1. 17轮的LBLOCK相关密钥不可能差分

| left | right | subkey |
| --- | --- | --- |
| 0000 0000 0000 0000 0000 0000 0000 0000 | 0000 0000 0000 0000 0000 0011 0000 0000 | 00000000 |
| 0000 0000 0000 0011 0000 0000 0000 0000 | 0000 0000 0000 0000 0000 0000 0000 0000 | 00030000 |
| 0000 0000 0000 0000 0000 0000 0000 0000 | 0000 0000 0000 0011 0000 0000 0000 0000 | 00000000 |
| 0000 0011 0000 0000 0000 0000 0000 0000 | 0000 0000 0000 0000 0000 0000 0000 0000 | 00000000 |
| ??01 0000 0000 0000 0000 0000 0000 0000 | 0000 0011 0000 0000 0000 0000 0000 0000 | 01800000 |
| ??1? 0000 ???? ?1?? 0000 0000 0000 0011 | ??01 0000 0000 0000 0000 0000 0000 0000 | 00000000 |
| 0000 ???? ???? ???? 0000 ??10 ??01 0000 | ??1? 0000 ???? ?1?? 0000 0000 0000 0011 | 00000006 |
| ???? ???? 0000 ???? ???? ???? ??1? ???? | 0000 ???? ???? ???? 0000 ??10 ??01 0000 | 30000000 |
| ???? ???? ???? ??10 ???? ???? ???? ???? | ???? ???? 0000 ???? ???? ???? ??1? ???? | 00000000 |
| ???? ???? ???? ???? ???? ???? ???? ???? | ???? ???? ???? ??10 ???? ???? ???? ???? |  |
| ???? 0000 ???? 0000 ???? ???? ???? 0000 | ???? ???? ???? ??01 ???? ???? ???? 0000 |  |
| ???? ??01 ?1?0 0000 ???? 0000 0000 0000 | ???? 0000 ???? 0000 ???? ???? ???? 0000 | 000000c0 |
| ???? 0000 0000 0000 ???? 0000 0011 0000 | ???? ??01 ?1?0 0000 ???? 0000 0000 0000 | 00000000 |
| ?1?0 0000 0000 0000 0000 0000 0000 0000 | ???? 0000 0000 0000 ???? 0000 0011 0000 | 00000000 |
| 0000 0000 0000 0000 0011 0000 0000 0000 | ?1?0 0000 0000 0000 0000 0000 0000 0000 | 00006000 |
| 0000 0000 0000 0000 0000 0000 0000 0000 | 0000 0000 0000 0000 0011 0000 0000 0000 | 00000000 |
| 0000 0000 0011 0000 0000 0000 0000 0000 | 0000 0000 0000 0000 0000 0000 0000 0000 | 00000000 |
| 0000 0000 0000 0000 0000 0000 0000 0000 | 0000 0000 0011 0000 0000 0000 0000 0000 | 00300000 |
| 0011 0000 0000 0000 0000 0000 0000 0000 | 0000 0000 0000 0000 0000 0000 0000 0000 | 00000000 |