针对流密码 HC-256′的区分攻击

李顺波* 胡予濮 王 艳
(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

摘 要：流密码 HC-256′是 eSTREAM 计划候选密码 HC-256 的改进算法，至今未见关于 HC-256′的安全性分析结果。该文提出了一种针对 HC-256′的线性区分攻击，利用不同的非线性函数代替内部状态更新函数来寻找偶数位置上密钥流生成序列的弱点，通过线性逼近 HC-256′的内部状态构造区分器。分析结果表明，需要约 2^{281} bit，就能以 0.9545 的区分优势对密钥流进行区分。同时，该攻击为解决 Sekar 等人在 2009 年 IWSEC 会议上提出的问题进行了有益的探索。

关键词：密码分析；流密码；区分攻击；eSTREAM；HC-256
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2012)04-0807-05
DOI: 10.3724/SP.J.1146.2011.00863

Distinguishing Attack on Stream Cipher HC-256′

Li Shun-bo Hu Yu-pu Wang Yan
(*Key Lab of Computer Network and Information Security, Xidian University, Xi'an* 710071, *China*)

Abstract: Stream cipher HC-256′ is an improved algorithm of HC-256 which is proposed as a candidate to the eSTREAM project. Until now, there has not any cryptanalysis on HC-256′. In this paper, a linear distinguishing attack on HC-256′ is presented. This method uses different nonlinear functions instead of state update functions to exploit the weaknesses in the even positions output bits of the keystream generation sequence. By linear approximation to the internal state bits, a distinguisher is built. The result shows that there needs about 2^{281} bit keystream with advantage 0.9545 to distinguish HC-256′ form random sequence. Thereby, this is a beneficial attempt to solve a problem which is given by Sekar et al in IWSEC 2009.

Key words: Cryptanalysis; Stream cipher; Distinguishing attack; eSTREAM; HC-256

1 引言

为进一步推进流密码的研究，2004 年欧洲启动了 eSTREAM 计划[1]，主要任务是征集安全快速的流密码算法，至 2005 年 4 月，共征集到 34 个候选算法。HC-256[2]和 HC-128[3]都是基于表驱动的候选流密码算法，由于其运行速度快、安全性能高，至今未见有效的分析方法。为了避免从系统内部恢复出初始密钥，文献[2]设计了 HC-256 的改进算法——HC-256′，其内部状态 P 和 Q 每运行一步就交替更新一次，具有更高的安全性；还未发现任何关于 HC-256′的分析结果，其安全性分析已经成为一个热点问题。

文献[4]利用线性逼近区分攻击对流密码 HC-256 进行了安全性分析，需要约 $2^{279.8}$ bit 的密钥流字节就可以把密钥流序列和随机序列区分；然而对 HC-256 的改进算法 HC-256′能否利用区分攻击进行安全性分析是一个有意义的研究课题。本文提出了一种针对流密码 HC-256′的线性区分攻击。首先利用假设检验给出了区分优势的计算公式；然后，对偶数位置上的输出序列字节利用不同的非线性函数表示不同的内部状态更新函数，在最低位比特通过线性逼近构建几乎最优区分器。结果表明，需要约 2^{281} bit 就能以 0.9545 的区分优势将 HC-256′的密钥流序列和随机序列区分开。

2 基础知识

2.1 区分攻击

区分攻击[5](distinguishing attack)是一种灵活有效的密码分析方法，2002 年由 Coppersmith 等人提出，其基本思想是通过观察某些输入与输出比特之间的关系来判别这些比特是来自真随机源还是来

2011-08-19 收到，2011-11-25 改回
国家 973 计划项目(2007CB311201)，保密通信国防科技重点实验室基金(9140C110201110C1102)，国家自然科学基金(60970119, 60833008)和西安建筑科技大学青年基金(QN1024)资助课题
*通信作者：李顺波 shunboli@163.com

自密码，将其转化为一个假设检验问题。尽管从攻击结果上看，区分攻击是最弱的，但面对区分攻击，密码设计者往往很难做到疏而不漏。因此区分攻击已经成为判定密码性质好坏的一个严格的安全标准。许多流密码算法都遭到区分攻击的威胁，如Shannon[6,7], SN3[8]和 RC4[9,10]等。

