一种适用于 RFID 标签的安全化密码算法实现

王晨旭[1],韩 良[1],喻明艳[2],王进祥[2]
(1.哈尔滨工业大学(威海)信电学院,山东威海 264209;2.哈尔滨工业大学航天学院,黑龙江哈尔滨 150001)

摘 要: 鉴于射频识别(RFID)标签芯片苛刻的资源要求,为解决差分功耗分析(Differential Power Analysis,DPA)对密码算法实现方面的威胁难题,将新型 DPA 防护技术 threshold 与 *Piccolo* 密码算法相结合,提出了一种适用于 RFID 标签芯片应用的安全化密码算法实现方案.分别基于布尔式重组和改进型穷举搜索的方式实现了面积最优的 S 盒及其逆的 threshold(3,3)分享,提出了基于锁存器方式解决 S 盒及其逆实现中潜在的毛刺威胁问题,在 Chartered 0.18μm 工艺和 100 kHz RFID 运行频率下,将该方案的资源消耗控制在 2155 个等效门,平均电流约为 2.60μA,基于 FPGA 的 DPA 攻击安全性分析结果表明该方案适合于低成本 RFID 标签芯片对密码算法轻型及实现安全的要求.

关键词: RFID 标签芯片; 安全; *Piccolo*; 差分功耗分析; threshold
中图分类号: TP309.2 **文献标识码:** A **文章编号:** 0372-2112 (2014)08-1465-09
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.08.002

A Secure Cipher Implementation Suitable for RFID-Tags

WANG Chen-xu[1], HAN Liang[1], YU Ming-yan[2], WANG Jin-xiang[2]
(1. *School of Information & Electrical Engineering, Harbin Institute of Technology at Weihai, Weihai, Shandong* 264209;
2. *School of Astronautics, Harbin Institute of Technology, Harbin, Heilongjiang* 150001)

Abstract: Hash resource required for RFID-tags chips, a secure and lightweight cipher implementation is proposed to solve the threat posed by differential power analysis(DPA). The proposed implementation is based on *Piccolo* cipher, in combination with the recently proposed masking method named threshold. Boolean equation rearrangement and improved exhaustive search method was respectively applied to S-Box and inverted S-Box to get their optimal area costs for threshold(3,3) share. A method based on latch is proposed to resist the latent glitch threat. Based on Chartered 0.18μm and 100 kHz operating frequency for RFID applications, the proposed cipher implementation costs as low as 2155 gate equivalents and consumes 2.60μA average current. The security of the implementation is evaluated based on real power traces from an FPGA platform. DPA attack results show the proposed implementation with threshold countermeasure is suitable for secure low-cost passive RFID-tag ICs.

Key words: RFID-tags IC; security; *Piccolo*; differential power analysis(DPA); threshold

1 引言

近年来,射频识别(RFID)标签的应用日益广泛,为了保障此类安全敏感设备的数据安全,通常在其中嵌入密码算法.然而,对于一个被动式 RFID 标签芯片,由于其本身不带电源,只能通过电磁耦合获取较少电量,文献[1]指出即使包括模拟前端部分在内,一个低成本 RFID 标签芯片的面积通常在 1000 个等效门(Gate Equivalents,GE)到 10000 GE 之间,此时留给密码算法部分的空间通常只在 200 GE 到 2000 GE 之间.在此情况下,占用资源少、功耗低的轻量级分组密码算法成为一个比较热门的话题[2~4],其中,PRESENT[2]和 *Piccolo*[3]是两种最典型的轻量级密码算法,其中 PRESENT 密码算法属于 SPN 结构;而 Piccolo 是索尼公司在 CHES2011 上提出的 Feistel 结构型分组密码算法.

虽然轻量级密码算法在提出时均保证了其算法本身的安全性,然而,近年来,密码算法的实现安全性却受到了差分功耗分析(Differential Power Analysis,DPA)攻击的严峻挑战[5~7],为了充分保障密码芯片的安全,在设计密码芯片之时通常都会加入 DPA 防护措施[8~12],文献[13]针对这些传统防护措施进行了研究,指出这些防护措施在提高安全性的同时也显著增加了芯片面积和功耗,不太适用于资源受限的 RFID 标签芯片中,正因如此,一些主流芯片制造商都把抗 DPA 攻击的安全化

收稿日期:2013-09-30;修回日期:2014-06-17;责任编辑:马兰英
基金项目:国家自然科学基金(No.61202481)

RFID 标签作为其下一代产品[14],现有研究成果中也很少宣称其抗 DPA 攻击的密码算法实现是轻量级的,Karpinskyy 等人在文献[15]中展示了轻量级分组密码算法 mCrypton 的抗 DPA 攻击掩码实现方式,其中 64 位密钥版本的 mCrypton 实现要求 6929 GE;Moradi 等人将 AES 加密单元压缩至迄今为止最小的 2400 GE,然而一旦加入防护措施[16,17],其电路规模将达到 10000 GE 以上[18];显然,这些研究结果都很难在 RFID 标签芯片中应用,文献[14]首次研究了抗 DPA 攻击的分组密码算法在 RFID 标签芯片中实现的可能性,作者将 Threshold 技术实现于串行化 PRSENT 密码算法,仅仅要求 2300 GE 即可实现抵抗 DPA 攻击的加密算法,然而作者在其重要的 S 盒实现中没有考虑毛刺(Glitch)的潜在威胁[19,20].鉴于 Feistel 结构型密码算法的优势,本文则尝试将 threshold 技术与 Feistel 结构型密码算法 *Piccolo* 相结合,提出了 *Piccolo* 密码算法 S 盒及其逆的优化 threshold 实现,并解决了其毛刺隐患问题,给出一种可用于 RFID 标签芯片的安全化密码算法实现方案并评价了该实现的安全性.

