基于随机加法链的高级加密标准抗侧信道攻击对策

黄 海*① 冯新新② 刘红雨② 厚 娇③ 赵玉迎③ 尹莉莉① 姜久兴③

①(哈尔滨理工大学软件与微电子学院 哈尔滨 150080)

②(哈尔滨理工大学计算机科学与技术学院 哈尔滨 150080)

③(哈尔滨理工大学理学院 哈尔滨 150080)

摘 要：侧信道攻击已经对高级加密标准(AES)的硬件安全造成严重威胁，如何抵御侧信道攻击成为目前亟待解决的问题。字节替换操作作为AES算法中唯一的非线性操作，提高其安全性对整个加密算法有重要意义。该文提出一种基于随机加法链的AES抗侧信道攻击对策，该对策用随机加法链代替之前固定的加法链来实现有限域GF(2^8)上的乘法求逆操作，在此基础上研究随机加法链对算法安全性和有效性方面的影响。实验表明，所提随机加法链算法比之前固定的加法链算法在抵御侧信道攻击上更加安全、有效。

关键词：高级加密标准；侧信道攻击；字节替换；加法链

中图分类号：TP309.7 **文献标识码**：A **文章编号**：1009-5896(2019)02-0348-07

DOI: 10.11999/JEIT171211

Random Addition-chain Based Countermeasure Against Side-channel Attack for Advanced Encryption Standard

HUANG Hai① FENG Xinxin② LIU Hongyu② HOU Jiao③ ZHAO Yuying③
YIN Lili① JIANG Jiuxing③

①(*School of Software and Microelectronics*, *Harbin University of Science and Technology*, *Harbin* 150080, *China*)

②(*School of Computer Sciences and Technology*, *Harbin University of Science and Technology*, *Harbin* 150080, *China*)

③(*School of Sciences*, *Harbin University of Science and Technology*, *Harbin* 150080, *China*)

Abstract: Side channel attacks have serious threat to the hardware security of Advanced Encryption Standard (AES), how to resist the side channel attack becomes an urgent problem. Byte substitution operation is the only nonlinear operation in AES algorithm, so it is very important for the whole encryption algorithm to improve its security. In this paper, a countermeasure against side-channel attack is proposed based on random addition-chain for AES by replacing the fixed addition-chain with random addition-chain to realize the inverse operation of multiplication in a finite field GF(2^8). The impact of the random addition-chain on the security and effectiveness of the algorithm is studied. Experimental results show that the proposed random addition-chain based algorithm is more secure and effective than the previous fixed addition-chain based algorithms in defending against side channel attacks.

Key words: Advanced Encryption Standard (AES); Side channel attack; Byte substitution; Addition chains

1 引言

自从Rijndael算法被定为高级加密标准(Advanced Encryption Standard, AES)以来，一直是国内、外密码算法研究人员的研究热点。由于AES算法拥有安全和高效等优点，所以被广泛应用于移动电话、智能芯片和移动支付等各种实际应用中。

由于密码芯片的普及，想要保证其关键信息被安全地保存和传输，就要提高其安全性，有效抵御外界攻击。侧信道攻击[1](Side Channel Attack, SCA)的出现，给密码芯片的安全带来严重威胁。常见的侧信道攻击有功耗攻击、电磁攻击和运行时间攻击等，其中差分功耗攻击(Differential Power

收稿日期：2017-12-21；改回日期：2018-11-06；网络出版：2018-11-19
*通信作者： 黄海 ic@hrbust.edu.cn
基金项目：国家自然科学基金(61604050, 51672062)
Foundation Items: The National Natural Science Foundation of China (61604050, 51672062)

Analysis, DPA)是侧信道攻击中最有效的方式。研究如何抵抗DPA是当前一个热门话题。字节替换是AES算法中唯一的非线性操作，是侧信道攻击的主要攻击点，因此对AES字节替换的研究至关重要，提高字节替换抵抗侧信道攻击的能力在很大程度上提高了整个AES算法的安全性。目前，对AES算法中字节替换的研究有很多，主要可分为3个方向。一是基于查找表[2]，这种方法速度快，但是占用面积大；2014年，刘国强等人[3]提出利用动态S盒来提高S盒的安全性；2017年，臧鸿雁等人[4]提出基于混沌系统设计新的构造S盒的方法，采用均匀化方法处理的混沌系统能够产生密码性更好的S盒；钟卫东等人[5]在2017年提出基于秘密共享的AES的S盒优化方案，该方案减少了S盒占用的空间，降低了消耗；针对AES算法加解密的不同结构，张伟等人[6]提出了优化方案，采用基于正规基的有限域的算法来实现S盒和逆S盒，减少了资源消耗。二是基于复合域的算法，这种方法是将高阶有限域内的计算转化为低阶的有限域内的计算，虽然比标准AES算法慢，但是减少了占用面积。三是利用加法链[7]来计算有限域元素的乘法逆元，再进行仿射变换并与0x63异或得到该元素字节替换后的值。由于基于加法链的字节替换相比其它2种方法在存储面积和计算复杂度上具有较大优势，所以本文研究基于加法链的抗功耗攻击策略。

