基于汉明重的 PRESENT 密码代数旁路攻击

吴克辉 王 韬 赵新杰 刘会英
(军械工程学院计算机工程系 石家庄 050003)

摘 要 研究了分组密码代数旁路攻击原理及模型、非线性布尔方程组转化为 SAT 问题的方法,提出了一种基于汉明重的 PRESENT 密码代数旁路攻击方法,降低了求解非线性多元方程组的复杂度,减少了旁路攻击所需样本量,并通过实验对理论正确性进行了验证。结果表明,在已知明文条件下,利用一个样本前 3 轮的 S 盒输入、输出汉明重在 0.63s内即可恢复 80bit PRESENT 完整密钥;在未知明密文和 S 盒输入、输出汉明重随机选取条件下,也可恢复 PRESENT 完整密钥。

关键词 代数旁路攻击,代数攻击,旁路攻击,汉明重,PRESENT
中图法分类号 TP393 **文献标识码** A

Hamming Weight-based Algebraic Side-channel Attack against PRESENT

WU Ke-hui WANG Tao ZHAO Xin-jie LIU Hui-ying
(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract This paper examined the theory and model of algebraic side-channel attack against block ciphers, the method of converting non-linear boolean equation system to SAT problem, proposed a method of Hamming weight based algebraic side-channel cryptanalysis against PRESENT, reduced the complexity of solving non-linear boolean equation system and the sample size of side-channel attack, finally testified the validity of theory through experiments. Results show that if knowing one sample of plaintext, it can recover 80 bit keys of PRESENT with Hamming weights of S-box inputs and outputs of front 10 round in 0.63 seconds; if plaintext and cipher are unknow or the used Hamming weights of S-box input are random, it can also make a success of recovering complete PRESENT key.

Keywords Algebraic side-channel attack, Algebraic attacks, Side-channel attack, Hamming weight, PRESENT

1 引言

密码算法的安全性可从算法设计安全性和实现物理安全性这两个方面考虑,前者主要使用线性攻击、差分攻击、代数攻击等数学分析方法进行评估,后者主要使用旁路攻击、故障攻击等方法进行评估。代数攻击主要通过研究密码算法的代数结构,建立关于明密文、加密中间状态与密钥的代数方程组,求解方程组恢复密钥。由于在有限域上求解多元非线性方程组是一个 NP 完全问题[1],求解方程组的复杂度以指数级递增,使得在有限的时间、空间内实现方程组的完全求解比较困难,因此限制了代数攻击应用的实效性,对分组密码安全威胁较小。旁路攻击将密码实现看作一个在硬件平台上运行加解密程序的物理过程,通过采集加解密程序在实现过程中泄露的时间、功耗、电磁、声音等物理效应信息,利用差分分析、模板分析、相关性分析等方法来破解密钥。然而由于旁路攻击受设备与环境影响较大、噪声与攻击所需样本量大,一般只局限于分析分组密码第一轮或最后一轮,在一定程度上影响了其在实际攻击中的应用。

代数旁路攻击的出现,突破了代数攻击领域求解非线性多元方程组的瓶颈,弥补了传统旁路攻击样本量大、分析轮数少、旁路信息利用率低的缺陷,降低了求解方程组的复杂度和旁路攻击的样本量,甚至可在一条功耗曲线、未知明密文条件下成功获取加密密钥。目前,已有的代数旁路攻击仅限于功耗攻击和代数攻击的结合。文献[2,3]研究了基于碰撞的代数旁路攻击,文献[4]提出了具有容错功能的代数旁路分析方法。在对分组密码的代数旁路攻击方面,尚未发现国内公开发表的文献。

