Response to Reviewer 4 Comments

Point 1: In the authors’ response to original comment 3, the CRC module is replaced with the hash function. Even though corresponding comments and reference are added that there exist some lightweight hash functions, it is very unclear what the unique contributions are of the proposed protocol over existing related protocols which also only requires the hash module, for example, compared to reference: P. Gope, J. Lee, and T-Q. S. Quek, “Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions,” IEEE Transactions on Information Forensics and Security, vol. 13(11), pp. 2831-2843, 2018. The authors need to add a separate section that clearly states the unique contributions and advantages of the proposed protocol over other related ones.

Response 1: Thanks a lot for recommending the paper Gope et al. [47]. I have read it and added related discussion to Section 2 and Section 6. Section 6 is also revised to present the highlights of our proposed protocols.

Point 2: The biggest concern has not been appropriately addressed at all in the revised version, i.e., the implementation evaluation of the proposed protocol based on “Noisy PUF” is missing. The authors arbitrarily stated that “the implementation cost of our protocol can be A LITTLE BIT LOWER THAN [39]” without conducting any hardware validations at all. According to what is reported for the “ideal PUF” case, the proposed protocol has even larger overhead compared to the work: P. Gope, J. Lee, and T-Q. S. Quek, “Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions,” IEEE Transactions on Information Forensics and Security, vol. 13(11), pp. 2831-2843, 2018. Detailed comparisons regarding overhead as well as unique contributions of the proposed protocol with the abovementioned work and other works need to be provided.

Response 2: We have revised Section 7.2 to provide a more detailed implementation cost estimation. Detailed comparisons are presented in Section 6. The unique contributions are first briefly mentioned in Section 3 and then discussed in detail later in Section 6.

In addition, I have one question that I want to discuss with you. In Table IV of [47], Gope et al. compared the protocols in terms of the tag memory footprint. But I am quite confused about how they measure the memory footprint. In the table, they stated that the memory footprint of Aysu et al.’s scheme is 1392-bit, which is much smaller than the memory footprint provided in Table 3 of Aysu et al. [41]. From the memory footprint of other protocols, it seems that Gope et al. estimate the memory footprint by the maximum memory taken by the parameters that have to be in memory at the same time. I will appreciate you very much if you can let me know how they calculate the memory footprint.