# 一种基于随机求反的 S 盒抗 DPA 攻击安全结构

胡晓婷[1],戴泽龙[1*],覃中平[2],巩 固[1]
(1. 江苏师范大学 计算机科学与技术学院,江苏 徐州 221000;
2. 华中科技大学软件学院,湖北 武汉 430070)

**摘 要**:DPA 攻击(差分功耗攻击)作为一种重要的侧信道攻击方法,因其成功率较高而成为加密算法面临的主要威胁之一。S 盒是分组加密算法(高级加密标准(AES)、国产商业密码(SM4)等)中唯一的非线性运算,很大程度上决定了相关加密算法的安全性。S 盒的实现主要分为:查表法、组合逻辑和复合域方法。复合域方法因将 S 盒中的 GF(28)域上的求逆运算分解到低阶域上而使其硬件实现具有高性能、低面积等优势。该文提出了一种基于随机求反的复合域 S 盒抗 DPA 攻击安全结构,并据此设计了两类抗 DPA 攻击的 AES 安全结构:一种是基于随机取反的 AES 安全结构(RC-AES 安全结构),另一种是基于随机取反与一阶掩码结合的 AES 安全结构(RC-M-AES 安全结构)。实验证明,相较于已知文献中基于掩码保护的 AES,该文提出的 RC-AES 结构只需增加微小的面积开销就能有效抵抗 DPA 攻击,展现出显著的面积优势。同时,RC-M-AES 安全结构能在微小面积开销下,构建出比单独掩码方案更安全的密码芯片结构。此外,提出的 S 盒安全结构不仅适用于 AES,也适用于任何以替换函数作为唯一非线性运算的加密算法,具有较好的通用性。

**关键词**:复合域;S 盒;随机求反;抗 DPA 攻击;安全结构;高级加密标准
**中图分类号**:TP309.2;TN918.4 **文献标识码**:A **文章编号**:1673-629X(2024)11-0109-08
doi:10.20165/j.cnki.ISSN1673-629X.2024.0229

# A Secure Structure of S-Box Against DPA Attack Based on Random Complement

HU Xiao-ting[1],DAI Ze-long[1*],QIN Zhong-ping[2],GONG Gu[1]
(1. School of Computer Science and Technology,Jiangsu Normal University,Xuzhou 221000,China;
2. School of Software,Huazhong University of Science and Technology,Wuhan 430070,China)

**Abstract**:As an important side channel attack method,DPA attack (differential power analysis attack) has become one of the main threats to encryption algorithms due to its high success rate. In the block cipher algorithms (AES,SM4,etc.),S-box is the only one non-linear operation,which significantly influences the security of the corresponding encryption algorithms. Typically,there are usually three methods that can be employed to implement S-Box: look-up table method, combination logic, and composite field method. Comparatively,composite field method can offer advantages in hardware implementation such as high performance and low area by decomposing the inversion operation on GF(28) in S-Box into a low-order field. We propose a composite field S-box secure structure against DPA attack based on random complement,and accordingly design two types of AES security structures against DPA attacks. One is based on random complement of S-box (RC-AES),the other is based on the combination of random complement of S-box and first-order masking (RC-M-AES). Experimental results demonstrated that RC-AES structure can effectively anti-DPA attacks with only a small increase in area overhead compared with AES based on masking protection in known literatures. It implies that the proposed RC-AES structure has a significant area advantage. At the same time,RC-M-AES structure can gain a higher security by combining random complement and first-order masking with a small area overhead compared with that based on pure masking technology. Furthermore,the proposed S-box secure structure has good generality,and it can be applied to not only AES but also any encryption algorithm using substitution functions to be the only non-linear operation.

**Key words**:composite field;S-box;random complement;anti-DPA attack;secure structure;advanced encryption standard (AES)

**收稿日期**:2024-03-11 **修回日期**:2024-07-12
**基金项目**:江苏师范大学博士基金项目(20XSRX014)
**作者简介**:胡晓婷(1977-),女,博士,讲师,研究方向为密码芯片安全结构设计;通信作者:戴泽龙(2000-),男,硕士研究生,研究方向为密码芯片安全结构设计。

## 0 引 言

侧信道攻击是一种利用加密设备在加密过程中产生的物理特征信息(如电磁泄漏、时间延迟、功耗变化等)来获取加密数据的方法。差分功耗分析(Differential Power Analysis,DPA)攻击是常用的侧信道攻击之一。它基于电路功耗和信号处理之间的关联,在攻击过程中,通过测量和分析加密设备在不同操作时的功耗,从中推断出设备执行的操作和中间数据。DPA 自发表以来[1-2],已经被成功用于恢复多个未受保护的密码算法的密钥,如 DES、RSA、AES 等,给密码算法安全带来严重威胁。因此,寻找能够抵抗 DPA 攻击的方法具有重要意义。

分组加密算法(如 AES、SM4 等)中 S 盒作为唯一的非线性运算,很大程度上决定了算法的安全性。因此,设计抗 DPA 攻击的 S 盒安全结构对提高密码算法的安全性至关重要。目前,S 盒的硬件实现主要采用三种方法:基于直接映射(查表法,LUT)的实现、基于组合逻辑代数表达式的实现[3]和基于复合域算法的实现[4]。其中,基于 LUT 的方法具有电路结构简单,关键路径延时较低等优点,但因需要使用较大的 ROM 单元来存放 S 盒和逆 S 盒,导致其电路面积开销大,且 ROM 的速度较慢、带宽有限,数据的读取速度在很大程度上限制了系统的性能。基于组合逻辑的 S 盒由真值表直接导出的逻辑表达式来实现,不需要涉及到复杂的域操作,但因逻辑表达式比较复杂,需要大量的逻辑门来实现,资源开销较大。第三种基于复合域上的 S 盒实现则通过将高阶域上的运算分解到低阶域,从而简化了 S 盒运算中的求逆操作,有效减少了 S 盒的面积开销,此外,这种方法也丰富了 S 盒的设计,提高了 S 盒的安全性[5],因此近年来备受研究者关注。