2 基本理论及 *Piccolo* 密码算法简介

2.1 Threshold 型掩码方案的基本理论

传统掩码技术是一种(2,2)秘密分享(Secret Sharing)方案技术[21],随机掩码能够随机化密码算法运算期间的真值,使密码设备的能量消耗独立于加密过程的真值,扰乱了功耗信息的泄漏,从而使 DPA 攻击者的难度加大;文献[21]指出通过使用 n 个掩码可以抵抗 n 阶 DPA 攻击防护,但是文献[11]则指出这种(2,2)掩码技术的 DPA 防护效果并不理想,Nikova 等人基于此原理在文献[16,17]中扩展了掩码思想提出了使用(3,3)或者更多秘密分享的 threshold 实现技术(为书写方便下文将 Threshold Implementation 缩写为 TI),它的基本思想是将原先的单数据通路拆分成 N 条数据通路,任何一条数据通路只携带经过随机掩码后 N 分之一的信息,根据 TI 的指导思想[16,17],对于一个($N-1$)次的布尔函数式,要想保证电路被完全掩盖,至少需要 N 路基于 TI 理论的秘密分享.为了达到面积和复杂度的折衷,此处我们取 N 为 3,也即形成 TI(3,3)分享,下面以四输入布尔函数为例说明 TI(3,3)分享的基本原理.

如无特殊说明,下文的变量一般以大写字母(例如 $\boldsymbol{X}$,$\boldsymbol{X}_a$ 等)代表四个元素的向量,即 $\boldsymbol{X}\in \mathrm{GF}(2^4)$,以小写字母(例如 x,x_a 等)代表一位宽的变量,即 $x\in \mathrm{GF}(2)$;下文的函数名一般以大写字母(例如 F,F_a 等)代表具有四位输出的函数,以小写字母表示的函数(例如 f_1,f_{a1}等)代表一位输出的函数.如图 1(a)所示,假设某函数 F 是一个二次布尔函数式,所谓二次布尔函数式,是指函数 F 的每一位输出 $f(\boldsymbol{X})=f(x,y,z,w)$都不包含形如 xyz 或 $xyzw$ 的三次或四次项,依据 TI 理论,此时 F 可以拆分成如图 1(b)所示的 TI(3,3)分享结构,在图 1(b)中,a,b,c 表示分享后的三条通路,$\boldsymbol{X}_a$,$\boldsymbol{X}_b$,$\boldsymbol{X}_c$ 分别表示三个输入分享,F_a,F_b,F_c 分别表示三个输出分享,拆分要满足如下三条性质[16,17]:

(1)不完全性(Non-completeness)

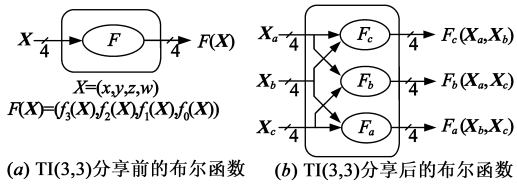
在图 1(b)中,每个输出分享至少独立于一个输入分享,例如,F_a 不依赖于 $\boldsymbol{X}_a$,换言之 F_a 只是 $\boldsymbol{X}_b$ 和 $\boldsymbol{X}_c$ 的函数.

(2)正确性(Correctness)

图 1(a)中,如果对于任意输入的 $\boldsymbol{X}$($\boldsymbol{X}$ 为分享前的输入变量),在图 1(b)中,总 $F(\boldsymbol{X}_a\oplus\boldsymbol{X}_b\oplus\boldsymbol{X}_c)=F_a(\boldsymbol{X}_b,\boldsymbol{X}_c)\oplus F_b(\boldsymbol{X}_a,\boldsymbol{X}_c)\oplus F_c(\boldsymbol{X}_a,\boldsymbol{X}_b)$ 有成立,则称 F_a,F_b,F_c 满足正确性.

(3)平衡性(Balance)

假设所有输入变量 x,y,…以及它们的输入分享均满足不完全性,如果 $\Pr(z=\bar{Z}\mid z=\bigoplus_i Z_i)=\mathrm{C}$(C 为常数)成立,则称 $z=\mathrm{NL}(x,y,\cdots)$的实现是平衡的.



(a) TI(3,3)分享前的布尔函数 (b) TI(3,3)分享后的布尔函数

图1 TI(3,3)分享的基本原理

上述三条性质中,性质(2)保证了正确的实现加密功能;性质(1)则是这种实现思想的关键,由它来保证加密过程的每个节点的能量消耗独立于真值;性质(3)则是为了保证加密过程中每个操作的输出作为下一个操作的输入仍然满足均匀分布.

2.2 *Piccolo* 密码算法简介

Piccolo 分组密码算法的分组长度为 64-bit,支持 80-bit 和 128-bit 两种密钥长度,分别用 *Piccolo*-80 和 *Piccolo*-128 表示,对应的迭代轮数分别为 25 轮和 31 轮.本文以 *Piccolo*-80 为研究对象,为方便解释,下文在无特殊说明的情况下,*Piccolo* 均指 *Piccolo*-80.限于篇幅,以下仅对算法的数据通路和 S 盒部分做简要介绍.

Piccolo 算法采用广义 Feistel 结构,数据处理部分以 64-bit 明文、白化密钥和轮密钥为输入经由 25 轮迭代后产生 64-bit 密文输出,如图 2 所示,从图中可以看出,除最后一轮外,每轮包含两类变换,分别是 F 函数 F:$\mathrm{GF}(2^{16})\rightarrow\mathrm{GF}(2^{16})$和轮置换 RP:$\mathrm{GF}(2^{64})\rightarrow\mathrm{GF}(2^{64})$,最后一轮不包含轮置换 RP.

Piccolo 的 F:$\mathrm{GF}(2^{16})\rightarrow\mathrm{GF}(2^{16})$也被称为超级 S 盒,采用两层 S 盒内夹混淆矩阵 $\boldsymbol{M}$ 层的三明治结构,具有

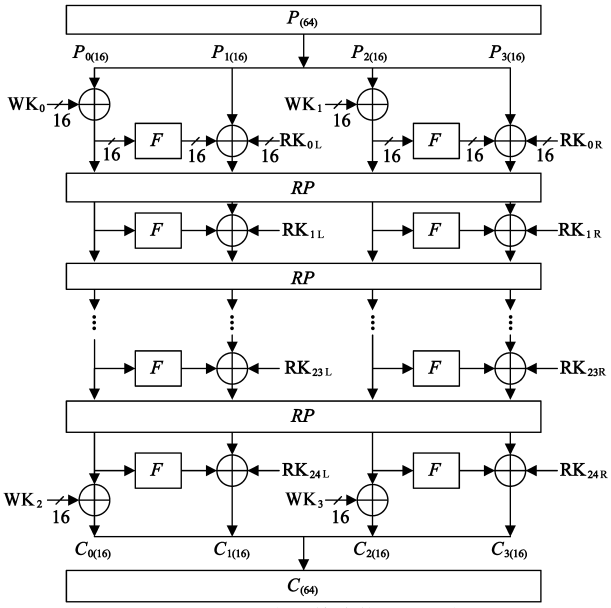


图2 *Piccolo*密码算法数据处理流程

更强的混淆能力,其中,S 盒 $S:\mathrm{GF}(2^4)\to\mathrm{GF}(2^4)$是 *Piccolo* 中唯一的非线性操作,其映射关系如表 1 所示.

