CLEFIA-128算法的不可能差分密码分析

邱丰品 卫宏儒

(北京科技大学数理学院 北京 100083)

摘 要 为研究分组密码CLEFIA-128抵抗不可能差分攻击的能力,基于一条9轮不可能差分路径,分析了13轮不带白化密钥的CLEFIA-128算法。利用轮函数中S盒差分分布表恢复部分密钥,利用轮密钥之间的关系减少密钥猜测量,并使用部分密钥分别猜测(Early Abort)技术有效地降低了复杂度。计算结果表明,该方法的数据复杂度和时间复杂度分别为$O(2^{103.2})$和$O(2^{124.1})$。

关键词 分组密码,不可能差分攻击,CLEFIA-128,S盒,Early Abort技术

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.11.043

Impossible Differential Cryptanalysis of CLEFIA-128

QIU Feng-pin WEI Hong-ru

(School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 100083, China)

Abstract To study the ability to resist the impossible differential cryptanalysis of the block cipher CLEFIA-128, the 13-round CLEFIA-128 without whitening key was analyzed based on one 9-round impossible differential role. It uses the output and input differences of S-boxes to recover round keys, utilizes the keys relations to reduce the number of guessed keys, and introduces the key-byte guessing(Early Abort) technique to reduce the complexity effectively. Computing result shows that the data complexity and time complexity of this method are $O(2^{103.2})$ and $O(2^{124.1})$ respectively.

Keywords Block cipher, Impossible differential attack, CLEFIA-128, S-box, Early Abort technique

1 引言

不可能差分分析[1]是由Biham提出来的,它作为差分密码分析的变形,因具有简单的分析过程和高效的攻击能力而引起了人们的广泛关注。不可能差分分析一般包括两个步骤:构造不可能差分路径和恢复密钥。不可能差分路径的构造是通过寻找加密方向概率为1的差分路径和解密方向概率为1的差分路径,在中间处构成矛盾,从而得到一条概率为0的路径。在恢复密钥阶段,利用构造的不可能差分链,得到满足差分链前后若干轮的明密文对,猜测相应的轮密钥,部分加解密后,所有符合该不可能差分链的候选密钥都是错误的,通过筛选掉这些错误的密钥猜测,再结合其它技术如穷举搜索等可恢复正确密钥。

CLEFIA算法[2,3]是索尼公司在FSE2007上提出的一种新的分组密码算法,它的数据分组长度为128比特,密钥长度为128/192/256比特,分别记为CLEFIA-128、CLEFIA-192和CLEFIA-256,相应的迭代轮数为18轮、22轮和26轮。CLEFIA安全性分析报告[4]给出了两条9轮不可能差分路径。王薇等人[5,6]基于一个不可能差分路径,提出了生日筛选法,将CLEFIA的不可能差分攻击扩展到12轮的CLEFIA-128/192/256、13轮的CLEFIA-192/256以及14轮的CLEFIA-256,改进了不可能差分的攻击结果。Tsunoo等人[7]结合线性变换的分支数即5,提出了新的9轮不可能差分路径,并将攻击结果扩展到12轮的CLEFIA-128/192/256、13轮的CLEFIA-192/256以及14轮的CLEFIA-256,进一步改进了对CLEFIA的不可能差分攻击结果。文献[8]称找到一个14轮无白化密钥的CLEFIA-128的不可能差分攻击,但最终被证实该攻击不成功。唐学海和Hamid Mala等人[9,10]都使用了两类9轮不可能差分路径,结合轮子密钥之间的关系,并使用Early Abort[11]技术成功攻击了带白化密钥和不带白化密钥的13轮CLEFIA-128算法。文献[12]利用9轮不可能差分路径分析了不带白化密钥的13轮CLEFIA-128算法。

