一类模加差分方程系统解个数的期望与方差

献给万哲先教授 90 华诞

冯秀涛^{1*}, 张凡¹, 黄慎²

1. 中国科学院数学与系统科学研究院数学机械化重点实验室, 北京 100190;

2. 武汉软件工程职业学院人文学院, 武汉 430205

E-mail: fengxt@amss.ac.cn, tzhangfan4@163.com, 635959386@qq.com

收稿日期: 2017-06-02; 接受日期: 2017-08-16; 网络出版日期: 2017-09-27; * 通信作者

国家自然科学基金 (批准号: 61572491 和 11688101) 和国家重点基础研究发展计划 (批准号: 2016YFB0800401) 资助项目

摘要 模 2^n 加法是一个非常重要的密码运算部件, 它已经被广泛用于各种对称密码算法的设计, 如 MD5、SNOW 3G、SPECK 和 ZUC 等. 差分故障攻击是针对密码算法实现的一种通用的安全性分析方法, 该攻击假设攻击者能在算法运行过程中动态注入故障. 在对采用模加运算的密码算法进行差分故障分析时, 攻击者往往会导出一个模加差分方程系统, 该方程系统中, 方程的个数恰好等于注入故障的次数, 其与方程系统的解个数密切相关. 由于注入故障次数和方程系统解个数是评估故障攻击复杂度的两个关键参数, 因此, 研究它们之间的关系非常有意义. 本文讨论了上述模加差分方程系统中一类特殊方程系统 (即模加差分相互独立且服从均匀分布) 的解个数的统计特性. 作为结果, 本文给出了它们的期望和方差. 本文的结果表明, 对一般的模加差分方程系统, 平均意义下, 需要注入大约 $\log_2(n) + 5$ 个故障可以确定方程系统的候选解.

关键词 模加 差分故障攻击 差分系统 期望 方差

MSC (2010) 主题分类 94A60

1 引言

模 2^n 加法“田”是一个非常重要的密码运算部件, 它在分组密码、序列密码和 Hash 函数中都有着广泛的应用. 例如, MD5^[1]、SNOW 3G^[2]、SPECK^[3] 和 ZUC^[4] 等算法都用到了模 2^{32} 加法. 与其他密码部件相比, 如 S 盒和线性置换 P 等, 模 2^n 加法不仅能提供非线性 (相对于模 2 加法) 混淆, 而且还具有良好的软硬件实现等特性.

差分分析是一种强有力的密码分析方法, 它几乎可以应用到所有的对称密码算法上. 其核心思想是, 通过选择具有特定差分关系的输入对, 在同一个变换下得到相应的输出对, 攻击者通过观察输出对之间的变化规律 (即输出差分) 来试图获取变换内部关于未知秘密的信息. 差分分析最早应用于分组密码 DES^[5], 之后被逐渐移植到序列密码^[6] 和 Hash 函数^[7] 中. 最近几年, 差分攻击思想被进一步应用到 Boomerang 攻击^[8] 和 Rectangle 攻击^[9].

英文引用格式: Feng X T, Zhang F, Huang S. The expectation and variance of the number of solutions of a class of differential system of modular addition (in Chinese). Sci Sin Math, 2017, 47: 1545–1556, doi: 10.1360/N012017-00115

故障攻击^[10] 是一种针对密码算法实现的攻击方法. 差分故障分析是最常见的一种故障分析方法. 该方法主要利用差分攻击思想, 通过在密码算法的实际运行过程中随机地注入故障, 并利用故障前后密码算法输出之间的变化规律来收集关于内部状态或密钥的方程, 最后通过求解这些方程来获取关于内部状态或者密钥的信息. 在具体实施过程中, 差分故障分析一般分为两步: 故障位置定位和差分方程系统求解. 其中故障位置定位主要依据故障注入前后密码算法输出的变化规律来确定故障发生的实际位置, 并依此来收集关于内部状态或者密钥的差分方程. 一旦得到差分方程系统后, 攻击者可以利用代数的方法求解该差分方程系统, 得到内部状态或者密钥的信息. 在故障攻击中, 注入故障的次数 r 和差分方程求解计算量是评估故障攻击复杂度的两个核心指标. 一般而言, 注入故障的次数 r 越大, 收集的差分方程个数就越多, 求解差分方程系统就越容易; 反之, 注入故障的次数 r 越小, 收集的差分方程个数就越少, 求解差分方程系统就越困难. 由于故障的注入, 往往伴随着物理设备的破坏, 因此, 在现实攻击中, 我们往往希望在差分方程求解复杂度可接受的情形下注入故障的次数越少越好.

对采用模 2^n 加法 “ $\boxplus$ ” 的密码体制, 攻击者在对其进行故障差分分析时往往会导出具有下述形式的差分方程系统:

$$\begin{cases} X \boxplus Y = Z, \\ (X \oplus \alpha^{(1)}) \boxplus (Y \oplus \beta^{(1)}) = Z \oplus \gamma^{(1)}, \\ \vdots \\ (X \oplus \alpha^{(r)}) \boxplus (Y \oplus \beta^{(r)}) = Z \oplus \gamma^{(r)}, \end{cases} \quad (1.1)$$

这里 r 为攻击者注入故障的次数, $(\alpha^{(i)}, \beta^{(i)})$ 和 $\gamma^{(i)}$ ($1 \leq i \leq r$) 分别为模加运算 $\boxplus$ 的输入输出差分. 文献 [11] 在对序列密码 SNOW 3G 进行差分故障分析时首次导出了上述方程系统 (1.1), 并利用 Gröbner 基方法从方程系统 (1.1) 中抽出线性方程, 然后进行求解. 文献 [12] 对分组密码 SPECK 进行差分故障分析时同样导出方程系统 (1.1), 并利用模加差分方程代数性质进行求解. 随后, 文献 [13] 利用 Gröbner 基方法结合非线性方程迭代求解方法大幅改进了文献 [12] 中的相关结果, 将注入故障的次数从 $n/3$ 降到 $\ln(n)$. 对于方程系统 (1.1) 还可以考虑借助 S- 函数方法^[14] 来求解.

在模加差分方程系统 (1.1) 中, 方程的个数即为注入故障的个数, 它与方程系统解的个数密切相关, 两者都是评估故障分析复杂度的关键参数. 因此, 在一般意义下, 研究这类模加差分方程系统的解的个数与注入故障个数的关系显得非常重要. 在这个工作中, 我们在输入输出差分 $(\alpha^{(i)}, \beta^{(i)})$ 和 $\gamma^{(i)}$ 相互独立且在空间 F_2^n 上服从均匀分布的假设下研究了方程系统 (1.1) 的解个数的统计特性, 给出了它们的期望和方差. 我们的结果表明, 在平均意义下, 需要注入大约 $\log_2(n) + 5$ 个故障可以确定方程系统 (1.1) 的候选解.

