基于多因子CSE算法的AES S-盒电路优化设计

曾 纯,吴 宁,张肖强,周 芳,叶云飞
(南京航空航天大学电子信息工程学院,江苏南京 210016)

摘 要: 针对高级加密标准(AES)S-盒优化,提出了一种新的多因子公共项消除(CSE)优化算法.多因子CSE算法通过对组合逻辑表达式中所含因子最多的公共项优先消除,以简化逻辑表达式,从而有效地减少S-盒电路结构中的GF(2^4)域乘法逆电路和映射矩阵电路的面积和时延.结果表明,多因子CSE算法具有计算速度快,优化效率高的特点.优化后的S-盒组合逻辑电路采用0.18μm CMOS工艺,设计出的S-盒面积-延时积比目前最小面积和最短延时的S-盒组合逻辑电路分别减少了10.32%和19.64%.

关键词: AES; S-盒; 多因子CSE算法
中图分类号: TN918.4 **文献标识码:** A **文章编号:** 0372-2112 (2014)06-1238-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.06.032

The Optimization Circuit Design of AES S-Box Based on a Multiple-Term Common Subexpression Elimination Algorithm

ZENG Chun, WU Ning, ZHANG Xiao-qiang, ZHOU Fang, YE Yun-fei
(*College of Electrical and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu* 210016, *China*)

Abstract: Aiming at the optimization of advanced encryption standard (AES) S-box, a novel multiple-term common subexpression elimination (CSE) algorithm was proposed. In order to simplify the combinational logic expressions, the common subexpressions containing the most factors took priority to be eliminated in the proposed approach, thus effectively reduced the area and latency of the GF(2^4) multiplicative inverse circuit and the isomorphic mapping circuit in S-box. The results show that the multiple-term CSE algorithm achieves high computation and optimization efficiency. The optimized S-box is implemented in 0.18μm CMOS technology. Compared with the smallest S-box and the shortest delay S-box in the existing work, the optimized S-box saves about 10.32% and 19.64% of the area-delay product separately.

Key words: advanced encryption standard (AES); S-box; multiple-term common subexpression elimination (CSE) algorithm

1 引言

AES加密算法是目前常用的分组加密算法[1,2],而S-盒运算电路是AES硬件实现中资源消耗最多、功耗最大的部分,是AES硬件电路优化的关键[3].

本文所研究的S-盒基于GF(((2^2)^2)^2)复合域运算,并采用纯组合逻辑电路实现.这种S-盒硬件面积小,方便流水线结构设计和加解密复用.针对小面积、低时延的高性能S-盒研究,目前,有许多文献基于正规基[3,5,6,11]和多项式基[4,7~10,12]的复合域运算提出了多种设计方案.文献[5]基于正规基运算实现S-盒,所实现的S-盒具有最小的面积,但是其时延较长;文献[9]基于多项式基的复合域GF((2^4)^2)运算实现的S-盒,具有最短的时延,但其实现面积较大.影响S-盒电路优化的主要部分是其中的多常数乘法(Multiple Constant Multiplication, MCM)运算电路,包括仿射矩阵电路、映射矩阵电路等.对MCM电路的优化,常用公共项消除(Common Subexpression Elimination, CSE)算法[13],文献[5]提出了基于穷举算法的CSE(Exhaust-CSE)算法,文献[7]提出基于贪婪算法的CSE(Greedy-CSE)算法,Greedy-CSE算法简单但容易陷入局部最优的结果中,Exhaust-CSE算法优化效果好但计算速度慢.本文综合考虑S-盒电路实现的面积和时延,基于正规基计算出S-盒电路组合逻辑表达式,并提出一种计算速度快、优化效率高的多因子CSE算法优化S-盒中GF(2^4)域乘法逆电路和映射矩阵乘法电路,使S-盒电路达到非常小的面积-延时积.

