击成功率	97.0%	6.2%	<1%	<1%
随机字节数需求	0	0	240	240
吞吐量（相对）	100%	95%	25%	50%
代码/存储开销	100%	110%	200%	150%

在安全增益方面，本文方案的核心优势在于在同等条件下（3 000条功耗曲线），成功将攻击率由97%削减至6.2%，且吞吐量几乎不受影响，代码与存储开销增加极小，且实现复杂度与随机数需求与无防御时相同。需要补充的是，该残余攻击成功率的来源可归纳为两类客观约束，即硬件底层的固有非理想性（如时钟抖动引起的功耗噪声）与攻击模型的局限性。前者是由物理层产生的随机波动导致功耗曲线残留，为攻击保留极小的信息泄漏窗口。后者是由于本文攻击方法可能未覆盖高阶侧信道泄漏或时间侧信道等维度，客观上为残余攻击留存了理论可能。同时，相较于无防御时97%的攻击成功率，6.2%的攻击成功率已经实现“数量级安全增益”，满足轻量密码对“低开销–高安全”的需求。若要追求接近0的攻击成功率，需引入硬件级定制化防护（如抗噪声电源、时钟校准电路），这将大幅突破ASCON“轻量部署”的设计约束，与物联网终端的资源受限特性冲突 。因此，当前残余风险是“算法级防护”在轻量级场景下的合理代价。

相比之下，文献[24]和文献[25]的掩码方案，虽然能达到极高的安全性（攻击成功率低于1%），但它们的代价极其高昂。首先，其吞吐量会大幅降低至无防御状态的25%~50%。其次，方案的安全性依赖高质量的随机数源（每轮需要240 B），并带来显著的资源开销。更关键的是，其实现复杂度是一项工程难题，开发者需小心处理复杂的逻辑以避免引入新的安全漏洞。

因此，本文防御方案以一种可量化的、极低的软硬件成本，换取了安全性的巨大提升。这种在安全性与性能之间取得的均衡，证明了其在物联网设备中具有极高的使用价值和部署潜力。

3.4　未来工作

尽管本文方案在软件层面取得了良好效果，但其核心瓶颈在于无法完全消除通用MCU底层硬件执行时的物理功耗差异，这为更高阶或更精密的攻击留下了可能。为突破这一软件实现的固有局限，未来的研究应将功耗均衡思想从算法级下沉到硬件级。一个极具潜力的研究思路是在FPGA或专用集成电路上，通过双轨预充电逻辑等技术进行门级电路设计，实现真正与数据无关的、恒定的S盒功耗。这种硬件级的内在安全特性，可以进一步与轻量级的软件防御措施（如一阶掩码）相结合，构建出软硬件协同的混合防御架构，从而以远低于传统高阶掩码方案的资源开销，实现更高级别的侧信道安全防护。

4　结束语

本研究证实，尽管ASCON等轻量级加密算法在理论设计上考虑了侧信道防御，但是在资源受限的物联网设备上实现时，依然会暴露出显著的安全脆弱性。因此，本文提出了一种针对ASCON算法的逐比特攻击方案，通过优化攻击策略与数据预处理，成功验证了这一风险。对应地，本文设计了一种功耗均衡S盒防御方案，展示了从算法层面构建有效防护的可行路径。

这种攻防协同的研究为物联网安全领域提供了关键启示，即算法设计与硬件防护必须进行一体化设计。未来研究应聚焦于探索开销更低、兼容性更强的软硬件协同防御机制，从而在保障物联网设备性能与成本优势的同时，为其构建真正“端到端”的、可信赖的安全体系。

参考文献：

[1] SULEIMAN T A, ADINOYI A. Telemedicine and smart healthcare: the role of artificial intelligence, 5G, cloud services, and other enabling technologies[J]. International Journal of Communications, Network and System Sciences, 2023, 16(3): 31-51.

[2] YANG Y C, WU L F, YIN G S, et al. A survey on security and privacy issues in Internet-of-things[J]. IEEE Internet of Things Journal, 2017, 4 (5): 1250-1258.

[3] CHEHAB M, MOURAD A. LP-SBA-XACML: lightweight semantics based scheme enabling intelligent behavior-aware privacy for IoT[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(1): 161-175.

[4] OMOLARA A E, ALABDULATIF A, ABIODUN O I, et al. The Internet of Things security: a survey encompassing unexplored areas and new insights[J]. Computers & Security, 2022, 112: 102494.

[5] WANG C Y, WANG D, DUAN Y H, et al. Secure and lightweight user authentication scheme for cloud-assisted Internet of Things[J]. IEEE

Transactions on Information Forensics and Security, 2023, 18: 2961-2976.

[6] KHAN S, FERREIRA LOPES MARTINS P A, SOUSA B, et al. A comprehensive review on lightweight cryptographic mechanisms for industrial Internet of Things systems[J]. ACM Computing Surveys, 2025, 58(1): 1-37.

[7] 何乐生, 冯毅, 岳远康, 等. 针对物联网设备的旁路攻击及防御方法的研究[J]. 通信学报, 2025, 46(2): 166-175.
HE L S, FENG Y, YUE Y K, et al. Research on side-channel attacks and defense methods for IoT devices[J]. Journal on Communications, 2025, 46(2): 166-175.

