Zodiac 算法新的不可能差分攻击*

李 超[1,2]，魏悦川[2,3]
（1. 国防科技大学 理学院，湖南 长沙 410073；
2. 国防科技大学 计算机学院，湖南 长沙 410073；
3. 中国科学院 软件研究所，北京 100039）

摘 要：重新评估了 Zodiac 算法抵抗不可能差分攻击的能力。通过分析 Zodiac 算法的线性层，给出了 Zodiac 算法两条新的 14 轮不可能差分。利用新的不可能差分，结合 Early－Abort 技术对完整 16 轮的 Zodiac 算法进行了不可能差分攻击。攻击过程中一共恢复 6 个字节的密钥，其时间复杂度只有 $2^{32.6}$ 次加密，数据复杂度约为 $2^{85.6}$ 个明文，该攻击结果与已有最好的结果相比，时间复杂度降低了一个因子 2^{33}。结果表明由于 Zodiac 算法线性层的扩散性差，使得该算法对不可能差分分析是不免疫的。

关键词：Zodiac；不可能差分攻击；攻击复杂度
中图分类号：TN918 **文献标志码**：A **文章编号**：1001－2486(2012)05－0132－05

New impossible differential cryptanalysis of Zodiac

LI Chao[1,2], *WEI Yuechuan*[2,3]
(1. College of Science, National University of Defense Technology, Changsha 410073, China;
2. College of Computer, National University of Defense Technology, Changsha 410073, China;
3. Institute of Software, Chinese Academy of Sciences, Beijing 100039, China)

Abstract: The security of block cipher Zodiac against impossible differential cryptanalysis was re-evaluated. By analyzing the properties of diffusion layer P, two new 14-round impossible differentials of Zodiac were introduced. Based on the new impossible differential characteristics and combining with the Early-Abort technique, an effective attack was applied to the full 16-round Zodiac, and the data complexity was 285.6 chosen plaintexts and the time complexity is only 232.6 encryptions. Compared with the previous best result, the time complexity in this paper decreases with a factor of 233. The result shows that Zodiac is vulnerable to impossible differential cryptanalysis due to its poor diffusion.

Key words: Zodiac; impossible differential; attack complexity

不可能差分分析是差分密码分析的一个变种，这个概念由 Biham 和 Knudsen 分别独立提出[1－2]。通常的差分分析方法通过寻找高概率差分来恢复密钥，不可能差分则与之相反，寻找的是不可能出现的差分，若某个猜测密钥能使不可能差分出现，则一定是错误密钥，从而淘汰。不可能差分攻击是对分组密码比较有效的攻击之一，它是当前对简化轮数的 Rijndael 算法和 Camellia 算法等最有效的攻击手段[3－6]。

Zodiac 算法[7]是韩国学者为 SoftForm 公司开发的一个分组密码，该密码于 2000 年被提交至 ISO/IEC JTC1/SC27－Korea。Zodiac 采用 128 比特分组，其结构为传统的 Feistel 结构，支持 128/192/256 比特的密钥。与 DES 算法类似，该算法对输入明文和输出密文采用了相应的初始置换和输出变换。Zodiac 算法共迭代 16 次轮变换，每一轮变换均由密钥加变换、线性 P 变换以及非线性 S 盒变换组成。Zodiac 的线性层 P 的扩散性较差，是该算法的一个主要弱点，目前对 Zodiac 最有效的两种分析方法，不可能差分分析[8－10]和 Square 攻击[9,11－12]都是基于这一特点进行的。

算法提出后，密码学界对 Zodiac 抗已知攻击的能力做了评估。Hong 等[8]学者指出，Zodiac 算法存在 14 轮和 15 轮不可能差分，利用 14 轮不可能差分对完整 16 轮的 Zodiac 算法成功实施了不可能差分攻击，然而该攻击的效率不是很高，时间复杂度为 2^{119}。由于找到的不可能差分的形式对攻击效率有很大的影响，虽然 Zodiac 算法的 15 轮不可能差分存在，但是应用该不可能差分却很难实施攻击。2009 年，Shakiba 给出了两条具有更高攻击效率的 13 轮不可能差分[10]，利用其攻击完整 16 轮 Zodiac 的时间复杂度降为 $2^{65.3}$。

