基于多个独立区分特征的序列密码最优联合区分器

高海英，金晨辉
（解放军信息工程大学 电子技术学院，河南 郑州 450004）

摘 要：如何综合利用多个区分特征得到区分优势更大的区分器一直是密码分析者有待解决的问题。在假设多个区分特征相互独立的条件下，给出了综合利用多个区分特征的最优联合区分器，给出了该区分器的区分优势的计算方法，证明了联合区分器利用的区分特征越多，在相同的数据复杂度的条件下，区分优势就越大；在相同的区分优势的条件下，区分攻击的数据复杂度就越小。若利用单个区分特征的区分攻击的数据复杂度是 N，则联合利用 k 个具有相同优势的区分特征进行区分攻击的数据复杂度约为 N/k。

关键词：序列密码；区分特征；最优区分器；区分优势
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1000-436X(2012)07-0044-05

Optimal combined distinguisher of stream cipher with multiple independent distinguishing characters

GAO Hai-ying, JIN Chen-hui
(Electronic Technology Institute, PLA Information Engineering University, Zhengzhou 450004, China)

Abstract: It is an open problem to combine many distinguishing characters to construct a distinguisher with more advantage. An optimal combined distinguisher based on multiple independent distinguishing characters was proposed. The computing method of distinguishing advantage of this combined distinguisher was presented and the conclusion was given that the data complexity decreased on the condition of same distinguishing advantage, and the distinguishing advantage increased on the condition of the same data complexity when more distinguishing characters were used in distinguishing attack. Let N denote the data complexity of distinguisher with only one character, then the data complexity of combined distinguisher with k-independent characters was about N/k for special case that all distinguishing advantages of k-independent characters were equal.

Key words: stream cipher; distinguishing character; optimal distinguisher; distinguishing advantage

1 引言

根据分析目的不同，可将序列密码的分析方法分为 2 类[1]：一类是密钥恢复攻击，其攻击目的是恢复出密钥 K；一类是区分攻击，其攻击目的是判定一个给定的序列是一个特定的序列密码算法产生的乱数序列或者是一个真随机序列。对一个序列密码算法的区分攻击主要分 2 步完成，第一步是区分特征的构造，区分特征是攻击者利用序列密码的第 i 个乱数至第 $i+d$ 个乱数构造的不服从均匀分布的特征 ξ_i (其中，d 与具体的区分特征相关)，借助该区分特征将乱数序列与随机序列区分开；第二步是利用区分器给出判定结果。区分器就是一个利用区分特征给出判定结果的算法，该算法的输入是一个

收稿日期：2011-08-30；**修回日期**：2012-02-17
基金项目：国家自然科学基金资助项目（60821001, 60803157, 90604022）
Foundation Item: The National Natural Science Foundation of China (60821001, 60803157, 90604022)

给定的序列，输出是 0 或 1。若输出是 0，则判定输入序列是一个真随机序列；输出是 1，则判定输入序列是由一个特定的序列密码算法产生的。一个区分攻击的区分效果通过区分优势[2]来判定，区分优势等价于判定正确的概率减去判定错误的概率。若区分优势为 0，则该区分攻击的输出是随机猜测结果，是毫无意义的；若区分优势是 1，则输出结果一定是正确的。因此，区分优势越大，该区分攻击的区分效果越好。区分优势由 2 个关键因素决定，一个是区分特征，区分特征 ξ_i 分布的越不均匀，区分效果越好；另一个是区分器，针对某个给定的区分特征，使得区分优势达到最大的判决算法就是针对该区分特征的最优区分器。文献[2]给出了针对单个区分特征的最优区分器。

目前，对区分攻击的研究主要集中在对序列密码的区分特征的构造方面，相关文献有文献[3~8]等，但在区分器的设计方面，存在这样的问题有待解决：攻击者找到了多个区分特征，利用文献[2]的方法，针对每个区分特征都可以得到一个区分优势较小的最优区分器，如何综合利用多个区分特征设计一个区分优势更大的最优区分器呢？本文在假设多个区分特征相互独立的条件下，给出了综合利用多个区分特征的最优联合区分器，给出了区分优势的计算方法，证明了该区分器利用的区分特征越多，区分优势就越大，并通过具体的例子，说明了在数据量相同的条件下，使用联合区分器将提高区分攻击的区分优势；在相同区分优势的条件下，使用联合区分器将降低区分攻击的数据复杂度。