复合域 S 盒的实现性能依赖于分解后所使用的低阶域及表示基。2001 年,Satoh 等人[6]提出了 AES S 盒的紧凑实现,该实现基于多项式基(Polynomial Basis,PB)表示的塔域 GF(((2²)²)²)。Canright[7]通过使用正规基(Normal Basis,NB)表示进一步减少了 S 盒的门数。最近,Nogami 等人[8]提出了一种基于混合基(Mixed Basis,MB)的 AES 的高效实现方案,有效降低了求逆电路的门数和延时。与前几种基于 GF(((2²)²)²)的方法不同,Jeon 等人[9]提出了基于 GF((2⁴)²)的求逆方案,该方案通过资源共享有效降低了异或门的数量。上述几种方案都使用非冗余形式(即 m 比特)表示 GF(2ᵐ)上的元素。Nekado 等人[10]则提出了 GF((2⁴)²)上基于冗余表示基(Redundantly Represented Basis ,RRB[11])的高效求逆方案。Ueno 等人[12-14]结合 NB、RRB、PRR[15](Polynomial Ring Representation,PRR)三种表示基,提出了一种复合域 GF((2⁴)²)上的 S 盒实现方法,该方案目前在 GF((2⁴)²)域上是最高效的。

然而,以上文献提出的结构主要聚焦在复合域 S 盒的高效实现,没有考虑结构的抗攻击能力。众所周知,S 盒作为影响主流密码算法安全性的关键操作之一,其抗攻击的实现也是 S 盒研究中的重要分支[16-18]。目前抗攻击的复合域 S 盒结构主要基于两类技术:门限技术[19-21]和掩码技术[22-25]。门限技术最早由 Nikova 等人[19]提出,该方案将输入变量分割成多个份额,并通过布尔掩码将目标函数划分为若干分量函数。每个分量函数仅依赖于部分输入份额,这样即使攻击者获取 $d$ 个份额,也无法仅凭这些信息直接计算出完整的中间值,这在理论上保证了在 $d$ 阶 DPA 下的安全性。Ueno 等人[20]在此基础上提出了一种更高级的门限方案,通过引入随机数的方式,构建了基于门限技术的 Native-AES 安全结构,提高了加密算法的安全性。蒲金伟等人[21]引入了面向域的方法,降低了 Native-AES 结构中的随机数消耗,并通过优化加密顺序,提高了门限 AES 的加密速度。尽管门限技术能够为硬件电路提供高安全性,但其所需要的面积开销通常是未加保护的结构的倍数,相比之下,掩码技术所需面积开销更小,应用更加广泛。掩码技术通过在算法执行过程中引入随机掩码,改变中间值的敏感数据,使得 DPA 获取错误的数据。掩码技术在复合域上的应用,既有效控制了 S 盒的面积开销,又有效增强了电路的安全性。

复合域掩码技术最早由 Oswald 等人[22]提出,该方案使用基于 PB 的复合域 GF(((2²)²)²)掩码方案保护 AES 抵抗侧信道攻击。为减少面积开销,Zakeri 等人[23]通过使用 NB 对 Oswald 等人提出的方案进行优化,有效降低了运算复杂度。最近,姜久兴等人[24]提出了基于复合域通用高阶掩码的防护方案,通过关键模块复用有效降低了复合域 S 盒求逆算法的复杂度,从而获得了较佳的性能。姜佳怡等人[25]提出一种新型掩码算法,通过引入全掩码技术,有效提升了算法硬件实现的抗功耗攻击能力。但以上两种方案都是基于 PB 的 GF(((2²)²)²)实现的,不能直接用于 NB、MB 表示的 S 盒实现上。

该文对复合域 S 盒的构造进行研究,提出了一种通用的基于随机求反的复合域 S 盒安全结构,该方案在不改变求逆操作的前提下,通过随机在同构映射之后和逆同构映射之前加入特定操作,将 S 盒中的求逆结果随机取反,进而影响其瞬时输出数据与电路功耗之间的关联性,提升电路的抗 DPA 攻击能力。与一阶掩码方案相比,该方案面积开销更小,且能和高阶掩码方案进行结合,进一步降低加密数据与功耗之间的相

关性,增强加密电路抗 DPA 攻击的性能。

具体来说,该文主要贡献如下:

(1)提出了一种通用的基于随机求反的复合域 S 盒抗 DPA 攻击安全结构。

(2)基于该文提出的 S 盒结构,设计实现了一个抗 DPA 攻击的 AES 电路,硬件综合和安全性分析结果表明,该文设计实现的 AES 安全结构在面积开销较小的情况下就能有效抵抗 DPA 攻击。

(3)将该方案和文献[24]中提出的 S 盒高阶掩码方案结合,提出了基于随机取反与一阶掩码结合的 AES 安全结构。实验结果表明,该方案通过微小的面积开销构建出比掩码方案更安全的密码芯片结构。

## 1　复合域 S 盒实现原理

有限域上 S 盒的实现由求逆和仿射两个部分构成。在具体实现过程中,基于 GF($2^8$)上非零元素 $a$ 的求逆等价于求解 $a^{254}$(0 的求逆为 0),其计算需要大量的时间和面积开销。复合域 S 盒上的求逆操作通过将高阶域上的运算分解到低阶域上,降低了运算的复杂度。