本文在一个9轮不可能差分路径的基础上,利用S盒差分分布表,同时结合轮密钥之间的关系和Early Abort技术,分析了未使用白化密钥的13轮CLEFIA-128算法,数据复杂度低于之前分析无白化密钥的13轮CLEFIA-128的数据复杂度。

2 CLEFIA-128算法

CLEFIA算法采用具有4个分支的广义Feistel结构,每个分支32bit数据,且白化密钥作用在开头和结尾轮。本文

到稿日期:2014-11-16 返修日期:2015-02-01 本文受2013年国家自然科学基金(61272476),内蒙古自治区科技创新引导奖励资金(2012)资助。

邱丰品(1990—),女,硕士,主要研究方向为密码学,E-mail:qiufengpin1101@163.com(通信作者);卫宏儒(1963—),男,副教授,主要研究方向为数学、信息安全与密码学、物联网关键技术。

只给出加密流程，如图 1 所示。

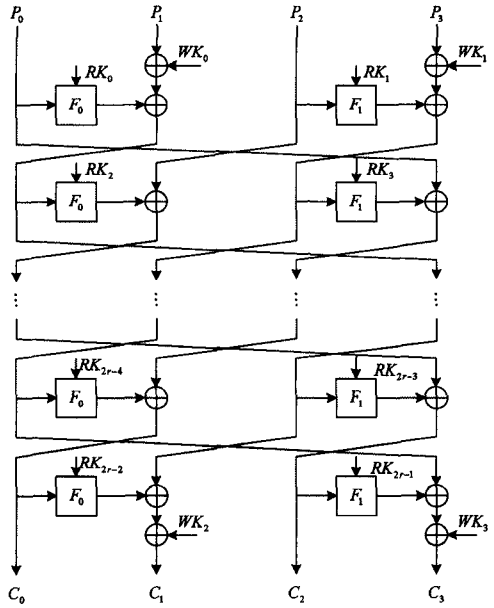

图 1　CLEFIA 算法的加密流程

2.1　符号说明

对算法中符号的说明如下：

$P=P_0 \mid P_1 P_2 \mid P_3$：128bit 明文 P 由 4 个 32bit 字 P_i 连接；

$C=C_0 \mid C_1 \mid C_2 \mid C_3$：128bit 密文 C 由 4 个 32bit 字 C_i 连接；

C^r, C^{r^*}：第 r 轮输出；

$C_i^r, C_i^{r^*}$：C^r, C^{r^*} 的第 $i(0 \leqslant i<4)$ 个 32bit 字；

$\Delta P, \Delta C$：明文差分和密文差分；

ΔC_i^r：第 r 轮输出中第 i 个 32bit 字的差分；

$RK_{i,j}$：轮密钥 RK_i 的第 j 个字节；

$X[a-b]$：X 中的第 a bit 到第 $b$bit；

$M_i(a)$：矩阵 M_i 对输入 32bit 字 a 做运算。

2.2　CLEFIA 算法简介

$WK_0, WK_1, WK_2, WK_3 \in \{0,1\}^{32}$ 是白化密钥，$RK_i \in \{0,1\}^{32}(0 \leqslant i<2r)$ 为轮密钥，由密钥扩展算法得到。算法具体如下：

