改进的 7 轮 AES-192 和 8 轮 AES-256 的中间相遇攻击

董晓丽[1]，胡予濮[1]，陈杰[1,2]，李顺波[1,3]，杨旸[1]

(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，陕西 西安 710071；
2. 中国科学院 软件研究所信息安全国家重点实验室，北京 100049；3. 西安建筑科技大学 理学院，陕西 西安 710055)

摘 要：利用 AES 密码算法轮变换的特点，构造了一个 5 轮中间相遇攻击区分器的新变体。基于该区分器变体，使用时空折中方法，针对 7 轮 AES-192 和 8 轮 AES-256 分别给出了新的攻击方法。研究结果表明，与 FSE2008 提出的针对 AES 的中间相遇攻击结果比较，新分析所需的时间复杂度和存储复杂度降低。

关键词：分组密码；AES；密码分析；中间相遇攻击；时间复杂度

中图分类号：TN918.1 **文献标识码**：A **文章编号**：1000-436X(2010)9A-0197-05

Improved meet-in-the-middle attacks on 7-round AES-192 and 8-round AES-256

DONG Xiao-li[1], HU Yu-pu[1], CHEN Jie[1,2] , LI Shun-bo[1,3], YANG Yang[1]

(1. Key Laboratory of Computer Networks & Information Security of Ministry of Education,Xidian University, Xi'an 710071, China;
2. State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100049, China;
3. School of Science，Xi'an University of Architecture and Technology, Xi'an 710055, China)

Abstract: A new variant of 5-round distinguisher of meet-in-the-middle attack on AES was constructed by exploiting the properties of the round transform of AES. Based on the variant of distinguisher, meet-in-the-middle attacks on 7-round AES-192 and 8-round AES-256 were presented by using the time-memory tradeoff approach. It is shown that the new results are better than the cryptanalytic results presented at FSE2008 on reduced AES in terms of the time complexity and the memory complexity.

Key words: block cipher; AES; cryptanalysis; meet-in-the-middle attack; time complexity

1 引言

高级加密标准 AES[1]分组长度是 128bit，其密钥长度有 128、192 和 256bit 3 种。自 2000 年 AES 入选以来，它已经成为全球最受关注和广泛使用的分组密码之一。

AES 的安全性分析是近年来国内外分组密码研究的重点之一。AES 的设计者[2]提出 6 轮 AES-128 的平方攻击，需要 2^{32} 选择明文和 2^{72} AES 加密。文献[3]把攻击的时间复杂度降为 2^{44} 。利用 AES-192 和 AES-256 的密钥编排方案，攻击[4]可以扩展到 7 轮。文献[5]基于 3 轮加密后的碰撞性质，7 轮 AES-192 和 AES-256 需要 2^{32} 选择明文和 2^{140} AES 加密，且 AES-128 的攻击优于穷举搜索。文献[6,7]

收稿日期：2010-08-10

基金项目：国家自然科学基金资助项目（60970119, 60833008）；国家重点基础研究发展计划（"973"计划）基金资助项目（2007CB311201）；西安建筑科技大学青年基金资助项目（QN1024）

Foundation Items: The National Natural Science Foundation of China (60970119, 60833008); The National Basic Research and Program (973 Program) (2007CB311201); Youth Foundation of Xian Uuiversity of Architecture and Technology(QN1024)

提出 7 轮 AES 的不可能差分攻击，但时间复杂度高于平方攻击。新的不能差分攻击[8~11]降低了上述不可能差分攻击时间复杂度。飞来器攻击[12]分析 5 轮 AES 需要 2^{46} 选择明文和 2^{46} 步分析，分析 6 轮 AES 需要 2^{78} 选择明文， 2^{78} 步分析和 2^{78} 字节。文献[13]提出 AES 的代数攻击。文献[14]首次提出 AES 的 5 轮区分器，基于该区分器攻击 7 轮 AES-192 和 8 轮 AES-256，它还给出时空折中方法平衡开销。文献[15]指出[14]中 AES 内部加密函数的表达式可以被简化，基于此区分器成功攻击 7 轮 AES-128，7 轮 AES-192 和 8 轮 AES-256，并指出在单钥下针对 7 轮 AES-128 的攻击在线时间复杂度是目前最低的。AES 的相关密钥攻击[16~21]扩展到 10 轮。Biryukov 等[22, 23]利用相关密钥飞来器攻击，首次完成了全轮(12 轮)AES-192 与(14 轮) AES-256 的分析，理论上首次攻破了 AES-192 与 AES-256。

