

一种低功耗抗差分功耗分析攻击的 SM4 算法实现

牛砚波, 蒋安平

(北京微电子技术研究所, 北京 100076)

摘 要: 128 位的 SM4 算法是我国公布的第一个商用密码算法, 主要应用于无线局域网. 为了提高算法的抗差分功耗分析攻击能力, SM4 算法采用了加法掩码的方法来抵抗一阶差分功耗分析攻击. 通过功耗分析攻击实心眼可以发现, 加法掩码后的 SM4 算法能够有效地抵抗差分功耗分析攻击. 为了实现一款面积小、功耗低 SM4 算法硬件电路, SM4 S 盒硬件电路采用了 PPRM 结构. 在 SMIC 0.18 μm 的工艺库下功耗仿真值为 0.74 mW@10 MHz, PPRM 结构的 S 盒与复合域方法实现的 S 盒相比功耗减少了 70%.

关键词: SM4 算法; S 盒; PPRM 结构; 加法掩码

中图分类号: TN492

文献标识码: A

文章编号: 1000-7180(2014)09-0028-05

A Low Power Implementation of SM4 Cipher with Resistance to Differential Power Analysis Attack

NIU Yan-bo, JIANG An-ping

(Beijing Institute of Microelectronics Technology, Beijing 100076, China)

Abstract: The 128-bit SM4 algorithm is the first commercial cipher published by China, which is mainly used in wireless LAN. In order to improve the algorithm's resistance to differential power analysis attack, the additive masking is adopted to keep the SM4 cipher resistant to the first-order DPA. The simulation results show that the counteractive against differential power analysis attack is credible. In order to realize a small-area, low-power circuit of SM4 cipher, the PPRM architecture is adopted in the hardware implementation of SM4 S-box. A power consumption of 0.74 mW@10 MHz using SMIC 0.18 μm technology is achieved, which is 70% less than that of the SM4 S-Box in composite field.

Key words: SM4-cipher; S-box; PPRM architecture; additive masking

1 引言

2006 年, 我国官方公布了第一个商用密码算法——SMS4 算法^[1], 并在 2012 年公布了 SM4 算法标准, SM4 算法不管是对无线局域网产业还是商用密码研究都有重要的意义.

密码算法在芯片或硬件系统运行的过程中, 除输入和输出信息之外还会产生电流功耗、电磁辐射等侧信道信息. Kocher 等人在 1998 年提出了一种新的密码分析攻击方法——差分功耗分析攻击方法^[2], 差分功耗分析攻击方法通过分析功耗曲线, 利用数据在运算过程中与功耗的相关性可

以获得在芯片内部执行加密和解密运算的相关密钥信息, 这种攻击方法严重威胁到 SM4 算法加解密数据的安全.

现在无论是无线局域网的普及, 手持入网设备的普及, 还是 WAPI 标准的提出, 都对 SM4 算法硬件电路实现的功耗提出了更高的要求, 面积小、功耗低的算法电路实现成为近些年的一个重点研究方向. 在 SM4 算法实现过程中, 传统查表法 S 盒设计简单, 但是有大的硬件开销, 文献[3-4]提出的复合域法实现的 S 盒可以很好地降低硬件开销, 但是带来更大的功耗延时积.