基于加法链的S盒实现方法及其抗功耗攻击策略已受到越来越多的研究者关注。2010年，文献[7]根据已有理论，GF (2^8)里元素的乘法逆元等于该元素的254次幂，该文提出一条利用有限域平方和乘法相结合的方法求得乘法逆元，这种方案能有效抵抗差分功耗攻击。2012年，Carlet等人[8]在文献[7]的基础上，提出了第1种能够应用到软件中且有效保护任意阶的任意S盒的掩码方式。2013年，文献[9]分析和提高了文献[8]中的一般高阶掩码方式，主要采用的是分而治之的方法，为S盒获得有效的方式，并且提出多项式链的概念。2014年，文献[10]指出，当S盒的输入尺寸大于4时，可以对文献[8]提出的方式作出改进。尽管基于加法链得到字节替换的方法比较安全，但是目前有关加法链的研究，只应用了1条加法链，很难抵抗高阶侧信道攻击。

为了解决上述问题，本文在王晓东[11]的最短加法链算法的基础上，提出一种基于随机加法链的S盒抗功耗攻击的方法，其中心思想是利用16条功耗特性不同的加法链取代只有1条加法链的方法，这样增加了攻击者攻击的难度，提高了密码算法的安全性。加法链的选取首先设定有限域平方和乘法的个数，找到所有最优的加法链，然后选择16条功耗特性不同的加法链。算法执行过程中，明文中不同的字节可以调用不同的加法链，而且调用的方式也可不同，如可采用顺序调用、循环调用和随机调用。所提方法相比现有的基于加法链方法，以牺牲少量面积为代价，大幅度提高了AES算法抵抗侧信道攻击的能力。

2　AES算法和侧信道攻击

2.1　AES算法简介

AES算法既是对称加密算法，也是迭代分组密码算法，其主要部分分为加密、解密、密钥扩展。AES算法的明文固定为128 bit，它的密钥是可变的，可以是128 bit、196 bit和256 bit 3种情况，其对应的轮变换次数分别是10, 12和14。本文使用的密钥是128 bit，即轮变换次数为10。

字节变换作为AES算法中唯一的非线性操作，并且在加解密算法中，正反字节替换和密钥扩展3个操作中都使用了S盒。2016年，刘艳萍等人[12]优化了AES算法中的密钥扩展算法，该方案通过循环移位来改进密钥扩展的算法，进一步改善了AES算法中种子密钥的安全性。所以S盒在AES算法中利用率很高，字节替换的好坏决定了AES的硬件实现效率。

目前完成字节替换的方式有3种，第1种方式为查找表法，它计算速度快，但会占用很多资源。第2种方式是基于复合域的算法[13]，依据有限域的特点，域GF $\left[\left(2^4\right)^2\right]$与GF $\left(2^8\right)$是同构变换，把GF $\left(2^8\right)$上的求逆变换转化到GF $\left[\left(2^4\right)^2\right]$上作求逆运算[14]，以此减少了逻辑关系的运算复杂度，降低了S盒的面积。而第3种方式是基于有限域GF $\left(2^8\right)$上的性质$x^{255}=1$，则有限域GF $\left(2^8\right)$上元素x的乘法逆元$x^{-1}=x^{254}$，所有求有限域上一元素的乘法逆元，只要求这个元素的254次方就行。基于加法链的字节替换算法在抵抗高阶侧信道攻击上比其他两种方式更有效。

2.2　侧信道攻击

侧信道攻击在现代密码学中是一种重要的密码分析方法。这类攻击通常利用密码系统中的泄漏信息来获得密钥，一般攻击方法有功耗分析、电磁辐射分析和时间分析等。由于测试功耗的方法简单，功耗曲线也容易分析，所以功耗分析攻击在实际生活中应用最广。崔琦等人[15]在传统模板攻击的基础上，提出了优化方案，简化了模板结构，而且改进了模板构建方法。2017年，王建新等人[16]提出的方案提高了能量分析的效果，以AES-128算法为攻击的目标，通过对采集的能量曲线进行滑动平均滤波，再通过相关能量分析来攻击密码算法。段晓毅等人[17]以带固定值掩码的AES为研究对象，考虑了