区分攻击的关键是寻找适当的区分器，更具体地说，区分器是指区分一串密钥流和一串真正随机序列的一种有效算法，且以密钥流的某些弱点为基础，而正是这些弱点体现了给定的密钥流具有的不随机性。区分器就是利用这些弱点来设计算法的。

一个区分器D 将密钥流生成器与随机生成器区分开的成功性称为区分优势(或成功概率)，由以下两个概率决定：

(1)当所给序列来自于密钥流生成器时，回答为“密钥流序列”的概率 $P_0(D)$；

(2)当所给序列来自于随机生成器时，回答为“密钥流序列”的概率 $P_1(D)$。

定义1[11] 区分优势就是将给定序列判定为密钥流序列的概率与将随机序列判定为密钥流序列的概率之差。记为 $\mathrm{Adv}(D)$，即 $\mathrm{Adv}D=\left|P_0(D)-P_1(D)\right|$。

定义2[7] 设 $\Pr(D)$ 为一个逼近D成立的概率，则偏差 $\varepsilon=2\Pr(D)-1$，即 $\Pr(D)=(1/2)(1+\varepsilon)$。

2.2 假设检验

设原假设 H_0：序列 X 来自密钥流生成器，即 $P_X=P_0(z_i)$；

备择假设 H_1：序列 X 来自随机生成器，即 $P_X=P_1(z_i)$。

为区分序列 $X=\{z_0,z_1,\cdots,z_{N-1}\}$ 来自密钥流序列还是随机序列，利用 Neyman-Pearson 引理和文献[11-13]中区分优势的计算方法。记 N 为序列 X 的样本数，$\varepsilon_z=P_0(z_i)-P_1(z_i)$，渐进似然率为 $\mathrm{LLR}=\sum_{i=0}^{N-1}\log_2\frac{P_0(z_i)}{P_1(z_i)}$，两分布 P_0 和 P_1 的变分距离为 $D(P_0\,||\,P_1)=\sum_{z_i\in\{0,1\}}P_0(z_i)\log_2\frac{P_0(z_i)}{P_1(z_i)}$；且满足 $D(P_0\,||\,P_1)\approx\frac{1}{2}\sum_{z_i\in\{0,1\}}\frac{\varepsilon_z}{P_1(z_i)}$。则区分攻击算法如下。

区分攻击算法

输入：N bit 序列$(z_0,z_1,\cdots,z_{N-1})$

输出：序列来自随机序列还是密钥生成序列

(1)计算 $\mathrm{LLR}=\sum_{i=0}^{N-1}\log_2\frac{P_0(z_i)}{P_1(z_i)}$

(2)如果 $\mathrm{LLR}\ge 0$，输出“序列来自密码”，否则，输出“序列来自随机序列”。

因此，该区分优势为 $\mathrm{Adv}(D)=|\,P_0[D(z_i)=1]-P_1[D(z_i)=1]\,|$，其中 $D(z_i)=\begin{cases}1, & \mathrm{LLR}\ge 0\\ 0, & \text{其它}\end{cases}$。

由于统计量 $D(z_i)\in\{0,1\}$ 服从二项分布，且是独立同分布的随机变量。当 N 无限增大时，利用中心极限定理，该二项分布无限趋于标准正态分布，

$$\Pr\left(\frac{\mathrm{LLR}-N\mu_i}{\sigma_i\sqrt{N}}<t\,|\,P_X=P_i\right)\xrightarrow{N\to\infty}\Phi(t),\ \ i=0,1$$

即

$$P_0[D(z)=1]=P_0[\mathrm{LLR}\ge 0]\approx\Phi\left(\frac{\sqrt{N}\mu_0}{\sigma_0}\right)$$

$$P_1[D(z)=1]=P_1[\mathrm{LLR}\ge 0]\approx\Phi\left(\frac{\sqrt{N}\mu_1}{\sigma_1}\right)$$

