

带权重的多所有者标签所有权动态转换协议

甘勇, 杨宗琴, 贺蕾, 杜超, 刘思聪

(郑州轻工业学院计算机与通信工程学院, 河南 郑州 450002)

摘要: 采用拉格朗日插值算法, 提出了一种带有不同权重的多所有者标签所有权动态转换协议。当标签所有权发生变化时, 该协议能恢复出原有密钥, 验证所有者的合法性, 并使用秘密共享门限方案, 根据所有者的新权重重新分发子密钥, 提高了所有权转换的安全性和灵活性。对该协议进行了仿真实验, 实验结果表明, 该协议具有较低的计算量和较少的计算时间, 适用于低成本的 RFID 标签。

关键词: 多所有者; 拉格朗日算法; 密钥共享; 所有权动态转换

中国分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00120

Tag dynamic ownership transfer protocol for multi-owner with weights

GAN Yong, YANG Zong-qin, HE Lei, DU Chao, LIU Si-cong

(School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China)

Abstract: A dynamic ownership transfer protocol of RFID tag based on Lagrange algorithm was proposed to achieve the transfer for multi-owner with different weights. When the ownership of a tag changed, the agreement could recover the original secret key to verify the legitimacy of the owners, and use secret sharing algorithm to re-distribute sub-key according to the new weights of the owners to make the security and flexibility of the ownership transfer improved. The simulation is carried out to show that it adapts to a low-cost RFID tag because the calculation and time consuming are low in the protocol.

Key words: multi-owner, Lagrange algorithm, shared secret key, dynamic ownership transfer

1 引言

无线射频识别 (RFID, radio frequency identification) 是一种不需要接触实物、仅通过电子磁场实现自动识别目标的技术。近年来, RFID 技术已被广泛应用在供应链管理、零售百货、安全防伪、交通运输等各个领域。然而, 它在为电子交易带来便利的同时, 也带来了新的安全和隐私问题。虽然目前有许多 RFID 的安全协议^[1~5], 但

是大多数协议都容易受到各种攻击, 且可扩展性、可定制性都存在不足。当 RFID 标签要进行所有权转换时, 由于 RFID 的存储能力和计算能力都非常有限, 不能执行复杂的密码算法, 原所有者、新所有者和 RFID 标签的安全隐私都难以得到保证^[6]。

目前, 对 RFID 标签所有权转换问题的研究主要集中于单所有者的所有权转换。然而, 在实际应用中, 标签可能会有多个所有者, 且不同所

收稿日期: 2016-11-01; 修回日期: 2016-12-27。通信作者: 甘勇, ganyong@zzuli.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61572445); 河南省高等学校重点科研基金资助项目 (No.16A520075)

Foundation Items: The National Natural Science Foundation of China (No.61572445), Key Scientific Research Projects of Universities of Henan Province (No.16A520075)

有者所占有的权重也可能不相同,同时,有些所有者可能还会出售自己所持有的份额,因此在标签的生命周期内,不同所有者所占有的权重可能会发生变化。例如,某一公司由多位股东组成,他们所持有的股份也不相同,股份多的股东作为公司的实际控制人往往自己就能对公司事务做出决策,但当有股东出售了自己的股份导致股本结构变化使其不能独自决策时,就需要联合一到多个股东,因为只有支持该决策股东的股份多于某个阈值才能确定该决策;又或者某个股东把自己的股份全部出售给其他人,自己不再是决策者,不能再参与任何决策。RFID 标签的所有权转换中也面临类似问题,如一个 RFID 标签具有多个所有者,即 P_1 、 P_2 、 P_3 。所有者 P_1 拥有标签所有权的权重为 1,所有者 P_2 拥有标签所有权的权重为 1,所有者 P_3 拥有标签所有权的权重为 2,当标签的所有权需要进行转换时,只有同意进行所有权转换的所有者的权重值大于预先设定好的阈值,才可以将标签的所有权转交给其他实体。因此,对基于不同权重的所有者之间 RFID 所有权动态转换有重要的研究价值。

