Abstract

Secure applications protect valuable information and defend every vulnerability. The goal of a secure application design is to create a cost effective system where information is securely protected. Cryptography is one of the effective tools that has powerful implications for information security. Since cryptographic solutions are continuously evolving, algorithms that were once considered secure are no longer secure now in practice. Therefore, poorly deployed systems are being threatened by increasing adversarial processing power, low-cost devices, weaker cryptographic algorithms, new demand of security and privacy issues, and technological advances. This has lead the US and Japan government to launch special programmes and bodies to define cryptography standards, specifications and recommendations to cope with the security and privacy requirement of the future. This theses presents our research results on the design and analysis of cryptographic solutions for Vehicle Ad hoc NETwork (VANET) and low cost Radio Frequency IDentification (RFID) systems.

Motivated by the recent attention on exploiting group signature approach in the design of VANET security scheme, we attempt to integrate all the potential properties of group signature in an individual scheme, so that it can best meet the demand and needs of the wide range of VANET services. To this end, we propose a new group signature model that is more application friendly, optimally secure with a relaxed privacy definition to satisfy practical privacy requirement of VANETs. Moreover, we investigate the feasibility of implementing batch verification of group signatures into a real life VANET environment. In addition, we improve an existing batch verification system on identity based group signature and determine where and when batch verification may be infeasible in practice.

Inspired to realize ubiquitous computing, machine perception and the rapidly growing trend in insecurity and terrorism, the RFID technology plays an indispensable role in various fields. With the use of tags and transponders (tracking \& tracing), RFID technology is seeking to venture into the transport and logistics systems, pharmaceutical and clothing industry as well as monitoring and safeguarding the citizen. However, the exclusive features of RFID introduces new security and privacy concern from the end users' view point and resource restriction into the tag from the engineering perspective. Security concerns in the form of authentication of tags and reader and privacy concerns related to undercover tag/communication tracking of tagged items. Today's RFID system facilitates the real-time tracking of physical items in the supply chain. This enables the physical data flow of a tagged item with its location to be matched with the information flow in the enterprises' information management systems. The weak privacy protection may jeopardize the entire supply chain exposed to industrial espionage, while vulnerable security may lead to the acts of eco-terrorism and economic sabotage. However, we first identified the major prior works in the area of RFID security such as tag authentication, tag ownership transfer, RFID-enabled supply chain path authentication etc. To this end, we adopted a new, growing and promising direction in the lightweight cryptographic research, namely Hop-per-Blum (HB)-family

protocol based on the Learning Parity from Noise (LPN) problem. Since the inner computations in the HB-family protocol comprises only matrix vector multiplications over GF(2) they are extremely efficient and may even be suitable for practical RFID applications. Meanwhile the security is equivalent to well-known hardness assumptions from coding theory and lattices. We ideated the demand of efficient, robust, forward secure mutual authentication protocol for RFID systems in HB-family settings. We propose two mutual authentication protocols at this end: one is between a tag and a back-end RFID reader/server. The other protocol, that may follow the former one, is among the RFID entities where an RFID reader and a back-end server are not identical. To address the ownership transfer problem in a large inventory system, we build a new, improved model consisting of several Semi Trusted Parties (STPs) and a trusted server.

Our model can ease the ownership process for the consumers in the remote location, and allows simultaneous transfer ownership of multiple tags from one owner to another. Our construction uses a new variant of Homomorphic Aggregated signature, a lightweight searchable encryption, Field LPN and pseudo-inverse matrix as cryptographic primitives. Finally, we propose a path authentication protocol for an RFID-enabled supply chain. Compared to Elliptic curve Elgamal Re-encryption based construction our Homomorphic Message Authentication Code on Arithmetic circuit based solution offers a new privacy direction to the path privacy with an efficient and effective label of security and prevention of counterfeiting.

Our innovation has the potential to pave the way for more secure RFID-enabled services. All the secure and privacy-preserving protocols will enable RFID and vehicle industries to implement confidently and take advantage of emerging opportunities.

Keywords: Quantum Cryptography, Privacy, VANET, RFID, Group Signature.