基于 FPGA 实现的 DES 抗能量攻击设计研究

温圣军,张鲁国
WEN Sheng-jun,ZHANG Lu-guo

解放军信息工程大学 电子技术学院,郑州 450004
Institute of Electronic Technology,the PLA Information Engineering University,Zhengzhou 450004,China

WEN Sheng-jun,ZHANG Lu-guo.Design and research of DES against power analysis attacks based on FPGA.Computer Engineering and Applications,2010,46(6):98-99.

Abstract: Aimed at the DES design method against power analysis attacks mentioned in reference [1],an improved one is proposed.Compared with the method of reference [1],it has the same ability against the power analysis attacks.By analyzing the improved algorithm in theory,it is applicable for this method to make use of in the process of most of cipher algorithm's design and implementation against power analysis attacks.The improved algorithm,while implemented based on FPGA,can not only save about eighty percent hardware storage resources,but also keep the operation rate in the same time.

Key words: Triple Digital Encryption Standard(TDES);power analysis attack;logic resource;applicability

摘 要:针对文献[1]中提出的 DES 算法抗能量攻击设计方法,给出了对此方法的改进。改进后的设计方法与原方法相比,具有相同的能量攻击抵御能力。对改进算法的理论分析表明,此方法可适用于大多数分组密码算法的抗能量攻击设计,且相对于文献[1]中的方法,当基于 FPGA 具体实现时,改进算法可以在保持原有运行速度不变的情况下,节省约 80%的硬件存储资源消耗。

关键词:三重数字加密标准算法(TDES);能量攻击;逻辑资源;适用性
DOI:10.3778/j.issn.1002-8331.2010.06.028 **文章编号:**1002-8331(2010)06-0098-02 **文献标识码:**A **中图分类号:**TP393

能量攻击是由 Kocher 等人于 1998 提出,专门针对密码算法在实际使用过程中的一种攻击方法,其攻击原理依赖于密码算法在执行过程中,消耗能量与密钥的相关性。尽管与密码分析方法相比,能量攻击只能够针对一种特定的密码算法进行攻击,但对于应用于不同平台的密码系统,能量攻击往往具有更大的安全威胁。

在目前已经提出的众多能量攻击防护方法中,Boolean 掩盖法是一种有效的防护设计方法,被广泛应用于 DES 及 AES 的具体实现中。最近有文献指出,能量攻击同样可以适用于基于 FPGA 实现的密码算法,对 FPGA 实施能量攻击主要基于以下两条:首先,可以将 FPGA 中的能量消耗归结为存储器/寄存器中的比特跳变数;第二,存储器比特跳变数与片内秘密信息相关。文献[1]给出了基于 FPGA 实现的 DES 及 TDES 抗能量攻击的一种设计方法,是一种标准的 Boolean 掩盖法。

1 基于 FPGA 实现的 DES 能量攻击原理

1.1 基于 FPGA 的能量攻击原理

在对设计信息以及 FPGA 执行所知很少(而实际上大多数的信息是可得的)的情况下,以商用 FPGA 在晶体管级的行为为准。最普遍的可编程逻辑技术是静态 RAM,其存储单元、逻辑块以及块间联系都使用 CMOS 门构造。对这些电路,能量主要消耗来自动态能量消耗,即对一个单一的 CMOS 门而言,可以作如下表示:

$$P_D=C_L V_{DD}^2 P_{0\text{-}1} F$$

其中,C_L 是门负载能力,V_{DD} 是电压,$P_{0\text{-}1}$ 是 0 到 1 输出变换的概率,F 为时钟。等式表明 CMOS 电路的能量消耗是与数据相关的。文献[1]指出:能量消耗依赖于寄存器值跳变的次数。因而,可以基于下述假设来进行 FPGA 能量攻击:时间 T 的能量消耗由在该时间器件内部寄存器跳变的个数决定。首先作一个定义:一个寄存器是满的,如果其跳变泄露秘密信息,否则寄存器是空的[1]。显然一个输入寄存或者一个输出寄存是空的,因为它们只包括明文或者密文。在 DES 算法中,对于初始密钥加,由 $result=input \oplus key$,假设结果存储于 R,两个连续输入为 $input1$、$input2$,则寄存器能量消耗为 $H(input1 \oplus input2)$,寄存器为空的。事实上,线性变换后的寄存器一直是空的,只有经过非线性 S 盒,寄存器才能与密钥有关。因此,能量消耗依赖于 $H(sbox(input1 \oplus key)+sbox(input2 \oplus key))$。对能量攻击的防护设计,主要设计重点也在于非线性变换环节。

