针对物联网设备的旁路攻击及防御方法的研究

何乐生[1,2]，冯毅[1]，岳远康[1]，杨崇宇[1]，胡崇辉[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：物联网设备通常使用计算能力受限的微控制器来实现，因而只能采用轻量级对称加密算法来保证其数据安全，且其自身的特点决定了只能被部署在开放环境中，极易遭受旁路攻击。针对这一问题，在基于自主设计的旁路攻击验证平台上开展实验，并提出了安全密钥管理方案及改进的S盒设计，作为旁路攻击防御方法。验证平台由两级差分放大器和抗干扰有限冲激响应（FIR）滤波器构成，能够捕捉微弱的功耗变化，并设计了针对轻量级加密算法的两轮相关能量攻击。通过获取正确密钥相关系数置信度的评估方法，在对PRESENT算法的3 000条功耗曲线进行10 000次攻击后，成功率超过96%，正确密钥的相关性均值均超过0.6，在95%的置信水平下，拥有狭窄的置信区间，而采用改进后的算法进行相同实验时，攻击成功率仅为9.12%。

关键词：物联网安全；轻量级密码；旁路攻击；相关能量分析
中图分类号：TN918.9
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025028

Research on side-channel attacks and defense methods for IoT devices

HE Lesheng[1,2], FENG Yi[1], YUE Yuankang[1], YANG Chongyu[1], HU Chonghui[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: Internet of things (IoT) devices are typically implemented using microcontrollers with limited computational capabilities, which necessitate the use of lightweight symmetric encryption algorithms to ensure data security. Due to their inherent characteristics, these devices can only be deployed in open environments, making them highly vulnerable to side-channel attacks. To address this issue, experiments were conducted on a self-designed side-channel attack validation platform, where a secure key management scheme and an improved S-box design were proposed as countermeasures against side-channel attacks. The validation platform consisted of a two-stage differential amplifier and an anti-interference finite impulse response (FIR) filter, which were capable of capturing subtle power consumption fluctuations. A two-round correlated energy attack targeting lightweight encryption algorithms was also designed. By evaluating the confidence of the correct key correlation coefficient, after 10 000 attacks on 3 000 power consumption traces of the PRESENT algorithm, a success rate of over 96% is achieved, with the mean correlation of the correct key exceeding 0.6. At a 95% confidence level, a narrow confidence interval is obtained. In contrast, when the improved algorithm is used in the same experiment, the attack success rate is only 9.12%.

Keywords: IoT security, lightweight cryptosystem, side-channel attack, correlation power analysis

0　引言

随着5G通信、嵌入式技术和云计算的快速发展，物联网（IoT, Internet of things）技术已经广泛应用于各行各业，推动了智能家居、智慧城市和智

收稿日期：2024–10–17；**修回日期：**2025–02–10
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)

能医疗设备的普及，极大地提升了人们的生活质量。同时，智慧农业、智慧工厂和智慧电网等应用在提高生产效率方面也发挥了重要作用。然而，物联网的快速发展也带来了日益严重的安全问题[1]。大量物联网设备承载着涉及个人隐私和商业机密的数据，一旦安全防护措施不足，便可能面临数据泄露、信息篡改和身份伪造等严重风险[2-4]。物联网安全直接关系到国家的经济发展和公民的隐私保护，因此，如何确保物联网信息的安全已成为亟待解决的关键问题。

在信息安全领域中，加密算法通常用于确保信息的机密性和完整性。然而，由于大多数的物联网设备由微控制单元（MCU, microcontroller unit）组成，MCU 的计算和存储资源有限，传统的加密算法难以直接应用于这些设备。为应对这一挑战，专为资源受限的物联网设备设计的轻量级加密算法应运而生。这些算法在保证安全性的同时，最大程度地降低了能耗和内存占用[5-6]，切实满足了物联网设备的要求。高安全性与轻量级（HIGHT, high security and light weight）[7]、多重输入块序列（MIBS, multiple input block sequence）[8]和 GIFT[9]等轻量级加密算法，已广泛应用在各类物联网设备中。它们不仅有效保障了数据的机密性和完整性，还能在资源受限的环境下高效运行，成为确保物联网安全的重要手段[10-14]。

虽然轻量级加密算法在物联网设备上显示出一定的优势，但其在实际应用中的安全性仍需进一步验证。物联网设备通常部署在开放且易受攻击的环境中，攻击者能够轻松获取物联网设备，这使旁路攻击成为窃取设备内部敏感信息的高效手段[15]。旁路攻击以其低成本和操作简便的特性已成为现实中的常见威胁，攻击者可通过极低的技术门槛获取加密密钥和其他敏感数据，进而破坏通信安全、篡改数据，甚至控制设备。这为物联网系统的安全性和数据完整性带来了严峻挑战。因此，现有轻量级加密算法在面对旁路攻击时的脆弱性，凸显出对其安全性进行更深入研究和评估的迫切性，以确保这些算法在真实的物联网环境中能够提供足够的防护，保证系统的整体安全性和稳定性。

为了分析现有轻量级加密算法的潜在漏洞，本文选择 PRESENT 算法作为研究对象，进行旁路攻击分析。PRESENT 算法由 Bogdanov 等[16]提出，基于替换-置换网络（SPN, substitution permutation network）结构，采用 64 位数据块和 80 位或 128 位密钥长度。该算法旨在实现小巧的硬件占用和低功耗，因此成为存储和计算资源有限系统中的理想选择。PRESENT 算法已广泛应用于无线传感器网络、可穿戴设备、智能卡、支付设备、智能交通系统和工业自动化等领域[17]。在无线传感器网络中，PRESENT 算法能够有效保障数据传输的安全性，在可穿戴设备（如智能手表、健康监测器）中，它不仅保护用户隐私数据，还能显著延长设备的续航时间。此外，PRESENT 算法在智能卡和支付设备中加密个人信息和交易数据，有效防范恶意攻击；在智能交通系统中，它保障车载传感器与交通信号之间的安全数据传输；在工业自动化和远程监控中，PRESENT 算法保护设备控制指令和监测数据的安全性。总体而言，PRESENT 算法为这些资源受限的设备提供了高效的加密和身份验证功能，同时满足低功耗和小硬件占用的严格要求[18]。

