基于塔域的通用循环移位掩码设计方法

严迎建 汪 晶* 刘燕江

(中国人民解放军战略支援部队信息工程大学 郑州 450001)

摘 要：该文分析了塔域的运算特性，提出了基于塔域分解的非线性变换实现方法，设计了求逆运算的随机掩码方案，利用循环移位对随机掩码进行移位变换，形成了基于塔域的循环移位随机掩码方案，实现了所有中间值的随机化隐藏，提高了算法的抗能量攻击能力。该文在高级加密标准(AES)算法上进行验证，利用T-test和相关性分析对掩码方案进行安全性评估。该掩码方案无明显信息泄露点，可有效抵抗相关性攻击，另外较现有文献的掩码方案，资源开销更小，通用性更好。

关键词：能量攻击；掩码；复合域；分组密码

中图分类号：TN918.4; TP309.7 **文献标识码**：A **文章编号**：1009-5896(2021)09-2489-09

DOI: 10.11999/JEIT210588

Design Method of Generic Cyclic Shift Mask Based on Tower Field

YAN Yingjian WANG Jing LIU Yanjiang

(*Information Engineering University, People's Liberation Army Strategic Support Force, Zhengzhou* 450001, *China*)

Abstract: The operation characteristics of the tower field is analyzed, a nonlinear transformation realization method based on the tower domain is proposed. A random mask schedule for the inversion operation is designed, and cyclic shift is used in the randomization of mask, forming cyclic shift random mask scheme based on the tower domain, realizing the randomized hiding of all intermediate values and improving the ability of the algorithm to resist power attacks. The method proposed is verified on the Advanced Encryption Standard (AES) algorithm with the use of T-test and correlation analysis to evaluate the security of the masking scheme. There is no obvious information leakage points in the schedule, proving the ability to effectively resist correlation attacks. In addition, compared with the mask schedule in existing reference, the mask schedule proposed in this paper has less resource overhead and better generality.

Key words: Power attack; Mask; Composite field; Block cipher

1 引言

侧信道分析技术是密码芯片在运行过程中面临的重要安全性威胁之一。自Paul Kocher提出简单能量攻击技术以来，各类侧信道攻击技术如相关能量攻击[1]、互信息分析[2]、矩相关差分攻击[3]、深度学习差分攻击[4]等被相继提出，广泛应用于密码算法的侧信道攻击领域。侧信道分析技术已经成为密码算法的主要安全性威胁之一。为了保证密码算法的安全性，安全防护方法层出不穷[5,6]，目前掩码方案以其严谨的数学推导被认为是最具信服力的安全防护技术[7,8]。然而，传统的掩码方案在提高安全性的同时也不可避免地增加了硬件资源开销，这严重限制了掩码方案的应用。

具体来说，旋转S盒掩码(Rotating S-box Mask, RSM)方案是一种易于软硬件实现的轻量级低熵掩码方案[9–11]，用于差分能量分析竞赛4.2版(Differential Power Analysis contest V4.2, DPA contest)[12]的高级加密标准(Advanced Encryption Standard, AES)抗侧信道攻击防护，得到国内外学者的广泛研究。然而，该方案在实现过程中也存在一些缺陷：(1)掩码固定，不能抵抗基于偏移量的1阶差分攻击[13]；(2)要预先计算并存储各个掩码所对应的S盒，增大面积开销和资源占用率。针对上述问题，国内外研究学者也提出了众多改进方案。文献[14]提出了S盒随机和汇编编写敏感模块等措施，但实现过程相对复杂；徐佩等人[13]提出了随机偏移量和多种掩码相结合的方法提高了算法的安全性，同时也提高了算法的复杂度与资源消耗；姜久兴等人[15]分析了RSM方案中掩码特点，提出了共

收稿日期：2021-06-16；改回日期：2021-07-15；网络出版：2021-08-18
*通信作者： 汪晶 cristal_97@163.com

用S盒的方案以减少查表实现S盒的计算数量，但应用范围相对有限。

为此，本文在RSM方案的基础上，基于塔域实现分组密码算法S盒加掩运算。对于运算较为复杂的求逆运算，通过同构映射，选择合适的不可约多项式，将GF(2^8)上的求逆运算转换到GF(2^4)，并将GF(2^4)上的求逆运算转换到GF(2^2)，以简化运算过程。基于塔域分解的思想，直接对加入掩码后的S盒进行运算，可避免对不同S盒的预先计算和存储，以节省硬件开销和资源占用。

2 现有掩码的非线性变换实现方式分析

掩码方法的实质是将敏感信息分布在不同的部分中。对掩码方法来说，主要分为掩码和掩码补偿计算。密码算法中的线性部分很容易添加掩码，而字节替代等非线性运算环节添加掩码较为复杂[16]。

针对分组密码算法的能量攻击，通常选择能量消耗较大的字节替代作为攻击点，因此S盒的计算是掩码方案中的关键部分。未防护S盒输入为x，输入掩码为m，输出掩码为n，在未防护S盒计算的基础上，加掩S盒的计算方式为

$$\mathrm{MSB}(x \oplus m) = \mathrm{SB}(x) \oplus n \tag{1}$$

与未防护S盒相比，加入随机数之后的S盒计算方式较为复杂。目前有3种实现方式：

(1)通过查找表的方式实现，预先计算不同掩码所对应的加掩S盒并存放在特定随机存取存储器(Random Access Memory, RAM)中，其计算方式如表1所示。

