基于冗余有限域算术的 AES S 盒高效故障检测方案

戴 强,戴紫彬,李 伟
(解放军信息工程大学,河南郑州 450001)

摘 要: 为使 AES S 盒的多奇偶校验故障检测方案具备预期故障检测能力,提出了由预期故障覆盖率确定预测奇偶总数的参数计算模型. 根据模型确定的预测奇偶总数,为基于冗余有限域算术的 S 盒定制了两种多分块多奇偶校验的故障检测方案. 推导优化了各分块预测奇偶计算公式,并通过穷举搜索找到了使整个电路结构最优的多项式系数与映射矩阵. 仿真结果表明两种方案的随机多故障覆盖率均约为 97%,验证了参数计算模型的有效性,突发故障覆盖率分别约为 61.8%、76.3%,优于已有文献中大部分故障检测方案. 综合结果表明,对比于已有文献中具有相似故障检测能力的故障检测 S 盒电路,所设计电路的面积-延时积最小.

关键词: AES; S 盒; 复合域; 故障检测
中图分类号: TP302 **文献标识码:** A **文章编号:** 0372-2112 (2018)11-2650-10
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.11.012

Highly Efficient Fault Detection Schemes for AES S-Box Based on Redundant GF Arithmetic

DAI Qiang, DAI Zi-bin, LI Wei
(*PLA Information Engineering University, Zhengzhou, Henan* 450001, *China*)

Abstract: In order to achieve the expected fault detection capability for the multi-parity based fault detection scheme of AES S-box, a parameter calculation model was proposed to determine the total number of predicted parities according to the expected fault coverage. Two multi-parity based fault detection schemes which divided S-box based on redundant GF arithmetic into multiple blocks were designed on the basis of that number calculated by the model. The formulas for predicting the parity of each block was derived and optimized, and the polynomial coefficients and the mapping matrices were found by exhaustive search to get the optimum circuit. The simulation results show that the fault coverage of the two fault detection schemes is both about 97% for the random multiple faults which verifies the effectiveness of the parameter calculation model. The fault coverage of the two schemes for the burst faults are 61.8% and 76.3%, respectively, which are better than most fault detection schemes in existing works. Synthesis results show that the area-delay products of the two S-box circuits with fault detection capability are smallest compared to their counterparts with similar fault detection capabilities in existing literatures.

Key words: advanced encryption standard (AES); S-box; composite fields; fault detection

1 引言

由环境因素引起的自然故障与错误注入攻击插入的恶意故障,将极大降低 AES 算法电路[1]的可靠性,并可能导致密钥泄露[2]. 作为 AES 算法中唯一的非线性操作,S 盒电路是 AES 硬件实现中资源消耗最多的部分,实现 S 盒电路的故障检测对增强 AES 硬件可靠性与抗错误注入攻击能力至关重要.

相比于硬件冗余[3]、时间冗余[4]、混合冗余[5],基于信息冗余(即错误检测码)的并发错误检测方法,可以较小的硬件或时间开销获得高的故障覆盖率. 而相比于循环冗余校验码[6]、鲁棒码[7]等错误检测码,基于奇偶校验码的故障检测电路硬件开销较小[8]. 面向资源受限型应用,S 盒多采用硬件开销小的复合域实现方式,因此众多文献对复合域 S 盒的奇偶校验故障检测方案展开了研究.

文献[9,10]在特定复合域上考虑 S 盒中 GF(2^8)乘法求逆运算的奇偶校验错误检测,但未探讨转换与仿射矩阵及多项式系数对故障检测 S 盒电路设计的影

收稿日期:2017-11-03;修回日期:2018-01-28;责任编辑:蓝红杰
基金项目:国家自然科学基金(No.61404175)

响,且文献[10]给出的分块方案与子域求逆预测奇偶计算公式并非最优形式,其文中提到的映射矩阵也并非使整个故障检测 S 盒电路面积最小的选择. 文献[11~13]对 S 盒采用单比特奇偶校验方法,其故障检测能力有限. 文献[14~17]通过将基于正规基或多项式基的复合域 S 盒划分为多个子块,为每个子块设置奇偶校验位,进而比较子块的预测奇偶与实际奇偶以检测错误. 相比于单比特奇偶校验方法,这种分块多奇偶校验方法具有更高的故障覆盖率. 然而,文献[14~17]均未提出用于故障检测的预测奇偶数量确定方法,且各文献中故障检测 S 盒电路的面积、延时与 S 盒实现采用的复合域与表示基的类型密切相关.

为使 S 盒电路具备预期的故障检测能力,需确定用于故障检测的预测奇偶数量. 本文针对复合域 S 盒实现,提出了多奇偶校验故障检测方案的结构参数计算模型,可根据该模型确定用于 S 盒电路故障检测的预测奇偶数量;为构造面积小、性能高的故障检测 S 盒电路,选择基于冗余有限域算术的复合域 S 盒实现,定制了两种分块奇偶校验故障检测方案,推导并优化了各块的预测奇偶计算公式,并通过穷举搜索找到了分别使故障检测 S 盒电路延时最小与面积最小的多项式系数与映射矩阵. 实验结果表明所设计的故障检测 S 盒电路的故障覆盖率、面积-延时性能均优于已有文献方案.

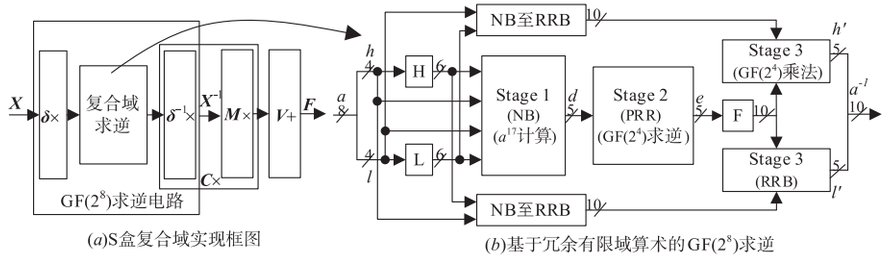
2　基于冗余有限域算术的复合域 S 盒实现

S 盒的复合域运算包括 $GF(2^8)$ 域乘法逆运算和仿射运算,如公式(1)所示.

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

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 $\boldsymbol{S}$ 盒变换后输出向量,$\boldsymbol{\delta}$ 和 $\boldsymbol{\delta}^{-1}$ 为基于复合域乘法逆运算的映射矩阵和逆映射矩阵. 通常,将仿射运算矩阵和逆映射矩阵合并为一个矩阵 $\boldsymbol{C}$ 以简化电路结构,则 $\boldsymbol{C} = \boldsymbol{M}\boldsymbol{\delta}^{-1}$.