* **收稿日期**：2012－03－02
基金项目：国家自然科学基金资助项目(61070215, 61103192)；信息安全国家重点实验室开放基金资助项目(01－02－5)
作者简介：李超(1966—)，男，湖南汨罗人，教授，博士，博士生导师，E-mail：lichao_nudt@sina.com

本文进一步研究了 Zodiac 算法抵抗不可能差分攻击的能力,给出了两条新的 14 轮不可能差分,在此基础上,对完整 16 轮的 Zodiac 算法进行了攻击,进而给出了对 Zodiac 算法新的攻击结果。其攻击效率与原有结果相比,数据复杂度有所升高,而时间复杂度有了较大幅度下降。

1　Zodiac 算法介绍

1.1　符号说明

P, P':128 比特输入明文对;

C, C':128 比特输出密文对;

$X_i^L=(X_{i,0}^L,X_{i,1}^L,\cdots,X_{i,7}^L)$:第 i 轮输出的左半部分;

$X_i^R=(X_{i,0}^R,X_{i,1}^R,\cdots,X_{i,7}^R)$:第 i 轮输出的右半部分;

$K_i=(K_{i,0},K_{i,1},\cdots,K_{i,7})$:第 i 轮轮密钥;

$a,b,\cdots$:差分为非零的字节;

$A,B,\cdots$:差分为任意值的字节;

?:差分为未知或者不必关心的字节。

1.2　算法介绍

Zodiac 算法采用传统的 Feistel 型结构,通过迭代 16 轮轮函数构成。在第一轮之前和最后一轮之后分别有初始变换和输出变换,并且在迭代前后分别异或于一个白化密钥,由于初始变换、输出变换以及白化密钥不影响本文的分析,因此在本文的描述和分析中都不考虑这两个变换和白化密钥的影响。

设 Zodiac 算法的输入为 $P=(X_0^L,X_0^R)\in(F_2^{64})^2$,则 Zodiac 算法第 1 到 16 轮变换定义如下:

$$\begin{cases}X_i^L=F(X_{i-1}^L\oplus K_i)\oplus X_{i-1}^R,\\ X_i^R=X_{i-1}^L,\end{cases}\quad(1\leqslant i\leqslant 16)$$

(X_{16}^L,X_{16}^R)即为明文 P 对应的密文。轮函数定义为 $F(X)=S(\boldsymbol{P}(X))$。其中,线性层 $\boldsymbol{P}$ 可以表示为 F_2 上的矩阵,如下所示。

$$\boldsymbol{P}=\begin{pmatrix}0&0&1&1&1&0&0&0\\1&1&0&0&0&0&0&0\\0&1&1&0&0&0&0&0\\0&0&1&1&0&0&0&0\\1&0&0&0&0&0&1&1\\0&0&0&0&1&1&0&0\\0&0&0&0&0&1&1&0\\0&0&0&0&0&0&1&1\end{pmatrix}$$

图 1 为 Zodiac 轮函数的示意图,其中 S_1 和 S_2 均为非线性变换(S 盒)。由于本文不考虑轮密钥之间的影响,因此我们不介绍密钥扩展算法。

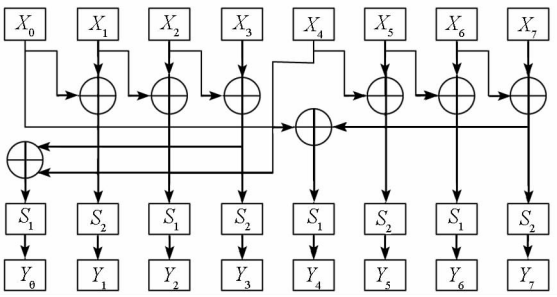

图 1　Zodiac 算法的轮函数

Fig. 1　Round function of Zodiac

1.3　扩散层的对称性质

文献[10]通过研究矩阵 $\boldsymbol{P}$ 的性质指出,在只考虑字节是否为零而不考虑字节具体值(即截断差分)的情形下,Zodiac 算法具有如下对称性质。