其原理是首先通过同构变换 $f$ 将 GF($2^8$)上的元素 $a$ 映射到复合域 GF(($2^4$)$^2$)上的 $q$,然后在复合域 $F$(($2^4$)$^2$)域上求解 $q$ 的逆元 $q^{-1}$,最后通过逆同构变换 $f^{-1}$ 将元素 $q^{-1}$ 映射回 GF($2^8$),得到 $a$ 的逆元 $a^{-1}$。在这个过程中,求解 $q^{-1}$ 的过程可以被简化为 GF($2^4$)上的运算组合,显然,GF($2^4$)上的 4 比特运算,其复杂程度比 8 比特运算的复杂度低很多。例如,假定 $a \in$ GF($2^8$),$q \in$ GF(($2^4$)$^2$)是 $a$ 在 GF(($2^4$)$^2$)的映射元素,在基于多项式基表示的 GF(($2^4$)$^2$)上,$q^{-1}$ 可以表示为 $(b,c)^{-1} = (d^{-1}b, d^{-1}(b+c))$,其中 $b$、$c$ 分别表示 $q$ 的高 4 位和低 4 位,$d = b^2\lambda + bc + c^2$,这里求解 $d^{-1}$ 的运算在 GF($2^4$)上进行,运算复杂度降低。复合域 S 盒基本实现流程如图 1 所示。

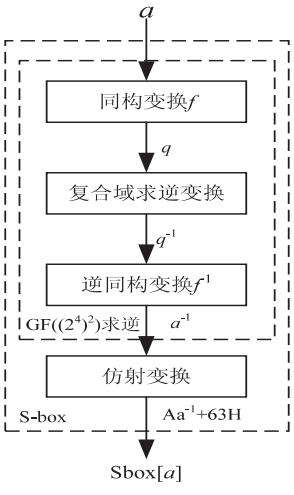



图 1　复合域 S 盒实现流程

## 2　提出的基于随机求反的 S 盒抗 DPA 攻击安全结构

### 2.1　基于随机求反的 S 盒安全结构

从复合域 S 盒的构造上出发,对变换矩阵(同构矩阵和逆同构矩阵)的性质进行研究,利用加密算法中相邻两轮之间的变换关系,提出了一种抗侧信道攻击的安全结构,它在不改变求逆操作的基础上,可以对加密过程中 S 盒的输出随机求反,从而影响加密结果的侧信道信息。

该安全结构如图 2 所示,主要由复合域 S 盒变换模块(黑色实线标注的部分,下文简称 SBM)和随机求反控制模块(灰色阴影的部分,下文简称 CM)构成。其中,SBM 模块与图 1 结构相同,由同构变换 $f$、复合域求逆变换、逆同构变换 $f^{-1}$ 和仿射变换四个子模块构成,主要完成复合域上的 S 盒变换。CM 模块由随机数生成器 LFSR,两个($n$ +1)比特右移寄存器 $X$,$Y$,两个二选一数据选择器和两个 8 比特异或操作构成,主要控制实现 S 盒输出的随机求反,改变输出数据的汉明权重,降低功耗与数据之间的相关性,增强 S 盒的抗 DPA 攻击能力。

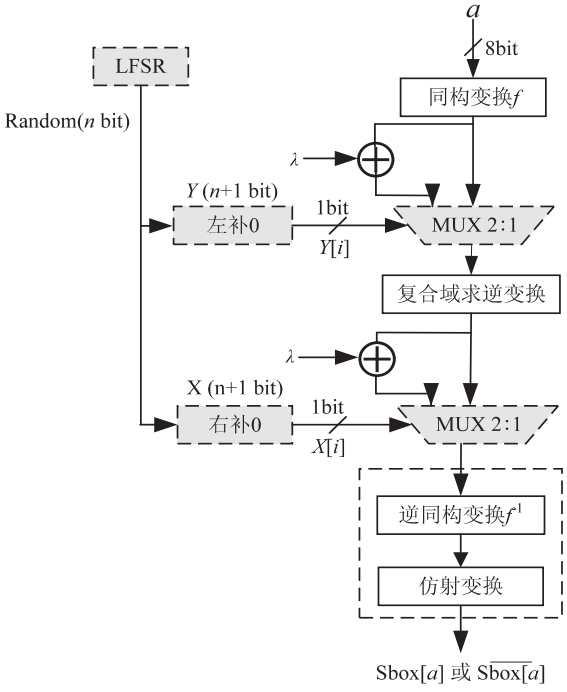



图 2　基于随机求反的 S 盒抗 DPA 攻击安全结构

在 CM 模块中,通过同构变换之后和逆同构变换之前的两个异或操作相互配合以实现加密过程中对 S 盒输出的随机取反和修正操作。LFSR 模块则被用来产生 $n$ 比特随机数(这里 $n$ = AES 的加密轮数−1),该 $n$ 比特随机数经左补 0 和右补 0 分别被送到($n$ +1)比特的右移寄存器 $X$,$Y$ 中,然后由 $X$,$Y$ 的($n$ +1)个比特对来分别控制两个二选一数据选择器,完成 S 盒输出的取反和修正。具体讲,就是在第 $i$ 轮时,通过右移寄

存器将 $X[i]$ 和 $Y[i]$ 移出,并用它们分别控制两个多路选择器的二选一操作。当右移寄存器 $X$ 输出信号 $X[i]=1$ 时,第二个多路选择器选择异或 $\lambda$ 的路径,对本轮以及下一轮输入数据进行求反,隐藏原始加密数据的汉明权重,降低加密数据与功耗之间的相关性,增强其抗 DPA 攻击的能力。与第二个多路选择器相同,当 $Y[i]=1$ 时,对上一轮取反的数据进行还原,不影响求逆运算步骤。由于 $X$,$Y$ 的 $(n+1)$ 个比特对由 LFSR 模块产生,其具有随机性,将之与求反模块进行结合,使得求反操作在加密轮数中随机出现,以增强结构的安全性。

