PRESENT 密码代数故障攻击

吴克辉[1]，赵新杰[1]，王韬[1]，郭世泽[2]，刘会英[1]
(1. 军械工程学院 计算机工程系，河北 石家庄 050003；2. 北方电子设备研究所，北京 100083)

摘 要：提出了一种新的 PRESENT 密码故障分析方法——代数故障攻击。将代数攻击和故障攻击相结合，首先利用代数攻击方法建立密码算法等效布尔代数方程组；然后通过故障攻击手段获取错误密文信息，并将故障差分和密文差分转化为额外的布尔代数方程组；最后使用 CryptoMiniSAT 解析器求解方程组恢复密钥。结果表明：在 PRESENT-80 的第 29 轮注入宽度为 4 的故障，故障位置和值未知时，2 次故障注入可在 50s 内恢复 64bit 后期白化密钥，将 PRESENT-80 密钥搜索空间降低为 2^{16}，经 1min 暴力破解恢复完整主密钥；和现有 PRESENT 故障攻击相比，该攻击所需样本量是最小的；此外该代数故障分析方法也可为其他分组密码故障分析提供一定思路。

关键词：故障攻击；代数攻击；代数故障攻击；PRESENT 密码
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2012)08-0085-08

Algebraic fault attack on PRESENT

WU Ke-hui[1], ZHAO Xin-jie[1], WANG Tao[1], GUO Shi-ze[2], LIU Hui-ying[1]
(1. Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China;
2. The Institute of North Electronic Equipment, Beijing 100083, China)

Abstract: A new fault analysis method on PRESENT — algebraic fault attack was proposed. This attack combined conventional algebraic cryptanalysis with fault attack ,firstly built equivalent Boolean algebraic equations of cipher encryption by algebraic cryptanalysis method; secondly got information of fault cryptograph by fault attack technique, and transformed differential of fault and cryptograph into additional algebraic equations; finally utilized Crypto Mini SAT solver to solve the equations and recover key. Experiments demonstrate that after injecting 4-bit fault to the 29^{th} round of PRESENT-80,the fault location and fault value are unknown, only 2 injectings can recover 64-bit last whitening key in 50 seconds that reduce master key of PRESENT-80 searching space to 2^{16}, then recover the master key after 1 minute brute-force-search on average; compared with previous fault attack on PRESENT, the amount of this attack sample is the smallest； meanwhile, the analysis method proposed can be applied into the algebraic fault attack of other block ciphers.

Key words: fault attack; algebraic attack; algebraic fault attack; PRESENT

1 引言

密码算法安全性分析可分为面向设计的数学分析和面向实现的旁路分析 2 种。前者将密码实现视为黑盒，通过观测密码输入和输出，利用差分分析、线性分析、代数分析等数学方法分析其安全性，但受复杂度限制，现有方法仅能对算法安全性进行理论分析，很少能对其构成实际威胁；后者将密码

收稿日期：2011-07-30；**修回日期**：2011-10-24
基金项目：国家自然科学基金资助项目(60772082, 61173191)；河北省自然科学基金资助项目(08M010)
Foundation Items: The National Natural Science Foundation of China (60772082, 61173191); The Natural Science Foundation of Hebei Province (08M010)

实现视为灰盒，通过观测密码实现过程中泄露的时间、功耗、电磁、声音、故障等信息，结合密码输入和输出，利用简单分析、差分分析、相关分析、碰撞分析、互信息分析等方法，基于密钥分而治之的思想，在极小的代价下快速恢复密钥，目前已对多种密码算法的各种实现构成严峻威胁。在旁路分析中，根据密码运行泄露信息不同，可将其分为计时分析、功耗分析、电磁分析、故障分析等。

密码故障分析作为一种有效的旁路攻击方法，最早由 Boneh 等人[1,2]在 1996 年提出，并成功攻破 RSA 签名算法。随后 Biham 和 Shamir 于 1997 年提出了差分故障分析（DFA, differential fault analysis）方法，对 DES 密码进行了攻击。此后密码学家在此基础上实现了针对分组密码的差分故障攻击[3~5]。然而差分故障分析也具有一定的缺点：需要结合具体算法结构和操作进行密钥推导，分析方法繁琐；另外，即使在相同故障模型下，针对同一密码算法分析中，研究者常会得到不同的实验结果，这些都大大限制了差分故障攻击的通用性和实用性。因此，研究通用、自动化的分析方法一直是密码故障分析尚待解决的一个公开问题。

2002 年，Courtois 等[6]在亚密会上首次提出代数攻击的思想，将密码算法用代数方程组来等价表示，通过求解方程组方法进行密钥恢复。由于该方法可利用解析器进行密钥的自动化求解，可充分利用计算机资源，因此，代数攻击为密码分析提供了一种新的通用分析手段。然而，随着分组密码轮数的增加，未知变量和代数方程组规模也会递增，在有限复杂度内进行密钥求解是一个 N-P 完全问题，这些都极大限制了代数分析的实用性。2009 年，Renauld[7,8]等将代数攻击和旁路分析相结合，提出代数旁路攻击(ASCA, algebraic side-channel attack)思想，在代数攻击基础上，通过旁路攻击手段采集密码执行泄露的中间状态信息，并将其转化为额外的代数方程组，结合密码算法方程组，加快代数方程组求解速度。结果表明：针对 PRESENT 和 AES 密码算法，基于汉明重泄露模型，使用 zChaff 解析器，一条功耗曲线分析即可恢复完整密钥。代数旁路分析为密码旁路分析提供了一种新的通用手段，现有攻击大都基于功耗泄露模型，如何引入新的泄露模型是代数旁路分析的一个热点问题。

