A.2 Dependency of Subtweakeys

Let K_i $(0 \le i < 384)$ denote the master key bits. Suppose TK^1 takes $K_0 \sim K_{127}$, TK^2 takes $K_{128} \sim K_{255}$, and TK^3 takes $K_{256} \sim K_{383}$, respectively.

If $STK_r[i_r] = LFSR_2^r(TK^2[i]) \oplus LFSR_3^r(TK^3[i])$ and let $i = 0$, we have

$$
\begin{aligned}
STK_0[0][0] &= K_{128} + K_{256},\\
STK_0[0][1] &= K_{129} + K_{257},\\
STK_0[0][2] &= K_{130} + K_{258},\\
STK_0[0][3] &= K_{131} + K_{259},\\
STK_0[0][4] &= K_{132} + K_{260},\\
STK_0[0][5] &= K_{133} + K_{261},\\
STK_0[0][6] &= K_{134} + K_{262},\\
STK_0[0][7] &= K_{135} + K_{263},\\
STK_{15}[1][0] &= K_{129} + K_{131} + K_{133} + K_{257} + K_{259} + K_{261},\\
STK_{15}[1][1] &= K_{130} + K_{132} + K_{134} + K_{258} + K_{260} + K_{262},\\
STK_{15}[1][2] &= K_{131} + K_{133} + K_{135} + K_{259} + K_{261} + K_{263},\\
STK_{15}[1][3] &= K_{128} + K_{132} + K_{256} + K_{260},\\
STK_{15}[1][4] &= K_{129} + K_{133} + K_{257} + K_{261},\\
STK_{15}[1][5] &= K_{130} + K_{134} + K_{258} + K_{262},\\
STK_{15}[1][6] &= K_{131} + K_{135} + K_{259} + K_{263},\\
STK_{15}[1][7] &= K_{128} + K_{132} + K_{134} + K_{256} + K_{260} + K_{262}.
\end{aligned}
$$

It is easy to see that $STK_{15}[1]$ can be derived from $STK_0[0]$. Specifically,

$$
\begin{aligned}
STK_{15}[1][0] &= STK_0[0][1] + STK_0[0][3] + STK_0[0][5],\\
STK_{15}[1][1] &= STK_0[0][2] + STK_0[0][4] + STK_0[0][6],\\
STK_{15}[1][2] &= STK_0[0][3] + STK_0[0][5] + STK_0[0][7],\\
STK_{15}[1][3] &= STK_0[0][0] + STK_0[0][4],\\
STK_{15}[1][4] &= STK_0[0][1] + STK_0[0][5],\\
STK_{15}[1][5] &= STK_0[0][2] + STK_0[0][6],\\
STK_{15}[1][6] &= STK_0[0][3] + STK_0[0][7],\\
STK_{15}[1][7] &= STK_0[0][0] + STK_0[0][4] + STK_0[0][6].
\end{aligned}
$$

If $STK_r[i_r] = TK^1[i] \oplus LFSR_2^r(TK^2[i]) \oplus LFSR_3^r(TK^3[i])$ and let $i = 0$, we have

$$
\begin{aligned}
STK_0[0][0] &= K_0 + K_{128} + K_{256},\\
STK_0[0][1] &= K_1 + K_{129} + K_{257},\\
STK_0[0][2] &= K_2 + K_{130} + K_{258},\\
STK_0[0][3] &= K_3 + K_{131} + K_{259},\\
STK_0[0][4] &= K_4 + K_{132} + K_{260},\\
STK_0[0][5] &= K_5 + K_{133} + K_{261},\\
STK_0[0][6] &= K_6 + K_{134} + K_{262},\\
STK_0[0][7] &= K_7 + K_{135} + K_{263},\\
STK_{15}[1][0] &= K_0 + K_{129} + K_{131} + K_{133} + K_{257} + K_{259} + K_{261},\\
STK_{15}[1][1] &= K_1 + K_{130} + K_{132} + K_{134} + K_{258} + K_{260} + K_{262},\\
STK_{15}[1][2] &= K_2 + K_{131} + K_{133} + K_{135} + K_{259} + K_{261} + K_{263},\\
STK_{15}[1][3] &= K_3 + K_{128} + K_{132} + K_{256} + K_{260},\\
STK_{15}[1][4] &= K_4 + K_{129} + K_{133} + K_{257} + K_{261},\\
STK_{15}[1][5] &= K_5 + K_{130} + K_{134} + K_{258} + K_{262},\\
STK_{15}[1][6] &= K_6 + K_{131} + K_{135} + K_{259} + K_{263},\\
STK_{15}[1][7] &= K_7 + K_{128} + K_{132} + K_{134} + K_{256} + K_{260} + K_{262}.
\end{aligned}
$$