(1) $C_0^0=P_0, C_1^0=P_1 \oplus WK_0, C_2^0=P_2, C_3^0=P_3 \oplus WK_1$

(2) 对 $i=1,2,\cdots,r-1$ 做如下计算：

$C_0^i=C_1^{i-1} \oplus F_0(C_0^{i-1}, RK_{2i-2}), C_1^i=C_2^{i-1}$

$C_2^i=C_3^{i-1} \oplus F_1(C_2^{i-1}, RK_{2i-1}), C_3^i=C_0^{i-1}$

(3) 最后一轮 r：

$C_0^r=C_0^{r-1}, C_1^r=C_1^{r-1} \oplus F_0(C_0^{r-1}, RK_{2i-2}) \oplus WK_2$

$C_2^r=C_2^{r-1}, C_3^r=C_3^{r-1} \oplus F_1(C_2^{r-1}, RK_{2i-1}) \oplus WK_3$

F_0 和 F_1 的定义表述如下：

$$F_0(C_0^{i-1}, RK_{2i-2})=M_0\begin{Bmatrix} S_0(C_{0,0}^{i-1} \oplus RK_{2i-2,0}) \\ S_1(C_{0,1}^{i-1} \oplus RK_{2i-2,1}) \\ S_0(C_{0,2}^{i-1} \oplus RK_{2i-2,2}) \\ S_1(C_{0,3}^{i-1} \oplus RK_{2i-2,3}) \end{Bmatrix}$$

$$F_1(C_2^{i-1}, RK_{2i-1})=M_1\begin{Bmatrix} S_1(C_{2,0}^{i-1} \oplus RK_{2i-1,0}) \\ S_0(C_{2,1}^{i-1} \oplus RK_{2i-1,1}) \\ S_1(C_{2,2}^{i-1} \oplus RK_{2i-1,2}) \\ S_0(C_{2,3}^{i-1} \oplus RK_{2i-1,3}) \end{Bmatrix}$$

其中，S_0 和 S_1 是 2 个非线性 8×8 的 S 盒，M_0 和 M_1 是 4×4 的 Hadamard 字节矩阵。矩阵中的元素属于由不可约多项式 $z^8+z^4+z^3+z^2+1$ 确定的有限域 F_{2^8}。

$$M_0=\begin{pmatrix} 01 & 02 & 04 & 06 \\ 02 & 01 & 06 & 04 \\ 04 & 06 & 01 & 02 \\ 06 & 04 & 02 & 01 \end{pmatrix}, M_1=\begin{pmatrix} 01 & 08 & 02 & 0a \\ 08 & 01 & 0a & 02 \\ 02 & 0a & 01 & 08 \\ 0a & 02 & 08 & 01 \end{pmatrix}$$

2.3　r 轮 CLEFIA-128 算法密钥扩展

CLEFIA 算法的种子密钥可以为 128bit，192bit，256bit，经过密钥扩展方案生成白化密钥 $WK_i(0 \leqslant i<4)$ 和轮密钥 $RK_j(0 \leqslant j<2r)$，其中 r 是加密轮数。下面介绍主密钥为 128bit 时 CLEFIA 的密钥扩展算法。CLEFIA-128 的密钥扩展算法主要包括两部分：密钥字的生成和轮密钥的选取。

(1)128bit 的密钥字 L 的生成。利用 24 个预先给定的 32bit 常数 $CON_i(0 \leqslant i<24)$ 作为轮密钥，种子密钥 $K=\| K_0 \| K_1 \| K_2 \| K_3 \|$ 作为输入，计算生成 128bit 密钥字 $L=E_{CON}(K)$，其中 E 表示没有初始和末尾白化的 12 轮 CLEFIA 算法。

定义如下基于比特的置换 Σ[4]：

Σ：

$$\begin{cases} \{0,1\}^{128} \to \{0,1\}^{128}, \\ X \mapsto X[7-63] \| X[121-127] \| X[0-6] \| X[64-120] \end{cases}$$

同时，给定另外 36 个 32bit 常数：$CON_i^{128}(24 \leqslant i<60)$。下面，利用这 36 个额外的常数和 Σ 置换对 K 和 L 进行变换，从而完成轮密钥的选取。

(2)轮密钥的选取

步骤 1　$WK_0 \| WK_1 \| WK_2 \| WK_3 \| =K$；

步骤 2　对 $i=0,1,2,\cdots,8$ 做如下变换：

$T=L \oplus (CON_{24+4i} \| CON_{24+4i+1} \| CON_{24+4i+2} \| CON_{24+4i+3} \|)$；