随着 RFID(射频识别)技术的发展,RFID 系统信息安全的重要性日益突出,对在 RFID 标签上使用的轻型分组密码的安全性提出了更高的要求。PRESENT 是由 A. Bogdanov 等人[5]于 2007 年提出的一种超轻量级分组密码算法,在 0.18μm工艺下仅需的逻辑单元为 1570GE,良好的硬件实现效率非常适合在 RFID 标签、传感器网络等资源受限环境中使用。本文针对 PRESENT 密码,基于汉明重模型,将功耗攻击与代数攻击结合,利用旁路攻击技术采集 PRESENT 运行时泄露的功耗信息并转化为 S 盒输入、输出汉明重,结合密码算法代数特性建立关于明密文、S 盒输入、输出变量与密钥的代数方程组,将其转化为 SAT 问题并利用 MiniSAT2.0 软件

到稿日期:2011-01-17 返修日期:2011-04-23 本文受国家自然科学基金(60772082),河北省自然科学基金(08M010)资助。
吴克辉(1986-),男,硕士生,主要研究方向为分组密码代数旁路攻击,E-mail:our616@163.com;王 韬(1964-),男,教授,博士生导师,主要研究方向为信息安全、密码学;赵新杰(1986-),男,博士生,主要研究方向为分组密码旁路分析和故障分析;刘会英(1984-),男,博士生,主要研究方向为图像加密和密码旁路分析。

求解。实验结果表明，PRESENT 易遭受基于汉明重的代数旁路攻击的威胁，在已知明密文、未知明密文或者汉明重随机选取条件下，均可成功恢复 PRESENT 80bit 完整密钥。

本文第 2 节概述分组密码代数旁路攻击原理及模型；第 3 节介绍 PRESENT 密码算法、PRESENT 代数方程组建立方法、代数方程组转化为 SAT 问题的方法，以及基于汉明重的代数旁路攻击分析方法和实验结果分析比较；最后为结束语。

2 分组密码代数旁路攻击原理及模型

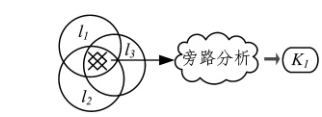
密码系统的安全性都基于一个事实，即求解一个有限域 $GF(q)$ 上的系数任意选取的非线性多元方程组是 NP-hard 问题。随着 XL[6,7]、Grobner 基[8]等方程组求解方法的出现，代数攻击的研究对象开始转向 AES、Serpent 等分组密码，由于求解代数方程组的复杂度极高，目前对于分组密码的代数攻击一般只限于低轮数。

代数旁路攻击在代数攻击的基础上，利用旁路攻击技术采集密码加解密程序在运行过程中泄露的物理效应信息，将其转化为关于中间状态变量的代数方程，联合密码代数方程组求解以获取密钥。如式(1)、式(2)所示，相比于代数攻击，代数旁路攻击将获取的中间状态信息转化为更多的代数方程 $f_{\text{Side-Channel}}(s_j, h_j, m_j, \cdots)=0$，从而能够更快速、高效地求解方程组；中间状态信息可以是查 S 盒索引值 s_j，S 盒输入、输出汉明重 h_j，也可以是碰撞信息 m_j 等和密钥 k_i 密切相关的旁路信息。

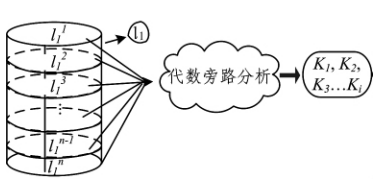
$$G_{\substack{\text{algebraic}\\ \text{attack}}}\begin{cases} f_1(p_i, c_i, k_i)=0 \\ f_2(p_i, c_i, k_i)=0 \\ \cdots\cdots \\ f_m(p_i, c_i, k_i)=0 \end{cases} \tag{1}$$

$$G_{\substack{\text{algebraic}\\ \text{Side-Channel}\\ \text{attack}}}\begin{cases} f_1(p_i, c_i, k_i)=0 \\ \cdots\cdots \\ f_m(p_i, c_i, k_i)=0 \\ f_{\text{Side-Channel}}(s_j, h_j, m_j, \cdots)=0 \end{cases} \tag{2}$$

