7 轮 AES-128 的非对称不可能飞来器攻击

董晓丽[1)] 胡予濮[1)] 陈 杰[1),3)] 韦永壮[1),2)]

[1)](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)

[2)](桂林电子科技大学信息与通信学院 广西 桂林 541004)

[3)](中国科学院软件研究所信息安全国家重点实验室 北京 100049)

摘 要 分组密码是信息安全中实现数据加密、认证和密钥管理的核心密码算法,其安全性分析是密码学的重要课题之一.基于差分分析原理,文中提出了分组密码新的分析方法:非对称不可能飞来器攻击.该方法是通过构造非对称不可能飞来器区分器,排除满足这种关系的密钥,并最终恢复出秘密密钥的一种攻击方法.利用密钥编排方案,基于差分表查询技术和数据多次利用技术,把新方法应用于 AES-128.研究结果表明:攻击 7 轮 AES-128 所需的数据复杂度为 $2^{105.18}$ 个选择明文,时间复杂度为 $2^{115.2}$ 次加密,存储复杂度为 $2^{106.78}$ 个 AES 分组.就攻击轮数、数据复杂度和时间复杂度而言,新分析优于已有针对 AES-128 的攻击.

关键词 密码分析;分组密码;AES;飞来器;时间复杂度

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2011.01300

An Asymmetric Impossible Boomerang Attack on 7-Round AES-128

DONG Xiao-Li[1)] HU Yu-Pu[1)] CHEN Jie[1),3)] WEI Yong-Zhuang[1),2)]

[1)](*Key Laboratory of Computer Networks & Information Security of Ministry of Education, Xidian University, Xi'an* 710071)

[2)](*School of Information and Communication, Guilin University of Electronic Technology, Guilin, Guangxi* 541004)

[3)](*State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100049)

Abstract Block cipher is the core of cryptography that provides data encryption, authentication and key management in information security. The security of block cipher is an important issue in the cryptanalysis. Based on the principle of differential cryptanalysis, this paper introduces a new cryptanalytic technique on block cipher: asymmetric impossible boomerang attack. The technique used asymmetric impossible boomerang distinguisher to eliminate wrong key material and leave the right key candidate. With key schedule considerations, techniques of looking up differential tables and re-using the data, the authors apply asymmetric impossible boomerang attack to AES-128. It is shown that attack on 7-round AES-128 requires data complexity of about $2^{105.18}$ chosen plaintexts, time complexity of about $2^{115.2}$ encryptions and memory complexity of about $2^{106.78}$ AES blocks. The presented result is better than any previous published cryptanalytic results on AES-128 in terms of the numbers of attacked rounds, the data complexity and the time complexity.

Keywords cryptanalysis; block cipher; AES; boomerang; time complexity

---

收稿日期:2010-10-20;最终修改稿收到日期:2011-05-16.本课题得到国家自然科学基金(60970119,60833008)、国家"九七三"重点基础研究发展规划项目基金(2007CB311201)、中央高校基本科研业务费专项资金(K50510010018)资助.**董晓丽**,女,1982 年生,博士研究生,主要研究方向为分组密码的设计与分析.E-mail: dxl_xaut@163.com. **胡予濮**,男,1955 年生,博士,教授,博士生导师,主要研究领域为密码学与信息安全. **陈 杰**,女,1979 年生,博士,副教授,主要研究方向为分组密码的设计与分析. **韦永壮**,男,1976 年生,博士,主要研究方向为密码函数与分组密码的分析.

1 引　言

现代密码学是解决信息安全问题的有效手段. 分组密码是现代密码学的一个重要研究方向，属于对称密码体制. 它可以直接用来加密消息，对消息提供保密性；可以用来构造消息认证码(MAC)和 Hash 函数来保障数据的真实性和完整性. 分组密码还具有简洁、快速、易于标准化等特点，因此在信息安全领域有着最广泛的应用.

自 2000 年，NIST 宣布 Rijndael[1] 是高级加密标准(AES)征集比赛中的获胜者，它已经成为全球最受关注和广泛使用的分组密码算法之一. 同时，涌现出了一些新的针对 AES 的攻击，包括平方攻击[2-3]、碰撞攻击[4]、不可能差分攻击[5-9]、飞来器攻击[10]、中间相遇攻击[11]、相关密钥攻击[12-13]等.

单密钥模型下，AES-128 的攻击结果如下：1997 年，AES 的设计者 Daemen 等人[2]首次提出了 6 轮 AES-128 的平方攻击，需要 2^{32} 个选择明文和 2^{72} 次加密. 2000 年，Ferguson 等人[3]把攻击 6 轮 AES-128 的时间复杂度降为 2^{44}. 同时，7 轮 AES-128 的平方攻击需要 $2^{127.977}$ 个选择明文和 2^{120} 次加密. 同年，Gilbert 等人[4]提出 7 轮 AES-128 的碰撞攻击，需要 2^{32} 个选择明文和 2^{128} 次加密. 2000 年，Biham 等人[5]首次将不可能差分攻击应用于 AES，攻击 5 轮 AES-128 需要 $2^{29.5}$ 个选择明文和 2^{31} 次加密. 2002 年，Cheon 等人[6]提出 6 轮 AES-128 的不可能差分攻击，需要 $2^{91.5}$ 个选择明文和 2^{122} 次加密. 2004 年，Biryukov 等人[10]提出 5 轮 AES-128 和 6 轮 AES-128 的飞来器攻击. 5 轮 AES-128 攻击中需要 2^{39} 个选择明文和 2^{39} 次加密，6 轮 AES-128 攻击中需要 2^{71} 个选择明文和 2^{71} 次加密. 2007 年，Zhang 等人[7]和 Lu[8]分别提出改进的 7 轮 AES-128 的不可能差分攻击，其中文献[8]中复杂度较低，需要 $2^{112.2}$ 个选择明文和 $2^{115.6}$ 次加密. 文献[9]中，Lu 同时提出 6 轮 AES-128 的不可能飞来器攻击，需要 $2^{112.2}$ 个选择明文和 $2^{112.3}$ 次加密. 2008 年，Lu 等人[9]提出 7 轮 AES-128 的不可能差分攻击，需要 $2^{112.2}$ 个选择明文和 $2^{117.2}$ 次存储访问. 2010 年，Dunkelman 等人[11]提出 7 轮 AES-128 的中间相遇攻击，依据时空折中需要约 2^{116} 个选择明文和约 2^{116} 次加密.