本文尝试将代数攻击和故障攻击相结合，衍化出一种新的代数旁路攻击手段——代数故障攻击，并应用其对 PRESENT 轻型分组密码进行故障分析。现有 PRESENT 故障攻击大都基于差分故障分析思想开展，文献[9]首次对 PRESENT-80 加密过程进行了差分故障分析，40-50 对正确-故障样本可恢复后期白化密钥，将主密钥搜索空间降低到 2^{16}，文献[10]提出了一种基于故障传播路径的差分故障分析方法，8 次故障注入即可将 PRESENT-80 密钥空间降低到 $2^{14.7}$；文献[11]对 PRESENT 密钥扩展进行了故障分析，64 次故障注入可恢复第 51bit 后期白化密钥，将主密钥空间降低到 2^{29}。在轻型分组密码代数故障攻击方面，笔者尚未发现国内外有公开发表的文献。

本文首次提出针对 PRESENT 的代数故障分析方法，在 PRESENT 加密第 29 轮注入宽度为 4 的故障模型下，2 次故障注入可在 50s 内恢复 64bit 后期白化密钥，将 PRESENT-80 密钥搜索空间降低为 2^{16}，并给出了有效故障样本的判断方法；和现有 PRESENT 故障攻击相比，文中攻击所需样本量是最小的。

本文结构如下：第 2 节阐述 PRESENT 分组密码算法，第 3 节给出了代数故障攻击原理，第 4 节介绍 PRESENT 故障攻击模型，第 5 节给出了 PRESENT 代数故障攻击具体过程，第 6 节为结束语。

2 PRESENT 密码算法

PRESENT 是由 Bogdanov[12]等人于 2007 年提出的轻量级分组密码，具有良好的硬件实现效率，在 0.18μm 工艺下仅需 1570GE 逻辑单元，可在 RFID 卡以及传感器网络等资源受限环境中广泛使用。算法采用 SPN 结构，分组长度为 64bit，支持 80bit、128bit 2 种密钥长度，共迭代 31 轮。

加密过程如下。

轮函数 F 由轮密钥加、S 盒代换、P 置换 3 部分组成。

1) 轮密钥加 AK：64bit 轮输入同轮密钥进行异或。

2) S 盒代换层 SL：将轮密钥加 64bit 输出查找 16 个 4 进 4 出的 S 盒。

3) P 置换层 DL：通过置换表 $P(i)$对 S 盒代换 64bit 输出按比特进行重新排列。

为提高算法安全性，PRESENT 在第 31 轮后使用 64bit 密钥 K^{32} 进行后期白化操作，具体加密流程如图 1 所示。

密钥扩展算法如下。

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 64bit 组

成。当生成第 i 轮密钥 K^i 后，密钥寄存器 K 通过以下方法进行更新：

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

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

$[k_{19}k_{18}k_{17}k_{16}k_{15}]=[k_{19}k_{18}k_{17}k_{16}k_{15}]\oplus$round_counter

其中，round_counter 为当前的加密轮数。易见，只需分析出 64bit 后期白化密钥，即可将 80bit PRESENT 的主密钥搜索空间降低到 2^{16}。

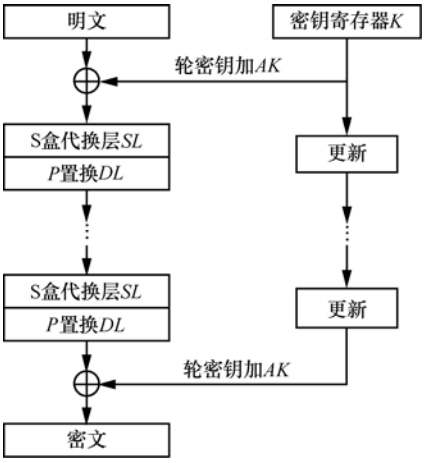


图 1　PRESENT 加密流程

3　代数故障攻击

如图 2 所示，代数故障攻击一般可分为 3 个阶段：密码算法方程组构建、故障注入及利用和代数方程组求解。其中，P、X_i、C 分别表示明文、中间状态以及密文，K、rk 分别表示主密钥和轮密钥。f 和 g 分别表示加密操作和密钥扩展。X_i^*和 C^*分别表示注入故障中间状态及错误密文输出，而ΔX_i 和 ΔC 则分别表示注入故障差分和密文差分值。

1) 密码算法方程组构建

将密码算法加密和密钥扩展分别表示为关于 P、X_i、C、K、rk 的代数方程组 $f()$和 $g()$。给定一个密码算法的代数方程组，密钥恢复等价于代数方程组求解。代数方程组构造过程中，最为关键的是如何构造非线性部件 S 盒对应代数方程组。常用的 S 盒代数方程组构造方法包括待定系数法、比较系数法[13]。本文主要参考文献[14]中基于高斯消元法构造 S 盒代数方程组的方法，对 PRESENT 密码的 S 盒构建等效方程组。

