doi:10.3969/j.issn.1000-436x.2014.02.023

对轻量级密码算法 MIBS 的相关密钥不可能差分攻击

陈平，廖福成，卫宏儒
(北京科技大学 数理学院，北京 100083)

摘 要：研究了轻量级分组密码算法 MIBS 抵抗相关密钥不可能差分的能力。利用 MIBS-80 密钥编排算法的性质，给出了一个密钥差分特征，并结合特殊明密文对的选取，构造了一个 10 轮不可能差分。在此不可能差分特征上进行扩展，对 14 轮的 MIBS-80 进行了攻击，并给出了复杂度分析。此攻击的结果需要的数据复杂度为 2^{54} 和时间复杂度为 2^{56}。

关键词：轻量级分组密码；MIBS 算法；相关密钥；不可能差分攻击
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)02-0190-04

Related-key impossible differential attack on a lightweight block cipher MIBS

CHEN Ping, LIAO Fu-cheng, WEI Hong-ru
(School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 100083, China)

Abstract: The strength of MIBS algorithm against the related-key impossible differential attack was examined. MIBS is a lightweight block cipher algorithm. By using the key-expanding properties of MIBS-80 algorithm, a related-key differential feature was presented and a 10-round impossible differential method was constructed by combining special cipher-plaintexts. Based on the impossible differential method, an attack to 14-round MIBS-80 algorithm was given, and the attack complexity both on data and on time were gained. Analysis results indicate the attack to MIBS of 14 rounds MIBS-80 algorithm needs 2^{54} chosen plaintext operations and 2^{56} encrypting computations.

Key words: lightweight block cipher; MIBS algorithm; related-key; impossible differential attack

1 引言

为了能够应用在 RFID (radio frequency identification)、无线传感技术等设备资源和计算能力有限的环境中，轻量级分组密码的设计与研究越来越受密码分析者的关注。MIBS[1]是在 2009 年提出的一个轻量级分组密码算法，它的资源占用量较少，可以很好地适用于资源受限的微型计算设备。此算法自提出到目前已有不少分析：文献[2]给出了对 MIBS-64 的 13 轮的差分分析；文献[3]对 MIBS 进行了 18 轮的线性分析和 14 轮的差分分析，此外还完成了 12 轮的不可能差分分析；文献[4]指出了文献[3]中对 MIBS 进行不可能差分分析的错误，并提出了新的不可能差分分析；文献[5]给出了对 MIBS 的 4、5 轮积分区分器，并利用该区分器对此算法进行了 8 轮和 9 轮的 Integral 攻击；此外，文献[6]利用等价结构的思想对 MIBS 进行了 8~11 轮的中间相遇攻击。

相关密钥不可能差分分析是把相关密钥分析[7,8]和不可能差分分析[9]结合起来的一种分析方法。与不可能差分分析相比，它最大优点就是利用了密钥扩展算法的结构，通过找到不同轮数间密钥的相关关系对明密文对差分的影响得到不可能差分路径。这种攻击方法已经应用在了 AES[10,11]，LBLOCK[12]

收稿日期：2013-05-19；**修回日期**：2013-12-06
基金项目：国家自然科学基金资助项目(61174209, 61272476)；内蒙古自治区科技创新引导奖励基金资助项目(2012)
Foundation Items: The National Natural Science Foundation of China(61174209, 61272476); The Oriented Award Foundation for Science and Technological Innovation, Inner Mongolia Autonomous Region(2012)

等分组密码算法中。本文将利用相关密钥与不可能差分相结合的方法，首次对 MIBS-80 进行相关密钥不可能差分攻击。

2　MIBS 分组密码算法描述

MIBS 是一种 Feistel 型结构的分组密码算法，分组长度是 64 bit，支持长度为 64 bit 和 80 bit 的密钥，加密轮数为 32 轮。对于密钥长度为 64 bit 和 80 bit 的加密过程是一样的，只是密钥生成算法有所不同。由于本文只对 MIBS-80 进行分析，因而在下面只介绍 MIBS-80 的密钥编排算法。