本文的主要贡献：基于差分分析原理，提出了分组密码新的分析方法——非对称不可能飞来器攻击. 首先描述了非对称不可能飞来器攻击，并给出了详细的理论支持. 该攻击是通过构造非对称不可能飞来器区分器，排除满足这种关系的密钥，并最终恢复出秘密密钥的一种攻击方法. 然后，构造了 4 轮 AES 非对称不可能飞来器区分器，利用密钥编排方案，差分表查询技术和数据多次利用技术，针对 7 轮 AES-128 进行新分析. 所需的数据复杂度为 $2^{105.18}$ 个选择明文，时间复杂度为 $2^{115.2}$ 次加密，存储复杂度为 $2^{106.78}$ 个 AES 分组. 就攻击轮数、数据复杂度和时间复杂度而言，新分析优于已有针对 AES-128 的攻击.

本文第 2 节为基础知识，介绍 AES 算法和不可能飞来器区分器；第 3 节详细描述新的密码分析方法：非对称不可能飞来器攻击；第 4 节把非对称不可能飞来器攻击应用于 7 轮 AES-128；第 5 节给出本文的分析结果及与已有结果的比较，并提出下一步工作的方向.

2 基础知识

2.1 AES 介绍

AES[1]分组长度是 128bit，密钥长度有 128bit、192bit 和 256bit 3 种，分别用 AES-128、AES-192 和 AES-256 表示，且分别迭代 10 轮、12 轮和 14 轮. AES-128 分组表示为字节 A_i 为元素的 4×4 矩阵 $((A_0,A_1,A_2,A_3)^{\mathrm{T}},(A_4,A_5,A_6,A_7)^{\mathrm{T}},(A_8,A_9,A_{10},A_{11})^{\mathrm{T}},(A_{12},A_{13},A_{14},A_{15})^{\mathrm{T}})$.

AES 的每一轮由以下 4 种变换组成：字节代替(SB)：每个字节进行 S 盒变换；行移位(SR)：每行循环左移位(第 i 行循环左移 i 个字节，$i=0,1,2,3$)；列混淆(MC)：在 $GF(2^8)$ 上每列左乘矩阵；密钥加(ARK)：中间状态异或 128bit 子密钥. AES 第 0 轮之前有密钥加法运算(这个密钥又称为白化密钥)；最后一轮没有列混淆变换. AES 密钥编排算法把秘密密钥扩充成 $128(R+1)$bit 子密钥，其中 R 表示轮数.

AES-128 密钥方案由 128bit 密钥 $K=(W_0,W_1,W_2,W_3)$ 生成 $W_4,W_5,\cdots,W_{43}$，其中 W_i 为 32bit 字. 密钥生成如下：

1. 用户密钥 $K=(W_0,W_1,W_2,W_3)$.

2. For $i=4$ to $i=43$

   If $i\equiv0\bmod4$, then

   $$W_i\equiv W_{i-4}\oplus SB(RotByte(W_{i-1}))\oplus Rcon(i/4),$$

   else $W_i\equiv W_{i-4}\oplus W_{i-1}$.

3. $K_{-1}=(W_0,W_1,W_2,W_3)$，$K_r=(W_{4(r+1)},W_{4(r+1)+1},W_{4(r+1)+2},W_{4(r+1)+3})$，$0\le r\le9$.

其中 K_r 表示 r 轮子密钥，K_{-1} 表示白化密钥.

$RotByte(\cdot)$表示一字节的循环；$Rcon(\cdot)$表示轮常量.

本文使用的记号：P 表示明文，C 表示密文. X_r^I 表示第 r 轮的输入，X_r^{SB}、X_r^{SR}、X_r^{MC}、X_r^O 分别表示第 r 轮 SB、SR、MC、ARK 的中间值，显然 $X_{r-1}^O=X_r^I$. 同一轮 MC 和 ARK 交换，子密钥要用等价子密钥 $\widetilde{K}_i$，且满足 $\widetilde{K}_i=MC^{-1}(K_i)$. $X_{r,i}$ 表示 X_r 的第 i 字节 $(i=0,1,2,\cdots,15)$. $X_{r,Col(l)}$ $(l=0,1,2,3)$表示 X_r 的第 l 列. $X_{r,SR(Col(l))}$ $(l=0,1,2,3)$表示 X_r 中相应于第 l 列 SR 变换后位置的 4 个字节；同理 $X_{r,SR^{-1}(Col(l))}$ $(l=0,1,2,3)$表示 X_r 中相应于第 l 列 SR^{-1} 变换后位置的 4 个字节. $Pr(\cdot)$表示相应事件的概率. $Y\sim Poi(\lambda)$表示随机变量 Y 服从参数为 λ 的泊松分布.

2.2 不可能飞来器区分器

分组密码 $E:\{0,1\}^k\times\{0,1\}^n\rightarrow\{0,1\}^n$ 表示为两个算法级联的形式 $E^1\circ E^0$，即算法 E 在密钥 K 下加密明文 P 也可以表示为 $E_K(P)=E_K^1\circ E_K^0(P)$. 选择 N 元组 $(X_0,X_1,\cdots,X_{N-1})$，其中 $X_{2i+1}=X_{2i}\oplus\alpha_i(0\leq i\leq N/2-1)$，$E(X_{(2j+2)\bmod N})=E(X_{2j+1})\oplus\gamma_j(0\leq j\leq N/2-1)$. 不可能飞来器区分器包括：(1)算法 E^0 中 $Pr(\alpha_i\rightarrow\beta_i)=1(0\leq i\leq N/2-1)$；(2)算法 $(E^1)^{-1}$ 中 $Pr(\delta_j\rightarrow\gamma_j)=1(0\leq j\leq N/2-1)$；(3)$(\bigoplus_{i=0}^{N/2-1}\beta_i)\oplus(\bigoplus_{j=0}^{N/2-1}\gamma_j)\neq 0$，其中 $\alpha_i,\beta_i,\delta_j,\gamma_j$ $(0\leq i\leq N/2-1,0\leq j\leq N/2-1)$是 n-bit 块.

由于不可能飞来器区分器的结构对称，且 N 为偶数$(N\geq 2)$. 因此本文称之为对称不可能飞来器区分器，相应的攻击为对称不可能飞来器攻击. $N=4$ 情况如图 1 所示.

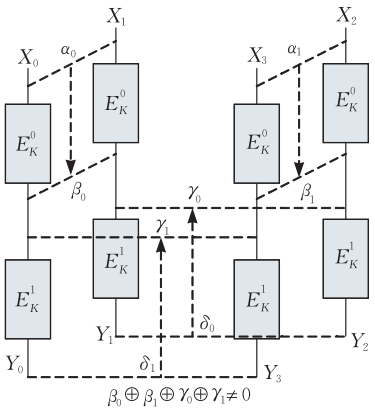

图 1 不可能飞来器区分器

3 非对称不可能飞来器攻击

基于差分分析技术和不可能飞来器攻击，本节提出新的密码分析方法——非对称不可能飞来器攻击.

