基于最优区分器的多差分密码分析方法

高海英 金晨辉
(解放军信息工程大学 郑州 450001)

摘 要 如何利用多个差分特征对分组密码算法进行差分攻击,从而精确地估计出分组密码算法抵抗差分攻击的能力,是一个重要的研究课题.文中基于最优区分器的思想,提出了一种多差分密码分析方法.针对每个实验密钥,构造出基于多个差分特征的统计量,根据统计量的大小判决实验密钥是否为正确密钥.给出了多差分分析方法的计算复杂度,分析了正确密钥、错误密钥对应统计量的概率分布规律,并在此基础上给出了多差分分析方法的成功率和数据复杂度之间的关系.通过具体实例表明,在成功率相同的条件下,基于的差分特征越多,需要的数据复杂度越小.

关键词 分组密码;最优区分器;多差分密码分析;差分特征;成功率;密码学
中图法分类号 TN918 **DOI号** 10.3724/SP.J.1016.2015.00814

Multiple Differential Cryptanalysis Based on Optimal Distinguisher

GAO Hai-Ying JIN Chen-Hui
(*PLA Information Engineering University, Zhengzhou* 450001)

Abstract It is an important research topic to attack a block cipher using multiple differentials for exactly estimating the resistibility against differential cryptanalysis. In this paper, a multiple differential cryptanalysis method is proposed based on optimal distinguisher. For each experimental key, a statistic is constructed using multiple differentials, and thus we determine whether the experimental key is correct according to the statistics. We analyze the computational complexity of multiple differential cryptanalysis, the probability distribution of statistics corresponding correct key and incorrect key, and give the relation of success probability and data complexity. Example shows that the data complexity is decreased with more differentials in multiple differential cryptanalysis under the condition of same success probability.

Keywords block cipher; optimal distinguisher; multiple differential cryptanalysis; differential characteristic; success probability; cryptography

1 引 言

差分密码分析方法是Biham和Shamir[1]在1990年欧洲密码年会上提出的一种对迭代型分组密码算法的选择明文攻击方法.其基本思想是利用分组密码算法的差分统计量分布的不平衡性这个信息泄漏特点,构造出一个或几个具有较高转移概率的差分特征,对最后一圈的若干密钥比特进行攻击.利用该方法已成功攻击了多个分组密码算法[2-5],并扩展出一系列不同的差分分析方法,例如截断差分和高阶差分分析[6]、不可能差分分析[7]、条件差分分析方法[8]等.

文献[1]的差分分析方法只使用了一个差分特

收稿日期:2013-07-01;最终修改稿收到日期:2014-10-31.本课题得到国家密码发展基金(MMJJ201401002)、国家自然科学基金(61272488,61272041,61202491)资助.**高海英**,女,1978年生,博士,副教授,主要研究方向为密码理论.E-mail:ghyyueyue@126.com.**金晨辉**,男,1965年生,博士,教授,博士生导师,主要研究领域为密码理论和信息安全.

征，如何综合利用多个差分特征对算法进行攻击？为了解决该问题，Biham 和 Shamir[9] 提出了综合利用多个具有相同输出差分的差分特征的差分分析方法；Knudsen[6] 提出了截断差分分析方法，但是该方法要求输出差分必须构成一个线性空间. 2011 年，Blondeau 等人[10] 提出了具有普适性的多差分攻击方法，该方法综合利用了多个输入差分、多个输出差分的差分特征（差分特征中的输入差分和输出差分没有特殊要求），但是，文章构造的统计量没有利用最优区分的思想，给出的多差分分析方法不是最优的，即没有最大限度地利用差分特征分布不均匀性这个信息泄漏特点. 为了给出最优的多差分攻击方法，2012 年 Blondeau 等人[11] 提出了针对单个输入差分、多个输出差分情况的多差分攻击方法，并给出了任意成功率条件下的数据复杂度的计算公式，但文中没有针对多个输入差分、多个输出差分的情况提出攻击方法.

针对多个输入差分、多个输出差分的情况，如何设计多差分分析方法？为了解决该问题，本文基于最优区分器的思想和策略提出了一种多差分分析方法，并给出了任意成功率条件下的数据复杂度的计算公式. 在已知数据量的条件下，给出了成功率为 1 时，候选密钥量的个数的期望值. 最后，通过具体实例得出：在成功率相等的条件下，利用的差分特征越多，攻击所需的数据复杂度就越小.

本文第 2 节简要介绍最优区分器；第 3 节介绍基于最优区分器的多差分密码分析方法；第 4 节对多差分分析方法的各项性能指标进行分析；第 5 节给出了多差分密码分析方法的一个具体应用；最后一节对全文进行总结和展望.

2　最优区分器

由于文章给出的多差分密码分析方法是基于最优区分器的思想提出的，因此，本节首先介绍最优区分器.

设一条序列 $\bar{s}=\{s_i\}_{i=1}^{n}$，$s_i\in F_2^m$，且 s_i 是独立同分布的，并且若 s_i 服从 D_0 分布，则对于 $\forall a\in F_2^m$，令 $Pr_{D_0}[a]=Pr_{D_0}[s_i=a]=p_a$；若 s_i 服从 D_1 分布，令 $Pr_{D_1}[a]=Pr_{D_1}[s_i=a]=1/2^m$.

区分器是一种判定算法，该算法的目的是在已知上述条件的前提下，给出 s_i 服从何种分布（D_0 或 D_1）的判定结果. 所谓最优区分器，即使得区分优势达到最大的判定算法，文献[12]基于后验概率的思想提出了一种最优区分器，现将该区分器描述如下.

最优区分器.

输入：一条 n 长序列 $\bar{s}=\{s_i\}_{i=1}^{n}$，$s_i\in F_2^m$

输出：若输出 0，则判定 $\bar{s}$ 服从 D_0 分布；若输出 1，则判定 $\bar{s}$ 服从 D_1 分布

1. 计算 LLR(Logarithmic Likelihood Ratio)统计量：

$$LLR(\bar{s})=\sum_{a\in F_2^m}N(a|\bar{s})\log\frac{Pr_{D_0}[a]}{Pr_{D_1}[a]}\tag{1}$$

其中 $N(a|\bar{s})$ 表示序列 $\bar{s}$ 中 a 的个数.

2. 输出判定结果 $A(\bar{s})$：

$$A(\bar{s})=\begin{cases}0, & \text{当 } LLR(\bar{s})>0\\ 1, & \text{其他}\end{cases}.$$

文献[12]定义了区分器的区分优势为

$$\begin{aligned}Adv(A(\bar{s}))&=Pr_{D_0}[A(\bar{s})=0]-Pr_{D_1}[A(\bar{s})=0]\\&=1-2P_e,\end{aligned}$$

其中，$P_e=\frac{1}{2}(\alpha_1+\alpha_2)$，$\alpha_1$ 是将 $\bar{s}$ 服从 D_0 分布判断为服从 D_1 分布的错误概率，α_2 是将 $\bar{s}$ 服从 D_1 分布判断为服从 D_0 分布的错误概率.

