After the publication of this paper, we realized a flaw in our analysis which renders the attack described in section 4.1 invalid. In particular, in section 4.1 Key recovery attacks on ARIA, as part of the key recovery attacks procedure, we partially decrypt the ciphertexts. To do this, we suggested guessing some round key nibbles along with some intermediate state values to be able to append a large number of rounds after the linear hull distinguisher. This is, however, not correct because these intermediate state values do not have the same value for all the plaintexts/ciphertexts considered. This means that the counter based approach to identify the correct key will not indicate the right key guess and thus this attack is invalid.

It is interesting to note that this observation also invalidates the other published linear attack of Liu et al. in ICICS'11 (ref [17] of our paper).