$L=\Sigma L$；

如果 i 是奇数：

$T=T \oplus K$；

$RK_{4i} \| RK_{4i+1} \| RK_{4i+2} \| RK_{4i+3}=T$。

3　CLEFIA-128 的几点理论

文献[5]与文献[9]分别给出 CLEFIA-128 的几点定理和性质：

定理 1[5]　对于 F 函数 (F_0, F_1)，若已知两个 32bit 输入 (In, In') 及相应的输出差分 ΔOut，则求解 F 函数的子密钥 RK 只需一次 F 运算。

性质 1[9]　若已知 32bit RK_{24}，可以计算 10bit 的 $RK_3[18-20,25-31]$，22bit $RK_1[10-31]$。

性质 2[9]　若已知 32bit RK_{25}，可以计算 10bit 的 $RK_2[22-31]$，22bit $RK_3[0-17,21-24]$。

性质 3[9]　9 轮不可能差分路径：对于 9 轮的 CLEFIA 算法，若明文差分为 $(0,00\alpha\beta,0,0)$，则输出差分不可能为 $(0,00\gamma 0,0,0)$，这条不可能差分路径记为 $(0,00\alpha\beta,0,0) \not\to (0,00\gamma 0,0,0)$。

4　CLEFIA-128 的不可能差分攻击

将 9 轮不可能差分 $(0,00\alpha\beta,0,0) \not\to (0,00\gamma 0,0,0)$ 用于第

3 轮到第 11 轮，下面将阐述没有白化的 13 轮 CLEFIA-128 的不可能差分攻击，如图 2 所示。

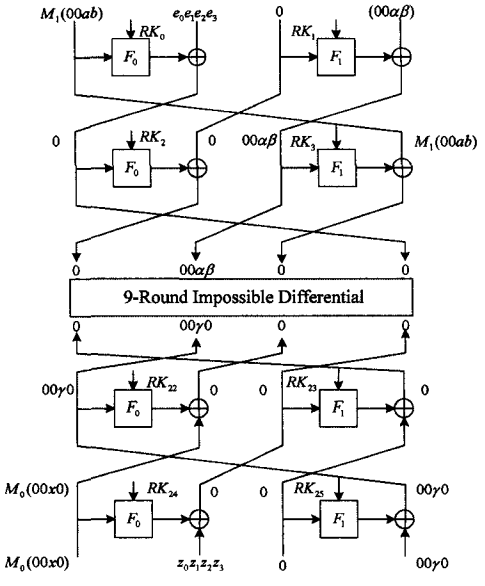

图 2　13 轮 CLEFIA-128 的不可能差分攻击

具体攻击步骤如下：

(1)选择明文

令明文的差分为：

$\Delta P_0=M_1(00ab)$，$\Delta P_1=(e_0e_1e_2e_3)$，$\Delta P_2=(0000)$，$\Delta P_3=(00\alpha\beta)$

定义如下明文结构：

$P_0=M_1(\alpha_1\alpha_2\beta_1\beta_2)$，$P_1=(\beta_3\beta_4\beta_5\beta_6)$，$P_2=(\alpha_3\alpha_4\alpha_5\alpha_6)$，$P_3=(\alpha_7\alpha_8\beta_7\beta_8)$

其中，$a,b,e_0,e_1,e_2,e_3,\alpha,\beta$ 为所有非零字节，$\alpha_i(1\leqslant i\leqslant 8)$是常数，$\beta_i(1\leqslant i\leqslant 8)$取任意值。该明文结构包括 2^{64} 个明文，可以形成 2^{127} 个明文对。本文选取 2^n 个结构，则共有 2^{n+64} 个明文、2^{n+127} 个数据对。

(2)过滤数据

经过 13 轮加密后的明文，选择密文对差分为 $\Delta C_0=M_0(00x0)$、$\Delta C_1=(z_0z_1z_2z_3)$、$\Delta C_2=(0000)$、$\Delta C_3=(00\gamma0)$的密文对，则过滤概率约为 2^{-80}，即大约剩余 2^{n+47} 个数据对满足这种形式的明文差分和密文差分。