为确保 PRESENT 算法在实际应用中能有效抵御旁路攻击，学术界不断对其抗旁路攻击性进行评估和验证。文献[19]通过多模型差分故障分析，发现最少需要 17 个故障密文才能恢复 64 位密钥。文献[20]通过优化后的差分故障攻击，平均只需 9 个故障密文即可恢复 64 位密钥。差分故障攻击虽然计算资源要求低、适用性强且成功率高，但依赖于故障注入和精确控制，成本较高且易受现代防护措施影响。文献[21]通过计算机模拟功耗曲线，采用相关能量分析攻击，成功恢复了 PRESENT 算法 80 位主密钥的前 64 位，将密钥的搜索空间缩小至 2^{16}。尽管计算机模拟功耗曲线能有效降低旁路攻击的成本和时间，但模拟功耗曲线难以准确反映实际设备的功耗情况。物联网环境中，复杂且难以预测的电磁干扰和噪声等因素会显著影响旁路攻击的成功率。

本文提出了一套系统化的旁路攻击方案，涵盖了功耗曲线采集的硬件设计和旁路攻击算法的设计。通过开发高精度功耗采集系统，捕捉物联网设备在加密运算时的功耗波动，并结合抗干扰有限冲激响应（FIR）滤波器和两轮相关能量分析（CPA, connectional power analysis），在少量的功耗曲线下成功恢复 PRESENT 算法的完整密钥，验证了该方案的有效性。基于此，本文提出了针对该方案的防御设计，包括安全密钥管理方案和基于布尔函数的

S盒方案，旨在提升物联网设备的抗攻击能力，为物联网安全研究提供了有价值的参考。

1　针对物联网设备的旁路攻击方案设计

1.1　PRESENT算法

PRESENT算法是一种轻量级分组加密算法，由31轮加密组成，提供80位和128位2种密钥长度版本。80位密钥长度版本已足够满足标签式部署中通常要求的安全性。图1展示了PRESENT算法加密流程，每轮加密过程包括3个步骤：轮密钥更新、S盒替换和P置换，加密在第31轮运算结束后进行白化操作，以进一步增强安全性。

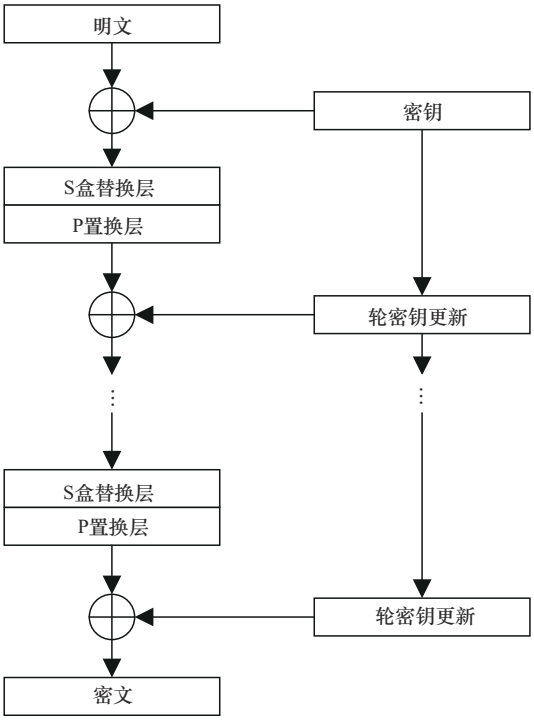


图1　PRESENT算法加密流程

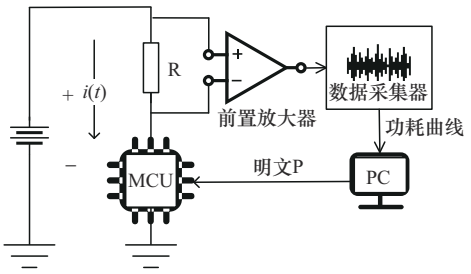
PRESENT算法的密钥扩展相对简单，密钥扩展的主要任务是从初始的密钥中生成32个轮密钥。扩展过程采用简化的位移和轮密钥异或操作，通过固定的规则生成每一轮所需的密钥。具体扩展步骤如下：80位主密钥K表示为$k_{79}k_{78}\cdots k_1k_0$。第$i$轮密钥由主密钥$K$的前64位组成。当生成第$i$轮密钥$K_i$后，通过式(1)更新$K$。

$$\begin{aligned}&[k_{79}k_{78}\cdots k_1k_0]=[k_{18}k_{17}\cdots k_{20}k_{19}]\\&[k_{79}k_{78}k_{77}k_{76}]=\mathrm{Sbox}[k_{79}k_{78}k_{77}k_{76}]\\&[k_{19}k_{18}k_{17}k_{16}k_{15}]=[k_{19}k_{18}k_{17}k_{16}k_{15}]+C\end{aligned}\quad(1)$$

