Survey on passive RFID tag cryptography for nonspecialists

Summary

This paper introduces a summarized representation of the field that surrounds the RFID technology (or at least the already written part of the paper). It classifies : the usages of the RFID, categories of RFID, the functioning principle of the passive RFID, where it explains how power management, signal processing, memory, computation of cryptography work together. This paper also show a brief explanation of the 5 main cryptography protocols and the Avoine model. All these together sum up all what GENERAL information one newcomer in this field of research needs to know about passive RFID.

Comments

It looks like the main work was put in the background part but I am not 100% sure. Assuming it was not my number of comments is limited because the most part is very vaguely explained and it it only the background. Maybe the details will come in the My work part and everything will be better explained. Taking into consideration that it is only 4 pages that means that only half of the work is done and assuming that the author knows what needs to be done, I couldn't write everywhere: "More explanation is needed".

Strengths

+ III A) Very well structured and the language is very nice and understandable

+ Overall very good bullet points that make the text easy to follow.

Weaknesses

- the introduction of the topic is too short and after reading it, didn't raise too much interest. I would suggest a more general phrasing for the first paragraphs of the introduction, not directly diving into the usages of RFID.

- Some visuals/images would be nice. For example in section IV or V

- Maybe explain a bit more in the background what HMAC und MAC codes are and what do they offer.

- Again I assume this will be completed before the Abgabe, but the related work should have a more in-depth comparison in-between the different surveys/papers and what aspects of the topic they describe.

- Personally I would like to see some type of example of a RFID reading scenario, like the maths and cryptography behind it.