1.2 文献[1]中 DES 抗能量攻击算法设计

采用 Boolean 掩盖法,将 DES 处理过程中的所有中间值进行置乱,其关键是 S 盒。在文献[1]中,作者基于以下几条定理对 DES 进行了重新设计:

基金项目:现代通信国家重点实验室基金资助资目(No.9140C1106030806)。
作者简介:温圣军(1983-),男,硕士研究生,研究方向:密码学与密码工程;张鲁国(1963-),男,副教授,硕士生导师,研究方向:嵌入式信息安全系统与密码工程。
收稿日期:2008-09-12 **修回日期:**2008-11-07

定理 1 Let $P:GF(2)^n \rightarrow GF(2)^n$ be a bit permutation and b, b_1, b_2 be three Boolean vectors $\in GF(2)^n$, such that $b=b_1 \oplus b_2$。Then, we have: $P(b)=P(b_1) \oplus P(b_2)$。

定理 2 Let b, b_1, b_2, a, a_1, a_2 be six Boolean vectors $\in GF(2)^n$ such that $b=b_1 \oplus b_2$ and $a=a_1 \oplus a_2$, Then, we have: $a \oplus b=(a_1 \oplus a_2) \oplus (b_1 \oplus b_2)=(a_1 \oplus b_1) \oplus (a_2 \oplus b_2)$。

定理 3 Let $S:GF(2)^n \rightarrow GF(2)^m$ be *a S-box* and b, b_1, b_2 be three bitvectors $\in GF(2)^n$ such that $b=b_1 \oplus b_2$。Then，存在 *a S-box* $S:GF(2)^n \rightarrow GF(2)^m$ such that: $S(b)=S(b_1) \oplus S'(b_1, b_2)$。

利用定理 3，修改 DES 原 *S* 盒，可以实现对 DES 中间值的整体掩盖。其实现框图如图 1、2 所示。

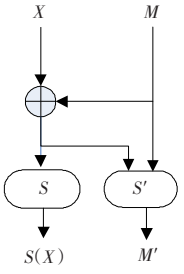

图 1　掩盖后 *S* 盒

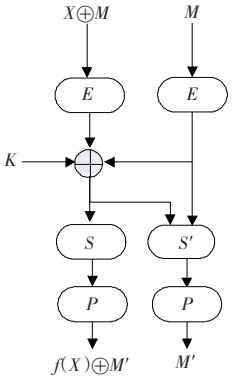

图 2　掩盖后非线性函数 *f*

2　对文献[1]方法的改进

在文献[1]中，为实现 DES 的 *S* 盒掩盖，需要对原本的 S 盒，结合一个的 12 bit 到 4 bit 转换的 *S′* 来实现。显然，要完成整个 DES 中 *S* 盒的掩盖，需要增加的存储区为 $2^{12} \times 4$ bit，约为 16 Kbit。这仅仅是对 DES 的 *S* 盒，若对 AES 的 *S* 盒按此方法进行掩盖设计，需要增加的存储区将是巨大的。针对文献[1]中方法的这一缺点，通过分析对 FPGA 的能量攻击原理，提出了对 DES 算法抗能量攻击的改进设计方案，使得需要增加的存储区只需原算法中 *S* 盒所需的存储区大小即可。具体的算法改进描述如下：