收稿日期:2013-02-18;修回日期:2013-07-23;责任编辑:覃怀银
基金项目:国家自然科学基金资助项目(No.61376025, No.61106018);江苏省产学研前瞻性联合研究项目(No.BY2013003-11)

2　AES S-盒复合域电路实现

S-盒的复合域运算包括 GF(2^8)域乘法逆运算和仿射运算,如表达式(1)所示.

$$\boldsymbol{F}^{\mathrm{T}} = \boldsymbol{M}(\boldsymbol{\delta}^{-1}(\boldsymbol{\delta}\boldsymbol{X}^{\mathrm{T}})^{-1}) + \boldsymbol{V}^{\mathrm{T}} \tag{1}$$

式中:上标 T 为向量的转置符,$\boldsymbol{X}$ 为输入向量,$\boldsymbol{M}$ 为仿射矩阵,$\boldsymbol{V}$ 为仿射运算过程的常向量,$\boldsymbol{F}$ 为 S-盒变换后输出向量[4],$\boldsymbol{\delta}$ 和 $\boldsymbol{\delta}^{-1}$为基于复合域乘法逆运算的映射矩阵和反映射矩阵.$\boldsymbol{\delta}$ 与 $\boldsymbol{\delta}^{-1}$的关系为 $\boldsymbol{\delta}\times\boldsymbol{\delta}^{-1} = \boldsymbol{E}$,$\boldsymbol{E}$ 为单位矩阵.$\boldsymbol{M}$ = [0x8E,0xC7,0xE3,0xF1,0xF8,0x7C,0x3E,0x1F],$\boldsymbol{V}$ = [0x63],矩阵的行向量采用 16 进制表示.通常,将仿射运算矩阵和反映射矩阵合并为一个矩阵 $\boldsymbol{L}$ 以简化电路结构,则 $\boldsymbol{L} = \boldsymbol{M}\boldsymbol{\delta}^{-1}$.

基于复合域运算的 S-盒电路实现结构框图如图 1(*a*)所示.其中,GF(2^8)域乘法逆运算电路包括复合域乘法逆电路和 $\boldsymbol{\delta}$、$\boldsymbol{\delta}^{-1}$映射电路两大部分.

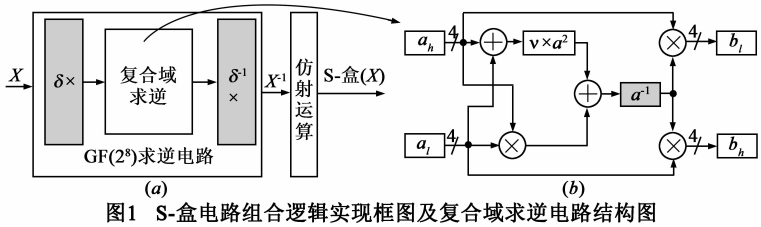

图1　S-盒电路组合逻辑实现框图及复合域求逆电路结构图

选取复合域 GF((2^4)^2)的正规基(Y^{16},Y)和不可约多项式 $f(y) = y^2 + y + \upsilon$,系数 $\upsilon \in$ GF(2^4),得到 GF((2^4)^2)域的乘法逆运算表达式如表达式(2)所示[5],乘法逆电路结构如图 1(*b*)所示.

$$\begin{aligned} b &= b_h Y^{16} + b_l Y = a^{-1} \\ &= (a_h a_l + (a_h^2 + a_l^2)\upsilon)^{-1}(a_l Y^{16} + a_h Y) \end{aligned} \tag{2}$$

式中,a,$b \in$ GF(2^8);a_h,a_l,b_h,$b_l \in$ GF(2^4).

选取复合域 GF((2^2)^2)的正规基(Z^4,Z)和不可约多项式 $f(z) = z^2 + z + N$,系数 $N \in$ GF(2^2).选取系数 $\upsilon = (0001)_4$,$N = (10)_2$,可以求得 $\boldsymbol{\delta}$ = [0x98,0xF3,0xF2,0x48,0x09,0x81,0xA9,0xFF]和 $\boldsymbol{\delta}^{-1}$ = [0x64,0x78,0x6E,0x8C,0x68,0x29,0xDE,0x60][5].

AES S-盒通过基于正规基复合域电路实现[5],得到的各部分运算电路资源消耗和关键路径如表 1 所示.其中,XOR 表示异或门,AND 表示与门.