以 AES-128 为例,AES 的加密轮数为 10,则 $n=9$,$X$,$Y$ 为 10 比特寄存器。由于 LFSR 产生的伪随机数可能存在重复性,通过选取抽头为[9,5],使得 LFSR(如图 3 所示)生成一个 9 位的最大状态数为 $(2^9-1)$ 的伪随机数。在 AES 的 10 轮加密过程中,根据 $X$ 和 $Y$ 的 10 个比特数对控制加密过程中逆同构变换之后和同构变换之前的异或操作,实现 S 盒输出的随机取反和修正操作,干扰加密数据和功耗之间的关联性。以 $X$ 控制信号为例,如果 $X[i]$ 为 1,意味着本轮需要在逆同构变换之前做异或 $\lambda$ 的运算,否则不需要(通过二选一数据选择器选择)。$Y$ 控制信号类似。需要注意的是,S 盒的输出取反操作(由 $X[i]$ 控制)和修正操作(由 $Y[i]$ 控制)不是在同一轮完成,而是在相邻两轮中完成的,即上一轮取反,下一轮修正。这个两轮之间的同步是通过 $X$ 和 $Y$ 错位配对实现的,即在构造 $X$ 和 $Y$ 时,通过对同一数右补 0 和左补 0 保证加密过程第 $i$ 轮的控制信号 $X[i]$ 和第 $(i+1)$ 轮的控制信号 $Y[i+1]$ 始终是相等的,从而保证上一轮的 S 盒取反操作能在下一轮修正。

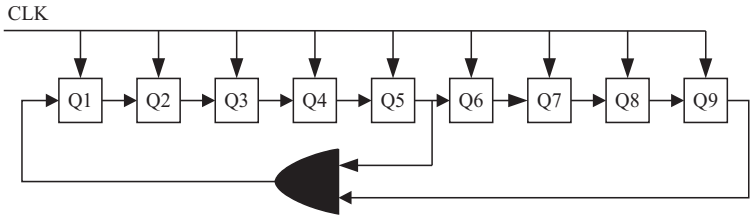



图 3 9 bit 伪随机数生成器

### 2.2 方案正确性证明

针对不同的加密算法,S 盒变换可能有所不同,下面以 AES 算法中的 S 盒为例验证方案的正确性。

为了表述方便,用 $f(x)=\boldsymbol{T}\otimes x$ 表示同构变换 $f$(简写为 $f(x)=\boldsymbol{T}\bullet x$),用 $f^{-1}(x)=\boldsymbol{T}^{-1}\otimes x$ 表示逆同构变换 $f^{-1}$(简写为 $f^{-1}(x)=\boldsymbol{T}^{-1}\bullet x$),这里 $\boldsymbol{T}$ 为 GF$(2^8)$ 到 GF$(2^4)^2$ 上的同构矩阵,$\boldsymbol{T}^{-1}$ 为 $\boldsymbol{T}$ 的逆矩阵。

定理 1:假定 AES 中 S 盒的输入为 $a$,S 盒的第 $i$ 轮原始输出为 $S_b^i[a]$,则当 $\lambda=\boldsymbol{T}\otimes ffH=\boldsymbol{T}\bullet ffH$,且 $X[i]=1$,$Y[i]=0$ 时,即在复合域求逆操作之后、逆同构变换之前,对输出添加一个异或 $\lambda$ 的操作时,图 2 所示方案中 S 盒将输出 $S_b^i[a]$ 的反码形式,记为 $\overline{S_b^i[a]}$。

证明:根据 AES 的构造原理,S 盒替换操作可以表示为式 1。

$$S_b^i[a]=(\boldsymbol{A}a^{-1})\oplus 63H \tag{1}$$

这里 $\boldsymbol{A}$ 表示 S 盒替换操作中的仿射变换矩阵。则由图 1 所示的复合域 S 盒计算流程,可将式 1 转化为式 2。

$$S_b^i[a]=\boldsymbol{A}(\boldsymbol{T}^{-1}((\boldsymbol{T}\bullet a)^{-1}))\oplus 63H \tag{2}$$

然而,如果按图 2 所示,在复合域求逆操作之后、逆同构变换之前,对输出添加一个异或 $\lambda$ 的操作,此时,假定 S 盒的输出为 $\tilde{S}_b^i[a]$,则 $\tilde{S}_b^i[a]$ 可以表示为式 3。

$$\begin{aligned}\tilde{S}_b^i[a]&=\boldsymbol{A}(\boldsymbol{T}^{-1}((\boldsymbol{T}\bullet a)^{-1}\oplus\lambda))\oplus 63H=\\&\boldsymbol{A}(\boldsymbol{T}^{-1}((\boldsymbol{T}\bullet a)^{-1}))\oplus(\boldsymbol{T}^{-1}\lambda))\oplus 63H=\\&\boldsymbol{A}(\boldsymbol{T}^{-1}((\boldsymbol{T}\bullet a)^{-1}))\oplus(\boldsymbol{T}^{-1}T\bullet ffH))\oplus\\&63H=\\&\boldsymbol{A}(\boldsymbol{T}^{-1}((\boldsymbol{T}\bullet a)^{-1}))\oplus ffH)\oplus 63H=\\&\boldsymbol{A}(\overline{\boldsymbol{T}^{-1}((\boldsymbol{T}\bullet a)^{-1})})\oplus 63H\end{aligned} \tag{3}$$

由于仿射矩阵 $\boldsymbol{A}$ 的每一行中“1”的个数为奇数,对任意一个 $X\in$ GF$(2^8)$ 上的元素,公式 4 成立。

$$\overline{\boldsymbol{A}\boldsymbol{X}}=\boldsymbol{A}\bar{\boldsymbol{X}} \tag{4}$$

因此,式 3 可以表示为式 5。

$$\begin{aligned}\tilde{S}_b^i[a]&=\boldsymbol{A}(\overline{\boldsymbol{T}^{-1}((\boldsymbol{T}\bullet a)^{-1})})\oplus 63H=\\&\overline{\boldsymbol{A}(\boldsymbol{T}^{-1}((\boldsymbol{T}\bullet a)^{-1}))}\oplus 63H=\\&\overline{\boldsymbol{A}(\boldsymbol{T}^{-1}((\boldsymbol{T}\bullet a)^{-1}))\oplus 63H}=\\&\overline{S_b^i[a]}\end{aligned} \tag{5}$$

由此定理 1 得证。

定理 2:假定在 AES 加密过程中,本轮 S 盒变换接收的输入是前一轮 S 盒取反的结果 $\overline{S_b^i[a]}$,则在本轮加密中,令 $Y[i]=1$,即在同构变换之后加入异或 $\lambda$ 的操作,该操作能抵消上一轮 S 盒取反对本轮加密结果造成的影响,即:

$(\boldsymbol{T}\bullet\overline{S_b^i[a]})\oplus\lambda=\boldsymbol{T}\bullet S_b^i[a]$.