基于冗余有限域算术的复合域 S 盒[18]实现框图如图 1 所示. 图 1(a)中复合域求逆运算使用 Itoh-Tsujii 算法[19]高效实现,其过程主要包括输入 a 的 16 次幂与 17 次幂计算、$GF(2^4)$ 求逆运算、$GF(2^4)$ 乘法运算三大部分,分别对应图 1(b)中 Stage1、Stage2、Stage3. 图 1(a)首先通过 $\boldsymbol{\delta}\times$ 完成域 $GF(2^8)$ 至复合域 $GF((2^4)^2)$ 的转换得到输入 a,其中复合域 $GF((2^4)^2)$ 上元素以正规基(Normal Base,NB)(α^{16},α)(表示 α 为不可约多项式 $f(x)=x^2+\mu x+\nu$ 的根). 图 1(b)中 Stage1 利用域 $GF(2^4)$ 的正规基 $(\beta^{2^3},\beta^{2^2},\beta^{2^1},\beta^{2^0})=(\beta^3,\beta^4,\beta^2,\beta^1)$(表示 β 为四阶全一多项式 $g(x)=x^4+x^3+x^2+x+1$ 的根),计算输入 a 的 17 次幂,再将计算结果转换成多项式环表示(Polynomial Ring Representation,PRR)结果. Stage2 完成基于 PRR 的 $GF(2^4)$ 上元素求逆运算. Stage3 完成基于冗余表示基(Redundantly Represented Basis,RRB)的 $GF(2^4)$ 上元素乘法运算. H、L 与 F 模块用于实现 Stage1 与 Stage3 中的共享子表达式,从而减小硬件开销. 图 1(b)的输出 a^{-1} 为 RRB 表示,对其进行 RRB 至 NB 的转换后,再经过逆映射矩阵与仿射变换可得到最终 S 盒输出. 值得注意的是,图 1 中 a^{17} 与 $\boldsymbol{\delta}\times$、$\boldsymbol{C}\times$ 的计算表达式随 (μ,ν) 取值改变而改变,其它模块计算表达式固定.



(a)S盒复合域实现框图　　(b)基于冗余有限域算术的GF(2^8)求逆

图1　基于冗余有限域算术的复合域S盒实现

3　多分块多奇偶校验的故障检测方案

3.1　结构参数计算模型

S 盒的多分块多奇偶故障检测方案中,分块数量与用于各块错误检测的预测奇偶数量,是决定其故障检测能力的关键因素[17]. 本文将故障检测方案中用于检测故障的预测奇偶比特总数量定义为该方案的结构参数.

定义 1　故障检测方案中用于检测故障的预测奇偶比特总数称之为该方案的结构参数 N_p.

N_p 的取值直接影响故障检测方案的故障检测能力. 为使故障检测方案达到预期的随机多故障覆盖率目标,本文构建了如下计算模型以确定 N_p.

首先,假定多故障随机分布在各个分块中,块 $i(1\leqslant i\leqslant n,n$ 为总块数)的故障检测逻辑对该块发生故障的检测概率为 p_i(p_i 相互独立),则块 i 的故障检测逻辑未检测到该块发生故障的概率为 $1-p_i$. 当且仅当所有分块的故障检测逻辑均无法检测到其分块发生的故障时,此时认为故障检测逻辑无法检测到整个电路中发生的故障,

则整个电路的故障覆盖率(Fault Coverage,FC)为:

$$FC\% = 100 \times \left(1 - \prod_{i \in S}(1 - p_i)\right)\% \tag{2}$$

这里 S 是插入故障的块数. 对于随机分布故障,当每个块的预测奇偶数量为 1 时[20],$p_i \approx 1/2$. 此时公式(2)可简化为 $FC\% = 100 \times (1 - (1/2)^n)\%$. 实际情况下,相比于面积较小的分块,面积越大的分块更容易受到内部故障与故障攻击影响[17],故通常对面积较大分块设置多奇偶校验,以增强 p_i. 本文设定各块预测奇偶数量最大为 2,且预测奇偶数量为 2 时,鉴于预测交叉奇偶检测突发故障的优势[21],为块设置两比预测交叉奇偶以检测故障. 假设块输出出现不同比特数故障的概率相同,下面给出定理 1,说明故障检测概率 p_i 与块预测奇偶数量 c_i 的关系.

定理 1 块 i 用于检测故障的预测奇偶比特数为 c_i 且 $1 \leqslant c_i \leqslant 2$,则对块 i 输出的随机多比特故障,其故障检测概率 $p_i' \approx 1 - (1/2)^{c_i}$.

证明:

设块 i 的输出共有 m 比特,且对于块输出发生的随机多比特故障,不同位数故障出现的概率相同. 当 $c_i = 1$ 时,出现不同位数故障的种类共有 $2^m - 1$,其中奇数与偶数位比特故障种类数分别为 2^{m-1}、$2^{m-1} - 1$,此时偶数位比特故障无法检测,则 $p_i = 2^{m-1}/(2^m - 1) \approx 1/2$.

当 $c_i = 2$ 时,块输出出现不同位数故障的种类数有 $2^m - 1$,无法检测到的故障种类数共有 $2^{m-2} - 1$,此时 $p'_i = \dfrac{2^m - 2^{m-2}}{2^m - 1} \approx 1 - (1/2)^2$. 得证.

根据定理 1,随着块 i 的预测奇偶数量增加,p_i 也随着增加. 此时公式(2)变为

$$FC\% = 100 \times \left(1 - \prod_{i \in S}(1 - p_i')\right)\% \approx 100 \times \left(1 - \left(\frac{1}{2}\right)^{N_p}\right)\% \tag{3}$$

这里 $N_p = \sum_{1 \leqslant i \leqslant n} c_i \geqslant n$. 公式(3)表明故障覆盖率与 N_p 成正比. 理论上故障覆盖率越高,越有利于对故障的检测,但相应增加的 N_p 所导致的奇偶计算硬件开销,可能超出某些应用的承受范围. 因此,在实际故障检测电路设计时,需考虑故障覆盖率与开销的折中. 为此,首先给电路的故障覆盖率设置最低要求值 $FC_{\min}\%$,由 $FC_{\min}\%$ 得到所需最小预测奇偶总数 $N_{\min}$,然后完成相应故障检测方案设计,并评估电路开销是否超过约束,若未超过,则考虑加大 $N_{\min}$. 由 $FC_{\min}\%$ 得到 N_p 的计算公式如公式(4)所示,这里符号 $\lceil x \rceil$ 表示大于或等于 x 的最小正整数.

$$N_p \geqslant N_{\min} = \lceil \log_2 (1 - FC_{\min}\%)^{-1} \rceil \tag{4}$$

若分块数 n 等于 $N_{\min}$,则整个电路划分为 $N_{\min}$ 个分块,各分块的预测奇偶数量为 1;若 n 小于 $N_{\min}$,则依据各块的面积大小,给面积大的分块分配更多的预测奇偶数.

