Response to Reviewer 3 Comments

**Point 1:** The authors base the security on PUF, however most PUFs are not so perfect (not very stable, not very reliable etc.) --- i.e. the solution presented as an example. The problem with PUF implementation is that the responses are not certain and here --- if one wraps that in CRC code and performs an authentication --- many of them will fail if one assesses the result binary. Usually there is a need of correction of the PUF responses or an evaluation how far is a response from the expected one.

**Response 1:** We proposed an enhanced protocol based on noisy PUF in Section 4.5.

**Point 2:** The authors use a few times RNG. What are the expectations concerning RNG? TRNG? PRNG? How good one? What kind of vulnerabilities introduces a weak RNG?

**Response 2:** The EPC Class-1 Generation-2 standard states that “Tags shall implement a random or pseudo-random number generator” in Section 6.3.2.5. We assume that, in our proposed protocol, each RFID tag is a EPC Class-1 Generation-2 tag equipped with a TRNG. With a weak RNG, an attacker is possible to guess out the random number generated and then break our scheme. But we think the detailed design of a RNG is out of the scope of our manuscript.

**Point 3:** The authors mentioned “physical attack”. I’m guessing based on [5] that as a side-channel attack. However physical attacks are just a part of many SCAs and the physical ones are usually the most expensive and difficult to perform in practice. What about other SCAs?

**Response 3:** Physical attack is a kind of side-channel attack (SCA) in which an attacker has physical access to a tag and can retrieve some useful data stored in the tag. Although expensive, most of existing protocols are vulnerable to such attack. And we want to show that our proposed protocol has the advantage that it can defend against physical attacks.

For other SCAs, as we discussed in Section 4.1, we just consider the adversary as a Dolev-Yao intruder with the capabilities of physical attacks and clone attacks in addition.

**Point 4:** What happens in case when Auth1 in step M4 fails? The tag does not compute the rest? Does it even answer?

If yes, there is possibility for the attacker to feed many Ci-Ri pairs to the tag (generating N and computing CRC) and checking one by one if a response fits to the challenge (brute force checking).

If no, the same scenario, but with timing attack, which was not consider here.

**Response 4:** If Auth1 in step M4 fails, the tag will not compute the rest. We revised our paper, using a hash function instead of the CRC. So now Auth1=Hash(N||Ri). Since the attacker does not know N or Ri, the brute force checking is almost equivalent to a brute force attack to a hash function.

**Point 5:** Have the authors considered complex attacks (for example repetition attack on CRC in M3 after blocking M5)?

**Response 5:** We revise our proposed protocol, using a hash function instead of a CRC function, so now such attack can hardly break our scheme. In Section 5.3, we also use a formal verification tool, Scyther, to validate the security correctness of our proposed protocol.

**Point 6:** Why do you assume the wire connection (line: 164)? Did you mean secure? Wire is not much more secure then air.
Response 6: We intended to mean secure. The description is revised as you suggested.

Point 7: I think that the assumption for the server of “no limitation on computation or storage” may be a little overkill...
Response 7: The description is revised to “RFID tags have limited resources of computation power and storage while backend servers are trusted and have no such limitation.”

Point 8: I’m glad that the authors included comparisons to other protocols, however I think they should be much more detailed.
Response 8: It’s really a good idea. However, to do so, each protocol needs at least 2 pages which not only makes our manuscript to be like a survey but also may result in the page limits problem. On the other hand, some of RFID protocol papers do include other protocols’ details. But such paper just first presents the details of one existing protocol and then proposed an improved scheme based on it. To the best of our knowledge, most of RFID protocol papers do not give details of other protocols to be compared with.

Point 9: The language must be significantly improved (preferably by a native speaker who understand the subject). Just a few examples of unfortunates:
- one of the key technique
- logical gates available can be used for the security
- In 2002, the first PUF is invented.
- PUF techniques can has good resistance
- cryptograph function
- with the transmitted nonce until find a match
Response 9: We proof read our manuscript.

Point 10: The style must be improved - a few unfortunates:
- the adversary “A” is written different on page 7 and half of 8 and the rest of the article
- many variables are sometimes written in italics, sometimes not
- “Internet of things (IOT)” - line 85
Response 10: We revised our manuscript as you suggested.