给出区分优势的计算公式为

$$Adv(A(\bar{s}))=1-2\phi\left(-\frac{\sqrt{n\cdot\Delta(D_0)}}{2}\right),$$

其中

$$\Delta(D_0)=\sum_{a\in F_2^m}\frac{(Pr_{D_0}[a]-Pr_{D_1}[a])^2}{Pr_{D_1}[a]},$$

$$\phi(x)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x}e^{-\frac{u^2}{2}}du.$$

并且证明了上述区分器是最优区分器.

3　多差分密码分析方法

3.1　相关定义

令 E 表示一个 r 圈迭代型分组密码算法，该算法的密钥是 K，分组规模是 m 比特，K_r 是第 r 圈子密钥，F 表示圈函数. 设明文空间为 X，密文空间是 Y. 对于任意明文分组 $x\in X$，相应的密文表示为 $y=E_K(x)$，其中 $E_K(x)=F_{K_r}\circ\cdots\circ F_{K_1}(x)$.

下面介绍与多差分密码分析方法相关的定义.

定义 1.　设 (δ_0,δ_{r-1}) 是分组密码算法 E 的 $(r-1)$ 圈差分特征，该差分特征的概率定义为

$$Pr[\delta_0\to\delta_{r-1}]=$$
$$Pr_{X,K}[F_{K_r}^{-1}(E_K(X))\oplus F_{K_r}^{-1}(E_K(X\oplus\delta_0))=\delta_{r-1}].$$

一般情况下，当 K_r 是错误密钥时，$Pr[\delta_0\to\delta_{r-1}]=2^{-m}$.

针对分组密码算法 E，假设攻击者找到了多个

具有较大概率的$(r-1)$圈差分特征，这些差分特征构成集合 $\Delta=\{(\delta_0^{(i)},\delta_{r-1}^{(i,j)})\mid i=1\cdots|\Delta_0|,j=1,\cdots,|\Delta_{r-1}^{(i)}|\}$，令其中输入差分构成的集合为 Δ_0，$\Delta_0\overset{\text{def}}{=}\{\delta_0,\exists\delta_{r-1},(\delta_0,\delta_{r-1})\in\Delta\}=\{\delta_0^{(1)},\cdots,\delta_0^{(|\Delta_0|)}\}$，针对 Δ_0 中的每个输入差分 $\delta_0^{(i)}$，将对应的输出差分集合记为 $\Delta_{r-1}^{(i)}\overset{\text{def}}{=}\{\delta_{r-1}\mid(\delta_0^{(i)},\delta_{r-1})\in\Delta\}=\{\delta_{r-1}^{(i,1)},\cdots,\delta_{r-1}^{(i,|\Delta_{r-1}^{(i)}|)}\}$.

下面介绍本文提出的多差分密码分析方法.

3.2 基于最优区分器的多差分密码分析

假设$|\Delta_0|=1$，即 Δ 中输入差分只有一种，记为 $\delta_0^{(i)}$，其对应的输出差分记为 $\delta_{r-1}^{(i)}$. 假设当 K_r 是正确圈子密钥时，$\delta_{r-1}^{(i)}$ 服从 D_0 分布；当 K_r 是错误圈子密钥时，$\delta_{r-1}^{(i)}$ 服从 D_1 分布. 因此，判定实验密钥 K_r 是否是正确圈子密钥等价于区分 $\delta_{r-1}^{(i)}$ 服从 D_0 分布或 D_1 分布.

依此类推，针对$|\Delta_0|>1$ 的情况，假设当 K_r 是正确圈子密钥时，输出差分构成的向量$(\delta_{r-1}^{(1)},\delta_{r-1}^{(2)},\cdots,\delta_{r-1}^{(|\Delta_0|)})$服从 $\overline{D}_0$ 分布；当 K_r 是错误圈子密钥时，$(\delta_{r-1}^{(1)},\delta_{r-1}^{(2)},\cdots,\delta_{r-1}^{(|\Delta_0|)})$服从$\overline{D}_1$分布. 因此，判定实验密钥 K_r 是否是正确圈子密钥等价于区分$(\delta_{r-1}^{(1)},\delta_{r-1}^{(2)},\cdots,\delta_{r-1}^{(|\Delta_0|)})$服从$\overline{D}_0$分布或$\overline{D}_1$分布.

利用最优区分器判决 $\delta_{r-1}^{(i)}$ 服从 D_0 或 D_1 分布，需要计算统计量 $LLR^{(i)}$. 同理，为了区分$(\delta_{r-1}^{(1)},\delta_{r-1}^{(2)},\cdots,\delta_{r-1}^{(|\Delta_0|)})$服从$\overline{D}_0$或$\overline{D}_1$分布，需要计算统计量 $\overline{LLR}$. 下面分别介绍 $LLR^{(i)}(i=1\cdots|\Delta_0|)$和$\overline{LLR}$的构造方法.

首先假设当 K_r 是正确圈子密钥时，$\delta_{r-1}^{(i)}$ 服从 D_0 分布，具体描述如下：

(1) $\forall j\in\{1,2,\cdots,|\Delta_{r-1}^{(i)}|\}$，$Pr_{D_0}[\delta_{r-1}^{(i)}=\delta_{r-1}^{(i,j)}]=p^{(i,j)}$，且 $p^{(i,j)}$ 是已知的；

(2) $\forall\beta\in F_2^m$，且 $\beta\notin\Delta_{r-1}^{(i)}$，$Pr_{D_0}[\delta_{r-1}^{(i)}=\beta]=\left(1-\sum_{1\le j\le|\Delta_{r-1}^{i}|}p^{(i,j)}\right)/(2^m-|\Delta_{r-1}^{(i)}|)$，为描述方便，令 w_i 表示$\left(1-\sum_{1\le j\le|\Delta_{r-1}^{i}|}p^{(i,j)}\right)/(2^m-|\Delta_{r-1}^{(i)}|)$.

同时假设当 K_r 是错误圈子密钥时，$\delta_{r-1}^{(i)}$ 服从 D_1 分布：$\forall\beta\in F_2^m$，$Pr_{D_1}[\delta_{r-1}^{(i)}=\beta]=2^{-m}$.