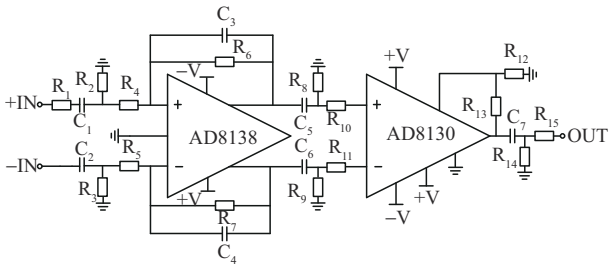
其中，Sbox为S盒替换，C为轮计数器值。密钥寄存器向左旋转61位，最左边的4位通过S盒替换层处理。接着，轮计数器值C与密钥K的$k_{19}k_{18}k_{17}k_{16}k_{15}$位进行异或运算，轮计数器的最低有效位位于右侧。

1.2　功耗曲线采集方案的设计

本文方案设计选择MCU芯片作为旁路攻击的目标板，在MCU芯片上部署PRESENT算法，工作频率为8 MHz。MCU芯片通过串口与计算机（PC）连接，计算机生成随机的明文发送给目标板，同时记录明文。为了采集高质量的功耗曲线，需要在MCU与电源之间配置一个取样电阻R，并移除MCU芯片电源周围的去耦电容。此外，在取样电阻R后加入前置放大电路，通过数据采集器采集功耗曲线并将数据发送给计算机，整体采集方案如图2(a)所示。



(a) 整体采集方案



(b) 前置放大电路设计

图2　功耗曲线采集方案

MCU芯片在工作时的功耗变化非常微弱，通常在毫安级别，这使得功耗分析变得更加困难。因此，设计高性能的功耗曲线前置放大电路至关重要。该前置放大电路由两级运算放大器级联组成，分别为AD8138和AD8130。两级放大器具有不同的功能和特点，旨在实现最佳的信号放大和处理效果。

AD8138[22]是一款高性能的全差分放大器，其共模抑制比典型值为77 dB，有效解决了高位电流检测方法中较大共模信号的问题，显著抑制了共模噪声，减少了外部噪声和干扰的影响。AD8138具有高达320 MHz的带宽和高增益性能，适用于前置放大电

路。此外，AD8138 的噪声电压密度为 5 nV/√Hz。同时，它具备差分输入和输出能力，进一步提高了抗干扰能力，确保信号的完整性。

AD8130[23]作为第二级放大器，在信号的进一步放大和转换中起着至关重要的作用。它提供高达 270 MHz 的带宽，确保信号的高频成分不被丢失。AD8130 的典型压摆率为 1 090 V/μs，适合处理快速变化的信号。在功耗曲线分析中，信号的快速变化往往包含关键的信息。AD8130 的噪声电压密度为 12.5 nV/√Hz，在高速信号处理中，其低噪声特性确保了信号放大的同时不会引入过多的噪声，从而保持较高的信噪比。AD8130 能够将差分信号转换为单端信号，简化了后续电路设计，并减少了信号链中的潜在误差[24]。

功耗曲线采集装置前置放大电路设计如图 2(b)所示，其中，R_1的阻值与采样电阻 R 相同，用于平衡同相与反相输入端；C_1、C_2、C_5、C_6和C_7在信号链中用于阻断各级之间的直流电平，防止各级放大器的直流偏置相互干扰；R_2、R_3、R_8、R_9、R_{10}、R_{11}、R_{14}和R_{15}用于实现信号链中的阻抗匹配，提高信号传输效率和电路稳定性；C_3和C_4用于相位补偿，防止运算放大器自激振荡并抑制高频噪声；R_4、R_6、R_5和R_7用于控制 AD8138 的增益；R_{12}和R_{13}控制 AD8130 的增益。

1.3　功耗曲线预处理

在功耗采集过程中，系统会受到环境干扰、电磁干扰和测量设备固有噪声的影响，产生高频噪声，这些噪声可能掩盖 MCU 芯片的真实功耗变化，导致关键信息不明显或难以提取，从而增加分析难度，甚至导致错误结果。为了提高功耗分析的效率，并增强正确密钥和错误密钥之间的区分度，本文在进行 CPA 之前对功耗曲线进行了预处理，使用 FIR 滤波器对功耗曲线进行滤波，以减少高频噪声的干扰。

目标板以 8 MHz 的频率工作，为避免混叠并提高信号采样精度，滤波器的采样率设置为 40 MHz。为了确保滤波器能够保留这一频率及其附近的有用信号成分，并保证通带和阻带之间留有一定的过渡带宽，选择 10 MHz 作为截止频率，归一化截止频率f_c为

$$f_c = \frac{f_{\text{cutoff}}}{f_{\text{sampling}}} \tag{2}$$

其中，f_{cutoff}为截止频率，f_{sampling}为采样频率。

滤波器的阶数决定了其冲激响应的长度和频率响应的陡峭程度。本文选择了 281 阶 FIR 滤波器（即 N=281），高阶数提供了更好的频率选择性。

窗函数用于控制 FIR 滤波器的频率响应特性，汉明窗在通带波纹和阻带衰减之间提供了较好的平衡，本文选择汉明窗进行设计，其窗函数的数学表达式为

$$w[n] = 0.54 - 0.46\cos\left(\frac{2\pi n}{N}\right), \quad 0 \leqslant n \leqslant N \tag{3}$$