掩码技术的特点，提出一种高阶差分功耗分析的方案。该方案利用在功耗曲线上的两个信息点的联合分布来避开掩码对加密算法的保护，仅需几百条功耗曲线就能成功破解密钥。所以差分功耗分析对密码芯片类的安全性造成很严重的威胁，找到具有抵御DPA攻击的方法有着重要的意义。

3 目前已有的基于代数方法求字节替换方案

加法链是由有限域平方和乘法组合而成，因为有限域乘法是非线性操作，而有限域平方是线性操作，所以有限域乘法的复杂度远大于有限域平方。为减少字节替换的复杂度，需要使用尽量少的有限域乘法操作。

3.1 基于加法链的字节替换

2010年，文献[7]提出一般加法链实现有限域的乘法逆元。2012年，Carlet等人[8]扩展了文献[7]的方案，提出了割圆类概念，将有限域GF(2^8)上的元素按求以它们为幂指数时的复杂度分类，分在一类的就表示复杂度一样。比如有限域GF(2^8)中的127, 254是一类，则计算x^{127}和x^{254}的复杂度一样。2013年，Roy等人[9]在Carlet等人的方案上进行了分析和改进，提出了有限域GF(2^n)上的多项式链的概念。他们通过研究不同的分圆类加法链来分析有限域GF(2^n)上最优的求幂加法链。证明了分圆类加法链最小长度的下限。2014年，Coron等人[10]提出了新的方案，他们在文献[7]的基础上提出了掩码更新。该方案在于适应ISW方案[18]，直接处理一个以$a\times g(a)$的乘积形式，其中$g(a)$是线性函数。此外还提供了一个改进，允许避免使用有限域GF(2^n)上耗费大的乘法，使得该方案更安全有效。

3.2 基于复合域的字节替换

为减少S盒中乘法求逆操作的计算消耗，文献[13]提出了基于复合域GF (16)上的乘法逆运算。假设一个复合域GF $((2^n)^m)$和GF $\left(2^k\right)$满足$k=mn$，则称GF $((2^n)^m)$和GF $\left(2^k\right)$为同构域，它们上的乘法和平方等操作可以转化到同构域上的乘法和平方。较低阶域上的乘法与加法操作所需的硬件复杂度低于较高阶域上的乘法与加法操作。文献[19]采用的方法是基于多项式基的复合域GF $\left(\left(2^4\right)^2\right)$上的计算，这是实现S盒最快速的算法。文献[6]通过采用基于正规基的复合域算法实现了面积复杂度最小的S盒，可以有效减少资源消耗。文献[20]通过随机调用不同的同构域来实现AES算法，这给差分功耗攻击带来更大的困难，提高了AES算法的安全性。同样，文献[21]也提出了利用随机的塔域代替固定的塔域的算法，结合布尔掩码，提高了算法抵抗侧信道攻击的能力。

4 本文的方案

目前存在的基于加法链的字节替换方案中，只有固定的一条加法链，这些方案很难抵抗高阶侧信道攻击。本文根据王晓东[11]的最短加法链的程序得知，$x\rightarrow x^{254}$的一条最短加法链如式(1)

$$\begin{aligned}x &\xrightarrow{S} x^2 \xrightarrow{S} x^4 \xrightarrow{S} x^8 \xrightarrow{S} x^{16} \xrightarrow{S} \\ & x^{32} \xrightarrow{S} x^{64} \xrightarrow{M} x^{80} \xrightarrow{M} x^{84} \xrightarrow{S} \\ & x^{168} \xrightarrow{M} x^{252} \xrightarrow{M} x^{254}\end{aligned} \tag{1}$$

式(1)中的S, M分别表示平方和乘法操作。可以看出，最短加法链需要11步操作，即有限域乘法和平方操作一共11个。由于乘法操作最少为4个，所以最优的加法链是由4个乘法操作和7个平方操作组成的。

为使字节替换随机使用加法链，需找到多条最优的加法链。文献[12]通过构造状态空间树来解决最短加法链的问题。状态空间树如图1所示。由于明文是含有16个字节，该文需要找到16条功耗特性不同的加法链。这要求找到大量的含有4个乘法操作和7个平方操作的加法链，可以通过穷举法得到一些符合条件的，不过这种方式很费时费力，不一定能在短时间内找到符合条件的16条，本文在文献[12]的基础上，通过设立条件，比如1→254需要经过11步操作得到符合条件。