由上述算法可知，m,n的取值不同，所对应的加掩S盒也不同，且复杂度呈指数增长，另外所耗费的硬件资源也呈指数增长。因此，基于查找表的实现方式不适于加入随机掩码的加密算法。

(2)通过加法链的方式实现[17]，这种方法直接求元素的逆元。若x为GF(2^8)上的元素，则$x^{-1}=x^{254}$，其计算方式如表2所示。

从上述算法可知，基于乘法链的计算方法较为复杂，需择优选取运算方案，加入随机掩码之后，会使乘法链路运算更复杂，电路的性能大大下降。

表 1 加掩S盒计算算法

输入：m,n,x	
输出：MSB	
(1)	for i=0 to 255 do
(2)	$\mathrm{MSB}(x \oplus m) = \mathrm{SB}(x) \oplus n$
(3)	end for
(4)	Return MSB

表 2 加法链计算算法

输入：x		
输出：x^{254}		
(1)	$z \leftarrow x^2$	$[z=x^2]$
(2)	$y \leftarrow zx$	$[y=x^2x=x^3]$
(3)	$w \leftarrow y^4$	$[w=(x^3)^4=x^{12}]$
(4)	$y \leftarrow yw$	$[w=x^3x^{12}=x^{15}]$
(5)	$y \leftarrow y^{16}$	$[w=(x^{15})^{16}=x^{240}]$
(6)	$y \leftarrow yw$	$[w=x^{240}x^{12}=x^{252}]$
(7)	$y \leftarrow yz$	$[w=x^{252}x^2=x^{254}]$

(3)通过复合域实现[18]。GF(((2)^2)^2)^{2}可视为GF((2)^2)^{2}上的2维线性空间，因此，GF(((2)^2)^2)^{2}上的运算可转换为GF((2)^2)^{2}上的运算；同理，GF((2)^2)^{2}上的运算可转换为GF(2)^{2}上的运算，GF(2)^{2}上的运算可转换为GF(2)上的运算。通过逐级分解，可将GF(((2)^2)^2)^{2}上较为复杂的运算转换成GF(2)上的运算，这种明显层次的复合域结构称为塔域。

相较于查找表的实现方式和加法链的实现方式，基于复合域的实现方式结构更为简单，也更适于加入随机掩码之后的运算。因此，本文基于塔域开展随机掩码设计，在保证安全性的情况下，最大可能地降低了掩码算法的复杂度，进而降低了硬件开销。

3 基于塔域的加掩S盒设计方法

3.1 基于塔域的非线性变换分析

S盒是密码算法中的非线性环节，也是能量攻击中信息泄露较多的部分[7]。不同算法的S盒构造方法不同，其中基于有限域乘法逆的构造方法在密码算法的非线性环节中得到广泛应用，如AES, Camellia, SMS4等算法的S盒构造。基于有限域乘法逆的S盒由乘法逆复合仿射变换。不同算法具体构造不同，但结构相似，实现流程如图1所示。

以AES算法为例，AES的S盒由求逆运算和仿射变换两部分组成，其中，直接对GF(256)上的元素求逆相对复杂，故可通过同构映射δ实现有限域GF(256)中元素到复合域GF(((2)^2)^2)^{2}中的元素的映射，在复合域中完成求逆运算。具体实现方法如下：

设γ, γ^{16}为不可约多项式$g(x)$的根，GF(((2)^2)^2)^{2}上的元素A可表示为$A=a_1\gamma^{16}+a_0\gamma$，$a_1$，$a_0 \in$ GF((2)^2)^2。

$$\begin{aligned}A^{-1}=&v(A^{17})^{-1}A^{16}\\=&(AA^{16})^{-1}A^{16}\\=&((a_1\gamma^{16}+a_0\gamma)(a_0\gamma^{16}+a_1\gamma))^{-1}(a_0\gamma^{16}+a_1\gamma)\\=&(a_0^2+a_1^2)\gamma^{17}+a_0a_1(\gamma^2+\gamma^{32}))^{-1}\\&\cdot(a_0\gamma^{16}+a_1\gamma)\\=&((a_0+a_1)^2\gamma^{17}+a_0a_1(\gamma+\gamma^{16})^2)^{-1}\\&\cdot(a_0\gamma^{16}+a_1\gamma)\\=&((a_0+a_1)^2+a_0a_1(\gamma+\gamma^{16})^2)^{-1}(a_0\gamma^{16}+a_1\gamma)\\=&(a_0a_1+(a_0+a_1)^2\alpha^2\beta)^{-1}(a_0\gamma^{16}+a_1\gamma)\end{aligned}\tag{2}$$

记元素A的逆元为A^{-}，$A^{-1}=d_1\gamma^{16}+d_0\gamma$，$d_1$，$d_0\in\mathrm{GF}((2)^2)^2$，则

$$\left.\begin{aligned}d_0&=\{a_0a_1+(a_0+a_1)^2\lambda\}^{-1}a_1\\d_1&=\{a_0a_1+(a_0+a_1)^2\lambda\}^{-1}a_0\end{aligned}\right\}\tag{3}$$

其运算结构如图2所示，将$\mathrm{GF}(((2)^2)^2)^2$上的求逆运算转换成$\mathrm{GF}((2)^2)^2$上的乘方、常数乘和求逆运算。

同理，对于$\mathrm{GF}((2)^2)^2$上的元素求逆计算方法与上文相同，$\mathrm{GF}(2)^2$运算相对比较简单，逆元和平方和通过高低位互换即可实现。

3.2 基于塔域的加掩S盒设计方法

通过复合域结构可以简化求逆运算。为实现加密算法的抗能量攻击，需对运算中可能存在信息泄露的中间值进行随机化处理。利用复合域结构实现乘法逆运算的掩码防护是实现加掩S盒运算的关键。