滤波器的设计过程如下。

1) 理想低通滤波器的冲激响应计算

理想低通滤波器的冲激响应为一个无限长度的 Sinc 函数。理想的冲激响应如式(4)所示。

$$h[n] = \frac{\sin(2\pi f_c n)}{\pi n} \tag{4}$$

2) 窗口函数的应用

使用汉明窗对理想的冲激响应进行加窗处理，得到实际的 FIR 滤波器系数。

$$h[n] = h_d[n] \times w[n] \tag{5}$$

FIR 滤波器频率响应如图 3 所示。

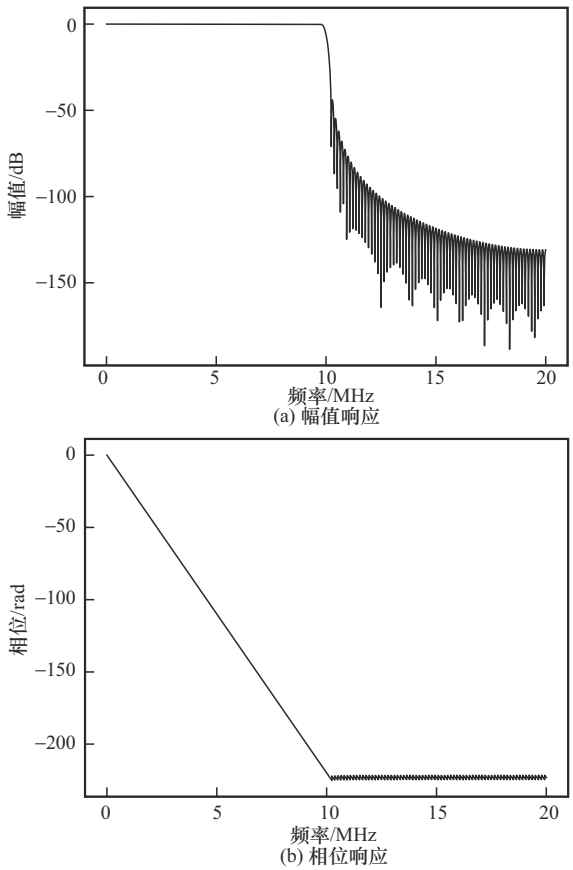


图 3　频率响应

1.4 攻击算法

CPA攻击包括以下几个步骤：首先，采集功耗曲线，计算加密过程中的中间值，并利用功耗模型将这些中间值映射为理论功耗；然后，计算实际功耗与理论功耗之间的相关性，并通过寻找与实际功耗具有最大相关性的理论功耗；最后，确定对应的猜测密钥，并得到正确密钥[25]。

在PRESENT算法中，完整的加密过程包含31轮，如果仅针对第一轮加密的S盒进行CPA，能够恢复的只是完整密钥的前64位。因此，为了获得PRESENT算法的完整密钥，本文设计了两轮CPA方案。由于物联网设备的功耗变化与逻辑门状态变化的次数（即位的翻转）密切相关，汉明重量模型能够有效反映实际硬件的功耗特性[26]，因此采用汉明重量模型对理论耗功耗进行刻画。两轮CPA的中间值t和s分别是第一轮和第二轮轮加密S盒的输出值。S盒具有较高的非线性度，其输出依赖于具体的输入值，并且在这一阶段，密钥尚未经过多轮变换的扩散[27]。具体攻击步骤如下。

1) 采集功耗曲线

通过串口将计算机生成的n条64位随机明文发送至加密设备，并同时进行功耗数据采集。功耗曲线包含第一轮和第二轮加密的功耗特征，每组功耗曲线可同时用于两轮CPA。每条功耗曲线有w个采样点，形成大小为$n\times w$的矩阵$\boldsymbol{D}$。

2) 第一轮CPA

① 计算中间值。PRESENT算法中每个明文为64位，由于S盒设计为4位输入输出的，因此将64位分成16个4位明文块，用P_n来表示，猜测密钥Kguess_k为4位（k=16），每个明文块与Kguess通过式(6)计算出S盒输出的猜测值，得到一个大小为$n\times k$的模拟功耗矩阵$\boldsymbol{T}$。

$$t_{n,k}=\text{Sbox}(P_n\oplus\text{Kguess}_k) \tag{6}$$

② 模拟功耗曲线。由①中得到的矩阵$\boldsymbol{T}$映射为模拟功耗矩阵$\boldsymbol{H}$，计算矩阵$\boldsymbol{T}$中每一位元素的汉明重量，得到$h_{n,k}$。

$$h_{n,k}=\text{HW}(t_{n,k}) \tag{7}$$

其中，HW为计算汉明重量。

③ 计算相关系数$r_{k,w}$并得到最大值。对模拟功耗矩阵$\boldsymbol{H}$的每一列$\boldsymbol{h}_k$和真实功耗矩阵$\boldsymbol{D}$的每一列$\boldsymbol{d}_w$求相关系数，得到相关系数矩阵$\boldsymbol{R}$，最大的相关系数对应的猜测密钥即正确密钥，$r_{k,w}$的计算式为

$$r_{k,w}=\frac{\sum_{n=1}^{N}(h_{n,k}-\overline{h}_k)(d_{n,w}-\overline{d}_{n,w})}{\sqrt{\sum_{n=1}^{N}(h_{n,k}-\overline{h}_{n,k})^2\sum_{n=1}^{N}(d_{n,w}-\overline{d}_{n,w})^2}} \tag{8}$$

其中，$d_{n,w}$是实际功耗数据，$\overline{d}_{n,w}$是实际功耗数据的均值，$h_{n,k}$是模拟功耗值，$\overline{h}_k$是模拟功耗的均值，N为功耗迹线数量。

④ 第一轮加密密钥恢复。使用不同的明文块，重复①~③得到第一轮加密密钥K_1，K_1为初始密钥K的前64位，即$K_1=[K_1(7)K_1(6)\cdots K_1(0)]$。

3) 第二轮CPA

使用已知明文P_n、第一轮CPA得到的64位密钥K_1和猜测密钥Kguess_k，通过式(9)计算第二轮加密S盒输出的中间值。

$$s_{n,k}=\text{Sbox}[\text{PL}(\text{Sbox}(p_n\oplus K_1))\oplus\text{Kguess}_k] \tag{9}$$

