基于复合域通用低熵高阶掩码的设计与实现

姜久兴[①] 赵玉迎[①] 黄 海*[②] 谢光辉[②] 厚 娇[①] 冯新新[③]

[①](哈尔滨理工大学理学院 哈尔滨 150080)

[②](哈尔滨理工大学软件与微电子学院 哈尔滨 150080)

[③](哈尔滨理工大学计算机科学与技术学院 哈尔滨 150040)

摘 要：通过对基于复合域S-box构造算法的深入研究，该文提出一种低面积复杂度的通用低熵高阶掩码算法。在有限域GF(2^4)上引入低熵掩码思想，并采用部分模块复用设计，有效降低了基于复合域S-box求逆运算的乘法数量。该算法能够适用于由求逆运算构成的任意分组加密算法，进一步将本方案应用于分组加密算法高级加密标准(AES)，给出了详细的综合仿真结果并进行了版图面积优化，较传统的掩码方案相比有效减少了逻辑资源的使用，此外，对其安全性进行了理论验证。

关键词：高阶掩码；复合域算法；S-box；低熵；高级加密标准

中图分类号：TN918.4; TP309.7 **文献标识码**：A **文章编号**：1009-5896(2020)03-0779-08

DOI: 10.11999/JEIT190257

Design and Implementation of Generic Low-entropy High-order Composite Field Based Masking Scheme

JIANG Jiuxing[①] ZHAO Yuying[①] HUANG Hai[②] XIE Guanghui[②]
HOU Jiao[①] FENG Xinxin[③]

[①](*School of Sciences*, *Harbin University of Science and Technology*, *Harbin* 150080, *China*)

[②](*School of Software and Microelectronics*, *Harbin University of Science and Technology*, *Harbin* 150080, *China*)

[③](*School of Computer Sciences and Technology*, *Harbin University of Science and Technology*, *Harbin* 150040, *China*)

Abstract: Based on the in-depth research on the S-box constitution arithmetic of composite, an area optimized generic low-entropy higher-order masking scheme is proposed in this paper. The low entropy masking method is introduced on GF(2^4), and the partial module reusing design is adopted, which reduces effectively the number of multiplications based on the S-box inversion operation of the composite. The algorithm can be applied to any order masking scheme of arbitrary S-box composed of inversion operation. This scheme is applied to AES, gives detailed simulation results and optimizes the layout area, compared with the traditional masking scheme, reduces effectively the use of logical resources. In addition, the security is theoretically proved.

Key words: High-order masking; Composite arithmetic; S-box; Low entropy; Advanced Encryption Standard(AES)

收稿日期：2019-04-16；改回日期：2019-09-16；网络出版：2019-10-14

*通信作者： 黄海 ic@hrbust.edu.cn

基金项目：国家自然科学基金(61604050, 51672062)，黑龙江省普通本科高等学校青年创新人才培养计划(UNPYSCT-2017081)，黑龙江省博士后科研启动基金(LBH-Q18065)

Foundation Items: The National Natural Science Foundation of China (61604050, 51672062), The University Nursing Program for Young Scholars with Creative Talents in Heilongjiang Province (UNPYSCT-2017081), The Heilongjiang Postdoctoral Funds for Scientific Research Initiation (LBH-Q18065)

1 引言

S-box是分组密码中唯一的非线性变换，也是极易受到差分功耗攻击(Differential Power Attack, DPA)的模块[1,2]，因此，针对S-box安全性的研究具有重要意义[3,4]。掩码是防御S-box免受DPA、高阶DPA攻击的一项重要技术手段[5,6]，主要有3类：基于复合域、基于查找表[7,8]及基于加法链[9,10]的S-box掩码方案，相较于后两种方案，基于复合域掩码方案具有掩码操作简单、硬件成本相对较低等优势，但目前该类掩码方案均为1阶掩码，难以扩展到高阶，主要原因为：(1)仅针对AES算法设计的掩码方案，不具通用性；(2)算法的高复杂度导致硬件实现难度大；(3)采用软件实现的掩码方案不具备通用性。

考虑到掩码复杂度与安全性两个维度的折中关系，低熵掩码方案应运而生。相较于全掩码方案，低熵掩码方案的掩码值不再是任意值，而变成了满足特定关系的一组固定值，并由此衍生出各种不同的低熵掩码方案。目前，低熵掩码思想只是应用于基于查找表的S-box中，Nassar等人[11]提出的即是一种典型的低熵掩码方案，但此类方案的安全性仍然存在一定缺陷，且硬件资源占用依然较高。

基于以上方案中的不足之处，本文通过在有限域GF(2^4)上引入低熵掩码思想来优化复合域求逆运算算法，在此基础上运用模块复用设计，有效降低基于复合域S-box求逆运算过程中所需的乘法数量，得到一种低面积复杂度的低熵掩码方案。本方案适用于由求逆运算构成的任意分组密码算法，并能够扩展到更高阶掩码方案。