证明:

$$(\boldsymbol{T}\bullet\overline{S_b^i[a]})\oplus\lambda=(\boldsymbol{T}\bullet\overline{S_b^i[a]})\oplus(\boldsymbol{T}\bullet ffH)=\boldsymbol{T}(\overline{S_b^i[a]}\oplus ffH)=\boldsymbol{T}\bullet S_b^i[a] \tag{6}$$

由此定理 2 得证。

### 2.3　$\lambda$ 的有效性证明

由于 $\lambda$ 的值和同构矩阵 $\boldsymbol{T}$ 相关,为了使方案有效,应该保证 $\lambda=\boldsymbol{T}\bullet ffH\neq 00H$,该条件可以由定理 3 保证。

定理 3:如果存在同构矩阵 $\boldsymbol{T}$ 能将有限域 $GF(2^8)$ 上的元素映射到为 $GF(2^4)^2$ 上,则 $\boldsymbol{T}\bullet ffH\neq 00H$。

证明:

利用反证法,假设 $\lambda=\boldsymbol{T}\bullet ffH=00H$,可得出 $\boldsymbol{T}$ 的每一行和值为 0,即:

$$\sum_{j=1}^{8}T_{ij}=0,\ i=1,2,\cdots,8 \tag{7}$$

其中,$T_{ij}$ 表示矩阵 $\boldsymbol{T}$ 的第 $i$ 行第 $j$ 列的数。

根据矩阵的乘法性质,有 $\boldsymbol{T}\boldsymbol{T}^{-1}=\boldsymbol{T}^{-1}\boldsymbol{T}=\boldsymbol{E}$,这里 $\boldsymbol{E}$ 为单位矩阵,则 $\boldsymbol{E}$ 中第 $i$ 行的所有元素之和可以表示为式 8。

$$\sum_{j=1}^{8}E_{ij}=\boldsymbol{T}_i^{-1}\boldsymbol{T}_1^{\mathrm{T}}+\boldsymbol{T}_i^{-1}\boldsymbol{T}_2^{\mathrm{T}}+\cdots+\boldsymbol{T}_i^{-1}\boldsymbol{T}_8^{\mathrm{T}}=\boldsymbol{T}_i^{-1}(\boldsymbol{T}_1^{\mathrm{T}}+\boldsymbol{T}_2^{\mathrm{T}}+\cdots+\boldsymbol{T}_8^{\mathrm{T}}),\ i=1,2,\cdots,8 \tag{8}$$

其中,$\boldsymbol{T}_i^{-1}$ 和 $\boldsymbol{T}_i^{\mathrm{T}}$ 分别表示矩阵 $\boldsymbol{T}^{-1}$ 的第 $i$ 行和矩阵 $\boldsymbol{T}$ 的 $i$ 列。

由式 7 可得 $(\boldsymbol{T}_1^{\mathrm{T}}+\boldsymbol{T}_2^{\mathrm{T}}+\cdots+\boldsymbol{T}_8^{\mathrm{T}})=00H$,从而得 $\boldsymbol{E}$ 的每一行的和值为 0,即 $\sum_{j=1}^{n}E_{ij}=0,i=1,2,\cdots,8$,这与单位矩阵 $\boldsymbol{E}$ 的性质 $\sum_{j=1}^{n}E_{ij}=1,i=1,2,\cdots,8$ 矛盾,即与逆同构矩阵存在条件矛盾,假设不成立,从而定理 3 得证。

## 3　随机求反 S 盒在 AES 抗 DPA 攻击安全结构设计中的应用

为了验证 2.1 提出的随机求反 S 盒的抗 DPA 攻击特性和硬件实现性能,给出两类基于该 S 盒的 AES 安全结构设计和实现,并在第 4 节给出了相关性能参数及其比较。本节主要介绍两类 AES 安全结构。

### 3.1　基于随机求反 S 盒的 AES 抗 DPA 攻击安全结构(RC–AES 安全结构)

在 AES 中,不同的密钥长度决定了算法中的迭代轮数,该文以密钥长度为 128 比特的 AES(下文简称 AES–128)为例进行说明。在 AES–128 算法中,加密迭代轮数为 10,对应图 2 中 LSFR 生成的随机数就是 9 比特,相应的控制 S 盒取反和修正的 $X,Y$ 信号对为 10 对。

图 4 给出了基于随机求反 S 盒的密钥长度为 128 比特的 AES 抗 DPA 攻击安全结构。该结构由文中提出的随机求反 S 盒与 AES 的其他模块构成。具体工作时,如果某一轮的 S 盒被随机取反,则该轮 AES 的结果也将被取反。这是由于 AES 的行移位,列混合和密钥加操作为线性操作,行移位不改变 S 盒的取反特性,列混合和轮密钥加操作只涉及有限域上的多项式乘法和加法操作,而逻辑取反运算对于多项式乘法和异或运算具有运算保持性,所以如果中间轮 S 盒的输出取反,则 AES 的中间输出结果也会相应取反,该中间结果将在下一轮的 S 盒中进行修正,从而保证 AES 最终加密结果正确。