文献[14]指出 AES 的性质：当明文集中仅有一个活性字节而其余字节固定时，4 轮 AES 加密后，密文的每一字节完全由固定的 25 个字节决定。本文使用上述性质和 AES 密码算法轮变换的特点，构造了 AES 的 5 轮中间相遇攻击区分器的新变体。基于该区分器变体和时空折中方法，针对 7 轮 AES-192，8 轮 AES-256 分别给出了新攻击方法。与文献[14]的攻击结果相比，新分析所需的预计算复杂度、时间复杂度和存储复杂度均降低。

2 AES

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 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 1 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[1]把秘密密钥扩充成128(R+1)bit 子密钥，其中 R 表示轮数。

本文在 AES 分析中，使用下列符号。$K^{(r)}$、$C^{(r)}$ 表示 r 轮轮密钥和密文，其中 $K^{(0)}$表示白化密钥。$SB^{(r)}$、$SR^{(r)}$、$MC^{(r)}$、$ARK^{(r)}$分别表示第 r 轮 *SB*、*SR*、*MC*、*ARK* 的中间值。相应 $K_{ij}^{(r)}$、$C_{ij}^{(r)}$、$SB_{ij}^{(r)}$、$SR_{ij}^{(r)}$、$MC_{ij}^{(r)}$、$ARK_{ij}^{(r)}$ 表示第 i 行，j 列的相应值。$a||b$ 表示串 a 与串 b 的级联。本文的运算是在 $GF(2^8)$上的，且⊕表示长度相同串的比特异或。

3 AES 的 5 轮区分器

下面[14]为 5 轮 AES 的性质：考虑 5 轮 AES（没有白化）的演化过程。假设 a_{ij} 为明文第 i 行，第 j 列，经过 AES S 盒变换后定义 t_{ij}=S(a_{ij})。第一轮变换后数据状态矩阵为 $((2t_{11}\oplus c_1, t_{11}\oplus c_2, t_{11}\oplus c_3, 3t_{11}\oplus c_4)^{\mathrm{T}}, (m_{12}, m_{22}, m_{32}, m_{42})^{\mathrm{T}}, (m_{13}, m_{23}, m_{33}, m_{43})^{\mathrm{T}}, (m_{14}, m_{24}, m_{34}, m_{44})^{\mathrm{T}})$ 其中 $m_{ij}, c_i (1\leqslant i\leqslant 4, 2\leqslant j\leqslant 4)$是固定值，这些值依赖固定字节和子密钥值。

性质 1[14] 考虑一个集合：a_{11} 活跃而其他字节固定的 256 个明文。4 轮 AES 加密这一集合。函数 $f_1: a_{11}\rightarrow S(C_{11}^{(4)})$ 由 25 个字节决定。

证明 下面方程(1~4)成立，

$$C_{11}^{(3)} = 2S(2S(2t_{11}\oplus c_1)\oplus c_5)\oplus 3S(S(3t_{11}\oplus c_4)\oplus c_6)\oplus S(2S(t_{11}\oplus c_3)\oplus c_7)\oplus S(S(t_{11}\oplus c_2)\oplus c_8)\oplus K_{11}^{(3)} \quad (1)$$

$$C_{22}^{(3)} = S(S(3t_{11}\oplus c_4)\oplus c_9)\oplus 2S(3S(t_{11}\oplus c_3)\oplus c_{10})\oplus 3S(S(t_{11}\oplus c_2)\oplus c_{11})\oplus S(3S(2t_{11}\oplus c_1)\oplus c_{12})\oplus K_{22}^{(3)} \quad (2)$$

$$C_{33}^{(3)} = S(S(t_{11}\oplus c_3)\oplus c_{13})\oplus S(2S(t_{11}\oplus c_2)\oplus c_{14})\oplus 2S(S(2t_{11}\oplus c_1)\oplus c_{15})\oplus 3S(2S(3t_{11}\oplus c_4)\oplus c_{16})\oplus K_{33}^{(3)} \quad (3)$$

$$C_{44}^{(3)} = 3S(3S(t_{11}\oplus c_2)\oplus c_{17})\oplus S(S(2t_{11}\oplus c_1)\oplus c_{18})\oplus S(3S(3t_{11}\oplus c_4)\oplus c_{19})\oplus 2S(S(t_{11}\oplus c_3)\oplus c_{20})\oplus K_{44}^{(3)} \quad (4)$$