FPGA 能量攻击的原理在于，片内存储区数值跳变个数不同可以反映为能量消耗差异，Boolean 掩盖法的目的就在于将内部存储区中数值进行随机化，使得能量消耗差异与实际的内部敏感信息无关，从而实现对能量攻击的防护。同理，如果对于任意的两个输入，内部存储器数值跳变的个数是恒值，这样能量消耗就没有差异性，也可以实现对能量攻击的防护。提出的改进方案是在线性变换时采用 Boolean 掩盖法，使得能量消耗差异与实际存储器数据无关，而在 *S* 盒变换时，使得任意的两个输入，在经过新的 *S* 盒后，存储区内部跳变值为恒值，然后在出 *S* 盒后再进行掩盖，通过这样的结合来共同实现对能量攻击的防护设计。以 DES 的第一个 *S* 盒为例，来说明新 *S* 盒的设计规则如表 1，表 2。

按照 $\bar{S}1$ 的构造方法，可以得到整个 $\bar{S}$ 盒，将得到的 $\bar{S}$ 与原 *S* 盒联合使用，就组成了新的 *S* 盒。因此，只需要对单一的 *S*1 盒进行详细分析，就可知整个新 *S* 盒的抗能量攻击设计思想。图 3 为新 *S* 盒结构图，图 4 为掩盖后新的非线性函数 *f*。为叙述方便，新 *S*1 盒记为 *S*1′，新 *S* 盒记为 *S′*。

表 1　DES 算法 *S*1-盒对照表

行	列															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

表 2　DES 算法 *S*1-盒按位取补对照表 $\bar{S}1$

行	列															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	11	2	14	13	0	4	7	12	5	9	3	10	6	15	8
1	15	0	8	11	1	13	2	14	5	9	3	4	6	10	12	7
2	11	14	1	7	2	9	13	4	0	3	6	8	12	5	10	15
3	0	3	7	13	11	6	14	8	10	4	12	1	5	15	9	2

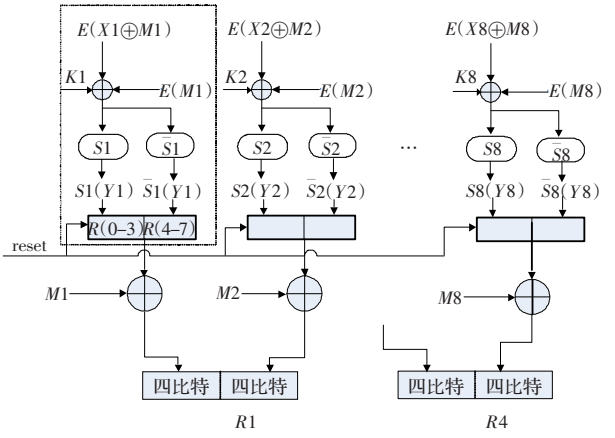

图 3　新 *S* 盒结构图

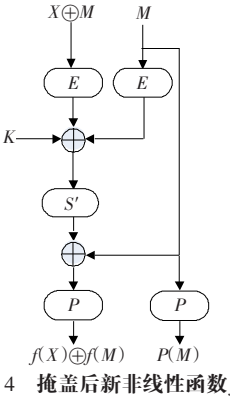

图 4　掩盖后新非线性函数 *f*

图 3 中的虚线框内部分即为新构造 *S*1′结构图。以一次 DES 数据加密的能量变化检测为例，对 *S*1′的具体运算过程进行分析。一次能量检测需要以同一密钥进行两组明文的加密操作，1.2 节的定理 1 及定理 2 保证了线性变换不会对能量攻击提供帮助，因此，可以直接假设 *S*1′的两次输入：分别记为 *Z*1=*Input*1⊕*key*1、*Z*2=*Input*2⊕*key*1。*Z*1 进入 *S*1′后，同时经 *S*1 盒与 $\bar{S}1$ 盒得到两个四比特输出，作为 *R* 的两个四比特进行寄存。由图 3 可知，前四比特为正确的 *S*1 盒输出，后四比特为冗余输出。得到输出后，将 *R* 的前四比特与掩盖值 *M* 的前四比特进行异或掩盖，作为 *P* 盒输入的前四比特寄存在 *R*1 中，在完成这些步骤后，最后将 *R* 作清零处理。*Z*2 处理过程与 *Z*1 完全相同。分析处理过程中的能量消耗变化，对于 *R*1，由于寄存数据已经被掩盖，寄存器为空，因而能量消耗变化依赖于寄存器 *R*。根据

（下转 111 页）