2.1　加密过程

设 64 bit 的输入明文 $P_0 = L_0 \| R_0$，$L_0, R_0 \in Z_2^{32}$，$k_i \in Z_2^{32} (1 \leqslant i \leqslant 32)$ 是第 i 轮的轮密钥，MIBS 的加密迭代过程如下。

1) 输入明文 (L_0, R_0)，且以 4 bit 为一个单位，称为半字节 (nibble)。其中，记 $L_0 = (X_{0,8}, X_{0,7}, X_{0,6}, X_{0,5}, X_{0,4}, X_{0,3}, X_{0,2}, X_{0,1}), X_{0,j} \in Z_2^4 (1 \leqslant j \leqslant 8)$。

2) 对 $i = 1:32$，$L_i = F(L_{i-1}, K_i) \oplus R_{i-1}$，$R_i = L_{i-1}$。轮函数 $F(L_{i-1}, K_i)$ 包括轮密钥加、S 盒变换、混合层及 P 置换。其中，S 是 4×4 的非线性 S 盒，混合层为线性变换，P 置换为顺序的置换，混合层和 P 置换可以描述为线性变换 L [5]：$(Y_{i,8}, Y_{i,7}, \cdots, Y_{i,1}) = L(X_{i,8}, X_{i,7}, \cdots, X_{i,1})$，其中，

$$
\begin{aligned}
&Y_{i,1} = X_{i,1} \oplus X_{i,2} \oplus X_{i,4} \oplus X_{i,5} \oplus X_{i,7} \oplus X_{i,8},\\
&Y_{i,2} = X_{i,2} \oplus X_{i,3} \oplus X_{i,4} \oplus X_{i,5} \oplus X_{i,6} \oplus X_{i,7},\\
&Y_{i,3} = X_{i,1} \oplus X_{i,2} \oplus X_{i,3} \oplus X_{i,5} \oplus X_{i,6} \oplus X_{i,8},\\
&Y_{i,4} = X_{i,2} \oplus X_{i,3} \oplus X_{i,4} \oplus X_{i,7} \oplus X_{i,8},\\
&Y_{i,5} = X_{i,1} \oplus X_{i,3} \oplus X_{i,4} \oplus X_{i,5} \oplus X_{i,8},\\
&Y_{i,6} = X_{i,1} \oplus X_{i,2} \oplus X_{i,4} \oplus X_{i,5} \oplus X_{i,6},\\
&Y_{i,7} = X_{i,1} \oplus X_{i,2} \oplus X_{i,3} \oplus X_{i,6} \oplus X_{i,7},\\
&Y_{i,8} = X_{i,1} \oplus X_{i,3} \oplus X_{i,4} \oplus X_{i,6} \oplus X_{i,7} \oplus X_{i,8}
\end{aligned}
$$

而线性变换 L 是可逆的，其逆 L^{-1} 表示为 $(X_{i,8}, X_{i,7}, \cdots, X_{i,1}) = L^{-1}(Y_{i,8}, Y_{i,7}, \cdots, Y_{i,1})$，其中，

$$
\begin{aligned}
&X_{i,1} = Y_{i,2} \oplus Y_{i,4} \oplus Y_{i,6} \oplus Y_{i,7} \oplus Y_{i,8},\\
&X_{i,2} = Y_{i,1} \oplus Y_{i,4} \oplus Y_{i,5} \oplus Y_{i,7} \oplus Y_{i,8},\\
&X_{i,3} = Y_{i,1} \oplus Y_{i,3} \oplus Y_{i,4} \oplus Y_{i,5} \oplus Y_{i,6},\\
&X_{i,4} = Y_{i,2} \oplus Y_{i,3} \oplus Y_{i,5} \oplus Y_{i,6} \oplus Y_{i,7},\\
&X_{i,5} = Y_{i,1} \oplus Y_{i,3} \oplus Y_{i,4} \oplus Y_{i,5} \oplus Y_{i,7} \oplus Y_{i,8},\\
&X_{i,6} = Y_{i,1} \oplus Y_{i,2} \oplus Y_{i,4} \oplus Y_{i,5} \oplus Y_{i,6} \oplus Y_{i,8},\\
&X_{i,7} = Y_{i,1} \oplus Y_{i,3} \oplus Y_{i,5} \oplus Y_{i,6} \oplus Y_{i,7} \oplus Y_{i,8},\\
&X_{i,8} = Y_{i,1} \oplus Y_{i,2} \oplus Y_{i,3} \oplus Y_{i,4} \oplus Y_{i,6} \oplus Y_{i,7}
\end{aligned}
$$