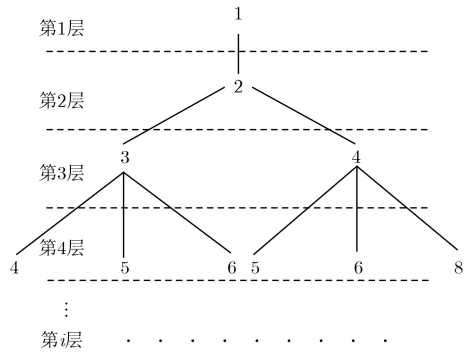


图 1 最短加法链问题的状态空间树

如图1所示，第i层结点用b_i表示，可以看出第i层的子结点$b_{i+1}>b_i$。而第i层的结点可以通过式(2)得到

$$b_i=b_j+b_k, 1\le k\le j\le i \tag{2}$$

本文根据状态空间树找到所有最短加法链的中心思想是：控制搜索的深度为12，即不断向下搜索时，在第12层，得到254，则找到一条最短加法链，此时回到父结点，再看其子结点是否有没遍历的，如果是，继续搜索子节点，如果否，继续返回上一层。无论在12层是否找到254，都返回上一层，直到停留在顶层结点1处，所有最短的加法链都已找到。

4.1 加法链生成算法

本文根据最优的加法链需要4个乘法和7个平方操作，通过C语言编程将符合条件的加法链全部找到，共1191条。根据功耗特性的不同(即乘法和平方的位置不完全一样)，将所有加法链分成117组，每组的加法链功耗特性相同，本方案需要16个不同功耗特性的加法链，所以通过随机数发生器从117组中找到16组不同的加法链，为方便分析，本文采用的16个不同组里的16条加法链如表1所示。

表 1　16条不同功耗特性的加法链

序号	加法链路径
(1)	1→2→4→8→16→32→64→80→84→168→252→254
(2)	1→2→4→8→16→32→64→80→84→86→168→254
(3)	1→2→4→8→16→32→48→50→100→200→250→254
(4)	1→2→4→8→16→32→48→50→100→102→204→254
(5)	1→2→4→8→16→32→48→50→54→100→200→254
(6)	1→2→4→8→16→32→40→80→84→168→252→254
(7)	1→2→4→8→16→32→40→80→84→86→168→254
(8)	1→2→4→8→16→32→40→42→84→126→127→254
(9)	1→2→4→8→16→32→40→42→43→84→ 127→254
(10)	1→2→4→8→16→32→36→72→144→216→252→254
(11)	1→2→4→8→16→24→40→50→100→200→250→254
(12)	1→2→4→8→16→24→48→50→100→102→204→254
(13)	1→2→4→8→16→24→48→50→54→100→200→254
(14)	1→2→4→8→16→24→28→56→112→224→252→254
(15)	1→2→4→8→16→24→28→56→112→113→226→254
(16)	1→2→4→8→16→24→28→30→56→112→224→254

由表1可看出，每条加法链的乘法和平方操作的位置不完全一致，则说明这16条加法链功耗特性不一样。由于明文是128位，可看作16个字节，每1个字节占8位，正好可以在每轮字节替换时，每个字节调用不同的加法链，在硬件实现上是并行调用加法链的，这样不仅提高效率，而且提高安全性。

4.2 循环调用加法链

该方案的中心思想是：在每轮字节替换开始时，生成1个1～16的随机数，假设生成a，则第1个字节调用第a条加法链，第2个字节调用第$(a\%16+1)$条加法链，即16个字节根据随机数循环调用加法链，保证16条加法链同时用上。某一轮的字节替换部分流程图如图2所示。

如图2，字节替换的输入为16个字节，记为$\{m_1, m_2, \cdots, m_{16}\}$, 16条加法链分别表示为$\{S_1(x), S_2(x), \cdots, S_{16}(x)\}$。由于每轮生成的随机数可能都不一样，所以每轮的每1个字节调用的加法链也不同，提高了攻击者的攻击难度。