其中，PL为P置换层，得到大小为$n\times k$的中间值矩阵$\boldsymbol{S}$，将中间值矩阵$\boldsymbol{S}$映射为假设能量消耗矩阵，⊕为异或运算，找到与真实功耗曲线矩阵相关性最大的中间值，由此得到对应的第二轮加密的轮密钥$K_2=[K_2(7)K_2(6)\cdots K_2(0)]$。

4) 第二轮加密密钥恢复

在第一轮CPA中获得了K_1，根据轮密钥生成算法，第二轮轮密钥中$K_2[2]$、$K_2[1]$、$K_2[0]$是由初始密钥K中的$K[9]$、$K[8]$、$K[7]$、$K[0]$变换得到，通过式(10)即可恢复初始密钥的后16位，即$K[8]$、$K[9]$。

$$\begin{aligned}
&K_2[0]=(K_2[0]\,\&0\text{x}0\text{F})\,|\,(\text{S}^{-1}[K_2[0]>>4]<<4)\\
&K_2[2]=K[9]<<5\,|\,K[0]>>3\\
&K_2[1]=K[8]<<5\,|\,K[9]>>3\\
&K_2[0]=K[7]<<5\,|\,K[8]>>3
\end{aligned} \tag{10}$$

其中，S^{-1}为S盒替换层的逆运算。

2 CPA防御方案

为了进一步提升物联网设备的安全性，建议在轻量级加密算法设计中加入以下措施以抵抗相关能量攻击。

2.1 加入安全密钥管理方案

在基于SPN结构的传统轻量级加密算法中，每轮加密的轮密钥由主密钥生成的，因此轮密钥与

主密钥之间存在一定的相关性。一旦获得轮密钥，就可以通过轮密钥生成算法恢复出主密钥。为了解决这个问题，建议引入安全密钥管理方案。

以认证序列构造（ASCON, authenticated sequence construction）算法[28]为例，在初始化过程中引入了初始向量（IV）和身份认证标识（ID），与主密钥共同生成状态字节 S，每轮加密时，状态字节 S 用于生成轮密钥。在 ASCON 算法轮加密中，使用状态字节 S 中的前 64 位与填充后的明文前 64 位进行运算，从而得到密文。相关能量分析可以通过这一计算产生的功耗信息进行攻击。然而，由于 320 位的状态字节 S 是由上一轮的 S 生成的，攻击者必须获得某一轮的完整状态字节 S，才能通过逆运算恢复出初始状态 S。因此，攻击者即使获得了某一轮状态字节 S 的前 64 位，也无法恢复出完整密钥。

2.2　优化 S 盒的实现方式

大多数轻量级加密算法，如轻量级加密设备（LED, lightweight encryption device）、高级加密标准（AES, advanced encryption standard）和 PRESENT 算法，通常采用基于查表的 S 盒实现。这种实现方式的优点在于高效和灵活，通过一次内存访问即可获得对应的输出，并且能够根据需求轻松扩展至不同的输入位宽。然而，查表 S 盒依赖的内存访问会引发显著的功耗变化，特别是在不同输入数据访问不同表项时，这种功耗差异可能十分明显，相关能量分析正是利用这些差异来推测初始密钥。

ASCON 算法中使用的 S 盒是基于布尔函数实现的。由于不涉及大规模的内存访问，ASCON 算法的功耗波动主要来自逻辑运算。每个逻辑门的功耗相对固定，使得攻击者很难通过功耗波动找到相关性，从而提高了抵抗 CPA 攻击的能力。

3　旁路攻击及防御结果

3.1　功耗曲线采集

实验环境如表 1 所示。在实验中，使用 STM32-F030 作为目标板部署 PRESENT 算法。示波器的采样频率为 500 MHz。执行加密算法时，明文 P 为随机 64 位数据，密钥为固定的 80 位数据。输入随机明文 P，并采集相应的功耗曲线，每条曲线包含 5 000 个采样点。

表 1　实验环境

设备	型号
CPU	Intel(R) Core(TM) i7-10875H
内存	16 GB
开发板	STM32F030
示波器	Agilent DSO-X 2024A
软件	Visual Studio Code 2019

3.2　CPA 攻击结果

本节展示了在 MCU 架构上实现的 PRESENT 算法的 CPA 攻击结果。图 4 展示了基于 1 000 条功耗曲线的正确密钥与错误密钥的相关系数对比。从图 4 中可以清晰看到正确密钥与错误密钥在相关系数上的显著差异。当密钥猜测正确时，相关系数曲线会出现一个尖峰，尖峰对应的猜测密钥即正确密钥。通过对 PRESENT 算法进行两轮 CPA，可以成功恢复出 80 位初始密钥。

3.3　攻击结果评估

完整的攻击要使用 2 次 CPA，第二轮的成功与否依赖于第一轮的成功，只有在两轮分析都成功的情况下，攻击才算成功。为了评估整体攻击的成功率，在不同数量功耗曲线下分别进行 10 000 次完整攻击，成功率对比如表 2 所示。

表 2　在不同数量功耗曲线下分别进行 10 000 次完整攻击的成功率对比

功耗曲线数量/条	未加入预处理	加入预处理
50	25.31%	56.18%
100	33.48%	62.76%
150	44.89%	73.26%
200	50.25%	81.89%
300	55.31%	87.57%
500	64.26%	90.24%
800	68.31%	93.78%
1 200	73.48%	95.16%
1 500	76.89%	96.62%
2 000	79.25%	96.89%
2 500	81.31%	97.27%
3 000	82.26%	97.74%