Among them, there are four dependent linear relations as follows.

$$
\begin{aligned}
STK_{15}[1][4] = {} & STK_0[0][0] + STK_0[0][3] + STK_0[0][4] + STK_{15}[1][0] + STK_{15}[1][3],\\
STK_{15}[1][5] = {} & STK_0[0][0] + STK_0[0][1] + STK_0[0][3] + STK_0[0][5] + STK_{15}[1][0] +\\
& STK_{15}[1][1] + STK_{15}[1][3],\\
STK_{15}[1][6] = {} & STK_0[0][0] + STK_0[0][1] + STK_0[0][2] + STK_0[0][3] + STK_0[0][6] +\\
& STK_{15}[1][0] + STK_{15}[1][1] + STK_{15}[1][2] + STK_{15}[1][3],\\
STK_{15}[1][7] = {} & STK_0[0][0] + STK_0[0][1] + STK_0[0][2] + STK_0[0][7] + STK_{15}[1][0] +\\
& STK_{15}[1][1] + STK_{15}[1][2].
\end{aligned}
$$

A.3 33-Round Attack on SKINNY-64-192

We present the 33-round rectangle attack on SKINNY-64-192 based on the boomerang distinguisher from [16]. Specifically, we append 2 rounds to the 31-round attack and search for the optimal key-recovery strategy that considers the strong key bridge. Our attack is shown in Figure 9.

Data complexity The probability of the whole attack is $Pr = P^2 = 2^{57.56}$, and other parameters of the attack are: $r_b = 60, r_f = 64, |k_b \cup k_f| = 160, |k_b \cap k_f| = 76$. The data complexity is $D_R = 4D = 4 \cdot y \cdot 2^{r_b} = \sqrt{s} \cdot 2^{n/2+2}/P = \sqrt{s} \cdot 2^{62.78}$.

Time complexity The best strategy is to guess 46 subtweakey cells in advance, as marked in red squares in Figure 9. These are only $|k'_b \cup k'_f| = 108$ information bits in these 46 subtweakey cells due to the strong key bridge. Under this key guessing strategy, $r'_b = r_b, r'_f = 28$, and $r^*_b = 0, r^*_f = 36$. The time complexity of the attack is as follows:

$$
\begin{aligned}
T_0 &= D_R = \sqrt{s} \cdot 2^{62.78}, \\
T_1 &= 2^{|k'_b \cup k'_f|} \cdot D_R \cdot \frac{7}{34} = \sqrt{s} \cdot 2^{108+62.78-2.28} = \sqrt{s} \cdot 2^{168.50}, \\
T_2 &= 2^{|k'_b \cup k'_f|} \cdot D = \sqrt{s} \cdot 2^{108+60.78} = \sqrt{s} \cdot 2^{168.78}, \\
T_3 &= 2^{|k'_b \cup k'_f|} \cdot D^2 \cdot 2^{2r^*_f - 2n} \cdot \epsilon = s \cdot 2^{108+60.78\times 2+36\times 2-128} \cdot \epsilon = s \cdot 2^{173.56} \cdot \epsilon, \\
T_4 &= 2^{k-h}.
\end{aligned}
$$

To extract the other subtweakey cells, it takes five steps, and the complexity ϵ is 1. For convenience, we denote the number of quartets remaining as Q, and the detailed computation of ϵ proceeds as follows.