[8] TANKSALE V. Efficient elliptic curve diffie – Hellman key exchange for resource-constrained IoT devices[J]. Electronics, 2024, 13(18): 3631.

[9] BERNSTEIN D J. ChaCha, a variant of Salsa20[C]//Workshop Record of SASC 2008 - The State of the Art of Stream Ciphers. Lausanne: ECRYPT, 2008: 3-5.

[10] THAKOR V A, RAZZAQUE M A, KHANDAKER M R A. Lightweight cryptography algorithms for resource-constrained IoT devices: a review, comparison and research opportunities[J]. IEEE Access, 2021, 9: 28177-28193.

[11] 王振宇, 郭阳, 李少青, 等. 面向轻量级物联网设备的高效匿名身份认证协议设计[J]. 通信学报, 2022, 43(7): 49-61.
WANG Z Y, GUO Y, LI S Q, et al. Design of efficient anonymous identity authentication protocol for lightweight IoT devices[J]. Journal on Communications, 2022, 43(7): 49-61.

[12] KAUR J, CANTO A C, KERMANI M M, et al. A comprehensive survey on the implementations, attacks, and countermeasures of the current NIST lightweight cryptography standard[J]. arXiv Preprint, arXiv: 2304.06222, 2023.

[13] SURYATEJA P S, RAO K V. A survey on lightweight cryptographic algorithms in IoT[J]. Cybernetics and Information Technologies, 2024, 24(1): 21-34.

[14] ZHANG J L, CHEN C C, CUI J H, et al. Timing side-channel attacks and countermeasures in CPU microarchitectures[J]. ACM Computing Surveys,2024, 56(7): 1-40.

[15] DOBRAUNIG C, EICHLSEDER M, MENDEL F, et al. Ascon v1.2: lightweight authenticated encryption and hashing[J]. Journal of Cryptology, 2021, 34(3): 33.

[16] WEISSBARTL, PICEKS. Lightweight but not easy: side-channel analysis of the ascon authenticated cipher on a 32-bit microcontroller[J]. Cryptology ePrint Archive, 2023: 1598.

[17] ROHIT R, HU K, SARKAR S, et al. Misuse-free key-recovery and distinguishing attacks on 7-round ascon[J]. IACR Transactions on Symmetric Cryptology, 2021: 130-155.

[18] BAUDRIN J, CANTEAUT A, PERRIN L. Practical cube attack against nonce-misused ascon[J]. IACR Transactions on Symmetric Cryptology, 2022: 120-144.

[19] ALI M T. Generic CPA decryption attack on ascon-128 in nonce-misuse setting by exploiting XOR patterns[C]//Proceedings of the 2024 14th International Conference on Electrical Engineering (ICEENG). Piscataway: IEEE Press, 2024: 172-174.

[20] NG J S, CHEN J C, KYAW N A, et al. A highly efficient power model for correlation power analysis (CPA) of pipelined advanced encryption standard (AES)[C]//Proceedings of the 2020 IEEE International Symposium on Circuits and Systems (ISCAS). Piscataway: IEEE Press, 2020: 1-5.

[21] 潘力, 韦永壮. 轻量级认证加密算法ASCON的差分功耗分析[J]. 桂林电子科技大学学报, 2023, 43(2): 142-148.
PAN L, WEI Y Z. Differential power analysis of lightweight authenticated encryption algorithm ASCON[J]. Journal of Guilin University of Electronic Technology, 2023, 43(2): 142-148.

[22] SAMWEL N, DAEMEN J. DPA on hardware implementations of Ascon and Keyak[C]//Proceedings of the Computing Frontiers Conference. New York: ACM Press, 2017: 415-424.

[23] REZAEEZADE A, BASURTO-BECERRA A, WEISSBART L, et al. One for all, all for Ascon: ensemble-based deep learning side-channel analysis[C]//Applied Cryptography and Network Security Workshops. Berlin: Springer, 2024: 139-157.

[24] MAINKA L, PAPAGIANNOPOULOS K. Combined masking and Shuffling for Side-channel secure ascon on RISC-V[C]//Constructive Approaches for Security Analysis and Design of Embedded Systems. Berlin: Springer, 2026: 451-477.

[25] SALOMON D, LEVI I. MaskSIMD-lib: on the performance gap of a generic C optimized assembly and wide vector extensions for masked software with an Ascon-p test case[J]. Journal of Cryptographic Engineering, 2023, 13(3): 325-342.

[作者简介]

何乐生（1977– ），男，白族，云南昆明人，博士，云南大学副教授，主要研究方向为嵌入式系统及物联网应用、微弱信号采集和处理及其在生物电信号和射电天文信号处理等。

靳亚灿（1999– ），男，河南安阳人，云南大学硕士生，主要研究方向为轻量级密码安全性分析、嵌入式开发等。

张孝蔚（2000– ），男，四川内江人，云南大学硕士生，主要研究方向为侧信道攻击、轻量级密码安全性分析等。

晋兵（1999– ），男，云南昭通人，云南大学硕士生，主要研究方向为图像处理、模式识别和人工智能等。