由于

$$S(C_{11}^{(4)}) = S(2S(C_{11}^{(3)})\oplus 3S(C_{22}^{(3)})\oplus S(C_{33}^{(3)})\oplus S(C_{44}^{(3)})\oplus K_{11}^{(4)}) \quad (5)$$

因此 25 个固定值字节

$$(c_1,\cdots,c_{20}, K_{11}^{(3)}, K_{22}^{(3)}, K_{33}^{(3)}, K_{44}^{(3)}, K_{11}^{(4)}) \quad (6)$$

完全可以表达函数 $f_1: a_{11}\rightarrow S(C_{11}^{(4)})$。

结合 1 轮的解密，得到下列 5 轮区分器。

性质 2[14] 考虑一个集合：a_{11} 活跃而其他字节固定的 256 个明文。5 轮 AES 加密这一集合。令 S^{-1} 为 AES 中 S 盒的逆变换，且 $k^{(5)} = 0E\cdot K_{11}^{(5)}\oplus 0B\cdot K_{21}^{(5)}\oplus 0D\cdot K_{31}^{(5)}\oplus 09\cdot K_{41}^{(5)}$。则

$S^{-1}[0E\cdot C_{11}^{(5)}\oplus 0B\cdot C_{21}^{(5)}\oplus 0D\cdot C_{31}^{(5)}\oplus 09\cdot C_{41}^{(5)}\oplus k^{(5)}]$

是 a_{11} 的函数，且完全由 5 个密钥字节和 20 个同时

依赖密钥和固定字节的字节决定。因此 $f_2: a_{11} \to S^{-1}[0E \cdot C_{11}^{(5)} \oplus 0B \cdot C_{21}^{(5)} \oplus 0D \cdot C_{31}^{(5)} \oplus 09 \cdot C_{41}^{(5)} \oplus k^{(5)}]$ 完全由 26 个常数字节决定。

4　AES 的 5 轮区分器的新变体

基于上节中性质 1，性质 2，结合 AES 密码算法轮变换的特点，得到下面的性质。

性质 3　考虑一个集合：a_{11} 活跃而其他字节固定的 256 个明文。4 轮 AES 加密这一集合，求得函数 $f_1: a_{11} \to S(C_{11}^{(4)})$。5 轮 AES 加密这一集合，求得函数 $f_2: a_{11} \to S^{-1}[0E \cdot C_{11}^{(5)} \oplus 0B \cdot C_{21}^{(5)} \oplus 0D \cdot C_{31}^{(5)} \oplus 09 \cdot C_{41}^{(5)} \oplus k^{(5)}]$，则

$$\forall T \in \{0,1\}^8, f_1(0) \oplus f_2(0) = f_1(1) \oplus f_2(1) = \cdots = f_1(T) \oplus f_2(T) \quad (7)$$

且称串 $f_1(0) \| f_1(1) \| \cdots \| f_1(T)$ 与串 $f_2(0) \| f_2(1) \| \cdots \| f_2(T)$ 相匹配。

证明　由 AES 密码算法轮变换的特点，可得 $f_1(a_{11}) \oplus k_5 = f_2(a_{11})(0 \leqslant a_{11} \leqslant 255)$，其中 $k^{(5)} = 0E \cdot K_{11}^{(5)} \oplus 0B \cdot K_{21}^{(5)} \oplus 0D \cdot K_{31}^{(5)} \oplus 09 \cdot K_{41}^{(5)}$。因此式（7）成立。

上述性质的提出，使得在实际攻击中，不需要猜测 $k^{(5)}$。

5　攻击 7 轮 AES-192

这一部分将基于上述的 5 轮区分器变体给出 7 轮 AES 的中间相遇的攻击方法。该攻击的基本思路为：首先利用性质 1 预计算所有可能的映射，即 $f_1: a_{11} \to S(C_{11}^{(4)})$；其次选择加密明文集合，并猜测相关的子密钥进行部分加解密。最后比较解密值和预计算表中的值，如果部分解密后相应的值和与预计算里的值满足式(7)，则猜测的密钥很可能是正确的密钥。

