International Journal of Software Innovation
Volume 6 • Issue 2 • April-June 2018

A Novel RFID Anti-Counterfeiting Based on Bisectional Multivariate Quadratic Equations

Xiaoyi Zhou, Hainan University, Haikou, China
Jixin Ma, University of Greenwich, London, UK
Xiaoming Yao, Hainan University, Haikou, China
Honglei Li, Hainan University, Haikou, China

ABSTRACT

This article proposes a novel scheme for RFID anti-counterfeiting by applying bisectional multivariate quadratic equations (BMQE) system into an RF tag data encryption. In the key generation process, arbitrarily choose two matrix sets (denoted as A and B) and a base RAB such that [(AB)⃗]=λ 〖R_AB〗 ^T, and generate 2n BMQ polynomials (denoted as ρ) over finite field F_q. Therefore, (F_q, ρ) is taken as a public key and (A,B,λ) as a private key. In the encryption process, the EPC code is hashed into a message digest d_m. Then d_m is padded to d_m^' which is a non-zero 2n×2n matrix over F_q. With (A,B,λ)and d_m^', s_m is formed as an n-vector over F_2. Unlike the existing anti-counterfeit scheme, the one the authors proposed is based on quantum cryptography, thus it is robust enough to resist the existing attacks and has high security.

KEYWORDS

Bisectional Multivariate Quadratic Equation, Counterfeit, Cryptography, Ergodic Matrix, RFID

1. INTRODUCTION

RFID (Radio-frequency identification) technology, with its advantages that universal anti-counterfeiting methods (such as laser holographic imaging and chemical markers) are short of, has now become one of the most promising tools to solve the problem of supply chain data counterfeiting.

RFID is a non-contact identification technology to identify the presence of an object through radio signals, which can quickly track items and exchange data. The identification process is without manual intervention and can work in a variety of harsh environment. Therefore, RFID technology has been widely used in the supply chain management. The typical applications include: the tracking and management of container or dangerous goods such as gas tank, the logistics of agricultural products, the storage management, etc. The key to these applications lies in the automatic identification of the product, so that all the information in the enterprise's MIS system or ERP system can get real-time transmission and reflection. Through the RFID supply chain management, enterprises obtain the supply chain flow of goods in a more accurate, more timely and more detailed manner, so as to provide helps for the daily operation and decision-making. RFID is having a profound impact on the mode of production for enterprise supply chain management.

DOI: 10.4018/IJSI.2018040101

However, with signal broadcasting, resource limitation and wireless transmission, the RF tags are facing security attacks such as monitoring, tracking, tampering and so on. A reliable communication system must ensure the transmission of confidential data, as well as the integrity and availability of data (Wang, 2010). However, due to the physical characteristics of RF tag, its computing speed, storage space and communication capacity are very limited, which increases the difficulty of the research of RFID technology security mechanism. Unfortunately, most of the current researches focus on the security and privacy of tags and readers, and pay little attention to the security of RF tags. More worrying, the existing EPCglobal standard EPCC1G2 allows RF tags to be read and written (Yuan, 2010). Malicious attackers can not only access to the RF tags or even tamper and forge them, but also speculate consumers' favourites by tracing the characteristics of the tags.

At present, there are two main methods for RFID system security: 1) the security mechanism based on physical methods, such as Sleep command, using Faraday nets mask, clipping label method, etc., for active shielding and interference, etc. The physical method is direct and effective, but depends on the additional equipment, it increases the cost of using the label and has a certain risk; 2) authentication technology based on cryptographic authentication techniques, such as the Hash function mechanism and symmetric keys (Sajadieh, 2015, Lin, 2015 and So, 2017). But for Hash functions, even MD5 hash function, which is widely used as a computer security domain, has been shown to be unable to resist strong collision attacks (Liang, 2007). The symmetric key technology has such disadvantages as simple encryption algorithm, low encryption strength, limited key length (56 bits, /128 bits) and so on. Moreover, the symmetric key technology is difficult to manage key distribution, which is not conducive to managing (Shen, 2013).

Relatively speaking, the public key cryptosystem has made up the imperfection of Hash function and mechanism of the symmetric key (Zhou, 2011 and Zhou, 2013), but with the development of computer processing capability continues to improve, The shortcomings of the traditional public key cryptography are becoming more and more prominent, which makes the research of quantum cryptography go deeper. In May 3, 2017, a science explosive news about the world's first light quantum computer being invented in China indicates that once the quantum computer is put into use, public key cryptography will be completely broken, including RSA, DSA and ECC. Therefore, we should seize the time to study the existing alternative technologies of public key cryptography, to meet the challenges of quantum computers, and ensure the security of information in the quantum age. Due to the widespread application of RFID technology in the era of Internet of things, the potential threat of data security should be paid more attention to.

Therefore, how to solve the counterfeit problems of RF tags data and security of communication process, and to ensure that the proposed scheme can apply to the tags with limited ability, has become one of the key issues for the sustainable development of RFID (Wang, 2017 & Gao, 2017).

2. DEVELOPMENT OF RFID ANTI-COUNTERFEIT TECHNOLOGY

In recent years, RFID technology has made some breakthroughs in worldwide security applications, many researchers proposed RFID technology based on privacy and security issues. For example, personal information can be leaked when the RF tag reader secretly scans, records and tracks the tag, or secretly check the user carried paste the electronic tag object, resulting in leakage of personal information; reissue molecules can counterfeit electronic tags to deceive the reader complete illegal certification.

In order to solve the problem of privacy disclosure, Weis (Weis, 2003) proposed a hash-lock method. In his scheme, the private key K of the tag and the MetaID corresponding to it are stored in a database. When an RF tag reader sends a query request to an RF tag, the tag responds the reader with MetaID. Then the reader sends it to the database for the corresponding private key. The reader will send K to the RFID tag when K is received. By comparing Hash(K) and MetaID, the ID of the RFID tag will be sent if they are the same.