3) 输出密文 $C_i = (L_i, R_i), 1 \leqslant i \leqslant 32$。

2.2　MIBS-80 密钥扩展算法

设长度为 80 bit 的主密钥为 $\tilde{K} = (\tilde{K}_{79}, \tilde{K}_{78}, \cdots, \tilde{K}_0)$，由主密钥生成 32 个 32 bit 的轮密钥 $k_i (1 \leqslant i \leqslant 32)$ 的过程如下。

$\text{state}^i \leftarrow \tilde{K}$，对 $i = 1, 2, \cdots, 32$，

1) $\text{state}^i = \text{state}^i >>> 19$；

2) $\text{state}^i = S(\text{state}^i_{[79:76]}) \| S(\text{state}^i_{[75:72]}) \| \text{state}^i_{[71:0]}$；

3) $\text{state}^i = (\text{state}^i_{[79:19]}) \| (\text{state}^i_{[18:14]}) \oplus \text{Round\_counter} \| \text{state}^i_{[13:0]}$；

4) $k_i = \text{state}^i_{[79:48]}$。

2.3　轮密钥的相关性质

类似文献[4]的做法，由 MIBS-80 密钥生成算法易知轮密钥有如下性质。

性质 1　为了计算轮密钥 k_1，仅需知道 $\tilde{K}_{[18:0]}$ 和 $\tilde{K}_{[79:67]}$，记作 $\tilde{K}_{[18:0]} \| \tilde{K}_{[79:67]} \Rightarrow k_1$，同样地，可得到 $\tilde{K}_{[25:0]} \| \tilde{K}_{[79:74]} \Rightarrow k_{14}$，$\tilde{K}_{[58:55]} \Rightarrow k_{13,4}$，$\tilde{K}_{[21:18]} \Rightarrow k_{2,4}$。其中，方括号中的数字代表半字节中比特位。

3　对 14 轮的 MIBS 的相关密钥不可能差分分析

本节给出 MIBS 的 10 轮相关密钥不可能差分路径，并在这一路径前面加 2 轮，后面加 2 轮，以构成对 MIBS 的 14 轮攻击。

3.1　相关密钥不可能差分路径

由 MIBS-80 的密钥扩展算法分析知，MIBS 的轮密钥是由初始密钥经过行移位、S 盒变换、异或轮常数得到的。从差分角度看，行移位影响的是活跃 S 盒的位置，第 2 步的最左端两半字节的 S 盒变换影响其个数，而密钥扩展算法的一个差分 2 次经过 S 盒的轮数间隔较大，这样活跃 S 盒的增长个数较慢。考虑到此性质，为使密钥差分链的轮数尽量多，选取初始主密钥差分为 $\Delta\tilde{K} = (00000000000000080000)$，$\Delta k_i (1 \leqslant i \leqslant 10)$ 的变化如下：(00000000)，(00002000)，(00000000)，(00000000)，(00000000)，(00020000)，(00000000)，(00000000)，(00000000)，(00200000)。

选取明文输入差分形式为(00000000,00002000)时，根据加密算法迭代 6 轮的差分变化如表 1 所示。

表 1 加密时的相关密钥差分特征

轮数 (i)	ΔL_{i-1}	ΔR_{i-1}	Δk_i
1	00000000	00002000	00000000
2	00002000	00000000	00002000
3	00000000	00002000	00000000
4	00002000	00000000	00000000
5	$t0tt0tt$	00002000	00000000
6	$(c_8c_7c_6c_5c_4c_3c_2c_1)\oplus$ (00002000)	$t0tt0tt$	0002000