对中间值X异或掩码M进行随机化，记为X'。经过A变换之后，$X'=X_0'\gamma+X_1'\gamma^{16}$，$\mathrm{M}=M_0\gamma+M_1\gamma^{16}$，$X=X_0\gamma+X_1\gamma^{16}$，其中，$X_0'=X_0+M_0$，$X_1'=X_1+M_1$。

S盒的输入是经过加掩防护的，欲使S盒中间值均加掩防护，需对求逆运算进行修正，修正后的求逆计算为

$$(X_0'\gamma+X_1'\gamma^{16})^{-1}=Y_0'\gamma+Y_1'\gamma^{16}\tag{4}$$

Y_0'和Y_1'为对求逆运算的输出值，分别用M_0和M_1进行加掩防护

$$\left.\begin{aligned}Y_0'&=M_0+X_1'D'^{-1}+X_1'M_2\\&\quad+D'^{-1}M_1+M_1M_2\\Y_1'&=M_1+X_0'sD'^{-1}+X_0'M_2\\&\quad+D'^{-1}M_0+M_0M_2\end{aligned}\right\}\tag{5}$$

其中，$M_2=(M_0+M_1)^2\times\lambda$，用于对$\mathrm{GF}(2^8)$上求逆运算中间值的加掩，$D'$为加掩后结果，其计算方式为

$$\begin{aligned}D'=&(X_1'+X_0')^2\times\lambda+X_1'\times X_0'+X_1'\times M_0\\&+X_0'\times M_1+M_0\times M_1\end{aligned}\tag{6}$$

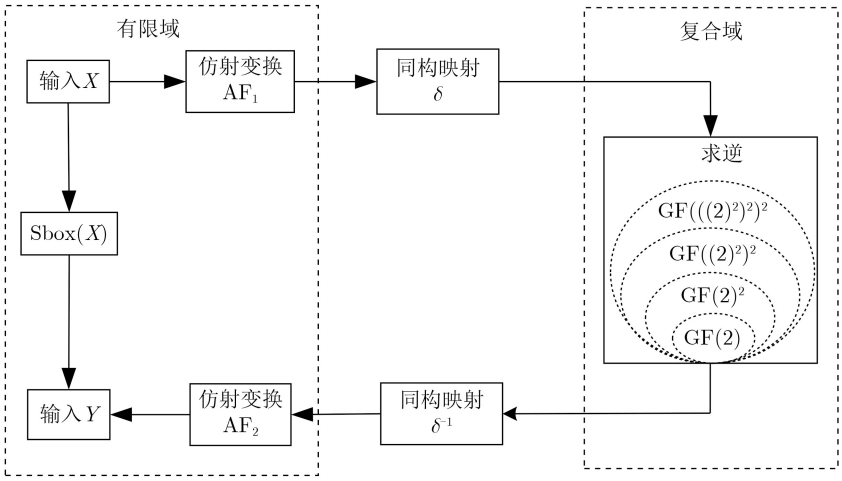

图 1 基于塔域的S盒运算结构

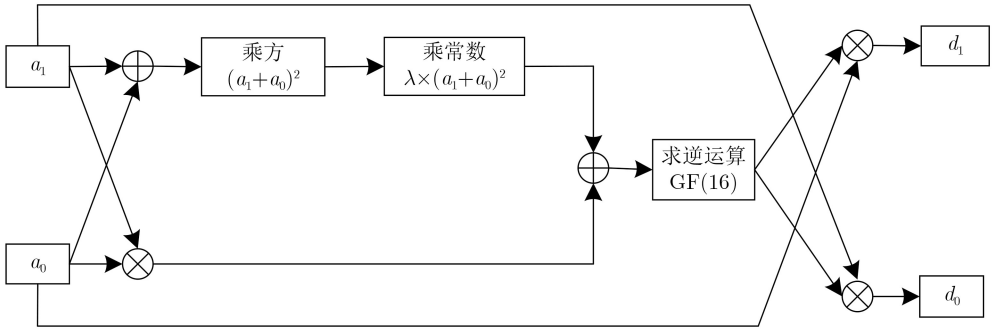

图 2 $\mathrm{GF}(((2)^2)^2)^2$上元素乘法逆计算结构图

对D'^{-1}的计算过程也要进行防护，$D'=d_0'\beta+d_1'\beta^4$，$M_2=m_0\beta+m_1\beta^4$，$D'^{-1}=d_0'^{-1}\beta+d_1'^{-1}\beta^4$，$m_0$和$m_1$分别用于$d_0'^{-1}$和$d_1'^{-1}$的随机化

$$\left.\begin{aligned} d_0'^{-1}&=m_0+d_1'\times k'^{-1}+d_1'\times m_2\\ &\quad+k'^{-1}\times m_1+m_1\times m_2\\ d_1'^{-1}&=m_1+d_0'\times k'^{-1}+d_0'\times m_2\\ &\quad+k'^{-1}\times m_0+m_0\times m_2 \end{aligned}\right\} \tag{7}$$

其中，$m_2=\alpha^2\times(m_0+m_1)$，用于对GF(2⁴)上求逆运算中间值的加掩，$k'$为加掩后的结果，计算方式为

$$\begin{aligned} k'=&(d_1'+d_0')^2\times\alpha+d_1'\times d_0'+d_1'\times m_0\\ &+d_0'\times m_1+m_0\times m_1 \end{aligned} \tag{8}$$