假设 $\delta_{r-1}^{(i)}(i=1\cdots|\Delta_0|)$是相互独立的，令 $\delta_{r-1}=(\delta_{r-1}^{(1)},\delta_{r-1}^{(2)},\cdots,\delta_{r-1}^{(|\Delta_0|)})$，则可以计算出：

$\forall(\gamma_1,\cdots,\gamma_{|\Delta_0|})\in(F_2^m)^{|\Delta_0|}$，

$$Pr_{D_0}[\delta_{r-1}=(\gamma_1,\cdots,\gamma_{|\Delta_0|})]=\prod_{i=1}^{|\Delta_0|}Pr_{D_0}[\delta_{r-1}^{i}=\gamma_i],$$

$$Pr_{\overline{D}_1}[\delta_{r-1}=(\gamma_1,\cdots,\gamma_{|\Delta_0|})]=\prod_{i=1}^{|\Delta_0|}Pr_{D_1}[\delta_{r-1}^{(i)}=\gamma_i].$$

已知 M 个明文对$\{(x_k,x_k\oplus\delta_0^{(i)})\}_{k=1}^M(i\in\{1,\cdots,|\Delta_0|\})$，以及对应的密文对$\{(y_k,y_k')\}_{k=1}^M$，设第 r 圈的子密钥 K_r 有 2^{n_k} 个可能值，记为 $K_r^t(1\le t\le 2^{n_k})$，利用实验密钥 $K_r^t(1\le t\le 2^{n_k})$解密$\{(y_k,y_k')\}_{k=1}^M$，得到$\{(z_k,z_k')\}_{k=1}^M$，令序列$\overline{\delta_{r-1}^{(i)}(K_r^t)}=\{z_k\oplus z_k'\}_{k=1}^M,i\in\{1,\cdots,|\Delta_0|\}$.

根据式(1)，基于差分特征$(\delta_0^{(i)},\delta_{r-1}^{(i,1)})$，$(\delta_0^{(i)},\delta_{r-1}^{(i,2)})$，$\cdots$，$(\delta_0^{(i)},\delta_{r-1}^{(i,|\Delta_{r-1}^{(i)}|)})$构造的统计量 $LLR^{(i)}(\overline{\delta_{r-1}^{(i)}(K_r^t)})$如下所示：

$$\begin{aligned}LLR^{(i)}(\overline{\delta_{r-1}^{(i)}(K_r^t)})&=\sum_{a\in F_2^m}N(a\mid\overline{\delta_{r-1}^{(i)}(K_r^t)})\log\frac{Pr_{D_0}[a]}{Pr_{D_1}[a]}\\&=\sum_{a\in\Delta_{r-1}^{(i)}}N(a\mid\overline{\delta_{r-1}^{(i)}(K_r^t)})\log\frac{Pr_{D_0}[a]}{Pr_{D_1}[a]}+\\&\quad\sum_{a\notin\Delta_{r-1}^{(i)}}N(a\mid\overline{\delta_{r-1}^{(i)}(K_r^t)})\log\frac{Pr_{D_0}[a]}{Pr_{D_1}[a]}\\&=\sum_{\delta_{r-1}^{(i,j)}\in\Delta_{r-1}^{(i)}}N(\delta_{r-1}^{(i,j)}\mid\overline{\delta_{r-1}^{(i)}(K_r^t)})\log\frac{p^{(i,j)}}{2^{-m}}+\\&\quad\left(M-\sum_{\delta_{r-1}^{(i,j)}\in\Delta_{r-1}^{(i)}}N(\delta_{r-1}^{(i,j)}\mid\overline{\delta_{r-1}^{(i)}(K_r^t)})\right)\cdot\log\frac{w_i}{2^{-m}}\end{aligned}\quad(2)$$

下面分析如何利用集合 Δ 中的所有差分特征构造相应的统计量$\overline{LLR}$.

设$|\Delta_0|+1$ 个明文$(x_k,x_k\oplus\delta_0^{(1)},x_k\oplus\delta_0^{(2)},\cdots,x_k\oplus\delta_0^{(|\Delta_0|)})$构成一个明文向量，已知 M 个明文向量构成的向量序列$\{(x_k,x_k\oplus\delta_0^{(1)},x_k\oplus\delta_0^{(2)},\cdots,x_k\oplus\delta_0^{(|\Delta_0|)})\}_{k=1}^M$，以及相应的密文向量序列$\{(y_k,y_k^{(1)},\cdots,y_k^{(|\Delta_0|)})\}_{k=1}^M$. 利用实验密钥 $K_r^t(1\le t\le 2^{n_k})$解密$\{(y_k,y_k^{(1)},\cdots,y_k^{(|\Delta_0|)})\}_{k=1}^M$，得到$\{(z_k,z_k^{(1)},\cdots,z_k^{(|\Delta_0|)})\}_{k=1}^M$，计算得出

$$\{(z_k\oplus z_k^{(1)},z_k\oplus z_k^{(2)},\cdots,z_k\oplus z_k^{(|\Delta_0|)})\}_{k=1}^M,$$

令序列$\overline{\delta_{r-1}(K_r^t)}=\{(z_k\oplus z_k^{(1)},z_k\oplus z_k^{(2)},\cdots,z_k\oplus z_k^{(|\Delta_0|)})\}_{k=1}^M$.

根据式(1)可得

$$\begin{aligned}\overline{LLR}(\overline{\delta_{r-1}(K_r^t)})&=\sum_{\gamma\in(F_2^m)^{|\Delta_0|}}N(\gamma\mid\overline{\delta_{r-1}(K_r^t)})\log\frac{Pr_{\overline{D}_0}[\gamma]}{Pr_{\overline{D}_1}[\gamma]}\\&=\sum_{(\gamma_1,\cdots,\gamma_{|\Delta_0|})\in(F_2^m)^{|\Delta_0|}}N((\gamma_1,\cdots,\gamma_{|\Delta_0|})\mid\overline{\delta_{r-1}(K_r^t)})\cdot\\&\quad\log\left(\frac{Pr_{D_0}[\gamma_1]}{2^{-m}}\right)+\\&\quad\sum_{(\gamma_1,\cdots,\gamma_{|\Delta_0|})\in(F_2^m)^{|\Delta_0|}}N((\gamma_1,\cdots,\gamma_{|\Delta_0|})\mid\overline{\delta_{r-1}(K_r^t)})\cdot\end{aligned}$$

$$\log\left(\frac{Pr_{D_0}[\gamma_2]}{2^{-m}}\right)+\cdots+\sum_{(\gamma_1,\cdots,\gamma_{|\Delta_0|})\in(F_2^m)^{|\Delta_0|}}N((\gamma_1,\cdots,\gamma_{|\Delta_0|})|\overline{\delta_{r-1}(K_r^t)})\cdot\log\left(\frac{Pr_{D_0}[\gamma_{|\Delta_0|}]}{(2^{-m})}\right)$$

$$=\sum_{\gamma_1\in F_2^m}N(\gamma_1|\overline{\delta_{r-1}^{(1)}(K_r^t)})\cdot\log\left(\frac{Pr_{D_0}[\gamma_1]}{2^{-m}}\right)+\sum_{\gamma_2\in F_2^m}N(\gamma_2|\overline{\delta_{r-1}^{(2)}(K_r^t)})\cdot\log\left(\frac{Pr_{D_0}[\gamma_2]}{2^{-m}}\right)+\cdots+\sum_{\gamma_{|\Delta_0|}\in F_2^m}N(\gamma_{|\Delta_0|}|\overline{\delta_{r-1}^{(|\Delta_0|)}(K_r^t)})\cdot\log\left(\frac{Pr_{D_0}[\gamma_{|\Delta_0|}]}{(2^{-m})}\right)$$

$$=LLR^{(1)}(\overline{\delta_{r-1}^{(1)}(K_r^t)})+LLR^{(2)}(\overline{\delta_{r-1}^{(2)}(K_r^t)})+\cdots+LLR^{(|\Delta_0|)}(\overline{\delta_{r-1}^{(|\Delta_0|)}(K_r^t)}) \tag{3}$$