表 1 *Piccolo* 算法 S 盒 4-bit 双射映射表

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(X)$	E	4	B	2	3	8	0	9	1	A	7	F	6	C	5	D

3　S 盒及其逆的 TI(3,3)分享实现

像传统掩码技术一样,threshold 实现的难点和重点在于密码算法非线性 S 盒的实现.对于一个布尔函数式 F,要想实现其 TI(3,3)分享并保证满足以上三条性质,需保证原函数 F 为二次布尔函数式,如果 F 为三次布尔函数式,则要将其分解为两个二次布尔函数式的级联. *Piccolo* 的 S 盒及其逆都是三次函数,为实现其 TI(3,3)分享,所以需要将二者进行二次分解.

3.1　S 盒的二次分解

定义 $X=(x,y,z,w)$为 S 盒的输入,s 为 S 盒的输出,下标 3 表示输出的最高有效位,下标 0 表示输出的最低有效位.根据文献[3],可以将 *Piccolo* 的 S 盒的输出(s_3,s_2,s_1,s_0)直接写成布尔表达式,并根据$\overline{x+y}=1\oplus x\oplus y\oplus xy$ 和$\overline{x+y}=\bar{x}\cdot\bar{y}$ 对其化简:

$$s_3=\overline{(x+y)}\oplus w=1\oplus x\oplus y\oplus w\oplus xy$$

$$s_2=\overline{(y+z)}\oplus x=1\oplus x\oplus y\oplus z\oplus yz$$

$$s_1=\overline{\overline{(s_3+z)}\oplus y}=1\oplus y\oplus\overline{s_2}\cdot\bar{z}$$

$$s_0=\overline{(s_2+s_3)}\oplus z=z\oplus\overline{s_2}\cdot\overline{s_3}$$

仔细观察可以发现 s_3 和 s_2 都是只有一次项和二次项,三次项仅 s_1 和 s_0 中出现,并且其复用了 s_3 和 s_2 的结果.如果认为 s_3 和 s_2 是 s_1 和 s_0 的输入,那么 s_1 和 s_0 也可以认为是二次运算,因此我们可以将 S 盒拆分成如图 3 所示的 P,Q 两个二次布尔函数的级联:

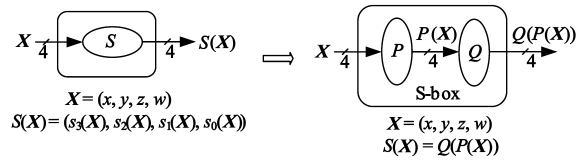


图3 *Piccolo* S盒的二次分解

此处,$P(X)=P(x,y,z,w)=(p_3,p_2,p_1,p_0)$,$Q(P(X))=Q(P(x,y,z,w))=(q_3,q_2,q_1,q_0)$,其中:

$$p_3=y \qquad q_3=1\oplus p_1$$

$$p_2=1\oplus z \qquad q_2=1\oplus p_0$$

$$p_1=x\oplus y\oplus w\oplus xy \qquad q_1=1\oplus p_3\oplus p_2p_1$$

$$p_0=x\oplus y\oplus z\oplus yz \qquad q_0=1\oplus p_2\oplus p_1p_0$$

相应的函数 P 和 Q 查找表如表 2 所示.

表 2 经 S 盒分解后的 P 和 Q 查找表

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$P(X)$	4	6	1	3	F	D	B	9	7	5	2	0	E	C	A	8
$Q(X)$	F	B	7	2	E	A	4	1	D	9	5	0	C	8	6	3

3.2　S 盒逆的二次分解

通常,对于 Feistel 结构型密码算法,无论加密还是解密都不需要使用 S 盒逆, *Piccolo* 算法的提出者在文献[3]中指出采用 S 盒逆可以有效节约硬件成本,因此,本文出于 RFID 标签芯片应用的目的完成了 S 盒逆的 TI(3,3)分享实现.与 S 盒相似,先实现 S 盒逆的分解获得二次布尔函数 P 和 Q,但是,由于文献[3]并未给出 S 盒逆的布尔表示式,也无法将其写成简易的布尔表示式,所以 S 盒逆的二次分解过程成为了 *Piccolo* 密码算法 TI 实现的难点.

假设 S 盒逆已经完成二次分解,并得到如图 3 所示的两个二次布尔函数 P 和 Q 的级联.此时,$(p_3,p_2,p_1,p_0)=P(X)=P(x,y,z,w)$中的每一位 $p_i(0\leqslant i\leqslant 3)$都应该形如:

$$p_i=a_0\oplus a_1x\oplus a_2y\oplus a_3z\oplus a_4w\oplus a_5xy\oplus a_6xz\oplus a_7xw\oplus a_8yz\oplus a_9yw\oplus a_{10}zw$$

由此,对于 P 和 Q 的四个比特,采用向量表示法,可以将 $P(X)$和 $Q(X)$表示为:

$$P(X)=A_0\oplus A_1x\oplus A_2y\oplus A_3z\oplus A_4w\oplus A_5xy\oplus A_6xz\oplus A_7xw\oplus A_8yz\oplus A_9yw\oplus A_{10}zw$$

$$Q(X)=B_0\oplus B_1x\oplus B_2y\oplus B_3z\oplus B_4w\oplus B_5xy\oplus B_6xz\oplus B_7xw\oplus B_8yz\oplus B_9yw\oplus B_{10}zw$$

此处,$A_i\in\mathrm{GF}(2^4)(0\leqslant i\leqslant 10)$,可以看出,为确定函数 P 和 Q,需要确定 88 个待定系数,为此,我们需要在 2^{88}的搜索空间中搜索出满足以下条件的函数 P 和 Q.