为了解决上述问题, 本文提出基于 PPRM 结

构^[5]采用加法掩码的SM4算法实现方法,并以此实现一款具有抗差分功耗分析攻击能力、功耗低、面积小适用于嵌入式电路的SM4算法^[6]电路模块。

2 SM4 算法介绍

SM4 算法是一种 32 轮非线性迭代分组密码算法,每次加解密数据及密钥均为 128 位,其加密流程如图 1 所示。

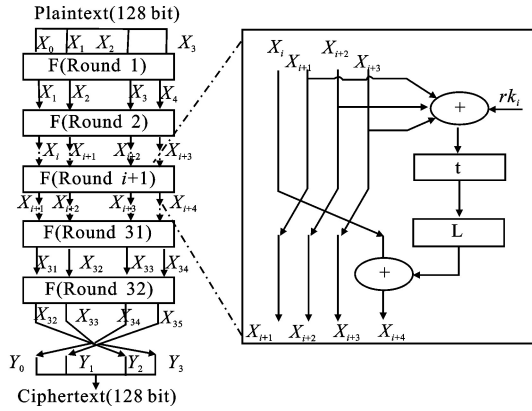


图 1 SM4 密码算法加密流程

2.1 加解密算法

设明文输入为 $X = (X_0, X_1, X_2, X_3) \in (Z_2^{32})^4$, 密文输出为 $Y = (Y_0, Y_1, Y_2, Y_3) \in (Z_2^{32})^4$, 轮密钥为 $rk \in Z_2^{32}$, $(X_i, X_{i+1}, X_{i+2}, X_{i+3})$ 表示第 $(i+1)$ 轮运算的输入, 其中 $i \in \{0, 1, 2, \dots, 31\}$, 则算法的加密变换为

$$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}) = X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i) \quad (1)$$

$$(Y_0, Y_1, Y_2, Y_3) = R(X_{32}, X_{33}, X_{34}, X_{35}) = (X_{35}, X_{34}, X_{33}, X_{32}) \quad (2)$$

式中, $i \in \{0, 1, 2, \dots, 31\}$, F 为轮函数, T 为合成置换, R 为反序变换。合成置换 T 由非线性变换和线性变换组合而成, 即 $T(\cdot) = L(\tau(\cdot))$ 。非线性变换有四个并行的 S 盒构成, 每个 S 盒为固定 8 bit 输出的置换运算, 记为 $Sbox(\cdot)$, 设置换输入为

$$A = (a_0, a_1, a_2, a_3) \in (GF(2^8))^4, \text{ 输出为}$$

$$B = (b_0, b_1, b_2, b_3) \in (GF(2^8))^4, \text{ 则:}$$

$$B = (b_0, b_1, b_2, b_3) = t(A) = (Sbox(a_0), Sbox(a_1), Sbox(a_2), Sbox(a_3)) \quad (3)$$

非线性变换的输出即线性变换 L 的输入, 设 L 的输入为 B , 输出为 C , 则

$$C = L(B) = B \oplus (B \lll 2) \oplus (B \lll 10) \oplus (B \lll 18) \oplus (B \lll 24) \quad (4)$$

式中, $\lll i$ 表示 32 bit 循环左移 i 位。

算法中解密时的线性变换与加密时的线性变换结构相同, 加密与解密不同之处仅是轮密钥的使用顺序不同。

2.2 密钥扩展算法

轮密钥由加密密钥通过密钥扩展算法生成, 其结构与加密运算类似, 只是其中的 L 线性变换部分不同。设加密密钥为 $MK = (MK_0, MK_1, MK_2, MK_3) \in (GF(2^{32}))^4$ 密钥为 $rk_i \in Z_2^{32}$, $i \in \{0, 1, 2, \dots, 31\}$, $K_i \in GF(2^{32})$, $i \in \{0, 1, 2, \dots, 31\}$, 则轮密钥生成方法如下:

$$(K_i, K_{i+1}, K_{i+2}, K_{i+3}) = (MK_0 \oplus FK_0, MK_1 \oplus FK_1, MK_2 \oplus FK_2, MK_3 \oplus FK_3) \quad (5)$$

$$rk_i = K_{i+4} = K_i \oplus T'(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i) \quad (6)$$