表 1　AES S-盒各部分电路资源消耗和关键路径

复合域乘法逆					$\boldsymbol{\delta}$		$\boldsymbol{L}$		S-盒			
电路	资源消耗		关键路径		资源	路径	资源	路径	资源消耗		关键路径	
	XOR	AND	XOR	AND	XOR	XOR	XOR	XOR	XOR	AND	XOR	AND
GF(2^4)域乘法逆	14	9	5	1								
GF(2^4)域乘法器	10	9	5	1	24	3	17	3	111	36	22	3
$\upsilon \times a^2$	3	– –	1	– –								
GF(2^8)域乘法逆	70	36	16	3								

3　多因子 CSE 算法

3.1　多因子 CSE 算法描述

Exhaust-CSE 和 Greedy-CSE 算法都是基于双因子 CSE 算法,即每个公共项仅含有两个和项.针对双因子 CSE 算法的缺陷,本文提出了一种多因子 CSE 优化算法.多因子 CSE 优化算法关注公共项中因子数目,在每次迭代中将所含因子数目最多的公共项作为消除对象.若消除对象不止一个,则采用穷举算法将每个消除对象都计算一遍.

多因子 CSE 优化算法具体流程为:

(1)识别逻辑表达式中所有的公共项;

(2)选择所含因子数目最多的公共项;

(3)从(2)中选择出现次数最多的公共项作为消除对象;

(4)采用新因子代替选择的公共项;

(5)重复(1)~(4),直到表达式中没有公共项为止.

以乘矩阵[0x1,0xf,0xf,0x9]电路为例,用多因子 CSE 算法合并逻辑表达式中公共项的运算过程如表达式(3)所示.

$$\begin{bmatrix} y_4 \\ y_3 \\ y_2 \\ y_1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} x_4 \\ x_3 \\ x_2 \\ x_1 \end{bmatrix} = \begin{bmatrix} x_3 + x_2 + x_1 \\ x_3 + x_2 \\ x_3 + x_2 \\ x_4 + x_3 + x_2 + x_1 \end{bmatrix}$$
$$= \begin{bmatrix} (x_3 + x_2 + x_1)_{b_1} \\ x_3 + x_2 \\ x_3 + x_2 \\ x_4 + b_1 \end{bmatrix} = \begin{bmatrix} ((x_3 + x_2)_{b_2} + + x_1)_{b_1} \\ b_2 \\ b_2 \\ x_4 + b_1 \end{bmatrix} \tag{3}$$

选择公共项 $x_3 + x_2 + x_1$合并为新因子 b_1,第二轮选择公共项 $x_3 + x_2$合并为新因子 b_2.采用多因子 CSE 算法对逻辑组合电路优化的过程与结果如图 2 所示.

3.2　多因子 CSE 算法性能分析

CSE 算法中需要合并的公共项数量(即 CSE 迭代次

数)是一个概率事件,可以采取建立概率模型的方法对CSE算法的复杂度进行分析.由于这个概率模型不属于本文的研究范围,因此本文采用事后统计的方法来分析CSE算法的性能.

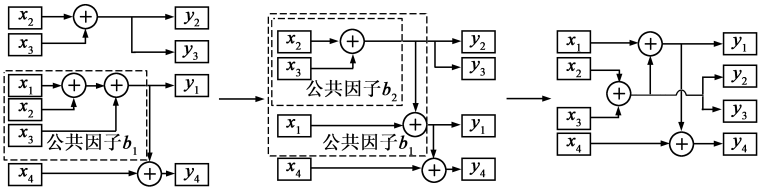

图2 CSE算法合并逻辑组合电路中公共项

在标准基系数$(\lambda,\varphi)=((1100)_2,(10)_2)$下,选取8组矩阵$L_1\sim L_8$作为测试矩阵,分别采用Greedy-CSE算法、Exhaust-CSE算法和多因子CSE算法进行优化.通过Matlab仿真,记录三种算法对每组测试矩阵进行优化的计算时间如图3所示,其中Exhaust-CSE算法计算时间超过1s的,在图中均按1s显示.