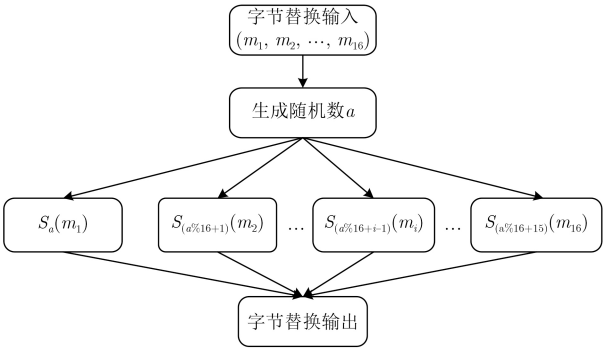


图 2 一轮的字节替换

4.3 乱序调用加法链

该方案比循环调用加法链方案使用更多次的随机数发生器，在安全性上提高了很多。此方案的思想是：在每轮字节替换前，通过随机数发生器生成16个1～16不重复的数，组成1个数组，比如{3, 6, 10, 8, 7, 1, 11, 13, 16, 5, 2, 4, 12, 14, 9, 15}，这种情况就是第1个字节调用第3条加法链，第2个字节调用第6条加法链，…，第16个字节调用第15条加法链。这样的数组是1～16随机排列，共有16！种情况，所以每轮调用加法链的情况基本上不一样，增加了加密算法的随机性。在增加不多的随机数的情况下，很大程度提高了加密算法的安全性。生成16个1～16的不同随机数算法如表2。

表 2　随机数生成算法

将包含1～16的数组完全打乱
输入：$a[16]$={1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16}
输出：1～16随机排列后的数组
(1)srand((unsigned)time(NULL))/*随机数发生器的初始函数*/
(2)int i,j,temp
(3)for i from 16 to 1 do /*i 从16递减到1 */
(4)j=rand()%(i+1) /*生成0～i的随机数*/
(5)Temp=$a[j]$ /*交换数组中第i+1个数和第j+1个数*/
(6)$a[j]$=$a[i]$
(7)$a[i]$=temp
(8)end for

如表2所示，该算法将使每轮的16个字节随机调用16条加法链，相比以前的加法链——16个字节调用相同的加法链，攻击者只需要获取到1个字节上的中间值，就能获取其他15个字节上的中间值。而乱序调用加法链的方案，需要分别破解16条加法链上的中间值。

乱序调用加法链的设计方案，充分采用随机化的思想，使得加密算法在每轮调用加法链的方式都不一样，这种随机性具有不可预测性，解决了调用

固定加法链安全性较低的问题，同时使得攻击者攻击的成本呈指数级增加，提高了密码算法的安全性。

4.4 安全性分析

本文从不同功耗特性的加法链中，随机选取16条加法链，这样的随机加法链算法可能性很多，这给攻击者攻击AES算法造成了很大困难。此外，在加密算法的每轮字节替换前都要生成随机数，来决定每个字节调用哪一条加法链，这样的方法类似随机调用塔域，提高了算法的安全性。此外，相较于文献[7]的方案，在字节替换处，只有1条固定的加法链，攻击者只要攻击成功其中1个字节的加法链，就很容易得到整个密钥。而本文的方案需要16条加法链，且这16条功耗特性不同，这增加了差分功耗攻击的难度。由于功耗攻击是利用加密过程中的泄漏信息来破解密钥，如果实现掩码过的中间结果的分布概率与敏感的信息是不相关的，这种情况理论上是可以抵抗DPA攻击的。有3种理论对此作为引证。3条引理如下：

引理 1 假设a,a'是GF(2^8)上的任意元素，b, b'在$\{0, 1, \cdots, 255\}$上服从均匀分布，并且分别独立于a, a'，那么$z=(a\oplus m)(a'\oplus m')$服从式(3)定义的分布概率。

引理 2 假设a是GF(2^8)上的一个元素，如果b在$\{0, 1, \cdots, 255\}$上服从均匀分布，并且独立于a，则$a\oplus r$服从均匀分布，如式(3)：

$$P(z=i)=\begin{cases}(2^9-1)/2^{16}, i=0\\(2^8-1)/2^{16}, i\neq 0\end{cases} \tag{3}$$

引理 3 若a,b是有限域GF(2^k)上的任意值，m_a，m_b是有限域GF(2^k)上独立均匀分布的。$(a+m_a)\times(b+m_b)$的分布概率如式(4)：