2 通用低熵高阶掩码方案

在基于复合域的S-box运算过程中，有限域GF($(2^n)^m$)是GF(2^n)的m阶扩展域，有限域GF(2^n)是GF(2)的n阶扩展域，称GF($(2^n)^m$)为复合域，其子域为GF(2^n)。有限域GF(2^k)和复合域GF($(2^n)^m$)(k=m·n)具有同构关系，两个域之间的元素能够相互线性映射，简单来讲，将有限域GF(2^k)上的运算映射到复合域GF($(2^n)^m$)上执行，而GF($(2^n)^m$)上的运算又可以映射到GF(2^n)上执行，层层降维简化了复杂运算的硬件实现难度。

2.1 基于复合域的掩码方案研究现状

基于复合域掩码方案的核心是优化有限域GF(2^8)上求逆运算算法，设法减少求逆运算中使用的乘法数量。2005年，Oswald等人[12]提出在复合域GF(2^2)实现S-box掩码以抵御零值攻击，但域之间的转换会增加硬件开销。为避免此类硬件开销，文献[13]直接在复合域GF(2^4)上进行S-box掩码方案的设计，文献[14]则是选取不同正规基的掩码方案。文献[15,16]提出将复合域GF(2^4)上的运算变换成一系列重计算查找表的软件实现方案，但会占用大量ROM空间。汪鹏君等人[17]基于关键模块重用的思想提出一种能够抵御零值攻击的有效求逆算法。Ahn等人[18]对文献[15]的算法进行了优化，利用更少的查找表和异或操作以降低占用的ROM资源，但又引入了RAM等资源，复合域GF(2^4)上掩码方案求逆过程表示为

$$d+m_l=(a_h+m_h)^2\times \mathrm{P}_0+(a_l+m_l)\times(a_h+a_l+m_l)+m_h^2\times \mathrm{P}_0+m_l\times(a_h+m_l) \tag{1}$$

$$a'_h+m_h=(d^{-1}+m_l)\times(a_h+m_l)+m_l\times(d^{-1}+a_h+m_l)+m_h \tag{2}$$

$$a'_l+m_l=(d^{-1}+m_l)\times(a_h+a_l+m_l)+m_l\times(d^{-1}+a_h+m_l)+m_l \tag{3}$$

其中，a, m表示有限域GF(2^8)上任意元素，a_h, a_l, m_h, m_l, d, d^{-1}表示复合域GF(2^4)上的元素。a与a_h, a_l, m与m_h, m_l之间存在映射关系，d^{-1}为d的求逆运算值，P_0为常数。

在有限域运算中，掩码求逆的运算复杂度主要体现在乘法运算数量上。在复合域GF(2^4)上，对Ahn掩码方案运算数量进行1个统计，共需6个乘法和2个标量乘法。如果对硬件实现进行1个统计的话，1个乘法需16个与和15个异或运算共同完成，1个平方则仅需2个异或运算。

2.2 本文提出的通用低熵高阶掩码算法

基于对现有掩码方案的深入研究，本文给出一种通用低熵高阶掩码算法，核心思想是在复合域GF(2^n)上使用一类掩码值，即将m_i映射到其复合域得到m_{hi}, m_{li}，为了在算法优化中有效减少求逆运算过程所需的乘法数量，令m_{hi}=m_{li}。但有限域GF(2^k)上随机掩码值的数量并没有减少，保证了安全性。算法1是本文的通用低熵高阶掩码算法，如表1所示，其中，a代表敏感变量，m_i代表随机输入的掩码值，函数f_d, f_{bh}, f_{bl}是有限域GF(2^n)上的函数。

在算法1中，不同域之间的转换需要同构矩阵，同构矩阵的选取同样也会影响算法硬件实现的复杂度，本掩码方案中的同构矩阵采用的是域转换中比较常用的一种，同构矩阵$\boldsymbol{\delta}$, $\boldsymbol{\delta}^{-1}$如式(4)所示。

表 1　低熵通用高阶掩码算法

算法1　低熵通用高阶掩码算法

输入：经掩码值$x=a+m_1+m_2+\cdots+m_d$，掩码值$m_1,m_2,\cdots,m_d$

输出：输入值的求逆$a^{-1}+m_1+m_2+\cdots+m_d$

(1) 通过同构矩阵$\boldsymbol{\delta}$，将有限域GF(2^k)上的输入值x,m_1, m_2, $\cdots$,m_d分别映射到有限域GF(2^n)上，$(x_h,x_l)\leftarrow x$; $(m_{h1},m_{l1})\leftarrow m_1$; $(m_{h2},m_{l2})\leftarrow m_2$; $\cdots$; $(m_{hd},m_{ld})\leftarrow m_d$;

(2) 将有限域GF(2^k)上的求逆运算转化成有限域GF(2^n)上的加法、乘法，求逆运算；

(3) 利用有限域GF(2^n)上的运算求取d的掩码防护值$d+m_{h1}+m_{h2}+\cdots+m_{hd}$，

$$\begin{aligned}d+m_{h1}+m_{h2}+\cdots+m_{hd}=&f_d(x_h,(x_l+m_{h1}+m_{h2}+\cdots+m_{hd}+m_{l1}+m_{l2}+\cdots+m_{ld}),\\&(x_h+x_l+m_{l1}+m_{l2}+\cdots+m_{ld}),m_{h1},m_{h2},\cdots,m_{hd},m_{l1},m_{l2},\cdots,m_{ld},\mathrm{P}_0)\\=&{a_h}^2\times\mathrm{P}_0+a_h\times a_l+{a_l}^2+m_{h1}+m_{h2}+\cdots+m_{hd};\end{aligned}$$