2 相关工作

RFID 作为一种自动识别技术,其主要功能就是被系统识别,识别也是通过标签数据对其附着物进行判定,这就导致所要面临的问题,即隐私性与安全性。标签的隐私与安全问题是影响其广泛应用的主要原因之一,在标签的所有权转换过程中,隐私与安全需要满足 3 个方面的要求。

1) 在所有权转换过程中,能够抵抗假冒攻击、重传攻击、中间人攻击等。

2) 所有权转换后,原所有者不能够继续访问标签,以保护新所有者的隐私,实现后向安全。

3) 新所有者得到所有权后,不能访问标签之前的数据,保护原所有者的隐私,实现前向安全。

2.1 标签所有权转换协议

目前,国内外研究学者对 RFID 标签的所有权安全转换协议进行了大量的研究,大致可以分为带有可信第三方(TTP, trusted third party)的协议^[7,8]和不带 TTP 的协议^[2,9]。其中,最早的所有权

转换方案是由 Osaka 等^[7]提出的,该协议虽然基于散列和密钥加密函数,但不能抵抗同化攻击、重放攻击等。Jäppinen 等^[10]尝试在此方案上进行改进,然而他们的方案仍不能抵抗同化攻击^[11]。Dimitriou 等^[12]提出了一种基于随机数和密钥加密的授权和所有权转换协议 RFIDDOT,实现了密钥能在相对隐私的环境下进行更新,但该协议不能保证新所有者的隐私^[11]。Kulseng 等^[13]提出了 2 种轻量级的 RFID 所有者转换协议,其中一个带有 TTP,一个不带 TTP,前者当攻击者选择性阻断信息后不能实现同步,后者不能抵抗攻击者窃听无线信道^[11]。Chen 等^[14]先后提出不同的所有权转换协议。一种仅使用了伪随机噪声发生器(PRNG, pseudorandom noise generator)和循环冗余码校验(CRC, cyclic redundancy check),但该协议容易受到 DoS 攻击;另一种为移动 RFID 设计的方案^[15]发现不能抵制服务器、读卡器和标签的假冒攻击和追踪攻击^[16]。Zuo 等^[17]提出了一种群组所有权转换协议,但该协议不能抵抗去同步攻击^[18]。在文献[19~22]中,没有一个方案能同时满足采用 TTP,适应于多标签多所有者又能保证所有者隐私的。尽管文献[22]采用了 TTP,但该方案需要标签使用 PRNG 生成新密钥,由于标签的局限性,它可能不能执行这一重要功能。文献[23]在文献[21]的基础上,提出了一种针对多标签多所有者且能保护所有者隐私的安全所有权转换协议。张学军等^[24]根据阅读器产生的随机数对将要传送的信息进行循环左移,提出了基于循环移位的轻量型相互认证协议,并用 GNY 逻辑对协议的安全性进行了证明。贺蕾等^[25~27]分别提出使用随机排列函数的所有权转换协议对标签进行授权访问,以及轻量级 RFID 标签所有权匿名安全转换协议。但以上这些协议大多是针对单所有者标签的所有权转换,只有少量针对的是多所有者标签的所有权转换,但其多所有者的份额或权重是一样的,这些协议并不适应于具有不同权重的多所有者标签所有权转换。

2.2 密钥共享门限方案

在多所有者 RFID 标签进行所有权转换时,往往要用到秘密共享门限算法。秘密共享门限方

案领域内的研究工作起源于 Shamir^[28]和 Blakley^[29]分别基于 Lagrange 插值法和多维空间点独立提出的 (t, n) 秘密共享门限算法。在 (t, n) 门限秘密共享中, 密钥分发者首先将密钥分割成 n 份子密钥, 然后将这 n 份子密钥分发给标签的 n 个所有者, 当需要恢复出密钥时, 至少有 t 个所有者合作恢复密钥。而如今秘密共享方案有很多种, 如可验证的密钥共享门限方案、动态的密钥共享方案、理性的密钥共享方案以及多密钥共享门限方案等。但目前所提出的这些密钥共享门限方案并不完全适应于带有不同权重的多所有者的标签所有权转换。