2　背景知识

设一个序列密码的乱数序列 $\bar{s}=\{s_i\}_{i=1}^{n}, s_i\in Z_2^t$，即乱数规模是 t bit，假设攻击者已经构造出一个针对该序列密码的区分特征 z_i，例如，区分特征 $z_i=s_i\oplus s_{i+3}\oplus s_{i+10}$，则 $z_i\in Z_2^t$，$1\leqslant i\leqslant n-10$；若攻击者构造出的区分特征 $z_i=s_i(0)\oplus s_{i+3}(0)\oplus s_{i+10}(0)$，其中，$\oplus$ 表示逐比特模 2 加运算，$s_i(0)$ 表示 s_i 的最低位比特，则 $z_i\in Z_2$，$1\leqslant i\leqslant n-10$。

设攻击者构造出的区分特征 z_i（$z_i\in Z_2^m$，$m\in\{1,2,\cdots,t\}$）服从分布 $D1$：$\forall a\in Z_2^m$，$\Pr_{D1}[z_i=a]=p_a$。定义 $D0$ 是均匀分布，则 $\Pr_{D0}[z_i=a]=1/2^m$。

文献[2]给出了利用上述区分特征的最优区分器，现将该区分器描述如下。

输入：一条 n 长序列 $\bar{s}=\{s_i\}_{i=1}^{n}, s_i\in Z_2^t$。

输出：若输出 1，则判定 $\bar{s}$ 是序列密码算法的乱数序列；若输出 0，则判定 $\bar{s}$ 是随机序列。

Step1　由 $\bar{s}$ 计算出特征序列 $\bar{z}=\{z_i\}_{i=1}^{N}, z_i\in Z_2^m$；

Step2　计算：

$$LLR(\bar{z})=\sum_{\substack{a\in Z_2^m\\ N(a|\bar{z})>0}} N(a\,|\,\bar{z})\log\frac{\Pr_{D1}[a]}{\Pr_{D0}[a]}$$

其中，$N(a\,|\,\bar{z})$ 表示序列 $\bar{z}$ 中 α 的个数。

Step3 输出 $A(\bar{s})$：

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

文献[2]定义了利用区分特征 z_i（$z_i\in Z_2^m$）进行区分攻击的区分优势为 $Adv(A(\bar{s}))=\Pr_{D1}[A(\bar{s})=1]-\Pr_{D0}[A(\bar{s})=1]=1-2P_e$，其中，$P_e=\frac{1}{2}(\alpha_1+\alpha_2)$，$\alpha_1$ 是将随机序列判断为乱数序列的错误概率，α_2 是将乱数序列判断为随机序列的错误概率；给出了该区分器的区分优势 $Adv(A(\bar{s}))=1-2\phi\left(-\frac{\sqrt{N\beta}}{2}\right)$，其中，$\beta=\sum_{a\in Z_2^m}\frac{(\Pr_{D1}[a]-\Pr_{D0}[a])^2}{\Pr_{D0}[a]}$，$\phi(x)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x}\mathrm{e}^{-\frac{u^2}{2}}\mathrm{d}u$；并且证明了上述区分器是针对区分特征 z_i 的最优区分器。

3　基于 2 个独立区分特征的最优联合区分器

设一个序列密码的乱数序列 $\bar{s}=\{s_i\}_{i=1}^{n}, s_i\in Z_2^t$，即乱数规模是 t bit，已知攻击者针对该序列密码算法构造了 2 个相互独立的区分特征 z_{i1} 和 z_{i2}，其中，$z_{i1}\in Z_2^{m1}$，$z_{i2}\in Z_2^{m2}$，$m1,m2\in\{1,2,\cdots,t\}$，如下表示：

区分特征 1：$\forall a\in Z_2^{m1}$，$\Pr_{D1}[z_{i1}=a]=p_a^{(1)}$，令 $\Pr_{D0}[z_{i1}=a]=1/2^{m1}$；