(4) 在有限域GF(2^n)上对$d+m_{h1}+m_{h2}+\cdots+m_{hd}$进行掩码求逆，求逆结果为$d^{-1}+m_{h1}+m_{h2}+\cdots+m_{hd}$;

(5) 利用有限域GF(2^n)上的运算求取x_h,x_l的掩码防护值${x_h}'+m_{h1}+m_{h2}+\cdots+m_{hd}$, ${x_l}'+m_{l1}+m_{l2}+\cdots+m_{ld}$，

$$\begin{aligned}{x_h}'+m_{h1}+m_{h2}+\cdots+m_{hd}=&f_{bh}(x_h,(d^{-1}+m_{h1}+m_{h2}+\cdots+m_{hd}),\\&(x_h+m_{h1}+m_{h2}+\cdots+m_{hd}+d^{-1}+m_{h1}+m_{h2}+\cdots+m_{hd}),m_{h1},m_{h2},\cdots,m_{hd})\\=&a_h\times d^{-1}+m_{h1}+m_{h2}+\cdots+m_{hd};\\{x_l}'+m_{l1}+m_{l2}+\cdots+m_{ld}=&f_{bl}(x_h,(d^{-1}+m_{h1}+m_{h2}+\cdots+m_{hd}),(x_l+m_{h1}+m_{h2}+\cdots+m_{hd}+m_{l1}+m_{l2}+\cdots+m_{ld}),\\&(x_h+x_l+m_{l1}+m_{l2}+\cdots+m_{ld}),m_{h1},m_{h2},\cdots,m_{hd},m_{l1},m_{l2},\cdots,m_{ld})\\=&(a_h+a_l)\times d^{-1}+m_{l1}+m_{l2}+\cdots+m_{ld};\end{aligned}$$

(6) 通过同构逆矩阵$\boldsymbol{\delta}^{-1}$，将有限域GF(2^n)上的求逆结果映射回有限域GF(2^k)上，得到有限域GF(2^k)上求逆结果$a^{-1}+m_1+m_2+\cdots+m_d$。

$$\boldsymbol{\delta}=\begin{bmatrix}\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{0}\\\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}\\\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{0}\\\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{1}\\\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1}\\\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1}\end{bmatrix},$$

$$\boldsymbol{\delta}^{-1}=\begin{bmatrix}\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}\\\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}\\\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{0}\\\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}\\\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}\\\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}\end{bmatrix}\tag{4}$$

2.3　AES低熵高阶掩码方案

为验证本文给出方案的通用性，本节以AES S-box进行验证。AES S-box由非线性求逆函数和线性仿射变换两部分组成。本文方案可应用于AES非线性求逆，用f表示。f是$F_2[x]/p(x)$上的函数，$p(x)$为不可约多项式$x^8+x^4+x^3+x+1\in F_2[x]$，当$a=0$时，$f(a)=0, a\neq 0$时，$f(a)=a^{-1}$。对于AES，有限域GF($2^8$)上的求逆运算要映射到域GF($2^4$)上完成，而域GF($2^4$)上的求逆运算要映射到域GF($2^2$)上完成，因此其2阶掩码算法具体过程如表2。算法2是在通用算法1中选取两个随机掩码值，如表1所示，具体执行步骤如下：

首先，令k=8(k=2n)，按照算法2顺序执行，将经掩码的输入值映射到GF(2^4)进行运算，计算得到中间值$d^{-1}+m_{h1}+m_{h2}$；其次，令k=4，将中间值$d^{-1}+m_{h1}+m_{h2}$映射到GF(2^2)并按照算法2顺序执行，计算得到中间值$d^{-1}+m_{h1}+m_{h2}$；最后，回到算法2顺序执行(5), (6), (7)步骤，计算得到S-box经掩码输出结果。在整个求逆运算过程中，真实输入输出值、中间值均在掩码的防御之下执行运算。

3　AES低熵高阶掩码硬件实现

AES低熵高阶掩码硬件实现过程包含AES数据通路和掩码修正两个模块。为了保证算法的安全性，掩码AES架构设计中的每一轮都要添加新的掩码值(由掩码修正模块产生)，并确保所有中间值均在掩码掩护之下。图1中，X为明文，M为随机掩码值，K为密钥值，Xi, Mi分别为明文、随机掩码的中间值，Ciper out是输出的密文。

算法2对应的有限域GF(2^8)上求逆算法的结构框图如图2所示，其中X^2为有限域GF(2^4)上的平方模块，$X^2\times\mathrm{P}_0$为有限域GF(2^4)上平方与常数P_0相乘的模块，$\oplus$为有限域GF(2^4)上的异或操作，Inversion in GF(2^4)为有限域GF(2^4)上的求逆模块，其求逆过程与图2相似，不同点在于有限域GF(2^2)上的求逆过程等价于域GF(2^2)上的平方运算。

此外，本文提出的方案也同样适用于AES密钥扩展模块。密钥扩展模块是将AES算法初始128 bit密钥平均分为4组，进行密钥扩展操作，共产生44组密钥，每组32 bit。当分组的组数是4的倍数