若$k'=a_0'\alpha+a_1'\alpha^2$，则$k'^{-1}=a_1'\alpha+a_0'\alpha^2$。

通过以上计算，求逆运算中的所有中间值都通过掩码进行随机化处理。

基于塔域实现加掩S盒的运算结构如图3所示，其中，x表示掩码防护前S盒的输入值，m表示输入值所加掩码，n表示输出值所加掩码。GF(2⁸)上的中间值和掩码先经过同构变换映射成塔域上的元素，然后参与GF(2⁴)上的乘方、常数乘和求逆运算，完成GF(2⁸)上元素的加掩。其中，GF(2⁴)上求逆运算与GF(2⁸)上求逆运算结构相同。

4 基于塔域的循环移位掩码设计及安全性分析

基于塔域的加掩S盒的实现方式对基于有限域乘法逆构造的S盒掩码防护具有通用性，并且对输入掩码的取值没有限制。本文基于RSM掩码开展防护技术研究，通过循环移位一个字节实现每一轮掩码的动态更新，以消除加密运算中间值组合与能量轨迹之间的相关性，并结合加掩S盒实现方法，进一步提高掩码随机性。本节以AES加密算法为研究对象，介绍了基于塔域的掩码方案实现方法并分析了安全性。另外，本方法可迁移到其他分组加密算法中，通用性好。

4.1 基于塔域的加掩AES-128算法设计

本文基于复合域的加掩防护方案无需预算查找表的值，可任意选择掩码输入，适用于具有S盒和线性扩散层的SPN结构分组密码。下面对提出的掩码方案进行详细描述。

设明文和密文均为$\mathrm{GF}(2^a)^t$上的元素，a，$t\in\mathrm{Z}^+$。S盒为GF(2^a)上的非线性函数，每一轮轮函数中有t个S盒操作。第r轮的输入数据记为X_r，密钥记为K_r，用M和N表示随机掩码，本方案中，N为M循环左移一个字节。P表示$\mathrm{GF}(2^a)^t$到$\mathrm{GF}(2^a)^t$的线性操作，τ_c表示向左循环移位c个字节，S表示轮函数的字节替代操作，$S_{(M,N)}$表示加入掩码运算之后的每一轮字节替代操作，计算方式为$S_{(M,N)}(X)=S(X\oplus M)\oplus N$，加掩S盒使用上文所提基于复合域的方式实现。基于塔域的循环移位掩码方案如表3所示。

本文以AES-128算法为例对所提方案进行应用。AES算法SP结构的分组加密算法，混乱层为字节替代，扩散层由行移位、列混合、圈密钥加组成。

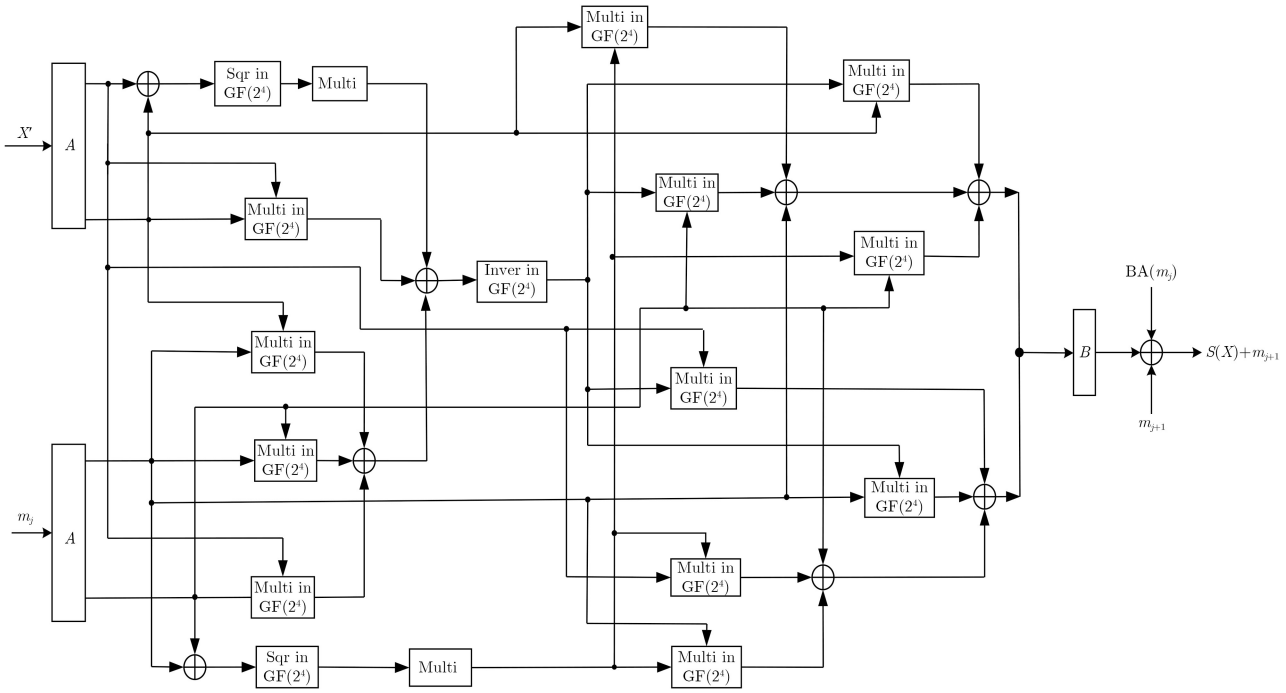

图 3 基于塔域AES加掩S盒硬件实现

基于塔域的循环移位AES-128加掩算法如图4所示。其中，SB表示16个字节的字节替代，每个字节作为加掩S盒的输入，S盒采用3.2小节提出的基于塔域的加掩S盒实现方式；SR表示行移位操作；MC表示列混合操作。之后对掩码进行修正，MMS为前9轮加密的掩码修正值，实现上一轮线性运算部分掩码的消除和下一轮掩码的添加；MS为最后一轮的掩码修正值，其值为输出掩码列混合之后的值。输出掩码为输入掩码循环左移1个字节之后的值。