旁路攻击主要利用密码算法执行过程中泄露的旁路信息进行密钥分析。受计算能力和资源的限制，密码算法在密钥使用时总是分割为若干个子密钥块，按照一定顺序加密。由于不同子密钥块的旁路信息都是可测的，通过统计和分析大量样本(一般是第一轮或最后一轮)中每个子密钥块对应的旁路信息，可交叉缩小每个子密钥块的穷举范围，直至锁定正确子密钥块，如图 1(a)所示，曲线 l_1，l_2，l_3 表示 3 个样本分别恢复的子密钥块 K_1 的候选值集合，正确的候选值为 3 个样本的交集。在真实情况下，常需要上百甚至上万个样本方可恢复正确 K_1 值。



(a) 旁路攻击原理



(b) 代数旁路攻击原理

图 1

与旁路攻击不同，代数旁路攻击将加密过程描述为关于明密文、中间状态与密钥的代数方程组，深入密码算法的每一轮分析未知变元的相互作用。如图 1(b)所示，曲线 $l_1^1, l_1^2, \cdots, l_1^n$ 表示一个样本 l_1 条件下，与完整密钥 $K_1, K_2, \cdots, K_n$ 相关的密码算法每一轮的功耗(或电磁、时间等)曲线。总的来说，代数旁路攻击具有以下特性：

(1)能够挖掘、利用密码设备泄露的全轮的物理效应信息；

(2)在理想情况下，利用一个样本(一条功耗、电磁、时间曲线等)即可恢复全部密钥；

(3)在未知明密文的条件下，也可成功；

(4)理论上，能够与多种旁路信息模型结合。

分组密码代数旁路攻击主要包括建立密码算法的代数方程组、采集旁路信息、求解方程组 3 个步骤。建立密码算法代数方程组的方法，包括以密码算法中间状态比特块为未知变量建立方程组的方法[6]、以密码算法中间状态比特位为未知变量建立方程组的方法[9]。本文以中间状态比特位为未知变量，研究 PRESENT 密码的多元二次代数方程组，详见 3.2 节。

求解多元非线性方程组的方法主要包括线性化方法(直接线性化 XL[6,7]、扩展线性化 XSL[10])、基于 Grobner 基的方法(F4 算法[8]、F5 算法[11])和转化为可满足性(SAT)问题利用 SAT 解析器求解的方法。本文基于 MiniSAT2.0 软件求解，详见 3.3 节。

3 基于汉明重的 PRESENT 代数旁路攻击

3.1 PRESENT 密码算法

PRESENT[5]分组密码算法采用 SPN 结构，分组长度为 64 位，支持 80 位、128 位两种密钥长度。共迭代 31 轮，每轮轮函数 F 由轮密钥加、S 盒代换、P 置换 3 部分组成。为提高算法安全性，PRESENT 在第 31 轮运算结束后使用 64 位密钥 K_{32} 进行后期白化操作。具体加密流程如图 2 所示。

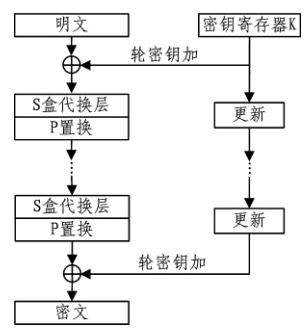


图 2 PRESENT 加密流程图

密钥扩展算法：首先将初始主密钥存储在寄存器 K 中，表示为 $k_{79}k_{78}\cdots k_0$。第 i 轮密钥 K_i 由寄存器 K 的前 64 位组成。当生成第 i 轮密钥 K_i 后，通过以下方法更新密钥寄存器 K：

$$[k_{79}k_{78}\cdots k_1k_0]=[k_{18}k_{17}\cdots k_{20}k_{19}]$$

$$[k_{79}k_{78}k_{77}k_{76}]=S[k_{79}k_{78}k_{77}k_{76}]$$

$$[k_{19}k_{18}k_{17}k_{16}k_{15}]=[k_{19}k_{18}k_{17}k_{16}k_{15}]\oplus \text{round\_counter}$$