其中 $\Phi(t)$ 为标准正态分布函数，μ_0,μ_1 分别为统计量 $D(z_i)$ 在假设 H_0 和 H_1 下的数学期望，即 $\mu_0=D(P_0\,||\,P_1)$，$\mu_1=-D(P_1\,||\,P_0)$；σ_0,σ_1 为其对应的标准方差，且满足 $\sigma_j^2=\sum_{z_i}P_j(z_i)\left(\log_2\frac{P_0(z_i)}{P_1(z_i)}\right)^2-\mu_j^2$，$j=0,1$；化简得

$$\mu_0\approx-\mu_1\approx\frac{1}{2}\sum\frac{\varepsilon_z^2}{P_1(z_i)},\quad\sigma_0^2\approx\sigma_1^2\approx\sum\frac{\varepsilon_z^2}{P_1(z_i)}$$

令常数 d 满足 $N=\dfrac{d}{\sum\frac{\varepsilon_z^2}{P_1(z_i)}}$，则 $\mu_0=\frac{1}{2}\sqrt{\frac{d}{N}}\,\sigma_0$。

所以

$$\begin{aligned}\mathrm{Adv}(D)&=|\,P_0[D(z)=1]-P_1[D(z)=1]\,|\\&\approx\Phi\left(\frac{\sqrt{N}\mu_0}{\sigma_0}\right)-\Phi\left(\frac{\sqrt{N}\mu_1}{\sigma_1}\right)\\&=\Phi\left(\frac{\sqrt{N}\mu_0}{\sigma_0}\right)-\Phi\left(-\frac{\sqrt{N}\mu_0}{\sigma_0}\right)\\&=2\Phi\left(\frac{\sqrt{N}\mu_0}{\sigma_0}\right)-1=2\Phi(\sqrt{d}/2)-1\end{aligned}$$

当 $\varepsilon_z<<P_1(z_i)$，且随机分布 $P_1(z_i)=1/2$ 时，由表 1 计算得 $\sum\frac{\varepsilon_z^2}{P_1(z_i)}\approx\varepsilon^2$，则 $d=\varepsilon^2\cdot N$，即 $\mathrm{Adv}(D)=2\Phi\left(\frac{\varepsilon\sqrt{N}}{2}\right)-1$。因此得到了定理 1。

表 1 $P_j(z_i)$ 和 ε_z 的取值

	$P_0(z_i)$	$P_1(z_i)$	ε_z
$z_i=0$	$(1+\varepsilon)/2$	$1/2$	$\varepsilon/2$
$z_i=1$	$(1-\varepsilon)/2$	$1/2$	$-\varepsilon/2$

定理 1　若偏差 $\varepsilon = 2\Pr(D) - 1$，则区分攻击的区分优势为 $\mathrm{Adv}(D) = 2\Phi\left(\frac{\varepsilon\sqrt{N}}{2}\right) - 1$，其中 Φ 为标准正态分布，N 为区分攻击所需要的密钥流比特。

同时，给出文献[2]中一个重要引理。

引理 1[2]　设 H 是 m bit 输入 n bit 输出的 S-盒，且 $m \geq n$。若 x_1, x_2 是 H 的两个随机 m bit 输入，则 $\Pr[H(x_1) = H(x_2)] = 2^{-m} + 2^{-n} - 2^{-m-n}$。

3　流密码 HC-256′

流密码 HC-256′ 是 HC-256 的改进算法，都是文献[2]中提出的面向软件实现的快速同步流密码，256 bit 密钥(K)和 256 bit 初始化向量($\boldsymbol{IV}$)，内部状态 P 和 Q 都为 1024 bit。HC-256′ 借鉴了 RC4 的思想，同时引入了面向字节的非线性函数来更新系统的内部状态，运行速度很快，具有更高的安全性。其初始化和非线性函数都和 HC-256 是一样的；但唯一的差别在于密钥流生成算法。HC-256 的密钥流生成算法是连续运行 1024 步更新一次状态 P，再连续运行 1024 步更新另一个状态 Q。而 HC-256′ 的密钥流生成算法是内部状态 P 和 Q 每运行一步就需要更新一次。具体算法如 3.1 节–3.3 节所述。