4.2 安全性分析

密码算法在处理与明文和密钥相关的中间值的过程中会产生信息泄露，差分能量攻击就是利用这些泄露进行密钥恢复。本文针对能量攻击中应用最广泛的差分能量攻击对本文的掩码方案进行安全性分析。依赖于明文Z和密钥K的中间变量称为敏感变量，记为Z。将加密过程中的一个运算记为g，如S盒运算或者异或等，则Z可表示为$Z=g(X,K)$。其中，X和g均为已知，Z的信息泄露则意味着密钥K的信息泄露。

文献[19]提出了抵抗差分攻击的评估指标最优预测相关系数ρ_{opt}，该指标表明组合函数和预测函数之间的最大相关性

$$\rho_{\text{opt}}^{(d)}=\frac{\sigma\left(\mathrm{E}[\left(\mathrm{HW}(Z\oplus M)-\frac{n}{2}\right)^{d}|Z]\right)}{\sigma\left(\left(\mathrm{HW}(Z\oplus M)-\frac{n}{2}\right)^{d}\right)} \tag{9}$$

其中，$\mathrm{E}(x)$表示随机变量x的期望，$\mathrm{E}(x|y)$表示条件期望，$\sigma(x)$表示方差。在此基础上，文献[9]对RSM算法的安全性进行了分析，即1阶和2阶的最优预测相关系数均为0。

当d=1时，对密码算法的抗1阶差分能量攻击的能力进行分析

$$\begin{aligned}\rho_{\text{opt}}^{(1)}=&\frac{\mathrm{Var}\left(\mathrm{E}\left[\left(\mathrm{HW}(Z\oplus M)-\frac{n}{2}\right)|Z\right]\right)}{\mathrm{Var}\left(\mathrm{HW}(Z\oplus M)-\frac{n}{2}\right)}=\frac{\mathrm{E}^2\left(\frac{-1}{2}\sum_{i=1}^{n}(-1)^{(z\oplus m)_i}\right)-\mathrm{E}\left(\frac{-1}{2}\sum_{i=1}^{n}(-1)^{(z\oplus m)_i}\right)^2}{\mathrm{E}\left(\mathrm{E}\left[\frac{-1}{2}\sum_{i=1}^{n}(-1)^{(z\oplus m)_i}|Z\right]\right)^2-\mathrm{E}^2\left(\mathrm{E}\left[\frac{-1}{2}\sum_{i=1}^{n}(-1)^{(z\oplus m)_i}|Z\right]\right)}\\=&\frac{1}{n}\sum_{i=1}^{n}\left(\frac{1}{\mathrm{Card}[M]}\sum_{m\in M}(-1)^{m_i}\right)^2\end{aligned} \tag{10}$$

本方案中$n=8$，m服从均匀分布，可知$\sum_{m\in M}(-1)^{m_i}=0$，则$\rho_{\text{opt}}^{(1)}=0$。故在实施1阶CPA攻击时，预测中间值与功耗泄露之间的最大相关系数为0，即不能通过计算相关系数计算出正确密钥值。

当d=2时，对密码算法的抗2阶差分能量攻击的能力进行分析

$$\begin{aligned}\rho_{\text{opt}}^{(2)}=&\frac{\mathrm{Var}\left(\mathrm{E}\left[\left(\mathrm{HW}(Z\oplus M)-\frac{n}{2}\right)^2|Z\right]\right)}{\mathrm{Var}\left(\left(\mathrm{HW}(Z\oplus M)-\frac{n}{2}\right)^2\right)}\\=&\frac{1}{n(n-1)}\\&\cdot\left(\frac{1}{\mathrm{Card}[M]^2}\sum_{m,m'}\left(\sum_{i}(-1)^{(m\oplus m')_i}\right)^2-n\right)\end{aligned} \tag{11}$$

RSM方案依据以上条件对掩码选择进行约束，并用SAT-solver方法求解出符合条件的掩码值，因而也导致许多针对这一攻击的方法产生。本文所提方案对掩码不满足约束条件，即$\rho_{\text{opt}}^{(2)}\neq 0$。高阶侧信道安全的定义：

定义1　如果加密算法的中间变量的任何d元组都独立于与密钥相关的敏感变量，那么它就可以实现d阶SCA安全性。

基于以上定义，下面分别对所提方案的抗差分能量攻击的安全性进行分析。

设加密运算中间值$u\in\mathrm{GF}(2^n)$，掩码m服从$\mathrm{GF}(2^n)$中的均匀分布，$u'=u\oplus m$为加掩之后的结果。用$P(A)$表示事件A发生的概率，α和β分别表示u'和u的任意取值，则

表 3　基于塔域的循环移位掩码加密算法

输入：明文X_0，密钥K

输出：密文X''_{R+1}

(1)　计算第1轮的输入数据X'_1，

$X'_1=X_0\oplus K_0\oplus M$

(2)　计算轮函数的输出

for r=1 to R–1,
$X''_{r+1}=P(S_{(M,N)}(X'_r))\oplus K_r$
$X'_{r+1}=X''_{r+1}\oplus(\tau_{c_r+1}(M)\oplus P(\tau_{c_r}(N)))$
$c_{r+1}=(c_r+1)\bmod t$