本文余下部分内容组织如下: 第 2 节介绍关于模加运算的一些基本知识, 并根据给定的输入输出差分给出了计算模加差分方程系统解个数的方法; 第 3 节进一步给出了模加差分方程系统解个数的期望和方差的数学表达式, 并讨论了故障注入次数与方程解之间的关系.

2 背景知识

为了方便本文的描述, 首先介绍一些基本定义和概念, 然后给出在输入输出差分给定时计算模加差分方程系统 (1.1) 解个数的方法.

2.1 基本定义和概念

对给定的一个 n 比特整数 X , 总记

$$X = x_{n-1}x_{n-2}\cdots x_1x_0 = \sum_{i=0}^{n-1} x_i 2^i,$$

这里 $x_i \in \{0, 1\}$ 为 X 的二进制表示中第 i ($0 \leq i \leq n-1$) 比特的取值.

对方程系统 (1.1), 我们引入如下一些定义:

定义 1 对 $i = 0, 1, \dots, n-1$, $k = 0, 1, \dots, r$, 定义

$$x_i^{(k)} := x_i^{(0)} \oplus \alpha_i^{(k)}, \quad y_i^{(k)} := y_i^{(0)} \oplus \beta_i^{(k)}, \quad z_i^{(k)} := z_i^{(0)} \oplus \gamma_i^{(k)},$$

这里, $x_i^{(0)}$ 、 $y_i^{(0)}$ 、 $z_i^{(0)}$ 、 $\alpha_i^{(k)}$ 、 $\beta_i^{(k)}$ 和 $\gamma_i^{(k)}$ 分别表示 X 、 Y 、 Z 、 $\alpha^{(k)}$ 、 $\beta^{(k)}$ 和 $\gamma^{(k)}$ 的第 i 比特取值. 设进位比特

$$c_{i+1}^{(k)} := x_i^{(k)} y_i^{(k)} \oplus (x_i^{(k)} \oplus y_i^{(k)}) c_i^{(k)}, \quad c_0^{(k)} = 0.$$

于是, 对 $0 \leq i \leq n-1$ 和 $0 \leq k \leq r$, 有

$$z_i^{(k)} = x_i^{(k)} \oplus y_i^{(k)} \oplus c_i^{(k)}, \quad c_{i+1}^{(k)} = (x_i^{(0)} \oplus \alpha_i^{(k)})(y_i^{(0)} \oplus \beta_i^{(k)}) \oplus (x_i^{(0)} \oplus \alpha_i^{(k)} \oplus y_i^{(0)} \oplus \beta_i^{(k)}) c_i^{(k)}. \quad (2.1)$$

定义 2 $I(a, b)$ 表示由二元组 $(a, b) \in \{0, 1\}^2$ 确定的集合, 定义如下:

$$I(a, b) = \begin{cases} \{(0, 0), (0, 1), (1, 0)\}, & (a, b) = (0, 0), \\ \{(1, 1)\}, & (a, b) = (0, 1), \\ \{(0, 0)\}, & (a, b) = (1, 0), \\ \{(0, 1), (1, 0), (1, 1)\}, & (a, b) = (1, 1). \end{cases}$$

记 $(c, d) \oplus I(a, b) := \{(c \oplus s, d \oplus t) \mid (s, t) \in I(a, b)\}$.

定义 3 令 $\mathbf{c}_i = (c_i^{(0)}, c_i^{(1)}, \dots, c_i^{(r)})$. 定义

$$U(\mathbf{c}_i, \mathbf{c}_{i+1}) = \left| \bigcap_{k=0}^r ((\alpha_i^{(k)}, \beta_i^{(k)}) \oplus I(c_i^{(k)}, c_{i+1}^{(k)})) \right|.$$

2.2 基本性质

由进位比特 $c_i^{(k)}$ 的表达式 (2.1), 根据定义直接验证可得

$$(x_i^{(0)} \oplus \alpha_i^{(k)}, y_i^{(0)} \oplus \beta_i^{(k)}) \in I(c_i^{(k)}, c_{i+1}^{(k)}), \quad k = 0, 1, \dots, r. \quad (2.2)$$

于是有 $(x_i^{(0)}, y_i^{(0)}) \in \bigcap_{k=0}^r ((\alpha_i^{(k)}, \beta_i^{(k)}) \oplus I(c_i^{(k)}, c_{i+1}^{(k)}))$. 根据 $U(\mathbf{c}_i, \mathbf{c}_{i+1})$ 的定义, 我们有如下引理成立:

引理 1 $0 \leq U(\mathbf{c}_i, \mathbf{c}_{i+1}) \leq 3$. 进一步, 有

(1) $U(\mathbf{c}_i, \mathbf{c}_{i+1}) = 3$ 当且仅当对所有的 $k = 0, 1, \dots, r$, 有 $c_i^{(k)} = c_{i+1}^{(k)}$, 且所有的 $(\alpha_i^{(k)} \oplus c_i^{(k)}, \beta_i^{(k)} \oplus c_{i+1}^{(k)})$ 均相等.

(2) $U(\mathbf{c}_i, \mathbf{c}_{i+1}) = 2$ 当且仅当对所有的 $k = 0, 1, \dots, r$, 有 $c_i^{(k)} = c_{i+1}^{(k)}$, 且所有的 $(\alpha_i^{(k)} \oplus c_i^{(k)}, \beta_i^{(k)} \oplus c_{i+1}^{(k)})$ 只能取两个不同的值.

(3) $U(\mathbf{c}_i, \mathbf{c}_{i+1}) = 1$ 当且仅当以下两个条件有一个成立:

(i) 对所有的 $k = 0, 1, \dots, r$, 有 $c_i^{(k)} = c_{i+1}^{(k)}$, 且所有的 $(\alpha_i^{(k)} \oplus c_i^{(k)}, \beta_i^{(k)} \oplus c_{i+1}^{(k)})$ 只能取三个不同的值;

(ii) 集合 $\{k \mid c_i^{(k)} \neq c_{i+1}^{(k)}, 0 \leq k \leq r\}$ 非空, 且要求

$$\begin{aligned} (\alpha_i^{(k)} \oplus c_i^{(k)}, \beta_i^{(k)} \oplus c_{i+1}^{(k)}) &= \mathbf{e}, \quad k \in \{k \mid c_i^{(k)} \neq c_{i+1}^{(k)}, 0 \leq k \leq r\}, \\ (\alpha_i^{(k)} \oplus c_i^{(k)}, \beta_i^{(k)} \oplus c_{i+1}^{(k)}) &\neq \mathbf{e} \oplus (0, 1), \quad k \in \{k \mid c_i^{(k)} = c_{i+1}^{(k)}, 0 \leq k \leq r\}, \end{aligned}$$

这里 $\mathbf{e} \in \{0, 1\}^2$ 是常向量.