表 2 AES低熵通用高阶掩码算法

算法2 有限域$\mathrm{GF}(2^k)$上对掩码单元$a'=a+m_1+m_2$求逆

输入：$(x=a+m_1+m_2,m_1,m_2)\in \mathrm{GF}(2^k)$

输出：$(x'=a^{-1}+m_1+m_2)$

(1) 映射$\boldsymbol{\delta}(m_1)\to(m_{h1},m_{l1})\in \mathrm{GF}(2^n)$，映射$\delta(m_2)\to(m_{h2},m_{l2})\in \mathrm{GF}(2^n)$；

(2) 映射$\delta(x)\to(x_h,x_l)\in \mathrm{GF}(2^n)$，即$\{(x_h,x_l)=(a_h+m_{h1}+m_{h2},a_h+m_{l1}+m_{l2})\}$；

(3) $d+m_{h1}+m_{h2}=(x_h)^2\mathrm{P}_0+{m_h}_1^2\mathrm{P}_0+{m_h}_2^2\mathrm{P}_0+(x_l+m_{h1}+m_{h2}+m_{l1}+m_{l2})^2+x_h(x_l+m_{h1}+m_{h2}+m_{l1}+m_{l2})+(x_h+x_l+m_{l1}+m_{l2})(m_{h1}+m_{h2})+{m_h}_1^2+{m_h}_2^2+m_{h1}+m_{h2}$；

(4) $d^{-1}+m_{h1}+m_{h2}=$算法2.$(d+m_{h1}+m_{h2},m_{h1},m_{h2})$；

(5) ${x_h}'+m_{h1}+m_{h2}=x_h(d^{-1}+m_{h1}+m_{h2})+(x_h+d^{-1}+m_{h1}+m_{h2}+m_{h1}+m_{h2})(m_{h1}+m_{h2})+m_{h1}+m_{h2}$；

(6) ${x_l}'+m_{l1}+m_{l2}=x_h(d^{-1}+m_{h1}+m_{h2})+(x_l+m_{h1}+m_{h2}+m_{l1}+m_{l2})(d^{-1}+m_{h1}+m_{h2})+(x_h+x_l+m_{l1}+m_{l2})(m_{h1}+m_{h2})+{m_h}_1^2+{m_h}_2^2+m_{l1}+m_{l2}text$

(7) 映射$\delta^{-1}({x_h}'+m_{h1}+m_{h2},{x_l}'+m_{l1}+m_{l2})\to(a^{-1}+m_1+m_2)$。