预处理前后的成功率对比如图 5 所示。通过图 5 可以看出，经过预处理后，在少量的功耗曲

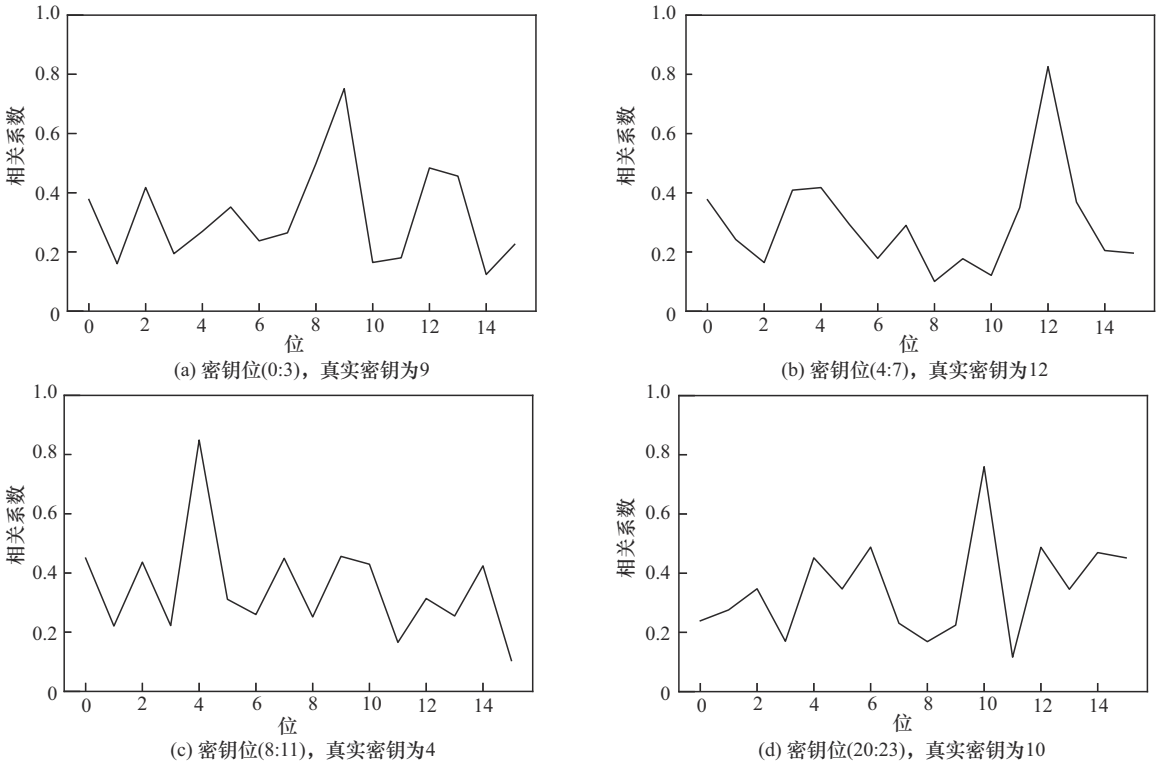


图4　相关系数对比

线数量下能达到更高的成功率，尤其是在样本数量较少的情况下。此外，预处理过程有效降低了噪声干扰，使得相关能量分析更具鲁棒性和可靠性。

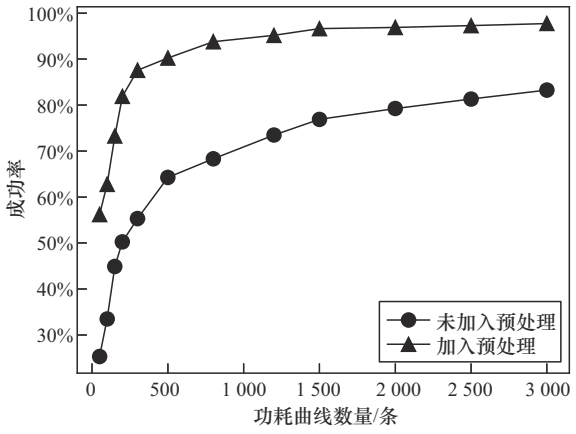


图5　预处理前后的成功率对比

为进一步量化攻击的成功率并提供对结果的统计保证，计算了3 000条曲线下10 000次相关能量攻击时正确密钥相关性的均值及其95%置信区间。采用Fisher Z变换方法计算正确密钥相关系数均值的置信区间。计算置信区间的步骤如下。

1) Fisher Z变换：对每次实验的正确密钥的相关系数R_i进行Fisher Z变换，将其转换为Z_i值。

2) 计算均值和标准误差：对n次实验得到的Z_i值求平均，并计算标准误差。

3) 计算置信区间：使用式(11)计算Z值的置信区间。

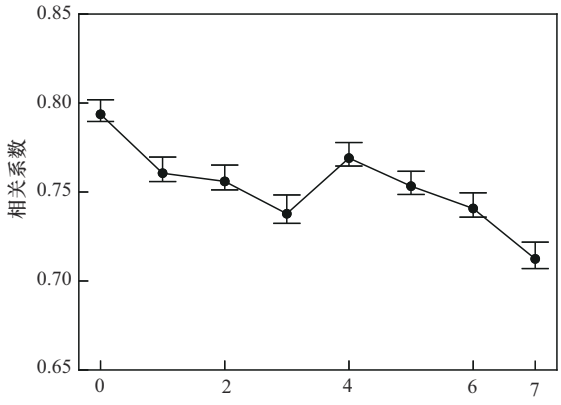
$$z_{\mathrm{CI}} = \bar{z} \pm z_{\frac{\alpha}{2}} \frac{\sigma_z}{\sqrt{n}} \tag{11}$$