系统参数 $FK_i, i \in \{0, 1, 2, 3\}$ 和固定参数 $CK_i, i \in \{0, 1, 2, 3\}$ 均为常数, 式中, $T'(\cdot)$ 变换与加密变换中的 $T(\cdot)$ 变换基本相同, 只是其中的线性变换 L 修改为以下 L' 即

$$L'(B) = B \oplus (B \lll 13) \oplus (B \lll 23) \quad (7)$$

系统参数 $FK_i, i \in \{0, 1, 2, 3\}$ 的取值采用 16 进制表示为 $(a3b1bac6)$, $(56aa3350)$, $(677d9197)$, $(b27022dc)$, 固定参数 CK_i 的取值方法为

$$CK_i = (CK_{i,0}, CK_{i,1}, CK_{i,2}, CK_{i,3}) \in (GF(2^8))^4, \text{ 设 } CK_{i,j} \text{ 为第 } j \text{ 字节固定参数, 则}$$

$$CK_{i,j} = (4 \times i + j) \times 7 \pmod{256} \quad (8)$$

2.3 S 盒

S 盒是 SM4 算法中最重要的部分, 其置换表用 16 进制表示, 如图 2 所示。S 盒也可以通过有限域求逆和仿射变换组成, 其代数结构如下:

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	d6	90	e9	fe	cc	e1	3d	b7	16	b6	14	c2	28	fb	2c	05
1	2b	67	9a	76	2a	be	04	c3	aa	44	13	26	49	86	06	99
2	9c	42	50	f4	91	ef	98	7a	33	54	0b	43	ed	cf	ac	62
3	e4	b3	1c	a9	c9	8	e8	95	80	df	94	fa	75	8f	3f	a6
4	47	07	a7	fc	f3	73	17	ba	83	59	3c	19	e6	85	4f	a8
5	68	6b	81	b2	71	64	da	8b	f8	eb	0f	4b	70	56	9d	35
6	1e	24	0e	5e	63	58	d1	a2	25	22	7c	3b	01	21	78	87
7	d4	00	46	57	9f	d3	27	52	4c	36	02	e7	a0	c4	c8	9e
8	ea	bf	8a	d2	40	c7	38	b5	a3	f7	f2	ce	f9	61	15	a1
9	e0	ae	5d	a4	9b	34	1a	55	ad	93	32	30	f5	8c	b1	e3
a	1d	f6	e2	2e	82	66	ca	60	c0	29	23	ab	0d	53	4e	6f
b	d5	db	37	45	de	fd	8e	2f	03	ff	6a	72	6d	6c	5b	51
c	8d	1b	af	92	bb	dd	bc	7f	11	d9	5c	41	1f	10	5a	d8
d	0a	c1	31	88	a5	cd	7b	bd	2d	74	d0	12	b8	e5	b4	b0
e	89	69	97	4a	0c	96	77	7e	65	b9	f1	9	c5	6e	c6	84
f	18	f0	7d	ec	3a	dc	4d	20	79	ee	5f	3e	d7	cb	39	48

图 2 SM4 S 盒数据输入输出置换

$$Sbox(a) = I(a \cdot A_1 + C_1) \cdot A_2 + C_2 \quad (9)$$

aa 中, a 为 S 盒的 8 bit 输入, I 为 $GF(2^8)$ 上的乘法求逆, 循环矩阵 $A_1, A_2 \in GL(8, 2)$ 和向量 $C_1, C_2 \in GF(2^8)$ 分别为

$$\mathbf{A}_1 = \mathbf{A}_2 = \begin{pmatrix} 11100101 \\ 11110010 \\ 01111001 \\ 10111100 \\ 01011110 \\ 00101111 \\ 10010111 \\ 11001011 \end{pmatrix} \quad (10)$$

$$\mathbf{C}_1 = \mathbf{C}_2 = (1, 1, 0, 0, 1, 0, 1, 1) \quad (11)$$

式中, GF 域上的乘法求逆的八次不可约多项式为

$$f(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1 \quad (12)$$

3 针对 SM4 算法的差分功耗分析攻击与防护

电路功耗由静态功耗和动态功耗组成. 在进行数据加解密运算的时候, 动态功耗占主要部分, 动态功耗包括充放电电容引起的功耗, 以及直接通路电流引起的功耗. 在处理不同汉明重量的数据时, 逻辑门中的电容充放电情况不同, 从而产生不同的功耗, 这些功耗反应了算法的执行和当前处理数据的特征. 在利用功耗分析攻击平台^[7]进行密钥攻击的时候, 通过分析功耗曲线获得在某个芯片内部执行加密盒加密运算操作的相关信息, 完成功耗分析攻击.