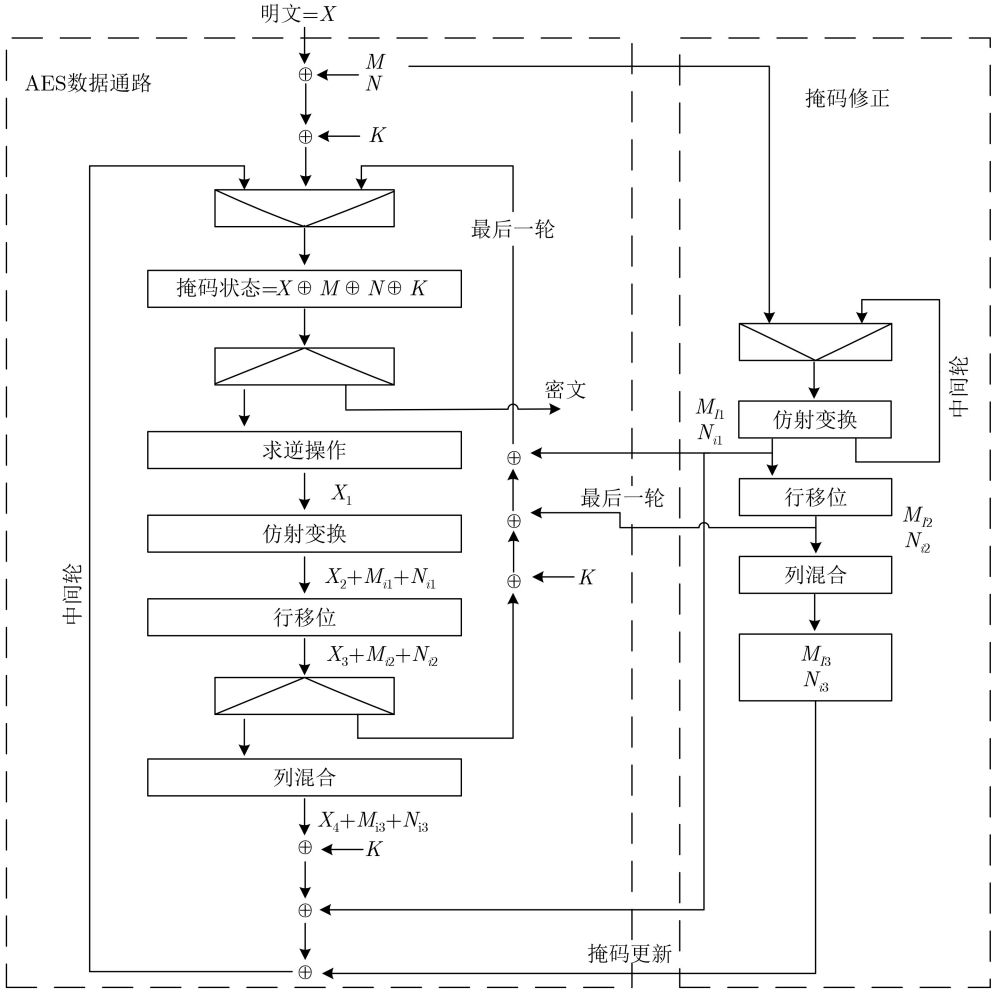


图 1 AES高阶掩码实现流程

时，需执行密钥扩展唯一的非线性操作字节替换，共需4个S-box，其与轮操作中的S-box相同，所以本文给出的方案也适用于密钥扩展模块。进行密钥扩展时，首先将128 bit密钥与随机掩码进行异或，然后分成4组分别进行密钥扩展，并采用本文提出的方案进行掩码。由于密钥扩展产生的密钥添加了掩码，为了得到正确的密文，在进行密钥加操作后要去掉密钥的掩码值，由于列混合操作的中间值是带有掩码的数据，因此不会暴露真实的中间结果。

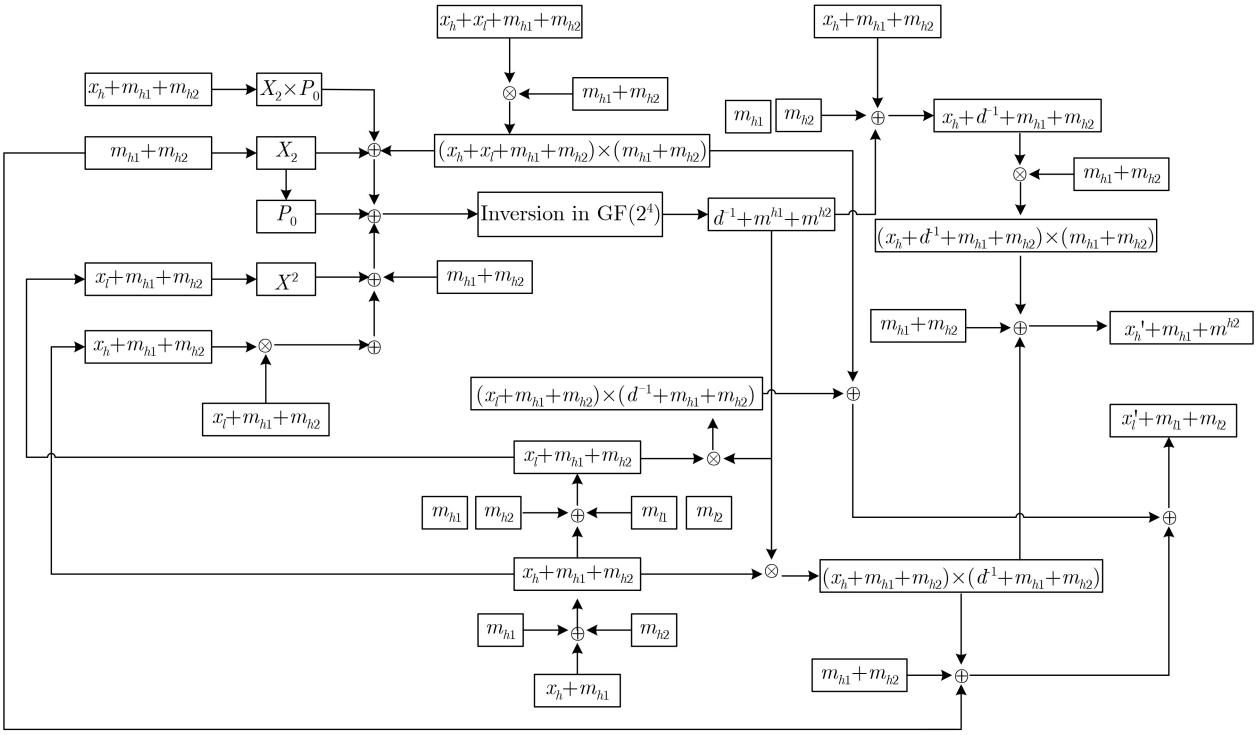


图 2 有限域GF(2^8)求逆算法结构

4　结果分析与比较

4.1　功能验证

为验证采用本文方案的S-box, AES算法逻辑功能的正确性，本文运用Verilog语言及相应的EDA工具分别对S-box, AES算法的不同掩码方案进行了功能仿真和逻辑综合。图3(a)—图3(c)为S-box非掩码、1阶掩码、2阶掩码的部分功能验证结果，图3(d)—图3(f)为AES非掩码、1阶掩码、2阶掩码的部分功能验证结果。通过对比，图3中功能验证结果均是正确的，这也进一步表明本文给出的算法能够适用于AES，并得到正确的功能。