证明 表 1 刻画了 $(\alpha_i^{(k)} \oplus c_i^{(k)}, \beta_i^{(k)} \oplus c_{i+1}^{(k)}, c_i^{(k)} \oplus c_{i+1}^{(k)})$ 与 $(\alpha_i^{(k)}, \beta_i^{(k)}) \oplus I(c_i^{(k)}, c_{i+1}^{(k)})$ 的关系. 根据表 1, 我们容易验证结论是成立的. $\square$

上面的引理给出了 $U(\mathbf{c}_i, \mathbf{c}_{i+1})$ 的大小与 $(\mathbf{c}_i, \mathbf{c}_{i+1})$ 以及 $(\alpha_i^{(k)}, \beta_i^{(k)})_{1 \leq k \leq r}$ 之间的关系. 注意到差分方程系统 (1.1) 是由一个实际的密码体制推导而来, 因此, 该系统总是有解, 不妨记 $x = (x_{n-1}, x_{n-2}, \dots, x_0)$, $y = (y_{n-1}, y_{n-2}, \dots, y_0)$ 和 $z = (z_{n-1}, z_{n-2}, \dots, z_0)$ 为方程系统 (1.1) 的一个解.

为了方便叙述, 规定在下文中, $c_i^{(k)}$ 表示 (X, Y, Z) 取 (x, y, z) 时方程系统 (1.1) 中第 k 个方程的第 i 个进位比特, 这里 $0 \leq k \leq r$ 和 $0 \leq i \leq n$. 换言之, 在表达式 (2.1) 中, 将 $x_i^{(0)}$ 和 $y_i^{(0)}$ 分别替换成 x_i 和 y_i . 对给定的 r 个输入输出差分对 $(\alpha^{(k)}, \beta^{(k)}, \gamma^{(k)})$ 和 $0 \leq i \leq n-2$, 设

$$\begin{aligned} \mathbf{c}_i^0 &= (0, \alpha_i^{(1)} \oplus \beta_i^{(1)} \oplus \gamma_i^{(1)}, \dots, \alpha_i^{(r)} \oplus \beta_i^{(r)} \oplus \gamma_i^{(r)}), \\ \mathbf{c}_i^1 &= (1, 1 \oplus \alpha_i^{(1)} \oplus \beta_i^{(1)} \oplus \gamma_i^{(1)}, \dots, 1 \oplus \alpha_i^{(r)} \oplus \beta_i^{(r)} \oplus \gamma_i^{(r)}). \end{aligned}$$

并令

$$T_i^{(k)} = (\alpha_i^{(k)} \oplus c_i^{(k)} \oplus c_i^{(0)}, \beta_i^{(k)} \oplus c_{i+1}^{(k)} \oplus c_{i+1}^{(0)}, c_i^{(k)} \oplus c_{i+1}^{(k)} \oplus c_i^{(0)} \oplus c_{i+1}^{(0)}).$$

记 $T_i = (T_i^{(1)}, \dots, T_i^{(r)})$, 根据上述定理可知 $U(\mathbf{c}_i, \mathbf{c}_{i+1})$ 依赖于 T_i . 下面定义矩阵

$$\mathbf{M}_i(T_i) = \begin{pmatrix} U(\mathbf{c}_i^0, \mathbf{c}_{i+1}^0) & U(\mathbf{c}_i^1, \mathbf{c}_{i+1}^0) \\ U(\mathbf{c}_i^0, \mathbf{c}_{i+1}^1) & U(\mathbf{c}_i^1, \mathbf{c}_{i+1}^1) \end{pmatrix},$$

这里 $i = 0, 1, \dots, n-2$. 于是有下面的定理:

表 1 $(\alpha_i^{(k)} \oplus c_i^{(k)}, \beta_i^{(k)} \oplus c_{i+1}^{(k)}, c_i^{(k)} \oplus c_{i+1}^{(k)})$ 与 $(\alpha_i^{(k)}, \beta_i^{(k)}) \oplus I(c_i^{(k)}, c_{i+1}^{(k)})$ 的关系

$(\alpha_i^{(k)} \oplus c_i^{(k)}, \beta_i^{(k)} \oplus c_{i+1}^{(k)}, c_i^{(k)} \oplus c_{i+1}^{(k)})$	$(\alpha_i^{(k)}, \beta_i^{(k)}) \oplus I(c_i^{(k)}, c_{i+1}^{(k)})$
(0,0,0)	$\{(0,0), (0,1), (1,0)\}$
(0,1,0)	$\{(0,1), (0,0), (1,1)\}$
(1,0,0)	$\{(1,0), (1,1), (0,0)\}$
(1,1,0)	$\{(1,1), (1,0), (0,1)\}$
(0,0,1)	$\{(1,0)\}$
(0,1,1)	$\{(1,1)\}$
(1,0,1)	$\{(0,0)\}$
(1,1,1)	$\{(0,1)\}$

定理 1 对任意给定的 $(\alpha^{(k)}, \beta^{(k)}, \gamma^{(k)})_{1 \leq k \leq r}$, 方程系统 (1.1) 解的个数

$$N(\alpha, \beta, \gamma) = 4 \times \mathbf{u} \left(\prod_{i=0}^{n-2} \mathbf{M}_i(T_i) \right) \mathbf{v}, \quad (2.3)$$

这里 $\mathbf{u} = (1, 1)$, $\mathbf{v} = (1, 0)$.

证明 我们通过构造二部图来证明这个定理. 对 $i = 0, 1, \dots, n-1$, 第 i 个二部图的两个顶点 $v_i[0] = 0$ 和 $v_i[1] = 1$ 表示第 i 个进位比特的两个状态. 相邻二部图的任意两个顶点 $v_i[s_i]$ 到 $v_{i+1}[s_{i+1}]$ 存在有向边, 且权重是 $U(\mathbf{c}_i^{v_i[s_i]}, \mathbf{c}_{i+1}^{v_{i+1}[s_{i+1}]})$, 这里 $s_i, s_{i+1} \in \{0, 1\}$. 根据第 0 个比特的进位始终为零, 则从顶点 $v_0[0]$ 出发的任意一条路径的权重之积是

$$\prod_{i=0}^{n-2} U(\mathbf{c}_i^{v_i[s_i]}, \mathbf{c}_{i+1}^{v_{i+1}[s_{i+1}]})$$

它表示第 i 个进位比特取值为 $v_i[s_i]$ 时, $x_0^{(0)}, y_0^{(0)}, \dots, x_{n-2}^{(0)}, y_{n-2}^{(0)}$ 的可能个数. 于是,

$$\mathbf{u} \left(\prod_{i=0}^{n-2} \mathbf{M}_i \right) \mathbf{v} = \sum_{s_0=0, s_1, \dots, s_{n-2} \in \{0, 1\}} \prod_{i=0}^{n-2} U(\mathbf{c}_i^{v_i[s_i]}, \mathbf{c}_{i+1}^{v_{i+1}[s_{i+1}]})$$

