Response to Reviewer 4 Comments

Point 1: The paper needs further proof read to correct grammar mistakes and inappropriate terms and phrases. For example, the sentence “EPC Gen2 tags is the mainstream for the develop RFID applications” needs to be revised at several places.
Response 1: We have proof read our manuscript.

Point 2: In sections 4.2 the assumption 2 is not appropriate since the reliability of regenerating the same responses for PUFs depends on the strength and overhead of the error correction mechanism. The authors need to provide more performance and overhead information of the error correction scheme before making the assumption.
Response 2: We revise our manuscript as follows. We first propose a lightweight RFID mutual authentication protocol based on ideal PUFs in Section 4.4. Then we enhance this protocol so that it can be adopted with noisy PUFs in Section 4.5.

Point 3: In section 5.2.1 Theorem 2, it is incorrect to state that “A cannot inverse the CRC function” because unlike hash, CRC can be easily reversed. Therefore, the security of reverse-engineering the inputs (which are the secrets) of the CRC function from its plain outputs in the whole protocol needs to be re-evaluated, so are the validity, performance and overhead of the overall proposed protocol.
Response 3: We now use a hash function instead of the CRC function. The relevant parts are also revised.

Point 4: Step 3 states that “Upon receiving the session identity SIDiT from T, S uses it as an index to search a matched entry.”, which indicates that the proposed protocol still needs exhaustive search at the server. It is contradictory to what the authors claimed in section 6 that the protocol does not need exhaustive search and is thus scalable.
Response 4: Here the exhaustive search indicates that the backend server has to perform some operations (i.e., hash function or cryptographic function) before checking every record in the database. As discussed in Section 3, according to [41], if the server can find the identity of tag by directly checking the received data, the time cost can be constant. In our protocols, the server can locate the tag in the database by directly checking received SID.

Point 5: The paper lacks experimental implementations to evaluate and validate the cost, performance and the scalability of the proposed protocol, as can be referred to in reference [40]. The authors need to add this part as the experimental evaluation part.
Response 5: In Section 5.3, we use a formal verification tool to validate the security correctness of our proposed protocol. In Section 7, the implementation of our proposed protocol is discussed.

Point 6: In section 4.2, it is incorrect to state that “A PUF can be considered as a challenge-response pair (CRP)” since a PUF instance typically maps a set of challenges to a set of responses.
Response 6: We revised the description. In addition, a noisy-PUF based protocol is proposed in Section 4.5.