条件(1):P 和 Q 都是双射变换.

条件(2):满足 $S^{-1}(x,y,z,w)=Q(P(x,y,z,w))$.

条件(3):能够满足上文中引用的三条 TI 性质.

如果直接在 2^{88} 的搜索空间内搜索,则很难在有意义的时间内完成工作,因此,我们必须采用快速搜索算法,考虑到如果 P 是双射变换,那么 Q 也必然是双射变换,于是问题转化为搜索所有可能的二次函数 P,然后验证 Q 是否满足所需条件[14],采用这种方式,可以将搜索空间降低为 2^{44};其基本搜索算法如下:

Step1:搜寻满足式(1)的双射 P 的所有系数组合,由 P 的这些系数组合构成集合 G1.

Step2:在 G1 中找出子集 G2,使得满足条件(2)的二次布尔函数 Q 存在.

Step3:从 G2 中找出子集 G3,使函数 P 经过 TI(3,3)分享后满足 TI 理论的均匀性.

Step4:遍历满足以上条件的函数 P 的系数组合形成的集合 G3,找出相应的满足式(1)和 TI 理论三条性质的函数 Q 的系数组合,由此确定由函数 P 与 Q 的系数组合构成的集合 G4.

事实上,即便将搜索空间降低为 2^{44},搜索函数 P 和 Q 的目标系数组合仍需花费较多时间,我们在搜索过程中充分利用了上述三个条件并充分考虑了硬件的特点,将搜索空间降低为 $2^{21}\sim2^{22}$ 并最终搜索 26680 个满足条件的函数 P 和 Q 的系数组合.所有这些组合虽然都能满足功能正确的要求,但显然 P 和 Q 函数的不同构成会显著影响最终电路面积,因此需要从 G4 中找出面积最优的组合.通常异或门(XOR)相对与门(AND)具有更大的版图面积,仿照文献[14],假设一个 AND 门的等效门权重为 1GE,一个 XOR 门的等效门权重为 2GE,按照 TI(3,3)分享理论,在分享前 p_i 或者 $q_i(0\leqslant i\leqslant3)$ 中的每 1 个 XOR 门经过分享实现后都拓展成三路,一共需要 3 个 XOR 门,即权重为 6,而每一个 AND 门经过分享实现后需要 3×3 个 XOR 门和 3×3 个 AND 门,即权重为 27.据此,可以采用下式对 G4 进行筛选,得到 3 个等效门预估个数最小的结果构成集合 G5,其等效门预估权重为 194.

(3,3)分享后等效门权重≈2×P 和 Q 中常数项总个数
+6×P 和 Q 中一次项总个数
+27×P 和 Q 中二次项总个数
−6×(4+4)

在 3 个结果中有 1 项结果的 p_1 和 p_0 的 $x\oplus w\oplus xy$ 与 q_3 和 q_0 中的 zw 是可以复用的,采用此项结果将会获得最大的硬件复用,因此选择此项结果.最后,考虑函数 P 的 4 位输出的顺序,可以得到 4! ×3=72 个结果.实际中我们最终选定的组合如下式所示,相应的函数 P 和 Q 查找表如表 3 所示.

$$P(x,y,z,w)=(p_3,p_2,p_1,p_0)$$
$$p_3=x$$
$$p_2=1\oplus y$$
$$p_1=x\oplus y\oplus w\oplus xy$$
$$p_0=y\oplus z\oplus w\oplus xy\oplus xw$$
$$Q(x,y,z,w)=(q_3,q_2,q_1,q_0)$$
$$q_3=1\oplus y\oplus zw$$
$$q_2=1\oplus w$$
$$q_1=1\oplus z$$
$$q_0=x\oplus yw\oplus zw$$

表 3 经 S 盒逆分解后的 P 和 Q 查找表

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$P(X)$	4	7	5	6	3	0	2	1	E	C	F	D	A	8	B	9
$Q(X)$	E	A	C	1	6	3	4	8	F	B	D	0	7	2	5	9

3.3 S 盒及其逆的简单 TI(3,3)分享实现

将三次的 S 盒及其逆用 P 和 Q 两个二次布尔函数级联替代后,电路已经适合使用 TI(3,3)秘密分享来实现.S 盒及其逆可以采用相似的方式进行,这里以 S 盒为例说明 P 和 Q 函数拆分成 a,b,c 三条通路的过程,拆分过程要满足上文中的三条性质,如图 4 所示.

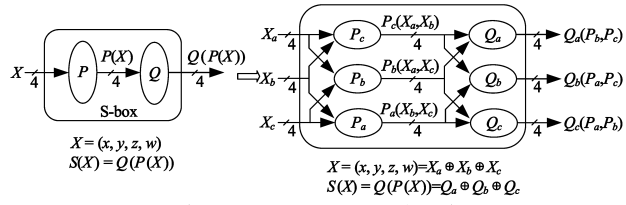


图4 S盒二次分解后的(3,3)分享示意图

首先,我们先将 S 盒的 4-bit 输入 $\boldsymbol{X}=(x,y,z,w)$ 由三组数据 $X_i=(x_i,y_i,z_i,w_i)(i=a,b,c)$ 来表达,且满足($x=x_a\oplus x_b\oplus x_c$, $y=y_a\oplus y_b\oplus y_c$, $z=z_a\oplus z_b\oplus z_c$, $w=w_a\oplus w_b\oplus w_c$),并且假设它们的条件概率分布都为均匀分布.下面我们以 P 函数的最低位 p_0 为例,具体说明 P,Q 函数的 TI(3,3)分享实现.