性质 1[10]　若$(\Delta X_L^L\|\Delta X_R^L,\Delta X_L^R\|\Delta X_R^R)\rightarrow(\Delta Y_L^L\|\Delta Y_R^L,\Delta Y_L^R\|\Delta Y_R^R)$是 Zodiac 算法的 n 轮截断差分,则$(\Delta X_R^L\|\Delta X_L^L,\Delta X_R^R\|\Delta X_L^R)\rightarrow(\Delta Y_R^L\|\Delta Y_L^L,\ \Delta Y_R^R\|\Delta Y_L^R)$是一条 n 轮截断差分。

由性质 1,可以得到以下推论:

推论 1　若$(\Delta X_L^L\|\Delta X_R^L,\Delta X_L^R\|\Delta X_R^R)\rightarrow(\Delta Y_L^L\|\Delta Y_R^L,\Delta Y_L^R\|\Delta Y_R^R)$是 Zodiac 算法的 n 轮不可能差分,且这一不可能差分由中间矛盾的两条截断差分连接而成,则$(\Delta X_R^L\|\Delta X_L^L,\ \Delta X_R^R\|\Delta X_L^R)\rightarrow(\Delta Y_R^L\|\Delta Y_L^L,\Delta Y_R^R\|\Delta Y_L^R)$也是一条 n 轮不可能差分。

2　新的 14 轮不可能差分区分器

本节考虑 Zodiac 算法的不可能差分。

定理 1　以下两条差分

$(00000AAA,BBBB0CDE)\rightarrow$

$(00000FFF,00000000)$,

$(0AAA0000,0CDEBBBB)\rightarrow$

$(0FFF0000,00000000)$

是 Zodiac 算法的两条 14 轮不可能差分,其中 $E\neq B\oplus D$。

证明　设算法的输入差分为(00000*AAA*, *BBBB*0*CDE*),其中 $E\neq B\oplus D$,根据算法流程可知,第 2 轮中 P 变换的输出为$(0000B\oplus D\oplus E???)$,其中 $B\oplus D\oplus E\neq 0$,因而该轮 F 函数的输出具有(0000a ???)的形式,继续迭代得到 $\Delta X_6=(???\ f????,\ ??\ d\oplus BB????)$。再考虑解密方向,第 14 轮差分为(00000*FFF*,00000000),则解密 8 轮,得到 $\Delta X_6=(???\ 0????,????????)$。由加密方向看 $\Delta X_{6,3}\neq 0$,而由解密方向看 $\Delta X_{6,3}=0$,相互矛盾,因此是 Zodiac 算法的不可能差分。图 2 给出了算法流程中每一轮的差分。