4.2　掩码复杂度比较

表3给出了在复合域GF(2^4)上不同掩码方案的乘法、标量乘法、平方运算的数量。与文献[18]相比，本文方案降低了1个乘法运算，即便增加了2个平方运算，但根据前面分析可知引入的资源是十分有限的。对比不同掩码方案结果表明，本文掩码方案需要的运算数量虽不是最少，但占用的资源却是最少的，能够得到低面积复杂度的硬件实现。

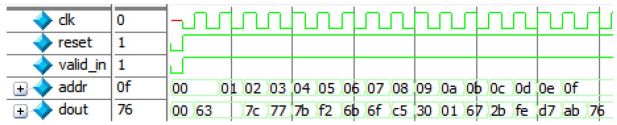
表4中给出了S-box不同掩码方案的总逻辑单元、总寄存器的数量。由于仅实现了S-box模块，所以占用的资源极少。由于本文给出的算法具有通用性，不但适用于任意分组密码S-box，同样适用于任意阶掩码，因此本文1阶、2阶掩码方案相差约14.7%。2阶较1阶掩码仅增加1个输入掩码及几个异或操作，并没有增加运算数量，因此本文方案在高阶掩码中具有一定的优势。

表5中给出了AES不同掩码方案的资源占用情况。从结果来看，本文2阶掩码方案的资源占用情况甚至要小于Oswald1阶掩码方案。由于Ahn等人提出的是软件实现的掩码方案，若要实现高阶掩码，需要重新进行设计，不具通用性。本文2阶较1阶掩码资源占用相差约25.2%，主要由于新增了一个掩码及相关异或操作，掩码修正模块也增加了对此掩码的修正及相关操作，因此带来一部分资源的增加也是正常的。综合分析结果显示，本文给出的方案不论是在算法灵活性还是在资源占用等方面均具有一定优势，存在一定价值。

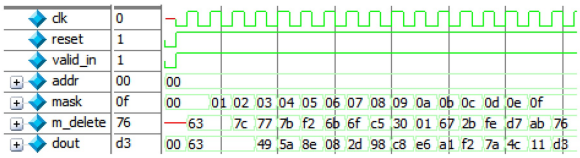
4.3　综合结果

为了更加接近实际的芯片面积，本文采用TSMC 40 nm标准工艺库，利用EDA工具Synopsys DC对采用本文掩码方案的S-box, AES进行了综合分析，分别给出了本文方案的S-box, AES的非掩码、1阶掩码、2阶掩码的综合情况(如表6所示)。

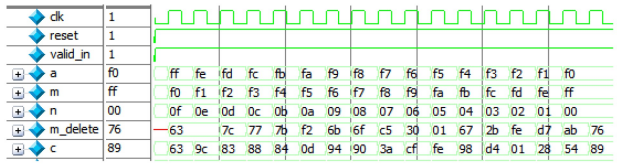
进行综合之后，利用EDA工具DC产生的网表文件作为自动布局布线工具ICC的输入文件，对S-box的非掩码、1阶掩码、2阶掩码版图进行面积优化，设置工作频率为50 MHz，芯片利用率为0.6的情况下，得到S-box不同掩码阶数的版图面积分别为24.4×24.1 μm^2, 32.5×32.6 μm^2, 34.6×33.5 μm^2(如图4所示)。



(a) S-box的非掩码仿真结果

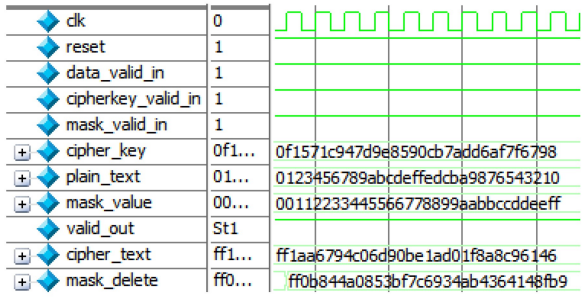


(b) S-box的1阶掩码仿真结果

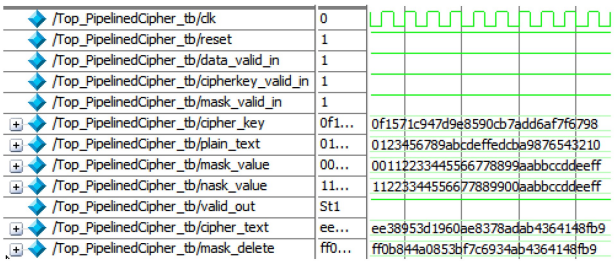


(c) S-box的2阶掩码仿真结果

(d) 非掩码AES加密结果



(e) 1阶掩码AES加密结果



(f) 2阶掩码AES加密结果

图 3 S-box, AES的不同掩码功能验证结果

表 3 不同方案的S-box实现对比

	乘法	标量乘法	平方
非掩码	3	1	1
Oswald[12]	9	2	2
汪鹏君[17]	6	2	2
Ahn[18]	6	2	0
本文方法	5	2	2

表 4 不同S-box方案实现结果对比情况

思想	总的逻辑单元	总的寄存器
非掩码	102(<1%)	8(<1%)
Oswald[12]1阶掩码	247(<1%)(142.2%)	8(<1%)
汪鹏君[17]1阶掩码	202(<1%)(98%)	8(<1%)
Ahn[18]1阶掩码	188(<1%)(84.3%)	8(<1%)
本文方法1阶掩码	178(<1%)(74.5%)	8(<1%)
本文方法2阶掩码	193(<1%)(89.2%)	8(<1%)