3.1 非对称不可能飞来器区分器

定义 1(非对称不可能飞来器区分器). 分组密码算法 $E=E^1\circ E^0$，非对称不可能飞来器区分器包括：

(1)算法 E^0 中，$Pr(\alpha_i\rightarrow\beta_i)=1(0\leq i\leq N-2)$；

(2)算法$(E^1)^{-1}$中，$Pr(\delta\rightarrow\gamma)=1$；

(3)$\beta_0\oplus\beta_1\oplus\cdots\oplus\beta_{N-2}\oplus\gamma\neq 0$，

其中 $\alpha_0,\beta_0,\alpha_1,\beta_1,\cdots,\alpha_{N-2},\beta_{N-2},\delta,\gamma$ 是 n-bit 块.

可以看出，非对称不可能飞来器区分器结构非对称，且满足 $N\geq 2$. $N=4$ 情况如图 2 所示.

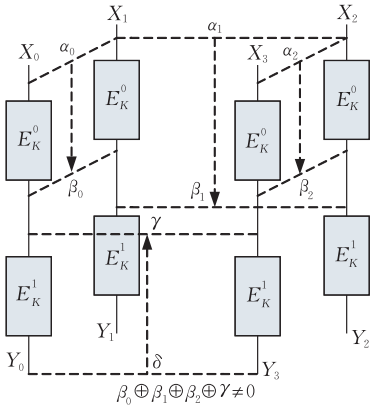

图 2 非对称不可能飞来器区分器

下面的定理对非对称不可能飞来器区分器提供了理论基础.

定理 1. 分组密码算法 $E=E^1\circ E^0$，密钥为 K，$X_i(0\leq i\leq N-2)$是 n-bit 块，$X_i\oplus X_{i+1}=\alpha_i(0\leq i\leq N-2)$，$E_K^0(X_0)\oplus E_K^0(X_{N-1})=\gamma$. 假定算法 E^0 满足 $P(\alpha_i\rightarrow\beta_i)=1(0\leq i\leq N-2)$，算法$(E^1)^{-1}$满足 $Pr(\delta\rightarrow\gamma)=1$，且 $\beta_0\oplus\beta_1\oplus\cdots\oplus\beta_{N-2}\oplus\gamma\neq 0$. 下列等式不能成立：

$$E_K(X_0)\oplus E_K(X_{N-1})=\delta \tag{1}$$

证明. 假定 $\exists X_1,X_n,K$ 使等式(1)成立. 算法 E^0 满足 $Pr(\alpha_i\rightarrow\beta_i)=1(0\leq i\leq N-2)$，其中 $X_i\oplus X_{i+1}=\alpha_i$，$E_K^0(X_i)\oplus E_K^0(X_{i+1})=\beta_i(0\leq i\leq N-2)$，下列等式成立的概率为 1：

$$\begin{aligned}
&E_K^0(X_0)\oplus E_K^0(X_{N-1})\\
&=(E_K^0(X_0)\oplus E_K^0(X_1))\oplus\cdots\oplus\\
&(E_K^0(X_i)\oplus E_K^0(X_{i+1}))\oplus\cdots\oplus(E_K^0(X_{N-2})\oplus E_K^0(X_{N-1}))\\
&=((E_K^1)^{-1}(E_K(X_0))\oplus(E_K^1)^{-1}(E_K(X_1)))\oplus\cdots\oplus\\
&\quad((E_K^1)^{-1}(E_K(X_i))\oplus(E_K^1)^{-1}(E_K(X_{i+1})))\oplus\cdots\oplus\\
&\quad((E_K^1)^{-1}(E_K(X_{N-2}))\oplus(E_K^1)^{-1}(E_K(X_{N-1})))\\
&=\beta_0\oplus\beta_1\oplus\cdots\oplus\beta_i\oplus\cdots\oplus\beta_{N-2}.
\end{aligned}$$

由于算法 $(E_K^1)^{-1}$ 满足 $Pr(\delta\rightarrow\gamma)=1$，即当

$E_K(X_0)\oplus E_K(X_{N-1})=\delta$，下列等式成立的概率为 1：

$$E_K^0(X_0)\oplus E_K^0(X_{N-1})=$$
$$(E_K^1)^{-1}(E_K(X_0))\oplus(E_K^1)^{-1}(E_K(X_{N-1}))=\gamma.$$

因此，与条件 $\beta_0\oplus\beta_1\oplus\cdots\oplus\beta_{N-2}\oplus\gamma\neq 0$ 相矛盾，定理成立. 证毕.

3.2 密钥恢复

分组密码算法 E 表示为 4 个算法级联形式 $E=E^{\text{aft}}\circ E^1\circ E^0\circ E^{\text{bef}}$，其中 $E^1\circ E^0$ 表示非对称不可能飞来器区分器 $\beta_0\oplus\beta_1\oplus\cdots\oplus\beta_{N-2}\oplus\gamma\neq 0$，$E^{\text{bef}}$ 表示 E^0 之前加密轮，E^{aft} 表示 E^1 之后加密轮. 假定 K_{bef}、K_{aft} 分别是算法 E^{bef}、E^{aft} 的子密钥猜测，则攻击者检验 N 元明/密文组 $((P_0,C_0),(P_1,C_1),\cdots,(P_{N-1},C_{N-1}))$ 是否满足非对称不可能飞来器区分器的 N 个条件：

$$E_{K_{\text{bef}}}^{\text{bef}}(P_i)\oplus E_{K_{\text{bef}}}^{\text{bef}}(P_{i+1})=$$
$$\alpha_i,(E_{K_{\text{aft}}}^{\text{aft}})^{-1}(C_0)\oplus(E_{K_{\text{aft}}}^{\text{aft}})^{-1}(C_{N-1})=\delta,$$
$$0\leq i\leq N-2.$$

假如存在 N 元明/密文组满足上面的等式，则子密钥猜测 $(K_{\text{bef}},K_{\text{aft}})$ 是不正确的. 因此有足够多的明/密文组，通过丢弃所有错误的子密钥猜测，攻击者能够寻找到算法 E^{bef}，E^{aft} 中正确的子密钥.