1. Derive $STK_{29}[1,3]$. After guessing k'_b, k'_f, $\Delta X_{29}[13,15]$ is known. Since $\Delta W_{28}[13] = \Delta X_{29}[1] \oplus \Delta X_{29}[13]$ and $\Delta W_{28}[15] = \Delta X_{29}[3] \oplus \Delta X_{29}[15]$, we can determine $\Delta X_{29}[1,3]$. Therefore, we can derive $Y_{29}[1,3]$ from the known input and output differences of the S-boxes. Then $STK_{29}[1,3] = Y_{29}[1,3] \oplus Z_{29}[1,3]$. As the candidates for $STK_{29}[1,3]$ suggested by the two pairs in a quartet should coincide, there is a $2c$-bit filter and thus $Q \cdot 2^{-2c}$ quartets remain.
2. Guess $STK_{29}[0]$, then we can determine $\Delta X_{28}[13]$. Since $\Delta X_{28}[13] = \Delta X_{28}[9] = \Delta X_{28}[1]$, we can determine $\Delta X_{28}[1]$ and should have $\Delta X_{28}[13] = \Delta X_{28}[9]$. The latter is a $2c$-bit filter. Similar to the first step, we can derive $STK_{28}[1]$. Two derived $STK_{28}[1]$ values should be the same, which is a c-bit filter. The time complexity of this step is $Q \cdot 2^{-c}$ and $Q \cdot 2^{-4c}$ quartets remain.
3. Guess $STK_{29}[2,4]$, and then compute $\Delta X_{28}[15]$. Note that $\Delta X_{28}[15] = \Delta X_{28}[3] = \Delta X_{28}[7]$ should hold. Thus, we can determine $\Delta X_{28}[3,7]$. From the differences before and after the S-boxes, derive $Y_{28}[3,7]$ and $STK_{28}[3,7]$. Note that the values of $STK_{28}[3,7]$ suggested by the two pairs should be the same, which is a $2c$-bit filter. The time complexity of this step is $Q \cdot 2^{-2c}$ and $Q \cdot 2^{-4c}$ quartets remain.

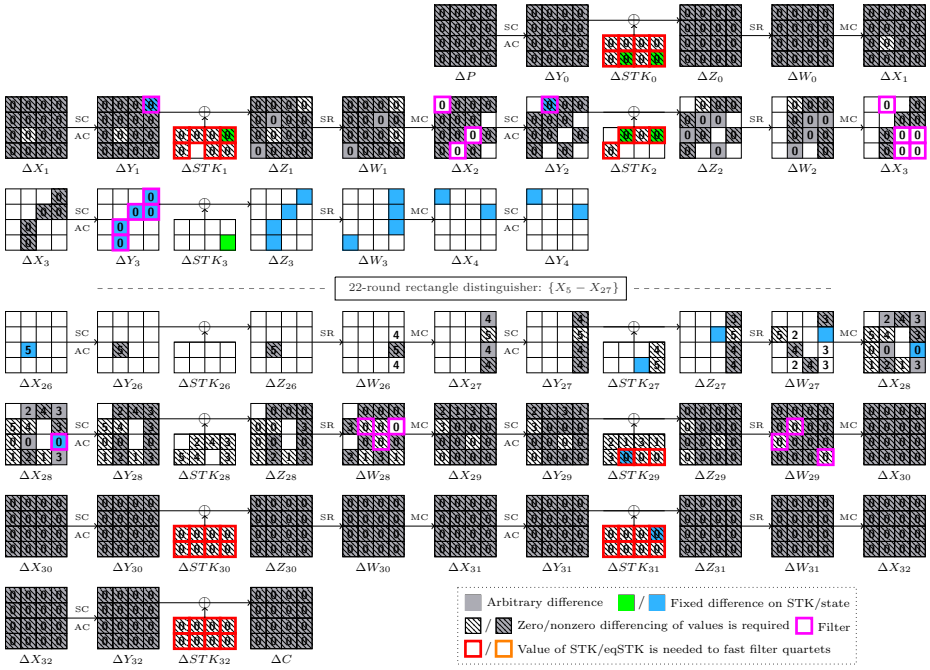

Figure 9: Rectangle attack on 33-round `SKINNY-64-192`

4. Guess $STK_{28}[2]$, compute $\Delta X_{27}[15]$. And $\Delta X_{27}[15] = \Delta X_{27}[3] = \Delta X_{27}[11]$ should hold. Likewise, derive $STK_{27}[3]$ and $Z_{27}[11]$, and further derive $STK_{28}[5]$ from $Z_{27}[11]$ and other known state cells. The derived values for the two derived subtweakey cells should coincide, meaning a $2c$-bit filter. The time complexity of this step is $Q \cdot 2^{-3c}$ and $Q \cdot 2^{-5c}$ quartets remain.
5. Guess $STK_{28}[4]$ and $STK_{27}[7]$, compute $\Delta X_{26}[9]$ and check if it equals the specific value. This is a $2c$-bit filter. The time complexity of this step is $Q \cdot 2^{-3c}$ and $Q \cdot 2^{-5c}$ quartets remain.

We choose $s = 4$ and $h = 24$, we obtain a 33-round attack on `SKINNY-64-192`, whose data, memory and time complexities are $2^{63.78}$, $2^{63.78}$, and $2^{175.56}$, respectively. The probability of success is about 92.3%.