根据前述结果:$p_0=x\oplus y\oplus z\oplus yz$,将四个变量的三输入分享代入得到:

$$p_0=x_a\oplus x_b\oplus x_c\oplus y_a\oplus y_b\oplus y_c\oplus z_a\oplus z_b\oplus z_c\oplus(y_a\oplus y_b\oplus y_c)\cdot(z_a\oplus z_b\oplus z_c)$$

其中:$(y_a\oplus y_b\oplus y_c)\cdot(z_a\oplus z_b\oplus z_c)=y_az_a\oplus y_bz_b\oplus y_cz_c\oplus y_az_b\oplus y_az_c\oplus y_bz_a\oplus y_bz_c\oplus y_cz_a\oplus y_cz_b$,此时,我们希望将输出结果 p_0 也拆分成三输出分享:p_{a0},p_{b0},p_{c0} 分配时的基本约束条件则为上述三条性质,例如,y_az_b, y_bz_a 只能分配在 p_{c0} 中;对于只有单一分享元素的项我们则采用了惯例将其分配在相邻下一个分享里,例如将 x_a

和 $y_a z_a$ 分配在 p_{b0} 中,于是,p_0 的(3,3)分享实现为:

$$p_{a0} = x_b \oplus y_b \oplus z_b \oplus y_b z_b \oplus y_b z_c \oplus y_c z_b$$

$$p_{b0} = x_c \oplus y_c \oplus z_c \oplus y_c z_c \oplus y_a z_c \oplus y_c z_a$$

$$p_{c0} = x_a \oplus y_a \oplus z_a \oplus y_a z_a \oplus y_a z_b \oplus y_b z_a$$

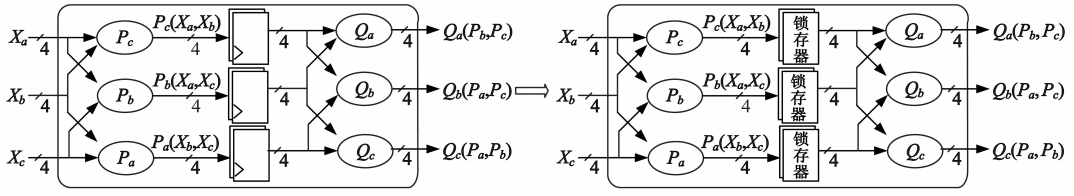
之后,仿照此方法可以分别完成 p_1, p_2, p_3 的(3,3)分享.至此,单一通路的 P 和 Q 就分别被三个通路分享,而且 P 和 Q 已经能够满足正确性和不完全性,还需要验证以上分享方案能够满足均匀性.由于 P 和 Q 经过(3,3)分享后都是 12 位输入、12 位输出的布尔函数,因此,对于 P 和 Q 可以使用相似的验证方法,这里以 P 为例,如果 P 的 12 位输入($\boldsymbol{X}_a, \boldsymbol{X}_b, \boldsymbol{X}_c$)和 12 位输出($P_a, P_b, P_c$)能够形成双射,也即对于固定的 P,且满足 $P = P_a \oplus P_b \oplus P_c$ 的 2^8 种输出各出现一次,从而满足输出的条件分布为均匀分布的要求,即满足性质 3.基于此,我们遍历 P 和 Q 的输入发现每种输出都只出现一次,证明经过上述(3,3)分享后的 P 和 Q 都满足均匀性.

仿照上述方法,可以完成 S 盒逆的 TI(3,3)分享,此处不再赘述.

3.4　考虑毛刺威胁的 S 盒及其逆的 TI(3,3)实现

在 CMOS 电路中,组合逻辑单元彼此连接,受各单元的路径和传播延迟不同的影响,电路的输出和中间值会出现临时的状态,这就是所谓的毛刺(Glitches).在某些复杂的 CMOS 电路中,毛刺的出现增加了电路的转换状态,并且像雪崩(Avalanche)一样在电路之间传播,成为电路功耗的主要部分.由于毛刺的产生与制造工艺和实现细节都息息相关,所以很难用数学模型对毛刺进行建模,尽管如此,毛刺的出现及其多少与数据之间存在相关性已经成为公认的事实,这使得电路容易受到 DPA 攻击[19,20].

3.3 中关于 S 盒及其逆的安全实现方案中虽然服从 TI 的三条性质,但是算法合理性与电路实现方面的安全性还存在一定的距离,图 4 中,实现 P 函数的三个分享通路在延迟上的不同可能会在某条分享通路(这里假设是 P_a)上出现毛刺,这个毛刺的存在会使 X_a, X_b, X_c 这三个变量的信息同时出现在 Q_b, Q_c 函数的实现上,违背了 TI 实现对通路不完全性的重要要求,给电路带来安全隐患.为消除这种毛刺威胁,自然的想法是:采用触发器对 P 和 Q 进行隔离,如图 5(a)所示,这些触发器可以将来自函数 P 的毛刺阻断在进入 Q 之前,事实上,在组合逻辑中插入触发器更加类似于流水线的实现方式,针对流水线的特点,一级触发器就会造成一个节拍(周期)的延迟,这样会对原有设计控制通路造成影响,给设计带来难度,此外触发器本身的实现面积较大.



(a) 基于触发器解决方案　　(b) 基于锁存器解决方案

图5　考虑毛刺威胁的S盒及其逆的TI(3,3)实现

考虑到上述弊端,并结合标准单元库中一般都包含钟控锁存器的事实,本文引入了基于锁存器的解决方案,如图 5(b)所示.在以 Chartered 0.18μm CMOS 为目标工艺的实现中,本文选用了低电平有效的锁存器 TLATN(假设电路其余部分的触发器为上升沿有效),控制信号选择时钟信号,在时钟为高电平时保持数据,低电平时更新数据,同时保证 P 函数的组合逻辑运算在高电平期间完成(这在运行频率要求不高的密码芯片设计中是容易做到的),这样就能在让毛刺有效地止步于锁存器.在实际实现中,采用这种锁存器的方案比触发器的方案能够节省约 45 个 GE 的面积空间,并且对控制通路不必做任何调整.