其中，$\bar{z}$是Z_i的平均值，σ_z是标准差，z是对应置信水平的Z分数。

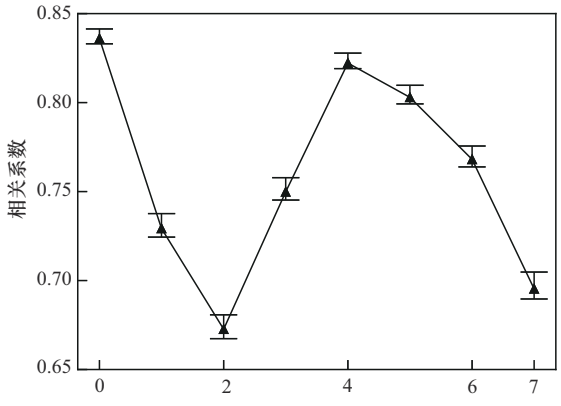
4) 反变换：将Z值的置信区间反变换为相关系数的置信区间。

通过上述计算得出的正确密钥相关系数的95%置信区间为（$\mathrm{CI}_r[0],\mathrm{CI}_r[1]$）。

最大相关性均值及其95%置信区间如图6所示。从图6可以看出，在10 000次完整攻击下，正确密钥的相关性均值始终超过0.65，且在大多数情况下都表现出较高的稳定性。此外，正确密钥的相关性均值还伴随着狭窄的置信区间，表明在多次攻击实验中，攻击结果具有较高的一致性和可靠性。尽管存在一定的噪声干扰，攻击方法依然能够显著区分正确密钥与错误密钥，进一步验证了本文方案在实际应用中的有效性和稳健性。



(a) 第一轮相关系数均值及置信区间



(b) 第二轮相关系数均值及置信区间

图6　最大相关性均值及其95%置信区间

3.4　防御方法效果

为了验证本文防御策略的有效性，本文通过实验对比了AES算法、PRESENT算法和ASCON算法在遭受CPA、差分功耗分析（DPA, differential power analysis）[29]和差分电磁分析（DEMA, differential electromagnetic analysis）[30]时加入防御措施前后的成功率。

在目标板STM32F030上部署相应的加密算法，并采用本文设计的功耗采集方案记录功耗曲线。同时，在目标板周围部署电磁采集线圈，用于收集电磁泄漏能量迹。本文共采集了3 000条功耗曲线和电磁能量迹，分别对其进行了CPA、DPA和DEMA。经过10 000次完整攻击实验后，得到如表3所示的结果。

从表3可以看到，使用查表法实现S盒的加密算法攻击成功率普遍超过90%，而使用布尔函数实现S盒的加密算法攻击成功率均不超过10%。因此，在加入防御方案之后，旁路攻击的成功率大幅度下降，防御方案对各类旁路攻击手段具有抑制效果。

表3　多种算法在不同攻击场景下的攻击成功率

算法	S盒类型	CPA	DPA	DEMA
AES	查表法	98.86%	95.34%	94.23%
	布尔函数	8.56%	6.76%	4.56%
PRESENT	查表法	96.89%	94.26%	93.46%
	布尔函数	9.12%	7.85%	8.21%
ASCON	查表法	94.23%	93.23%	90.45%
	布尔函数	7.94%	9.54%	3.21%

4　结束语

本文设计并验证了一种适用于真实物联网环境下的轻量级加密算法旁路攻击方案。通过设计功耗曲线采集装置，成功捕捉并放大微弱的功耗信号。同时，引入功耗曲线预处理技术，提升了功耗分析的准确性。实验结果表明，在少量功耗曲线下，攻击拥有较高的成功率。针对未来轻量级加密算法的设计，提出了安全密钥管理方案及优化S盒实现方式的建议。

为了进一步提升物联网设备的安全性，建议采用ASCON算法，并结合其内建的安全密钥管理方案和基于布尔函数实现的S盒设计。下一步，笔者将继续探索轻量级加密算法的高效防护方案。

参考文献：

[1] AHMED T, SAMIMA S, ZUHAIR M, et al. FIMBISAE: a multimodal biometric secured data access framework for Internet of medical things ecosystem[J]. IEEE Internet of Things Journal, 2023, 10(7): 6259-6270.

[2] 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.

[3] 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.

[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] 王楚豫, 谢磊, 赵彦超, 等. 基于RFID的无源感知机制研究综述[J]. 软件学报, 2022, 33(1): 297-323.
WANG C Y, XIE L, ZHAO Y C, et al. Survey on RFID-based battery-less sensing[J]. Journal of Software, 2022, 33(1): 297-323.

[6] 李文婷, 汪定, 王平. 无线传感器网络下多因素身份认证协议的内部

人员攻击[J]. 软件学报, 2019, 30(8): 2375-2391.
LI W T, WANG D, WANG P. Insider attacks against multi-factor authentication protocols for wireless sensor networks[J]. Journal of Software, 2019, 30(8): 2375-2391.

[7] HONG D, SUNG J, HONG S, et al. HIGHT: a new block cipher suitable for low-resource device[C]//International Workshop on Cryptographic Hardware and Embedded Systems-CHES 2006. Berlin: Springer, 2006: 46-59.

[8] IZADI M, SADEGHIYAN B, SADEGHIAN S S, et al. MIBS: a new lightweight block cipher[C]//Cryptology and Network Security. Berlin: Springer, 2009: 334-348.

[9] BANIK S, PANDEY S K, PEYRIN T, et al. GIFT: a small present: towards reaching the limit of lightweight encryption[C]// Cryptographic Hardware and Embedded Systems-CHES 2017. Berlin: Springer, 2017: 321-345.

[10] NAGARAJAN S M, DEVERAJAN G G, KUMARAN U, et al. Secure data transmission in Internet of medical things using RES-256 algorithm[J]. IEEE Transactions on Industrial Informatics, 2022, 18(12): 8876-8884.