由图3可知,多因子CSE算法远比Exhaust-CSE算法快,比Greedy-CSE算法平均计算时间缩短了47.8%.对各CSE算法的计算时间测试结果表明,多因子CSE算法具有计算速度快的特点.

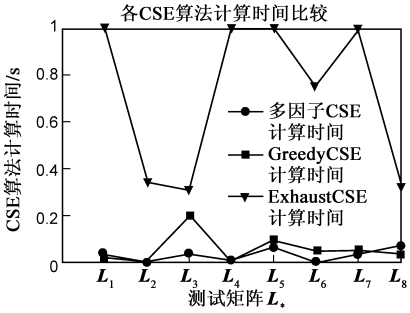

图3 各CSE算法优化测试矩阵性能分析曲线

4 基于多因子CSE算法的S-盒电路优化

4.1 基于多因子CSE算法的GF(2^4)域乘法逆电路优化

选择GF(2^4)域的正规基(Z^4,Z)[5],其乘法逆表达式如式(4)所示,式中$c\in GF(2^4)$,$c_h,c_l\in GF(2^2)$.选择GF(2^2)域的正规基(W^2,W),其乘法运算如表达式(5)所示,乘法逆电路如表达式(6)所示,式中$m,n\in GF(2^2)$,$m_h,m_l,n_h,n_l\in GF(2)$.

$$c^{-1}=(c_hc_l+(c_h+c_l)^2N)^{-1}(c_lZ^4+c_hZ) \tag{4}$$

$$\begin{aligned}m\times n=&(m_hn_h+(m_h+m_l)(n_h+n_l))W^2\\&+(m_ln_l+(m_h+m_l)(n_h+n_l))W)\end{aligned} \tag{5}$$

$$m^{-1}=m_lW^2+m_hW \tag{6}$$

结合表达式(4)~(6),取$N=(10)_2$,可计算出正规基下GF(2^4)域乘法逆组合逻辑表达式如表达式(7)所示,式中,$c_1,c_2,c_3,c_4\in GF(2)$.如表达式(7)所示,表达式中既包含了与门又包含了异或门,所用门电路资源为18XOR+16AND,关键路径为4XOR+2AND.采用多因子CSE算法来优化组合逻辑表达式:首先对与门进行CSE优化;再对异或门CSE优化,优化结果如表达式(7)所示.

$$\begin{aligned}\begin{pmatrix}c_3\\c_2\\c_1\\c_0\end{pmatrix}^{-1}&=\begin{pmatrix}c_2c_1c_0+c_3c_1+c_2c_1+c_1+c_0\\c_3c_1c_0+c_3c_1+c_2c_1+c_2c_0+c_0\\c_3c_2c_0+c_3c_1+c_3c_0+c_3+c_2\\c_3c_2c_1+c_3c_1+c_3c_0+c_2c_0+c_2\end{pmatrix}\\&=\begin{pmatrix}(c_2c_1)_{b_3}c_0+(c_3c_1)_{b_1}+b_3+c_1+c_0\\b_1c_0+b_1+b_3+((c_2c_0)_{b_4}+c_0\\b_2c_2+b_1+(c_3c_0)_{b_2}+c_3+c_2\\b_1c_2+b_1+b_2+b_4+c_2\end{pmatrix}\\&=\begin{pmatrix}(c_2c_1)_{b_3}c_0+((c_3c_1)_{b_1}+b_3+c_0)_{c_4}+c_1\\b_1c_1+(c_2c_0)_{b_4}+c_4\\(c_3c_0)_{b_2}c_2+(b_1+b_2+c_2)_{c_3}+c_3\\b_1c_2+b_4+c_5\end{pmatrix}\end{aligned} \tag{7}$$

从(7)的计算结果可直观的看出,采用多因子CSE算法对GF(2^4)域乘法逆电路优化计算后,电路仅需要资源12XOR+8AND,关键路径为3XOR+1AND.优化后电路资源节省了25.0% XOR和55.6% AND,关键路径缩短25.0% XOR和50.0% AND.

