Accepted Manuscript

Certain types of M-fuzzifying matroids: A fundamental look at the security protocols in RFID and IoT

Shao-Jun Yang, Xinyi Huang

PII: S0167-739X(17)32294-X
DOI: https://doi.org/10.1016/j.future.2018.04.028
Reference: FUTURE 4106

To appear in: *Future Generation Computer Systems*

Received date : 8 October 2017
Revised date : 19 March 2018
Accepted date : 10 April 2018

Please cite this article as: S.-J. Yang, X. Huang, Certain types of M-fuzzifying matroids: A fundamental look at the security protocols in RFID and IoT, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.04.028

Certain types of M-fuzzifying matroids: A fundamental look at the security protocols in RFID and IoT[☆]

Shao-Jun Yang[a,*], Xinyi Huang[a]

[a] *The Fujian Provincial Key Laboratory of Network Security and Cryptology, College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, P.R. China.*

Abstract

Security protocols for RFID and IoT are often built on NP-hard problems. The greedy algorithm is an effective method to solve some NP-hard problems. However, the greedy algorithm can get the optimal solution if and only if the structure of the solutions is a matroid. This paper focuses on M-fuzzifying matroids. The notions of acyclic matroids, simple matroids, paving matroids and uniform matroids are generalized to fuzzy setting, which are called M-fuzzifying acyclic matroids, M-fuzzifying simple matroids, fuzzifying paving matroids and fuzzifying uniform matroids, respectively. From the sense of categorical, the relationships between M-fuzzifying matroids, M-fuzzifying acyclic matroids and M-fuzzifying simple matroids are investigated.

Keywords: Radio Frequency Identification, M-fuzzifying acyclic matroid, M-fuzzifying simple matroid, fuzzifying paving matroid, fuzzifying uniform matroid

1. Introduction

The development of Radio Frequency Identification (RFID) brings great challenges to the security and privacy of current systems and processes. One of effective approaches to protect RFID systems safely is cryptography. The security of the algorithms and protocols in RFID are often reduced to some

[☆]The project is supported by the National Natural Science Foundation of China (11701089).

[*]Corresponding author

Email address: shaojunyang@outlook.com (Shao-Jun Yang)