(3)恢复密钥

1)恢复 32bit RK_0

由于明文 P_0 和 P_0^* 已知，根据 S 盒差分分布表，第 1 轮 S 盒的输入差分和输出差分分别为 $M_1(00ab)$，$M_0(e_0e_1e_2e_3)$，由定理 1 经过一次 F 运算，可计算 32bit RK_0。

2)恢复 32bit RK_{24}

由于密文 C_0 和 C_0^* 已知，根据 S 盒差分分布表，最后一轮 S 盒的输入差分和输出差分分别为 $M_0(00x0)$，$M_0(z_0z_1z_2z_3)$，由定理 1 经过一次 F 运算，可计算 32bit RK_{24}。

3)猜测 32bit RK_{25}

对剩余的数据对解密，解密密文(C_2^{13}，C_3^{13})和(C_2^{13*}，C_3^{13*})，得到第 12 轮部分输出 C_3^{12} 和 C_3^{12*}，易知密文差分 $C_3^{12}\oplus C_3^{12*}=(00\gamma0)$。此步不过滤数据对。

4)猜测 10bit RK_1

根据性质 1 可从 RK_{24} 中计算出 22bit RK_1，因此，只需猜测 $RK_1[0-9]$。此步不过滤数据对。

5)计算 16bit $RK_{3,2}$ 和 $RK_{3,3}$

根据性质 1 和性质 2 可从 RK_{24}、RK_{25} 中计算 16bit 的 $RK_{3,2}$ 和 $RK_{3,3}$。通过此步过滤的概率约为 2^{-16}，因此，大约剩余 2^{n+31} 个数据对。

6)计算 8bit $RK_{22,2}$

由密钥扩展方案，可从 RK_0 中计算出 8bit $RK_{22,2}$。

分析完第 6)步的数据对后，大约还有 $(2^{106}-1)(1-\frac{2^{42}}{2^{106}})^{2^{n+31}}$ 个猜测密钥，要完全淘汰错误密钥，则 $(2^{106}-1)(1-\frac{2^{42}}{2^{106}})^{2^{n+31}}<1$，则 $n=39.2$，即需要 $2^{39.2}$ 个明文结构，则攻击的数据复杂度为 $2^{103.2}$ 个选择明文，时间复杂度主要集中在以下各步：第 3)步为 $2\times\frac{1}{2}\times\frac{1}{13}\times2^{32}\times2^{n+47}\approx2^{114.5}$；第 4)步为 $2\times\frac{1}{4}\times\frac{1}{13}\times2^{42}\times2^{n+47}\approx2^{123.5}$；第 5)步为 $2\times\frac{1}{8}\times\frac{1}{13}\times2^{42}\times2^{n+47}+2\times\frac{1}{8}\times\frac{1}{13}\times2^{42}\times2^{n+39}\approx2^{122.5}$；第 6)步为 $2\times\frac{1}{8}\times\frac{1}{13}\times2^{106}\times\{1+(1-2^{-8})+(1-2^{-8})^2+\cdots+(1-2^{-8})^{2^{n+31}-1}\}\approx2^{108.3}$。

综上所述，攻击没有白化的 13 轮 CLEFIA-128 需要的数据复杂度为 $2^{103.2}$，时间复杂度为 $2^{124.1}$ 次 13 轮加密。

表 1 显示了未使用白化密钥的 13 轮 CLEFIA-128 算法的不可能差分密码分析结果比较。

表 1　无白化密钥的 13 轮 CLEFIA-128 算法的不可能差分密码分析结果比较

攻击轮数	数据复杂度	时间复杂度	参考文献
13	$2^{111.3}$	$2^{117.5}$	[9]
13	$2^{109.5}$	$2^{112.9}$	[10]
13	2^{120}	$2^{125.5}$	[12]
13	$2^{103.2}$	$2^{124.1}$	本文

