# KASUMI

November 10, 2022

| Round | $KL_{i,1}$ | $KL_{i,2}$ | $KO_{i,1}$ | $KO_{i,2}$ | $KO_{i,3}$ | $KI_{i,1}$ | $KI_{i,2}$ | $KI_{i,3}$ |
|---|---|---|---|---|---|---|---|---|
| 1 | $K_1 \lll 1$ | $K'_3$ | $K_2 \lll 5$ | $K_2 \lll 8$ | $K_3 \lll 13$ | $K'_1$ | $K'_4$ | $K'_8$ |
| 2 | $K_2 \lll 1$ | $K'_4$ | $K_3 \lll 5$ | $K_3 \lll 8$ | $K_4 \lll 13$ | $K'_2$ | $K'_1$ | $K'_1$ |
| 3 | $K_3 \lll 1$ | $K'_1$ | $K_4 \lll 5$ | $K_4 \lll 8$ | $K_1 \lll 13$ | $K'_3$ | $K'_2$ | $K'_2$ |
| 4 | $K_4 \lll 1$ | $K'_2$ | $K_1 \lll 5$ | $K_1 \lll 8$ | $K_2 \lll 13$ | $K'_4$ | $K'_3$ | $K'_3$ |
| 5 | $K_1 \lll 1$ | $K'_3$ | $K_2 \lll 5$ | $K_2 \lll 8$ | $K_3 \lll 13$ | $K'_1$ | $K'_4$ | $K'_4$ |
| 6 | $K_2 \lll 1$ | $K'_4$ | $K_3 \lll 5$ | $K_3 \lll 8$ | $K_4 \lll 13$ | $K'_2$ | $K'_5$ | $K'_5$ |
| 7 | $K_3 \lll 1$ | $K'_1$ | $K_4 \lll 5$ | $K_4 \lll 8$ | $K_1 \lll 13$ | $K'_3$ | $K'_6$ | $K'_6$ |
| 8 | $K_4 \lll 1$ | $K'_2$ | $K_1 \lll 5$ | $K_1 \lll 8$ | $K_2 \lll 13$ | $K'_4$ | $K'_7$ | $K'_7$ |

Table 1: Round subkeys