(3)　计算密文X''_{R+1}
$X''_{R+1}=S_{(M,N)}(X'_R)\oplus K_R$
$X'_{R+1}=X''_{R+1}\oplus\tau_{c_{R+1}}(N)$

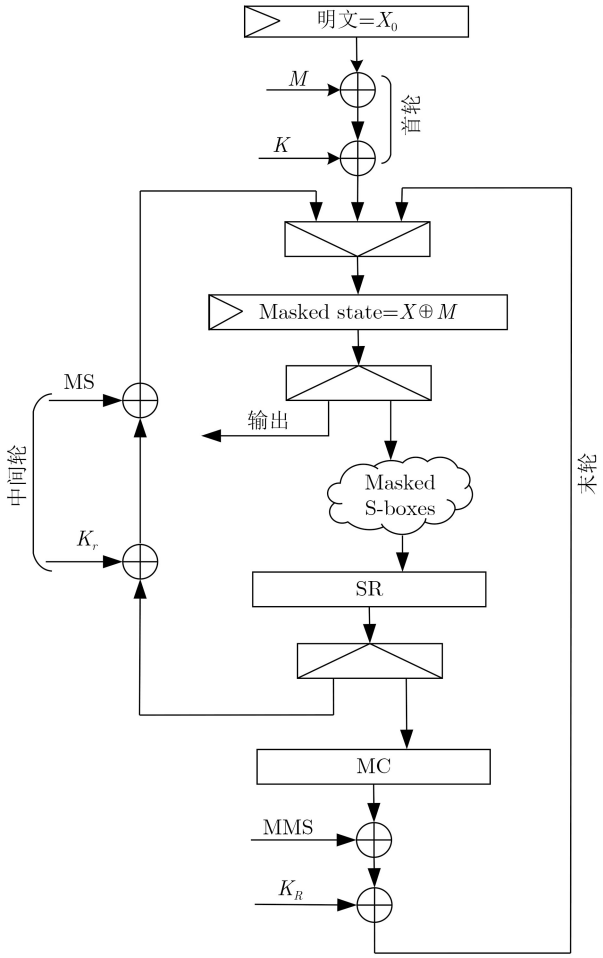

图 4 基于塔域的AES-128加掩算法

$$P(u'=\beta|u=\alpha)=P(m=\alpha\oplus\beta)=\frac{1}{2^n} \tag{12}$$

因而加密计算中的任意中间值也服从随机分布，故中间值的概率分布与密钥无关，不能通过1阶差分能量攻击的方式实现密钥的正确猜测。

设$u_i^{'}$和$u_j^{'}\in \mathrm{GF}(2^n)$分别为两个经掩码防护之后的中间值，$u_i^{'}=u_i\oplus m_i$，$u_j^{'}=u_j\oplus m_j$，则$u_i^{'}$和$u_j^{'}$的联合分布概率为

$$\begin{aligned}P(u'_i=&\alpha_i,u'_j=\alpha_j)\\=&P(m_i=u_i\oplus\alpha_i,m_j=u_j\oplus\alpha_j)\\=&P(m_i=u'_i,m_j=u'_j)\\=&P(m_i=u'_i)P(m_j=u'_j)\\=&\frac{1}{2^n}\end{aligned} \tag{13}$$

由上述推导可知，两个经掩码防护之后的中间值的任意组合服从随机均匀分布，独立于和密钥相关的敏感变量。即不能通过计算两个中间变量的组合实现2阶差分能量攻击。

5 结果分析

5.1 功能仿真分析

为验证基于塔域的高级加密标准加掩算法的正确性，用Verilog HDL语言对本文所提方案进行编码，并用VCS对其进行功能仿真。本文所提加掩方案的AES算法的功能仿真波形如图5所示。

进行功能仿真时，选用的密钥为0x0011_2233_4455_6677_8899_aabb_ccdd_eeff，明文为0x0123_4567_89ab_cdef_0123_4567_89ab_cdef，掩码随机选择，所得加密结果为0x363e_ff6c_de1a_dea8_b244_ad2e_3c4e_bdc8，所得结果与未加防护AES计算结果相同，因此可以验证本文所提加掩方案的功能正确性。

5.2 资源占用评估

除字节替换部分采用不同实现方式以外，其他模块实现方式均相同。对无防护的AES算法、基于RSM加掩方案的AES算法、基于塔域的加掩AES算法进行Verilog编程，并用Vivado软件进行综合，综合结果如表4所示。

由表4可知，本文所提基于塔域的AES掩码防护方案占用的查找表资源为2918，相较于RSM方案和S盒共用掩码方案，分别减少了72.52%和25.12%；在触发器占用方面，本方案使用的触发器数目为394，相较于无防护的AES算法减少了35.30%，相较于RSM方案和S盒共用掩码方案均减少了46.54%。总的来说，本方案在查找表和触发器方面的占用均小于现有方案，因此本方案的面积开销更小。

5.3 抗能量攻击验证

5.3.1 实验平台

本文建立了能量攻击平台来评估方法的有效性，具体结构如图6所示。能量攻击平台包括PC、SAKURA-G开发板和LeCory示波器。PC发送和接收明密文，同时示波器采集芯片加密运行过程中的能量轨迹并保存，利用Python语言对采集的数据进行分析，评估掩码方案的抗能量攻击能力。