4 7 轮 AES-128 的非对称不可能飞来器攻击

4.1 AES-128 部分密钥编排结果

$$K_{6,0}=K_{5,0}\oplus S(K_{5,13})\oplus Rcon(7),$$
$$K_{6,3}=K_{5,3}\oplus S(K_{5,12})\oplus Rcon(7),$$
$$K_{6,13}=K_{5,13}\oplus K_{6,9}.$$

4.2 4 轮 AES 非对称不可能飞来器区分器

下面定理构造了 4 轮 AES 的非对称不可能飞来器区分器. 图 3 形象描述了此区分器的差分.

$$Round0:\xrightarrow{ARK}\begin{pmatrix}a_i&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\xrightarrow{SB}\begin{pmatrix}b_i&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\xrightarrow{SR}\begin{pmatrix}b_i&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\xrightarrow{MC}\begin{pmatrix}02\cdot b_i&0&0&0\\01\cdot b_i&0&0&0\\01\cdot b_i&0&0&0\\03\cdot b_i&0&0&0\end{pmatrix}\xrightarrow{ARK}\begin{pmatrix}02\cdot b_i&0&0&0\\01\cdot b_i&0&0&0\\01\cdot b_i&0&0&0\\03\cdot b_i&0&0&0\end{pmatrix}$$

$$Round1:\xrightarrow{SB}\begin{pmatrix}c_i&0&0&0\\d_i&0&0&0\\e_i&0&0&0\\f_i&0&0&0\end{pmatrix}\xrightarrow{SR}\begin{pmatrix}c_i&0&0&0\\0&0&0&d_i\\0&0&e_i&0\\0&f_i&0&0\end{pmatrix}\xrightarrow{MC}\begin{pmatrix}02\cdot c_i&01\cdot f_i&01\cdot e_i&03\cdot d_i\\01\cdot c_i&01\cdot f_i&03\cdot e_i&02\cdot d_i\\01\cdot c_i&03\cdot f_i&02\cdot e_i&01\cdot d_i\\03\cdot c_i&02\cdot f_i&01\cdot e_i&01\cdot d_i\end{pmatrix}\xrightarrow{ARK}\begin{pmatrix}02\cdot c_i&01\cdot f_i&01\cdot e_i&03\cdot d_i\\01\cdot c_i&01\cdot f_i&03\cdot e_i&02\cdot d_i\\01\cdot c_i&03\cdot f_i&02\cdot e_i&01\cdot d_i\\03\cdot c_i&02\cdot f_i&01\cdot e_i&01\cdot d_i\end{pmatrix}$$

$a_i,b_i,c_i,d_i,e_i,f_i(0\leq i\leq N-2)$ 表示任意非 0 字节.

(a) 算法 E^0 中 $\alpha_i\to\beta_i(0\leq i\leq N-2)$

$$Round2:\xleftarrow{SB^{-1}}\begin{pmatrix}0&?&?&?\\?&0&?&?\\?&?&0&?\\?&?&?&0\end{pmatrix}\xleftarrow{SR^{-1}}\begin{pmatrix}0&?&?&?\\0&?&?&?\\0&?&?&?\\0&?&?&?\end{pmatrix}\xleftarrow{MC^{-1}}\begin{pmatrix}0&?&?&?\\0&?&?&?\\0&?&?&?\\0&?&?&?\end{pmatrix}\xleftarrow{ARK}\begin{pmatrix}0&?&?&?\\0&?&?&?\\0&?&?&?\\0&?&?&?\end{pmatrix}\leftarrow$$

$$Round3:\xleftarrow{SB^{-1}}\begin{pmatrix}0&?&?&?\\0&?&?&?\\0&?&?&?\\0&?&?&?\end{pmatrix}\xleftarrow{SR^{-1}}\begin{pmatrix}0&?&?&?\\?&?&?&0\\?&?&0&?\\?&0&?&?\end{pmatrix}\xleftarrow{ARK}\begin{pmatrix}0&?&?&?\\?&?&?&0\\?&?&0&?\\?&0&?&?\end{pmatrix}$$

? 表示任意值.

(b) 算法 E^1 中 $\delta\to\gamma$

图 3　4 轮非对称不可能飞来器区分器的差分

定理 2.　4 轮 AES 非对称不可能飞来器区分器 $E^1\circ E^0$ 如下：

$((a_0,0,0,0),(0,0,0,0),(0,0,0,0),(0,0,0,0);\cdots(a_i,0,0,0),(0,0,0,0),(0,0,0,0),(0,0,0,0);\cdots\cdots;(a_{N-2},0,0,0),(0,0,0,0),(0,0,0,0),(0,0,0,0))\nrightarrow(X^O_{3,SR(Col(l))})_0\oplus(X^O_{3,SR(Col(l))})_{N-2}=0$，$l\in\{0,1,2,3\}$，其中 $a_i(0\leq i\leq N-2)$ 表示任意非 0 字节，? 表示任意值.

证明.　E^0 中 $\alpha_i\to\beta_i(0\leq i\leq N-2)$ 为 $((a_i,0,0,0),(0,0,0,0),(0,0,0,0),(0,0,0,0))\to((02\cdot c_i,01\cdot c_i,01\cdot c_i,03\cdot c_i)^{\mathrm{T}},(01\cdot f_i,01\cdot f_i,03\cdot f_i,02\cdot f_i)^{\mathrm{T}},(01\cdot e_i,03\cdot e_i,02\cdot e_i,02\cdot e_i)^{\mathrm{T}},(03\cdot d_i,02\cdot d_i,01\cdot d_i,01\cdot d_i)^{\mathrm{T}})$，如图 3(a)所示. 则 $\bigoplus_{i=0}^{N-2}(\alpha_i)\to\bigoplus_{i=0}^{N-2}(\beta_i)$ 为

$$((\bigoplus_{i=1}^{N-2}a_i,0,0,0),(0,0,0,0),(0,0,0,0),(0,0,0,0))\to((02\cdot\bigoplus_{i=1}^{N-2}c_i,\ 01\cdot\bigoplus_{i=1}^{N-2}c_i,\ 01\cdot\bigoplus_{i=1}^{N-2}c_i,\ 03\cdot\bigoplus_{i=1}^{N-2}c_i)^{\mathrm{T}},(01\cdot\bigoplus_{i=1}^{N-2}f_i,\ 01\cdot\bigoplus_{i=1}^{N-2}f_i,\ 03\cdot\bigoplus_{i=1}^{N-2}f_i,\ 02\cdot\bigoplus_{i=1}^{N-2}f_i)^{\mathrm{T}},(01\cdot\bigoplus_{i=1}^{N-2}e_i,\ 03\cdot\bigoplus_{i=1}^{N-2}e_i,\ 02\cdot\bigoplus_{i=1}^{N-2}e_i,\ 02\cdot\bigoplus_{i=1}^{N-2}e_i)^{\mathrm{T}},(03\cdot\bigoplus_{i=1}^{N-2}d_i,\ 02\cdot\bigoplus_{i=1}^{N-2}d_i,\ 01\cdot\bigoplus_{i=1}^{N-2}d_i,\ 01\cdot\bigoplus_{i=1}^{N-2}d_i)^{\mathrm{T}}),$$

可以看出，$\bigoplus_{i=1}^{N-2}\Delta\beta_i$ 第 l 列 4 个字节或者均为 0，或者

均不为 0. 所以 $\bigoplus_{i=1}^{n-1}\Delta\beta_i$ 有 5 种情况：(1) 16 个字节均不为 0；(2) 其中 1 列为 0，其余字节全不为 0；(3) 其中 2 列为 0，其余字节不为 0；(4) 其中 3 列为 0，其余字节不为 0；(5) 16 个字节都为 0.