根据表达式 (2.1) 可知, 第 $n-1$ 个进位比特与 $x_{n-1}^{(0)}, y_{n-1}^{(0)}$ 和 $z_{n-1}^{(0)}$ 无关, 此时约束 x_{n-2}, y_{n-2} 和 z_{n-2} 的方程只有一个, 形如

$$x_{n-1}^{(0)} \oplus y_{n-1}^{(0)} \oplus z_{n-1}^{(0)} = c,$$

这里 c 是与 x_{n-1}, y_{n-1} 和 z_{n-1} 相关的常数. 于是, x_{n-1} 和 y_{n-1} 的可能取值有 4 个. 因此有

$$N(\alpha, \beta, \gamma) = 4 \times \mathbf{u} \left(\prod_{i=0}^{n-2} \mathbf{M}_i(T_i) \right) \mathbf{v},$$

定理证毕. □

根据表 1 和引理 1, 我们很容易确定 $U(\mathbf{c}_i^0, \mathbf{c}_{i+1}^0)$ 和矩阵 $\mathbf{M}_i(T_i)$ 的取值, 结果如下:

引理 2 假设 $\mathbf{c}_i$ 和 $\mathbf{c}_{i+1}$ 均只有两个状态, 即 $\mathbf{c}_i^0, \mathbf{c}_i^1$ 和 $\mathbf{c}_{i+1}^0, \mathbf{c}_{i+1}^1$, 则

$$\begin{aligned} U(\mathbf{c}_i^0, \mathbf{c}_{i+1}^0) &= U(\mathbf{c}_i^1, \mathbf{c}_{i+1}^1) \in \{0, 1, 2, 3\}, \\ U(\mathbf{c}_i^0, \mathbf{c}_{i+1}^1) &= U(\mathbf{c}_i^1, \mathbf{c}_{i+1}^0) \in \{0, 1\}, \\ \mathbf{M}_i(T_i) &\in \left\{ \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}. \end{aligned}$$

$U(\mathbf{c}_i, \mathbf{c}_{i+1})$ 和 $\mathbf{M}_i(T_i)$ 的取值条件请参见附录 A.

根据 $\mathbf{M}_i(T_i)$ 的取值, 我们定义 $\lambda_i(T_i)$ 如下:

$$\mathbf{u} \mathbf{M}_i(T_i) = \lambda_i(T_i) \mathbf{M}_i(T_i), \quad \lambda_i(T_i) \in \{1, 2, 4\}.$$

于是有下面的推论成立:

推论 1 设 $\lambda_i(T_i)$ 如上定义, 则对任意 $(\alpha^{(k)}, \beta^{(k)}, \gamma^{(k)})_{1 \leq k \leq r}$, 方程系统 (1.1) 解的个数满足

$$N(\alpha, \beta, \gamma) = 4 \prod_{i=0}^{n-2} \lambda_i(T_i). \quad (2.4)$$

3 模加差分方程组解个数的期望和方差

本节将研究方程系统 (1.1) 解个数的期望和方差. 我们总是假设方程系统 (1.1) 中输入输出差分已知, 且输入差分相互独立且服从均匀分布. 在此之前, 首先引入如下一些随机变量.

设 $\mathbf{a}_i^{(k)}$ 、 $\mathbf{b}_i^{(k)}$ 和 $\mathbf{r}_i^{(k)}$ 分别表示 $\alpha_i^{(k)}$ 、 $\beta_i^{(k)}$ 和 $\gamma_i^{(k)}$ 的随机变量, $\mathbf{c}_i^{(k)}$ 表示进位 $c_i^{(k)}$ 的随机变量, $\mathbf{T}_i^{(k)}$ 表示 $T_i^{(k)}$ 的随机变量.

首先, 对任意给定的 $0 \leq i < n$, r 个随机变量 $(\mathbf{T}_i^{(k)})_{1 \leq k \leq r}$ 是相互独立的. 这是因为

$$\Pr\{\mathbf{T}_i^{(k)} = (a, b, c)\} = \Pr\{\mathbf{a}_i^{(k)} \oplus \mathbf{c}_i^{(k)} = a', \mathbf{b}_i^{(k)} \oplus \mathbf{c}_{i+1}^{(k)} = b', \mathbf{c}_i^{(k)} \oplus \mathbf{c}_{i+1}^{(k)} = c'\},$$

这里 $a' = c_i^{(0)} \oplus a$, $b' = c_{i+1}^{(0)} \oplus b$, $c' = c_i^{(0)} \oplus c_{i+1}^{(0)} \oplus c$. 而

$$\mathbf{a}_i^{(k)} \oplus \mathbf{c}_i^{(k)} = a', \quad \mathbf{b}_i^{(k)} \oplus \mathbf{c}_{i+1}^{(k)} = b', \quad \mathbf{c}_i^{(k)} \oplus \mathbf{c}_{i+1}^{(k)} = c'$$

等价于

$$\mathbf{a}_i^{(k)} = \mathbf{c}_i^{(k)} \oplus a', \quad \mathbf{b}_i^{(k)} = \mathbf{c}_i^{(k)} \oplus b' \oplus c', \quad (x_i \oplus a')(y_i \oplus b' \oplus c') = c'. \quad (3.1)$$

根据 $(\mathbf{a}_i^{(k)}, \mathbf{b}_i^{(k)})_{1 \leq k \leq r}$ 是相互独立的且 $(\mathbf{a}_i^{(k)}, \mathbf{b}_i^{(k)})$ 与 $\mathbf{c}_i^{(k)}$ 独立可得 $\mathbf{T}_i^{(k)}$ 的独立性. 于是有

$$\Pr\{\mathbf{T}_i^{(k)} = (a, b, c)\} = \begin{cases} \frac{1}{4}, & \text{如果 } (x_i \oplus a')(y_i \oplus b' \oplus c') = c' \text{ 成立,} \\ 0, & \text{如果 } (x_i \oplus a')(y_i \oplus b' \oplus c') = c' \text{ 不成立.} \end{cases} \quad (3.2)$$

设 $p_{i,t}^{(k)}$ 表示概率 $\Pr\{\mathbf{T}_i^{(k)} = (a, b, c)\}$, 这里 $t = c \cdot 2^2 + b \cdot 2 + a$. 对每个可能的 $(x_i, y_i, c_i^{(0)})$, 计算相应的 $p_{i,t}^{(k)}$, 表 2 给出具体的计算结果.

根据表 2 以及 $\mathbf{M}_i(T_i)$ 的取值及相应的取值条件, 对每个可能的 $(x_i, y_i, c_i^{(0)})$, 我们计算 $\mathbf{M}_i(T_i)$ 的概率分布, 具体结果见表 3.

通过计算, 我们发现 $\lambda_i(T_i)$ 的概率分布与 $(x_i, y_i, c_i^{(0)})$ 无关, 其概率分布在表 4 中给出.