3.1 针对 SM4 算法的差分功耗分析攻击方法

功耗分析攻击主要分为三种: 简单功耗分析攻击(SPA)、差分功耗分析攻击(DPA)和高阶功耗分析攻击(HOPA). 其中针对 AES、SM4 分组密码类, 差分功耗分析攻击是一种非常简有效攻击方法, 依据文献^[8], 其攻击步骤如下:

①随机产生 m 个 X_1, X_2, X_3 做异或运算得到 m 个输入明文;

②用第 1 步产生的明文和轮密钥做“异或”运算和“S 盒”运算, 保存相应的 S 盒输出结果, 记录汉明重量;

③猜测轮密钥的第一个字节可以有从 0x00 到 0xff 共 256 种可能的取值, 其中必有一个值与正确轮密钥的第一字节一致. 用第①步产生的明文的第一个字节分别和这 256 个值重复第②步计算, 保存相应的 256 组计算结果;

④设置选择函数: $D(X_m, b, K_s) = S(X_m \oplus K_s)_b$ 即根据第③步运算结果的任一比特位的值把第①步中的计算结果做分集, 分成 0 集合和 1 集合, 共得到 256 组分集;

⑤分别计算 256 组分集中 0 集合与 1 集合的平

均能量消耗值, 即平均汉明重量值;

⑥根据第⑤步的计算结果, 计算每组中两个集合的平均能量消耗差绝对值, 共得到 256 个结果;

⑦根据第⑥步的计算结果分析轮密钥第 1 字节的值, 如果功耗差分值接近于 0, 则表示相应的轮密钥假设值错误, 如果功耗差分值明显较大, 则相应的 8 bit 块密钥假设值正确. 以此为例可以得到另外 3 组 8 bit 块的密钥值, 最终得到该轮的 32 位密钥值;

如果能够得到一个轮的正确密钥值, 利用密钥扩展算法可以推导出密钥的初始密钥, 最终成功完成对 SM4 算法的差分功耗分析攻击.

3.2 针对差分功耗分析攻击的防护措施

为了提高 SM4 算法抗差分功耗分析攻击能力, 设计尝试从算法级、门级电路结构和晶体管级电路选取最佳的防御方法. 相比较于算法级和晶体管级电路防护方法, 门级结构电路防护方法可以在不改变加密标准算法的前提下, 利用传统标准单元库实现算法的抗差分功耗分析攻击能力, 门级结构电路防护中采用随机掩码的防护技术是最常用, 也是最有效的一种. 随机掩码技术^[9]是在算法的实现过程中引入随机数, 把所有与密钥有关的中间数全部掩蔽, 而该随机数由电路随机产生, 攻击者无法从外部获取有关随机数的信息, 这样电路功耗将与被随机数掩蔽后的中间数据相关, 而攻击者无法了解这些电路内部产生的随机数, 因此也就无法通过功耗分析攻击方法获取密钥等保密信息.

在随机掩码技术中, Akkar 和 Trichina 提出了乘法掩码^[10]的方法, 来抵抗一阶差分功耗分析攻击, 但是这种方法不能够抵抗零值攻击. 为了能够有效抵抗零值攻击, Elisabeth 提出了一种加法掩码技术^[11], 这种掩码技术实际上并不是单一的掩码技术, 而是综合了加法掩码技术和乘法掩码技术, 但运算过程中所得的中间数据均被加法掩码所掩蔽, 利用这种方式来减小功耗与明文数据操作的相关性, 从而实现抗差分功耗分析攻击能力与抗零值攻击能力.