图 5 基于塔域的循环移位加掩AES功能仿真图

表 4　不同方案总综合结果比较

方案	LUT	FF	BUFG
无防护AES	1245(303600)	609(607200)	1(32)
RSM方案[9]	10620(303600)	737(607200)	1(32)
S盒共用掩码方案[15]	3897(303600)	737(607200)	1(32)
本文方案	2918(303600)	394(607200)	1(32)

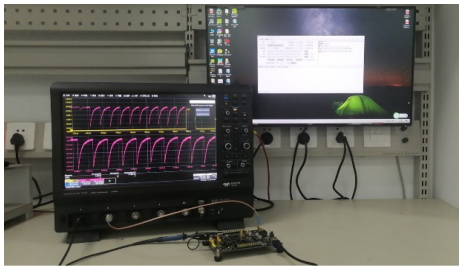

图 6 波形采集设备连接图

5.3.2　基于t检验的能量泄露评估

t检验是统计学中用来检验2个未知方差正态总体均值关系的假设检验方法。以t检验为理论基础的侧信道信息泄露评估方法具有简单、快捷、可靠，并且不需要掌握密码算法具体实现细节的优点。通过t检验计算结果可以评估功耗轨迹泄露大小和泄露位置，若t检验值的绝对值大于4.5，则可判断存在明显泄露。对无防护的AES算法和本文所提掩码方案的AES算法功耗轨迹进行t检验的结果如图7所示。

从图7可知，相较于未加防护措施的AES算法，加掩防护的AES功耗轨迹t检验的计算值更小，且绝对值均小于4.5，另外各采样点的t值差别较小，表明防护后的功耗曲线信息泄露较小且泄露区间不明显。

5.3.3　相关能量攻击分析

防护前后的算法均在FPGA上实现，因而采用汉明距离模型进行攻击。计算上一次加密的密文和此次加密的明文与密钥之间的异或值之间的汉明重量值作为假设中间值，选择一个字节的密钥作为分析对象，则有$2^8=256$种可能，对于每一种猜测密钥，计算假设中间值与功耗轨迹之间的相关系数，相关系数最大的值所对应的猜测密钥值即为正确密钥。理论上，以0.999的置信度区分相关系数为0和0.1至少需要1802条功耗轨迹，实际上能量攻击所需功耗轨迹与信噪比、攻击模型、预处理方式等也密切相关。实验过程中，选用2000条功耗轨迹对未加防护的AES算法进行分析，可得出正确密钥，实验结果如图8所示；选用20000条功耗轨迹基于塔域的加掩AES算法进行相关能量攻击，结果如图9所示。

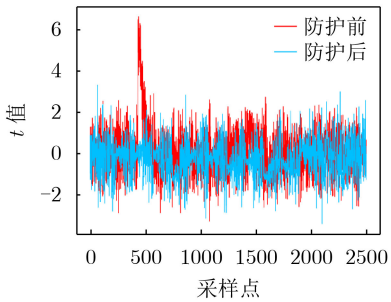

图 7 有无防护AES功耗轨迹t检验结果

实验选用AES算法的单个字节的密钥作为攻击对象(密钥值为0x0123456789ABCDEFFEDCBA9876543210)，从图8和图9可知，对于未加防护措施的AES算法，分析各猜测密钥与功耗曲线的相关系数，相关系数最大值所对应值即为猜测密钥，16个字节的计算密钥分别为0x0123456789ABCDEFFEDCBA9876543210，猜测值与正确值相同，即攻击成功。对于基于塔域的加掩AES防护方案，其计算相关系数值明显小于前者，几乎接近于0，所得猜测密钥为0xFBDD690DD4B64ABCD155C79595010A7B，与正确值不同，说明不能通过相关能量攻击的方法获取密钥。

6　结论

本文提出了一种基于塔域的AES循环移位掩码方案，通过塔域分解简化求逆运算，使用随机掩码及循环移位方案提高算法安全性。从理论上分析算

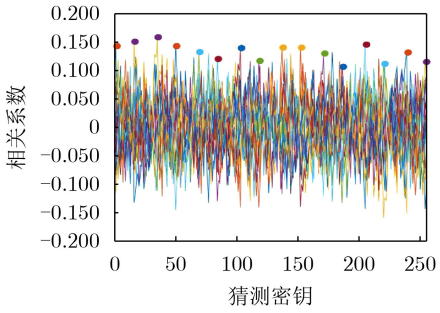

图 8 无防护AES相关能量攻击结果

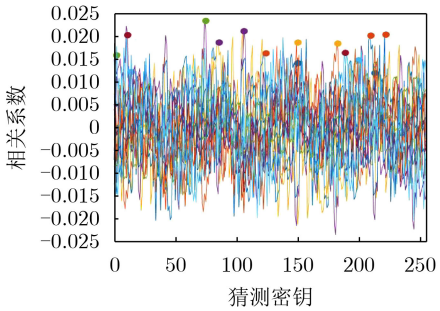

图 9 本文所提防护方案AES相关能量攻击结果

法抗能量攻击性能，并从功能仿真、资源占用和能量攻击方面对算法设计进行试验验证。与文献[9,15]相比，本文设计算法在硬件开销和安全性方面均有优势。另外，本文所提掩码实现方案适用于所有S盒运算可分解为求逆运算的密码算法，可提高分组加密算法的安全性、降低算法的硬件资源和实现成本。

参 考 文 献

[1] KOCHER P C, JAFFE J, and JUN B. Differential power analysis[C]. The 19th Annual International Cryptology Conference on Advances in Cryptology, Berlin, Germany, 1999: 388–397.