3.2 故障检测方案设计

参考 S 盒众多故障检测方案[14~17]的故障覆盖率,本文给定 $FC_{\min}\%$ 为 95%,由公式(4)计算得到 $N_{\min} = 5$,此时 $FC\% \approx 96.875\% > FC_{\min}\% = 95\%$. 为不引入过多硬件开销,本文设定故障检测方案的 N_p 为 5,此时对于不同分块方案,存在不同的预测奇偶数量分配情况:若 S 盒划分为 3 分块,则三个块的预测奇偶数量分配数为 1、1、3 或 2、2、1;若 S 盒划分为 5 分块,则每个分块的预测奇偶数量均为 1. 本文给出了两种分块方案:5 分块 5 奇偶方案与 3 分块 5 奇偶方案,如图 2 中方案一、二所示. 根据不同方案中分块的面积,给各分块分配了相应数量的预测奇偶数量. 方案一中存在 5 个分块,因此给 5 个分块各分配一个预测奇偶;方案二中块 1 与块 3 分别约占整个 S 盒面积的 41%、46%,因此给块 1 与块 3 各分配 2 个预测奇偶.

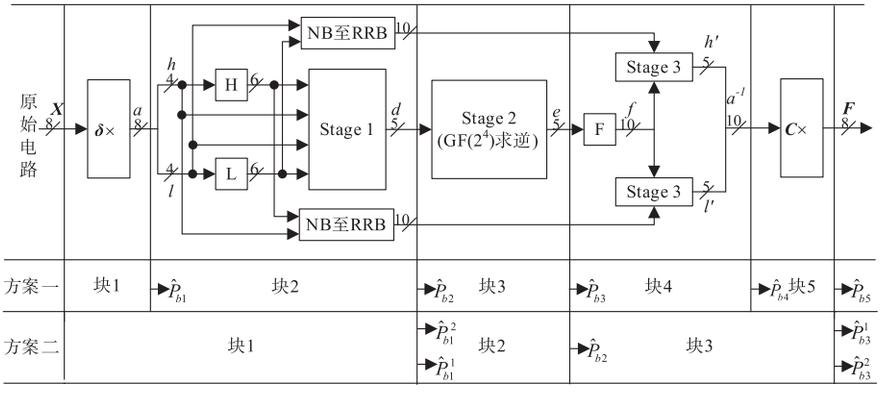


图2 多分块多奇偶故障检测方案

4　故障检测方案实现

4.1　块预测奇偶计算

由图 1 可知方案一、二的分块内主要包括 a^{17} 计算,基于 PRR 的 GF(2^4)乘法求逆,基于 RRB 的 GF(2^4)乘法,映射矩阵 $\boldsymbol{\delta}$,及联合矩阵 $\boldsymbol{C}$ 这 5 个子模块,下面首先推导出各子模块的最优预测奇偶计算公式,进而得到各分块的预测奇偶计算公式.

4.1.1　基于 PRR 的 GF(2^4)乘法求逆预测奇偶

引理 1[18] 设 d 为 GF(2^4)上元素,其 PRR 表示为 $d=d_4x^4+d_3x^3+d_2x^2+d_1x+d_0$,$d$ 的逆元 e,其 PRR 表示为 $e=e_4x^4+e_3x^3+e_2x^2+e_1x+e_0$,则

$$e_0=(d_1\vee d_4)(d_2\vee d_3) \tag{5}$$

$$e_1=((d_4+1)(d_1+d_2))\vee(d_0d_4(d_2\vee d_3)) \tag{6}$$

$$e_2=((d_3+1)(d_2+d_4))\vee(d_0d_3(d_1\vee d_4)) \tag{7}$$

$$e_3=((d_2+1)(d_1+d_3))\vee(d_0d_2(d_1\vee d_4)) \tag{8}$$

$$e_4=((d_1+1)(d_3+d_4))\vee(d_0d_1(d_2\vee d_3)) \tag{9}$$

定理 2　基于 PRR 的 GF(2^4)上求逆运算的预测奇偶 $\hat{P}$ 与预测交叉奇偶 $\hat{P}_1$、$\hat{P}_2$ 分别为

$$\begin{aligned}\hat{P}&=e_0+e_1+e_2+e_3+e_4\\&=\bar{d}_0(d_2d_4(d_1\vee d_3)+d_1d_3(d_2+d_4))\end{aligned} \tag{10}$$

$$\begin{aligned}\hat{P}_1&=e_0+e_2+e_4\\&=\bar{d}_0d_1d_2\bar{d}_3+\bar{d}_3d_4(d_1\vee d_2)+d_0\bar{d}_1d_3d_4+(d_2\vee d_3)\end{aligned} \tag{11}$$

$$\begin{aligned}\hat{P}_2&=e_1+e_3\\&=\bar{d}_0d_1d_2\bar{d}_4+d_4(d_1\vee d_2)+d_0\bar{d}_2d_3d_4+(d_2\vee d_3)\end{aligned} \tag{12}$$

证明:分别对公式(5)~(9)模 2 加结果,公式(5)、(7)、(9)模 2 加结果,公式(6)、(8)模 2 加结果进行有效逻辑化简后可得公式(10)~(12).

4.1.2　基于 RRB 的 GF(2^4)乘法预测奇偶

引理 2[10]　设 β 为四阶全一多项式的根,s、t、u 为 GF(2^4)上元素,s、t、$u\in$ GF(2^4),且 $u=s\times t$. 给定 s、t 的 RRB 表示为 $s=s_4\beta^4+s_3\beta^3+s_2\beta^2+s_1\beta+s_0$,$t=t_4\beta^4+t_3\beta^3+t_2\beta^2+t_1\beta+t_0$,$s_i$、$t_i\in$ GF(2)($0\leqslant i\leqslant 4$),$u=s\times t=u_4\beta^4+u_3\beta^3+u_2\beta^2+u_1\beta+u_0$,则 GF($2^4$)上基于 RRB 乘法运算的预测奇偶 $\hat{P}$ 为

$$\hat{P}=\sum_{0\leqslant i,j\leqslant 4,i\neq j}s_it_j \tag{13}$$

这里符号 $\sum$ 表示异或操作,且 $s_i,t_j\in$ GF(2). 预测交叉奇偶 $\hat{P}_1$ 与 $\hat{P}_2$ 分别为

$$\begin{aligned}\hat{P}_1&=u_0+u_2+u_4\\&=s_0(t_2+t_4)+s_1(t_3+t_4)+s_2(t_0+t_3)\\&\quad+s_3(t_1+t_2+t_3+t_4)+s_4(t_0+t_1+t_3+t_4)\end{aligned} \tag{14}$$

$$\begin{aligned}\hat{P}_2&=u_1+u_3\\&=s_0(t_1+t_3)+s_1(t_0+t_2)+s_2(t_1+t_4)\\&\quad+s_3(t_0+t_3)+s_4(t_2+t_4)\end{aligned} \tag{15}$$

4.1.3　a^{17} 计算的预测奇偶

图 1 中 a^{17} 计算结果 $d=hl\mu^2+(h+l)^2\nu$,设 d 的 PRR 表示为 $d=d_4x^4+d_3x^3+d_2x^2+d_1x+d_0$,这里 d_0、d_1、d_2、d_3、$d_4\in$ GF(2). 由文献[18]知 d_0、d_1、d_2、d_3、d_4 线性循环相关(即 $d_0+d_1+d_2+d_3+d_4=0$),故输出 d 的预测奇偶计算结果均为 0,实现开销为 0.

