Accepted Manuscript

Double verification protocol via secret sharing for low-cost RFID tags

Y. Liu, M.F. Ezerman, H. Wang

PII: S0167-739X(17)32351-8
DOI: https://doi.org/10.1016/j.future.2018.07.004
Reference: FUTURE 4322

To appear in: *Future Generation Computer Systems*

Received date : 14 October 2017
Revised date : 20 May 2018
Accepted date : 2 July 2018

Please cite this article as: Y. Liu, M.F. Ezerman, H. Wang, Double verification protocol via secret sharing for low-cost RFID tags, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.07.004

Double Verification Protocol via Secret Sharing for Low-Cost RFID Tags

Y. Liu[a], M. F. Ezerman[b,*], H. Wang[b]

[a]College of Computer Science and Technology, Jiangsu Normal University, Xuzhou, 221116, China.
[b]School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore.

Abstract

RFID tags have become ubiquitous and cheaper to implement. It is often imperative to design ultralightweight authentication protocols for such tags. Many existing protocols still rely on triangular functions, which have been shown to have security and privacy vulnerabilities. This work proposes UMAPSS, an ultralightweight mutual-authentication protocol based on Shamir's $(2,n)$ secret sharing. It includes mechanisms for double verification, session control, mutual authentication, and dynamic update to enhance security and provide a robust privacy protection. The protocol relies only on two simple bitwise operations, namely addition modulo 2^m and a circular shift $\mathrm{Rot}(x,y)$, on the tag's end. It avoids other, unbalanced, triangular operations.

A security analysis shows that the protocol has excellent privacy properties while offering a robust defense against a broad range of typical attacks. It satisfies common security and the low-cost requirements for RFID tags. It is competitive against existing protocol, scoring favourably in terms of computational cost, storage requirement, and communication overhead.

Keywords: RFID, low-cost, mutual authentication, secret sharing, ultralightweight.

1. Introduction

Radio Frequency Identification (RFID) brought automatic object identification by electromagnetic wave into sensor technology, requiring no physical contact, which was revolutionary. As costs steadily drop, RFID systems are increasingly deployed in varied environments, raising numerous security and privacy concerns. Many works have pointed out that RFID is vulnerable to practical malicious attacks (see [1] and [2]) and security threats (see [3] and [4]). These include eavesdropping, message interception and modification, blocking, jamming, counterfeiting, spoofing, traffic analysis, man in the middle (MITM), traceability, and desynchronization attacks. Effective authentication protocols to improve robustness, reliability, and security against major attacks, both passive and active, are crucial.

Based on memory type, power consumption, and price, RFID tags are either high-cost or low-cost. In 2007, Chien proposed a tag classification based on computational cost and supported on-tag operations [5]. High-cost tags fall into either *full-fledged* or *simple* class. The

*Corresponding author
Email addresses: lyl1980115@163.com, liuyali@jsnu.edu.cn (Y. Liu), fredezerman@ntu.edu.sg (M. F. Ezerman), HXWang@ntu.edu.sg (H. Wang)