式中，round_counter 为当前的加密轮数。易见，只需分析出第一轮的 64 位轮密钥 K_1，即可将 80 位 PRESENT 的主密钥搜索空间降低到 2^{16}。

3.2 建立 PRESENT 代数方程组

对一切密码系统的代数攻击都可以归结于建立和求解有

限域 $GF(q)$ 上系数任意选取的非线性多元方程组，而建立分组密码的超定、稀疏代数方程组一直是代数攻击领域研究的难点。关于 PRESENT 密码，设计者[5]证明了可以用 4216 个未知变元和 11067 个高次布尔方程来表示，S 盒可以用 21 个 8 元高次布尔方程表示。文献[13]去除冗余方程后，用 14 个 8 元高次布尔等效方程表示 PRESENT 的 S 盒。本文深入挖掘文献[9]中基于高斯消元法建立分组密码代数方程组的方法，扩展至 PRESENT 分组密码，用 9 个极端稀疏的 8 元二次布尔方程（MQ 方程）表示 PRESENT 的 S 盒，用大约 8000 个未知变元、20000 个 MQ 方程表示 32 轮 PRESENT 加密。其中 8000 个未知变元包括 4 种不同类型（$0\leqslant i\leqslant 63$）：

（1）X_i 表示每轮加密过程中查 S 盒的输入比特；

（2）Y_i 表示每轮加密过程中查 S 盒的输出比特；

（3）P_i 表示每轮加密过程中轮密钥加的输入比特；

（4）U_i 表示每轮加密过程中的轮密钥比特。

这样，用变元 P_i、K_i 与 U_i 表示轮密钥加变换，用变元 X_i、Y_i 表示 S 盒代换，用变元 Y_i 与 P_i 表示 P 置换。S 盒代换是 PRESENT 密码唯一的非线性变换，其代数方程共有 25 个单项式、9 个方程，方程最高次数为 2，极少的单项式、方程个数和极低的方程次数极大地降低了求解方程组的复杂度。此外，如考虑到轮密钥间的变换，每轮还将增加大约 200 个 MQ 方程。

3.3 代数方程组转化为 SAT 问题

SAT[14]是以 CNF（合取范式）语句为基础的异或逻辑表达形式，代数方程组转化为 SAT 问题，主要包括线性化方程组、线性方程组转化为 CNF 两个步骤。

（1）线性化方程组

对非线性多元方程组中出现的每一个次数 $d>1$ 的高次单项式，引入 1 个变元和 $d+1$ 个 CNF 子句，子句的总长度为 $3d+1$，并以变元代替高次方程组中相应的高次单项式。另外，CNF 中不包括常数项，需要引进一个变元代替常数 1，同时新增 1 个长度为 1 的子句。这样，非线性方程组转化为关于未知变元和常数变元的线性方程组。

（2）线性方程组转化为 CNF

当线性方程的单项式数量为 l 时，转化为：

$$\binom{l}{1}+\binom{l}{3}+\binom{l}{5}+\cdots+\binom{l}{j}=2^{l-1}\ (j=2\lfloor l/2\rfloor)$$

个 CNF 子句的相互合取，每个子句是 l 个变元分别取 m（m 为少于等于 l 的所有奇数）个否定变元的相互析取。当 l 较大时，转化为 CNF 子句的数量以指数级递增，会给 SAT 求解器的运算造成极大的困难，所以需要把长的方程分割成许多短的方程，每个短方程的单项式数量 n 可以为 3、4、5 或者更长，同时引进 $\lceil n/2\rceil-2\ (n>2)$ 个变元。