S 盒由线性转换和有限域求逆两部分组成, 在掩码过程中, 线性部分可以直接通过异或电路来实现, 而非线性运算即有限域求逆部分就需要通过添加修正项来完成掩码工作. Elisabeth 提出的加法掩码是在复合域内实现的, 令输入数据为 $a + m$, 其中 $a \in GF(2^8)$ 为原始输入, $m \in GF(2^8)$ 为随机掩码因子. 首先, 将每一个 8 位输入 a 都映射到 $GF(2^4)$ 域, 即 $a = a_h x + a_l$, $m = m_h x + m_l$ 其中 $a \in$

$GF(2^8)$, $a_h, a_l \in GF(2^4)$, $m_h, m_l \in GF(2^4)$, 求逆运算从 $GF(2^8)$ 域降低到 $GF(2^4)$ 域, 从而降低了S盒运算的复杂度, 掩码后的数据求逆可以通过式(13)~(16)求得。

$$((a_h + m_h)x + (a_l + m_l))^{-1} = (a'_h + m_h)x + (a'_l + m_l) \quad (13)$$

$$a'_h + m_h = \underbrace{(a_h + m_h)(d^{-1} + m_l)}_{dm4} + \underbrace{(d^{-1} + m_l)}_{C7} +$$

$$\underbrace{(a_h + m_h)m_l}_{C1} + \underbrace{m_h m_l}_{C5} + \underbrace{m_h}_{C6} \quad (14)$$

$$a'_l + m_l = (a'_h + m_h) + \underbrace{(a_l + m_l)(d^{-1} + m_l)}_{dm5} + \underbrace{(d^{-1} + m_l)m_l}_{C8} + \underbrace{(a_l + m_l)m_h}_{C2} + \underbrace{m_l + m_h m_l + m_h}_{C9 \quad C5 \quad C6} \quad (15)$$

$$d + m_h = \underbrace{(a_h + m_h)^2}_{dm1} \nu + \underbrace{(a_h + m_h)(a_l + m_l)}_{dm2} +$$

$$\underbrace{(a_l + m_l)^2}_{dm3} + \underbrace{(a_h + m_h)m_l}_{C1} + \underbrace{(a_l + m_l)m_h}_{C2} + \underbrace{m_h^2 \nu + m_l^2 + m_h m_l + m_h}_{C3 \quad C4 \quad C5 \quad C6} \quad (16)$$

通过以上计算公式可以发现, 运算过程中所有的中间项都被随机数进行了加法掩蔽, 这就减弱了功耗与执行数据的相关性, 提高了算法的抗差分功耗分析攻击能力。

4 基于PPRM结构的加法掩码SM4电路结构实现

Elisabeth提出的加法掩码是在复合域的基础上实现的, 虽然利用复合域进行求逆运算可以大大降低S盒硬件开销, 但是带来更大的延时和功耗; 依据文献[12], 相比于复合域方法实现的S盒, 基于PPRM结构的S盒运算电路具有更小的功耗与更快的运行速度。

4.1 PPRM结构

Tsutomu Sasao提出任何一个逻辑函数 $f(x_1, x_2, x_3, \dots, x_n)$ 均可以表示成如下表达式:

$$f = a_0 \oplus a_1 x_1 \oplus \dots \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus a_{13} x_1 x_3 \oplus \dots \oplus a_{m-1} x_n x_{n-1} \oplus \dots \oplus a_{12 \dots n} x_1 x_2 \dots x_n \quad (17)$$

式(17)中各项均不存在变量逻辑非运算, 因此式(17)称为正极性Reed-Muller展开式(PPRME), 所对应的电路结构称为PPRM结构。PPRM结构是由AND-XOR这样的逻辑模块构成, 即与门和或门

构成的逻辑模块, 或门逻辑单元后置于与门逻辑单元时, 利用与门的开关性可以减少信号传输过程中动态冒险的传播, 降低不必要的功耗。

对于一个固定的逻辑函数有且仅有一个正极性Reed-Muller展开式与之对应, 如果上述加法掩码S盒利用AND-XOR逻辑模块单元来实现复合域内的算术与逻辑运算, 就可以生成一个与复合域S盒相对应的PPRM结构S盒。