由于带故障检测 a^{17} 计算模块的实际奇偶计算所需门数在分块界限确定时就已经固定,且预测奇偶计算固定为 0,因此该模块的优化关键在于 a^{17} 计算原始模块的优化实现. 不同(μ,ν)组合下 a^{17} 计算逻辑表达式实现的硬件复杂性不同. 为使复合域 GF((2^4)^2)上 $f(x)=x^2+\mu x+\nu$ 为不可约多项式,μ,ν 需满足 $\mu^2/\nu\notin$ GF(2^2),共存在 120 种(μ,ν)组合符合该条件. 采用事后统计的方法,在求出 120 种(μ,ν)组合下的 a^{17} 计算逻辑表达式后,通过逻辑化简得到了 120 种表达式实现所需门数,其中表达式实现所需门数最少为 27XOR + 5AND + 10OR 或 27XOR + 10AND + 5OR(XOR 为异或门、AND 为与门、OR 为或门),延时最小为 3Tx + T_A 或 3Tx + To. 存在多个(μ,ν)组合使 a^{17} 计算所需面积、延时最小,考虑(μ,ν)组合对 $\boldsymbol{\delta}$、$\boldsymbol{C}$ 矩阵计算的影响(见 4.1.4 小节),本文选择 $\mu=\beta^4+\beta$ 且 $\nu=\beta$. 下面给出定理 4 计算此时 a^{17} 计算模块的预测奇偶.

定理 3　当 $\mu=\beta^4+\beta$ 且 $\nu=\beta$ 时,a^{17} 计算的预测奇偶 $\hat{P}=0$,预测交叉奇偶

$$\begin{aligned}\hat{P}_1=\hat{P}_2&=h_1(\bar{l}_2+l_3+l_4)+h_2(l_1+l_2+l_3+l_4)\\&\quad+h_3(l_1+l_2+l_3)+h_4(l_1+l_2+l_4)+l_1.\end{aligned}$$

证明:

当 $\mu=\beta^4+\beta$ 且 $\nu=\beta$ 时,$d=d_4x^4+d_3x^3+d_2x^2+d_1x+d_0$,其中

$$\begin{aligned}d_0&=(h_1l_2+h_2l_1+h_3l_4+h_4l_3+h_1l_1+h_4l_4)\\&\quad+(h_1+l_1+h_3+l_3+h_4+l_4)\\d_1&=(h_1l_2+h_2l_1+h_1l_3+h_3l_1+h_2l_2+h_4l_4)\\&\quad+(h_1+l_1+h_2+l_2+h_3+l_3+h_4+l_4)\\d_2&=(h_1l_3+h_3l_1+h_1l_4+h_4l_1+h_2l_3+h_3l_2+h_2l_2)\\&\quad+(h_1+l_1+h_2+l_2+h_3+l_3+h_4+l_4)\\d_3&=(h_1l_4+h_4l_1+h_2l_3+h_3l_2+h_2l_4+h_4l_2+h_3l_3)\\&\quad+(h_2+l_2+h_3+l_3+h_4+l_4)\\d_4&=(h_2l_4+h_4l_2+h_3l_4+h_4l_3+h_1l_1+h_3l_3)\\&\quad+(h_1+l_1+h_2+l_2+h_3+l_3)\end{aligned}$$

可得 $\hat{P}=\sum_{0\leqslant i\leqslant 4}d_i=0$

$$\begin{aligned}\hat{P}_1&=\hat{P}_2=d_0+d_2+d_4=d_1+d_3\\&=h_1(\bar{l}_2+l_3+l_4)+h_2(l_1+l_2+l_3+l_4)\\&\quad+h_3(l_1+l_2+l_3)+h_4(l_1+l_2+l_4)+l_1\end{aligned}$$　得证.

4.1.4　映射矩阵与联合矩阵预测奇偶

对于确定的某一(μ,ν)组合,可生成 8 个映射矩

阵[22]$\boldsymbol{\delta}$及相应的联合矩阵$\boldsymbol{C}$(本文将$\boldsymbol{\delta}$与其对应的$\boldsymbol{C}$称为一个矩阵对),因此共有960个矩阵对可用. 通过穷举960个矩阵对,可得到使故障检测S盒电路结构最优(面积或延时最小)的$\boldsymbol{\delta}$、$\boldsymbol{C}$. 首先,穷举后发现存在实现关键路径延时之和最小为5Tx的16个矩阵对,其中$\boldsymbol{\delta}$、$\boldsymbol{C}$实现关键路径分别为2Tx、3Tx. 表1列举了这16个矩阵对在公共项共享后实现所需面积、延时以及预测奇偶计算所需面积、延时,其中总面积为矩阵对及其预测奇偶计算实现所需面积之和,X表示异或门面积,Tx表示异或门延时.

表1 部分矩阵对及其预测奇偶计算对应面积/时间复杂性

编号	$\boldsymbol{\delta}+\boldsymbol{C}$计算		$\hat{P}_\delta+\hat{P}_C$计算		总面积
	面积	延时	面积	延时	
1、2	14X+22X	2Tx+3Tx	5X+1X	3Tx+1Tx	42X
3、4	12X+24X	2Tx+3Tx	2X+4X	2Tx+3Tx	
5、6	12X+24X	2Tx+3Tx	2X+4X	2Tx+3Tx	
7、8	14X+22X	2Tx+3Tx	5X+1X	3Tx+1Tx	
9、10	14X+22X	2Tx+3Tx	5X+1X	3Tx+1Tx	
11、12	12X+24X	2Tx+3Tx	2X+4X	2Tx+3Tx	
13、14	12X+24X	2Tx+3Tx	2X+4X	2Tx+3Tx	
15、16	14X+22X	2Tx+3Tx	5X+1X	3Tx+1Tx	

表1中16个矩阵对与其预测奇偶计算所需面积之和相等,均为42X,因此需进一步考虑不同矩阵对所对应(μ,ν)组合下的a^{17}计算实现所需面积、延时大小. 表2列举了这16个矩阵对所对应的μ,ν取值及相应的a^{17}计算实现所需面积与延时.

表2 矩阵对对应(μ,ν)系数及a^{17}计算对应面积/时间复杂性

编号	μ	ν	a^{17}计算	
			面积	延时
1、2	$\beta^4+\beta$	β	27X+10A+5O	$3T_X+T_A$
3、4	β^3	$\beta^4+\beta$	39X+10A+5O	$4Tx+T_A$
5、6	β^2	$\beta^4+\beta$	39X+10A+5O	$4Tx+T_A$
7、8	$\beta^3+\beta^2$	β^3	27X+10A+5O	$3T_X+T_A$
9、10	$\beta^3+\beta^2$	β^2	27X+10A+5O	$3T_X+T_A$
11、12	β^4	$\beta^3+\beta^2$	39X+10A+5O	$4Tx+T_A$
13、14	β	$\beta^3+\beta^2$	39X+10A+5O	$4Tx+T_A$
15、16	$\beta^4+\beta$	β	27X+10A+5O	$3T_X+T_A$

由表2可知,存在8个矩阵对(表中字体加粗编号)对应的a^{17}计算实现面积、延时最小. 因此,可任选这8个矩阵对之一,用于构造延时最小的故障检测S盒电路,本文选择了与文献[10,23]相同的映射矩阵对$\boldsymbol{\delta}_{15}$、$\boldsymbol{C}_{15}$(对应$\mu=\beta^4+\beta,\nu=\beta$),其中$\boldsymbol{\delta}_{15}$=[0x32,0xD6,0xC6,0x38,0x20,0x13,0x2F,0x66]、$\boldsymbol{C}_{15}$=[0x04,0x07,0xF8,0x24,0xDF,0x2D,0xB3,0x53,0x0B,0xC6],这里矩阵的列向量采用16进制表示.