在假设差分特征相互独立的条件下，式(3)给出了综合利用集合 Δ 中的所有差分特征构造的统计量$\overline{LLR}(\overline{\delta_{r-1}(K_r^t)})$的计算方法.

基于最优区分器的思想，利用差分特征$(\delta_0^{(i)},\delta_{r-1}^{(i,j)})(i=1,\cdots,|\Delta_0|,j=1,\cdots,|\Delta_{r-1}^{(i)}|)$对分组密码 E 进行多差分攻击的过程，等价于对 2^{n_k} 条输出差分序列$\overline{\delta_{r-1}(K_r^t)}(1\leq t\leq 2^{n_k})$进行最优判决的过程.

下面给出对 r 圈分组密码算法进行多差分攻击($|\Delta_0|>1$)的基本过程，记为算法 1.

算法 1.

1. 已知 M 个明文向量构成的序列$\{(x_k,x_k\oplus\delta_0^{(1)},x_k\oplus\delta_0^{(2)},\cdots,x_k\oplus\delta_0^{(|\Delta_0|)})\}_{k=1}^M$，相应的密文向量序列$\{(y_k,y_k^{(1)},\cdots,y_k^{(|\Delta_0|)})\}_{k=1}^M$. 利用实验密钥 $K_r^t(1\leq t\leq 2^{n_k})$解密$\{(y_k,y_k^{(1)},\cdots,y_k^{(|\Delta_0|)})\}_{k=1}^M$，得到$\{(z_k,z_k^{(1)},\cdots,z_k^{(|\Delta_0|)})\}_{k=1}^M$，计算出 $|\Delta_0|$ 条输出差分序列，分别是$\overline{\delta_{r-1}^{(1)}(K_r^t)}=\{z_k\oplus z_k^{(1)}\}_{k=1}^M$，$\overline{\delta_{r-1}^{(2)}(K_r^t)}=\{z_k\oplus z_k^{(2)}\}_{k=1}^M$，$\cdots$，$\overline{\delta_{r-1}^{(|\Delta_0|)}(K_r^t)}=\{z_k\oplus z_k^{(|\Delta_0|)}\}_{k=1}^M$.

2. 利用式(2)分别计算出 $LLR^{(i)}(\overline{\delta_{r-1}^{(i)}(K_r^t)})$，$1\leq i\leq|\Delta_0|$，然后，利用式(3)计算出$\overline{LLR}(\overline{\delta_{r-1}(K_r^t)})$. 对 2^{n_k} 个统计量$\overline{LLR}(\overline{\delta_{r-1}(K_r^t)})$按从大到小的顺序进行排序，将前 l 个统计量对应的圈子密钥作为候选密钥.

4　多差分密码分析方法的指标分析

本节分析算法 1 的计算复杂度、存储复杂度和成功率.

定理 1.　算法 1 的计算复杂度是 $O((|\Delta_0|+1)\cdot M\cdot 2^{n_k}/r)$次分组密码算法解密运算，存储复杂度是 $O((|\Delta_0|+1)\cdot M)$个明密对.

证明.　算法 1 中步 1 中需要进行 $(|\Delta_0|+1)\cdot M\cdot 2^{n_k}$ 次第 r 圈解密操作，步 2 中需要计算 2^{n_k} 个 LLR 统计量，并且需要对 2^{n_k} 个统计量的值进行排序. 由于步 2 的计算复杂度与步 1 的计算复杂度相比，具有较小的数量级，因此，算法 1 的计算复杂度记为 $O((|\Delta_0|+1)\cdot M\cdot 2^{n_k})$次圈函数解密运算，由于本文假设分组密码算法是 r 圈，因此，算法 1 的计算复杂度是 $O((|\Delta_0|+1)\cdot M\cdot 2^{n_k}/r)$次分组密码算法解密运算.

算法 1 需要存储 M 个明文向量$(x_k,x_k\oplus\delta_0^{(1)},x_k\oplus\delta_0^{(2)},\cdots,x_k\oplus\delta_0^{(|\Delta_0|)})$以及相应的密文向量$\{(y_k,y_k^{(1)},\cdots,y_k^{(|\Delta_0|)})\}_{k=1}^M$，因此，算法 1 的存储复杂度是 $O((|\Delta_0|+1)\cdot M)$个明密对.　　证毕.

另外注意，当 $|\Delta_0|=1$ 时，算法 1 的计算复杂度和存储复杂度与文献[11]的结果相同.

为了给出数据复杂度与成功率之间的关系，我们需要分析正确的圈子密钥 K_r^T 对应的统计量$\overline{LLR}(\overline{\delta_{r-1}(K_r^T)})$、错误的圈子密钥 K_r^F 对应的统计量$\overline{LLR}(\overline{\delta_{r-1}(K_r^F)})$的概率分布. 首先给出相关定义.

对于 $\forall(\gamma_1,\cdots,\gamma_{|\Delta_0|})\in(F_2^m)^{|\Delta_0|}$，令

$$\varepsilon_\gamma=Pr_{D_0}[\delta_{r-1}=(\gamma_1,\cdots,\gamma_{|\Delta_0|})]-Pr_{D_1}[\delta_{r-1}=(\gamma_1,\cdots,\gamma_{|\Delta_0|})],$$

并且令

$$\Delta(\overline{D}_0)=\sum_{\gamma\in(F_2^m)^{|\Delta_0|}}\frac{(Pr_{\overline{D}_0}[\delta_{r-1}=\gamma]-Pr_{\overline{D}_1}[\delta_{r-1}=\gamma])^2}{Pr_{\overline{D}_1}[\delta_{r-1}=\gamma]},$$

由于

$$Pr_{\overline{D}_1}[\delta_{r-1}=\gamma]=Pr_{\overline{D}_1}[\delta_{r-1}=(\gamma_1,\cdots,\gamma_{|\Delta_0|})]=\prod_{i=1}^{|\Delta_0|}Pr_{D_1}[\delta_{r-1}^{(i)}=\gamma_i]=(2^{-m})^{|\Delta_0|},$$