4.2 SM4 S盒电路结构实现

当把加法掩码后的SM4 S盒作为一个独立的8输入8输出的模块转换成PPRM结构时, 电路可能会带来很大的硬件开销。但是, 如果选择性地将电路分成几个模块分别转换成对应的PPRM结构, 即Multi-PPRM结构, 就可以实现一款功耗低、延时小、硬件开销适中的S盒电路模块。

依据文献[12], S盒采用了三阶PPRM结构: 前段转换, $GF(2^4)$ 域求逆, 后端转换。本设计将加法掩码后的S盒后端转换部分分成两级PPRM结构, 从而生成了四阶PPRM结构, 四部分电路均独立采用AND-XOR结构来实现, 其电路结构如图3所示。

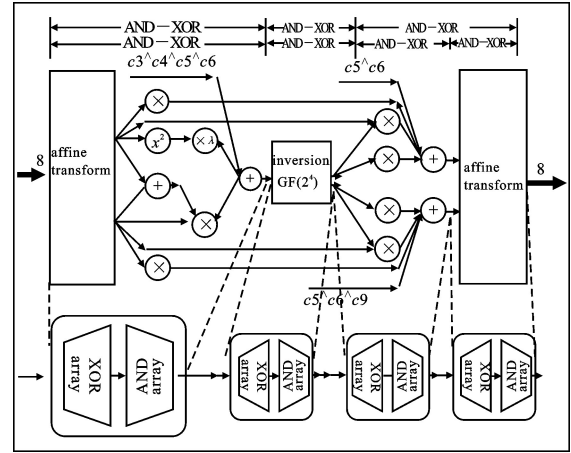


图3 基于PPRM结构加法掩码后的SM4 S盒

为了平衡信号经过第二阶的传输延时, 可以在第一阶直接到第三阶的信号传输过程中加入延时单元, 使得各路数据到达第三阶输入端的时间相同从而减少动态冒险的产生。

4.3 仿真结果与分析

4.3.1 差分功耗分析仿真

在电路抗差分功耗分析攻击能力方面, 利用密钥 $rk=241$ 对2000组随机生成的128 bit数据进行轮函数加密运算, 同时记录2000组随机数据所对应的密文和功耗曲线波形图。按照第3部分所描述的攻击方法对非掩码SM4算法和掩码SM4算法轮函数的一组

8bit 数据模块进行差分功耗分析攻击. 对非掩码 SM4 算法进行差分功耗分析攻击结果如图 4 所示, 当密钥假设值 $rk_{i,j,s}=241$ 时, 对应的功耗最大差分值最大, 表明差分功耗分析攻击成功. 对掩码 SM4 算法进行差分功耗分析攻击, 结果如图 5 所示, 与图 4 相比, 功耗差分值没有很明显的波峰, 而在对应的密钥假设值 $rk_{i,j,s}=241$ 所对应的功耗最大差分值更是处于波谷的地方, 通过差分功耗分析攻击并不能得出正确密钥值 $rk_{i,j,s}=241$, 表明该掩码技术使得 SM4 算法实现具有抗差分功耗分析攻击的能力.