引理 3 假设 n 个随机变量 $(\mathbf{a}_i^{(k)}, \mathbf{b}_i^{(k)})_{0 \leq i \leq n-1}$ 相互独立且服从均匀分布. 设随机变量 $\mathbf{r}_i^{(k)} = \mathbf{c}_i^{(0)} \oplus \mathbf{c}_i^{(k)} \oplus \mathbf{a}_i^{(k)} \oplus \mathbf{b}_i^{(k)}$, 这里 $0 \leq i < n$, 则随机变量 $(\mathbf{T}_i^{(k)})_{0 \leq i \leq n-2}$ 是独立的.

表 2 $p_{i,t}^{(k)}$ 与 $(x_i, y_i, c_i^{(0)})$ 之间的关系

$(x_i, y_i, c_i^{(0)})$	$p_{i,0}$	$p_{i,1}$	$p_{i,2}$	$p_{i,3}$	$p_{i,4}$	$p_{i,5}$	$p_{i,6}$	$p_{i,7}$
(0,0,0)	1/4	1/4	1/4	0	0	0	0	1/4
(0,0,1)	1/4	0	0	0	1/4	1/4	0	1/4
(0,1,0)	1/4	0	1/4	1/4	0	0	0	1/4
(0,1,1)	1/4	1/4	0	1/4	1/4	0	0	0
(1,0,0)	1/4	1/4	0	1/4	1/4	0	0	0
(1,0,1)	1/4	0	1/4	1/4	0	0	0	1/4
(1,1,0)	1/4	0	0	0	1/4	1/4	0	1/4
(1,1,1)	1/4	1/4	1/4	0	0	1/4	0	0

表 3 $(x_i, y_i, c_i^{(0)})$ 与 M_i 取值的概率

$(x_i, y_i, c_i^{(0)})$	$\begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
(0,0,0)	$\frac{1}{4^r}$	$\frac{2}{2^r} - \frac{2}{4^r}$	$\frac{1}{2^r} - \frac{1}{4^r}$	$\frac{4^r - 3 \cdot 2^r + 2}{4^r}$	0
(0,0,1)	$\frac{1}{4^r}$	0	$\frac{3}{2^r} - \frac{3}{4^r}$	0	$\frac{4^r - 3 \cdot 2^r + 2}{4^r}$
(0,1,0)	$\frac{1}{4^r}$	$\frac{2}{2^r} - \frac{2}{4^r}$	$\frac{1}{2^r} - \frac{1}{4^r}$	$\frac{4^r - 3 \cdot 2^r + 2}{4^r}$	0
(0,1,1)	$\frac{1}{4^r}$	$\frac{2}{2^r} - \frac{2}{4^r}$	$\frac{1}{2^r} - \frac{1}{4^r}$	$\frac{4^r - 3 \cdot 2^r + 2}{4^r}$	0
(1,0,0)	$\frac{1}{4^r}$	$\frac{2}{2^r} - \frac{2}{4^r}$	$\frac{1}{2^r} - \frac{1}{4^r}$	$\frac{4^r - 3 \cdot 2^r + 2}{4^r}$	0
(1,0,1)	$\frac{1}{4^r}$	$\frac{2}{2^r} - \frac{2}{4^r}$	$\frac{1}{2^r} - \frac{1}{4^r}$	$\frac{4^r - 3 \cdot 2^r + 2}{4^r}$	0
(1,1,0)	$\frac{1}{4^r}$	0	$\frac{3}{2^r} - \frac{3}{4^r}$	0	$\frac{4^r - 3 \cdot 2^r + 2}{4^r}$
(1,1,1)	$\frac{1}{4^r}$	$\frac{2}{2^r} - \frac{2}{4^r}$	$\frac{1}{2^r} - \frac{1}{4^r}$	$\frac{4^r - 3 \cdot 2^r + 2}{4^r}$	0

表 4 $\lambda_i(T_i)$ 的概率分布

$\lambda_i(T_i)$	1	2	4
概率	$\frac{4^r - 3 \cdot 2^r + 2}{4^r}$	$\frac{3}{2^r} - \frac{3}{4^r}$	$\frac{1}{4^r}$

证明 首先根据 $(a_{n-1}^{(k)}, b_{n-1}^{(k)})$ 与 $c_{n-1}^{(k)}$ 及 $(a_i^{(k)}, b_i^{(k)}, c_i^{(k)})_{0 \leq i \leq n-2}$ 相互独立, 有

$$\begin{aligned}
& \Pr\{a_i^{(k)} = a_i, b_i^{(k)} = b_i, c_i^{(k)} = c_i, 0 \leq i \leq n-1, \} \\
&= \Pr\{a_{n-1}^{(k)} = a_{n-1}, b_{n-1}^{(k)} = b_{n-1} \mid c_{n-1}^{(k)} = c_{n-1}, a_i^{(k)} = a_i, b_i^{(k)} = b_i, c_i^{(k)} = c_i, 0 \leq i \leq n-2\} \\
&\quad \times \Pr\{c_{n-1}^{(k)} = c_{n-1}, a_i^{(k)} = a_i, b_i^{(k)} = b_i, c_i^{(k)} = c_i, 0 \leq i \leq n-2\} \\
&= \frac{1}{4} \cdot \Pr\{c_{n-1}^{(k)} = c_{n-1}, a_i^{(k)} = a_i, b_i^{(k)} = b_i, c_i^{(k)} = c_i, 0 \leq i \leq n-2\}. \tag{3.3}
\end{aligned}$$

其次,

$$\begin{aligned}
& \Pr\{a_i^{(k)} = a_i, b_i^{(k)} = b_i, c_i^{(k)} = c_i, 0 \leq i \leq n-1\} \\
&= \Pr\{a_i^{(k)} = a_i, b_i^{(k)} = b_i, r_i^{(k)} = r_i, 0 \leq i \leq n-1\} \\
&= \frac{1}{4^n},
\end{aligned}$$

这里 $c_i = r_i \oplus a_i \oplus b_i \oplus c_i^{(0)}$. 于是,

$$\Pr\{c_{n-1}^{(k)} = c_{n-1}, a_i^{(k)} = a_i, b_i^{(k)} = b_i, c_i^{(k)} = c_i, 0 \leq i \leq n-2\} = \frac{1}{4^{n-1}} \text{ 或 } 0. \tag{3.4}$$

再次, 注意到 $c_0^{(k)}$ 恒为零, 于是有

$$\begin{aligned}
& \Pr\{c_{n-1}^{(k)} = c_{n-1}, a_i^{(k)} = a_i, b_i^{(k)} = b_i, c_i^{(k)} = c_i, 0 \leq i \leq n-2\} \\
&= \Pr\{a_i^{(k)} \oplus c_i^{(k)} = a_i \oplus c_i, b_i^{(k)} \oplus c_{i+1}^{(k)} = b_i \oplus c_{i+1}, c_i^{(k)} \oplus c_{i+1}^{(k)} = c_i \oplus c_{i+1}, 0 \leq i \leq n-2\}, \\
&= \Pr\{T_i^{(k)} = (a'_i, b'_i, c'_i), 0 \leq i \leq n-2\}, \tag{3.5}
\end{aligned}$$