上述过程构造的故障检测S盒是延时最优结构,但并非面积最小结构. 为得到面积最小的故障检测S盒,首先通过公共项消除算法获得了960个矩阵对计算所需最少门数,然后计算不同矩阵对所对应(μ,ν)组合下相应a^{17}计算模块实现所需门数,最终得到整个故障检测S盒电路实现所需门数,并从中选择出最小值. 具体过程不再详述,根据穷举结果可得故障检测S盒面积最小时对应矩阵对$\boldsymbol{\delta}_S$、$\boldsymbol{C}_S$(对应$\mu=\beta^4+\beta^3,\nu=\beta^4+\beta^3$):$\boldsymbol{\delta}_S$=[0xE8,0x26,0x02,0x73,0x48,0xE2,0x69,0xBB]、$\boldsymbol{C}_S$=[0x16,0xE8,0x61,0x3C,0xA3,0x10,0x45,0xE3,0xA7,0x11],其矩阵表示形式为:

$$\boldsymbol{\delta}_S=\begin{pmatrix}1&0&0&0&0&1&0&1\\1&0&0&1&1&1&1&0\\1&1&0&1&0&1&1&1\\0&0&0&1&0&0&0&1\\1&0&0&0&1&0&1&1\\0&1&0&0&0&0&0&0\\0&1&1&1&0&1&0&1\\0&0&0&1&0&0&1&1\end{pmatrix},$$

$$\boldsymbol{C}_S=\begin{pmatrix}0&1&0&0&1&0&0&1&1&0\\0&1&1&0&0&0&1&1&0&0\\0&1&1&1&1&0&0&1&1&0\\1&0&0&1&0&1&0&0&0&1\\0&1&0&1&0&0&0&0&0&0\\1&0&0&1&0&0&1&0&1&0\\1&0&0&0&1&0&0&1&1&0\\0&0&1&0&1&0&1&1&1&1\end{pmatrix}.$$

这里最低有效位在矩阵右下角. 至此,分别得到了使故障检测S盒电路延时最小、面积最小的映射矩阵对与多项式系数. 需要指出的是,本文的方案一、二采用$\boldsymbol{\delta}_{15}$、$\boldsymbol{C}_{15}$矩阵对(对应延时最小故障检测S盒),方案一*采用$\boldsymbol{\delta}_S$、$\boldsymbol{C}_S$矩阵对(对应面积最小故障检测S盒).

4.1.5 块预测奇偶计算公式

由各子模块预测奇偶计算公式,可得到方案一中5个预测奇偶分别为:

$$\hat{P}_{b1}=x_1+x_2+x_3+x_4+x_5+x_6$$

$$\hat{P}_{b2}=0$$

$$\hat{P}_{b3}=\bar{d}_0(d_2d_4(d_1\vee d_3)+d_1d_3(d_2+d_4))$$

$$\hat{P}_{b4}=\sum_{0\leqslant i\leqslant 3}\Big((h_i+l_i)\Big(\sum_{0\leqslant j\leqslant 4}f_j+f_{i+1}\Big)\Big)$$

$$\hat{P}_{b5}=a_1^{-1}+a_2^{-1}$$

方案二中5个预测奇偶分别为:

$$\hat{P}_{b1}^{1}=\sum_{1\leqslant i\leqslant 7,i\neq 3,6}x_i+x_2\Big(\sum_{1\leqslant i\leqslant 7,i\neq 2,6}x_i\Big)+x_5\Big(\sum_{3\leqslant i\leqslant 7,i\neq 5}x_i\Big)+x_0\Big(\sum_{2\leqslant i\leqslant 7,i\neq 4,6}x_i\Big)+x_3x_6$$

$$\hat{P}_{b1}^{2}=\hat{P}_{b1}^{1}$$

$$\hat{P}_{b2}=\bar{d}_0(d_2d_4(d_1\vee d_3)+d_1d_3(d_2+d_4))$$

$$\hat{P}_{b3}^{1}=\hat{P}_{b3}^{2}+h_0(e_0+e_1)+h_1(e_0+e_4)+h_2(e_3+e_4)+h_3(e_2+e_3)$$

$$\hat{P}_{b3}^{2}=l_0(e_0+e_1)+l_1(e_0+e_4)+l_2(e_3+e_4)+l_3(e_2+e_3)+h_0(e_2+e_4)+h_1(e_1+e_3)+h_2(e_0+e_2)+h_3(e_1+e_4)$$

由定理 3 知,a^{17} 计算的预测奇偶固定为 0,这使得方案一中 $\hat{P}_{b2}=0$、方案二中 $\hat{P}_{b1}^{2}=\hat{P}_{b1}^{1}$,从而有效减少了预测奇偶计算所需门数.

下面以方案一为例,说明块预测奇偶计算公式的硬件实现. 图 3(*a*)、(*b*)、(*c*)、(*d*)分别展示了方案一中分块 1、3、4、5 预测奇偶计算的硬件实现. 值得注意的是,分块 4 预测奇偶计算公式中的 $\sum_{0\leqslant j\leqslant 4}f_j$ 等于分块 3 的实际奇偶计算值,因此可与分块 3 的实际奇偶计算共享,而 $h_i+l_i(0\leqslant i\leqslant 3)$ 则是分块 1 实际奇偶计算公式的子表达式,因此可与分块 1 的实际奇偶计算公式共享子表达式以减少硬件开销.