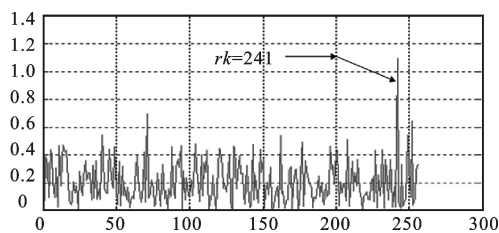


图 4 非掩码 SM4 差分功耗分析攻击结果波形图

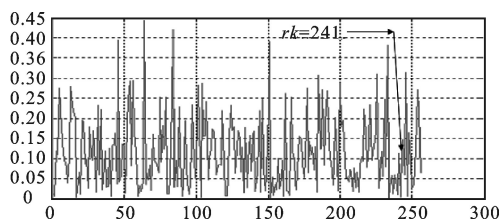


图 5 掩码 SM4 差分功耗分析攻击结果波形图

4.3.2 功耗比较

在 SM4 电路结构中, S 盒运算直接决定着 SM4 算法电路的功耗. 在 SMIC 0.18 μm CMOS 工艺下, 本设计对掩码 SM4 S 盒进行了设计综合验证, 通过 Design Compiler 综合得出 S 盒电路模块延时与面积消耗, 并利用 Prime Power 进行了功耗仿真, 得出的结果如表 1 所示. 仿真结果表明, 多阶 PPRM 结构可以以较小的面积代价实现更低的功耗消耗与更小的延时, 与复合域实现的 SM4 S 盒相比, 多阶 PPRM 结构 S 盒的功耗延时积减小了 70%, 因此更加适合于低功耗.

表 1 复合域与 PPRM 结构实现的 SM4 S 盒对比

S-box	Average power (mW@10 MHz)	Delay/ns	Area/ μm^2
Composite field	2.449 0	7.6	15 224.933 1
PPRM	0.737 0	4.2	18 394.992 4

5 结束语

本设计实现了一款具有抗差分功耗分析攻击能力、功耗低、速度快、面积适中的 SM4 算法电路模

块, 该电路模块非常适用于对功耗和速度有较高要求的无线局域网设备. 算法采用了加法掩码技术来减少功耗与明文数据操作的相关性, 以此来抵抗差分功耗分析攻击. 与文献[11]相比, 本设计采用了 PPRM 电路结构, 以较小的面积代价来降低电路功耗并提高电路运行速度. 最终仿真结果显示, 该 SM4 算法电路在差分功耗波形图正确密钥值点处具有较低的差分功耗值, 实现了抵抗差分功耗分析攻击的目标, 另外基于 PPRM 结构的 SM4 S 盒的功耗延时积为 0.74 mW@10 MHz, 与复合域 S 盒相比功耗延时积减小了 70%.

参考文献:

- [1] Office of state commercial cipher administration of china. SM4 cipher for WLAN products[EB/OL]. [2014-04-16]. <http://www.oscca.gov.cn/UpFile/200621016423197990.pdf>.
- [2] Paul Kocher, Joshua Jaffe, Benjamin Jun. Differential power analysis[C]//CR PTO. USA: California. 1999: 388-397.
- [3] 徐艳华, 白雪飞, 郭立, 等. 适合 SMS4 算法硬件实现的 S 盒构造新方法[J]. 中国科学技术大学学报, 2009, 39(11): 1164-1170.
- [4] Wen Ji, Lei Hu. New description of SM4 by an embedding over $\text{GF}(2^8)$ [C]//Indocrypt 2007. India: Chennai, 2007: LNCS 4859: 238-251.
- [5] Sasao T. Logic synthesis and optimization[M]. Massachusetts. Kluwer Academic Publishers, 1993: 287-312.
- [6] 白雪飞, 郭立, 徐艳华, 等. SMS4 密码算法的差分功耗分析攻击研究[J]. 小型微型计算机系统, 2009, 30(3): 541-544.
- [7] 刘鸣, 陈弘毅, 白国强, 等. 功耗分析研究平台及其应用[J]. 微电子学与计算机, 2005, 22(7): 134-138.
- [8] 沈薇, 郑秀林. SMS4 算法的能量分析攻击及其防御研究[D]. 西安: 西安电子科技大学, 2009.
- [9] 李浪, 李仁发, 吴克寿, 等. 简化固定值掩码二姐差分功耗攻击方法及其防御措施[J]. 小型微型计算机系统, 2010, 31(9): 1894-1898.
- [10] Jovan D Golic, Christophe Tymen. Multiplicative masking and power analysis of AES [C]//CHES 2002. USA: Redwood City, 2002: 198-212.
- [11] Elisabeth Oswald, Stefan Mangard, Norbert Pramstaller, et al. A side-channel analysis resistant description of the AES S-Box[C]//FSE 2005. France: Paris, 2005(3557): 413-423.

(下转第 38 页)

端数字滤波器. 仿真结果表明, 与传统 FIR 滤波器相比, 本文的 FRM 滤波器复杂度降低约 50%, 性能也优于 FIR 滤波器, 并且滤波器系数可配置, 因而在软件无线电中推广应用.