3.1 运算符号

流密码 HC-256′ 中的运算符号标注如下：

+：$x + y$ 表示 $x + y \bmod 2^{32}$；

⊟ ：$x \boxminus y$ 表示 $x - y \bmod 1024$；

$>>$ ：右平移算子，$x >> n$ 表示 x 向右平移 n bit；

$>>>$ ：右循环算子，$x >>> n$ 表示 x 向右循环移动 n bit，即 $(x >> n) \oplus (x << (32-n))$，$0 \leq n < 32$。

3.2 密钥初始化

密钥初始化过程中，内部状态是密钥和初始化向量的级联，256 bit 的密钥和初始化向量被分为 8 个 32 bit 的字，记为：$K = K_0 \,||\, K_1 \,||\, \cdots \,||\, K_7$ 和 $\boldsymbol{IV} = IV_0 \,||\, IV_1 \,||\, \cdots \,||\, IV_7$。将密钥和初始化向量扩展到 2560 个数组 W_i $(0 \leq i \leq 2559)$

$$W_i = \begin{cases} K_i, & 0 \leq i \leq 7 \\ IV_{i-8}, & 8 \leq i \leq 15 \\ f_2(W_{i-2}) + W_{i-7} + f_1(W_{i-15}) + W_{i-16} + i, & 16 \leq i \leq 2559 \end{cases}$$

其中

$$f_1(x) = (x >>> 7) \oplus (x >>> 18) \oplus (x >> 3)$$

$$f_2(x) = (x >>> 17) \oplus (x >>> 19) \oplus (x >> 10)$$

$$g_1(x,y) = ((x >>> 10) \oplus (y >>> 23)) + Q[(x \oplus y) \bmod 1024]$$

$$g_2(x,y) = ((x >>> 10) \oplus (y >>> 23)) + P[(x \oplus y) \bmod 1024]$$

$$h_1(x) = Q[x_0] + Q[256 + x_1] + Q[512 + x_2] + Q[768 + x_3]$$

$$h_2(x) = P[x_0] + P[256 + x_1] + P[512 + x_2] + P[768 + x_3]$$

其中 h_1, h_2 表示 32 bit 输入和 32 bit 输出的 S 盒，32 bit 字 $x = x_3 \,||\, x_2 \,||\, x_1 \,||\, x_0$ 中 x_0 表示 x 的最低位字节(least significant bit)，x_3 表示 x 的最高位字节(most significant bit)。

两数组 P 和 Q 表示 32 bit 内部状态，分别为：$P[i] = W_{i+512}$，$Q[i] = W_{i+1536}$，$0 \leq i \leq 1023$。

3.3 密钥流生成器

初始化 4096 步后输出密钥流比特 s_i，生成的密钥流长度为 2^{128} bit；其算法如下：

$i = 0$;

repeat until enough keystream bits are generated.

{

$j = i \bmod 1024$;

$P[j] = P[j] + P[j \boxminus 10] + g_1(P[j \boxminus 3], P[j \boxminus 1023])$;

$s_{2i} = h_1(P[j \boxminus 12]) \oplus P[j]$;

$Q[j] = Q[j] + Q[j \boxminus 10] + g_2(Q[j \boxminus 3], Q[j \boxminus 1023])$;

$s_{2i+1} = h_2(Q[j \boxminus 12]) \oplus Q[j]$;

$i = i + 1$; // each increment of i corresponds to 2 steps

}

end repeat

4　区分攻击 HC-256′

本节利用区分攻击分析流密码 HC-256′ 的安全性，关键是寻找 HC-256′ 密钥流生成器的弱点，而其困难在于内部状态 P 和 Q 每运行一步就要更新一次，P 和 Q 更新时的非线性函数是不同的。本文提出了一种新的区分攻击思想，把问题转化为判断在偶数(奇数)位置上的输出序列是来自密钥流序列还是随机序列。利用不同的非线性函数来表示不同的内部状态更新函数，旨在讨论在最低位比特状态 P 和密钥流 s_{2i} 的弱点。