区分特征 2：$\forall b\in Z_2^{m2}$，$\Pr_{D1}[z_{i2}=b]=p_b^{(2)}$，令 $\Pr_{D0}[z_{i2}=b]=1/2^{m2}$。

下面给出综合利用这 2 个区分特征的联合区分器，本文简记为算法 1。

输入：一条序列 $\bar{s}=\{s_i\}_{i=1}^{n}$，$s_i\in Z_2^t$。

输出：$A(\bar{s})$ 为 0 或 1。若 $A(\bar{s})=1$，则判定 $\bar{s}$ 是乱数序列；若 $A(\bar{s})=0$，则判定 $\bar{s}$ 是随机序列。

Step1 由 $\bar{s}$ 计算出特征序列 $\bar{z}=\{z_i\}_{i=1}^{N}$，其中，$z_i=(z_{i1},z_{i2})$，则 $z_i\in Z_2^{m1+m2}$。针对所有的 $(a,b)\in(Z_2^{m1},Z_2^{m2})$，计算出

$$\begin{aligned}&\Pr_{D1}[z_i=(z_{i1},z_{i2})=(a,b)]\\&=\Pr_{D1}[z_{i1}=a]\Pr_{D1}[z_{i2}=b]\\&=p_a^{(1)}p_b^{(2)}\end{aligned}$$

令 $\Pr_{D0}[(z_{i1},z_{i2})=(a,b)]=1/2^{m1+m2}$。

Step2 计算

$$LLR(\bar{z})=\sum_{\substack{c\in Z_2^{m1+m2}\\N(c|\bar{z})>0}}N(c\mid\bar{z})\log\frac{\Pr_{D1}[c]}{\Pr_{D0}[c]}$$，其中，$N(c\mid\bar{z})$ 表示序列 $\bar{z}$ 中 c 的个数。

Step3 输出 $A(\bar{s})=\begin{cases}1, & LLR(\bar{z})>0\\0, & \text{其他}\end{cases}$。

与文献[2]中的分析方法相似，算法 1 是综合利用 2 个独立区分特征的最优区分器，且算法 1 的区分优势 $Adv(A(\bar{s}))=1-2\phi\left(-\sqrt{N\beta}/2\right)$，其中，$\beta=\sum_{c\in Z_2^{m+n}}\frac{(\Pr_{D1}[c]-\Pr_{D0}[c])^2}{\Pr_{D0}[c]}$，$N$ 是由序列 $\bar{s}$ 构造出的序列 $\bar{z}$ 的长度，在区分攻击所需的数据复杂度较大的条件下，可以认为 N 与 n 近似相等。

定理 1 设基于区分特征 1 的最优区分器的区分优势为 $Adv(A_1(\bar{s}))$，基于区分特征 2 的最优区分器的区分优势为 $Adv(A_2(\bar{s}))$，由算法 1 得到的最优联合区分器的区分优势为 $Adv(A(\bar{s}))$，令

$$\beta_1=\sum_{a\in Z_2^{m1}}\frac{(\Pr_{D1}[a]-\Pr_{D0}[a])^2}{\Pr_{D0}[a]}$$

$$\beta_2=\sum_{b\in Z_2^{m2}}\frac{(\Pr_{D1}[b]-\Pr_{D0}[b])^2}{\Pr_{D0}[b]}$$

$$\beta=\sum_{c\in Z_2^{m1+m2}}\frac{(\Pr_{D1}[c]-\Pr_{D0}[c])^2}{\Pr_{D0}[c]}$$

则

$$Adv(A(\bar{s}))=1-2\phi\left(-\sqrt{N\beta}/2\right)$$

$\beta=\beta_1+\beta_2+\beta_1\beta_2$，当 $\beta_1\beta_2>0$ 时，$Adv(A(\bar{s}))>\max\left\{Adv(A_1(\bar{s})),Adv(A_2(\bar{s}))\right\}$。