4.2 基于多因子CSE算法的仿射运算和映射矩阵综合化简

根据表达式(1),$\boldsymbol{L}=\boldsymbol{M}\boldsymbol{\delta}^{-1}$,则$\boldsymbol{M}$和$\boldsymbol{\delta}^{-1}$矩阵乘积结果为$\boldsymbol{L}=[0x58,0x2D,0x9E,0x0B,0xDC,0x04,0x03,0x24]$.

采用多因子CSE算法对$\boldsymbol{\delta}$和$\boldsymbol{L}$电路的优化过程及结果如式(8)和式(9)所示.

$$\boldsymbol{\delta X}^{\mathrm{T}}=\begin{bmatrix}1&1&1&0&0&1&1&1\\0&1&1&1&0&0&0&1\\0&1&1&0&0&0&1&1\\1&1&1&0&0&0&0&1\\1&0&0&1&1&0&1&1\\0&0&0&0&0&0&0&1\\0&1&1&0&0&0&0&1\\0&1&0&0&1&1&1&1\end{bmatrix}\begin{bmatrix}x_7\\x_6\\x_5\\x_4\\x_3\\x_2\\x_1\\x_0\end{bmatrix}=\begin{bmatrix}x_7+x_6+x_5+x_2+x_1+x_0\\x_6+x_5+x_4+x_0\\x_6+x_5+x_1+x_0\\x_7+x_6+x_5+x_0\\x_7+x_4+x_3+x_1+x_0\\x_0\\x_6+x_5+x_0\\x_6+x_3+x_2+x_1+x_0\end{bmatrix}=\begin{bmatrix}x_7+x_5+(x_6+x_2+(x_1+x_0)_{x_{10}})_{x_8}\\(x_6+x_5+x_0)_{x_9}+x_4\\x_9+x_1\\x_9+x_7\\x_7+x_4+x_3+x_{10}\\x_0\\x_9\\x_8+x_3\end{bmatrix}\tag{8}$$

$$\boldsymbol{LY}^{\mathrm{T}}=\begin{bmatrix}0&0&1&0&1&0&0&0\\1&0&0&0&1&0&0&0\\0&1&0&0&0&0&0&1\\1&0&1&0&1&0&0&0\\1&1&1&1&1&0&0&0\\0&1&1&0&1&1&0&1\\0&0&1&1&0&0&1&0\\0&1&0&1&0&0&1&0\end{bmatrix}\begin{bmatrix}y_7\\y_6\\y_5\\y_4\\y_3\\y_2\\y_1\\y_0\end{bmatrix}=\begin{bmatrix}y_5+y_3\\y_7+y_3\\y_6+y_0\\y_7+y_5+y_3\\y_7+y_6+y_5+y_4+y_3\\y_6+y_5+y_3+y_2+y_0\\y_5+y_4+y_1\\y_6+y_4+y_0\end{bmatrix}=\begin{bmatrix}(y_5+y_3)_{y_9}\\y_7+y_3\\(y_6+y_0)_{y11}\\(y_7+y_9)_{y_8}\\y_8+(y_6+y_4)_{y_{10}}\\y_{11}+y_9+y_2\\y_5+y_4+y_1\\y_{10}+y_0\end{bmatrix}\tag{9}$$

由表达式(8)和表达式(9)可知,$\boldsymbol{\delta}$ 和 $\boldsymbol{M\delta}^{-1}$矩阵乘电路采用 CSE 算法优化后分别节省资源 41.7% XOR 和 35.3% XOR.

5　S-盒优化结果及分析

在复合域中,采用多因子 CSE 算法对 AES S-盒进行优化,各模块电路的资源消耗和关键路径如表 2 所示.

表 2 与表 1 相比,S-盒中 GF(2^4)域乘法逆电路资源优化了 14.3% XOR 和 11.1% AND,关键路径减少了 40.0% XOR;映射-仿射电路资源共优化了 39.0% XOR,关键路径减少了 40.0% XOR. 优化后 S-盒所需资源比优化前共节省 16.2% XOR 和 2.8% AND,关键路径缩短了 9.1% XOR.

