We thank the reviewers for their valuable comments, and are happy to take the editorial suggestions into account.

Reviewer A:

- about the additional information \cQ’\_S: following our presentation, they are not given to the adversary. We will clarify.

But in fact, just as [CS14] revealing the keys, they could be given at the end of the interaction. We think the difference is purely presentational.

- tightness: it seems difficult to conclude on general t-round linear SPNs... Similar intricateness exists in Feistel ciphers, which is also “structurally rich”.

Regarding 2n/3 security, we conjecture 3 or 4 rounds are tight. We will add a conclusion including this.

- linear layers built upon cyclic codes (with no zero entries) naturally satisfy properties 1 and 2. To ensure that the inverse satisfies properties 3 and 4, we made an exhaustive search. The search space is small enough.

Reviewer B:

- Thanks for the advice and we’ll add a summary table, a conclusion, and a clarification in Lemma 4.

- Thanks for pointing that a factor 2 is missed in Lemma 2, and we will correct.

The lemma allows using multiple primitives. It was first applied to key-alternating ciphers using independent round permutations [HT16]. Though we will recheck the concrete factors to ensure preciseness.

Reviewer C:

- \mathbb{F} is GF(2^n): we will add.

- the definition of colliding query: it has to fulfill one of the conditions. In fact, in a good transcript, a construction query couldn’t fulfill both (e.g., if it fulfills 1 and 2, then it fulfills B-3).