证明 根据 β 的定义可得：

$$\begin{aligned}\beta&=\sum_{c\in Z_2^{m1+m2}}\frac{(\Pr_{D1}[c]-\Pr_{D0}[c])^2}{\Pr_{D0}[c]}\\&=2^{m1+m2}\sum_{c\in Z_2^{m1+m2}}\left(\Pr_{D1}[c]-\frac{1}{2^{m1+m2}}\right)^2\\&=2^{m1+m2}\sum_{\substack{a\in Z_2^{m1}\\b\in Z_2^{m2}}}\left(p_a^{(1)}p_b^{(2)}-\frac{1}{2^{m1+m2}}\right)^2\\&=2^{m1+m2}\sum_{\substack{a\in Z_2^{m1}\\b\in Z_2^{m2}}}\left(p_a^{(1)}p_b^{(2)}\right)^2-2\sum_{\substack{a\in Z_2^{m1}\\b\in Z_2^{m2}}}\left(p_a^{(1)}p_b^{(2)}\right)+1\\&=2^{m1+m2}\sum_{a\in Z_2^{m1}}\left(p_a^{(1)}\right)^2\sum_{b\in Z_2^{m2}}\left(p_b^{(2)}\right)^2-\\&\quad 2\sum_{a\in Z_2^{m1}}p_a^{(1)}\sum_{b\in Z_2^{m2}}p_b^{(2)}+1\\&=2^{m1+m2}\sum_{a\in Z_2^{m1}}\left(p_a^{(1)}\right)^2\sum_{b\in Z_2^{m2}}\left(p_b^{(2)}\right)^2-1\end{aligned}$$

同理，

$$\begin{aligned}\beta_1&=\sum_{a\in Z_2^{m1}}\frac{(\Pr_{D1}[a]-\Pr_{D0}[a])^2}{\Pr_{D0}[a]}\\&=2^{m1}\sum_{a\in Z_2^{m1}}\left(p_a^{(1)}-1/2^{m1}\right)^2\\&=2^{m1}\sum_{a\in Z_2^{m1}}\left(p_a^{(1)}\right)^2-2\sum_{a\in Z_2^{m1}}p_a^{(1)}+1\\&=2^{m1}\sum_{a\in Z_2^{m1}}\left(p_a^{(1)}\right)^2-1\end{aligned}$$

$$\beta_2=2^{m2}\sum_{b\in Z_2^{m2}}\left(p_b^{(2)}\right)^2-1$$

则

$$\begin{aligned}\beta-\beta_1&=2^{m1+m2}\sum_{a\in Z_2^{m1}}\left(p_a^{(1)}\right)^2\sum_{b\in Z_2^{m2}}\left(p_b^{(2)}\right)^2-1-\\&\quad 2^{m1}\sum_{a\in Z_2^{m1}}\left(\Pr_{D1}(a)\right)^2+1\\&=2^{m1}\sum_{a\in Z_2^{m1}}\left(p_a^{(1)}\right)^2\left[\sum_{b\in Z_2^{m2}}\left(p_b^{(2)}\right)^2-1\right]\\&=\beta_2(\beta_1+1)\end{aligned}$$

故 $\beta=\beta_1+\beta_2+\beta_1\beta_2$。

已知条件 $\beta_1\beta_2>0$，因此，$\beta=\beta_1+\beta_2+\beta_1\beta_2>\max\{\beta_1,\beta_2\}$。

令 n_1，n_2 分别表示特征序列 $\{z_{i1}\}$ 和 $\{z_{i2}\}$ 的长度，N 是联合特征序列 $\{z_i\}$ 的长度，由 $\beta>\max\{\beta_1,\beta_2\}$，且 N,n_1,n_2 近似相等，可得

$$1-2\phi\left(-\sqrt{N\beta}/2\right)>$$

$$\max\left\{1-2\phi\left(-\sqrt{n_1\beta_1}/2\right),1-2\phi\left(-\sqrt{n_2\beta_2}/2\right)\right\}$$