选取 10 轮加密后的密文差分形式为(00000000, 0020000)时，进行 5 轮解密，其差分变化如表 2 所示。

表 2 解密时的相关密钥差分特征

轮数 / i	ΔL_i	ΔR_i	Δk_i
10	00000000	00200000	00200000
9	00200000	00000000	00000000
8	00000000	00200000	00000000
7	00200000	$www00ww0$	00000000
6	$www00ww0$	ΔR_6	00020000

其中，$c_i(1\leqslant i\leqslant 8)$, t, w 均为 4 bit 未知非零值。

由表 1 和表 2 知，从加密方向看，$\Delta R_6=\Delta L_5=(c_8c_7c_6c_5c_4c_3c_2c_1)\oplus(00002000)$，结合解密方向看，$\Delta R_6\oplus\Delta L_7=(c_8c_7c_6c_5c_4c_3c_2c_1)\oplus(02002000)$，从而 $L^{-1}(\Delta R_6\oplus\Delta L_7)=(t_80t_6t_5t_40t_2t_1)\oplus(02022020)=(t_8\ 2t_6\ ??0?t_1)$，与单从第 7 轮加密 ΔL_6 经过轮密钥加和 S 盒后的 $(w_8w_7w_600w_3w_20)$ 矛盾($t_i(i=1,2,4,5,6,8)$, $w_i(i=2,3,6,7,8)$ 均为 4 bit 未知非零值)。所以，构成不可能差分

$$(00000000,00002000)\xrightarrow[10r]{\Delta\tilde{K}=(0000000000000080000)}(00000000,00200000)$$

3.2 对 14 轮的 MIBS 的相关密钥不可能差分攻击

在这个 10 轮不可能差分前面添加 2 轮，后面加 2 轮，构成对 MIBS 的 14 轮相关密钥不可能差分。此时，需要将 $\Delta\tilde{K}$ 逆推 2 轮，得到当 $\Delta\tilde{K}=(0000020000000000000)$，经过密钥扩展算法的 2 轮迭代，即满足 3.1 节中的 10 轮不可能差分的密钥输入差分形式。同时，选取明文对差分为如下形式 $(\Delta L_0,\Delta R_0)=((g0gg,g0gg),L(y_80y_6y_5,y_40y_2y_1)\oplus(0000,2000))$，经过 2 轮加密算法的迭代，得到满足 10 轮不可能差分的明文对输入差分形式，则 MIBS 的 14 轮不可能差分如图 1 所示，其中，?代表 4 bit 不确定的任意值。

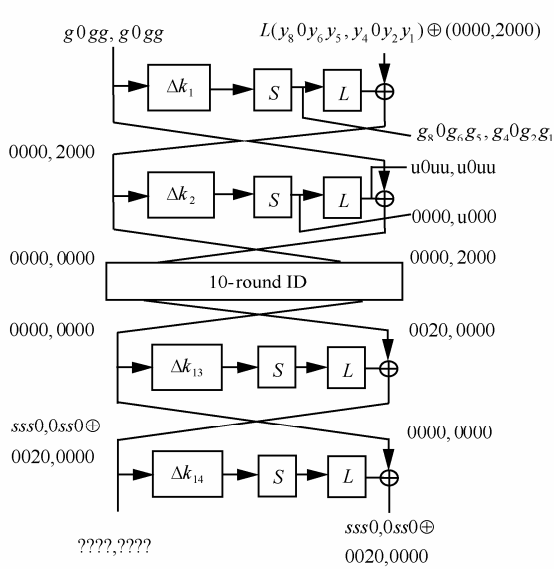

图 1 MIBS 的 14 轮不可能差分

根据这个性质，可以对 14 轮 MIBS 算法进行攻击。步骤如下。

1) 选择 2^{28} 个明文来构造一个结构，其中，$g,y_i(i=1,2,4,5,6,8)\in Z_2^4$，其余位置取常数，每个结构大约形成 2^{55} 个明文对满足如下输入差分

$$(\Delta L_0,\Delta R_0)=((g0gg,g0gg),\ L(y_80y_6y_5,y_40y_2y_1)\oplus(0000,2000))$$