结束语　本文利用已有的 9 轮不可能差分路径，将 S 盒差分分布表和过滤数据对的方法相结合，分析了未使用白化密钥的 13 轮 CLEFIA-128 算法，利用轮密钥间的关系减少了密钥猜测量，并使用 Early Abort 技术降低了计算复杂度。

参 考 文 献

[1] Biham E, Biryukov A, Shamir A. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials[C]// Advances in Cryptology-Eurocrypt, 1999. Springer Berlin Heidelberg, 1999:12-23

[2] Shirai T, Shibutani K, Akishita T, et al. The 128-bit Blockcipher CLEFIA (Extended Abstract) [C] // Proc. of FSE' 07. Dubrovnik, Croatia: [s. n.], 2007:181-195

[3] Sony Corporation. The 128-bit Blockcipher CLEFIA: Algorithm Specification Revision 1. 0[OL]. (2007-06-01). http://www.sony.net/products/cryptography/clefia/index.html,

[4] Sony Corporation. The 128-bit Blockcipher CLEFIA, Security and Performance Evaluations, Revision1. 0[EB/OL]. (2007-06-01). http://www.Sony.net/Products/cryptography/cle-fia/

[5] 王薇. 分组密码 CLEFIA 与基于四圈 AES 的消息认证码的安全性分析[D]. 济南:山东大学,2009
Wang Wei. Cryptanalysis of Block Cipher CLEFIA and MACs based on four rounds AES[D]. Jinan: Shandong University, 2009

[6] Wang Wei, Wang Xiao-yun. Improved impossible differential Cryptanalysis of CLEFIA [EB/OL]. (2008-05-05). http://eprint.iacr.org/2007/466

[7] Tsunoo Y, Tsujihara E, Shigeri M, et al. Impossible differential Cryptanalysis of CLEFIA [C]// Proc. of FSE'08. Atlanta, USA:[s.n.],2008:398-411

[8] Zhang Wen-ying, Han Jing. Impossible differential analysis of reduced round CLEFIA[C]// Proc. of Inscrypt'08. Beijing, China,2008:181-191

[9] Tang X, Sun B, Li R, et al. Impossible differential cryptanalysis of 13-round CLEFIA-128[J]. Journal of Systems and Software, 2011,84(7):1191-1196

[10] Mala H, Dakhilalian M, Shakiba M. Impossible differential attacks on 13-round CLEFIA-128[J]. Journal of Computer Science and Technology,2011,26(4):744-750

[11] Wu Wen-ling, Zhang Lei, Zhang Wen-tao. Improved impossible differential Cryptanalysis of reduced-round Camellia[C]// Proc. of SAC'08. [S.l.]:ACM Press,2008:442-456

[12] 郑秀林,连至助,鲁艳蓉,等. CLEFIA-128 算法的不可能差分密码分析[J]. 计算机工程,2012,38(3):141-144
Zheng Xiu-lin, Lian Zhi-zhu, Lu Yan-rong, et al. Impossible differential Cryptanalysis of CLEFIA-128 algorithm[J]. Computer Engineering,2012,38(3):141-144

(上接第 187 页)

[2] 朱树永. 协议识别技术研究[D]. 长沙:国防科技大学,2008
Zhu Shu-yong. The study on protocol identification technology [D]. Changsha: National University of Defense Technology, 2008

[3] IANA[OL]. http://www.iana.org/assignments/port-umbers

[4] Liu R T, Huang N F, Chen C H, et al. A fast string-matching algorithm for network processor-based intrusion detection system [J]. ACM Transactions on Embedded Computing Systems, 2004,3(3):614-633

[5] IANA. Internet Assigned Numbers Authority [OL]. http://www.iana.org/assignments/port-numbers

[6] Kim M S, Won Y J, Hong J W K. Application-level traffic monitoring and an analysis on IP networks[J]. ETRI Journal,2005, 27(1):22-42