不同于其他类型的代数旁路攻击，代数故障攻击只需构建密码算法注入故障所在轮直至加密结束之间的代数方程组，因此攻击利用的代数方程组数量较少，便于求解。

2) 故障注入及利用

在构建密码算法等效代数方程组之后，需要进行故障注入和利用。故障注入的方法有很多，如光学辐射诱导、电压故障诱导、临界温度诱导、电磁

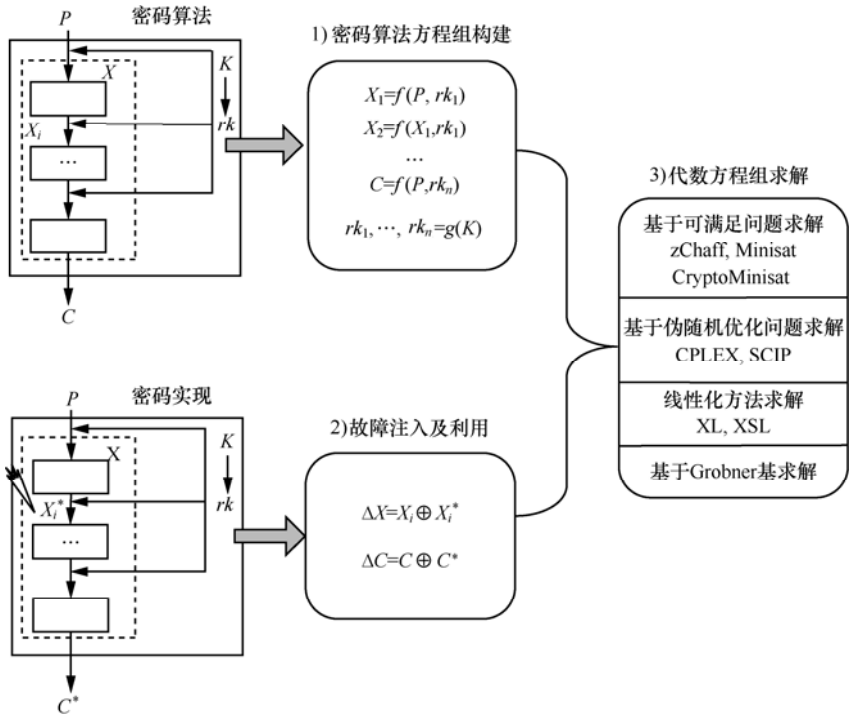


图 2　密码代数故障攻击模型

辐射诱导等。由于故障诱导不是本文研究重点，更多相关内容可参考文献[15]。故障利用的主要思想是将故障注入差分ΔX和密文输出差分ΔC使用代数方程组表示，同密码算法代数方程组联立，降低代数方程组的求解复杂度，加快方程组求解速度。

3) 代数方程组求解

代数方程组的求解问题一直是代数攻击领域研究的难点，在全轮分组密码中，密钥求解是一个N-P 完全问题，求解复杂度非常高，因此现有代数攻击仅能对约减轮的分组密码进行安全性分析。随着旁路信息的引入，代数方程组的求解速度可大大提高，从而对全轮密码算法实现构成严峻威胁。

目前，求解代数方程组主要包括基于可满足性问题[7,8]（使用 zChaff、Minisat、CryptoMinisat 等解析器）、基于伪随机优化问题[16]（使用 CPLEX、SCIP 解析器）、线性化(直接线性化 XL[17]、扩展线性化 XSL[18])、基于 Grobner 基[19]等方法。本文采用第 1 种，利用 CryptoMiniSAT 解析器进行密钥求解。

4　PRESENT 代数故障攻击模型

4.1　符号定义

A^i、B^i、C^i：分别表示第 i 轮轮密钥加、S 盒代换、P 置换输出；A^i*、B^i*、C^i*：分别表示第 i 轮轮密钥加、S 盒代换、P 置换故障输出；ΔA^i、ΔB^i、ΔC^i：分别表示第 i 轮轮密钥加、S 盒代换、P 置换故障输出差分。

4.2　故障模型

假设在 PRESENT 第 31 轮 S 盒输入注入 4bit 故障，则：

$$S[a]\oplus S[a\oplus f]=f' \tag{1}$$

其中，f 和 f' 为 S 盒输入和输出差分，a 为第 31 轮查表索引，将 a, f ($f\neq 0x00$)， f' 所有候选值代入式(1)，可得满足式(1)的 a 值统计，如表 1 所示。

表 1　PRESENT S 盒故障分析效率

a 数目	出现次数	出现概率	均值
2	2 880	0.75	1.5
4	960	0.25	1
总数	3 840	1	$2.5=2^{1.322}$

根据表 1，对于给定的 1 对输入和输出差分，可以获取 2～4 个 S 盒索引，2 对输入和输出差分即可以较高概率恢复 S 盒索引，结合密文恢复 4bit 后期白化密钥 K^{32}。攻击中，如果每个故障样本经传播后都能传播到 PRESENT 第 31 轮的 16 个 S 盒（如图 3 所示），则就有可能使用 2 个样本恢复 K^{32}。