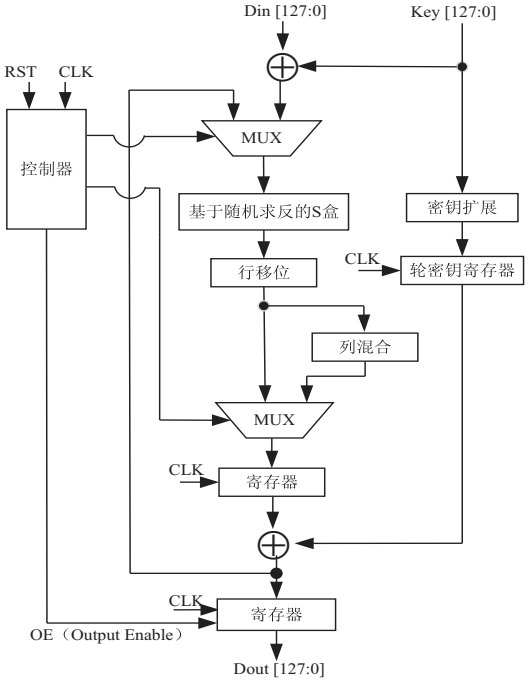



图 4　基于随机求反的 AES 安全结构

这里需要说明,大部分复合域 S 盒主要针对求逆操作进行优化[2–10],而本方案的 S 盒取反操作不受求逆操作的影响,因此,图 4 所示的结构适用于各类 S 盒的实现。

### 3.2　基于随机求反与掩码结合的 AES 安全结构(RC–M–AES 安全结构)

为了进一步提高 AES 算法的抗 DPA 攻击安全性,本节结合随机求反与掩码技术提出了更可靠的 AES 抗 DPA 攻击安全结构,如图 5 所示。图中右侧部分为添加掩码和随机求反操作的 AES 结构,左侧虚框部分用于掩码和随机求反的修正。该结构的主要优点有:(1)通过掩码对复合域求逆变换模块进行防护,弥补了 S 盒随机求反方案的不足。(2)相比于单纯的掩码

方案,结合了随机求反的方案能进一步降低功耗信息和原始加密信息之间的相关性,从而显著提升其抗侧信道攻击能力。

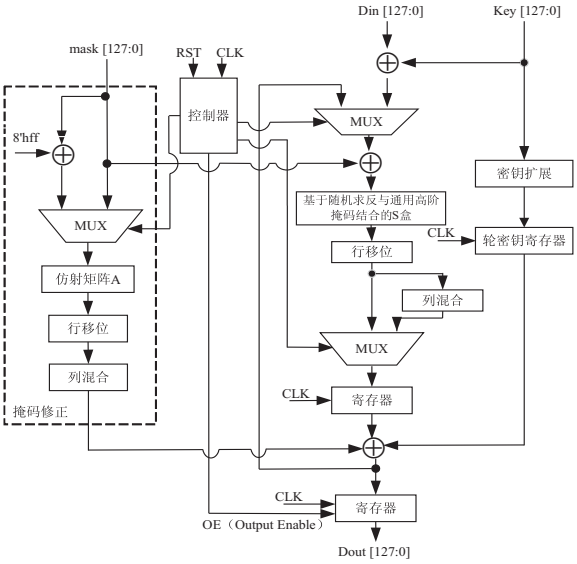


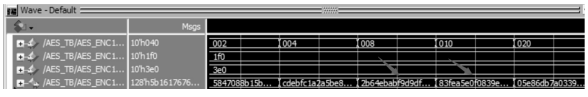

图 5 基于随机求反与通用掩码结合的 AES 安全结构

## 4 实验分析与比较

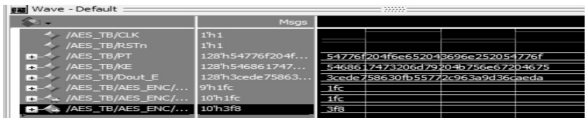
### 4.1 功能验证

为了验证第四节提出的两种 AES 抗 DPA 攻击安全结构(RC-AES 安全结构,RC-M-AES 安全结构)的正确性,该文采用 Verilog 语言对其进行建模,并使用 Modelsim 进行了仿真验证。同时,为方便对比,也对未加防护的 AES(下文简称标准 AES)进行了建模和仿真。图 6 展示了具体仿真结果。

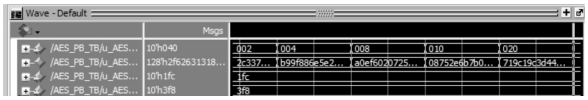
(a)标准 AES 前五轮输出



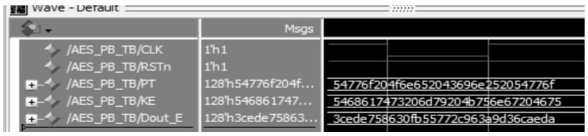
(b)RC-AES 前五轮输出



(c)RC-AES 加密结果



(d)RC-M-AES 前五轮输出



(e)RC-M-AES 加密结果

图 6 提出的两种 AES 安全结构的功能仿真结果

图 6(a)显示了标准 AES 加密的前五轮结果。以图 6(a)为参照,可以看到图 6(b)中 RC-AES 前五轮加密结果,其中箭头所指的第三、四轮被随机取反。然而,如图 6(c)所示,RC-AES 安全结构的最终加密结果不受中间轮结果取反的影响,最终加密结果是正确的。这意味着在加密过程中被随机取反的第三、四轮结果在后续加密轮中被修正。图 6(d)和 6(e)分别给出 RC-M-AES 安全结构前五轮加密结果和最后输出结果。对比图 6(b)和图 6(d)可以看出,RC-M-AES 安全结构隐藏了求反的操作,降低了输出与标准轮输出的相关性,其最终加密结果如图 6(e)所示,也是正确的。以上仿真结果表明第四节提出的两种 AES 抗 DPA 攻击安全结构是正确的。

### 4.2 综合结果

为了评估提出的安全结构方案的硬件性能,该文采用 Synopsys Design Compiler 在 TSMC 90nm 工艺下对其进行了逻辑综合。同时,为了对比,也对部分相关结构进行了复现和逻辑综合。

表 1 给出了提出的基于随机反码保护的复合域 S 盒和文献[26]提出的未加保护的复合域 S 盒的硬件实现综合结果。由表 1 可以看出,随机求反 S 盒仅通过额外增加约 4.72% 的面积开销即可实现对复合域 S 盒的防护。