选择 2^m 个这样的结构，则可以构成 2^{m+55} 个明密文对。

2) 选择密文差分满足形式 $(\Delta L_{14},\Delta R_{14})=((????,????),(sss0,0ss0)\oplus(0020,0000))$，其中，$\Delta L_{14}$ 可以通过 $\Delta L_{14}\oplus(0020,0000)=(sss0,0ss0)$ 来筛选，s 是未知非零值，?为不确定的任意值，则满足差分的概率为 2^{-28}，将满足条件的对保留，则剩下 2^{m+27} 对。

3) 猜测 32 bit 的 14 轮密钥 k_{14}，对于保留下来的每个对，进行 14 轮的解密运算，来筛选错误密钥。依次猜测 k_{14} 的各个半字节密钥，分别计算 $S(R_{14,i}\oplus k_{14,i})\oplus S(R'_{14,i}\oplus k_{14,i})=L^{-1}(L_{14}\oplus L'_{14})_{[i]}$，$1\leqslant i\leqslant 8$，满足条件的概率为 2^{-32}，则剩下 2^{m-5} 对。其中，方括号中的数字代表半字节的位置。

4) 猜测 $k_{13,4}$，进行 13 轮的解密运算，筛选错误密钥。注意到存在密钥差分 $\Delta k_{13,4}=4$，保留满足 $S(R_{13,4}\oplus k_{13,4})\oplus S(R'_{13,4}\oplus k_{13,4}\oplus 4)=L^{-1}(\Delta R_{14}\oplus(00200000))_{[4]}$ 的对，所以还剩有 2^{m-9} 组候选对。

5) 猜测第 1 轮的 32 bit 轮密钥，由 2.3 节中找到的轮密钥相关性质，容易得到 $k_{1,2[3]}$、$k_{1,3}$、$k_{1,4}$、$k_{1,5}$、$k_{1,6}$、$k_{1,7}$、$k_{1,8}$，故只需猜 $k_{1,1}, k_{1,2[2,1,0]}$ 这 7 bit 密钥。

由于有 $L^{-1}(\Delta R_0 \oplus \Delta L_1) = L^{-1}(\Delta R_0) \oplus L^{-1}(0000,2000) = L^{-1}(\Delta R_0) \oplus L^{-1}(0222,2220)$，那么 8 个半字节都只是由 $L^{-1}(\Delta R_0)$ 确定。那么，对剩下的对，先猜测 $k_{1,1}$，计算保留满足 $S(L_{0,1} \oplus k_{1,1}) \oplus S(L'_{0,1} \oplus k_{1,1}) = L^{-1}(\Delta R_0)_{[1]}$ 的对，再猜测 $k_{1,2[2,1,0]}$，保留满足 $S(L_{0,2} \oplus k_{1,2}) \oplus S(L'_{0,2} \oplus k_{1,2}) = L^{-1}(\Delta R_0)_{[2]} \oplus 2$ 的对，此时，还剩下 2^{m-17} 对。

6) 猜测第 2 轮的 $k_{2,4}$，根据轮密钥相关性质容易得到，故无需猜测。对剩余对，计算 $S(L_{1,4} \oplus k_{2,4}) \oplus S(L'_{1,4} \oplus 2 \oplus k_{2,4})$，并判断其值是否等于 $L^{-1}(\Delta L_0)_{[4]}$，如果成立，则表明这一密钥猜测满足了相关密钥不可能差分路线，从而是错误密钥，将其舍去。

分析了 2^{m-17} 个明密文对后，此时还剩下错误密钥的个数为 $n = 2^{32} \times 2^4 \times 2^7 \times (1-2^{-4})^{2^{m-17}}$，令 $n<1$，则无错误密钥剩余，此时求得 $m = 26$。

3.3 复杂度分析

统计以上攻击过程各步的 14 轮加密运算次数，利用复杂度计算的一般表达式为

$$\frac{\text{需要运算的}S\text{盒的个数}}{\text{加/解密一次运算中包含的}S\text{盒的个数}} \times \frac{1}{\text{轮数}} \times \text{对剩余候选密钥对猜测密钥量发生的复杂度}$$