[7] Chen C C, Wang S D. An efficient multicharacter transition string-matching engine based on the Aho-Corasick Algorithm [J]. ACM Transactions on Architecture and Code Optimization, 2013,10(4):1-22

[8] 刘佳雄. 基于 DPI 和 DFI 技术的对等流量识别系统的设计[D]. 秦皇岛:燕山大学,2010
Liu Jia-xiong. The design for a real-time P2P traffic detection system based on DPI and DFI[D]. Qinhuangdao: Yanshan University,2010

[9] Sen S, Spatscheck O, Wang Dong-mei. Accurate, scalable in network identification of P2P traffic using application signatures [C]// Proc of the 13th International World Wide Web Conference. 2004:512-521

[10] Schiller A C, Binkley J, Harley D. Botnets: the killer Web app [M]. St Louis Mo Syngress Publishing,2006

[11] Wang Y, et al. A semantics aware approach to automated reverse engineering unknown protocols[C]// 20th IEEE International Conference on Network Protocols(ICNP 2012). Austin, TX, USA: IEEE,2012:1-10

[12] Wang Y, Zhang N, Wu Y, et al. Protocol Specification Inference Based on Keywords Identification[M]// Advanced Data Mining and Applications. Springer Berlin Heidelberg,2013:443-454

[13] Kang H J, Kim M S, Hong J W K. A method on multimedia service traffic monitoring and analysis [C]// Proc. of International Workshop on Distributed System, Operations and Management. 2003:93-105

[14] Van Der M J, Caceres R, Chu Y, et al. Mmdump: A tool for monitoring Internet multimedia traffic[J]. ACM SIGCOMM Computer Communication Review,2000,30(5):48-59

[15] 李雄伟,王希武,王盼卿. 基于模式串匹配的 Ethernet 协议识别算法研究[J]. 计算机工程与应用,2007,43(29):143-145
Li Xiong-wei, Wang Xi-wu, Wang Pan-qing. Ethernet protocol identification algorithm based on pattern matching[J]. Computer Engineering and Applications,2007,43(29):143-145

[16] 何畏,汪荣贵,查全民. 一种新的快速移动单模式匹配算法[J]. 合肥工业大学学报(自然科学版),2010,33(5):665-669
He Wei, Wang Rong-gui, Zha Quan-min. A novel fast moving algorithm for single pattern matching[J]. Journal of Hefei University of Technology(Natural Science),2010,33(5):665-669

[17] 朱姣姣,叶猛. 多模式匹配及其改进算法在协议识别中的应用[J]. 电视技术,2012,36(7):60-63
Zhu Jiao-jiao, Ye Meng. Multi-pattern Matching and Application of Improved Algorithm to Protocol Identification [J]. Video Engineering,2012,36(7):60-63

[18] 张之远,叶文晨,陈云寰. 基于多模式匹配的状态检测技术[J]. 电子测量技术,2010,33(11):98-101
Zhang Zhi-yuan, Ye Wen-chen, Chen Yun-huan. Technology of stateful inspection based on the multi-pattern matching [J]. Electronic Measurement Technology,2010,33(11):98-101

[19] 王勇,吴艳梅,李芬,等. 面向比特流数据的未知协议关联分析与识别[J]. 计算机应用研究,2015,32(1):243-248
Wang Yong, Wu Yan-mei, Li Fen, et al. Protocol identification association analysis in mobile network environment[J]. Application Research of Computers,2015,32(1):243-248

[20] 琚玉建,谢绍斌,张薇. 网络协议帧切分优化过程研究与仿真[J]. 计算机仿真,2015,32(1):318-321
Ju Yu-jian, Xie Shao-bin, Zhang Wei. Research and Simulation of Optimization Process for Network Protocol Frame Segmentation [J]. Computer Simulation,2015,32(1):318-321