4　*Piccolo* 算法的串行化 TI(3,3)实现方案

文献[3]在提出 *Piccolo* 密码算法时,给出了两种建议的 *Piccolo* 实现方式:(1)基于轮的实现方式可以得到较高的吞吐量;(2)基于四位数据通路的串行化实现方式可以达到较少的实现面积.为了探讨 *Piccolo* 在 RFID 标签芯片中的可行性,我们首先实现了不带 DPA 防护的串行化实现方式(下称方案 1),然后基于 TI 理论完成了 *Piccolo* 的串行化 TI(3,3)实现(下称方案 2),其明文部分的数据通路如图 6 所示.图 6 中,实线部分为方案 1 的明文数据通路,在此基础上加入图中虚线部分则构成能够抵御 DPA 攻击的方案 2 的明文数据通路,其中虚线的 S 盒及其逆的 TI 实现中已经采用了锁存器电路解决毛刺威胁问题.

之后,我们基于 Chartered 0.18μm 工艺分别对 TI(3,3)实现前后的 *Piccolo* 算法进行了逻辑综合,综合工具采用 Synopsys 公司的 Design Compiler X-2005.09-SP4,为便于横向比较,逻辑综合时也采用了 100kHz 的 RFID 时

钟频率,综合结果如表 4 所示.从表 4 可以看出,加入了 TI(3,3)分享防护措施后,*Piccolo* 密码算法的串行化实现面积也仅仅约 2155GE,在考虑毛刺威胁后,比同样基于 0.18μm 的参考文献[14]的实现更加接近 2000GE 的门槛.

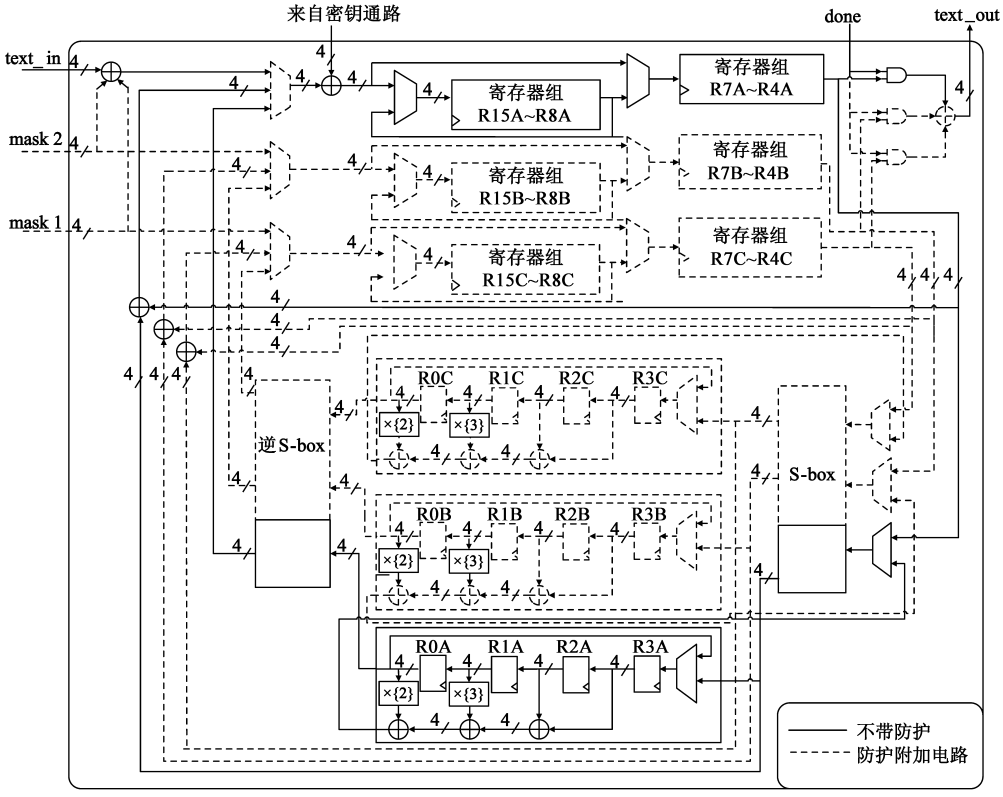


图6 安全化*Piccolo*密码算法明文数据通路

表 4 串行化 *Piccolo* 密码算法经 TI(3,3)分享前后的综合结果(单位:GE)

	控制通路	密钥部分数据通路	明文部分数据通路			汇总
			S 盒	S 盒逆	其它数据通路	
TI(3,3)分享前的综合结果	191	150	15	27	464	847
TI(3,3)分享后的综合结果	195	151	193	217	1399	2155

为了评估本文所提方案的功率消耗,我们采用 100kHz 的时钟频率,基于 PrimeTime PX C-2009.06 和 Chartered 0.18μm(1.8V)工艺估计了本文提出的安全方案的功耗,其功耗信息以及与均采用 0.18μm 工艺的其它文献实现方案的比较结果如表 5 所示.为了便于比较加入锁存器前后的结果,表中也列出了本文提出的安全方案在加入锁存器之前的结果,可以看出在加入锁存器后,虽然总面积有所增加,然而功耗却并没有增加,而是从 2.75μA 降低到 2.60μA,这主要是因为毛刺的减少降低了功耗.

综上所述,无论从面积还是从功耗上,本文所提方案相对于文献[14]都具有一定优势,而且能够应对潜在的毛刺威胁,表明所提出的实现方案适用于低成本 RFID 标签芯片的应用需求,为 RFID 标签芯片的安全化提供了一种可行的解决方案.

表 5 本文提出的安全实现方案与相关文献的比较结果

参考文献	面积(GE)	功耗@100KHz(μA)	毛刺隐患
文献[15]	6929	-	-
文献[14]	2282	3.20	有
本文方案(未加锁存器)	2059	2.75	有
本文方案(加入锁存器)	2155	2.60	无

"-"为没有明确给出或暂不明确

5 安全性评测及结果

5.1 实验配置

SASEBO(Side-channel Attack Standard Evaluation BOard)系列板是用于评测抗侧信道攻击能力的基准平台,由日本 AIST 信息安全研究中心开发.本文分别将前

文的两种实现方式分别实现于 SASEBO-G[22]电路板上,并搭建了如图 7 所示的功耗采集平台,其中,PC 机采用目前主流计算机,PC 机与 SASEBO-G 通过 RS-232 相连,并通过 GPIB 适配器控制示波器的行为.示波器的通道 2 采用普通单端探头用于接收 SASEBO-G 板上的触发信号,通道 1 采用差分探头用于探测 SASEBO-G 板上密码 FPGA 芯片的电流变化.由于图 6 中控制 FPGA 和密码 FPGA 之间需要有一定握手机制,因此在将密码算法实现于密码 FPGA 时,需要对实现稍作调整,需要说明的是,这些调整不会影响我们的评测结果.