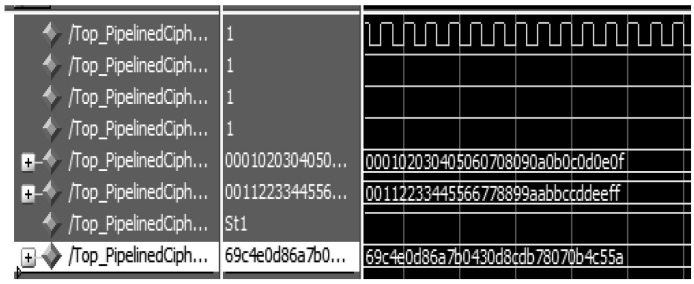
$$P_r((a+m_a)\times(b+m_b)=i)=\begin{cases}\left(2^{k+1}-1\right)/2^{2k}, i=0\\\left(2^k-1\right)/2^{2k}, i\neq 0\end{cases} \tag{4}$$

式(4)能证明有限域乘法的正确性。

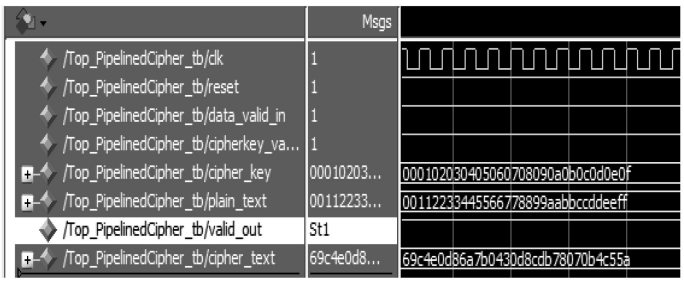
综上所述，本文的两种方案比以前的加法链方案安全有效，可以有效抵抗差分功耗攻击，增强算法的安全性。

5 仿真与结果比较

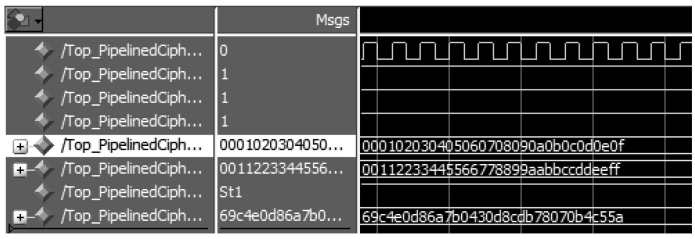
标准AES、本文的循环调用加法链以及乱序调用加法链的加密算法仿真结果如图3所示，其中，



(a) 基于查找表的AES仿真图



(b) 循环调用加法链的AES仿真图



(c) 随机调用加法链的AES仿真图

图 3 加密算法仿真结果

明文：256’h00112233445566778899aabbccddeeff；密钥：256′h000102030405060708090a0b0c0d0e0f；密文：256′h69c4e0d86a7b0430d8cdb78070b4c55a。

从图3中可以看出，本文提出的两种方案功能正确。此外，对标准AES、文献[7]方案和本文提出的两种方案采用流水线设计(10轮展开)，并通过Synopsys Design Compiler进行逻辑综合，得出了各方案不同模块的面积，单位为千等效门数(kGE)，如表3所示。

表 3　不同方案的不同模块的面积比较

方案	组合面积(kGE)					非组合面积(kGE)	网络互连面积(kGE)	总面积(kGE)
	字节替换	行移位	列混合	密钥加	密钥扩展			
标准AES	1067	32	149	66	1190	854	46	3404
文献[7]方案	2179	32	149	66	2328	675	26	5441
循环调用加法链	2162	32	149	66	2320	675	20	5424
乱序调用加法链	2165	32	149	66	2344	675	21	5452

从表3可知，本文的两种方案与标准AES算法相比，字节替换所需要的面积是其2倍，其他模块面积相等；与文献[7]方案相比，占用的总面积和各模块的面积几乎相等，但因为采用了随机调用多个加法链，大大提高AES的安全性。

将综合后的结果导入SOC Encounter，生成了乱序调用加法链的版图，如图4所示。

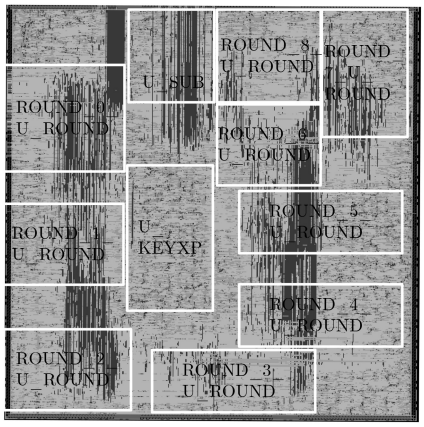


图 4 乱序调用加法链的版图

如图4，U_SUB表示单独的字节替换操作(用于AES的最后一轮)；ROUND_x_U_ROUND表示轮操作，包括字节替换，行移位，列混合，密钥加4个操作；U_KEYXP表示密钥扩展；未标框部分为顶层胶合逻辑。