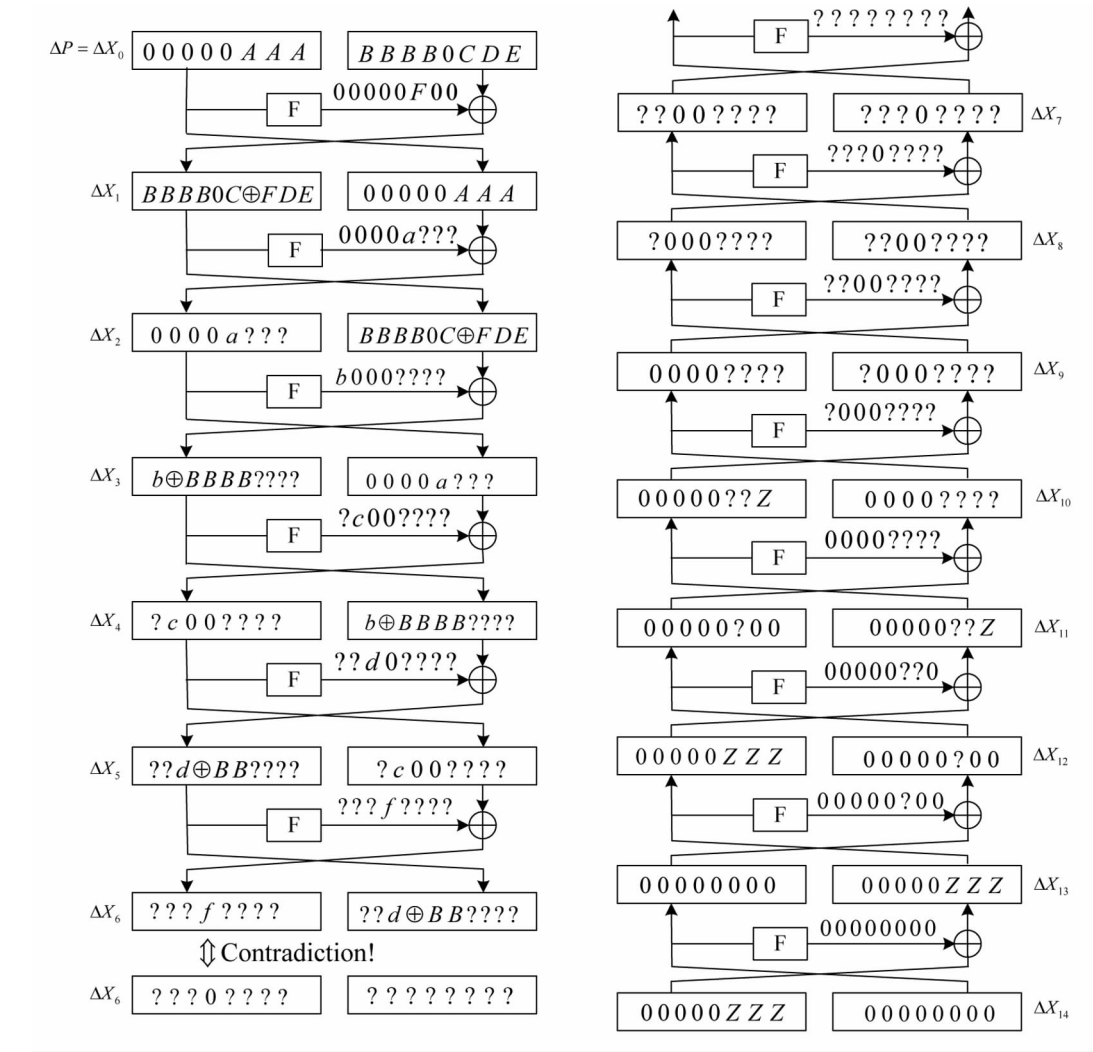

图 2 Zodiac 算法的 14 轮不可能差分

Fig. 2 14-round impossible differential of Zodiac

由推论 1,可以直接得到

$(0AAA0000, 0CDEBBBB) \rightarrow (0FFF0000, 00000000)$

也是一条不可能差分。

3 对完整 16 轮 Zodiac 算法的不可能差分攻击

3.1 攻击过程描述

基于上述 14 轮不可能差分区分器,在末尾加上两轮,可以得到对完整 16 轮 Zodiac 算法的不可能差分攻击,见图 3。在攻击中,假设轮密钥是随机的。令 Λ_1 为 $K_{16,6}$ 和 $K_{16,7}$ 所有的可能值构成的密钥空间,Λ_2 为 $K_{15,6}$ 所有的可能值构成的密钥空间。

首先,基于 ID - I,给出如下攻击过程。攻击过程如图 3 左部分所示。

Step 1 选择明文结构,使得

$$X_0^L = (c_0 c_1 c_2 c_3 c_4 x_0 x_0 x_0),$$

$$X_0^R = (x_1 x_1 x_1 x_1 c_5 x_2 x_3 x_4)$$

其中 $c_i (0 \leqslant i \leqslant 5)$ 为 F_2^8 上的常量,$x_i (0 \leqslant i \leqslant 4)$ 遍历 F_2^8,因而从该结构中选择出的明文其差分具有 $\Delta P = (00000AAA, BBBB0CDE)$ 的形式。每个结构中包含的明文量为 $2^{8\times 5} = 2^{40}$,可以形成 $2^{40} \times (2^{40} - 1)/2 \approx 2^{79}$ 个明文对。另外,为满足 $E \neq B \oplus D$,需要过滤掉使 $x_1 \oplus x_1' = x_3 \oplus x_3' \oplus x_4 \oplus x_4'$ 成立的明文对,这种明文对的数量约为 $(2^8 \times (2^8 - 1))^2 \times 2^8 \approx 2^{40}$,因此有用的明文对数量约为 $2^{79} - 2^{40} \approx 2^{79}$。

Step 2 将密文差分不满足(00000? 00, 00000?? Z)形式的明密文对过滤掉,只保存剩余的对。

Step 3 对于每个 $\lambda_1 \in \Lambda_1$,对 Step 2 中剩余的密文进行一轮解密,获得 $X_{15,5}^R$ 和 $X_{15,5}^R$,以及 $X_{15,6}^R$ 和 $X_{15,6}^R$;