即 $Adv(A(\bar{s}))>\max\left\{Adv(A_1(\bar{s})),Adv(A_2(\bar{s}))\right\}$。

4　基于 $k(k>2)$个独立区分特征的最优联合区分器

算法 1 是综合利用 2 个独立区分特征的最优联合区分器，若攻击者构造了针对该序列密码算法的 k ($k>2$)个独立区分特征，设第 j ($1\leqslant j\leqslant k$)个区分特征：$\forall a\in Z_2^{mj}$，$\Pr_{D1}[z_{ij}=a]=p_a^{(j)}$，令 $\Pr_{D0}[z_{ij}=a]=1/2^{mj}$，$\beta_j=\sum_{c\in Z_2^{mj}}\frac{(\Pr_{D1}[c]-\Pr_{D0}[c])^2}{\Pr_{D0}[c]}$，$m1,m2,\cdots,mk\in\{1,2,\cdots,t\}$。采用同样的思路可以构造综合利用这 k 个独立区分特征的最优联合区分器，本文简记为算法 2。

输入：一条序列 $\bar{s}=\{s_i\}_{i=1}^n$，$s_i\in Z_2^t$。

输出：$A(\bar{s})$ 为 0 或 1。若 $A(\bar{s})=1$，则判定 $\bar{s}$ 是乱数序列；若 $A(\bar{s})=0$，则判定 $\bar{s}$ 是随机数序列。

Step1　由 $\bar{s}$ 构造特征序列 $\bar{z}=\{z_i\}_{i=1}^N$，其中，$z_i=(z_{i1},\cdots,z_{ik})$，则 $z_i\in Z_2^{m1+m2+\cdots+mk}$。针对所有的 $(a_1,a_2,\cdots,a_k)\in(Z_2^{m1},\cdots,Z_2^{mk})$ 计算出

$$\Pr_{D1}[z_i=(z_{i1},\cdots,z_{ik})=(a_1,a_2,\cdots,a_k)]=\prod_{j=1}^k\Pr_{D1}[z_{ij}=a_j]=\prod_{j=1}^k p_{a_j}^{(j)}$$

令 $\Pr_{D0}[z_i=(z_{i1},\cdots,z_{ik})=(a_1,a_2,\cdots,a_k)]=1/2^{m1+\cdots+mk}$。

Step2　计算 $LLR(\bar{z})=\sum_{\substack{c\in 2^{m1+\cdots+mk}\\ N(c|\bar{z})>0}}N(c|\bar{z})\log\frac{\Pr_{D1}[c]}{\Pr_{D0}[c]}$，其中，$N(c|\bar{z})$ 表示序列 $\bar{z}$ 中 c 的个数。

Step3　输出 $A(\bar{s})=\begin{cases}1, & LLR(\bar{z})>0\\ 0, & \text{其他}\end{cases}$。

定理 2　由算法 2 得到的基于 k 个独立区分特征的最优联合区分器的区分优势 $Adv(A(\bar{s}))=1-2\phi\left(-\sqrt{N\gamma_k}/2\right)$，$\gamma_k$ 由以下递推关系计算得出：

$$\gamma_k=\begin{cases}\beta_1, & k=1\\ \gamma_{k-1}+\beta_k+\gamma_{k-1}\beta_k, & k>1\end{cases}$$

其中，$\gamma_k=\sum_{c\in Z_2^{m1+\cdots+mk}}\frac{(\Pr_{D1}[c]-\Pr_{D0}[c])^2}{\Pr_{D0}[c]}$。

证明　①当 $k=1$时，不失一般性，假设由第 1 个独立区分特征构成最优区分器，由文献[2]知，该区分器的区分优势 $Adv(A(\bar{s}))=1-2\phi\left(-\sqrt{N\gamma_1}/2\right)$，其中，$\gamma_1=\beta_1$。

②当 $k=j$ 时，不失一般性，假设由前 j 个独立区分特征构成最优联合区分器，设该区分器的区分优势 $Adv(A(\bar{s}))=1-2\phi\left(-\sqrt{N\gamma_j}/2\right)$，其中，$\gamma_j=\gamma_{j-1}+\beta_j+\gamma_{j-1}\beta_j$。