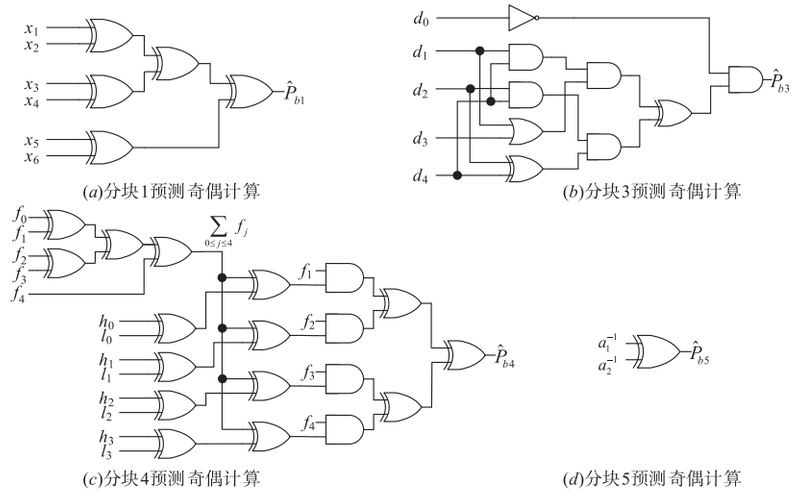


图3　方案一预测奇偶计算公式的硬件实现

4.2　结构复杂性分析

参照文献[14]中电路结构复杂性分析过程,对两种方案下故障检测 S 盒电路的时间与面积复杂性分析后,结果如表 3 所示,具体过程不再详述. 为得到更加直观的对比效果,根据文献[14]中异或门、与门、或门、非门面积的等效关系(与门、或门、非门面积分别等价于 0.6、0.6、0.2 个异或门面积),表 3 中得到了以异或门面积为单位的等效面积复杂性. 表 3 还列举了文献[8]、[14]故障检测 S 盒电路的面积与时间复杂性分析结果. 此外,鉴于文献[10]是基于冗余基实现的 GF(2^8)求逆故障检测电路,在其给出的 5 分块故障检测方案中增加 $\boldsymbol{\delta}_{15}\times$、$\boldsymbol{C}_{15}\times$ 模块后实现了完整的故障检测 S 盒电路,并在表 3 中展示了该电路的面积与时间复杂性.

表 3　电路结构复杂性分析

方案	时间复杂性	面积复杂性				等效面积复杂性
		原始电路	预测奇偶	实际奇偶	比较	
方案一	$3T_A+15T_X+T_O$	87X+38A+16O+8N	15X+9A+1O+1N	31X	4X	177.2X
方案二	$3T_A+15T_X+T_O$	87X+38A+16O+8N	37X+21A+1O+N	13X	5X	189.4X
方案一*	$3T_A+16T_X+T_O$	81X+43A+11O+8N	16X+9A+1O+1N	31X	4X	172.2X
文献[10]	$3T_A+15T_X+T_O$	87X+38A+16O+8N	21X+14A+2N	35X	4X	189.8X
文献[14]	$4T_A+27T_X$	119X+36A	14X+9A+3O+N	23X	5X	190X
文献[8]	$4T_A+24T_X$	118X+59A+9N+5O	24X+10A+2O	23X	5X	217.4X

备注:X 为异或门面积、A 为与门面积、O 为或门面积、N 为非门面积;
T_A 为与门延时、T_X 为异或门延时、T_O 为或门延时

由表3可知,本文方案一、一*、二的面积复杂性均小于文献[8]、[10]、[14],且方案一*的面积复杂性最小.本文方案一、二的时间复杂性与文献[10]相同,远小于文献[8]、[14],略小于方案一*.因此,从结构复杂性分析结果看,相比于已有文献方案,本文方案在面积-延时性能上具有明显优势.本文方案及其它文献方案的实际综合结果将在第6节给出.

5 错误仿真

为模拟自然故障与恶意故障攻击,分别进行了多随机故障与突发故障(即相邻故障)注入仿真实验[17,20].仿真实验使用固定故障模型,强制一个或多个节点为固定逻辑1或0,且与节点真实值无关.

5.1 多故障

仿真时,使用外部LFSRs(Linear Feedback Shifting Registers)生成伪随机故障向量与随机输入:对方案一,在五个块的输出使用一个36输出抽头LFSR(记作L1,其特征多项式为 $L_1(X)=X^{36}+X^{32}+X^{27}+X^{22}+X^{20}+X^{17}+X^{14}+X^{12}+X^{10}+X^9+X^7+X^6+X^4+X+1$)插入随机多故障;使用8比特输出抽头LFSR(记作L2,其特征多项式为 $L_2(X)=X^8+X^4+X^3+X^2+1$)产生S盒的随机输入.对于L1与L2的不同初始值,在注入故障次数为1000000时,仿真结果如表4所示.

表4 方案一多故障覆盖率

方案	初始值	检测数	误报数	故障覆盖率	误报率
方案一	$L_1=\{\text{AAFA2AFA2}\}_h$ $L_2=\{\text{9D}\}_h$	968866	3815	≈97%	≈0.38%
	$L_1=\{\text{22BBF2BBF}\}_h$ $L_2=\{\text{73}\}_h$	968666	3692	≈97%	≈0.37%

当L1与L2初始值分别为0xAAFA2AFA2与0x9D时,图4(*a*)、(*b*)分别展示了不同故障注入次数下的故障覆盖率与误报率.由表4与图4可知,多项式初始值与注入故障次数对故障覆盖率、误报率的影响可忽略不计.

对方案二,仍使用*L2*生成随机输入,在三个块的输出使用18输出抽头LFSR(记作L3,其特征多项式为 $L_3(X)=X^{18}+X^{16}+X^{14}+X^{11}+X^5+X^2+1$)插入随机多故障.对于L3与L2的不同初始值,在注入故障次数为1000000时,仿真结果如表5所示.

方案一、二的多故障覆盖率均约为97%,这与3.1节中参数计算模型给出的计算结果几乎相等,从而验证了电路结构参数设计模型的有效性.

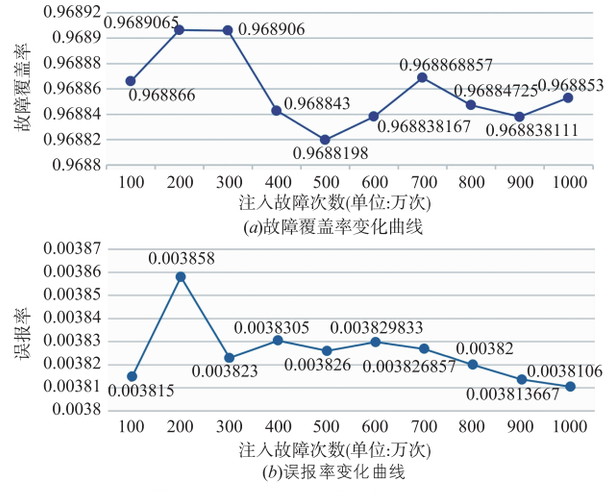


图4 故障覆盖率与误报率变化曲线

表5 故障覆盖率

方案	初始值	检测数	误报数	故障覆盖率	误报率
方案二	$L_3=\{\text{2AFA2}\}_h$ $L_2=\{\text{9D}\}_h$	968758	3908	≈97%	≈0.39%
	$L_3=\{\text{32BBF}\}_h$ $L_2=\{\text{73}\}_h$	968621	3793	≈97%	≈0.38%

5.2 突发故障

为模拟突发故障,仿真时在一个块或两个相邻块输出处注入故障[17].方案一中,对S盒随机输入、块1与块5输出,使用L2注入故障;对于块2与块3输出,使用5输出抽头LFSR(记作L4,其特征多项式为 $L_4(X)=X^5+X^2+1$)注入故障;对块4输出,使用10输出抽头LFSR(记作L4,其特征多项式为 $L_4(X)=X^5+X^2+1$)注入故障.故障数量、位置与类型都是随机选择的.方案二中,对S盒随机输入、块5输出使用L2注入故障,对于块1与块2输出,使用L5注入故障.对于100000个随机输入,在块的输出注入1000000个突发故障.