E^1 中 $\delta\rightarrow\gamma$ 为 $((X_3^O)_0\bigoplus(X_3^O)_{N-2})\rightarrow((X_2^{SB})_0\bigoplus(X_2^{SB})_{N-2})$，满足 $((X^O_{3,SR(Col(l))})_0\bigoplus(X^O_{3,SR(Col(l))})_{N-2}=0)\rightarrow((X^{SB}_{2,SR^{-1}(Col(l))})_0\bigoplus(X^{SB}_{2,SR^{-1}(Col(l))})_{N-2}=0)$，$l\in\{0,1,2,3\}$，如图 3(b)所示. γ 中每一列至少有一个字节为 0. 又因为选择明文攻击中选择的 N 元组中不会有相同的明文，所以 $\gamma\neq0$.

因此 $\bigoplus_{i=0}^{N-2}(\beta_i)\bigoplus\gamma\neq0$，定理成立. 证毕.

4.3 7 轮 AES-128 的非对称不可能飞来器攻击

取 $N=3$，图 4 形象给出了 7 轮 AES-128 的非对称不可能飞来器攻击.

$$Round0:\xrightarrow{ARK}\begin{pmatrix}g_i&0&0&0\\0&h_i&0&0\\0&0&o_i&0\\0&0&0&s_i\end{pmatrix}\xrightarrow{SB}\begin{pmatrix}q_i&0&0&0\\0&u_i&0&0\\0&0&v_i&0\\0&0&0&w_i\end{pmatrix}\xrightarrow{SR}\begin{pmatrix}q_i&0&0&0\\u_i&0&0&0\\v_i&0&0&0\\w_i&0&0&0\end{pmatrix}\xrightarrow{MC}\begin{pmatrix}a_i&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\xrightarrow{ARK}\begin{pmatrix}a_i&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$$

g_i，h_i，o_i，s_i，q_i，u_i，v_i，w_i($i=0,1$)表示任意非 0 字节.

(a) 算法 E^{bef}

$$Round4:\ \cdots\cdots\begin{pmatrix}z&0&0&0\\z&0&0&0\\z&0&0&0\\0&0&0&0\end{pmatrix}\xleftarrow{MC^{-1}}\begin{pmatrix}z&0&0&0\\z&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$$

$$Round5:\xleftarrow{SB^{-1}}\begin{pmatrix}z&0&0&0\\z&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}\xleftarrow{SR^{-1}}\begin{pmatrix}z&0&0&0\\0&0&0&z\\0&0&0&0\\0&0&0&0\end{pmatrix}\xleftarrow{ARK}\begin{pmatrix}z&0&0&0\\0&0&0&z\\0&0&0&0\\0&0&0&0\end{pmatrix}\xleftarrow{MC^{-1}}\begin{pmatrix}z&0&0&z\\z&0&0&z\\z&0&0&z\\z&0&0&z\end{pmatrix}\leftarrow$$

$$Round6:\xleftarrow{SB^{-1}}\begin{pmatrix}z&0&0&z\\0&0&z&z\\0&z&z&0\\z&z&0&0\end{pmatrix}\xleftarrow{SR^{-1}}\begin{pmatrix}z&0&0&z\\0&0&z&z\\0&z&z&0\\z&z&0&0\end{pmatrix}\xleftarrow{ARK}\begin{pmatrix}z&0&0&z\\0&0&z&z\\0&z&z&0\\z&z&0&0\end{pmatrix}$$

z 表示任意非 0 字节.

(b) 算法 E^{aft}

图 4 7 轮 AES-128 的非对称不可能飞来器攻击

4.3.1 攻击过程

由于攻击需要，第 4 轮和第 5 轮的 MC 和 ARK 交换.

预计算阶段.

1. $X^{MC}_{0,Col(0)}$ 的差分为下列 4 种情形之一：$(a,0,0,0)$，$(0,a,0,0)$，$(0,0,a,0)$或$(0,0,0,a)$，其中 a 表示任意非 0 字节(下同). 共有 $2^{32}\times4\times(2^8-1)\approx2^{42}$ 数据对. 对每一个数据对计算 $X^I_{0,SR^{-1}(Col(0))}$，将这些 4 字节的数据对以它们在这 4 个字节的差分为索引，存储于一张 Hash 表 $Hash_{-1}$，一个索引值平均对应 2^{10} 数据对.

2. $X^O_{5,Col(0)}$ 的差分如为$(a,0,0,0)$，有 $2^{32}\times(2^8-1)\approx2^{40}$ 数据对. 对每一个数据对计算 $X^{SR}_{6,SR(Col(0))}$，将这些 4 字节的数据对以它们在这 4 个字节差分为索引，存储于一张 Hash 表 $Hash_0$，一个索引值平均对应 2^8 数据对. 下面计算存储按照同样的方法. $X^O_{5,Col(0)}$ 的差分如为$(0,a,0,0)$，有约 2^{40} 数据对，计算 $X^{SR}_{6,SR(Col(0))}$. Hash 表 $Hash_1$ 存储数据对. $X^O_{5,Col(0)}$ 的差分如为$(0,0,a,0)$，有约 2^{40} 数据对，计算 $X^{SR}_{6,SR(Col(0))}$. Hash 表 $Hash_2$ 存储数据对. $X^O_{5,Col(0)}$ 的差分如为$(0,0,0,a)$，有约 2^{40} 数据对，计算 $X^{SR}_{6,SR(Col(0))}$. Hash 表 $Hash_3$ 存储数据对.