6　结束语

本文所提两种不同的基于随机加法链计算AES字节替换方案，都需要16个功耗特性不同的加法链，并且每条加法链含有4个乘法和7个平方操作。这两种方案比原先的只有1条加法链的方案安全性更高，增加的资源消耗不多，最终的仿真结果说明了方案的正确性。未来的研究方向是在这两种方案基础上增加掩码部分以抵抗更高阶的侧信道攻击。

参 考 文 献

[1] STANDAERT F X. Introduction to Side-channel Attacks[M]. Secure Integrated Circuits and Systems, Boston: Springer, 2010: 27–42. doi: 10.1007/978-0-387-71829-32.

[2] CORON J S. Higher order masking of look-up tables[C]. 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, 2014: 441–458. doi: 10.1007/978-3-642-55220-5_25.

[3] 刘国强, 金晨辉. 一类动态S盒的构造与差分性质研究[J]. 电子与信息学报, 2014, 36(1): 74–81. doi: 10.3724/SP.J.1146.2013.00416.

LIU Guoqiang and JIN Chenhui. Investigation on construction and differential property of a class of dynamic S-box[J]. *Journal of Electronics & Information Technology*, 2014, 36(1): 74–81. doi: 10.3724/SP.J.1146.2013.00416.

[4] 臧鸿雁, 黄慧芳. 基于均匀化混沌系统生成S盒的算法研究[J]. 电子与信息学报, 2017, 39(3): 575–581. doi: 10.11999/JEIT160535.

ZANG Hongyan and HUANG Huifang. Research on algorithm of generating S-box based on uniform chaotic system[J]. *Journal of Electronics & Information Technology*, 2017, 39(3): 575–581. doi: 10.11999/JEIT160535.

[5] 钟卫东, 孟庆全, 张帅伟, 等. 基于秘密共享的AES的S盒实现与优化[J]. 工程科学与技术, 2017, 49(1): 191–196. doi: 10.15961/j.jsuese.2017.01.025.

ZHONG Weidong, MENG Qingquan, ZHANG Shuaiwei, *et al*. Implementation and optimization of S-box on AES based on secret sharing[J]. *Advanced Engineering Sciences*, 2017, 49(1): 191–196. doi: 10.15961/j.jsuese.2017.01.025.

[6] 张伟, 高俊雄, 王耕波, 等. 一种优化的AES算法及其FPGA实现[J]. 计算机与数字工程, 2017, 45(1): 502–505. doi:

10.3969/j.issn.1672-9722.2017.03.020.

ZHANG Wei, GAO Junxiong, WANG Yunbo, *et al*. An optimized AES algorithm and its FPGA implementation[J]. *Computer & Digital Engineering*, 2017, 45(1): 502–505. doi: 10.3969/j.issn.1672-9722.2017.03.020.

[7] RIVAIN M and PROUFF E. Provably secure higher-order masking of AES[C]. Cryptographic Hardware and Embedded Systems, Santa Barbara, USA, 2010: 413–427. doi: 10.1007/978-3-642-15031-9_28.

[8] CARLET C, GOUBIN L, PROUFF E, *et al*. Higher-order masking schemes for s-boxes[C]. International Conference on FAST Software Encryption, Washington, DC, USA, 2012: 366–384. doi: 10.1007/978-3-642-34047-521.

[9] ROY A and VIVEK S. Analysis and improvement of the generic higher-order masking scheme of FSE 2012[C]. Cryptographic Hardware and Embedded Systems-CHES 2013, Santa Barbara, USA, 2013: 417–434. doi: 10.1007/978-3-642-40349-1-24.

[10] CORON J S, PROUFF E, RIVAIN M, *et al*. Higher-order side channel security and mask refreshing[C]. International Workshop on Fast Software Encryption 2013, Singapore, 2013: 410–424. doi: 1007/978-3-662-43933-3_21.

[11] 王晓东. 最短加法链算法[J]. 小型微型计算机系统, 2001, 22(10): 1250–1253. doi: 10.3969/j.issn.1000-1220.2001.10.026.

WANG Xiaodong. Shortest addition chain algorithm[J]. *Mini-Micro System*, 2001, 22(10): 1250–1253. doi: 10.3969/j.issn.1000-1220.2001.10.026.