表 2　采用多因子 CSE 算法优化的 S-盒各部分电路资源消耗和关键路径

复合域乘法逆					$\boldsymbol{\delta}$		$\boldsymbol{L}$		*S*-盒			
电路	资源消耗		关键路径		资源	路径	资源	路径	资源消耗		关键路径	
	XOR	AND	XOR	AND	XOR	XOR	XOR	XOR	XOR	AND	XOR	AND
GF(2^4)域乘法逆	12	8	3	1	14	3	11	3	93	35	20	3
GF(2^4)域乘法器	10	9	5	1								
$\upsilon\times a^2$	3	– –	1	– –								
GF(2^8)域乘法逆	68	35	14	3								

表 3　各方案的资源消耗和关键路径比较

方案	映射-仿射电路		GF(2^4)域乘法逆电路				S-盒			
	资源消耗	关键路径	资源消耗		关键路径		资源消耗		关键路径	
	XOR	XOR	XOR	AND	XOR	AND	XOR	AND	XOR	AND
[3]case Ⅲ	– –	– –	13	8	3	1	117	35	20	3
[5]	– –	– –	9	2NOR + 2NAND + 6AND	5	2	91	36	22	4
[6]case Ⅲ	29	6	13	9	5	2	96	36	20	4
[7]	– –	– –	– –	– –	– –	– –	126	36	25	4
[8]	– –	– –	– –	– –	– –	– –	123	36	23	4
[9]	31	8	14	9	3	2	120	35	19	4
本文	25	6	12	8	3	1	93	35	20	3

与论文[3,5~9]比较映射-仿射电路、$GF(2^4)$域乘法逆电路以及 S-盒电路性能,其所需资源和关键路径如表 3 所示.

由表 3 可知,在映射-仿射电路方面,与文献[6]和[9]相比,本文具有最小的资源消耗和最短的关键路径.在 $GF(2^4)$域乘法逆电路方面,本文 S-盒和文献[3]均有最短的关键路径,而资源节省了 7.7% XOR 和 11.1% AND;与文献[5]相比,本文的 $GF(2^4)$域乘法逆电路资源消耗稍微增加,但关键路径缩短了 40.0% XOR 和 50.0% AND.结果表明,多因子 CSE 算法具有较高的电路优化效率,采用多因子 CSE 算法优化的映射-仿射电路和 $GF(2^4)$域乘法逆电路均有较好的面积-延时性能.

比较整个 S-盒电路性能,论文[5]虽然具有最小的电路面积,但其牺牲了电路时延特性;论文[9]虽然具有最优的时延特性,但其电路面积较大.本文优化的 S-盒电路对面积和时延特性进行了折衷,相比于文献[5],在有限增加资源消耗的基础上,时延缩短了 9.1% XOR 和 25.0% AND,相比于文献[9],在时延相当的前提下,资源节省了 22.5% XOR.

采用 0.18μm CMOS 工艺,2 输入 1 输出 XOR 门面积为 26.6112μm^2,标准时延 1ns,2 输入 1 输出 AND 门面积为 13.3056μm^2,标准时延 1ns.由此计算本文和论文[5]、论文[9]的 S-盒组合逻辑电路的面积和时延结果如表 4 所示.

表 4 0.18μm COMS 技术综合 S-盒组合逻辑电路

方案	时延(ns)	面积(μm^2)	面积-延时积(μm^2·ns)
文[5]	26	2900.6208	75416.1408
文[9]	23	3659.0400	84157.9200
本文	23	2940.5376	67632.3648

根据表 4 数据计算,多因子 CSE 算法优化后的 S-盒面积-延时积比论文[5]减少了 10.32%,比论文[9]减少了 19.64%,具有更优的面积-延时性能.

6 结论

本文所讨论的 AES S-盒组合逻辑电路采用基于正规基的复合域运算,并提出了新的多因子 CSE 算法优化 S-盒中资源消耗较大的 $GF(2^4)$域乘法逆电路和映射矩阵电路.与 Greedy-CSE 算法和 Exhaust-CSE 算法相比,多因子 CSE 算法具有更快的计算速度.在 S-盒组合逻辑电路优化中,多因子 CSE 算法能够有效地消除电路冗余资源,具有较好的优化效果.采用 0.18μm CMOS 工艺实现 S-盒,电路面积为 2940.5376μm^2,面积-延时积为 67632.3648μm^2·ns,其面积-延时积比最小面积[5]和最短时延[9] S-盒组合逻辑电路分别减少了 10.32% 和 19.64%.