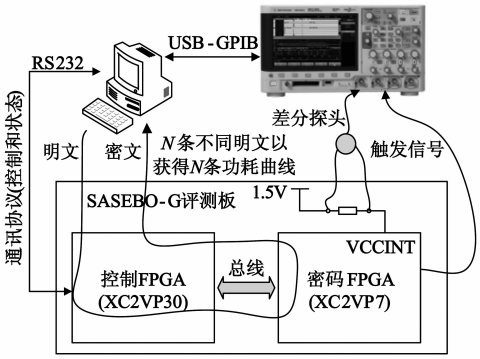


图7　功耗采集平台硬件原理图

实验中,最小 SoC 系统运行于 24MHz, *Piccolo* 密码算法运行于 4MHz,波特率设定为 115200;示波器采样率为 1GSa/s,由于触发信号保证了每次 *Piccolo* 加密时示波器采集的数据都能准确对齐,为了降低测量噪声,将示波器设置为 20 次平均采样模式,即每组明文重复执行加密过程 20 次,由示波器将 20 次采集到的数据自动平均.

5.2　加入防护前后的串行方案的 DPA 安全性对比分析

密码算法的串行化实现具有较小的实现面积,消耗更少的功耗,因此串行化实现是密码算法轻量级实现的最重要措施.串行化实现相对 DPA 攻击方面的安全性可以从两个方面进行分析:(1)串行化实现时,较低的密码电路功耗会降低所采集功耗信息的信噪比(Signal Noise Ratio, SNR),因此,单从这个方面来讲串行化实现能够增加 DPA 攻击的难度;(2)串行化实现的数据通路宽度较低,算法噪声被降到了较低限度,而且串行化实现更容易使攻击者基于分而治之的思想逐个攻击密钥段[14],因此,串行化实现又使 DPA 攻击的难度有所降低.

文中采用成功实施攻击所需的功耗曲线样本数量(MTD, Measurements To Disclosure)来评估 *Piccolo* 密码算法上述两种实现方式抗 DPA 攻击的能力及安全性[14].下文以针对首轮的明文攻击方式并以首轮密钥的第 2 个 Nibble 为攻击密钥段(下文简称 RK_2,其实际值为 2)并进行阐释,显然 RK_2 共有 16 个可能的密钥值.实验中,首先采用适量样本(保证能够成功攻击未加防护的电路)寻找实现方式一的密钥泄露点(攻击兴趣点),之后,在攻击兴趣点附近,通过不断变换攻击样本数量,针对加入防护前后的电路,重复实施 DPA 攻击,可以得出相关系数与样本数量的关系图,从中得出 MTD 并由此判断电路的防护能力.图 8 给出了基于汉明距离模型的攻击结果,从图 8(*a*)可以看出,随着功耗曲线样本数量的增加,正确密钥与功耗曲线的相关性相对其它密钥区别不断加大,大约 200 个样本即可成功破解 RK_2.从图 8(*b*)我们可以发现:(1)在相同的样本数量(如 10000 条功耗曲线)的前提下,所有可能密钥的相关系数取值范围远小于实现方案 1 的;(2)随着功耗曲线数量的增加,正确密钥的猜测值并没有从其它密钥值所处于的相关系数区间中游离出来,这说明 100000 条功耗曲线范围内无法应用 DPA 攻击获取 RK_2 的真实密钥值.

事实上,基于汉明重量模型的攻击我们也得到了类似的结论,限于篇幅,在此不再赘述.综上所述,本文所提出的的安全化密码算法实现方案不仅满足了实现面积轻型的要求,而且还提供了相当程度的 DPA 攻击安全性,能够运用于大部分对功耗和安全性有相当要求的场合(例如 RFID 标签芯片).

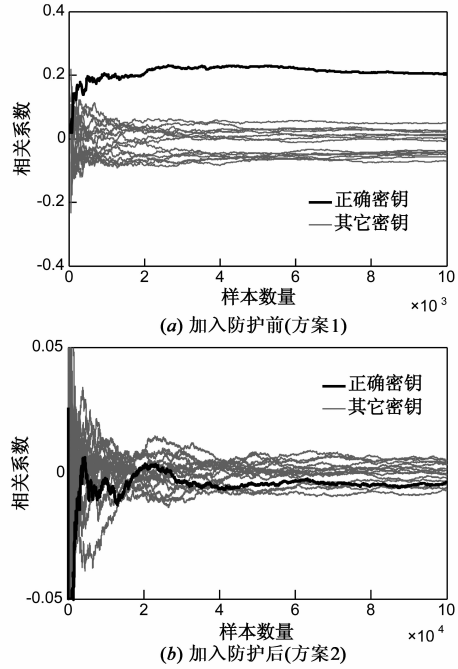


图8　在攻击兴趣点上RK_2相关系数与功耗样本数量的关系

6　结论

密码算法在低成本 RFID 标签芯片中面临面积和

DPA 安全性双重尴尬,本文基于 *Piccolo* 密码算法和新型 DPA 防护措施提出了一种适用于无源 RFID 标签芯片的安全化密码算法实现方案.为了能够将 Threshold 掩码方案应用于 *Piccolo* 密码算法的串行化实现之上,我们分别采用布尔式重组和改进型穷举搜索算法完成了 S 盒和 S 盒逆的面积最优的二次分解,在此基础上进行拆分形成 TI(3,3)分享并提出基于锁存器的解决方案用以解决 TI(3,3)分享后潜在的毛刺威胁问题,最终完成了能够抵御 DPA 攻击的 *Piccolo* 密码算法的完整 TI(3,3)分享型串行化实现.针对该实现,我们分别采用 DC 和 PTPX 基于 Chartered 0.18μm 工艺和 100kHz 的 RFID 运行频率进行综合和功耗估计,结果表明所提议的方案仅仅占用 2155GE,平均电流约为 2.60μA,从面积和电流上相对于已知参考文献都具有一定优势;基于 SASEBO-G 平台在实测功耗数据的情况下对该实现的 DPA 攻击结果表明该方案在保证了密码算法实现轻型的同时也满足了实现安全的要求.