此时，可能的故障传播过程为：在第 29 轮 A^{29} 注入宽度为 4 的故障（或者在 B^{29} 注入故障），使得 B^{29} 的 4 个比特全出错，即输出差分为 1111_2（$0x0f$），这 4 个比特经 P 置换可扩散至第 30 轮的 4 个 S 盒输入，经第 30 轮 S 盒后，输出差分全为 1111_2（$0x0f$），

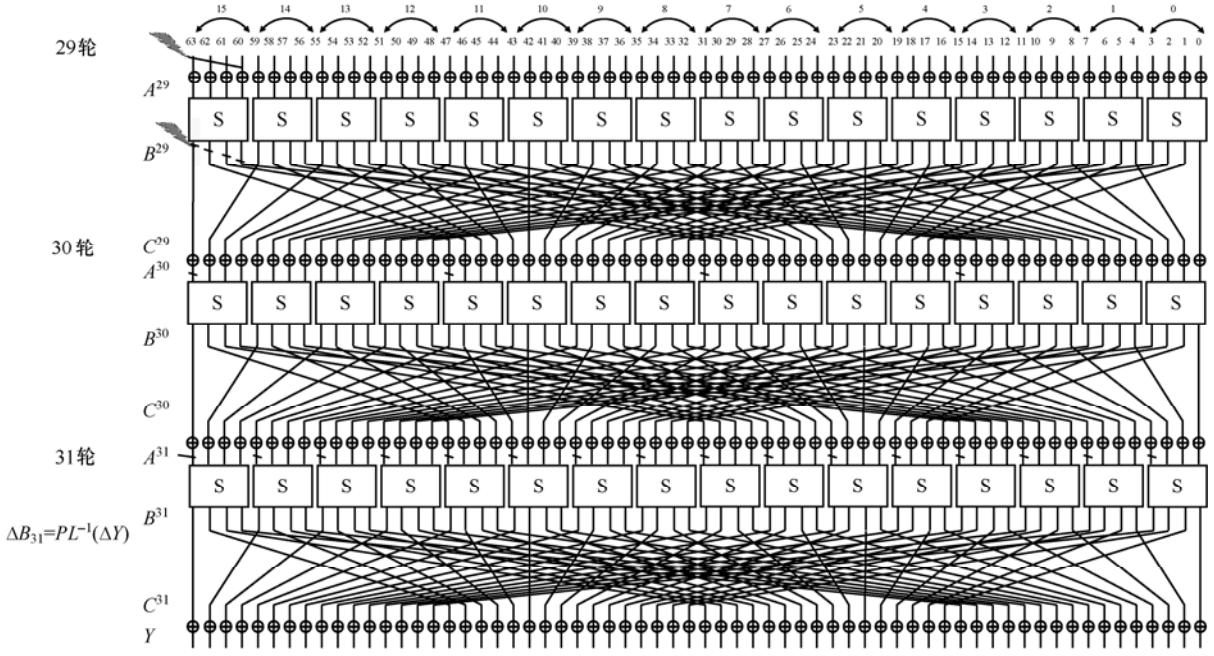


图 3　PRESENT 故障攻击模型

再经第 30 轮 P 置换扩散至第 31 轮的 16 个 S 盒，使得这 16 个 S 盒输入和输出差分均不为 0。表 2 为 PRESENT 的部分 S 盒差分表，其中输出差分中均出现 0xf，其对应 S 盒输入差分一共有 0x06, 0x07, 0x08, 0$x0f$ 4 种。根据上文分析，如果在 A^{29} 注入 4bit 故障，如果 S 盒输入差分为 0x06,0x07,0x08,0$x0f$ 中任意一种，就有可能使得 B^{29} 为 0$x0f$（或者直接在 B^{29} 注入差分为 0$x0f$ 故障），当扩散至第 30 轮 4 个 S 盒时，S 盒输入差分可能为 0x01,0x02,0x04,0x08，而当 30 轮 4 个 S 盒输入差分均为 0x08 时，恰好使得 30 轮的 4 个 S 盒输出差分均为 0$x0f$，然后经 P 转换传播后，使得 A^{31} 的 16 个 S 盒输入出现单比特故障。

综上，文中理想的故障模型为在第 29 轮 A^{29} 注入宽度为 4 的故障，其故障差分为 0x06,0x07, 0x08,0$x0f$，使得 B^{29} 的 4 个比特全出错，或者直接在 B^{29} 注入差分为 0$x0f$ 故障。