本文所提出的多因子 CSE 算法不仅适用于 AES S-盒电路的优化,也适用于更复杂的有限域 MCM 运算,如基于有限域的椭圆加密电路和 RS 编解码电路等.

参考文献

[1] FIPS-197. Advanced Encryption Standard (AES)[S].

[2] 高娜娜,李占才,王沁.一种可重构体系结构用于高速实现 DES、3DES 和 AES[J].电子学报,2006,34(8):1386 – 1390.
GAO Na-na, LI Zhan-cai, WANG Qin. A reconfigurable architecture for high-speed implementations of DES, 3DES and AES [J]. Acta Electronica Sinica, 2006, 34(8): 1386 – 1390. (in Chinese)

[3] M M Wong, M L D Wong, A K Nandi, et al. Composite field $GF(((2^2)^2)^2)$ advanced encryption standard (AES) S-box with algebraic normal form representation in the subfield inversion [J]. Circuits, Devices & Systems, IET, 2011, 5(6): 471 – 476.

[4] X Zhang. High-speed VLSI Architectures for Error-correcting Codes and Cryptosystems[D]. Minnesota: University of Minnesota, 2005.

[5] Canright D. A Very Compact Rijndael S-box[R]. California: Naval Postgraduate School, 2005.

[6] M M Wong, M L D Wong, A K Nandi, et al. Construction of optimum composite field architecture for compact high-throughput AES S-boxes[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2012, 20(6): 1151 – 1155.

[7] A Satoh, S Morioka, K Takano, et al. A compact Rijndael hardware architecture with S-box optimization[A]. Colin Boyd. Lecture Notes in Computer Science[C]. Australia: Springer Berlin Heidelberg, 2001. 239 – 254.

[8] N Mentens, L Batinan, B Preneeland, et al. A systematic evaluation of compact hardware implementations for the Rijndael S-box[A]. Alfred Menezes. Lecture Notes in Computer Science [C]. San Francisco: Springer Berlin Heidelberg, 2005, 323 – 333.

[9] X Zhang, Parhi, K K. High-speed VLSI architectures for the AES algorithm[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2004, 12(9): 957 – 967.

[10] Atri Rudra, Pradeep K Dubey, Charanjit S Jutla, et al. Efficient Rijndael encryption implementation with composite field arithmetic[A]. David Naccache. Lecture Notes in Computer Science[C]. France: Springer Berlin Heidelberg, 2001, 171 – 184.

[11] Mehran Mozaffari-Kermani, Arash Reyhani-Masoleh. A low-cost S-box for the advanced encryption standard using normal basis[A]. IEEE International Conference on Electro/Informa-

tion Technology, EIT'09[C]. Windsor: IEEE, 2009. 52 – 55.
[12] 王沁,梁静,齐悦.一种有效缩减 AES 算法 S 盒面积的组合逻辑优化设计[J].电子学报,2010,38(4):939 – 942.
WANG Qin, LIANG Jing, QI Yue. The area optimized implementation of S-box in AES algorithm[J]. Acta Electronica Sinica, 2010, 38(4): 939 – 942. (in Chinese)
[13] R Pasko, P Schau mont, V Derudder, et al. A new algorithm for elimination of common subexpressions [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 1999, 18(1): 58 – 68.

作者简介

曾　纯　女,1989 年 3 月出生于湖南省湘潭县,南京航空航天大学电子信息工程学院硕士生.主要研究方向专用集成电路设计.
E-mail: daisyzeng0407201@126.com

吴　宁(通讯作者)　女,1956 年生于安徽淮南,硕士,南京航空航天大学教授,博士生导师.主要研究方向数字系统理论与技术、电子系统集成与专用集成电路设计.
E-mail: wunee@nuaa.edu.cn