仿真结果如表6所示,方案一、二的突发故障覆盖率分别为61.8%、76.3%,误报率分别为1.3%、2.3%.方案一、二与已有文献方案的故障检测能力比较将在第6节展示.

表6 突发故障覆盖率

方案	检测数	误报数	故障覆盖率	误报率
方案一	617751	13112	≈61.8%	≈1.3%
方案二	762878	22755	≈76.3%	≈2.3%

6 综合结果与对比

本文采用Verilog语言对故障检测S盒电路进行描

述,并利用综合工具基于 65 nm CMOS 工艺标准单元库进行综合,综合时禁止 flatten 优化策略并设置面积优先. 表 7 展示两种方案下故障检测 S 盒电路的面积及对应的延时信息. 由表 7 可知,相比于原始 S 盒电路,方案一、二的电路面积分别增加了 22.36%、44.15%,延时分别增加了 12.08%、14.58%. 表 7 展示了采用矩阵对 $\boldsymbol{\delta}_S$、$\boldsymbol{C}_S$(对应故障检测 S 盒面积最小)时故障检测 S 盒电路的面积、延时. 此外,表 7 中还列举了采用双模冗余(Dual Modular Redundancy,DMR)与基于正规基置换的再计算方法(Normal Basis Recomputing with Permuted Operands,NREPO)时的电路面积与延时信息.

表 7　故障检测 S 盒电路综合结果

方案	面积(μm^2)	延时(ns)	面积-延时积($\mu m^2 \times ns$)	故障覆盖率(多故障)
原始	381.60	2.40	915.84	0
方案一	466.92	2.69	1256.01	≈97%
方案一 *	426.96	2.74	1169.87	≈97%
方案二	550.08	2.75	1512.72	≈97%
DMR	783.00	2.70	2114.10	≈100%
NREPO *[5]	783.00	2.70	2114.10	≈100%

备注:方案一 * 表示采用 $\boldsymbol{\delta}_S$、$\boldsymbol{C}_S$ 矩阵对的故障检测 S 盒电路;
NREPO * 表示 NREPO 的时间冗余等价转换为硬件冗余实现

由表 7 可知,尽管方案一、一 *、二的故障覆盖率略小于 DMR、NREPO,但面积、面积延时积均远小于 DMR、NREPO. 表 7 中方案一 * 的面积与面积延时积最小,但延时大于方案一,适合于对资源要求特别严格的应用. 而方案一的延时最小,面积大于方案一 *,更适合于对资源、性能均有一定要求的应用.

为了与已有文献中故障检测 S 盒电路进行直观比较,进一步减小最大路径延时约束后综合电路. 表 8 展示了本文方案与已有文献方案[17]的 ASIC 实现面积、延时,表中最后两列对比了各文献方案对突发故障与多故障的故障覆盖率. 值得注意的是,由于文献[10]仅给出了不包括映射矩阵对的故障检测 GF(2^8)求逆电路(包含故障检测电路)的面积、延时,因此无法直接与本文方案对比. 为公平比较,在文献[10]给出矩阵对样例及 GF(2^8)求逆电路的基础上,设计了一个完整的故障检测 S 盒电路(采用 5 分块 5 奇偶校验方案),并在本文相同条件下进行错误仿真与实际综合,仿真与综合结果如表 8 第 4 行所示.

使用 Xilinx ISE14.7 工具基于 Xilinx Virtex-6 XC6VLX240t FPGA 硬件平台进行方案的设计综合,综合时保持设计层次,综合策略设置面积优先. 本文方案与已有文献方案的面积、时钟频率、面积延时积等性能参数如表 9 所示. 表 9 中最后一列对比了各文献方案的多故障覆盖率.

表 8　65nm 工艺下各文献方案 ASIC 实现性能参数对比

方案	面积(μm^2)	延时(ns)	面积延时积($\mu m^2 \times ns$)	故障覆盖率	
				突发故障	多故障
方案一	583	1.80	1049.40	≈61.8%	≈97%
方案二	674	1.80	1213.20	≈76.3%	≈97%
文献[10]	627	1.80	1128.60	≈61.7%	≈97%
文献[14](NB)	858	1.90	1630.20	≈50%	≈97%
文献[15](PB)	865	1.82	1574.30	≈50%	≈97%
文献[17](PB)	953	1.80	1715.40	≈71.3%	≈97%
文献[13]	754	1.90	1432.60	≈50%	≈50%

备注:PB 指基于多项式基的故障检测 S 盒最佳优化;
NB 指基于正规基的故障检测 S 盒最佳优化

表 9　FPGA 实现性能参数对比

方案	硬件平台	时钟频率(MHz)	面积(Slices)	面积-延时积(Slices × ns)	故障覆盖率(多故障)
方案一	Xilinx Virtex-6	178.38	20	112	≈97%
方案二		169.09	25	148	≈97%
文献[12]		126.41	49	387	≈50%
文献[24]		254.71	122	479	≈50%

为了更好的说明本文方案的优势,选择以面积-延时积作为故障检测 S 盒电路优劣的评估标准[23]. 表 8 中方案一的面积-延时积最小,且突发故障故障覆盖率仅小于方案二与文献[17]. 方案二的故障覆盖率最高,且面积 - 延时积仅大于方案一与文献[10]. 对比与方案一故障覆盖率几乎相等的文献[10],方案一的面积 - 延时积减少了 7.02%. 对比最接近本文方案二故障检测能力的文献[17],方案二的面积 - 延时积减少了 29.28%,而方案一的突发故障覆盖率尽管略低于文献[17],但面积 - 延时积减少了 38.82%. 表 9 中方案一、二的多故障覆盖率优于文献[12]、[24],且电路面积均小于文献[12]、[24]. 尽管本文方案一、二的延时大于文献[24]、小于文献[12],但方案一、二的面积 - 延时积均小于文献[12]、[24]. 表 8 与表 9 的数据对比表明,本文所设计两种故障检测 S 盒电路,对多故障与突发故障的检测能力优于大部分同类文献,且方案一电路的面积-延时性能最优,这与 4.2 小节中电路结构复杂性分析结果一致.

7　结论

本文针对复合域 S 盒的多奇偶校验故障检测方案,提出了由故障覆盖率确定预测奇偶数量的结构参数计算模型,可用于指导 S 盒奇偶校验故障检测方案

的设计.对基于冗余有限域算术的 S 盒实现,由模型计算得到的预测奇偶数量定制了两种多分块多奇偶校验的故障检测方案.推导并优化了各分块预测奇偶计算公式,并通过穷举搜索找到了分别使故障检测 S 盒电路延时、面积最小的多项式系数与映射矩阵对.错误仿真结果表明,本文所提出两种方案的随机多故障覆盖率均约为 97%,从而验证了结构参数计算模型的有效性,且方案二的突发故障覆盖率为 76.3%,优于其它同类文献方案.综合结果表明,相比于已有文献,本文所设计的故障检测 S 盒电路具有最优的面积-延时性能.下一步将基于冗余有限域算术,设计支持故障检测的 AES 算法电路.