表 2　PRESENT 差分 S 盒（输出差分有 0$x0f$）

Δi	Δo			
	0x06	0x07	0x08	0$x0f$
0x00	0x06	0x01	0$x0f$	0$x0e$
0x01	0x08	0$x0f$	0$x0b$	0x04
0x02	0$x0f$	0x06	0x09	0x01
0x03	0$x0b$	0x02	0x03	0$x0f$
0x04	0$x0f$	0x02	0$x0d$	0x01
0x05	0$x0b$	0x06	0x07	0$x0f$
0x06	0x06	0$x0f$	0$x0b$	0x04
0x07	0x08	0x01	0$x0f$	0$x0e$
0x08	0x02	0x01	0$x0f$	0$x0e$
0x09	0$x0c$	0$x0f$	0$x0b$	0x04
0$x0a$	0$x0b$	0x08	0x09	0$x0f$
0$x0b$	0$x0f$	0$x0c$	0x03	0x01
0$x0c$	0$x0b$	0$x0c$	0$x0d$	0$x0f$
0$x0d$	0$x0f$	0x08	0x07	0x01
0$x0e$	0x02	0$x0f$	0$x0b$	0x04
0$x0f$	0$x0c$	0x01	0$x0f$	0$x0e$

4.3　故障样本筛选

根据 4.2 节，理想的故障样本对应的第 31 轮 16 个 S 盒输入差分应可能为 0x01,0x02,0x04,0x08 中 1 种，而第 31 轮 S 盒输出差分应有 16 个非零值。

在获取到故障密文样本后，首先将密文经逆 P 置换得到第 31 轮 S 盒输出差分ΔB^{31}，如果ΔB^{31} 的 16 个 S 盒输出均不为 0，且根据 PRESENT 单比特 S 盒输入差分对应 S 输出差分表，输出值均属于集合{0x03,0x05,0x06,0x07,0x09,0$x0a$,0$x0b$,0$x0c$,0$x0d$,0$x0e$, 0$x0f$}时，视为理想故障样本，否则剔除该故障样本。

需要说明的是，在故障宽度为 4 的情况下，如果在第 29 轮 P 置换输出到第 31 轮输出之间注入宽度为 4 的故障，由于 PRESENT 的 P 置换特性，均不能使得第 31 轮的 16 个输出差分全不为 0。而如果在第 29 轮前注入宽度为 4 的故障，经过多轮故障传播，第 31 轮的 16 个 S 盒输入差分很难满足均为单比特故障差分。

5　PRESENT 代数故障攻击

5.1　PRESENT 代数方程组构建

密码代数攻击都可归结于建立和求解有限域 $GF(q)$上系数任意选取的非线性布尔方程组，而建立分组密码 S 盒的超定、稀疏代数方程组一直是代数攻击研究的难点。本文参考文献[14]中基于高斯消元法建立 S 盒代数方程组的方法，用 9 个极端稀疏的八元二次布尔方程（MQ 方程）表示 PRESENT 的 S 盒，用大约 8 000 个未知变元、20 000 个 MQ 方程来表示 PRESENT 31 轮加密。未知变元包括 4 种类型，如表 3 所示。

表 3　　新增变元及说明

变元	说　明
p_i^r	第 r 轮轮密钥加输入比特
k_i^r	第 r 轮轮密钥比特
x_i^r	第 r 轮查 S 盒前输入比特
y_i^r	第 r 轮查 S 盒前输出比特

注：($0\leqslant r\leqslant 31, 0\leqslant i\leqslant 63$)

PRESENT 加密转化为以下等效布尔方程组：

$$p_i^r \oplus k_i^r = x_i^r \ (0\leqslant r\leqslant 31, 0\leqslant i\leqslant 63) \tag{2}$$

$$S(x_{4t}^r, x_{4t+1}^r, x_{4t+2}^r, x_{4t+3}^r) = y_{4t}^r, y_{4t+1}^r, y_{4t+2}^r, y_{4t+3}^r$$
$$(0\leqslant r\leqslant 30, 0\leqslant t\leqslant 15) \tag{3}$$

$$y_i^r = p_{g(i)}^{\ r+1} \ (0\leqslant r\leqslant 30, 0\leqslant i\leqslant 63) \tag{4}$$

式（2）表示 31 轮及白化轮加密过程中与轮密钥加操作；式（3）表示 31 轮加密过程中 S 盒代换操作；式（4）表示 31 轮加密过程中 P 置换操作，置换函数 g 详见文献[12]。此外，如考虑到轮密钥扩展，每轮还可增加大约 200 个 MQ 方程。