表 5 不同AES方案实现结果对比方案

思想	总的逻辑单元	组合逻辑	总的寄存器
非掩码	23890(21%)	19811(17%)	10769(9%)
Oswald[12]1阶掩码	45549(40%)(90.7%)	40368(35%)(103.8%)	16036(14%)(48.9%)
汪鹏君[17]1阶掩码	42161(37%)(76.5%)	36584(32%)(84.7%)	13780(12%)(28%)
Ahn[18]1阶掩码	42087(37%)(76.2%)	36510(32%)(84.3%)	12820(11%)(19%)
本文方法1阶掩码	38456(34%)(60.9%)	32879(28%)(66.1%)	12820(11%)(19%%)
本文方法2阶掩码	44475(39%)(86.1%)	38282(33%)(93.2%)	18980(17%)(76.2%%)

基础硬件综合条件与上述S-box相同，得到AES不同掩码阶数的硬件综合结果(如表7所示)。

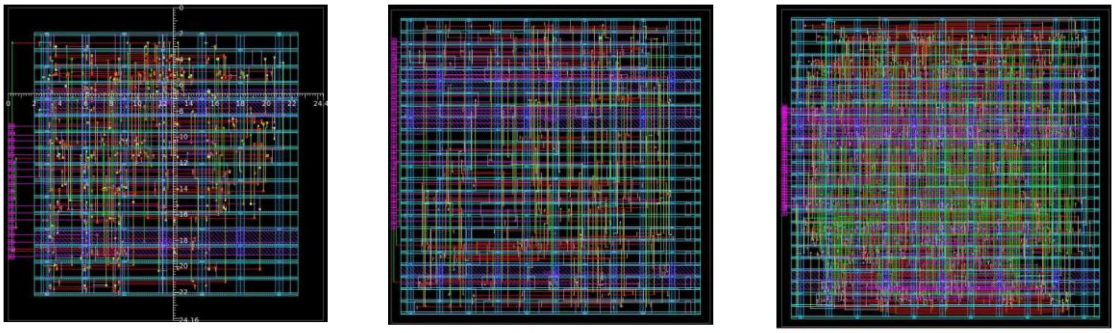
在工作频率为25 MHz，芯片利用率为0.7的情况下对AES不同掩码阶数进行自动布局布线，并对版图面积进行了优化，得到AES不同掩码阶数版图面积分别为310.5×309.9 μm^2, 401.9×402 μm^2, 561×560 μm^2(如图5所示)。

5 结束语

本文提出一种适用于分组加密算法的通用低熵高阶掩码方案，采用基于复合域的低熵掩码及关键模块复用设计，有效降低复合域求逆过程中的算法复杂度。将该算法应用于AES后，与文献[12,17,18]实现结果相比较，在面积上分别减少了27.9%, 11.9%, 5.3%，同时对该方案的安全性进行了理论验证，并

表 6　本方案S-box不同掩码阶数的综合结果

掩码阶数	逻辑名称	逻辑面积(μm²)	合计(μm²)
非掩码S-box	组合逻辑，缓冲器/反相器逻辑，非组合逻辑	221, 14, 46	268
1阶掩码S-box	组合逻辑，缓冲器/反相器逻辑，非组合逻辑	489, 19, 88	577
2阶掩码S-box	组合逻辑，缓冲器/反相器逻辑，非组合逻辑	551, 22, 88	639

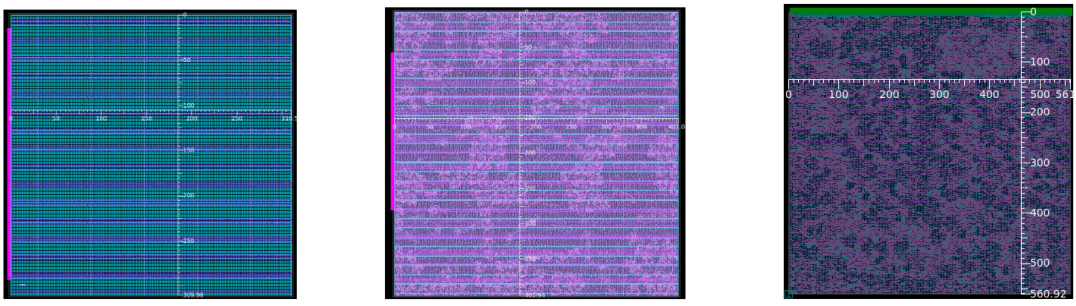


(a) 非掩码S-box版图　(b) 1阶掩码S-box版图　(c) 2阶掩码S-box版图

图 4 S-box不同掩码阶数的版图

表 7　本方案AES不同掩码阶数的综合结果

掩码阶数	逻辑名称	逻辑面积(μm²)	合计(μm²)
非掩码AES	组合逻辑，缓冲器/反相器逻辑，非组合逻辑	14484, 586, 53834	67518
1阶掩码AES	组合逻辑，缓冲器/反相器逻辑，非组合逻辑	53626, 2888, 59614	113241
2阶掩码AES	组合逻辑，缓冲器/反相器逻辑，非组合逻辑	116797, 4594, 100564	217361



(a) 非掩码AES版图　(b) 1阶掩码AES版图　(c) 2阶掩码AES版图

图 5 AES不同掩码阶数的版图

给出了详细的功能验证及硬件综合结果。下一步将搭建DPA攻击平台，对本文算法的安全性进行实验验证。

参 考 文 献

[1] HUANG Hai, LIU Leibo, HUANG Qihuan, *et al*. Low area-overhead low-entropy masking scheme (LEMS) against correlation power analysis attack[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2019, 38(2): 208–219. doi: 10.1109/TCAD.2018.2802867.