3. $X^O_{5,Col(3)}$ 的差分如为$(a,0,0,0)$，有约 2^{40} 数据对，计算 $X^{SR}_{6,SR(Col(3))}$. Hash 表 $Hash_{12}$ 存储数据对. $X^O_{5,Col(3)}$ 的差分如为$(0,a,0,0)$，有约 2^{40} 数据对，计算 $X^{SR}_{6,SR(Col(3))}$. Hash 表 $Hash_{13}$ 存储数据对. $X^O_{5,Col(3)}$ 的差分如为$(0,0,a,0)$，有约 2^{40} 数据对，计算 $X^{SR}_{6,SR(Col(3))}$. Hash 表 $Hash_{14}$ 存储数据对. $X^O_{5,Col(3)}$ 的差分如为$(0,0,0,a)$，有约 2^{40} 数据对，计算 $X^{SR}_{6,SR(Col(3))}$. Hash 表 $Hash_{15}$ 存储数据对.

在线阶段.

1. 定义一种结构 $Struc_i$. 2^{32} 个明文 $P_{i,j}$ 在字节 $SR^{-1}(Col(0))$取所有可能的值，其余字节固定. $Struc_i$ 产生 $C_{2^{32}}^2\approx2^{63}$ 个明文对(P_{i,j_0},P_{i,j_2})，每个明文对(P_{i,j_0},P_{i,j_2})形成 $P_{2^{32}-2}^1\approx2^{32}$ 个三元组$(P_{i,j_0},P_{i,j_1},P_{i,j_2})$，满足任意两两三元组的无序差分组$(P_{i,j_0}\bigoplus P_{i,j_1},P_{i,j_1}\bigoplus P_{i,j_2})$均不重复. 选择 $2^{73.18}$ 个结构 $Struc_i(i=0,1,\cdots,2^{73.18}-1)$，生成 $2^{73.18}\times2^{63}\times2^{32}=2^{168.18}$ 个三元组$(P_{i,j_0},P_{i,j_1},P_{i,j_2})$. 在选择明文攻击中，对于 $2^{73.18}\times2^{32}=2^{105.18}$ 个明文，获得相应密文 $C_{i,j}$. 选择三元组$(P_{i,j_0},P_{i,j_1},P_{i,j_2})$满足$(X^O_{6,SR(Col(1,2))})_{i,j_0}\bigoplus(X^O_{6,SR(Col(1,2))})_{i,j_2}=0$，其中 $0\leq j_0\neq j_2\leq2^{32}-1$. 剩余 $2^{168.18}\times2^{-64}=2^{104.18}$ 个三元组.

2. 初始化 2^{32} 个空列表，每个对应 $K_{-1,SR^{-1}(Col(0))}$ 的猜测值. 考虑剩余明文三元组$(P_{i,j_0},P_{i,j_1},P_{i,j_2})$，计算 $P_{i,j_0}\bigoplus P_{i,j_1}$ 和 $P_{i,j_1}\bigoplus P_{i,j_2}$ 在字节 $SR^{-1}(Col(0))$值，用 ΔP_0、ΔP_1 表示. 分别访问 $Hash_{-1}$ 中分别以 ΔP_0、ΔP_1 索引的库. 对于

ΔP_0索引库中的每一个数据对(x_0, y_0)，ΔP_1索引库中的每一个数据对(x_1, y_1)，如果存在 $P_{i,j_0} \oplus x_0 = P_{i,j_1} \oplus x_1$，则把明文三元组$(P_{i,j_0}, P_{i,j_1}, P_{i,j_2})$添加到相应密钥列表$P_{i,j_0} \oplus x_0$值中. $Pr(P_{i,j_0} \oplus x_0 = P_{i,j_1} \oplus x_1) = 2^{10} \times 2^{-32} = 2^{-22}$，因此$2^{104.18} \times 2^{10} \times 2^{-22} = 2^{92.18}$值分布在$2^{32}$个密钥上，即每个子密钥 $K_{-1,SR^{-1}(Col(0))}$剩余 $2^{60.18}$个三元组.

3. 对每个猜测值 $K_{-1,SR^{-1}(Col(0))}$，剩余的 $2^{60.18}$个三元组中选取 $2^{57.18}$个三元组$(P_{i,j_0}, P_{i,j_1}, P_{i,j_2})$，满足$(P_{i,j_0}, P_{i,j_2})$不重复. 由于对于每个 $K_{-1,SR^{-1}(Col(0))}$，步 2 中任意一个对(P_{i,j_0}, P_{i,j_2})相应的 2^{32}个三元组$(P_{i,j_0}, P_{i,j_1}, P_{i,j_2})$中，剩余概率为$2^{32} \times (2^{10} \times 2^{-32})^2 = 2^{-12}$. 由泊松分布 $Y \sim Poi(\lambda = 2^{-12})$，$Pr(Y \geqslant 9) \approx 2^{-126.5}$，剩余 9 个三元组$(P_{i,j_0}, P_{i,j_1}, P_{i,j_2})$对应相同$(P_{i,j_0}, P_{i,j_2})$的概率为 $2^{-126.5}$. 因为共有 2^{105}个三元组$(P_{i,j_0}, P_{i,j_1}, P_{i,j_2})$，所以剩余三元组中存在一个对$(P_{i,j_0}, P_{i,j_2})$对应 9 个三元组$(P_{i,j_0}, P_{i,j_1}, P_{i,j_2})$的概率非常低. 因此假定剩余三元组中每个对$(P_{i,j_0}, P_{i,j_2})$对应 8 个三元组$(P_{i,j_0}, P_{i,j_1}, P_{i,j_2})$，则剩余 $2^{60.18}$个三元组中至少有$2^{60.18} \times 2^{-3} = 2^{57.18}$个三元组$(P_{i,j_0}, P_{i,j_1}, P_{i,j_2})$满足$(P_{i,j_0}, P_{i,j_2})$不重复.

步 4～6 为$m=0,1,2,3$的循环执行.

4. 初始化 2^{32}空列表，每一个相应于 $K_{6,SR(Col(0)}$的猜测值. 考虑剩余三元组$(C_{i,j_0}, C_{i,j_1}, C_{i,j_2})$，且计算$(C_{i,j_0} \oplus C_{i,j_2})$在字节 $SR(Col(0))$值，用 ΔP_2表示. 访问 $Hash_m$中 ΔP_2为索引的库，对于该库中的每一个数据对(x_2, y_2)，计算 $C_{i,j_0} \oplus x_2$，则把三元组$(C_{i,j_0}, C_{i,j_1}, C_{i,j_2})$添加到相应密钥列表 $C_{i,j_0} \oplus x$ 值中. $2^{57.18} \times 2^8$值分布在 2^{32}个密钥上，因此每个 $K_{-1,SR^{-1}(Col(0))}$子密钥，剩余 $2^{57.18} \times 2^8 \times 2^{-32} = 2^{33.18}$个三元组.