因此, 针对具有不同权重的多所有者所有权的转换, 提出了一种带有权重的多所有者 RFID 标签所有权动态转换协议, 该协议使用秘密共享方案管理密钥, 利用拉格朗日公式根据所有者的权重对标签密钥进行恢复和再分发, 当标签所有者发生变化时能及时动态地更新密钥, 以保证标签的安全性和使用的灵活性。

3 方案描述

一个完整的标签所有者转换协议, 首先, 要保证新所有者能得到标签的所有相关信息 (包括控制权); 其次, 要保证原所有者不能再对标签进行任何操作, 新所有者也不能查询之前的数据, 要确保原所有者和新所有者的隐私安全; 最后, 还有满足 RFID 系统的其他安全和隐私性要求。根据以上条件, 本文设计采用基于拉格朗日密钥共享方案实现带有不同权重的多所有者标签所有权转换协议。

3.1 主要思想

在标签生命周期内, 不同所有者所占有的权重可能会发生变化, 有些所有者会出售自己所持有的权重, 还有些实体通过购买权重成为标签新的所有者之一。当标签的多个所有者权重发生变化或者有新的实体成为所有者时, 本文设计采用基于拉格朗日公式的 (w, t) 秘密共享门限方案实现带有不同权重的多所有者标签所有权的动态转换。即当多个所有者的权重总和为 w 时, 只有当参与恢复密钥的所有者权重之和等于或大于 t 时, 才能根据拉格朗日公式

$$f(0) = \sum_{i=1}^t y_i \left\{ \prod_{1 \leq j \leq t, i \neq j} \frac{0 - x_j}{x_i - x_j} \right\}$$

得出所共享的密钥, 否则不能恢复出密钥。若成功恢复密钥, 则立即更新密钥, 确保原所有者密钥的失效。然后根据密钥共享方案将标签的新密钥分成多个子密钥, 即需要标签任意选择 $t-1$ 个元素 $a_1, a_2, \dots, a_{t-1}$, 构造 $t-1$ 次多项式

$$f(x) = S_{\text{new}} + \sum_{i=1}^{t-1} a_i x^i$$

其中, S_{new} 为要共享的密钥。根据所有者的新权重 w_{ni} 为其分配相应的秘密份额

$$S_{ij} = f(x_{ij}), i \leq j \leq w_{ni}$$

其中, $x_{ij} = (i-1) m + j$, m 为参与方权重的上界。

因此, 加强了标签在所有权转换的安全性和实际运用中的灵活性。

3.2 系统初始化

设 $P = \{P_1, P_2, \dots, P_n\}$ 为标签的 n 个所有者, PID_i 为所有者 P_i 的唯一标识, w_i 为所有者 P_i 相应的权重, w_{ni} (上界为 m) 为所有者 P_i 新一轮对应的权重值, Q_1 为标签的新所有者, QID_1 为新所有者 Q_1 的唯一标志, Tag 代表标签, TID 代表标签的唯一标识, S 代表与原所有者通信的密钥, $S_{ij} (1 \leq j \leq w_i)$ 代表不同权重的所有者具有不同数量的子密钥, S_{nij} 代表所有权发生变化后各所有者通信得到的子密钥。

3.3 权重购买过程

假设一个标签 Tag 有 3 个所有者, 即 P_1, P_2, P_3 , 他们的权重各自分别为 1、1、2, 并且所有者之间的通信信道是安全的。具体的购买过程如图 1 所示。