已知在偶数位置上的密钥流输出算法为

$$P[i \bmod 1024] = P[i \bmod 1024] + P[i \boxminus 10] + g_1(P[i \boxminus 3], P[i \boxminus 1023])$$

$$s_{2i} = h_1(P[i \boxminus 12]) \oplus P[i \bmod 1024]$$

当 $10 \leq (i \bmod 1024) < 1023$ 时，记 $z_i = P[i \boxminus 12]$ 为 32 bit 字，$P[i \bmod 1024] = s_{2i} \oplus h_1(z_i)$，所以 $P[i \boxminus 10] = P[(i-10) \bmod 1024] = s_{2i-20} \oplus h_1''(z_{i-10})$。同理，

$P[i\boxminus 3]=s_{2i-6}\oplus h_2^{'}(z_{i-3})$, $P[i\boxminus 1023]=s_{2i-2046}\oplus h_2^{''}(z_{i-1023})$, $z_i=z_{i-1024}+z_{i-10}+g_1(z_{i-3},z_{i-1023})$。

因此在偶数位置上的反馈函数可以写成如下形式：

$$\begin{aligned}s_{2i}\oplus h_1(z_i)=&(s_{2i-2048}\oplus h_1^{'}(z_{i-1024}))\\&+(s_{2i-20}\oplus h_1^{''}(z_{i-10}))+g_1(s_{2i-6}\\&\oplus h_2^{'}(z_{i-3}),s_{2i-2046}\oplus h_2^{''}(z_{i-1023}))\end{aligned}\tag{1}$$

其中 $h_1(x),h_1^{'}(x),h_1^{''}(x),h_2^{'}(x),h_2^{''}(x)$ 是 5 个不同的 S-盒，分别代表对应的内部状态更新的非线性函数。

对于模 2^{32} 加法，直接把式(1)的密钥流序列区分开是非常困难的。但值得注意的是，在最低位比特，运算‘+’和‘$\oplus$’是一样的。因此，利用函数 $g_1(x)$，在最低位比特式(1)可以写成下列形式：

$$\begin{aligned}&s_{2i(0)}\oplus s_{2i-2048(0)}\oplus s_{2i-20(0)}\oplus s_{2i-6(10)}\oplus s_{2i-2046(23)}\\&=(h_1(z_i))_{(0)}\oplus(h_1^{'}(z_{i-1024}))_{(0)}\oplus(h_1^{''}(z_{i-10}))_{(0)}\\&\quad\oplus(h_2^{'}(z_{i-3}))_{(10)}\oplus(h_2^{''}(z_{i-1023}))_{(23)}\oplus(Q[r_i])_{(0)}\end{aligned}\tag{2}$$

其中 $r_i=(s_{2i-6}\oplus h_2^{'}(z_{i-3})\oplus s_{2i-2046}\oplus h_2^{''}(z_{i-1023}))\bmod 1024$，且为 10 bit 字节。

同理，当 $1024\cdot\alpha+10\le i,j<1024\cdot\alpha+1023$，且 $i\ne j$ 时有

$$\begin{aligned}&s_{2j(0)}\oplus s_{2j-2048(0)}\oplus s_{2j-20(0)}\oplus s_{2j-6(10)}\oplus s_{2j-2046(23)}\\&=(h_1(z_j))_{(0)}\oplus(h_1^{'}(z_{j-1024}))_{(0)}\oplus(h_1^{''}(z_{j-10}))_{(0)}\\&\quad\oplus(h_2^{'}(z_{j-3}))_{(10)}\oplus(h_2^{''}(z_{j-1023}))_{(23)}\oplus(Q[r_j])_{(0)}\end{aligned}\tag{3}$$

其中 $r_j=(s_{2j-6}\oplus h_2^{'}(z_{j-3})\oplus s_{2j-2046}\oplus h_2^{''}(z_{j-1023}))\bmod 1024$。要使得式(2)，式(3)在最低位比特时相等，即

$$\begin{aligned}&s_{2i(0)}\oplus s_{2i-2048(0)}\oplus s_{2i-20(0)}\oplus s_{2i-6(10)}\oplus s_{2i-2046(23)}\\&=s_{2j(0)}\oplus s_{2j-2048(0)}\oplus s_{2j-20(0)}\oplus s_{2j-6(10)}\\&\quad\oplus s_{2j-2046(23)}\end{aligned}\tag{4}$$