这里

$$\begin{aligned}a'_i &= b_i \oplus r_i, \\b'_i &= b_i \oplus r_{i+1} \oplus a_{i+1} \oplus b_{i+1}, \\c'_i &= a_i \oplus a_{i+1} \oplus b_i \oplus b_{i+1} \oplus r_i \oplus r_{i+1}.\end{aligned}$$

根据等式 (3.1)、(3.2) 和 (3.4), 有

$$\Pr\{\mathbf{T}_i^{(k)} = (a'_i, b'_i, c'_i), 0 \leq i \leq n-2\} = \prod_{i=0}^{n-2} \Pr\{\mathbf{T}_i^{(k)} = (a'_i, b'_i, c'_i)\}.$$

这说明 $n-1$ 个随机变量 $(T_i^{(k)})_{0 \leq i \leq n-2}$ 是相互独立的, 命题成立. $\square$

设 $E_r(x, y, z)$ 表示方程系统 (1.1) 解个数的期望, 则有

$$E_r(x, y, z) = \sum_{\substack{(\alpha, \beta) \in \{0, 1\}^n \\ \gamma = F(x, y, z, \alpha, \beta)}} N(\alpha, \beta, \gamma) \Pr\{(\mathbf{a}^{(k)}, \mathbf{b}^{(k)}, \mathbf{r}^{(k)}) = (\alpha, \beta, \gamma)\},$$

这里 F 定义如下:

$$\begin{aligned}F &= (F_1, F_2, \dots, F_r), \\ \gamma^{(k)} &= F_k(x, y, z, \alpha, \beta), \\ F_k(x, y, z, \alpha, \beta) &= (x \oplus \alpha^{(k)}) \boxplus (y \oplus \beta^{(k)}) \oplus z, \quad k = 1, \dots, r.\end{aligned}$$

定理 2 设 r 个输入差分 $(\mathbf{a}^{(k)}, \mathbf{b}^{(k)})$ 是相互独立且均匀分布的随机变量. 令 $(x \oplus \mathbf{a}^{(k)}) \boxplus (y \oplus \mathbf{b}^{(k)}) = z \oplus \mathbf{r}^{(k)}$, 则

$$E_r(x, y, z) = 4 \times \left(1 + \frac{3}{2^r}\right)^{n-1}. \quad (3.6)$$

证明 根据 (3.3) 和 (3.5), 有

$$E_r(x, y, z) = \sum_{\substack{\alpha_{n-1} \in \mathbb{F}_2^r \\ \beta_{n-1} \in \mathbb{F}_2^r}} \sum_{\substack{T_i \in S(x_i, y_i, c_i^{(0)}) \\ 0 \leq i \leq n-2}} 4 \times \prod_{i=0}^{n-2} \lambda_i(T_i) \frac{1}{4} \Pr\{\mathbf{T}_i = T_i, 0 \leq i \leq n-2\}.$$

上述表达式中 $S(x_i, y_i, c_i^{(0)}) = 0$ 表示 T_i 的可能取值, 这里

$$\begin{aligned}T_i &= (T_i^{(1)}, T_i^{(2)}, \dots, T_i^{(r)}), \\ T_i^{(k)} &= (a_i^{(k)}, b_i^{(k)}, c_i^{(k)}), \\ a_i^{(k)} &= \beta_i^{(k)} \oplus \gamma_i^{(k)}, \\ b_i^{(k)} &= \beta_i^{(k)} \oplus \alpha_{i+1}^{(k)} \oplus \beta_{i+1}^{(k)} \oplus \gamma_{i+1}^{(k)}, \\ c_i^{(k)} &= \alpha_i^{(k)} \oplus \beta_i^{(k)} \oplus \gamma_i^{(k)} \oplus \alpha_{i+1}^{(k)} \oplus \beta_{i+1}^{(k)} \oplus \gamma_{i+1}^{(k)},\end{aligned}$$

且它们满足

$$(x_i \oplus c_i^{(0)} \oplus a_i^{(k)})(y_i \oplus c_i^{(0)} \oplus b_i^{(k)} \oplus c_i^{(k)}) = c_i^{(0)} \oplus c_{i+1}^{(0)} \oplus c_i^{(k)}.$$

根据引理 3 和 $\lambda_i(T_i)$ 的概率分布, 有

$$\begin{aligned}
 E_r(x, y, z) &= 4 \times \sum_{T_0 \in S(x_0, y_0, c_0^{(0)})} \cdots \sum_{T_{n-2} \in S(x_{n-2}, y_{n-2}, c_{n-2}^{(0)})} \prod_{i=0}^{n-2} \lambda_i(T_i) \Pr\{T_i = T_i\} \\
 &= 4 \times \prod_{i=0}^{n-2} \sum_{T_i \in S(x_i, y_i, c_i^{(0)})} \lambda_i(T_i) \Pr\{T_i = T_i\} \\
 &= 4 \times \prod_{i=0}^{n-2} \left(4 \cdot \frac{1}{4^r} + 2 \cdot \left(\frac{3}{2^r} - \frac{2}{4^r} \right) + \frac{4^r - 3 \cdot 2^r + 2}{4^r} \right) \\
 &= 4 \times \prod_{i=0}^{n-2} \left(1 + \frac{3}{2^r} \right) \\
 &= 4 \times \left(1 + \frac{3}{2^r} \right)^{n-1}.
 \end{aligned}$$

于是命题成立. $\square$

从定理 2 可以看出, 方程系统 (1.1) 解个数的期望与方程系统具体的解是无关的, 换句话说, 也就是与产生该方程系统的密码系统所采用的密钥无关. 在实际密码分析中, 我们总是希望在能够获得方程系统确切解的条件下故障注入的次数越少越好. 方程系统 (1.1) 如果有解, 则其最高比特的解不能唯一确定, 因此, 我们希望除了最高比特位 x_{n-1} 、 y_{n-1} 和 z_{n-1} 外其他比特位总是有唯一解. 下面的定理揭示了在除最高比特位之外其他比特位有唯一解时故障注入次数 r 与 n 之间的关系. 据此可知, 在平均意义下, 我们只需注入大约 $\log_2(n) + 5$ 个故障便可以确定方程系统 (1.1) 的候选解.

定理 3 当 $r \geq \log_2(n) + 5$ 时, 有 $E_r(x, y, z) < 5$.