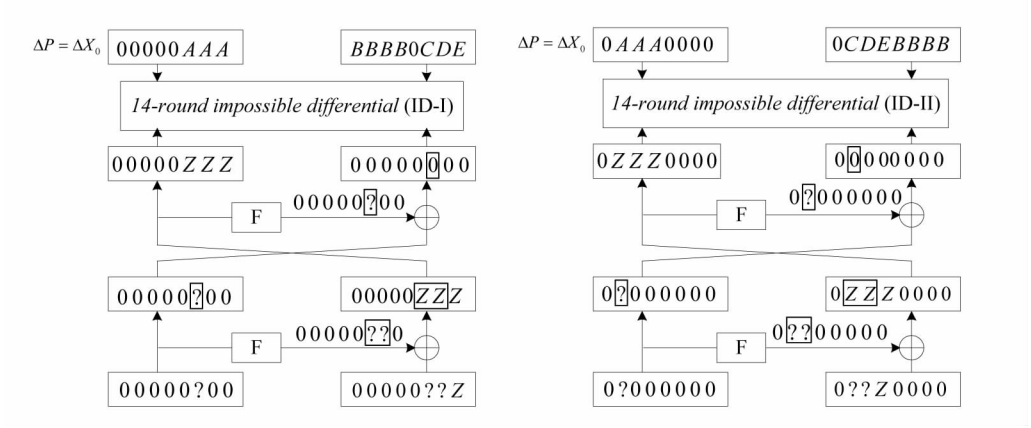

图 3　对 16 轮 Zodiac 算法的不可能差分攻击

Fig. 3　Impossible differential cryptanalysis of 16 – round Zodiac

如果 $\Delta X^R_{15,5}=Z$ 且 $\Delta X^R_{15,6}=Z$,对于每个 $\lambda_2\in\Lambda_2$,对第 15 轮的输出进行一轮解密,获得 $X^R_{14,5}$ 和 $X^R_{14,5}$,如果 $\Delta X^R_{14,5}=0$,则从密钥空间(Λ_1, Λ_2)中去除(λ_1, λ_2}。

Step 4　判断密钥空间中剩余元素的个数 $|(\Lambda_1,\ \Lambda_2)|\leqslant 1$ 是否成立,若成立,结束该过程,否则从 Step 2 中选择下一个明密文对进行 Step 3 操作。剩余的密钥作为正确的 $K_{16,5}$,$K_{16,6}$,$K_{15,5}$。

利用 ID – II,可以进行相似的攻击过程,恢复出 $K_{16,1}$,$K_{16,2}$和 $K_{15,1}$,见图 3 的右半部分。为降低复杂度,利用 early abort 技术,将 Step 3 中的操作作如下改进。

Step 3*　对于每个 $\lambda_{1,5}\in\Lambda_1$,对 Step 2 中剩余的密文进行一轮解密,获得 $X^R_{15,5}$ 和 $X^R_{15,5}$,如果 $\Delta X^R_{15,5}=Z$,则对于每个 $\lambda_{1,6}\in\Lambda_1$,对密文进行一轮解密,获得 $X^R_{15,6}$ 和 $X^R_{15,6}$,若 $\Delta X^R_{15,6}=Z$,对每个 $\lambda_{2,5}\in\Lambda_2$,对上述 15 轮输出进行一轮解密,获得 $X^R_{14,5}$和 $X^R_{14,5}$,如果 $\Delta X^R_{14,5}=0$,则从密钥空间(Λ_1, Λ_2)中去除(λ_1, λ_2)。

3.2　复杂度分析

在上述攻击过程中,利用一条不可能差分可以恢复 3 个字节的密钥,密钥空间为 2^{24},密钥通过检测的平均概率为 $1-2^{-24}$,Step 2 中过滤密文之后剩余的对数 N 需满足 $2^{24}\times(1-2^{-24})^N\approx 1$,故 $N=2^{28.6}$。过滤密文时满足差分为(00000?00, 00000?? Z)的概率为 2^{-96},因此选择的明密文对数量为 $N\times 2^{96}=2^{124.6}$,又因为一个结构中约有 2^{79}个明文对,所以需要选择 $2^{124.6}/2^{79}=2^{45.6}$个结构,综上,该攻击的选择明文量为 $2^{45.6}\times 2^{40}=2^{85.6}$。