等价于下面等式成立：

$$\begin{aligned}&(h_1(z_i))_{(0)}\oplus(h_1^{'}(z_{i-1024}))_{(0)}\oplus(h_1^{''}(z_{i-10}))_{(0)}\\&\quad\oplus(h_2^{'}(z_{i-3}))_{(10)}\oplus(h_2^{''}(z_{i-1023}))_{(23)}\oplus(Q[r_i])_{(0)}\\&=(h_1(z_j))_{(0)}\oplus(h_1^{'}(z_{j-1024}))_{(0)}\oplus(h_1^{''}(z_{j-10}))_{(0)}\\&\quad\oplus(h_2^{'}(z_{j-3}))_{(10)}\oplus(h_2^{''}(z_{j-1023}))_{(23)}\oplus(Q[r_j])_{(0)}\end{aligned}\tag{5}$$

由于 $z_i=z_{i-1024}+z_{i-10}+g_1(z_{i-3},z_{i-1023})$, $z_j=z_{j-1024}+z_{j-10}+g_1(z_{j-3},z_{j-1023})$。则式(5)可变为

$$\begin{aligned}&(h_1(z_{i-1024}+z_{i-10}+g_1(z_{i-3},z_{i-1023})))_{(0)}\oplus(h_1^{'}(z_{i-1024}))_{(0)}\\&\oplus(h_1^{''}(z_{i-10}))_{(0)}\oplus(h_2^{'}(z_{i-3}))_{(10)}\oplus(h_2^{''}(z_{i-1023}))_{(23)}\\&\oplus(Q[r_i])_{(0)}=(h_1(z_{j-1024}+z_{j-10}+g_1(z_{j-3},z_{j-1023})))_{(0)}\\&\oplus(h_1^{'}(z_{j-1024}))_{(0)}\oplus(h_1^{''}(z_{j-10}))_{(0)}\oplus(h_2^{'}(z_{j-3}))_{(10)}\\&\oplus(h_2^{''}(z_{j-1023}))_{(23)}\oplus(Q[r_j])_{(0)}\end{aligned}\tag{6}$$

根据上述推理，式(4)就是我们构造的区分器。式(4)成立的概率等价于式(6)成立的概率。而式(6)左边含有 138 bit 变量 $z_{i-3},z_{i-10},z_{i-1023},z_{i-1024}$ 和 r_i，记 $x_1=z_{i-3}\,||\,z_{i-10}\,||\,z_{i-1023}\,||\,z_{i-1024}\,||\,r_i$。式(6)右边也含有 138 bit 变量 $z_{j-3},z_{j-10},z_{j-1023},z_{j-1024}$ 和 r_j；记为 $x_2=z_{j-3}\,||\,z_{j-10}\,||\,z_{j-1023}\,||\,z_{j-1024}\,||\,r_j$。我们可以将式(6)两边看作两个 S-盒函数，要使得式(6)成立，就要满足以 138 bit 为变量的两个 S-盒相等，即 $H(x_1)=H(x_2)$。其中 H 表示随机选择的 138 bit 输入−1 bit 输出的 S-盒。利用引理 1，式(6)成立的概率为 $1/2+2^{-139}$。

因此，区分器式(4)成立的概率为 $p=1/2+2^{-139}=(1/2)(1+2^{-138})$。所以该区分器的偏差为 $\varepsilon=2^{-138}$。利用定理 1，当密钥流比特 $N=\varepsilon^{-2}=2^{276}$ 时，该区分攻击的区分优势为 0.3928；当 $N=16\cdot\varepsilon^{-2}=2^{280}$ 时，该攻击以 0.9545 的区分优势把密钥流序列和随机序列区分开。

然而，该区分攻击只讨论了在偶数位置上 HC-256′ 的安全性，用同样的方法可以分析在奇数位置上的安全性。综上所述，需要约 $2\cdot N=2^{281}$ bit 密钥流就能以 0.9545 的区分优势把流密码 HC-256′ 与随机序列区分开。

