Cryptology ePrint Archive: Report 2011/167

Identifying Large-Scale RFID Tags Using Non-Cryptographic Approach

Yalin Chen, Jue-Sam Chou, Cheng-Lun Wu, Chi-Fong Lin

Abstract: In this paper, we propose a new approach to identify a tag of a RFID system in constant time while keeping untraceability to the tag. Our scheme does not use any cryptographic primitives. Instead, we use a line in a plane to represent a tag. The points on the line, which are infinite and different each other, can be used as tag identification. We also explore the scalability of the proposed scheme. The result of experiments showed that a tag of the RFID system over 1,000,000 tags, embedded 3000 gates, can store 559 dynamic identity proofs.

Category / Keywords: radio frequency identification, RFID, identification protocol, privacy, untraceability, location privacy, scalability

Date: received 2 Apr 2011, last revised 11 Apr 2011

Contact author: yalin78900 at gmail com

Available formats: PDF | BibTeX Citation

Note: We correct a mistake. The update overhead of Alomair's scheme is O(1) rather than O(C).

Version: 20110411:064417 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]