[2] 欧庆于, 罗芳, 叶伟伟, 等. 分组密码算法抗故障攻击能力度量方法研究[J]. 电子与信息学报, 2017, 39(5): 1266–1270. doi: 10.11999/JEIT160548.

OU Qingyu, LUO Fang, YE Weiwei, *et al*. Metric for defences against fault attacks of block ciphers[J]. *Journal of Electronics & Information Technology*, 2017, 39(5): 1266–1270. doi: 10.11999/JEIT160548.

[3] CORON J S, GREUET A, PROUFF E, *et al*. Faster evaluation of sboxes via common shares[C]. The 18th International Conference on Cryptographic Hardware and Embedded Systems, Santa Barbara, USA, 2016: 498–514. doi: 10.1007/978-3-662-53140-2_24.

[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] 汪鹏君, 张跃军, 张学龙. 防御差分功耗分析攻击技术研究[J]. 电子与信息学报, 2012, 34(11): 2774–2784. doi: 10.3724/SP.J.1146.2012.00555.
WANG Pengjun, ZHANG Yuejun, and ZHANG Xuelong. Research of differential power analysis countermeasures[J]. *Journal of Electronics & Information Technology*, 2012, 34(11): 2774–2784. doi: 10.3724/SP.J.1146.2012.00555.

[6] 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.

[7] CORON J S. Higher order masking of look-up tables[C]. The 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques Advances in Cryptology, Berlin, Germany, 2014: 441–458.

[8] 徐佩. 智能卡AES加密模块抗侧信道攻击掩码技术研究与实现[D]. [硕士论文], 重庆大学, 2015: 26–53.
XU Pei. Research and implementation with mask technology on AES encryption module of smartcard against side channel attack[D]. [Master dissertation], The Chongqing University, 2015: 26–53.

[9] CARLET C and PROUFF E. Polynomial evaluation and side channel analysis[M]. RYAN P Y A, NACCACHE D, and QUISQUATER J J. The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday. Berlin, Heidelberg: Springer, 2016: 315–341. doi: 10.1007/978-3-662-49301-4_20.

[10] 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.

[11] 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]. 2012 Design, Automation & Test in Europe Conference & Exhibition, Dresden, Germany, 2012: 1173–1178.

[12] OSWALD E, MANGARD S, PRAMSTALLER N, *et al*. A side-channel analysis resistant description of the AES s-box[C]. The 12th International Workshop on Fast Software Encryption, Paris, France, 2005: 413–423. doi: 10.1007/11502760_28.

[13] ZAKERI B, SALMASIZADEH M, MORADI A, *et al*. Compact and secure design of masked AES s-box[C]. The 9th International Conference on Information and Communications Security, Zhengzhou, China, 2007: 216–229.

[14] TRICHINA E and KORKISHKO T. Secure AES hardware module for resource constrained devices[C]. Proceedings of the 1st European Workshop on Security in Ad-hoc and Sensor Networks, Heidelberg, Germany, 2005: 215–229. doi: 10.1007/978-3-540-30496-8_18.

[15] OSWALD E and SCHRAMM K. An efficient masking scheme for AES software implementations[C]. The 6th International Workshop on Information Security Applications. Jeju Island, Korea, 2006: 292–305.

[16] KIM H S, HONG S, and LIM J. A fast and provably secure higher-order masking of AES s-box[C]. Proceedings of the 13th International Conference on Cryptographic Hardware and Embedded Systems. Nara, Japan, 2011: 95–107.

[17] 汪鹏君, 郝李鹏, 张跃军. 防御零值功耗攻击的AES SubByte模块设计及其VLSI实现[J]. 电子学报, 2012, 40(11): 2183–2187. doi: 10.3969/j.issn.0372-2112.2012.11.007.
WANG Pengjun, HAO Lipeng, and ZHANG Yuejun. Design of AES subbyte module of anti-zero value power attack and its VLSI implementation[J]. *Acta Electronica Sinica*, 2012, 40(11): 2183–2187. doi: 10.3969/j.issn.0372-2112.2012.11.007.

[18] AHN S and CHOI D. An improved masking scheme for s-box software implementations[C]. The 16th International Workshop on Information Security Applications, Jeju Island, Korea, 2016: 200–212.

姜久兴：男，1963年生，教授，研究方向为集成电路设计.
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.
黄 海：男，1982年生，副教授，研究方向为信息安全，数字信号处理及集成电路设计等.
厚 娇：女，1988年生，硕士生，研究方向为计算机网络与信息安全.
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.