因此

$$\Delta(\overline{D}_0)=(2^m)^{|\Delta_0|}\sum_{\gamma\in(F_2^m)^{|\Delta_0|}}\varepsilon_\gamma^2 \tag{4}$$

定理 2.　$\overline{LLR}(\overline{\delta_{r-1}(K_r^T)})$和$\overline{LLR}(\overline{\delta_{r-1}(K_r^F)})$都服从正态分布，

$$\overline{LLR}(\overline{\delta_{r-1}(K_r^T)})\sim\mathcal{N}(M\mu_0,M\sigma_0^2),$$

$$\overline{LLR}(\overline{\delta_{r-1}(K_r^F)})\sim\mathcal{N}(M\mu_1,M\sigma_1^2),$$

且

$$\mu_0\approx-\mu_1\approx\frac{1}{2}\Delta(\overline{D}_0),\ \sigma_0^2\approx\sigma_1^2\approx\Delta(\overline{D}_0).$$

证明.　由文献[12]中的 Proposition 5 直接可得$\overline{LLR}(\overline{\delta_{r-1}(K_r^T)})$和$\overline{LLR}(\overline{\delta_{r-1}(K_r^F)})$的概率分布.　　证毕.

定理2分别给出了统计量$\overline{LLR}(\overline{\delta_{r-1}(K_r^T)})$和统计量$\overline{LLR}(\overline{\delta_{r-1}(K_r^F)})$服从的概率分布，利用该结论，我们在定理3中分析了算法1的数据复杂度和成功率之间的关系.

定理3. 令$d=M\cdot\Delta(\overline{D}_0)$，假设$\overline{LLR}(\overline{\delta_{r-1}(K_r^T)})$和$\overline{LLR}(\overline{\delta_{r-1}(K_r^F)})$相互独立，且假设攻击者选择前$l$个最大值对应的实验密钥作为候选密钥，则当数据复杂度是$(1+|\Delta_0|)\cdot M$时，算法1的成功率为

$$P_S=\sum_{j=1}^{l}C_{2^{n_k}-1}^{j-1}\cdot(\phi(-\sqrt{d/2}))^{j-1}\cdot(1-\phi(-\sqrt{d/2}))^{2^{n_k}-j} \tag{5}$$

证明. 由于假设$\overline{LLR}(\overline{\delta_{r-1}(K_r^T)})$和$\overline{LLR}(\overline{\delta_{r-1}(K_r^F)})$是相互独立的，由定理2可得$\overline{LLR}(\overline{\delta_{r-1}(K_r^T)})-\overline{LLR}(\overline{\delta_{r-1}(K_r^F)})$服从正态分布$N(\mu,\sigma^2)$，其中

$$\mu=M\mu_0-M\mu_1=M\Delta(\overline{D}_0),$$
$$\sigma^2\approx M\sigma_0^2+M\sigma_1^2=2M\Delta(\overline{D}_0),$$

因此，

$$Pr[\overline{LLR}(\overline{\delta_{r-1}(K_r^T)})-\overline{LLR}(\overline{\delta_{r-1}(K_r^F)})<0]=Pr\left[\frac{\overline{LLR}(\overline{\delta_{r-1}(K_r^T)})-\overline{LLR}(\overline{\delta_{r-1}(K_r^F)})-M\Delta(\overline{D}_0)}{\sqrt{2M\Delta(\overline{D}_0)}}<\frac{-M\Delta(\overline{D}_0)}{\sqrt{2M\Delta(\overline{D}_0)}}\right]\approx\phi(-\sqrt{M\Delta(\overline{D}_0)/2}),$$

其中，$\phi(x)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x}e^{-\frac{u^2}{2}}du$.

将$\overline{LLR}(\overline{\delta_{r-1}(K_r^t)})$按从大到小的顺序排列，令事件$A_j$表示排第$j$($1\le j\le l$)位的实验密钥是正确密钥，求出

$$Pr[A_j]=C_{2^{n_k}-1}^{j-1}\cdot(\phi(-\sqrt{d/2}))^{j-1}\cdot(1-\phi(-\sqrt{d/2}))^{2^{n_k}-j},$$

其中，$d=M\cdot\Delta(\overline{D}_0)$.

已知攻击者选择前l个最大值对应的实验密钥作为候选密钥，则算法1攻击成功的概率$P_S=Pr[$正确密钥落入候选密钥集$]=Pr[A_1\cup A_2\cup\cdots\cup A_l]$，由于$A_j$是互斥的，因此

$$P_S=Pr[A_1]+\cdots+Pr[A_l]=\sum_{j=1}^{l}C_{2^{n_k}-1}^{j-1}\cdot(\phi(-\sqrt{d/2}))^{j-1}\cdot(1-\phi(-\sqrt{d/2}))^{2^{n_k}-j}.$$

算法1用到了M长的明文向量序列以及对应的密文向量序列，因此，数据复杂度是$(1+|\Delta_0|)\cdot M$个明密对，通过上述分析可知，算法1的成功率是$\sum_{j=1}^{l}C_{2^{n_k}-1}^{j-1}\cdot(\phi(-\sqrt{d/2}))^{j-1}\cdot(1-\phi(-\sqrt{d/2}))^{2^{n_k}-j}$.

证毕.

下面分析算法1的成功率为1的条件下，l的取值应该是多少？

由定理3的证明过程可知：

$$Pr[\overline{LLR}(\overline{\delta_{r-1}(K_r^T)})-\overline{LLR}(\overline{\delta_{r-1}(K_r^F)})<0]\approx\phi(-\sqrt{M\Delta(\overline{D}_0)/2}).$$

因此，平均有$(2^{n_k}-1)\cdot\phi(-\sqrt{M\Delta(\overline{D}_0)/2})$个错误密钥的统计量的值大于正确密钥的统计量的值. 若使得成功率为1，则l的平均值是$1+(2^{n_k}-1)\cdot\phi(-\sqrt{M\Delta(\overline{D}_0)/2})$.

由定理3可知，为了得到算法1的数据复杂度和成功率的关系，需要计算$\Delta(\overline{D}_0)$($d=M\cdot\Delta(\overline{D}_0)$)，如果直接利用式(4)计算$\Delta(\overline{D}_0)$，计算复杂度较高，下面以定理4的形式给出计算$\Delta(\overline{D}_0)$的简单方法.