表 1 两种 S 盒逻辑综合结果

| 加密算法 | 工艺库(TSMC)、nm | 面积 /μm² |
|---|---|---|
| 复合域 S 盒[26] | 90 | 783 |
| 基于随机求反 S 盒 | 90 | 820 |

注:复合域 S 盒[26]结果为文中复现结果。

表 2 详细列出了不同 AES 实现方案的逻辑综合结果。对比标准 AES 实现,文中 3.1 节提出的 RC-AES 安全结构实现逻辑单元和面积开销分别增加了约 4.6% 和 2.1%,而 RC-M-AES 安全结构逻辑单元约为 119.2%。显然,基于随机求反的 AES 安全结构在总的逻辑单元和面积开销上具有显著的优势。对比文献[24]一阶掩码 AES 实现,加了随机取反的 RC-M-AES 安全结构在增加约 3.3% 的逻辑单元后,为原始加密数据提供了额外的线性防护,使其在掩码防护基础上更加安全,这个代价是可以接受的。另外,相较文献[24]中的二阶掩码 AES 实现,基于随机求反与一阶掩码结合的 RC-M-AES 安全结构减少约 10.7% 逻辑单元,而且由于文中所提出的随机求反方案所占逻辑单元固定,其与更高阶掩码结合时所增加的逻辑单元相对总的逻辑单元占比会更低,这在面积受限的应用中是非常有意义的。

表 2　不同 AES 的综合结果

| 加密算法 | 工艺库(TSMC)/nm | 总的逻辑单元 | 组合逻辑 | 总的寄存器 | 逻辑面积/μm² | 合计/μm² |
|---|---|---|---|---|---|---|
| 复合域 AES 实现[26] | 90 | 17 544 | 5 412 | 12 131 | 21 607,561,6 032 | 27 640 |
| 文中基于求反 AES 实现 | 90 | 18 359 | 5 820 | 12 539 | 22 205,1 250,6 032 | 28 238 |
| 一阶掩码 AES 实现[24] | 40 | 38 456 | 32 879 | 12 820 | 53 626,2 888,59 614 | 113 241 |
| 文中基于随机求反与一阶掩码结合的 AES 实现 | 90 | 39 731 | 31 080 | 8 561 | 58 877,697,6 087 | 64 965 |
| 二阶掩码 AES 实现[24] | 40 | 44 475 | 38 282 | 18 980 | 116 979,4 594,100 564 | 217 361 |

### 4.3　DPA 实验结果

为了评估文中提出的两类安全 AES 安全结构的抗 DPA 攻击能力,使用芯片物理攻击平台 Chipwhisperer-Lite。对标准 AES 实现、RC-AES 安全结构实现和 RC-M-AES 安全结构实现进行了 CPA 攻击。攻击点选取在第一轮 S 盒后,采集能量迹均为 5 000条,针对不同结构的 AES 实现,对密钥第一个字节的攻击结果如图 7 ~9 所示。

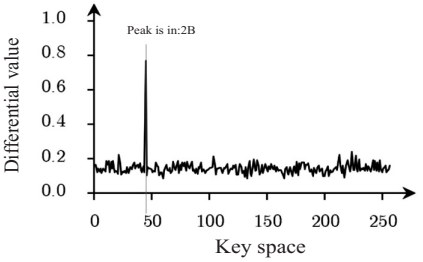



图 7　未加保护的 AES 第一个字节攻击结果

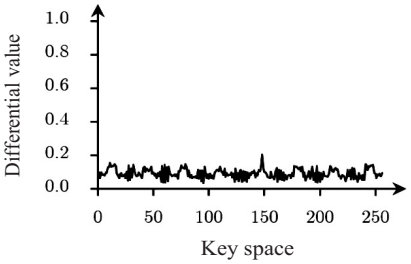



图 8　基于随机求反的 AES 第一个字节攻击结果

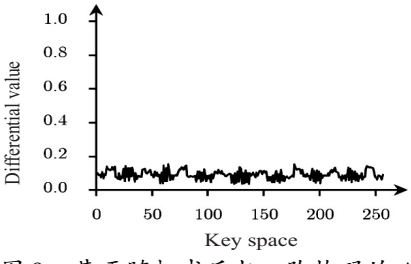



图 9　基于随机求反与一阶掩码的 AES 第一个字节攻击结果

其中图 7 在正确密钥 0X2B 处尖锋突出,而第一个密钥字节正是 0X2B,这说明未加防护的 AES 密码能够被 CPA 攻破。但图 8 和图 9 无明显尖峰,说明基于随机求反的 RC-AES 安全结构和联合随机求反和一阶掩码的 RC-M-AES 安全结构能够降低功耗信息和原始加密信息之间的相关性。同时,而相较图 8,图 9 尖峰更低,这说明随机求反与一阶掩码结合后的方案能更好地保护 AES 免受 DPA 攻击。

## 5　结束语

该文针对 DPA 攻击提出了一种复合域 S 盒的通用随机求反安全结构,并基于此 S 盒结构设计实现了两类抗 DPA 攻击的 AES 的实现方案。文中分别采用 Verilog 语言,Modelsim 软件及 Design Compiler 对提出的两类结构及其相关方案分别进行了建模、功能仿真和硬件综合,结果表明该文提出的两类 AES 安全结构跟其他方案相比具有显著的面积优势,这对面积受限的应用来说是非常有意义的。此外,还利用 Chipwhisperer-Lite 物理攻击平台对两类 AES 安全结构的抗 DPA 攻击性能进行了实验测试,测试结果表明提出的两类 AES 结构都可以在增加较少开销的情况下提高其抗 DPA 攻击能力。另外,该文基于随机求反的 S 盒方案适用于复合域上任何表示基的 S 盒实现,该 S 盒设计不仅适用于 AES 算法,同样适用于任何依赖替换函数作为唯一非线性运算的加密算法,具有较好的通用性。

基于文中研究成果,未来可以进一步探索将复合域 S 盒和随机求反安全结构应用于其他加密算法的设计和实现中(如 SM4 及 Midori、Skinny 等轻量级算法),并对所设计的算法结构的安全性及硬件性能进行评估,从而为不同的应用场景提供更加灵活的安全解决方案。此外,也可以考虑将该安全结构应用于物联网设备、智能卡等资源受限的场景中,以提供更好的安全性保障。

**参考文献:**

[1] KOCHER P, JAFFE J, JUN B. Differential power analysis [C]//Advances in cryptology—CRYPTO'99: 19th annual international cryptology conference. Santa Barbara: Springer, 1999:388-397.