其中，代换函数 S 的输入变元 x_1, x_2, x_3, x_4 和输出变元 y_1, y_2, y_3, y_4 满足以下 S 盒代数方程组：

$$\begin{cases} 1\oplus x_1\oplus x_2\oplus y_2\oplus x_1y_1\oplus x_1y_3\oplus x_1y_4\oplus x_4y_1=0 \\ x_1\oplus x_2\oplus x_4\oplus y_4\oplus x_1y_2\oplus x_2y_1\oplus x_2y_2\oplus x_2y_3\oplus \\ x_2y_4\oplus x_3y_1\oplus x_4y_1=0 \\ x_3\oplus x_1y_2\oplus x_1y_3\oplus x_1y_4\oplus x_2y_2\oplus x_3y_1\oplus x_3y_2=0 \\ x_3\oplus x_1y_2\oplus x_2y_2\oplus x_3y_3\oplus x_3y_4\oplus x_4y_1=0 \\ 1\oplus x_3\oplus x_4\oplus y_1\oplus x_1y_2\oplus x_1y_3\oplus x_3y_1\oplus x_4y_1=0 \\ x_1\oplus x_3\oplus y_3\oplus x_1y_3\oplus x_1y_4\oplus x_2y_1\oplus x_2y_2\oplus \\ x_2y_4\oplus x_3y_1\oplus x_4y_1=0 \\ x_2\oplus x_4\oplus x_1y_1\oplus x_1y_3\oplus x_1y_4\oplus x_2y_2\oplus x_2y_3\oplus \\ x_2y_4\oplus x_3y_4\oplus x_4y_2=0 \\ x_1\oplus x_1y_3\oplus x_2y_1\oplus x_2y_2\oplus x_2y_3\oplus x_2y_4\oplus x_4y_1\oplus \\ x_4y_3=0 \\ x_2\oplus x_4\oplus x_1y_2\oplus x_1y_3\oplus x_1y_4\oplus x_2y_3\oplus x_2y_4\oplus \\ x_3y_4\oplus x_4y_1\oplus x_4y_4=0 \end{cases}$$

5.2 故障信息利用

1) 故障位置已知

基于 4.2 节故障模型，第 29 轮ΔB^{29}中只有 1 个 S 盒输出差分为 0*x*0*f*，其他为 0。假如第 j 个 S 盒输出差分为 0*x*0*f*，则可表示为

$$\prod_{i=4j}^{4j+3}(B_i^r\oplus B_i^{r*})=1 \tag{5}$$

其他 15 个 S 盒输出差分均为 0，可表示为

$$\prod_{i=4m}^{4m+3}(B_i^r\oplus B_i^{r*}\oplus 1)=1\quad m\in[0,15], m\neq j \tag{6}$$

此外，由于正确和故障密文可直接代入正确和故障样本的等效代数方程组，相当于密文差分的间接代入，故无需再建立关于密文差分的代数方程。

2) 故障位置未知

基于 4.2 节故障模型，第 29 轮ΔB^{29}中只有 1 个 S 盒输出差分为 0*x*0*f*，非 0 差分对应的位置有 16 种可能。每种可能位置的故障差分表示为（$B_{i,j}^{r*}$表示第 j 种可能的故障位置情况下第 r 轮 S 盒代换的故障输出）：

$$\prod_{i=4m}^{4m+3}(B_i^r\oplus B_{i,j}^{r*}\oplus 1)=\beta_j\quad m,j\in[0,15] \tag{7}$$

由于只有 1 种可能位置的故障差分对应的代数方程组成立，即 16 个变量β_j中只有 1 个为 1，其余为 0，因此集合$(\beta_1, \beta_2, \beta_3, \cdots, \beta_j)$的汉明重为 1，即满足函数：

$$HW(\beta_1, \beta_2, \beta_3, \cdots, \beta_j)=1 \tag{8}$$

其中，汉明重函数 HW 如下：

对于 1 个 16bit 的集合 $X=(x^1, x^2, \cdots, x^{15}, x^{16})$，共有 17 种可能的汉明重 $HW(X)$ $(0\leqslant HW(X)\leqslant 16)$，可以分别用一个 5bit 的变量 $Y=(y_1, y_2, y_3, y_4, y_5)$表示。$X$、$Y$ 满足以下方程（其中，$1\leqslant i\leqslant j\leqslant m\leqslant n\leqslant p\leqslant q\leqslant s\leqslant t\leqslant 16$）：

$$\begin{cases} y_1=\prod_{i=1}^{16}x^i \\ y_2=\sum_{t=1}^{12\,870}a_tx_ix_jx_mx_nx_px_qx_sx_t \\ y_3=\sum_{t=1}^{1\,820}a_tx_ix_jx_mx_n \\ y_4=\sum_{t=1}^{120}a_tx_ix_j \\ y_5=\sum_{i=1}^{16}x_i \end{cases} \tag{9}$$

5.3 实验结果及比较

在普通 PC 机（CPU 为 Athlon 64 3 000+ 1.81GHz，内存为 1GB）上，利用 C++语言、CryptoMiniSAT 软件实现了 PRESENT 代数故障攻击仿真实验，攻击流程如图 4 所示。

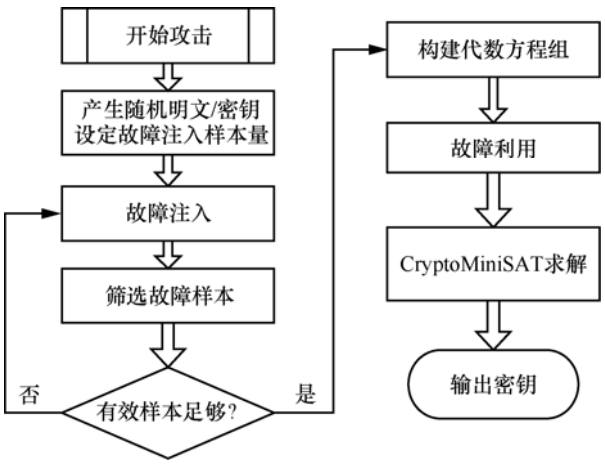


图 4 PRESENT 代数故障攻击流程

下面给出某次 PRESENT 代数故障攻击的过程。

1) 产生 1 个随机明文 P=232F2B98C151EAB5$_{16}$，密钥 K=7FB531421C9E023160B2$_{16}$，后期白化密钥为 62DE19A3B64AD6E8$_{16}$，此时正确密文为：E5B3136FD432ED2E$_{16}$；然后设定攻击样本量，在 PRESENT 加密第 29 轮注入 4 bit 随机故障。