定理4. 令

$$\Delta^{(i)}(D_0)=\sum_{\gamma_i\in F_2^m}\frac{(Pr_{D_0}[\delta_{r-1}^{(i)}=\gamma_i]-Pr_{D_1}[\delta_{r-1}^{(i)}=\gamma_i])^2}{Pr_{D_1}[\delta_{r-1}^{(i)}=\gamma_i]},$$

其中$i=1,2,\cdots,|\Delta_0|$，则

(1) $\Delta^{(i)}(D_0)=2^m\sum_{\delta_{r-1}^{(i,j)}\in\Delta_{r-1}^{(i)}}(Pr_{D_0}[\delta_{r-1}^{(i)}=\delta_{r-1}^{(i,j)}]-2^{-m})^2+2^m(2^m-|\Delta_{r-1}^{(i)}|)\left(\frac{(1-\sum_{1\le j\le|\Delta_{r-1}^{i}|}p^{(i,j)})}{(2^m-|\Delta_{r-1}^{(i)}|)}-2^{-m}\right)^2$ (6)

其中$p^{(i,j)}=Pr_{D_0}[\delta_{r-1}^{(i)}=\delta_{r-1}^{(i,j)}]$，$i=1,\cdots,|\Delta_0|$，$j=1,\cdots,|\Delta_{r-1}^{(i)}|$.

(2) $$\Delta(\overline{D}_0)\approx\sum_{i=1}^{|\Delta_0|}\Delta^{(i)}(D_0) \tag{7}$$

证明.

(1) 根据$\Delta^{(i)}(D_0)$的定义得到

$$\begin{aligned}\Delta^{(i)}(D_0)&=\sum_{\gamma_i\in F_2^m}\frac{(Pr_{D_0}[\delta_{r-1}^{(i)}=\gamma_i]-Pr_{D_1}[\delta_{r-1}^{(i)}=\gamma_i])^2}{Pr_{D_1}[\delta_{r-1}^{(i)}=\gamma_i]}\\&=2^m\sum_{\gamma_i\in F_2^m}(Pr_{D_0}[\delta_{r-1}^{(i)}=\gamma_i]-2^{-m})^2\\&=2^m\sum_{\gamma_i\in\Delta_{r-1}^{(i)}}(Pr_{D_0}[\delta_{r-1}^{(i)}=\gamma_i]-2^{-m})^2+2^m\sum_{\gamma_i\notin\Delta_{r-1}^{(i)}}(Pr_{D_0}[\delta_{r-1}^{(i)}=\gamma_i]-2^{-m})^2\\&=2^m\sum_{\delta_{r-1}^{(i,j)}\in\Delta_{r-1}^{(i)}}(Pr_{D_0}[\delta_{r-1}^{(i)}=\delta_{r-1}^{(i,j)}]-2^{-m})^2+\end{aligned}$$

$$2^m(2^m-|\Delta_{r-1}^{(i)}|)\left(\frac{\left(1-\sum_{1\le j\le|\Delta_{r-1}^i|}p^{(i,j)}\right)}{(2^m-|\Delta_{r-1}^{(i)}|)}-2^{-m}\right)^2,$$

其中 $p^{(i,j)}=Pr_{D_0}[\delta_{r-1}^{(i)}=\delta_{r-1}^{(i,j)}]$.

(2) 利用数学归纳法证明，具体证明过程如下：

① 当 $|\Delta_0|=1$ 时，$\Delta(\overline{D}_0)=\Delta^{(1)}(D_1)$；

② 当 $|\Delta_0|=2$ 时，

$$\Delta(\overline{D}_0)=\sum_{\gamma\in(F_2^m)^{|\Delta_0|}}\frac{(Pr_{D_0}[\delta_{r-1}=\gamma]-Pr_{\overline{D}_1}[\delta_{r-1}=\gamma])^2}{Pr_{\overline{D}_1}[\delta_{r-1}=\gamma]}$$

$$=\sum_{\gamma_1,\gamma_2\in F_2^m}\left((Pr_{D_0}[\delta_{r-1}^{(1)}=\gamma_1,\delta_{r-1}^{(2)}=\gamma_2]-Pr_{\overline{D}_1}[\delta_{r-1}^{(1)}=\gamma_1,\delta_{r-1}^{(2)}=\gamma_2])^2\right)\Big/\left(Pr_{\overline{D}_1}[\delta_{r-1}^{(1)}=\gamma_1,\delta_{r-1}^{(2)}=\gamma_2]\right)$$

$$=2^{2m}\cdot\sum_{\gamma_1,\gamma_2\in F_2^m}\left(Pr_{D_0}[\delta_{r-1}^{(1)}=\gamma_1,\delta_{r-1}^{(2)}=\gamma_2]-\frac{1}{2^{2m}}\right)^2$$

$$=2^{2m}\cdot\sum_{\gamma_1,\gamma_2\in F_2^m}(Pr_{D_0}[\delta_{r-1}^{(1)}=\gamma_1]Pr_{D_0}[\delta_{r-1}^{(2)}=\gamma_2])^2-2\cdot\sum_{\gamma_1,\gamma_2\in F_2^m}(Pr_{D_0}[\delta_{r-1}^{(1)}=\gamma_1]Pr_{D_0}[\delta_{r-1}^{(2)}=\gamma_2])+1$$

$$=2^{2m}\cdot\sum_{\gamma_1\in F_2^m}(Pr_{D_0}[\delta_{r-1}^{(1)}=\gamma_1])^2\sum_{\gamma_2\in F_2^m}(Pr_{D_0}[\delta_{r-1}^{(2)}=\gamma_2])^2-2\cdot\sum_{\gamma_1\in F_2^m}Pr_{D_0}[\delta_{r-1}^{(1)}=\gamma_1]\sum_{\gamma_2\in F_2^m}Pr_{D_0}[\delta_{r-1}^{(2)}=\gamma_2]+1$$

$$=2^{2m}\cdot\sum_{\gamma_1\in F_2^m}(Pr_{D_0}[\delta_{r-1}^{(1)}=\gamma_1])^2\sum_{\gamma_2\in F_2^m}(Pr_{D_0}[\delta_{r-1}^{(2)}=\gamma_2])^2-1,$$

同理，

$$\Delta^{(1)}(D_0)=\sum_{\gamma_1\in F_2^m}\frac{(Pr_{D_0}[\delta_{r-1}^{(1)}=\gamma_1]-Pr_{D_1}[\delta_{r-1}^{(1)}=\gamma_1])^2}{Pr_{D_1}[\delta_{r-1}^{(1)}=\gamma_1]}$$

$$=2^m\cdot\sum_{\gamma_1\in F_2^m}(Pr_{D_0}[\delta_{r-1}^{(1)}=\gamma_1]-2^{-m})^2$$

$$=2^m\cdot\sum_{\gamma_1\in F_2^m}(Pr_{D_0}[\delta_{r-1}^{(1)}=\gamma_1])^2-1,$$

$$\Delta^{(2)}(D_0)=2^m\cdot\sum_{\gamma_2\in F_2^m}(Pr_{D_0}[\delta_{r-1}^{(2)}=\gamma_2])^2-1,$$