综上，对于一个非线性多元布尔方程组，假设原始单项式个数为 m_{mon}，方程个数为 m_{equ}，各个方程的单项式平均数量为 m_{term}，单项式平均次数为 d，则按照上述方法转化为 CNF 后，变元总数：

$$n_{\mathrm{mon}}+n_{\mathrm{equ}}\cdot(\lceil n_{\mathrm{term}}/2\rceil-2)$$

CNF 子句总数：

$$n_{\mathrm{mon}}\cdot(d+1)+n_{\mathrm{equ}}\cdot(\lceil n_{\mathrm{term}}/2\rceil-1)\cdot 8$$

CNF 子句总长度：

$$n_{\mathrm{mon}}\cdot(3d+1)+n_{\mathrm{equ}}\cdot(\lceil n_{\mathrm{term}}/2\rceil-1)\cdot 32$$

利用上述方法，将 3.2 节建立的 32 轮 PRESENT 密码代数表达式转化为 CNF，大约共有 240000 个子句，子句总长度大约为 630000，增加了大约 20000 个变元。

3.4 基于汉明重的 PRESENT 代数旁路攻击

电子设备在运行中由于供给能量会消耗功率，当前先进的电子设备，大部分采用超大规模集成电路（VLSI）设计，VLSI 中占统治地位的是数字 CMOS 逻辑电路。当集成电路处理的数据发生变化时，反映在 CMOS 电路上即为状态的变化，导致 CMOS 电路的功率消耗。在 Mangard 等[15]撰写的 DPA 书中指出，由于 NMOS 管和 PMOS 管的导通功率消耗的差异特性，0 到 1 的翻转功耗要稍微大于 1 到 0 的翻转功耗，那么加密操作的功率消耗同原始操作数的汉明重成反比，而同结果操作数的汉明重成正比。因此，功耗曲线与 S 盒输入汉明重密切相关。通过对加密设备功耗曲线的分析能够提炼出 S 盒输入汉明重信息。

早在 2005 年，Agrawal 等[16]提出了两种基于汉明重模型的功耗分析方法：单比特模板攻击和加强的模板差分功耗攻击，并对使用了掩码的 DES 和 AES 算法进行了攻击实验。此后，基于汉明重模型的 DPA、CPA 逐渐成为功耗攻击主流的分析方法。文献[17]表明，在现有的实验条件下，基于模板分析理论，利用旁路攻击技术能够精确地采集密码设备运行过程中泄露的功耗信息，并转化为 S 盒输入、输出汉明重，对轻型分组密码 PRESENT 更为容易。但由于分析方法的局限性，DPA、CPA 一般只利用了第一轮或最后一轮的汉明重信息，却忽略了其他轮的 S 盒输入、输出汉明重对密钥破解的影响。本文提出的代数旁路分析方法，却能很好地解决上述问题，它可以利用 PRESENT 密码加密过程中泄露的每一轮每一次查 S 盒输入的汉明重，深入每一轮分析求解密钥。至于采集功耗信息的技术问题，参考文献[16,17]。本文侧重于分析方法的研究，这里不再赘述。

由 3.1 节可知，以 64 位 PRESENT 为例，31 轮加密中，每一轮查 S 盒 16 次，共查 $16*31=496$ 次 S 盒。假设查 S 盒输入变量值为 $x_1^i,x_2^i,x_3^i,x_4^i\ (1\leqslant i\leqslant 496)$，$H(x)$ 表示查 S 盒输入变量值的汉明重，依据第 2 节代数旁路攻击模型，转化为如下代数方程：

当 $H(x_1^i,x_2^i,x_3^i,x_4^i)=0$ 时，

$$x_1^i=0,x_2^i=0,x_3^i=0,x_4^i=0$$

当 $H(x_1^i,x_2^i,x_3^i,x_4^i)=1$ 或 3 时，

$$x_1^i\oplus x_2^i\oplus x_3^i\oplus x_4^i=1\Leftrightarrow x_1^i\oplus x_2^i\oplus x_3^i\oplus x_4^i\oplus 1=0$$