时间复杂度可以通过下式计算:

$(2/16)\times(2^{28.6}\times(2^8+2^{16}\times(1/2^8))+2^{24}\times(1/2^8)^2\times\sum_{i=0}^{2^{29}-1}(1-(1/2^8)^3)^i)\approx 2^{34.6}$,即攻击需要 $2^{34.6}$次 S 盒计算,一次 S 盒计算相当于 1/8 轮加密,考虑到基于 ID – II 的攻击复杂度与基于 ID – I 的攻击复杂度相同,因此,为恢复出 6 个字节密钥 $K_{16,1}$,$K_{16,2}$, $K_{16,5}$,$K_{16,6}$,$K_{15,1}$,$K_{15,5}$,本文攻击的时间复杂度约为($2\times 2^{34.6}$)/8 $=2^{32.6}$次一轮加密。

4　结论

本文对 Zodiac 算法的安全性进行了进一步的评估。发现了该算法两条新的 14 轮不可能差分,基于这两条不可能差分和 Early – Abort 攻击技术,给出了对完整 16 轮 Zodiac 算法的不可能差分攻击,对现有结果进行了改进,使时间复杂度大大下降。然而本文的数据复杂度仍然较高,在现有存储条件下,现实破译仍然存在困难。表 1 总结了对 Zodiac 攻击的现有结果。由于不可能差分的形式对攻击效率有很大影响,因此,如何寻找更加有效的不可能差分,降低数据复杂度以实现 Zodiac 的现实破译,还有待进一步研究。

表 1　对 Zodiac 算法的现有攻击结果

Tab. 1　The cryptanalytic results of Zodiac

攻击轮数	恢复密钥字节数	数据复杂度	时间复杂度	攻击类型	文献出处
16	9	$2^{103.6}$	2^{119}	Imp. Diff	[8]
16	32	$2^{16.5}$	$2^{221.7}$	Square	[11]
16	23	$2^{12.6}$	$2^{189.5}$	Square	[12]
16	23	2^{16}	2^{190}	Integral	[9]
16	14	$2^{71.3}$	$2^{65.3}$	Imp. Diff	[10]
16	6	$2^{85.6}$	$2^{32.6}$	Imp. Diff	本文

参考文献(References)

[1] Biham E, Biryukov A, Shamir A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials[C]//Stern

J eds. Eurocrypt 1999, LNCS, Springer, Heidelberg, 1999, 1592: 12 – 23.

[2] Knudsen L. DEAL—a 128 – bit block cipher[R]. Technical Report 151, Department of Informatics, University of Bergen, Bergen, Norway, 1998.

[3] Wu W, Zhang L, Zhang W. Improved impossible differential cryptanalysis of reduced – round camellia [C]//Avanzi R, Keliher L, Sica F eds. SAC 2008, LNCS, Springer, Heidelberg, 2009, 5381: 442 – 456.

[4] Zhang W, Wu W, Feng D. New results on impossible differential cryptanalysis of reduced AES[C]//ICISC 2007, LNCS, Springer, Heidelberg, 2007, 4817: 239 – 250.

[5] MalaH, Shakiba M, Dakhilalian M, et al. New results on impossible differential cryptanalysis of reduced – round camellia [C]//SAC 2009, LNCS, Springer, Heidelberg, 2009, 5867: 281 – 294.

[6] Wang W, Wang X. Impossible differential cryptanalysis of CLEFIA – 128/192/256 [J]. Journal of Software, 2009, 20(9): 2587 – 2596.

[7] Lee C, Jun K, Jung M, et al. Zodiac version 1.0 (revised) architecture and specification[R]. Standardization Workshop on Information Security Technology. Korean Contribution on MP18033, ISO/IEC JTC1/SC27 N2563. http://www. Kiss. or. kr/seed/index. html.

[8] Hong D, Sung J, Moriai S, et al. Impossible differential cryptanalysis of Zodiac[C]//FSE 2001, LNCS,. Springer, Heidelberg, 2002, 2355: 300 – 311.