则

$$\Delta(\overline{D}_0)-\Delta^{(1)}(D_0)=$$

$$2^{2m}\cdot\sum_{\gamma_1\in F_2^m}(Pr_{D_0}[\delta_{r-1}^{(1)}=\gamma_1])^2\sum_{\gamma_2\in F_2^m}(Pr_{D_0}[\delta_{r-1}^{(2)}=\gamma_2])^2-1-2^m\cdot\sum_{\gamma_1\in F_2^m}(Pr_{D_0}[\delta_{r-1}^{(1)}=\gamma_1])^2+1$$

$$=2^m\cdot\sum_{\gamma_1\in F_2^m}(Pr_{D_0}[\delta_{r-1}^{(1)}=\gamma_1])^2\cdot\left[2^m\sum_{\gamma_2\in F_2^m}(Pr_{D_0}[\delta_{r-1}^{(2)}=\gamma_2])^2-1\right]$$

$$=\Delta^{(2)}(D_0)(\Delta^{(1)}(D_0)+1)$$

由于 $\Delta^{(2)}(D_0)\cdot\Delta^{(1)}(D_0)\ll\max\{\Delta^{(2)}(D_0),\Delta^{(2)}(D_0)\}$，因此

$$\Delta(\overline{D}_0)=\Delta^{(1)}(D_0)+\Delta^{(2)}(D_0)+\Delta^{(1)}(D_0)\Delta^{(2)}(D_0)\approx\Delta^{(1)}(D_0)+\Delta^{(2)}(D_0)$$

③ 当 $|\Delta_0|=n$ 时，设 $\Delta(\overline{D}_0)\approx\sum_{i=1}^{n}\Delta^{(i)}(D_0)$；

④ 当 $|\Delta_0|=n+1$ 时，根据②的证明过程可得

$$\Delta(\overline{D}_0)-\left(\sum_{i=1}^{n}\Delta^{(i)}(D_0)\right)\approx\Delta^{(n+1)}(D_0)\left(\left(\sum_{i=1}^{n}\Delta^{(i)}(D_0)\right)+1\right),$$

因此，$\Delta(\overline{D}_0)\approx\sum_{i=1}^{n+1}\Delta^{(i)}(D_0)$. 证毕.

由定理 4 可知，在已知 $p^{(i,j)}(i=1,\cdots,|\Delta_0|,j=1,\cdots,|\Delta_{r-1}^{(i)}|)$ 的条件下，由式(6)可以计算出 $\Delta^{(i)}(D_0)$，$i=1,2,\cdots,|\Delta_0|$，然后，利用式(7)计算出 $\Delta(\overline{D}_0)$. 在已知 $\Delta(\overline{D}_0)$ 的条件下，我们就可以利用定理 3 的结论计算出算法 1 的数据复杂度和成功率之间的关系.

5　基于最优区分器的多差分密码分析的应用

本节通过一个例子给出算法 1 的具体应用.

已知一个 r 圈分组密码算法 E 的分组规模 $m=128$，第 r 圈子密钥 K_r 是 n_k 比特. 并且找到该算法的 48 个 $r-1$ 圈的高概率差分特征，其中输入差分构成的集合 $\Delta_0=\{\delta_0^{(1)},\cdots,\delta_0^{(16)}\}$，并且对于 $\forall i\in\{1,2,\cdots,16\}$，$|\Delta_{r-1}^{(i)}|=3$，记 $\Delta_{r-1}^{(i)}=\{\delta_{r-1}^{(i,1)},\delta_{r-1}^{(i,2)},\delta_{r-1}^{(i,3)}\}$.

已知：

(1) $Pr_{D_0}[\delta_0^{(i)}\to\delta_0^{(i,j)}]=2^{-114}$，$1\le i\le16$，$1\le j\le3$；

(2) $\forall\beta\in F_2^{128}$，且 $\beta\notin\Delta_{r-1}^{(i)}$，

$$Pr_{D_0}[\delta_0^{(i)}\to\beta]=(1-3\times2^{-114})/(2^{128}-3);$$

(3) $\forall\beta\in F_2^{128}$，$Pr_{D_1}[\delta_0^{(i)}\to\beta]=2^{-128}$.

下面给出利用算法 1 对该分组密码算法 E 的多差分密码分析方法.

1. 已知 M 个明文向量构成的序列 $\{(x_k,x_k\oplus\delta_0^{(1)},x_k\oplus\delta_0^{(2)},\cdots,x_k\oplus\delta_0^{(16)})\}_{k=1}^{M}$，相应的密文向量序列 $\{(y_k,y_k^{(1)},\cdots,y_k^{(16)})\}_{k=1}^{M}$. 利用实验密钥 $K_r^t(1\le t\le2^{n_k})$ 解密 $\{(y_k,y_k^{(1)},\cdots,y_k^{(16)})\}_{k=1}^{M}$，得到 $\{(z_k,z_k^{(1)},\cdots,z_k^{(16)})\}_{k=1}^{M}$，计算出 16 条输出差分序列，分别是 $\overline{\delta_{r-1}^{(1)}(K_r^t)}=\{z_k\oplus z_k^{(1)}\}_{k=1}^{M}$，$\overline{\delta_{r-1}^{(2)}(K_r^t)}=\{z_k\oplus z_k^{(2)}\}_{k=1}^{M}$，$\cdots$，$\overline{\delta_{r-1}^{(16)}(K_r^t)}=\{z_k\oplus z_k^{(16)}\}_{k=1}^{M}$.

2. 利用式(2)分别计算出 $LLR^{(i)}(\overline{\delta_{r-1}^{(i)}(K_r^t)})$，$1\le i\le16$，然后，利用式(3)计算出 $\overline{LLR}(\overline{\delta_{r-1}(K_r^t)})$. 对 2^{n_k} 个统计量 $\overline{LLR}(\overline{\delta_{r-1}(K_r^t)})$ 按从大到小的顺序进行排序，将前 l 个统计量对应的圈子密钥作为候选密钥.

下面分析上述多差分攻击算法的成功率与数据复杂度之间的关系.