[12] 刘艳萍, 李秋慧. AES算法的研究与其密钥扩展算法改进[J]. 现代电子技术, 2016, 39(10): 5–8. doi: 10.16652/j.issn.1004-373x.2016.10.002.

LIU Yanping and LI Qiuhui. Analysis of AES algorithm and its key extension algorithm improvement[J]. *Modern Electronics Technique*, 2016, 39(10): 5–8. doi: 10.16652/j.issn.1004-373x.2016.10.002.

[13] OSWALD E, MANGARD S, PRAMSTALLER N, *et al*. A side-channel analysis resistant description of the AES S-box[C]. International Workshop on Fast Software Encryption 2005, Paris, France, 2005: 413–423. doi: 10.1007/11502760-28.

[14] 夏克维, 李冰. AES算法中S-box和列混合单元的优化及FPGA实现[J]. 现代电子技术, 2009, 32(24): 11–14. doi: 10.16652/j.issn.1004-373x.2009.24.029.

XIA Kewei and LI Bing. Optimization of S-box and Mixcolumn blocks in AES encryption algorithm and FPGA implementation[J]. *Modern Electronics Technique*, 2009, 32(24): 11–14. doi: 10.16652/j.issn.1004-373x.2009.24.029.

[15] 崔琦, 王思翔, 段晓毅, 等. 一种AES算法的快速模板攻击方法[J]. 计算机应用研究, 2017, 34(6): 1801–1804. doi: 10.3969/j.issn.1001-3695.2017.06.045.

CUI Qi, WANG Sixiang, DUAN Xiaoyi, *et al*. Fast template DPA attack against AES algorithm[J]. *Application Research of Computers*, 2017, 34(6): 1801–1804. doi: 10.3969/j.issn.1001-3695.2017.06.045.

[16] 王建新, 方华威, 段晓毅, 等. 基于滑动平均的能量分析攻击研究与实现[J]. 电子与信息学报, 2017, 39(5): 1256–1260. doi: 10.11999/JEIT160637.

WANG Jianxin, FANG Huawei, DUAN Xiaoyi, *et al*. Research and implementation of power analysis based on moving average[J]. *Journal of Electronics & Information Technology*, 2017, 39(5): 1256–1260. doi: 10.11999/JEIT160637.

[17] 段晓毅, 王思翔, 崔琦, 等. 一种带掩码AES算法的高阶差分功耗分析攻击方案[J]. 计算机工程, 2017, 43(10): 120–125. doi: 10.3969/j.issn.1000-3428.2017.10.021.

DUAN Xiaoyi, WANG Sixiang, CUI Qi, *et al*. A high-order differential power analysis attack scheme with masked AES algorithm[J]. *Computer Engineering*, 2017, 43(10): 120–125. doi: 10.3969/j.issn.1000-3428.2017.10.021.

[18] ISHAI Y, SAHAI A, and WAGNER D. Private circuits: Securing hardware against probing attacks[C]. CRYPTO 2003: Advances in Cryptology – CRYPTO, Santa Barbara, USA, 2003: 463–481. doi: 10.1007/978-3-540-45146-4_27.

[19] ZHANG Xinmiao and PARHI K K. High-speed VLSI architectures for the AES algorithm[J]. *IEEE Transactions on Very Large Scale Integration Systems*, 2004, 12(9): 957–967. doi: 10.1109/TVLSI.2004.832943.

[20] JUNGK B, STÖTTINGER M, GAMPE J, *et al*. Side-channel resistant AES architecture utilizing randomized composite field representations[C]. International Conference on Field-Programmable Technology, Seoul, Korea, 2012: 125–128. doi: 10.1109/FPT.2012.6412123.

[21] BONNECAZE A, LIARDET P, and VENELLI A. AES side-channel countermeasure using random tower field constructions[J]. *Designs, Codes and Cryptography*, 2013, 69(3): 331–349. doi: 10.1007/s10623-012-9670-x.

黄 海：男，1982年生，副教授，硕士生导师，研究方向为信息安全、数字信号处理及VLSI集成电路设计.

冯新新：男，1991年生，硕士生，研究方向为计算机网络与信息安全.

刘红雨：男，1993年生，硕士生，研究方向为数字信号处理.

厚 娇：女，1988年生，硕士生，研究方向为计算机网络与信息安全.

赵玉迎：女，1990年生，硕士生，研究方向为计算机网络与信息安全.

尹莉莉：女，1986年生，博士生，讲师，研究方向为数字信号处理.

姜久兴：男，1963年生，教授，硕士生导师，研究方向为集成电路设计.