则由第$1\sim j$ 个区分特征构造的联合区分特征 $z_i^{'}$ 是：$\forall a_1\in Z_2^{m1},\cdots,a_j\in Z_2^{mj}$，$\Pr_{D1}[z_i^{'}=(z_{i1},\cdots,z_{ij})=(a_1,\cdots,a_j)]=p_{a_1}^{(1)}p_{a_2}^{(2)}\cdots p_{a_j}^{(j)}$，令 $\Pr_{D0}[z_i^{'}=(a_1,\cdots,a_j)]=1/2^{m1+\cdots+mj}$。

③ 当 $k=j+1$时，由前 $j+1$个独立区分特征构成最优联合区分器，设该区分器的区分优势 $Adv(A(\bar{s}))=1-2\phi\left(-\sqrt{N\gamma_{j+1}}/2\right)$，由第$1\sim(j+1)$ 个区分特征构造的联合区分特征 z_i 是：$\forall a_1\in Z_2^{m1},\cdots,a_{j+1}\in Z_2^{m(j+1)}$，

$$\Pr_{D1}[z_i=(z_i^{'},z_{i(j+1)})=((a_1,\cdots,a_j),a_{j+1})]=p_{a_1}^{(1)}p_{a_2}^{(2)}\cdots p_{a_j}^{(j)}p_{a_{j+1}}^{(j+1)},$$

令 $\Pr_{D0}[z_i=((a_1,\cdots,a_j),a_{j+1})]=1/2^{m1+\cdots+mj+m(j+1)}$。

由定理 1 可得：$\gamma_{j+1}=\gamma_j+\beta_{j+1}+\gamma_j\beta_{j+1}$。

因此，定理 2 得证。

已知由 k 个独立区分特征构造的最优联合区分器的区分优势是 $Adv(A(\bar{s}))=1-2\phi\left(-\sqrt{N\gamma_k}/2\right)$，因此，当 $N=\gamma_k^{-1}$，有 $Adv(A(\bar{s}))\approx 0.383$；当 $N=2\gamma_k^{-1}$，有 $Adv(A(\bar{s}))\approx 0.516$。这说明在区分优势为 0.516 的条件下，区分攻击的数据复杂度是 $2\gamma_k^{-1}$。特殊的情况，若 $\beta_i(1\leqslant i\leqslant k)$ 都相等，设利用利用单个区分特征的区分攻击的数据复杂度是 N，则联合利用 k 个区分特征的区分攻击的数据复杂度约为 N/k。

5　最优联合区分器的应用

本节通过一个具体的例子说明最优联合区分器能一定程度地降低区分攻击的数据复杂度。

假设一个序列密码算法的乱数序列是 $\bar{s}=\{s_i\}_{i=1}^n,s_i\in Z_2$。攻击者已经构造出针对该算法的 3 个区分特征，分别是 z_{i1}, z_{i2} , z_{i3}，且 z_{i1}, z_{i2}，$z_{i3}\in Z_2$，具体表示如下：

$\Pr_{D1}[z_{i1}=s_i\oplus s_{i+3}\oplus s_{i+10}=0]=0.5+2^{-80}$，

$\Pr_{D0}[z_{i1}=s_i\oplus s_{i+3}\oplus s_{i+10}=0]=0.5$，

其中，$1\leqslant i\leqslant n-10$；

$\Pr_{D1}[z_{i2}=s_{i+5}\oplus s_{i+13}=0]=0.5+2^{-80}$，

$\Pr_{D0}[z_{i2}=s_{i+5}\oplus s_{i+13}=0]=0.5$，

其中，$1\leqslant i\leqslant n-13$；

$\Pr_{D1}[z_{i3}=s_{i+7}\oplus s_{i+9}=0]=0.5-2^{-80}$，

$\Pr_{D0}[z_{i3}=s_{i+7}\oplus s_{i+9}=0]=0.5$，

其中，$1\leqslant i\leqslant n-9$。

假设这 3 个区分特征相互独立的条件下，由算法 2 给出综合利用这 3 个区分特征的最优联合区分器。

输入：一条序列 $\bar{s}=\{s_i\}_{i=1}^{n}, s_i\in Z_2$。

输出：$A(\bar{s})$ 为 0 或 1。若 $A(\bar{s})$=1，则判定 $\bar{s}$ 是该密码算法的乱数序列；若 $A(\bar{s})$=0，则判定 $\bar{s}$ 是随机数序列。