5. 初始化 2^{32}空列表，每一个相应于 $K_{6,SR(Col(3))}$的猜测值. 考虑剩余明文三元组$(C_{i,j_0}, C_{i,j_1}, C_{i,j_2})$，且计算$(C_{i,j_0} \oplus C_{i,j_2})$在字节 $SR(Col(3))$值，用 ΔP_3表示. 访问 $Hash_{12+(m+1) \bmod 4}$中 ΔP_3为索引的库，对于该库中的每一个数据对(x_3, y_3)，计算 $C_{i,j_0} \oplus x_3$，则把三元组$(C_{i,j_0}, C_{i,j_1}, C_{i,j_2})$添加到相应密钥列表 $C_{i,j_0} \oplus x_3$值中. $2^{33.18} \times 2^8$值分布在 2^{32}个密钥上，因此每个 $K_{6,SR(Col(3))}$子密钥，剩余 $2^{33.18} \times 2^8 \times 2^{-32} = 2^{9.18}$个三元组.

6. 猜 2 个字节的子密钥$(\widetilde{K}_{5,m}, \widetilde{K}_{5,12+(m+1) \bmod 4})$. 部分解密剩余三元组$(C_{i,j_0}, C_{i,j_1}, C_{i,j_2})$中的$(C_{i,j_0}, C_{i,j_2})$，检验是否$(X^O_{4,Col(m)})_{i,j_0} \oplus (X^O_{4,Col(m)})_{i,j_2}$只有 1 个字节为 0. 假如存在三元组满足这个条件，则丢弃密钥值$(K_{6,SR(Col(0))}, K_{6,SR(Col(3))}, \widetilde{K}_{5,m}, \widetilde{K}_{5,12+(m+1) \bmod 4}, K_{-1,SR^{-1}(Col(0))})$.

7. 对每个可能的子密钥值$(K_{6,SR(Col(0))}, K_{6,SR(Col(3))}, \widetilde{K}_{5,Col(0)}, \widetilde{K}_{5,Col(3)}, K_{-1,SR^{-1}(Col(0))})$，结合 AES-128 密钥方案，穷举确定剩余 24bit 密钥.

4.3.2　复杂度分析

预计算阶段.

时间复杂度为 $3 \times 2 \times 2^{42} \times 1/7 \times 1/4 \approx 2^{39.2}$次 7 轮 AES-128 加密，存储复杂度为 $3 \times 2 \times 2^{42} \times 1/4 \approx 2^{42.6}$个 AES 分组.

在线阶段. 需要 $2^{105.18}$个选择明文.

1. 存储复杂度为 $3 \times 2 \times 2^{104.18} = 2^{106.78}$个 AES 分组.

2. 时间复杂度为 $2 \times 2^{104.18} \times 2^{10} = 2^{115.18}$次存储访问，约相当于[12] $2^{108.18}$次 7 轮 AES-128 加密.

3. 存储复杂度为 $3 \times 2 \times 2^{60.18} \times 2^{32} = 2^{94.78}$个 AES 分组.

4. 时间复杂度为 $4 \times 2^{32} \times 2^{57.18} \times 2^8 = 2^{99.18}$次存储访问. 存储复杂度为 $3 \times 2 \times 2^{57.18} \times 2^8 = 2^{67.78}$个 AES 分组.

5. 时间复杂度为 $4 \times 2^{64} \times 2^{33.18} \times 2^8 = 2^{107.18}$次存储访问. 存储复杂度为 $3 \times 2 \times 2^{33.18} \times 2^8 = 2^{43.78}$个 AES 分组.

6. 时间复杂度为 $4 \times \{2 \times 2^{112} \times [1 + (1-2^{-6}) + \cdots + (1-2^{-6})^{2^{9.18}}] \times 2/16 \times 1/7\} \approx 2^{115.2}$次 7 轮 AES-128 加密.

对于每个 m，满足条件的三元组概率为 $4 \times 2^{-8} = 2^{-6}$. 对于每个猜测的 96bit 密钥值$(K_{6,SR(Col(0))}, K_{6,SR(Col(3))}, K_{-1,SR^{-1}(Col(0))})$，预计剩余约 $2^{16} \times (1-2^{-6})^{2^{9.18}} \approx 2^{2.82}$个子密钥$(\widetilde{K}_{5,m}, \widetilde{K}_{5,12+(m+1) \bmod 4})$. 考虑 4 个迭代 $m=0,1,2,3$，对于每个猜测的$(K_{6,SR(Col(0))}, K_{6,SR(Col(3))}, K_{-1,SR^{-1}(Col(0))})$，剩余约 $2^{2.82 \times 4} = 2^{11.28}$个子密钥$(\widetilde{K}_{5,Col(0)}, \widetilde{K}_{5,Col(3)})$. 由 AES-128 密钥方案，得到 $2^{96} \times 2^{11.28} \times 2^{-24} = 2^{83.28}$个可能的子密钥.

7. 时间复杂度为 $2^{83.28} \times 2^{24} = 2^{107.28}$次 7 轮 AES-128 加密.

因此，攻击所需要的数据复杂度为 $2^{105.18}$个选择明文，时间复杂度为 $2^{115.2}$次 7 轮 AES-128 加密，由步 6 决定；存储复杂度为 $2^{106.78}$个 AES 分组，由步 1 决定.

5　结　论

分组密码是信息安全的核心密码算法. 基于差分分析原理，本文提出了非对称不可能飞来器攻击这一新的分组密码分析方法. 该方法是通过构造非对称不可能飞来器区分器，排除满足这种关系的密钥，并最终恢复出秘密密钥的一种攻击方法. 然后，构造了 4 轮AES 非对称不可能飞来器区分器，利用密钥编排方案、差分表查询技术和数据多次利用技术，针对 AES-128 进行了新分析. 攻击 7 轮 AES-128 所需的数据复杂度为 $2^{105.18}$个选择明文，时间复杂度为 $2^{115.2}$次加密，存储复杂度为 $2^{106.78}$个 AES 分组. 与已有的结果比较见表 1，可以看出：新分析的攻击轮数达到 7 轮. 在 7 轮攻击中，时间复杂度低于已有攻击；数据复杂度也低于除文献[4]以外的攻击，而文献[4]为巨型攻击，因为它需要的时间复杂度为 2^{128}次加密，等于密钥穷举搜索. 因此针对 AES-128 的攻击，本文提出的密码分析方法更为新型有效.