[2] BRIER E, CLAVIER C, and OLIVIER F. Correlation power analysis with a leakage model[C]. The 6th International Workshop Cambridge, Cambridge, UK, 2004: 16–29.

[3] DURVAUX F and STANDAERT F X. From improved leakage detection to the detection of points of interests in leakage traces[C]. The 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, 2016: 240–262. doi: 10.1007/978-3-662-49890-3_10.

[4] TIMON B. Non-profiled deep learning-based side-channel attacks with sensitivity analysis[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2019, 2019(2): 107–131.

[5] DELGADO-LOZANO I M, TENA-SÁNCHEZ E, NÚÑEZ J, *et al*. Projection of dual-rail DPA countermeasures in future FinFET and emerging TFET technologies[J]. *ACM Journal on Emerging Technologies in Computing Systems*, 2020, 16(3): 1–16. doi: 10.1145/3381857.

[6] 黄海, 冯新新, 刘红雨, 等. 基于随机加法链的高级加密标准抗侧信道攻击对策[J]. 电子与信息学报, 2019, 41(2): 348–354. doi: 10.11999/JEIT171211.

HUANG Hai, FENG Xinxin, LIU Hongyu, *et al*. Random addition-chain based countermeasure against side-channel attack for advanced encryption standard[J]. *Journal of Electronics & Information Technology*, 2019, 41(2): 348–354. doi: 10.11999/JEIT171211.

[7] SHAHMIRZADI A R, BOŽILOV D, and MORADI A. New first-order secure AES performance records[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021, 2021(2): 304–327.

[8] 王立辉, 闫守礼, 李清. 一种轻量级数据加密标准循环掩码实现方案[J]. 电子与信息学报, 2020, 42(8): 1828–1835. doi: 10.11999/JEIT190870.

WANG Lihui, YAN Shouli, and LI Qing. A lightweight implementation scheme of data encryption standard with cyclic mask[J]. *Journal of Electronics & Information Technology*, 2020, 42(8): 1828–1835. doi: 10.11999/JEIT190870.

[9] NASSAR M, SOUISSI Y, GUILLEY S, *et al*. RSM: a small and fast countermeasure for AES, secure against 1st and 2nd-order zero-offset SCAs[C]. The 2012 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, 2012: 1173–1178. doi: 10.1109/DATE.2012.6176671.

[10] BHASIN S, DANGER J L, GUILLEY S, *et al*. A low-entropy first-degree secure provable masking scheme for resource-constrained devices[C]. The Workshop on Embedded Systems Security, Quebec, Canada, 2013: 1–10. doi: 10.1145/2527317.2527324.

[11] GROSSO V, STANDAERT F X, and PROUFF E. Low Entropy Masking Schemes, Revisited[M]. FRANCILLON A and ROHATGI P. Smart Card Research and Advanced Applications. Cham: Springer, 2013, 8419: 33–43.

[12] MARTINASEK Z, IGLESIAS F, MALINA L, *et al*. Crucial pitfall of DPA contest V4.2 implementation[J]. *Security and Communication Networks*, 2016, 9(18): 6094–6110. doi: 10.1002/sec.1760.

[13] 徐佩, 傅鹏. 防止差分功耗分析攻击的软件掩码方案[J]. 计算机应用研究, 2016, 33(1): 245–248. doi: 10.3969/j.issn.1001-3695.2016.01.057.

XU Pei and FU Li. Software-implemented mask scheme against differential power analysis attack[J]. *Application Research of Computers*, 2016, 33(1): 245–248. doi: 10.3969/j.issn.1001-3695.2016.01.057.

[14] BHASIN S, BRUNEAU N, DANGER J L, *et al*. Analysis and improvements of the DPA contest v4 implementation[C]. The 4th International Conference, Pune, India, 2014: 201–218.

[15] 姜久兴, 厚娇, 黄海, 等. 低面积复杂度AES低熵掩码方案的研究[J]. 通信学报, 2019, 40(5): 201–210.

JIANG Jiuxing, HOU Jiao, HUANG Hai, *et al*. Research on area-efficient low-entropy masking scheme for AES[J]. *Journal on Communications*, 2019, 40(5): 201–210.

[16] DUC A, FAUST S, and STANDAERT F X. Making masking security proofs concrete (or how to evaluate the security of any leaking device), extended version[J]. *Journal of Cryptology*, 2019, 32(4): 1263–1297. doi: 10.1007/s00145-018-9277-0.

[17] AHN S and CHOI D. An improved masking scheme for S-Box software implementations[C]. The 16th International Workshop, Jeju Island, South Korea, 2016: 200–212. doi: 10.1007/978-3-319-31875-2_17.

[18] SINGH A, PRASAD A, and TALWAR Y. Compact and Secure S-Box Implementations of AES—A Review[M]. SOMANI A K, SHEKHAWAT R S, MUNDRA A, *et al*. Smart Systems and IoT: Innovations in Computing. Singapore: Springer, 2020.

[19] PROUFF E, RIVAIN M, and BEVAN R. Statistical analysis of second order differential power analysis[J]. *IEEE Transactions on Computers*, 2009, 58(6): 799–811. doi: 10.1109/tc.2009.15.

严迎建：男，1973年生，教授，研究方向为安全专用芯片设计技术、侧信道分析等.

汪　晶：女，1997年生，硕士生，研究领域为安全专用芯片设计技术、侧信道分析.

刘燕江：男，1990年生，博士后，研究领域为安全专用芯片设计技术、侧信道分析和硬件木马检测等.

责任编辑：余　蓉