[11] FAN Q, CHEN J H, SHOJAFAR M, et al. SAKE*: a symmetric authenticated key exchange protocol with perfect forward secrecy for industrial Internet of things[J]. IEEE Transactions on Industrial Informatics, 2022, 18(9): 6424-6434.

[12] SAQIB M, MOON A H. A systematic security assessment and review of Internet of Things in the context of authentication[J]. Computers & Security, 2023, 125: 103053.

[13] 宋蝉, 张蕾, 吴文玲. SPN 型密码的通用子空间迹分析[J]. 软件学报, 2023, 34(12): 5807-5821.
SONG C, ZHANG L, WU W L. General subspace trail cryptanalysis of SPN ciphers[J]. Journal of Software, 2023, 34(12): 5807-5821.

[14] 康步荣, 张磊, 张蕊, 等. 抗随机数后门攻击的密码算法[J]. 软件学报, 2021, 32(9): 2887-2900
KANG B R, ZHANG L, ZHANG R, et al. Cryptographic algorithms against backdoored pseudorandom number generator[J]. Journal of Software, 2021, 32(9): 2887-2900.

[15] 杨帆, 张倩颖, 施智平, 等. 可信执行环境软件侧信道攻击研究综述[J]. 软件学报, 2023, 34(1): 381-403
YANG F, ZHANG Q Y, SHI Z P, et al. Survey on software side-channel attacks in trusted execution environment[J]. Journal of Software, 2021, 32(8): 2375-2391.

[16] BOGDANOV A, KNUDSEN L R, LEANDER G, et al. PRESENT: an ultra-lightweight block cipher[C]//Cryptographic Hardware and Embedded Systems-CHES 2007. Berlin: Springer, 2007: 450-466.

[17] SALLAM S, BEHESHTI B D. A survey on lightweight cryptographic algorithms[C]//Proceedings of the TENCON 2018 - 2018 IEEE Region 10 Conference. Piscataway: IEEE Press, 2018: 1784-1789.

[18] CHATTERJEE R, CHAKRABORTY R. A modified lightweight PRESENT cipher for IoT security[C]//Proceedings of the 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA). Piscataway: IEEE Press, 2020: 1-6.

[19] 唐明, 沈菲, 邓慧, 等. PRESENT 的多模型差分错误分析[J]. 计算机工程与科学, 2011, 33(10): 39-44.
TANG M, SHEN F, DENG H, et al. A multi-model differential fault analysis on PRESENT[J]. Computer Engineering & Science, 2011, 33 (10): 39-44.

[20] 陈伟建, 赵思宇, 邹瑞杰, 等. PRESENT 密码的差分故障攻击[J]. 电子科技大学学报, 2019, 48(6): 865-869.
CHEN W J, ZHAO S Y, ZOU R J, et al. The differential fault attack of PRESENT cipher[J]. Journal of University of Electronic Science and Technology of China, 2019, 48(6): 865-869.

[21] WANG C X, YU M Y, WANG J X, et al. A more practical CPA attack against PRESENT hardware implementation[C]//Proceedings of the 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems. Piscataway: IEEE Press, 2012: 1248-1253.

[22] ZHOU G, WU J. Hardware design of data acquisition and processing of digital IF receiver[C]//Proceedings of the 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet). Piscataway: IEEE Press, 2012: 2613-2615.

[23] KASSANOS P, SEICHEPINE F, YANG G Z. A comparison of front-end amplifiers for tetrapolar bioimpedance measurements[J]. IEEE Transactions on Instrumentation and Measurement, 2020, 70: 2000514.

[24] 肖晓明, 何为, 贺玉成. 基于生物电阻抗原理人体成分分析仪的设计与研究[J]. 中国医疗设备, 2015, 30(8): 9-13.
XIAO X M, HE W, HE Y C. Design and research of a human body composition analyzer based on the principle of bio-electrical resistance[J]. China Medical Devices, 2015, 30(8): 9-13.

[25] 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.

[26] PUTRA S D, SUMARI A D W, ASROWARDI I, et al. Power analysis in hamming weight model: attacking IoT encryption devices[C]//Proceedings of the 2021 4th International Conference on Signal Processing and Information Security (ICSPIS). Piscataway: IEEE Press, 2021: 41-44.

[27] BOEY K H, HODGERS P, LU Y X, et al. Security of AES Sbox designs to power analysis[C]//Proceedings of the 2010 17th IEEE International Conference on Electronics, Circuits and Systems. Piscataway: IEEE Press, 2010: 1232-1235.

[28] DOBRAUNIG C, EICHLSEDER M, MENDEL F, et al. ASCON: a new lightweight cryptographic algorithm for the Internet of things[J]. International Journal of Information Security, 2018, 17(5): 475-487.

[29] MARTINASEK Z, ZAPLETAL O, VRBA K, et al. Power analysis attack based on the MLP in DPA contest v4[C]//Proceedings of the 2015 38th International Conference on Telecommunications and Signal Processing (TSP). Piscataway: IEEE Press, 2015: 154-158.

[30] DING G L, ZHAO Q, CHU J, et al. Electromagnetic emanations of the ICs[C]//Proceedings of the 2007 International Symposium on Electromagnetic Compatibility. Piscataway: IEEE Press, 2007: 303-304.

[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。

冯毅（1999– ），男，回族，宁夏石嘴山人，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。

杨崇宇（1999– ），男，彝族，云南昆明人，云南大学硕士生，主要研究方向为嵌入式系统开发、物联网安全。

岳远康（1997– ），男，山东济宁人，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。

胡崇辉（1997– ），男，山东济宁人，云南大学硕士生，主要研究方向为物联网应用、嵌入式系统开发、物联网安全加密等。