得到第 3)步需要 $2 \times \frac{1}{8} \times \frac{1}{14} \times \sum_{i=0}^{7} (2^{m+27-4i} \times 2^{4+4i}) \approx 2^{m+25.2}$ 次；第 4)步需要 $2 \times \frac{1}{8} \times \frac{1}{14} \times 2^{32} \times 2^{m-5} \times 2^4 = 2^{m+25.2}$ 次，第 5)步需要 $2 \times \frac{1}{8} \times \frac{1}{14} \times 2^{32} \times 2^4 \times (2^{m-9} \times 2^4 + 2^{m-13} \times 2^7) = 2^{m+26.8}$ 次，第 6)步需要 $2 \times \frac{1}{8} \times \frac{1}{14} \times 2^{32} \times 2^4 \times 2^7 \times 2^{m-17} \approx 2^{m+20.2}$。取 $m = 26$，所以，总的时间复杂度为 2^{56} 次 14 轮加密运算。

经上所述，时间复杂度为 2^{56}，明文量为 2^{54}。

4 结束语

本文根据 MIBS-80 的密钥扩展算法的性质，结合不可能差分，构造了一个 10 轮相关密钥不可能差分路径，并将此不可能差分进行扩展，对 14 轮的 MIBS 进行了相关密钥不可能差分攻击。表 3 给出了本文方法与以往攻击结果的对比，和以往结果相比，较文献[3]和文献[4]的不可能差分攻击轮数增加，恢复 72 bit 的轮密钥只需猜测 43 bit 的主密钥，攻击的数据复杂度为 2^{54} 和时间复杂度为 2^{56}。

表 3　MIBS-80 的攻击结果比较

攻击方法	轮数	数据复杂度	时间复杂度	预计算复杂度	文献
Integral	9	$2^{39.6}$	$2^{68.4}$	—	[5]
中间相遇	11	$2^{24.9}$	$2^{66.25}$	$2^{51.03}$	[6]
差分	13	2^{62}	2^{25}	—	[2]
不可能差分	12	2^{62}	$2^{46.42}$	—	[3]
不可能差分	12	2^{59}	2^{63}	—	[4]
相关密钥不可能差分攻击	14	2^{54}	2^{56}	—	本文

参考文献：

[1] IZADI M, SADEGHIYAN B, SADEGHIAN S S. MIBS: a new lightweight block cipher[A]. CANS 2009[C]. Berlin: Springer, 2009. 334-348.

[2] 杨林, 王美琴. 约简轮的 MIBS 算法的差分分析[J]. 山东大学学报(理学版), 2010, 45(4):12-15.
YANG L, WANG M Q. Differential cryptanalysis of reduced-round MIBS[J]. Journal of Shandong University(Natural Science), 2010, 45(4):12-15.

[3] BAY A, NAKAHARA J J, VAUDENAY S. Cryptanalysis of reduced-round MIBS block cipher[A]. CANS 2010[C]. Berlin: Springer, 2010. 1-19.

[4] 杜承航, 陈佳哲. 轻量级分组密码算法 MIBS 不可能差分分析[J]. 山东大学学报(理学版), 2012, 47(7):55-58.
DU C H, CHEN J Z. Impossible differential cryptanalysis of reduced-round MIBS[J]. Journal of Shandong University(Natural Science), 2012, 47(7):55-58.

[5] 王高丽, 王少辉. 对 MIBS 算法的 Integral 攻击[J]. 小型微型计算机系统, 2012, 33(4):773-777.
WANG G L, WANG S H. Integral cryptanalysis of reduced-round MIBS block ciphe[J]. Journal of Chinese Computer Systems, 2012, 33(4):773-777.

[6] 刘超, 廖福成, 卫宏儒. 对 MIBS 算法的中间相遇攻击[J]. 内蒙古大学学报(自然科学版), 2013, 44(3):308-315.
LIU C, LIAO F C, WEI H R. Meet-in-the-middle attacks on MIBS[J]. Journal of Inner Mongolia University(Natural Science Edition), 2013, 44(3):308-315.