参考文献:

- [1] 栗欣, 吴佳, 曾捷. LTE-Advanced 主导 3G 无线通信走向未来[J]. 移动通信, 2009, 23(12): 48-54.
- [2] Su Yi, Ming Lei. Backhaul resource allocation in LTE-Advanced relaying systems [C]// Proceedings of 2012 IEEE Wireless Communications and Networking Conference. Shanghai, 2012:1207-1211.
- [3] Gozalvez J. First LTE-Advanced commercial network deployed [J]. IEEE Vehicular Technology Magazine, 2013, 8(1): 10-17.
- [4] Lu Na, Zhu Xue tian, Jiang Zheng. Performance of LTE-Advanced macro-pico heterogeneous networks [C]// Proceedings of 2013 IEEE Wireless Communications and Networking Conference. Shanghai, 2013: 545-550.
- [5] 梁学俊, 杨夏善, 吴伟民, 等. 基于硬件行为的 TD-LTE 关键技术仿真方案[J]. 微电子学与计算机, 2013, 30(11): 71-75.
- [6] Mitola J. The software radio architecture[J]. IEEE Communications Magazine, 1995, 33(5): 26-38.
- [7] 杨玉庆. 3GPP LTE 下行接收系统的数字信号处理与 VLSI 实现研究[D]. 上海: 复旦大学, 2011.
- [8] Hartley R I. Subexpression sharing in filters using canonic signed digit multipliers[J]. Circuits Syst. II: Analog and Digital Signal, 1996, 43(10): 677-688.
- [9] Peiro M M, Boemo E I, Wanhammar L. Design of high-speed multiplierless filters using a nonrecursive signed common subexpression algorithm [J]. IEEE Trans. Circuits Syst. II: Analog and Digital Signal Processing, 2002, 49(3): 196-203.
- [10] Vinod A P, Lai E M. On the implementation of efficient channel filters for wideband receivers by optimizing common subexpression elimination methods[J]. IEEE Trans. Computer-Aided Design Integrated Circuits and Systems, 2005, 24(2): 295-304.
- [11] Chen K H, Chiueh T D. A low-power digit-based reconfigurable FIR filter [J]. IEEE Trans. Circuits Syst. II: Express Briefs, 2006, 53(8): 617-621.
- [12] Tang Z W, Zhang J, Min H. A high-speed, programmable, CSD coefficient FIR filter [J]. IEEE Trans. Consumer Electronics, 2002, 48(11): 834-837.
- [13] Lim Y C. Frequency-response masking approach for the synthesis of sharp linear phase digital filters [J]. IEEE Trans. Circuits And Systems, 1986, 33(4): 357-364.
- [14] Lian Y, Zhang L, Ko C C. An improved frequency response masking approach for designing sharp FIR filters [J]. IEEE Trans. Signal Processing, 2001, 49(12): 2573-2581.
- [15] Lu W S, Hinamoto T. Optimal design of frequency-response-masking filters using semidefinite programming [J]. IEEE Trans. Circuits and Systems, 2003, 50(4): 557-568.

作者简介:

张永满 男, (1987-), 硕士研究生. 研究方向为 LTE-A 软基带通信.

梁利平 男, (1969-), 研究员. 研究方向为多核处理器与系统.

管武 男, (1981-), 副研究员. 研究方向为通信与信息系统.

吴俊东 男, (1992-). 研究方向为微电子.

(上接第 32 页)

- [12] Sumio Morioka Akashi Satoh. An optimized S-box circuit architecture for low power AES design [C] // CHES 2002. USA: Redwood City, LNCS 2523, 2003: 172-186.

作者简介:

牛砚波 男, (1987-), 硕士研究生. 研究方向为 VLSI 与 SOC 设计.

蒋安平 男, (1969-), 博士, 研究员. 研究方向包括 VLSI 与 SOC 设计、计算机体系结构等.