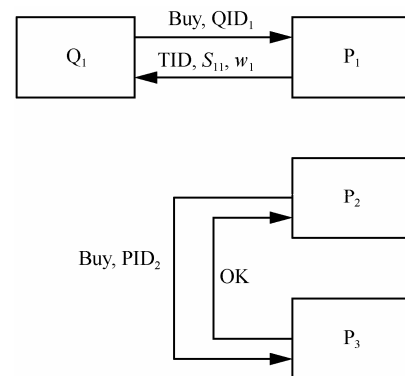


图 1 权重购买过程

从图1可以看出：当新实体 Q_1 向权重值为1的所有者 P_1 购买权重成为新的所有者时，新实体 Q_1 需要向原所有者 P_1 发送 Buy 请求，同时将自己的标识 QID_1 传给 P_1 ，如果原所有者 P_1 同意该申请，就将其权重值 w_1 、子密钥 S_{11} 以及标签的标识 TID，通过安全信道发送给新所有者 Q_1 ；权重为1的所有者 P_2 也向权重为2的所有者 P_3 购买部分权重，此时 P_2 也需要给 P_3 发送一个 Buy 请求，并带上自己的唯一标识 PID_2 ，如果所有者 P_3 同意该交易，将给原所有者 P_2 发送一个 OK 作为应答。所以，不仅原所有者之间的权重发生变化，同时还有新的实体成为新所有者。

3.4 所有权转换过程

当标签的所有者出售自己的权重，即标签所有者的权重或所有者发生变化后，所有者需要完成与标签之间的认证，并恢复出原有密钥 S 。当标签的所有者和权重都发生变化时，需要更新密钥。具体的认证恢复过程如图2所示。

1) 新所有者 Q_1 向原所有者 P_1 购买权重，成为新的所有者，生成随机数 R_{o1} ，向标签 Tag 发送请求。

2) 标签在收到 Q_1 发送的请求后，生成一个随机数 R_{r1} ，并计算 $M=H(TID \oplus R_{o1} \oplus R_{r1})$ ，将 M 和 R_{r1} 同时发送给 Q_1 。

3) 所有者 Q_1 收到消息后，用 R_{r1} 、 R_{o1} 和来自 P_1 的 TID 计算，如果存在 $H(TID \oplus R_{o1} \oplus R_{r1})=M$ ，则通过对标签的认证。所有者 Q_1 生成随机数 R_{r1} ，

并将 $H(R_{r1} \oplus R_{r1}) \oplus S_{11}$ 、 $H(R_{r1} \oplus R_{r1}) \oplus w_{n1}$ 、 $H(R_{r1} \oplus R_{r1}) \oplus w_1$ 、 R_{r1} 发送给标签 Tag。同样，当原所有者 P_2 、 P_3 验证标签后，分别将 $H(R_{r2} \oplus R_{r2}) \oplus S_{21}$ 、 $H(R_{r2} \oplus R_{r2}) \oplus w_{n2}$ 、 $H(R_{r2} \oplus R_{r2}) \oplus w_2$ 、 R_{r2} ，以及 $H(R_{r3} \oplus R_{r3}) \oplus S_{31}$ 、 $H(R_{r3} \oplus R_{r3}) \oplus S_{32}$ 、 $H(R_{r3} \oplus R_{r3}) \oplus w_{n3}$ 、 $H(R_{r3} \oplus R_{r3}) \oplus w_3$ 、 R_{r3} 发送给标签 Tag。

4) 标签收到所有者发送的消息后，首先计算参与恢复密钥所有者权重之和，当权重之和大于或等于门限值时才根据拉格朗日公式算法恢复出所有权转换密钥 S' ，此时用标签的密钥 S 与拉格朗日公式恢复出的密钥 S' 进行比较，若 $S=S'$ ，则该新所有者和原所有者都是合法的，即完成了双向验证，且恢复出标签的密钥 S 。

5) 标签更新密钥 S_{new} ，密钥共享方案将根据所有者新的权重值将标签的新密钥分成多份子密钥 S_{n11} 、 S_{n21} 、 S_{n22} 、 S_{n31} ，同时生成随机数 R_{n1} 、 R_{n2} 、 R_{n3} ，然后分别将各子密钥经过散列加密，即将 $H(R_{r1} \oplus R_{n1}) \oplus S_{n11}$ 、 $H(R_{r2} \oplus R_{n2}) \oplus S_{n21}$ 、 $H(R_{r2} \oplus R_{n2}) \oplus S_{n22}$ 、 $H(R_{r3} \oplus R_{n3}) \oplus S_{n31}$ 分发给各个所有者。