[7] KNUDSEN L R. Cryptanalysis of LOKI91[A]. Advances in Cryptology-Auscrypt 1992[C]. Gold Coast, Australia, 1992.196-208.

[8] BIHAM E. New types of cryptanalytic attacks using related keys[J]. Journal of Cryptology, 1994, 7(4):229-246.

[9] BIHAM E, BIRYUKOV A, SHAMIR A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials[A]. Advances in Cryptology-Eurocrypt 1999[C]. Berlin: Springer-Verlag, 1999. 12-23.

[10] BIHAM E, DUNKELMAN O, KELLER N. Related-key impossible differential attacks on 8-round AES-192[A]. CT-RSA 2006[C]. Berlin: Springer-Verlag, 2006.21-33.

[11] ZHANG W T, WU W L, ZHANG L. Related-key impossible differential

（下转第 201 页）

LI W G, YI K C, LIU Z J, *et al*. Improved beamforming algorithm of multi-user system[J]. Journal on Communications, 2009, 30(12): 79-84.

[10] SHEN H, XU W, ZHAO C. Efficient joint transmit and receive optimization for multiuser MIMO systems[A]. Wireless Communications and Networking Conference(WCNC)[C]. Shanghai, 2012.125-130.

[11] CHANG J H, TASSIYLAS L, RASHID-FARROKHI F. Joint transmitter receiver diversity for efficient space division multiaccess[J]. IEEE Trans Wireless Communications, 2002, 1(1):16-27.

[12] CHRISTENSEN S S, AGARWAL R, CARCALHO E D, *et al*. Weighted sum-rate maximization using weighted MMSE for MIMO-BC beamforming design[J]. IEEE Trans Wireless Communications, 2008, 7(12): 4792-4799.

[13] NEGRO F, SHENOY S P , GHAURI I, *et al*. Weighted sum rate maximization in the MIMO interference channel[A]. 2010 IEEE 21st International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)[C]. Instanbul, 2010.684-689.

[14] SHI Q, RAZAVIYAYN M, LUO Z Q, *et al*. An iteratively weighted MMSE approach to distributed sum-utility maximization for a MIMO interfering broadcast channel[J]. IEEE Trans on Signal Processing, 2011, 59(9): 4331-4340.

[15] ZHANG J, HEATH R W, KOUNTOURIS M, *et al*. Mode switching for the multi-antenna broadcast channel based on delay and channel quantization[J]. EURASIP Journal on Advances in Signal Processing, 2009, 2009:1-15.

作者简介：

黄莹（1989-），女，陕西西安人，西安交通大学硕士生，主要研究方向为下一代移动通信中的协作多点传输技术。

吕刚明（1980-），男，湖北襄阳人，博士，西安交通大学讲师、硕士生导师，主要研究方向为下一代移动通信传输与无线资源管理关键技术。

朱世华（1950-），男，浙江义乌人，西安交通大学教授、博士生导师，主要研究方向为多输入多输出（MIMO）系统、CDMA 系统多用户检测、数字传输与编码和交换与通信。

（上接第 193 页）

attacks on reduced-round AES-256[J]. Journal of Software, 2007, 18(11): 2893-2901.

[12] 詹英杰, 关杰, 丁林. 对简化版 LBLock 算法的相关密钥不可能差分攻击[J]. 电子与信息学报, 2012, 34(9):2161-2166.
ZHAN Y J, GUAN J, DING L. Related-key impossible differential attacks on reduced round LBLOCK[J]. Journal of Electronics & Information Technology, 2012, 34(9):2161-2166.

廖福成[通信作者]（1957-），男，陕西勉县人，北京科技大学教授、博士生导师，主要研究方向为控制理论与应用。E-mail: fcliao@ustb.edu.cn。

作者简介：

陈平（1987-），女，河北石家庄人，北京科技大学硕士生，主要研究方向为密码学。

卫宏儒（1963-），男，陕西扶风人，北京科技大学副教授，主要研究方向为数学、信息安全与密码学、物联网关键技术。