证明 假设 $x < 1$ 且 $mx < 1$, 则下面的不等式成立:

$$(1+x)^m = 1 + \sum_{i=1}^m \binom{m}{i} x^i < 1 + mx \sum_{i=1}^m \frac{1}{i!} < 1 + 2mx. \quad (3.7)$$

于是, 当 $r \geq \log_2(n) + 5$ 时, 有 $\frac{3(n-1)}{2^r} < 1$. 利用不等式 (3.7), 可得

$$E_r(x, y, z) = 4 \left(1 + \frac{3}{2^r} \right)^{n-1} < 4 + 8(n-1) \frac{3}{2^r} < 5.$$

故命题成立. $\square$

下面讨论方程系统 (1.1) 解个数的方差, 即

$$V_r(x, y, z) = \sum_{\substack{\alpha, \beta \in \{0,1\}^n \\ \gamma = F(x, y, z, \alpha, \beta)}} N^2(\alpha, \beta, \gamma) \Pr\{\mathbf{a} = \alpha, \mathbf{b} = \beta, \mathbf{r} = \gamma\} - E_r^2(x, y, z). \quad (3.8)$$

根据定理 2, 我们下面的定理:

定理 4 设 $(\mathbf{a}^{(k)}, \mathbf{b}^{(k)})$ 是 r 个相互独立且服从均匀分布的随机变量, 且 $(x \oplus \mathbf{a}^{(k)}) \oplus (y \oplus \mathbf{b}^{(k)}) = z \oplus \mathbf{r}^{(k)}$, 这里 $k = 1, 2, \dots, r$, 则

$$V_r(x, y, z) = 16 \times \left(1 + \frac{9}{2^r} + \frac{6}{4^r} \right)^{n-1} - 16 \times \left(1 + \frac{6}{2^r} + \frac{9}{4^r} \right)^{n-1}.$$

证明 根据表达式 (3.8), 我们只需要计算 $V_r(x, y, z)$ 的第一项, 即

$$\begin{aligned}
 & \sum_{\substack{\alpha, \beta \in \{0, 1\}^n \\ \gamma = F(x, y, z, \alpha, \beta)}} N^2(\alpha, \beta, \gamma) \Pr\{\mathbf{A} = \alpha, \mathbf{B} = \beta, \mathbf{R} = \gamma\} \\
 &= \sum_{\substack{\alpha_{n-1} \in \mathbb{F}_2^r \\ \beta_{n-1} \in \mathbb{F}_2^r}} \sum_{\substack{T_i \in S(x_i, y_i, c_i^{(0)}) \\ 0 \leq i \leq n-2}} 4^2 \prod_{i=0}^{n-2} \lambda_i^2(T_i) \Pr\{\mathbf{T}_i = T_i, 0 \leq i \leq n-2\} \\
 &= 16 \times \prod_{i=0}^{n-2} \sum_{T_i \in S(x_i, y_i, c_i^{(0)})} \lambda_i^2(T_i) \Pr\{\mathbf{T}_i = T_i\} \\
 &= 16 \times \prod_{i=0}^{n-2} \left(16 \cdot \frac{1}{4^r} + 4 \cdot \left(\frac{3}{2^r} - \frac{3}{4^r} \right) + \frac{4^r - 3 \cdot 2^r + 2}{4^r} \right) \\
 &= 16 \times \left(1 + \frac{9}{2^r} + \frac{6}{4^r} \right)^{n-1}.
 \end{aligned}$$

于是,

$$V_r(x, y, z) = 16 \times \left(1 + \frac{9}{2^r} + \frac{6}{4^r} \right)^{n-1} - 16 \times \left(1 + \frac{6}{2^r} + \frac{9}{4^r} \right)^{n-1}.$$

证毕. □

参考文献

- 1 Rivest R. The MD5 message-digest algorithm. <https://tools.ietf.org/pdf/rfc1321.pdf>, 1992
- 2 ETSI/SAGE. Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 2: SNOW 3G Specification, Version 1.1 (September 2006), 2006
- 3 Beaulieu R, Shors D, Smith J, et al. The Simon and Speck Families of Lightweight Block Ciphers. IACR Cryptology ePrint Archive 2013/404. <http://eprint.iacr.org/>, 2013
- 4 ETSI/SAGE TR 35.924. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 4: Design and Evaluation Report, 2006
- 5 Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. In: Advances in Cryptology-CRYPTO'90. Lecture Notes in Computer Science, vol. 537. Heidelberg: Springer-Verlag, 1991, 3-72
- 6 Wu H, Nguyen P H, Wang H, et al. Cryptanalysis of the Stream Cipher ZUC in the 3GPP Confidentiality & Integrity Algorithms 128-EEA3 & 128-EIA3. Singapore: Rump Session of Asiacrypt, 2010
- 7 Berson T A. Differential cryptanalysis mod 2^{32} with applications to MD5. In: Advances in Cryptology-EUROCRYPT'92. Lecture Notes in Computer Science, vol. 658. Heidelberg: Springer-Verlag, 1992, 71-80
- 8 Wagner D. The boomerang attack. In: Proceedings of the 6th International Workshop, FSE'99. Lecture Notes in Computer Science, vol. 1636. Heidelberg: Springer-Verlag, 1999, 156-179
- 9 Biham E, Dunkelman O, Keller N. The rectangle attack—Rectangling the serpent. In: Advances in Cryptology-EUROCRYPT'01. Lecture Notes in Computer Science, vol. 2045. Heidelberg: Springer-Verlag, 2001, 340-357
- 10 Biham E, Shamir A. Differential fault analysis of secret key cryptosystems. In: CRYPTO'97. Heidelberg: Springer-Verlag, 1999, 1294: 513-525
- 11 Debraize B, Marquez I. Fault analysis of the stream cipher snow 3G. In: Workshop on Fault Diagnosis and Tolerance in Cryptography-FDTC 2009. Lausanne: IEEE, 2009, 103-110
- 12 Harshal T, Shikha B, Debdeep M. Differential fault analysis on the families of simon and speck ciphers. In: Workshop on Fault Diagnosis and Tolerance in Cryptography-FDTC 2014. Busan: IEEE, 2014, 40-48
- 13 Huo Y, Zhang F, Feng X, et al. Improved differential fault attack on the block cipher SPECK. In: Fault Diagnosis and Tolerance in Cryptography-FDTC 2015. Saint Malo: IEEE, 2015, 28-34
- 14 Mouha N, Velichkov V, Cannière C D, et al. The differential analysis of S-functions. In: Selected Areas in Cryptography 2010. Heidelberg-Berlin: Springer, 2010, 6544: 36-56

附录 A

本附录主要给出 $U(\mathbf{c}_i, \mathbf{c}_{i+1})$ 和 $\mathbf{M}_i(T_i)$ 的取值条件.