当 $H(x_1^i,x_2^i,x_3^i,x_4^i)=2$ 时，

$$x_1^i\oplus x_2^i\oplus x_3^i\oplus x_4^i=0$$

当 $H(x_1^i,x_2^i,x_3^i,x_4^i)=4$ 时，

$$x_1^i=1,x_2^i=1,x_3^i=1,x_4^i=1$$

显然，采集到 S 盒输入、输出汉明重越多，在 PRESENT 密码代数方程组的基础上增加的代数方程越多，方程组越容易求解；当采集的 S 盒输入、输出汉明重的数量达到一定程度时，未知明密文条件下也可以成功求解方程组。

3.5 实验结果分析及比较

参考 3.2 节、3.4 节的方法，联立 PRESENT 密码代数方程、泄露的 S 盒输入、输出汉明重转化的代数方程组成 MQ 方程组，再利用 3.3 节的方法转化为 SAT 问题，基于 MiniSAT 2.0 软件在 PC 机（CPU 为 Athlon 64 3000+1.81GHz，内存为 1GB，Windows XP 操作系统）上求解方程组，获取密钥。

图 3 表示在一个样本条件下利用本文提出的分析方法成功获取 80bit 密钥，Minisat2.0 软件求解方程组的时间与汉明重数量的关系，横坐标表示利用 N 轮的汉明重信息。可见，

利用前3轮的S盒输入汉明重在0.63s就可以成功破解PRESENT 80bit密钥;增加S盒输入、输出汉明重信息相当于增加了方程个数,降低了求解方程组的复杂度,延长了求解方程组的时间。文献[13]在3593.6s内实现对3轮PRESENT密码的低轮代数分析,而本文仅在0.63s内实现了对PRESENT密码的3轮代数旁路分析,可以看出S盒输入、输出汉明重的引入对代数方程组复杂度的降低产生了巨大作用,攻击效率较高。

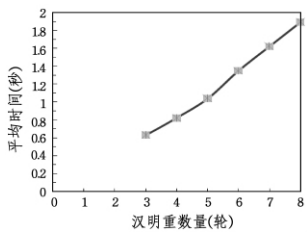


图3　一个样本恢复完整密钥时间

图4表示同一个样本条件下已知、未知明密文对恢复密钥比特个数的影响,纵坐标表示利用N轮S盒输入、输出汉明重恢复的密钥比特个数。可见,未知明密文条件下利用前4轮的S盒输入、输出汉明重即可成功破解密钥,相比已知明密文它需要更多汉明重信息。但与传统旁路攻击[16,17]和代数碰撞攻击[2,3]相比,本文方法的优势不仅在于只需要一个样本即可成功,更在于其在未知明密文条件下的效果良好。

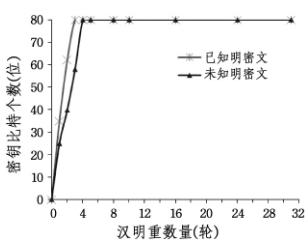


图4　已知、未知明密文条件下恢复密钥比较

考虑到真实攻击环境中噪声过大对采集功耗信息的影响,去噪声化效果不好将导致部分S盒输入、输出汉明重"丢失"[3],从而减少了汉明重信息,增加了求解方程组、破解密钥的难度。设a为功耗信息采集过程中S盒输入、输出汉明重的随机丢失率,图5表示不同样本条件下,随机丢失率a对恢复密钥个数的影响。可以看出,在汉明重随机选取条件下,当随机"丢失"的S盒输入、输出汉明重较多时,可以通过增加样本量,联立更多的方程获取密钥,表明本文方法在实际攻击中的可行性较强。相比代数碰撞攻击[2,3]只能分析密码算法的前2～4轮、碰撞信息采集难度大,本文方法能够深入分组密码算法全轮进行分析,采集旁路信息技术相对成熟[17],更具有广泛性和实用性,对硬件实现的分组密码安全威胁更大。

