B Classic Collision Attack on Reduced Saturnin

When searching trails for classic rebound attack on Saturnin, we just tweak the target of the model in Section 3 by removing the factor of the complexity of inbound part. Namely, the new target for $r_{in} = 2$ is

$$\sum Prob_r^i + \sum x_0^{i,j}. \tag{29}$$

As discussed in [23] and also in Section 6.1, when $r_{in} = 3$, the classic time complexity to solve Jean et al's 3-round inbound part is too large to be useful in the classic rebound attack. Hence, we only consider the case $r_{in} = 2$. The probability of the outbound phase has to be larger than $2^{-n/2}$.

Classic collision on 5-round Saturnin. We find a 5-round trail as shown in Figure 16. The probability to collide the plaintext and ciphertext is 2^{-64}. The inbound part covers 2 round from state Y_1 to state Z_3. The attack procedures are:

1. For fixed ΔY_1, and compute the ΔX_2.
2. For each 64-bit value $X_2[0,4,8,12]$, compute $X_2'[0,4,8,12]$, $Y_3[0,4,8,12]$ and $Y_3'[0,4,8,12]$. Insert $X_2[0,4,8,12]$ into table $L_0[\Delta Y_3[0,4,8,12]]$.
3. Similarly, build table L_1, L_2, L_3.
4. For each ΔZ_3,
   (a) Compute ΔY_3 and access L_0, L_1, L_2, L_3 to get the pair (X_2, X_2').
   (b) Check if the pair (X_2, X_2') leads to a collision.

Since in Step 4, we have 2^{64} possible differences for ΔZ_3, we are expected to check 2^{64} (X_2, X_2'). Since the probability of the outbound phase is 2^{-64}, we are expected to get one collision. The time complexity is about 2^{64} and the memory is about $2^{64} \times 4 = 2^{66}$.

Classic free-start collision on 6-round Saturnin. As shown in Figure 17, the inbound phase covers two rounds from state Z_1 to Z_3. The trail in Figure 17 is much easier than Figure 10 and there are no conditions on the key. Hence, we just randomly pick a difference for the key ΔK and a key pair (K, K') with $K \oplus K' = \Delta K$ to perform the rebound attack. Then, the probability of the outbound phase is $2^{-16-64} = 2^{-80}$ (note that the difference in both plaintext and ciphertext is equal to the difference in K). The procedures are:

1. Chosen a fixed difference for the key, i.e., ΔK and a fixed pair (K, K').
2. For each ΔY_1, compute ΔX_2,
   (a) Build super S-box tables L_0, L_1, L_2, L_3.
   (b) For each ΔX_4,
      i. Compute ΔY_3,
      ii. Access L_0, L_1, L_2, L_3 to get the the pair (X_2, X_2'),
      iii. Check if (X_2, X_2') leads to a collision.

We have $2^{16+64} = 2^{80}$ possible differences for $(\Delta Y_1, \Delta X_4)$. Since the probability of the outbound phase is 2^{-80}, we are expected to find one collision. The time complexity is about 2^{80} and the memory complexity is 2^{66}.