定义集合

$$S_E = \{k = 1, \dots, r; c_i^{(k)} \oplus c_{i+1}^{(k)} = c_i^{(0)} \oplus c_{i+1}^{(0)}\},$$

$$S_N = \{k = 1, \dots, r; c_i^{(k)} \oplus c_{i+1}^{(k)} \neq c_i^{(0)} \oplus c_{i+1}^{(0)}\}.$$

于是,

(1) $U(\mathbf{c}_i^0, \mathbf{c}_{i+1}^0) = U(\mathbf{c}_i^1, \mathbf{c}_{i+1}^1) \in \{0, 1, 2, 3\}$, 则

(i) $U(\mathbf{c}_i^0, \mathbf{c}_{i+1}^0) = 3$, 此时满足的条件是 $T_i^{(k)} = (0, 0, 0)$, $\forall k = 1, \dots, r$.

(ii) $U(\mathbf{c}_i^0, \mathbf{c}_{i+1}^0) = 2$, 此时满足的条件是

$$\begin{aligned} & \bigcup_{k=1}^r \{T_i^{(k)}\} \cup \{(0, 0, 0)\} = \{(0, 0, 0), (0, 1, 0)\}, \\ \text{或} & \bigcup_{k=1}^r \{T_i^{(k)}\} \cup \{(0, 0, 0)\} = \{(0, 0, 0), (1, 0, 0)\}, \\ \text{或} & \bigcup_{k=1}^r \{T_i^{(k)}\} \cup \{(0, 0, 0)\} = \{(0, 0, 0), (1, 1, 0)\}. \end{aligned}$$

(iii) $U(\mathbf{c}_i^0, \mathbf{c}_{i+1}^0) = 1$, 此时满足的条件是分为两种:

$$\begin{aligned} & \bigcup_{k=1}^r \{T_i^{(k)}\} \cup \{0, 0, 0\} = \{(0, 0, 0), (0, 1, 0), (1, 0, 0)\}, \\ \text{或} & \bigcup_{k=1}^r \{T_i^{(k)}\} \cup \{0, 0, 0\} = \{(0, 0, 0), (1, 0, 0), (1, 1, 0)\}, \\ \text{或} & \bigcup_{k=1}^r \{T_i^{(k)}\} \cup \{0, 0, 0\} = \{(0, 0, 0), (1, 1, 0), (0, 1, 0)\}; \end{aligned}$$

或者 $S_N \neq \emptyset$, 且

$$\begin{aligned} T_i^{(k)} &= (\mathbf{e}, 1), \quad \forall k \in S_N, \\ T_i^{(k)} &\in \{(\mathbf{e}, 0), (\mathbf{e} \oplus (1, 0), 0), (\mathbf{e} \oplus (1, 1), 0)\}, \quad \forall k \in S_E, \end{aligned}$$

这里 $\mathbf{e} \in \{(0, 0), (1, 0), (1, 1)\}$.

(2) $U(\mathbf{c}_i^0, \mathbf{c}_{i+1}^1) = U(\mathbf{c}_i^1, \mathbf{c}_{i+1}^0) \in \{0, 1\}$. 当 $U(\mathbf{c}_i^0, \mathbf{c}_{i+1}^1) = 1$ 时, 满足的条件是

$$\begin{aligned} T_i^{(k)} &= (0, 0, 0), \quad \forall k \in S_E, \\ T_i^{(k)} &= \{(0, 0, 1), (1, 0, 1), (1, 1, 1)\}, \quad \forall k \in S_N. \end{aligned}$$

接下来介绍 $\mathbf{M}_i(T_i)$ 的取值条件:

- (1) 当 $M_i(T_i) = (\begin{smallmatrix} 3 & 1 \\ 1 & 3 \end{smallmatrix})$, 要求的条件是 $T_i^{(k)} = (0, 0, 0), \forall k = 1, \dots, r$.
- (2) 当 $M_i(T_i) = (\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix})$, 要求的条件是 $\bigcup_{k=1}^r \{T_i^{(k)}\} \cup \{(0, 0, 0)\} = \{(0, 0, 0), (0, 1, 0)\}$ 或 $\bigcup_{k=1}^r \{T_i^{(k)}\} \cup \{(0, 0, 0)\} = \{(0, 0, 0), (1, 0, 0)\}$ 或 $\bigcup_{k=1}^r \{T_i^{(k)}\} \cup \{(0, 0, 0)\} = \{(0, 0, 0), (1, 1, 0)\}$.
- (3) 当 $M_i(T_i) = (\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix})$, 此时要求 $S_N \neq \emptyset$, 且 $T_i^{(k)} = (0, 0, 0), \forall k \in S_E; T_i^{(k)} = (e, 1), \forall k \in S_N$, 这里 $e \in \{(0, 0), (1, 0), (1, 1)\}$.
- (4) 当 $M_i(T_i) = (\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix})$, 此时的条件有以下两种:
- (i) $\bigcup_{k=1}^r \{T_i^{(k)}\} \cup \{(0, 0, 0)\} = \{(0, 0, 0), (0, 1, 0), (1, 0, 0)\}$ 或 $\bigcup_{k=1}^r \{T_i^{(k)}\} \cup \{(0, 0, 0)\} = \{(0, 0, 0), (1, 0, 0), (1, 1, 0)\}$ 或 $\bigcup_{k=1}^r \{T_i^{(k)}\} \cup \{(0, 0, 0)\} = \{(0, 0, 0), (0, 1, 0), (1, 1, 0)\}$;
- (ii) $S_E \neq \emptyset$ 和 $S_N \neq \emptyset$, 且 $\{(0, 0, 0)\} \subsetneq (\bigcup_{k \in S_E} T_i^{(k)}) \subseteq \{(e, 0), (e \oplus (1, 0), 0), (e \oplus (1, 1), 0)\}, T_i^{(k)} = (e, 1), \forall k \in S_N$, 这里 $e \in \{(0, 0), (1, 0), (1, 1)\}$.
- (5) 当 $M_i(T_i) = (\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix})$, 此时要求 $S_N \neq \emptyset$, 且 $T_i^{(k)} = (0, 0, 0), \forall k \in S_E, \bigcup_{k \in S_N} T_i^{(k)} \subset \{(0, 0, 1), (1, 0, 1), (1, 1, 1)\}$ 且至少两个元素在该集合中.

The expectation and variance of the number of solutions of a class of differential system of modular addition

FENG XiuTao, ZHANG Fan & HUANG Shen

Abstract The modular addition is an important nonlinear operation in symmetric ciphers, and has been widely used in the design of cryptographic primitives, such as MD5, SNOW 3G, SPECK, ZUC and so on. Differential fault attack is a general cryptanalytic method for cipher implementations with the assumption that an adversary is able to inject faults into the registers on the fly. A differential equation system of modular addition (DESMA, in short) is usually deduced during differential fault cryptanalysis of these ciphers. In this paper we present the relationship between the number of solutions of the DESMA and the number of injected faults, and give their expectation and variance. Our result shows that about $\log_2(n) + 5$ faults are required to determine the candidate solutions of the DESMA.

Keywords modular addition, differential fault attack, differential system, expectation, variance

MSC(2010) 94A60

doi: 10.1360/N012017-00115