表 1 单密钥下 AES-128 的攻击结果比较

攻击类型	轮数	数据复杂度(CP)	时间复杂度	存储复杂度	文献
平方攻击	6	2^{32}	2^{72}	2^{32}	[2]
平方攻击	6	$2^{34.6}$	2^{44}	2^{32}	[3]
平方攻击	7	$2^{127.997}$	2^{120}	2^{64}	[4]
碰撞攻击	7	2^{32}	2^{128}	2^{96}	[5]
不可能差分攻击	6	$2^{91.5}$	2^{122}	—	[6]
不可能差分攻击	7	$2^{115.5}$	2^{119}	2^{105}	[7]
不可能差分攻击	7	$2^{112.2}$	$2^{115.6}$	2^{105}	[8]
不可能差分攻击	7	$2^{112.2}$	$2^{117.2}$ MA	$2^{89.2}$	[9]
中间相遇攻击	7	2^{116}	2^{116}	2^{116}	[11]
飞来器攻击	6	2^{71}	2^{71}	2^{33}	[10]
不可能飞来器攻击	6	$2^{112.2}$	$2^{112.3}$	2^{49}	[8]
非对称不可能飞来器攻击	7	$2^{105.18}$	$2^{115.2}$	$2^{106.78}$	本文

注:CP 为选择明文;MA 为存储访问. 时间复杂度单位:加密次数;存储复杂度单位:AES 分组.

本文提出的非对称不可能飞来器攻击可以应用于其它分组密码算法分析中,研究中可以进一步关注.

参 考 文 献

[1] Daemen J, Rijmen V. The design of Rijndael: AES — The Advanced Encryption Standard. Berlin Heidelberg: Springer-Verlag, 2002

[2] Daemen J, Knudsen L, Rijmen V. The block cipher SQUARE//Proceedings of FSE1997-The 4th International Workshop on Fast Software Encryption. Haifa, Israel, 1997: 149-165

[3] Ferguson N, Kelsey J, Lucks S, Schneier B, Stay M, Wagner D, Whiting D. Improved cryptanalysis of Rijndael//Proceedings of FSE2000-The 7th International Workshop on Fast Software Encryption. New York, USA, 2001: 213-230

[4] Gilbert H, Minier M. A collision attack on 7 rounds of Rijndael//Proceedings of AES2000-The 3th International Conference on Advanced Encryption Standard. New York, USA. http://homes.esat.kuleuven.be/~abiryuko/Cryptan/11-hgilbert.pdf

[5] Biham E, Keller N. Cryptanalysis of reduced variants of Rijndael//Proceedings of AES2000-The 3th International Conference on Advanced Encryption Standard. New York, USA, 2000. http://www.madchat.fr/crypto/codebreakers/35-ebiham.pdf

[6] Cheon J, Kim M, Kim K, Lee J, Kang S. Improved impossible differential cryptanalysis of Rijndael and Crypton//Proceedings of ICISC 2001-The 4th International Conference on Information Security and Cryptology. Seoul, Korea, 2002: 39-49

[7] Zhang W, Wu W, Feng D. New results on impossible differential cryptanalysis of reduced AES//Proceedings of ICISC 2007-The 10th International Conference on Information Security and Cryptology. Seoul, Korea, 2007: 239-250

[8] Lu J. Cryptanalysis of block ciphers [Ph. D. dissertation]. University of London, Royal Holloway, England, 2008

[9] Lu J, Dunkelman O, Keller N, Kim J. New impossible differential attacks on AES//Proceedings of the Progress in Cryptology-NDOCRYPT 2008-The 9th International Conference on Cryptology in India. Kharagpur, India, 2008: 279-293

[10] Biryukov A. Boomerang attack on 5 and 6-round AES//Proceedings of AES2004-The 4th International Conference on Advanced Encryption Standard. Bonn, Germany, 2005: 11-15

[11] Dunkelman O, Keller N, Shamir A. Improved single-key attacks on 8-round AES//Proceedings of the Advances in Cryptology-ASIACRYPT 2010- The 16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore, 2010: 158-176

[12] Kim J, Hong S, Peneel B. Related-key rectangle attacks on reduced AES-192 and AES 256//Proceedings of FSE2007-The 14th International Workshop on Fast Software Encryption. Luxembourg, Luxembourg. 2007: 225-241

[13] Biryukov A, Khoveratocich D. Related-key cryptanalysis of the full AES-192 and AES-256//Proceedings of the Advances in Cryptology-ASIACRYPT200-The 15th International Conference on the Theory and Application of Cryptology and Information Security. Tokyo, Japan, 2009: 1-18

DONG Xiao-Li, born in 1982, Ph. D. candidate. Her research interests focus on design and analysis of block cipher.

HU Yu-Pu, born in 1955, Ph. D., professor, Ph. D. supervisor. His research interests include cryptology and network security.

CHEN Jie, born in 1979, Ph. D., associate professor. Her research interests include design and analysis of block cipher.

WEI Yong-Zhuang, born in 1976, Ph. D.. His research interests include analysis of cryptographic function and block cipher.

Background

This work is supported by the National Natural Science Foundation of China under grant Nos. 60970119, 60833008, the National Basic Research Program (973 Program) of China under grant No. 2007CB311201 and the Fundamental Research Funds for the Central Universities under grant No. K50510010018.

As AES has become one of the most worldwide used block ciphers, cryptanalysts had evaluated the security of AES against various cryptanalytic techniques, including impossible differential cryptanalysis, meet-in-the-middle attack, boomerang attack, square attack, related-key attack and so on. After 13 years of analysis, in the single-key attack model, attacks on AES-128 have been unable to go any further than 7 rounds. The best results are as follow: the first is an impossible differential attack in the doctoral dissertation of Lu J, which requires $2^{112.2}$ chosen plaintexts and $2^{115.6}$ encryptions; the second is an impossible differential attack at INDOCRYT 2008, which requires $2^{112.2}$ chosen plaintexts and $2^{117.2}$ memory accesses; the third attack is a meet-in-the-middle attack at ASIACRYPT2010, which requires 2^{116} chosen plaintexts and 2^{116} encryptions. In this paper, we introduced a new cryptanalytic technique on block cipher: asymmetric impossible boomerang attack. We applied asymmetric impossible boomerang attack to 7-round AES-128. It requires data complexity of about $2^{105.18}$ chosen plaintexts, time complexity of about $2^{115.2}$ encryptions and memory complexity of about $2^{106.78}$ AES blocks. The presented result is better than any previous published cryptanalytic results on AES-128 in terms of the numbers of attacked rounds, the data complexity and the time complexity.