2) 按照 4.3 节方法筛选有效故障样本，如第 1 个有效故障密文 C^{*1}=43371D628B872927$_{16}$，第 2 个有效故障密文 C^{*2}=E82435B139F6C697$_{16}$。

3) 参考 5.1 节方法构建 3 个样本（1 个正确样本，2 个故障样本）的 PRESENT 最后 3 轮代数方程组；参考 5.2 节方法将故障注入差分、密文差分转化为额外代数方程组。

4) 将密码算法和故障信息代数方程组转化为 SAT 子句，利用 CryptoMiniSA 解析器求解密钥。实验中 2 对 PRESENT 正确-故障样本 3 轮的代数方程组大约转化为 78 000 个 SAT 子句。解析器密钥求解结果如表 4 所示。

表 4　PRESENT 代数故障攻击结果

编号	K_i^{32}	编号	K_i^{32}	编号	K_i^{32}	编号	K_i^{32}
−834	0	−850	0	866	1	882	1
835	1	−851	0	−867	0	883	1
836	1	−852	0	868	1	−884	0
−837	0	853	1	869	1	885	1
−838	0	854	1	−870	0	−886	0
−839	0	−855	0	871	1	887	1
840	1	−856	0	872	1	888	1
−841	0	857	1	−873	0	−889	0
842	1	858	1	−874	0	890	1
843	1	−859	0	875	1	891	1
−844	0	860	1	−876	0	892	1
845	1	−861	0	−877	0	−893	0
846	1	−862	0	878	1	894	1
847	1	−863	0	−879	0	−895	0
848	1	864	1	880	1	−896	0
−849	0	865	1	−881	0	−897	0

如表 4 所示，编号 834 至 897 依次表示 64bit 的后期白化密钥比特值，如果编号为正，表示对应密钥位为 1，否则为 0。根据表 4，求解的后期白化密钥为 0110001011011110000110011010001110110110010010101101011011101000$_2$，即 62DE19A3B64AD6E8$_{16}$，同真实密钥一致，攻击成功；且故障已知时，耗时 16.35s，故障位置未知时，耗时 31.58s。

图 5 表示在 PRESENT 密码第 29 轮注入 4bit 故障，成功恢复 K^{32} 条件下，不同样本量对应的 CryptoMiniSAT 求解平均时间。可见最少仅需 2 对正确−故障样本即可将 PRESENT-80 密钥搜索空间降低为 2^{16}，且样本量同求解时间成正比；另外较之故障位置已知，故障位置未知条件下代数方程组复杂度稍高，导致 CryptoMiniSAT 解析器求解时间稍长。

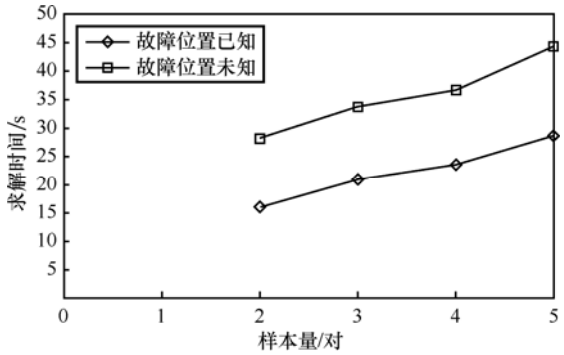


图 5　不同样本量下 CryptoMiniSAT 求解平均时间

实验结果同国内外 PRESENT 故障攻击比较如表 5 所示。可见，本文的攻击方案在故障样本量方面优势明显，攻击可行性较强，而且可利用解析器自动恢复密钥，具有一定的优越性。由于代数分析在分组密码领域的通用性，本文的分析方法可以扩展至其他分组密码的故障攻击，从而成为从故障攻击角度，评估分组密码实现安全性的通用手段之一。

表 5 实验结果同国内外 PRESENT 故障攻击比较

攻击	分析方法	故障样本量	结果均值
文献[9]	差分故障分析	40～50	2^{16}
文献[10]	差分故障分析	8	$2^{14.7}$
文献[11]	差分故障分析	64	2^{29}
本文攻击	代数故障分析	2	2^{16}

6　结束语

本文将代数攻击和故障攻击相结合，对代数故障攻击进行了研究。给出了代数故障攻击模型，以 PRESENT 轻型分组密码为例进行了攻击应用；首先建立了 PRESENT 故障攻击模型，然后给出了故障样本筛选、PRESENT 密码代数方程组构建、故障信息利用方法，最后通过仿真实验验证了攻击方法的可行性。

结果表明：应用文中故障模型，理想情况下，2 次故障注入，使用 CryptoMiniSAT 解析器进行方程组求解，即可恢复 PRESENT-80 的 64bit 后期白化密钥，耗时不超过 50s；同现有攻击相比，

文中提出故障模型所需的故障注入次数较小，给出的密文筛选方案明确，而且可使用解析器自动进行密钥求解，具有一定的优越性；此外，文中方法可为其他分组密码故障攻击提供一定的借鉴和参考。

参考文献：

[1] DONEH D, DEMILLO R, LIPTON R. On the importance of checking cryptographic protocols for faults[A]. Eurocrypt'97[C]. Konstanz, Germany, 1997. 37-51.