参考文献

[1] Juels A, Weis S A. Authenticating pervasive devices with human protocols[A]. 2005 25th Annual International Cryptology Conference Proceedings[C]. Berlin: Springer, 2005. 293 – 308.

[2] Bogdanov A, Knudsen L R, Leander G, et al. PRESENT: An ultra-lightweight block cipher[A]. 2007 9th International Workshop on Cryptographic Hardware and Embedded Systems Proceedings[C]. Berlin: Springer, 2007. 450 – 466.

[3] Shibutani K, Isobe T, Hiwatari H, et al. Piccolo: an ultra-lightweight blockcipher[A]. 2011 13th International Workshop on Cryptographic Hardware and Embedded Systems Proceedings[C]. Berlin: Springer, 2011. 342 – 357.

[4] Guo J, Peyrin T, Poschmann A, et al. The LED block cipher [A]. 2011 13th International Workshop on Cryptographic Hardware and Embedded Systems Proceedings[C]. Berlin: Springer, 2011. 326 – 341.

[5] Kocher P, Jaffe J, Jun B. Differential power analysis[A]. 1999 19th Annual International Cryptology Conference Proceedings [C]. Berlin: Springer, 1999. 388 – 397.

[6] Brier E, Clavier C, Olivier F. Correlation power analysis with a leakage model[A]. Joye M. 2004 6th International Workshop on Cryptographic Hardware and Embedded Systems Proceedings [C]. Berlin: Springer, 2004. 16 – 29.

[7] Breier J, Kleja M. On practical results of the differential power analysis[J]. Journal of Electrical Engineering, 2012, 63(2): 125 – 129.

[8] 李翔宇,孙义和.采用数据流模式提高乱序执行密码芯片的安全性[J].电子学报,2007,35(2):202 – 206.
Li Xiang-yu, Sun Yi-he. Improve the security of random executing encryption ICs by the data flow mode[J]. Acta Electronica Sinica, 2007, 35(2): 202 – 206. (in Chinese)

[9] Canright D, Batina L. A very compact "perfectly masked" S-box for AES[A]. 2008 6th International Conference on Applied Cryptography and Network Security Proceedings[C]. Berlin: Springer, 2008. 446 – 459.

[10] 乐大珩,张民选,李少青,等.一种新型的抗 DPA 攻击可配置逻辑结构[J].电子学报,2011,39(2):453 – 457.
Yue Da-heng, Zhang Min-xuan, Li Shao-qing, et al. A novel DPA-resistance configurable logic[J]. Acta Electronica Sinica, 2011, 39(2): 453 – 457. (in Chinese)

[11] Coron J S. A new DPA countermeasure based on permutation tables[A]. Ostrovsky R. 2008 6th International Conference on Security and Cryptography for Networks Proceedings[C]. Berlin: Springer, 2008. 278 – 292.

[12] 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.
Wang Peng-jun, Hao Li-peng, Zhang Yue-jun. Design of AES subbyte module of anti-zero value power attack and its VLSI implementation[J]. Acta Electronica Sinica, 2012, 40(11): 2183 – 2187. (in Chinese)

[13] Moradi A, Poschmann A. Lightweight cryptography and DPA countermeasures: a survey[A]. Financial Cryptography 2010 Workshops Proceedings[C]. Berlin: Springer, 2010. 68 – 79.

[14] Poschmann A, Moradi A, Khoo K, et al. Side-channel resistant crypto for less than 2, 300 GE[J]. Journal of Cryptology, 2011, 24(2): 322 – 345.

[15] Karpinskyy. Masked encryption algorithm mCrypton for resource-constrained devices[A]. 2007 IEEE 4th International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technolgy and Applications Proceedings [C]. NewYork: IEEE, 2007. 628 – 633.

[16] Nikova S, Rijmen V and Schläffer M. Secure hardware implementation of non-linear functions in the presence of glitches [A]. 2008 11th International Conference on Information Security and Cryptology Proceedings [C]. Berlin: Springer, 2009. 218 – 234.

[17] Nikova S, Rechberger C, Rijmen V. Threshold implementations against side-channel attacks and glitchs[A]. 2006 8th International Conference on Information and Communications Security Proceedings[C]. Berlin: Springer, 2006. 529 – 545.

[18] Moradi A, Poschmann A, Ling S, et al. Pushing the limits: a very compact and a threshold implementation of AES[A]. 2011 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques Proceedings (EUROCRYPT 2011)[C]. Berlin: Springer, 2011. 69 – 88.

[19] Mangard S, Pramstaller N, Oswald E. Successfully attacking masked AES hardware implementations[A]. 2005 7th Interna-

tional Workshop on Cryptographic Hardware and Embedded Systems Proceedings[C]. Berlin: Springer, 2005. 157 – 171.

[20] Mangard S, Popp T, Gammel B M. Side-channel leakage of masked CMOS gates[A]. The Cryptographers' Track at the RSA Conference 2005 Proceedings[C]. Berlin: Springer, 2005. 351 – 365.

[21] Chari S, Jutla C S, Rao J R, et al. Towards sound approaches to counteract power-analysis attacks[A]. 1999 19th Annual International Cryptology Conference Proceedings[C]. Berlin: Springer, 1999. 398 – 412.

[22] AIST of Japan. SASEBO-Gspecification[J/OL]. http://www.risec.aist.go.jp/project/sasebo, 2012-06-20.

作者简介

王晨旭　男, 1977 年 10 月出生, 河南淮阳人. 毕业于哈尔滨工业大学, 工学博士, 现为哈尔滨工业大学(威海)信息与电气工程学院讲师. 研究方向为芯片安全与嵌入式系统.

E-mail: wangchenxu@hit.edu.cn

韩　良(通信作者)　男, 1969 年 8 月出生, 吉林榆树人. 毕业于哈尔滨工业大学, 工学博士, 现为哈尔滨工业大学(威海)信息与电气工程学院副教授. 研究方向为超大规模集成电路设计.

E-mail: express@hit.edu.cn