参考文献

[1] 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)

[2] GUO Xiao-fei,Ramesh Karri. Recomputing with permuted operands:A concurrent error detection approach[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,2013,32(10):1595 – 1608.

[3] Malkin TG,Standaert FX,Yung M. A comparative cost/security analysis of fault attack countermeasures[A]. Proceedings of 3rd International Workshop on Fault Diagnosis & Tolerance in Cryptography[C]. Yokohama:Springer,2006. 159 – 172.

[4] Maistri P,Leveugle R. Double-data-rate computation as a countermeasure against fault analysis[J]. IEEE Transactions on Computers,2008,57(11):1528 – 1539.

[5] GUO Xiao-fei,Mukhopadhyay D,JIN Cheng-lu,et al. NREPO:Normal basis recomputing with permuted operands[A]. Proceedings of the 2014 IEEE International Symposium on Hardware-oriented Security & Trust[C]. Arlington:IEEE,2014. 118 – 123.

[6] YEN Chih-hsu,WU Bing-fei. Simple error detection methods for hardware implementation of advanced encryption standard[J]. IEEE Transactions on Computers,2006,55(6):720 – 731.

[7] Karpovsky M,Kulikowski KJ,Taubin A. Robust protection against fault-injection attacks on smart cards implementing the advanced encryption standard[A]. Proceedings of 34th Annual IEEE/IFIP International Conference on Dependable Systems & Networks[C]. Florence:IEEE,2004. 93 – 101.

[8] Mozaffari-Kermani M,Reyhani-Masoleh A. Parity-based fault detection architecture of S-box for advanced encryption standard[A]. Proceedings of the 21st IEEE International Symposium on Defect and Fault-Tolerance in VLSI Systems[C]. Arlington:IEEE,2006. 572 – 580.

[9] WU Shee-yau,YEN Huang-ting. On the S-box architectures with concurrent error detection for the advanced encryption standard[J]. Ieice Transactions on Fundamentals of Electronics Communications & Computer Sciences,2006,89 – A(10):2583 – 2588.

[10] Mozaffari-Kermani M,Jalali A,Azarderakhsh R,et al. Reliable inversion in GF(2^8) with redundant arithmetic for secure error detection of cryptographic architectures[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,2018,37(3):696 – 704.

[11] 赵佳,韩军,曾晓洋,等. AES 算法的并发错误检测方法及其 VLSI 实现[J].计算机研究与发展,2009,46(4):593 – 601.
ZHAO Jia,HAN Jun,ZENG Xiao-yang,et al. A two-dimensional parity-based concurrent error detection method for AES against differential fault attack and its VLSI implementation[J]. Journal of Computer Research and Development,2009,46(4):593 – 601. (in Chinese)

[12] 晏巍,王奕,李仁发.低成本 AES 错误检测方案的 FPGA 实现[J].小型微型计算机系统,2015,36(7):1644 – 1648.
YAN Wei,WANG Yi,LI Ren-fa. Low cost fault detection scheme for AES using FPGA implementation[J]. Journal of Chinese Computer Systems,2015,36(7):1644 – 1648. (in Chinese)

[13] Mozaffari-Kermani M,Reyhani-Masoleh A. Concurrent structure-independent fault detection schemes for the advanced encryption standard[J]. IEEE Transactions on Computers,2010,59(5):608 – 622.

[14] Mozaffari-Kermani M,Reyhani-Masoleh A. A lightweight concurrent fault detection scheme for the AES S-boxes using normal basis[A]. Proceedings of 10th International Workshop on Cryptographic Hardware and Embedded Systems[C]. Washington:Springer,2008. 113 – 129.

[15] Mozaffari-Kermani M,Reyhani-Masoleh A. A lightweight high-performance fault detection scheme for the advanced encryption standard using composite fields[J]. IEEE Transactions on VLSI Systems,2011,19(1):85 – 91.

[16] Ahmad N. Parity based fault detection techniques for S-box/inv S-box advanced encryption system[J]. ARPN Journal of Engineering and Applied Sciences,2015,10(19):9088 – 9092.

[17] Mozaffari-Kermani M,Reyhani-Masoleh A. A low-power high-performance concurrent fault detection approach for the composite field S-box and inverse S-box[J]. IEEE Transactions on Computers,2011,60(9):1327 – 1340.

[18] Ueno G,Homma N,Sugawara Y,et al. Highly efficient

GF(2^8) inversion circuit based on redundant GF arithmetic and its application to AES design[A]. Proceedings of 17th International Workshop on Cryptographic Hardware and Embedded Systems[C]. Saint-Malo: Springer, 2015. 63 – 80.

[19] Itoh T, Tsujii S. A fast algorithm for computing multiplicative inverses in GF(2^m) using normal bases[J]. Information and Computation, 1988, 78(3): 171 – 177.

[20] Breveglieri L, Koren I, Maistri P. An operation-centered approach to fault detection in symmetric cryptography ciphers[J]. IEEE Transactions on Computers, 2007, 56(5): 635 – 649.

[21] Aghaie A, Mozaffari-Kermani M, Azarderakhsh R. Reliable and fault diagnosis architectures for hardware and software-efficient block cipher KLEIN benchmarked on FPGA[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2017, PP(99): 1 – 1.

[22] ZHANG Xin-miao, Parhi KK. On the optimum constructions of composite field for the AES algorithm[J]. IEEE Transactions on Circuits & Systems II Express Briefs, 2006, 53(10): 1153 – 1157.

[23] 曾纯,吴宁,张肖强,等. 基于多因子 CSE 算法的 AES S 盒电路优化设计[J]. 电子学报, 2014, 42(6): 1238 – 1243.
ZENG Chun, WU Ning, ZHANG Xiao-qiang, et al. The optimization circuit design of AES S-box based on a multiple-term common subexpression elimination algorithm [J]. Acta Electronica Sinica, 2014, 42(6): 1238 – 1243. (in Chinese)

[24] Bertoni G, Breveglieri L, Koren I, et al. Error analysis and detection procedures for a hardware implementation of the advanced encryption standard[J]. IEEE Transactions on Computers, 2003, 52(4): 492 – 505.

作者简介

戴　强　男,1991 年生于江西乐安. 信息工程大学博士生,主要研究方向为安全专用芯片设计、密码硬件故障检测与容忍、可重构计算. E-mail: xierunyan123@163.com

戴紫彬　男,1966 年生于河南商丘. 信息工程大学教授,博士生导师. 研究方向为专用芯片设计、可重构芯片、可重构 SoC 设计.

李　伟　男,1983 年生于天津. 博士,副教授,主要研究方向可重构计算、密码处理器研究.