Step1 由 $\bar{s}$ 构造序列 $\bar{z}=\{z_i\}_{i=1}^{N}$，$1\leqslant N\leqslant n-13$，其中，

$$z_i=(s_i\oplus s_{i+3}\oplus s_{i+10}, s_{i+5}\oplus s_{i+13}, s_{i+7}\oplus s_{i+9})$$

则 $z_i\in Z_2^3$。针对所有的 $(a_1,a_2,a_3)\in(Z_2, Z_2, Z_2)$，计算

$$\begin{aligned}&\Pr_{D1}[z_i=(a_1,a_2,a_3)]\\&=\Pr_{D1}[s_i\oplus s_{i+3}\oplus s_{i+10}=a_1]\cdot\Pr_{D1}[s_{i+5}\oplus s_{i+13}=a_2]\cdot\\&\quad\Pr_{D1}[s_{i+7}\oplus s_{i+9}=a_3]\end{aligned}$$

令 $\Pr_{D0}[z_i=(a_1,a_2,a_3)]=1/2^3$。

Step2 计算 $LLR(\bar{z})=\sum_{\substack{c\in Z_2^3\\ N(c|\bar{z})>0}} N(c\,|\,\bar{z})\log\frac{\Pr_{D1}[c]}{\Pr_{D0}[c]}$，

其中，$N(c\,|\,\bar{z})$ 表示序列 $\bar{z}$ 中 c 的个数。

Step3 输出 $A(\bar{s})=\begin{cases}1, & LLR(\bar{z})>0\\ 0, & \text{其他}\end{cases}$。

可计算出 $\beta_1=\beta_2=\beta_3=2^{-158}$。

利用定理 2 可得：

$$Adv(A(\bar{s}))=1-2\phi\left(-\sqrt{N\gamma_3}/2\right)$$

其中，$N=n-13$，$\gamma_3=2^{-157}+2^{-158}+2^{-315}+2^{-316}+2^{-474}$。

假设攻击者具有相同的数据量，设已知数据量是 2^{159}，下面是区分器优势对比。

基于区分特征 1 的最优区分器的优势是 $1-2\phi\left(-\sqrt{2}/2\right)\approx 0.516$；基于区分特征 2 的最优区分器的优势是 $1-2\phi\left(-\sqrt{2}/2\right)\approx 0.516$；基于区分特征 3 的最优区分器的优势是 $1-2\phi\left(-\sqrt{2}/2\right)\approx 0.516$；最优联合区分器的优势是 $1-2\phi\left(-\sqrt{6}/2\right)\approx 0.781$。

假设在相同的区分优势 0.516 的前提下，下面是区分器所需要的数据复杂度的对比。

基于区分特征 1 的最优区分器的数据复杂度是 2^{159}；基于区分特征 2 的最优区分器的数据复杂度是 2^{159}；基于区分特征 3 的最优区分器的数据复杂度是 2^{159}；最优联合区分器的数据复杂度是 $2^{159}/3$。

由上述分析可知，在数据量相同的条件下，利用的区分特征越多，区分优势就越大；在区分优势相同的条件下，利用的区分特征越多，区分攻击所需的数据复杂度越少，特别地，若利用单个区分特征的区分攻击的数据复杂度是 N，则联合利用 k 个具有相同优势的区分特征进行区分攻击的数据复杂度约为 N/k。

6 结束语

文章给出了综合利用多个独立区分特征的最优联合区分器，并给出了区分优势的计算方法，证明了采用的独立区分特征越多，区分优势就越大。最优联合区分器可广泛地应用于密码分析领域的区分攻击，一定程度地降低区分攻击的数据复杂度。怎样综合利用多个不独立的区分特征设计区分优势更大的最优区分器，是有待解决的问题。

参考文献：

[1] MATIN H, THOMAS J, LENNART B. An overview of distinguishing attacks on stream ciphers [J]. Cryptography Communication, 2009, 1(1):71-94.

[2] THOMA B, PASCAL J, SERGE V. How for can we go beyond linear cryptanalysis?[A]. ASIACRYPT2004[C]. Korea, 2004. 432-450.