5.1　攻击过程

具体攻击过程如下，其中第 6 轮 $MC^{(6)}$ 与 $ARK^{(6)}$ 交换次序：

step1　对式(6)中 $2^{25\times8} = 2^{200}$ 可能参数值，据式(1)~式(5)，计算 $f_1: a_{11} \to S(C_{11}^{(4)})$，其中 $0 \leqslant a_{11} \leqslant 44$。

step2　选择 2^{32} 明文，满足主对角线取遍所有可能的值，而其余字节取值固定。令 K_{init} 表示白化子密钥 $(K_{11}^{(0)}, K_{22}^{(0)}, K_{33}^{(0)}, K_{44}^{(0)})$。使用 $K_{init}, K_{11}^{(1)}$ 部分加密 2^{32} 明文，选择 45 个明文的集合，满足 $C_{11}^{(1)}$ 取遍 0 到 44 这 45 个值，$C_{21}^{(1)}, C_{31}^{(1)}, C_{41}^{(1)}$ 字节固定。7 轮 AES 加密这一集合。

step3　令 K_{final} 表示 $(K_{11}^{(7)}, K_{24}^{(7)}, K_{33}^{(7)}, K_{42}^{(7)})$。$K_{final}$ 部分解密 Step2 中 45 个密文来获得 $ARK_{11}^{(6)}$。

step4　假如 $K_{init}, K_{11}^{(1)}$ 和 K_{final} 猜测正确，函数 $C_{11}^{(1)} \to S(C_{11}^{(5)})$ 必须与预计算表的函数之一满足式（7）。把第 3 步 45 个 $ARK_{11}^{(6)}$ 值组成的串和预计算表相应的串做比较，如果满足性质中定义的“匹配”，目前猜测的密钥以很大的概率为正确密钥，由于对每个错误的密钥匹配的概率为 $2^8 \times 2^{8\times25} \times 2^{-8\times45} = 2^{-152}$。

step5　使用相同的明文集，对不同的目标值 $ARK_{21}^{(6)}$、$ARK_{31}^{(6)}$、$ARK_{41}^{(6)}$ 重复 3 次攻击。由于已经发现 K_{init}，由后 2 轮攻击得出另外 15 个密钥字节。

step6　搜索剩余的密钥，最终获得主密钥。

5.2　复杂度分析

攻击需要 2^{32} 选择明文。预计算阶段为 $45\times2^{200} = 2^{205.5}$ 函数值计算，存储 $2^{205.5} \times 2^{-4} = 2^{201.5}$ AES 分组。密钥搜索阶段，每个子密钥 $K_{init}, K_{11}^{(1)}, K_{final}$ 对 45 个明文部分解密，时间复杂度为 $45\times2^{40}\times2^{32} = 2^{77.5}$ 部分 AES 加密，约等价于 $2^{69.5}$ AES 加密[14]。考虑对 4 个目标值的计算，预计算时间复杂度和密钥搜索阶段的时间复杂不变，而存储复杂度变为 $2^{203.5}$ AES 分组。

5.3　时空折中

利用文献[14]的时空折中方法，能平衡预计算的时间复杂度和密钥搜索阶段的时间复杂度：当预计算需要的计算量减少 n_1 倍，那么密钥搜索阶段的计算量增加 n_2 倍。若 $n_1, n_2 > 1$，且 n_1 相对大，那么对于正确密钥获得以上匹配的概率为 $1-(1-1/n_1)^{n_2} \approx 1-e^{-n_2/n_1}$。特别地，如果 $n_2 = 4n_1$，那么攻击成功的概率约为 98%。对 AES-192，基本的攻击是不可行的，但利用时空折中方法，当 $13.5 < n < 120.5$，使得攻击 7 轮 AES-192 变成可行(见表 1)。