[9] 孙兵,张鹏,李超. Zodiac 算法的不可能差分和积分攻击[J]. 软件学报,2011, 22(8): 1911 – 1917.
SUN Bing, ZHANG Peng, LI Chao. Impossible differential and integral cyptanalysis of Zodiac [J]. Journal of Software. 2011, 22(8): 1911 – 1917. (in Chinese)

[10] Shakiba M, Dakhilalian M, Mala H. An improved impossible differential cryptanalysis of Zodiac[J]. Journal of Systems and Software. 2010, 83: 702 – 709.

[11] Ji W, Hu L. Square attack on reduced-round Zodiac cipher [C]//ISPEC 2008, LNCS, Springer, Heidelberg, 2008, 4991: 377 – 391.

[12] 张鹏,李瑞林,李超. Zodiac 算法新的 Square 攻击[J]. 电子与信息学报,2010, 32(11): 2790 – 2794.
ZHANG Peng, LI Ruilin, LI Chao. New square attack on Zodiac[J]. Journal of Electronics & Information Technology, 2010, 32(11): 2790 – 2794. (in Chinese)

(上接第 67 页)

[4] Carevic D. Automatic estimation of multiple target positions and velocities using passive TDOA measurements of transients [J]. IEEE Transactions on Signal Processing,2007, 55(2): 424 – 436.

[5] Obozreniye V. The U.S. navyś "white cloud" space borne ELINT system[J]. Foreign Military Review,1993(7): 57 – 60.

[6] Foy W H. Position-location solutions by Taylor-series estimation[J]. IEEE Transactions on Aerospace and Electronic Systems, 1976, 12(2): 187 – 194.

[7] Torrieri J D. Statistical theory of passive location systems[J]. IEEE Transactions on Aerospace and Electronic Systems,1984, 20(2): 183 – 198.

[8] Mellen G, Pachter M, Raquet J. Closed-form solution for determining emitter location using time difference of arrival measurements [J]. IEEE Transactions on Aerospace and Electronic Systems,2003, 39(3): 1056 – 1058.

[9] Ho K C, Chan Y T. Solution and performance analysis of geolocation by TDOA [J]. IEEE Transactions on Aerospace and Electronic Systems,1993, 26(5): 748 – 753.

[10] 谢恺, 钟丹星, 邓新蒲, 等. 一种空间时差定位的新算法[J]. 信号处理,2006, 22(2): 129 – 135.
XIE Kai, ZHONG Danxing, DENG Xinpu, et al. A new algorithm for the time difference location in aerospace[J]. Signal Processing, 2006, 22(2): 129 – 135. (in Chinese)

[11] 刘海军, 叶浩欢, 柳征, 等. 基于星载干涉仪测向的辐射源定位综合算法[J]. 国防科技大学学报,2009, 31(6): 110 – 114.
LIU Haijun, YE Haohuan, LIU Zheng, et al. Integration algorithm of emitter location based on satellite-borne interferometer[J]. Journal of National University of Defense Technology, 2009, 31(6): 110 – 114. (in Chinese)

[12] 刘林, 范平志, 邓平. 基于 GDOP 加权的 GSM 移动台位置估计数据融合[J]. 电波科学学报,2007, 22(3): 486 – 490.
LIU Lin, FAN Pingzhi, DENG Ping. Data fusion based on GDOP weighting for GSM mobile position estimation [J]. Chinese Journal of Radio Science, 2007, 22(3): 486 – 490. (in Chinese)

[13] 钟丹星, 邓新蒲, 周一宇. 基于 WGS – 84 椭球模型的卫星测时差定位精度分析[J]. 电子对抗技术,2002, 17(5): 18 – 21.
ZHONG Danxing, DENG Xinpu, ZHOU Yiyu. Precision analysis of satellites DTOA location based on WGS-84 ellipsoid model [J]. Chinese Journal of Electronic Countermeasure Technology, 2002, 17(5): 18 – 21. (in Chinese)

[14] Kay S M. Fundamentals of statistical signal processing: estimation theory[M]. New Jersey: Prentice Hall PTR, 1993.

[15] Zhang D Q, Chang S F. Detecting image near-duplicate by stochastic attributed relational graph matching with learning [C] //Proceedings of ACM Multimedia, 2004: 877 – 884.