[2] BIHAM E, SHAMIR A. Differential fault analysis of secret key cryptosystems[A]. Crypto'97[C]. Santa Barbara, California, USA, 1997. 513-525.

[3] DEBDEEP M. An improved fault based attack of the advanced encryption standard[A]. AFRICACRYPT 2009[C]. Gammarh, Tunisia, 2009. 421-434.

[4] ZHAO X J, WANG T. Further improved differential fault analysis on camellia by exploring fault width and depth[EB/OL]. http: //eprint. iacr. org/2010/026.pdf, 2010.

[5] LI W, GU D W, LI J R. Differential fault analysis on the ARIA algorithm[J]. Information Sciences, 2008,178(19):3727–3737.

[6] NICOLAS T C, JOSEF P. Cryptanalysis of block ciphers with overdefined systems of equations[A]. ASIACRYPT 2002[C]. Berlin Heidelberg, 2002. 267-287

[7] MATHIEU R, FRANCOIS-X S. Algebraic side-channel attacks[A]. INSCRYPT 2009[C]. California, USA, 2009. 393-410.

[8] MATHIEU R, FRANCOIS-X, NICOLAS V-C. Algebraic side-channel attacks on the AES: Why time also matters in DPA[A]. CHES 2009[C]. California, USA, 2009. 97-111.

[9] 李卷孺, 谷大武. PRESENT 算法的差分故障攻击[A]. 中国密码学会 2009 年会[C]. 中国, 北京, 2009. 3-13.
LI J R, GU D W. Differential fault analysis on PRESENT[A]. CHINACRYPT 2009[C]. Beijing, China, 2009. 3-13.

[10] ZHAO X J, WANG T. Fault propagate pattern based DFA on SPN structure block ciphers using bitwise permutation, with application to PRESENT and PRINTcipher[EB/OL]. http://eprint.iacr.org/2011/089.pdf, 2011.

[11] WANG G L, WANG S S. Differential fault analysis on PRESENT key schedule[A]. International Conference on Computational Intelligence and Security (CIS 2010)[C]. 2010. 362-366.

[12] BOGDANOV A, KNUDSEN L R, LEANDER, *et al*. PRESENT: an ultra-lightweight block cipher[A]. CHES 2007[C]. Vienna, Austria, 2007. 450-466.

[13] 李伟博,解永宏,胡磊.分组密码 S 盒的代数方程[J].中国科学院研究生学报, 2008, 25(4):524-529.
LI W B, XIE Y H, HU L. Algebraic equations of sbox block cipher[J]. Journal of the Graduate School of the Chinese Academy of Sciences, 2008, 25(4):524-529.

[14] ALEX B, CHRISTOPHE D C. Block ciphers and systems of quadratic equations[A]. FSE 2003[C]. 2003. 274-289.

[15] GIRAUD C, THIEBEAULD H. A survey on fault attacks[A]. International Conference on Smart Card Research and Advanced Applications (CARDIS'O4)[C]. Toulouse, France, 2004. 22-27.

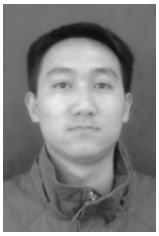
[16] YOSSED O, MARIO K, THOMAS P, *et al*. Side-channel analysis in the presence of errors[A]. CHES 2010[C]. Santa Barvara, California, 2010.428-442.

[17] COURTOIS N T, KLIMOV A, PARARIN J. Efficient algorithms for solving overdefind systems of multivariate polynomial equattion[EB/OL]. http://www.iacr.org/archive/enrocrypt2000/1807/18070398-new/.pdf,2000.

[18] KIPNIS A, SHAMIR A. Cryptanalysis of the HFE public key cryptosystem by relinearization[A]. Cryto99[C], Santa Barbara, California, USA, 1999. 19-30.

[19] SEGER A J M. Algeraic attacks from a Grobner basis perspectives[EB/OL]. http://www. win.true.nl/~henkvt/images/ReportSegers, 2004.

作者简介：



吴克辉（1986-），男，甘肃景泰人，军械工程学院硕士生，主要研究方向为分组密码旁路分析。

赵新杰（1986-），男，河南开封人，军械工程学院博士生，主要研究方向为分组密码旁路分析和故障分析。

王韬（1964-），男，河北石家庄人，博士，军械工程学院教授、博士生导师，主要研究方向为信息安全和密码学。

郭世泽（1969-），男，河北石家庄人，博士，北方电子设备研究所研究员、博士生导师，主要研究方向为信息安全和密码学。

刘会英（1984-），男，湖北黄石人，军械工程学院博士生，主要研究方向为图像加密和密码旁路分析。