6　攻击 8 轮 AES-256

攻击 8 轮 AES-256，需要在 7 轮攻击的基础上再猜测第 8 轮的 128bit 子密钥，数据复杂度，预计算时间复杂度和存储复杂度均不变，密钥搜索阶段

表 1　　**针对 AES 的中间相遇攻击结果比较**

分组密码	攻击类型	轮数	Data	Memory	Time	Pre.	文献
AES-128	MitM	7	2^{80}	2^{122}	2^{113}	2^{123}	[23]
AES-192	MitM	7	2^{80}	2^{122}	2^{113}	2^{123}	[23]
	MitM	7	2^{32}	2^{206}	2^{72}	2^{208}	[14]
	MitM-TM	7	2^{34+n}	2^{206-n}	2^{74+n}	2^{208-n}	[14]
	MitM	7	2^{32}	$2^{203.5}$	$2^{69.5}$	$2^{205.5}$	本文
	MitM-TM	7	2^{34+n}	$2^{203.5-n}$	$2^{71.5+n}$	$2^{205.5-n}$	本文
AES-256	MitM	7	2^{80}	2^{122}	2^{113}	2^{123}	[23]
	MitM	7	2^{32}	2^{206}	2^{272}	2^{208}	[14]
	MitM-TM	7	2^{34+n}	2^{206-n}	2^{74+n}	2^{208-n}	[14]
	MitM	8	2^{80}	2^{123}	2^{241}	2^{124}	[23]
	MitM	8	2^{32}	2^{206}	2^{200}	2^{208}	[14]
	MitM-TM	8	2^{34+n}	2^{206-n}	2^{202+n}	2^{208-n}	[14]
	MitM	8	2^{32}	$2^{203.5}$	$2^{197.5}$	$2^{205.5}$	本文
	MitM-TM	8	2^{34+n}	$2^{203.5-n}$	$2^{199.5+n}$	$2^{205.5-n}$	本文

注：Data 为数据复杂度；Time 为时间复杂度；Memory 为存贮复杂度；Pre 为预处理。存储的单位为 128bit 的分组；时间复杂度的单位为加密次数；MitM 表示中间相遇攻击；MitM-TM 表示中间相遇攻击的时空折中版本。特别地，如果预处理的计算量减少 2^n 倍，那么密钥搜索阶段的计算量增加 2^{n+2} 倍。

时间复杂度为 $2^{69.5+128}=2^{197.5}$AES 加密。采用时空折中方法[14]，平衡预处理和密钥搜索阶段的计算量。

7　结束语

分组密码及其工作模式[24]的安全受到广泛关注。本文分析了针对 AES 的中间相遇攻击。文献[14]首先提出了 AES 的 5 轮区分器，然后改进得到一种 5 轮区分器的变体降低攻击时间复杂度，该变体需要攻击者预计算阶段计算并存储差分值，密钥搜索阶段将相应部分加解密差分值与预计算阶段的差分值比较。本文利用 AES 密码算法轮变换的特点，构造了一个 AES 的 5 轮中间相遇攻击区分器的新变体。新变体无需攻击者计算、存储和比较差分值，不同的是密钥搜索阶段中比较匹配条件的变化，原来的比较要求两个串完全相同，新变体要求两个串逐字节差分相同。攻击过程中使用与文献[14]相比少量的数据量，基于区分器新变体和时空折中方法，针对 7 轮 AES-192 和 8 轮 AES-256 分别给出了新的攻击方法。从表 1 看出，与文献[14]中的攻击结果相比，新分析的预计算复杂度、时间复杂度和存储复杂度均降低。

参考文献：

[1] DAEMAN J, RIJMEN V. The design of Rijndael: AES: the Advanced Encryption Standard[M]. Berlin Heidelberg: Springer-Verlag, 2002.

[2] DAEMAN J, KNUDSEN L, RIJMEN V. The block cipher SQUARE[A]. FSE 1997[C].LNCS 1267, 1997. 149-165.

[3] FERGUSON N, KELSEY J,LUCKS S, *et al*. Improved cryptanalysis of Rijndael[A]. FSE 2000[C].LNCS 1978, 2002.213-230.

[4] LUCKS S. Attacking seven rounds of Rijndael under 192-bit and 256-bit keys[A]. The Third AES Candidate Conference 2000[C]. 2000.

[5] GILBERT H,MINIER M. A collision attack on 7 rounds of Rijndael[A]. The Third AES Candidate Conference 2000[C]. 2000.

[6] BIHAM E, KELLER N. Cryptanalysis of reduced variants of Rijndael[A]. The Third AES Candidate Conference 2000[C]. 2000.

[7] CHEON J, KIM M, KIM K, et al. Improved impossible differential cryptanalysis of Rijndael[A]. ICISC 2001[C]. LNCS 2288, 2002. 39-49.

[8] BAHRAK B. AREF M R. A novel impossible differential cryptanalysis of AES[A]. The Western European Workshop on Research in Cryptology 2007[C]. 2007.