5 结束语

本文利用线性区分攻击分析了流密码 HC-256′ 的安全性，通过线性逼近内部状态寻找密钥流生成器的弱点建立区分器，区分密钥流序列和随机序列需要约 2^{281} bit；且该攻击的区分优势为 0.9545。虽然该结果超过了密钥流序列的长度，但从理论上回答了 2009 年 Sekar 等人提出的开放问题。然而，近年来对 HC-256 的简化算法 HC-128 的研究仅限于文献[14–17]，能否利用区分攻击对流密码 HC-128 进行有效的安全性分析仍然是一个有意义的问题，值得做进一步研究。

参 考 文 献

[1] eSTREAM—the Ecrypt Stream Cipher Project[EB]. http://www.ecrypt.eu.org /stream/, 2005.

[2] Wu Hong-jun. A new stream cipher HC-256[C]. FSE 2004, New Delhi, India, 2004, 3017: 524–538.

[3] Wu Hong-jun. The stream cipher HC-128[C]. New Stream Cipher Designs, 2008, 4986: 39–47.

[4] Sekar G and Preneel B. Improved distinguishing attacks on HC-256[C]. IWSEC 2009, Toyama, Japan, 2009, 5824: 38–52.

[5] Coppersmith D, Halevi S, and Jutla C. Cryptanalysis of stream ciphers with linear masking[C]. CRYPTO 2002, Santa Barbara, California, 2002, 2442: 515–532.

[6] Ahmadian Z, Mohajeri J, Salmasizadeh M, *et al*.. A practical distinguisher for the Shannon cipher[J]. *The Journal of Systems and Software*, 2010, 83(4): 543–547.

[7] 常亚勤, 金晨辉. 对Shannon算法的线性区分攻击[J]. 电子与信息学报, 2011, 33(1): 190–193.
Chang Ya-qin and Jin Chen-hui. Linear distinguishing attack on Shannon algorithm[J]. *Journal of Electronics & Information Technology*, 2011, 33(1): 190–193.

[8] Keller N and Miller S D. Distinguishing attack on stream ciphers based on arrays of pseudo-random words[J]. *Information Processing Letters*, 2010, 110(4): 129–132.

[9] Maitra S, Paul G, and Gupta S. Attack on broadcast RC4 revisited[C]. FSE 2011, Lyngby, Denmark, 2011, 6733: 199–217.

[10] Sepehrdad P, Vaudenay S, and Vuagnoux M. Statistical attack on RC4 distinguishing WPA[C]. EUROCRYPT 2011, Tallinn, 2011, 6632: 343–363.

[11] Baigneres T, Junod P, and Vandenay S. How far can we go beyond linear cryptanalysis[C]. Asiacrypt 2004, Jeju Island, Korea, 2004, 3329: 432–450.

[12] Hell M, Johansson T, and Brynielsson L. An overview of distinguishing attacks on stream ciphers[J]. *Cryptography and Communications*, 2009, 1(1): 71–94.

[13] Crowley P. Improved cryptanalysis of Py[C]. Workshop on the State of the Art of Stream Ciphers (SASC 2006), Leuven, Belgium, 2006: 52–60.

[14] Liu Yun-yi and Qin Tuan-fa. The key and IV setup of the stream ciphers HC-256 and HC-128[C]. Networks Security, Wireless Communications and Trusted Computing, Wuhan, IEEE, 2009: 430–433.

[15] Maitra S, Paul G, and Raizada S. Some observations on HC-128[J]. *Designs, Codes and Cryptography*, 2010, 57(3): 1–15.

[16] Kircanski A and Youssef A M. Differential fault analysis of HC-128[C]. Africrypt 2010, South Africa, 2010, 6055: 261–278.

[17] Paul G, Maitra S, and Raizada S. A combinatorial analysis of HC-128[R]. Cryptology ePrint Archive, Report 2010/387, 2010.

李顺波：　男，1979 年生，讲师，博士生，研究方向为流密码的分析与设计.

胡予濮：　男，1955 年生，教授，博士生导师，长期从事密码学、信息安全等方面的研究.

王　艳：　女，1982 年生，讲师，博士生，研究方向为密码函数理论及其应用.