Response to the Reviewers

We thank both reviewers for the helpful comments and have addressed them all except for the following points for which we give explanations.

Response to Reviewer #1

Another general comment is that a first part of the paper talks about a nr1-round connector and a n_{r_2}-round differential, for a $(n_{r_1} + n_{r_2})$-round collision attack (see Figure 2), but in a second part several statements seem to contradict this.

1. line 372 "α_2 (ΔS_I)": more generally, isn't it "$\alpha_{n_{r_1}} = \Delta S_I$" according to Figure 2?
   In line 356, we stated that "Suppose we are to construct a connector of two rounds" for the sake of clarity. In this context, $n_{r_1} = 2$, $\Delta S_I = \alpha_2$. In the case of 3-round connectors, $\Delta S_I = \alpha_3$.
2. line 658: "n-round Keccak is to find good (n-1)-round trail cores": should it be "n_{r_2}-round trail cores" according to Figure 2?
   It can be regarded as n_{r_2}-round differential trails. According to the definition of trail cores in line 654, the n_{r_2} β_is of a n_{r_2}-round differential trail can act as a $(n_{r_2}+1)$-round trail core if the weight of the first round is minimal.
   To mount 5-round attacks, we utilize 4-round trail cores $(\beta_2, \beta_3, \beta_4)$ as shown in Appendix D. In 6-round attacks, since we fix the difference α_2, 5-round trails cores are needed, i.e., $(\beta_2, \beta_3, \beta_4, \beta_5)$.
   That is reason why we say "The first step of mounting collision attacks against n-round Keccak is to find good (n-1)-round trail cores."
3. line 679: why does the TDF depend on $n_r - 1$ weights, which would imply that $n_{r_1} = 1$ (and not 2 or 3)?
   As stated in line 658, we use $(n-1)$-round trail cores to attack n-round Keccak. A $(n-1)$-round trail core is composed of $n-2$ β_is. That is to say, β_2 is fixed (thus $\alpha_2 = L^{-1}(\beta_2)$ is fixed) for the 2-round connector; β_2, β_3 are fixed for the 3-round connector. Since these parts are fixed, the consumption of degrees of freedom by these parts are also fixed. Although TDF depends on $n_r - 1$ weights, this does not mean the length of the connector is only one round.
4. line 687: here the trail seems to be 3-round long instead of n_{r_2}-round long.
   True. In both 5-round and 6-round attacks, $n_{r_2} = 3$. However, this does not mean that we only need to search for 4-round trail cores (or 3-round differential trails). In the 6-round attack, the differential for the third round is known and fixed. So, for 6-round attacks, we need to search for 5-round trail cores (4-round differential trails).
5. lines 784-785 "we employ 4-round (5-round) trail cores [...] to mount collision attacks on 5-round (6-round) Keccak": following Figure 2, this would imply that $n_{r_1} = 1$, so 1-round connectors are used, but this is not what is written elsewhere in the paper.
   It is not the case, as explained in item 3.

6. line 554: $DF_i^{(2)}$ is actually equal to 5 minus the weight.
   line 560: $\sum(5 - DF_i^{(2)})$ is actually equal to the weight (is it $w(\beta_1)$?).
   Yes, but at that moment, the notion of weight is not introduced yet.
7. lines 763-771 "Keccak-f[1600]v1 [...] to search for differential trails". How does an implementation of the Keccak-f[1600] permutation helps look for finding differential trails? Shouldn't there be an implementation that instead expands a difference into compatible differences through some (inverse) steps?
   True. It contains an efficient implementation of the KECCAK permutation on GPU, upon which the search for good differential extensions is implemented.

Response to Reviewer #2

1. In Table 1, complexities for instances solved in Section 6 are just mentioned as "Practical". In Table 6, timings are given. Complexities should be summarized differently at some place, maybe as number of message pair evaluations or by another measure.
   Thanks for this comment. In the experiments, we just recorded the actual timings for finding a collision, from which only a rough number of tested message pairs can be calculated since the technique of early abortion was used. On the other hand, 2^w, as shown in Table 6, can act as an estimation of required message pairs for finding a collision. To provide accurate numbers of tested message pairs, we have to re-run the experiments, which takes time and consumes energy. Therefore, we prefer keeping the tables the same as before.

The revised version of the paper follows and a version of the paper highlighting the differences between the original version and the revised version comes subsequently.