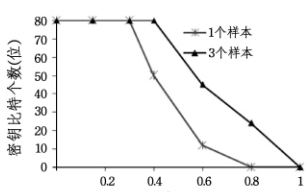


图5　不同样本条件下a对恢复密钥的影响

结束语　本文分析了分组密码代数旁路攻击的原理及模型,研究了建立PRESENT密码MQ代数方程组、非线性布尔方程组转化为SAT问题的方法,提出了一种新的PRESENT密码代数旁路分析方法。仿真实验表明,此类攻击效率高、可行性强,尤其在未知明密文条件下良好的效果将对硬件实现的PRESENT密码产生巨大的威胁。此外,本文方法也对其他分组密码的代数旁路分析提供了思路。

以下几个方面值得将来研究和关注:第一,针对RFID标签,通过物理实验采集PRESENT代数旁路攻击中的S盒输入、输出汉明重信息;第二,开展对SEA、AES、DES等其他分组密码的代数旁路攻击的研究;第三,开展分组密码抗代数旁路攻击技术的研究。

参考文献

[1] Garey M, JollIlson D. Computers and Interactability a guide to the theory of NP-completenss. Freemall:251-260

[2] Bogdanov A. Improved Side-channel Collision Attacks on AES [A] // SAC2007 [C]. LNC S 4876, Ottawa Canada, August 2007:84-95

[3] Bogdanov A, Kizhvatov I, Pyshkin A. Algebraic Methods in Side-channel Collision Attacks and Practical Collision Detection [A]// Indocrypt 2008[C]. LNCS 5365, Kharagpur, India, December 2008:251-265

[4] Oren Y, Kirschbaum M. Algebraic Side-channel Analysis in the Presence of Errors[A] // CHES 2010[C]. LNCS 6225, 2010: 428-442

[5] Bogdanov A, Knudsen L R, Leander, et al. PRESENT: an ultra-lightweight block cipher[A]// CHES 2007[C]. Vienna, Austria, 2007:450-466

[6] Courtois N, Pieprzyk J. Cryptanalysis of block ciphers with overdefined systems of equmions[A] // Asiacrypt 2002[C]. LNCS 2501, 2002:267-287

[7] Courtois N T, Klimov A, Patarin J. Efficient Algorithms for Solving Overdefind Systems of Multivariate Polynomial Equattion [EB/EL]. 2000

[8] Faugere J C. A New Efficient Algorithm for Computing Grobner Basic(F4)[EB/OL]. http://www. spaces. lip6. fr//@ paper/F99a. pdf, 1990

[9] Biryukov A, De Canniere C, Ciphers B. Systems of Quadratic Equations[A]// FSE 2003[C]. LNCS 2887, 2003:274-289

[10] Kipnis A, Shamir A. Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization[A]// Cryto99[C]. 1999:19-30

[11] Faugere J C. A New Efficient Algorithm for Computing Grobner Basic Without Redutio to Zero(F5) [EB/OL]. http://www. spaces. lip6. fr/@paper/F02a. pdf, 2002

[12] Seger A J M. Algeraic Attacks from a Grobner Basis Perspectives[EB/OL]. http://www. win. true. nl/～ henkvt/images/ReportSegers, 2004

[13] 卜凡,金晨辉. 针对低轮PRESENT的代数攻击[J]. 计算机工程,2010,36(6):128-130

[14] Bard G V, Courtois N T, Gregory C J. Efficient Methods for Conversion and Solution of Sparse Syetems of Low-degree Multivariate Polynomials over GF(2) via SAT-Solvers[EB/OL]. http:// eprint. iacr. org/2007/024, 2007

[15] Mangard S, Oswald E, Popp T. Power Analysis Attacks[M]. America: Springer, 2007

[16] Agrawal D, Rao J R, Rohatgi P, et al. Templates as Master Keys [A]// CHES 2005[C]. LNCS 3659. 2005:15-29

[17] Standaert F-X, Archambeau C. Using Subspace Based Template Attacks to Compare and Combine Power and Electromagnetic Information Leakages[A]// CHES 2008[C]. LNCS 5154. 2008: 411-425