[3] GAUTHAM S, SOURADYUTI P, BART P. Distinguishing attacks on the stream cipher[A]. FSE2006[C]. Graz, Austria, 2006. 405-421.

[4] NATHAN K, STEPHEN D M. Distinguishing attacks on stream ciphers based on arrays of pseudo-random words[J].Information Processing Letters, 2010, 110(4): 129-132.

[5] ORUMIEHCHI M A, MOHEBIPOOR S F. Distinguishing attacks on SN3 stream cipher[A]. Proceedings of the International Conference

（下转第 58 页）

[11] NORBERT E, GREENHALGH A, HANDLEY M, *et al*. Improved forwarding architecture and resource management for multi-core software routers [A]. IFIP Conference on Networking and Parallel Computing[J]. Gold Coast[C]. Australia: IEEE Computer Society, 2009.

[12] 徐明伟, 江学智, 陈文龙. 路由器分布式控制研究综述[J]. 电子学报, 2010,38(8): 1892-1899.
XU M W, JIANG X Z, CHEN W L. Survey on distributed control in a router[J]. Acta Eletronica Sinica, 2010, 38(8):1892-1899.

[13] MARKUS H, SJÖDIN P, HAGSAND O. Control and forwarding plane interaction in distributed routers[J]. IFIP International Federation for Information Processing Networking, 2005,3462: 1339-1342.

[14] Forwarding and control element separation (ForCES)[EB/OL]. http://www.rfc-editor.org/info/rfc5812, 2010.

[15] Netmagicresearch group. Using netmagic to accelerate network technology innovation[EB/OL]. http://www.netmagic.org/Data/documents/presentations/NetMagic%20 workshop.pdf.

[16] CHOI Y H, TIMOTHY M P. Crossbar analysis for optimal deadlock recovery router architecture[A]. Proceedings of the 10th International Parallel Processing Symposium[C]. Geneva, Switzerland, 1997. 583-588.

[17] GHODSI A, KOPONEN T, RAJAHALME J, *et al*. Naming in content-oriented architectures[A]. Proceedings of SIGCOMM Workshop on ICN[C]. Toronto, Ontario, Canada, 2011.

作者简介：

吕高锋（1980-），男，陕西扶风人，博士，国防科学技术大学助理研究员，主要研究方向为计算机网络、高性能路由器、统一交换技术等。

孙志刚（1973-），男，江苏东海人，博士，国防科学技术大学研究员，主要研究方向为网络体系结构、高速网络交换技术等。

林雨弦（1988-），男，福建福安人，国防科学技术大学硕士生，主要研究方向为计算机网络、可扩展路由器体系结构等。

陈一骄（1972-），男，湖南益阳人，博士，国防科学技术大学副研究员，主要研究方向为计算机网络、高性能路由器、网络安全等。

李韬（1983-），男，安徽萧县人，博士，国防科学技术大学助理研究员，主要研究方向为计算机网络、网络处理器、路由与交换技术。

（上接第 48 页）

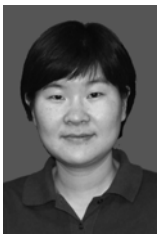
on Intelligent Information Hiding and Multimedia Signal Processing[C]. Harbin,China,2008.1392-1395.

[6] SUBHAMOY M, GOUTAM P, SHASHWAT R. Some observations on HC-128[EB/OL]. http://eprint.iacr.org 2008/499.pdf. 2010.10.

[7] GAUTHAM S, BART P. Improved distinguishing attacks on HC-256[A]. Proceedings IWSEC'09[C]. Toyama, Japan, 2009.38-52.

[8] SEKAR G, S, PRENEEL B. New weaknesses in the keystream generation algorithms of the stream ciphers Tpy and Py[A]. Proceedings of ISC'07- 10th Information Security Conference on Information Security[C]. Dresden, Germany, 2007. 249-262.

作者简介：



高海英(1978-)，女，河南沈丘人，博士，解放军信息工程大学副教授，主要研究方向为密码理论。

金晨辉（1965-），男，河南扶沟人，博士，解放军信息工程大学教授、博士生导师，主要研究方向为密码理论。