[2] GU S,LUO Z,CHU Y,et al. Trace alignment preprocessing in side-channel analysis using the adaptive filter [J]. IEEE Transactions on Information Forensics and Security,2023,18:

5580-5591.
[3] GLIGOROSKI D, MOE M E. On deviations of the AES S-box when represented as vector valued Boolean function[J]. International Journal of Computer Science and Network Security, 2007, 7(4): 156-163.
[4] RIJMEN V. Efficient implementation of the Rijndael S-box [J/OL]. 2000. http://www. esat. kuleuven. ac. be/ ~ rijmen/rijndael/sbox. pdf.
[5] LI W, BAI G, WU X. Hardware implementation of SM4 based on composite filed s-box and it´s security against machine learning attack[C]//2018 IEEE international conference on electron devices and solid state circuits (EDSSC). Shenzhen: IEEE, 2018: 1-2.
[6] SATOH A, MORIOKA S, TAKANO K, et al. A compact Rijndael hardware architecture with S-box optimization[C]//International conference on the theory and application of cryptology and information security. Berlin: Springer, 2001: 239-254.
[7] CANRIGHT D. A very compact Rijndael S-box[R]. Monterey: Naval Postgraduate School, 2004.
[8] NOGAMI Y, NEKADO K, TOYOTA T, et al. Mixed bases for efficient inversion in F ((2 2) 2) 2 and conversion matrices of subbytes of AES[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, 94(6): 1318-1327.
[9] JEON Y S, KIM Y J, LEE D H. A compact memory-free architecture for the AES algorithm using resource sharing methods[J]. Journal of Circuits, Systems, and Computers, 2010, 19(5): 1109-1130.
[10] NEKADO K, NOGAMI Y, IOKIBE K. Very short critical path implementation of AES with direct logic gates[C]//International workshop on security. Berlin: Springer, 2012: 51-68.
[11] WU H, HASAN M A, BLAKE I F, et al. Finite field multiplier using redundant representation[J]. IEEE Transactions on Computers, 2002, 51(11): 1306-1316.
[12] UENO R, HOMMA N, SUGAWARA Y, et al. Highly efficient GF (2^ 8) gf (2 8) inversion circuit based on redundant GF arithmetic and its application to AES design[C]//Cryptographic hardware and embedded systems-CHES 2015: 17th international workshop. Saint-Malo: Springer, 2015: 63-80.
[13] UENO R, HOMMA N, NOGAMI Y, et al. Highly efficient GF (2^ 8) GF (2 8) inversion circuit based on hybrid GF representations[J]. Journal of Cryptographic Engineering, 2019, 9: 101-113.
[14] NAKASHIMA A, UENO R, HOMMA N. AES S-Box hardware with efficiency improvement based on linear mapping optimization[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2022, 69(10): 3978-3982.
[15] DROLET G. A new representation of elements of finite fields GF (2/sup m/) yielding small complexity arithmetic circuits [J]. IEEE Transactions on Computers, 1998, 47(9): 938-946.
[16] SINGHA T B, PALATHINKAL R P, AHAMED S R. Securing AES designs against power analysis attacks: a survey[J]. IEEE Internet of Things Journal, 2023, 10(16): 14332-14356.
[17] 孟庆全,杨晓元,钟卫东,等. 抵抗差分功耗攻击的秘密共享 S 盒实现与优化[J]. 信息网络安全,2018(2):71-77.
[18] 豆道饶. 基于 NFSR 的密码 S 盒构造方法研究[D]. 桂林:桂林电子科技大学,2022.
[19] NIKOVA S, RECHBERGER C, RIJMEN V. Threshold implementations against side-channel attacks and glitches[C]//International conference on information and communications security. Berlin: Springer, 2006: 529-545.
[20] UENO R, HOMMA N, AOKI T. A systematic design of tamper-resistant galois-field arithmetic circuits based on threshold implementation with (d+1) input shares[C]//2017 IEEE 47th international symposium on multiple-valued logic (ISMVL). Novi Sad: IEEE, 2017.
[21] 蒲金伟,郑 欣,徐迎晖. AES 抗差分功耗分析高效门限实现[J/OL]. 小型微型计算机系统,1-7[2024-05-03]. http://kns. cnki. net/kcms/detail/21. 1106. TP. 20230915. 1105. 016. html.
[22] OSWALD E, MANGARD S, PRAMSTALLER N, et al. A side-channel analysis resistant description of the AES S-box[C]//Fast software encryption: 12th international workshop, FSE 2005. Paris: Springer, 2005: 413-423.
[23] ZAKERI B, SALMASIZADEH M, MORADI A, et al. Compact and secure design of masked AES s-box[C]//International conference on information and communications security. Berlin: Springer, 2007: 216-229.
[24] 姜久兴,赵玉迎,黄 海,等. 基于复合域通用低熵高阶掩码的设计与实现[J]. 电子与信息学报,2020,42(3):779-786.
[25] 姜佳怡,冯 燕,唐啸霖,等. 基于有限域的通用掩码防御方案设计与实现[J/OL]. 微电子学与计算机,1-11[2024-05-03]. http://kns. cnki. net/kcms/detail/61. 1123. TN. 20240204. 1154. 002. html.
[26] MUI E N C, ENGINEER D. Practical implementation of Rijndael S-box using combinational logic[J/OL]. 2007. http://www. xess. com/projects/Rijndael_SBox. pdf.