根据式(6)可计算出 $\Delta^{(i)}(D_0)(1\leq i\leq 16)$:

$$\Delta^{(i)}(D_0)=2^{128}\times\left[3\times(2^{-114}-2^{-128})^2+(2^{128}-3)\times\left(\frac{1-3\times 2^{-114}}{2^{128}-3}-2^{-128}\right)^2\right]\approx 2^{-99}.$$

根据式(7)可计算出

$$\Delta(\overline{D}_0)\approx\sum_{i=1}^{16}\Delta^{(i)}(D_0)=16\times 2^{-99}=2^{-95}.$$

根据式(5)计算出当数据复杂度是 $17\cdot M$ 个明密对时,对差分攻击的成功率是

$$P_S=\sum_{j=1}^{l}C_{2^{n_k}-1}^{j-1}\cdot(\phi(-\sqrt{d/2}))^{j-1}\cdot(1-\phi(-\sqrt{d/2}))^{2^{n_k}-j}=\sum_{j=1}^{l}C_{2^{n_k}-1}^{j-1}\cdot(\phi(-2^{-48}\sqrt{M}))^{j-1}\cdot(1-\phi(-2^{-48}\sqrt{M}))^{2^{n_k}-j}.$$

若令 $l=1$,假设在相同成功率的条件下,令基于单个输入差分、多个输出差分(假设只利用差分特征$(\delta_0^{(1)},\delta_{r-1}^{(1,1)})$,$(\delta_0^{(1)},\delta_{r-1}^{(1,2)})$,$(\delta_0^{(1)},\delta_{r-1}^{(1,3)})$)的多差分攻击的数据复杂度为 $N1$ 个明密对,基于多个输入差分、多个输出差分(利用的差分特征是$(\delta_0^{(i)},\delta_{r-1}^{(i,j)})$,$1\leq i\leq 3$,$1\leq j\leq 16$)的多差分攻击的数据复杂度为 $N2$ 个明密对,下面分析 $N1$ 和 $N2$ 的关系.

已知 $l=1$,且成功率相同,由定理 3 可得

$$(1-\phi(-\sqrt{(N1/2)\cdot\Delta^{(1)}(D_0)/2}))^{2^{n_k}-1}=(1-\phi(-\sqrt{(N2/(1+|\Delta_0|))\cdot\Delta(\overline{D}_0)/2}))^{2^{n_k}-1}\Leftrightarrow(N1/2)\cdot 2^{-99}=(N2/(1+|\Delta_0|))\cdot|\Delta_0|\cdot 2^{-95}\quad(8)$$

由式(8)计算出 $N1/N2=2|\Delta_0|/(|\Delta_0|+1)$,当 $|\Delta_0|=16$ 时,$N1/N2\approx 32$.

由 $N1/N2=2|\Delta_0|/(|\Delta_0|+1)$ 说明,在 $|\Delta_0|>1$,且攻击成功率相同的条件下,利用的差分特征越多,算法 1 所需的数据复杂度越小.

6 结束语

如何利用多个差分特征对分组密码算法进行攻击,从而降低基于单差分特征的差分攻击的数据复杂度,是密码分析领域的一个重要的研究问题.本文基于最优区分器的思想,提出了一种最优的多差分密码分析方法,并分析了该方法的各项性能指标.另外,本文分析得出,在相同成功率的条件下,采用的差分特征越多,所需的数据复杂度越小,并给出具体实例证明了该理论结果.我们下一步的工作重点是利用文章提出的多差分分析方法攻击具体的分组密码算法,从而给出该算法的精确的抗差分分析的能力.

致 谢 审稿专家和编辑老师为本文提出了宝贵的修改建议,在此表示衷心的感谢!

参 考 文 献

[1] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems//Proceedings of the 10th Annual International Cryptology Conference. Santa Barbara, USA, 1990: 2-21

[2] Zhang Lei, Zhang Wen-Tao, Wu Wen-Ling. Cryptanalysis of reduced-round SMS4 block cipher//Proceedings of Information Security and Privacy. Wollongong, Australia, 2008: 216-229

[3] Wang Mei-Qin. Differential cryptanalysis of reduced-round PRESENT//Proceedings of the 1st International Conference on Cryptology in Africa. Casablanca, Morocco, 2008: 40-49

[4] Courtois N T, Misztal M. First differential attack on full 32-round GOST//Proceedings of the 13th International Conference of Information and Communications Security. Beijing, China, 2011: 216-227

[5] Wang Gao-Li. Improved differential cryptanalysis of serpent //Proceedings of the 2010 International Conference on Computational Intelligence and Security. Nanning, China, 2010: 367-371

[6] Knudsen L R. Truncated and higher order differentials// Proceedings of the 2nd International Workshop on Fast Soft Encryption. Leuven, Belgium, 1994: 196-211

[7] Biham E, Biryukov A, Shamir A. Cryptanalsis of skipjack reduced to 31 rounds using impossible differentials//Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques. Prague, Czech Republic, 1999: 12-23

[8] Knellwolf S, Meier W, Plasencia N. Conditional differential cryptanalysis of NLFSR-based cryptosystems//Proceedings of the 16th International Conference on the Theory and Application of Cryptology and Information Security. Swissôtel Merchant Court, Singapore, 2010: 130-145

[9] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 1991, 4(1): 3-72

[10] Blondeau C, Gérard B. Multiple differential cryptanalysis: Theory and practice//Proceedings of the 18th International Workshop on Fast Soft Encryption. Lyngby, Denmark, 2011: 35-54

[11] Blondeau C, Gérard B, Nyberg K. Multiple differential cryptanalysis using LLR and χ^2 statistics//Proceedings of the 8th International Conference of Security and Cryptography

for Networks. Amalfi, Italy, 2012: 343-360

[12] Baigeres T, Junod P, Vaudenay S. How for can we go beyond linear cryptanalysis?//Proceedings of the 10th International Conference on the Theory and Application of Cryptology and Information Security. Jeju Island, Korea, 2004: 432-450

GAO Hai-Ying, born in 1978, Ph.D., associate professor. Her research interest focuses on cryptology theory.

JIN Chen-Hui, born in 1965, Ph. D., professor, Ph. D. supervisor. His research interests include cryptology theory and information security.

Background

Differential cryptanalysis method was proposed in EUROCRYPT 1990, and it was an efficient chosen-plaintext attack method for iterative block cipher. Today, many block ciphers have been attacked successfully, such as DES, Gost et al. Based on this method, many improved differential cryptanalysis methods were introduced, such as truncated and higher order differentials, impossible differentials et al.

In the fundamental differential cryptanalysis method, only one differential characteristic was used. So how to use multiple differential characteristics? In order to solve this problem, in 1991, Biham and Shamir presented an improved differential cryptanalysis method of using multiple differential characteristics with same output differential; in 1994, Knudsen produced truncated differential cryptanalysis method in which the differential characteristics must constitute a linear space; In 2011, Blondeau introduced an universal multiple differential cryptanalysis method, but this method was not optimal, then he introduced an optimal multiple differential cryptanalysis method in 2012, but in this method only the characteristics with same input differential were used. So, it is an open research topic that how to use characteristics with multiple input and output differentials. In this paper, a multiple differential cryptanalysis method is proposed based on optimal distinguisher. For each experimental key, a statistic is constructed based on multiple differentials, thus, we determine whether the experimental key is correct according to the statistics. In addition, we analyze the computational complexity of this method, the probability distributions of statistics corresponding correct key and incorrect key, and give the relation of success probability and data complexity. In the end, we give an example to show that the data complexity is decreased with more differentials under the condition of same success probability.

The research is supported by the National Fund Cipher Development Project (MMJJ201401002), the National Natural Science Foundation of China (61272488, 61272041, 61202491).