[9] PHAN R C-W. Impossible differential cryptanalysis of 7-round advanced encryption standard AES[J]. Information Processing Letters, 2004, 91(1):33-38.

[10] ZHANG W, WU W, FENG D. New results on impossible differential cryptanalysis of reduced AES[A]. ICISC 2007[C]. LNCS 4817, 2007. 239-250.

[11] LU J, DUNKELMAN O, KELLER N, *et al*. New impossible differential attacks on AES[A]. INDOCRYT 2008[C]. LNCS 5365, 2008. 279-293.

[12] BIRYUKOV A. Boomerang attack on 5 and 6-round AES[A]. The Fourth Conference on Advanced Encryption Standard 2004[C]. 2004.

[13] COURTOIS N, PIEPRZYK J. Cryptanalysis of block ciphers with overdefined systems of equations[A]. ASIACRYPT 2002[C]. LNCS2501, 2002.267-287.

[14] DEMIRCI H, SELCUK A. A meet in the middle attack on 8-round AES[A]. FSE2008[C]. LNCS, 5086, 2008.116-126.

[15] DEMIRCI H, TASKM I, COBAN M, *et al*. Improved meet-in-the-middle attacks on AES[A]. INDOCRYPT 2009[C]. LNCS 5922, 2009.144-156.

[16] JAKIMOSKI G, DESMEDT Y. Related-key differential cryptanalysis of 192-bit key AES variants[A]. SAC 2003[C]. LNCS 3006, 2004. 208-221.

[17] BIHAM E, DUNKELMAN O, KELLER N. Related-key impossible differential attacks on AES-192[A]. CT- RSA 2006[C]. LNCS 3860, 2006. 21-31.

[18] ZHANG W, ZHANG L,WU W, *et al*. Improved related-key impossible differential attacks on reduced round AES-192[A].SAC 2006[C]. LNCS 4356, 2007.15-27.

[19] BIHAM E, DUNKELMAN O, KELLER N. Related-key and boomerang attacks[A].EUROCRYPT 2005[C]. LNCS 3494,2005.507-525.

[20] HONG S, KIM J,LEE S, et al. Related-key rectangle attacks on reduced versions of SHACAL-1 and AES- 192[A].FSE 2005[C]. LNCS 3557,2005.368-383.

[21] KIM J, HONG S, PRENEEL B. Related-key rectangle attacks on reduced AES-192 and AES-256[A]. FSE 2007[C]. LNCS4593, 2007.225-241.

[22] BIRYUKOV A, KHOVRATOVICH D. Related-key cryptanalysis of the full AES-192 and AES-256[A]. Cryptology-ASIACRYPT2009[C]. LNCS 5912, 2009. 1-18.

[23] BIRYUKOV A, KHOVRATOVICH D, NIKOLIC I. Distinguisher and related-key attack on the full AES-256 (extended version)[A]. CRYPTO 2009[C]. LNCS 5677, 2009.231-249.

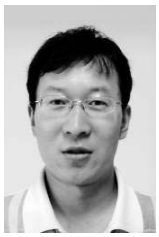
[24] 罗岚, 秦志光, 万国根等. 分组密码算法认证运算模式的注记及可证安全性[J]. 电子科技大学学报，2009,38(4):600-604.
LUO L, QIN Z G, WAN G G, *et al*. Note to the authentication operate modes of block cipher provable security[J]. Journal of University of Electronic Science and Technology of China, 2009,34(4):600-604.

作者简介：

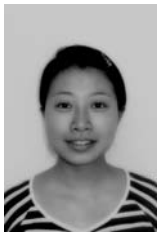
董晓丽（1982-），女，山西阳曲人，西安电子科技大学博士生，主要研究方向为密码学与信息安全。

胡予濮（1955-），男，河南濮阳人，西安电子科技大学教授、博士生导师，主要研究方向为密码学与信息安全。

陈杰（1979-），女，湖南澧县人，西安电子科技大学副教授、硕士生导师，主要研究方向为密码学与信息安全。



李顺波（1979-），男，陕西周至人，西安电子科技大学博士生，西安建筑科技大学讲师，主要研究方向为密码学与信息安全。



杨旸（1984-），女，湖北随州人，西安电子科技大学博士生，主要研究方向为密码学与信息安全。