4 安全性分析

该方案在进行 RFID 标签所有权转换时，不仅实现了所有权的完全转换，即原所有者不能再对标签进行任何操作，新所有者获得标签的所有信息，得到标签的所有权，从而保证了前向和后向安全性，以及在转换过程中面临的安全问题，下面从以下几个方面对该协议进行分析验证。

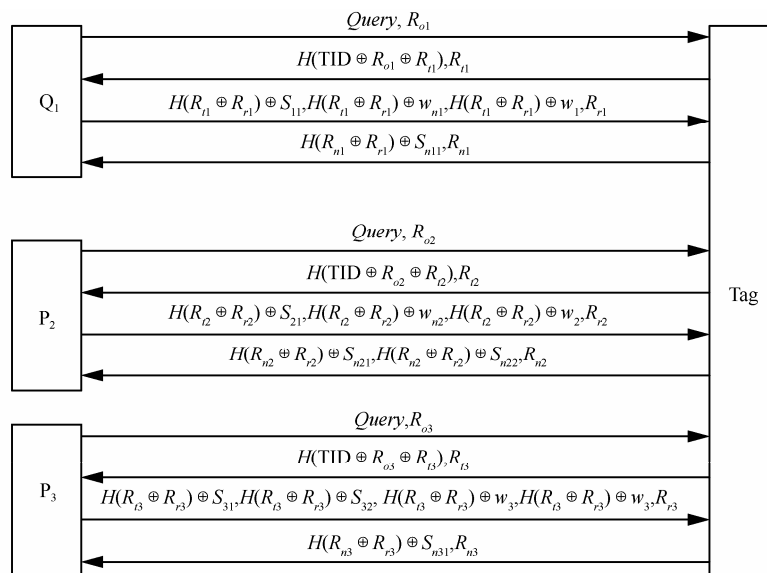


图2 RFID 标签所有权转换

1) 前向安全和后向安全

当所有权发生变化时, 标签就会更新密钥, 原有密钥就会失效, 使原所有者不能继续访问标签, 以保证后向安全。新所有者也只能得到它所购买的子密钥, 并不能恢复出密钥对标签进行查询以保证前向安全。

2) 假冒攻击

攻击者伪装成合法的所有者向标签发送 *Query* 和 R_{o1} , 攻击者获取标签的响应 $M = H(TID \oplus R_{o1} \oplus R_{i1})$ 、 R_{i1} , 在下次认证会话中, 当真正合法的所有者发送 *Query* 和 R'_{o1} 的时候, 攻击者伪装成合法标签响应 $M = H(TID \oplus R_{o1} \oplus R_{i1})$ 、 R_{i1} , 但由于在每一次认证会话中都产生一个随机数, 即 $R_{o1} \neq R'_{o1}$ 。因此, 真正合法的所有者不能验证 M , 协议将会终止。这样, 攻击者就无法假冒合法标签进行假冒攻击。

3) 重传攻击

在所有者向标签发送 *Query* 和 R_{o1} 之后, 攻击者获取标签的响应 $M = H(TID \oplus R_{o1} \oplus R_{i1})$ 、 R_{i1} , 在以后的认证会话中, 攻击者多次给所有者发送 $M = H(TID \oplus R_{o1} \oplus R_{i1})$ 、 R_{i1} , 从而实现重传攻击。但由于每次都会产生一个新的随机数, 所以所有者每次发送的查询和标签响应都不同。因此, 攻击者重复发送相同的消息是无法通过认证的。

4) 追踪

在伪装成合法的所有者向标签发送 *Query* 和 R_{o1} 之后, 攻击者获取标签的响应 $M = H(TID \oplus R_{o1} \oplus R_{i1})$ 、 R_{i1} , 并通过分析该响应来追踪发出该响应的标签。由于在每一次认证会话中, 标签都产生新的随机数 R'_{i1} , 加上 Hash 操作是单向安全的, 攻击者也就无从得知所收到的是哪个标签的响应 $H(TID \oplus R_{o1} \oplus R_{i1})$ 、 R_{i1} 。

5) 抗中间人攻击

在标签所有权转换的整个过程中都加入了双向认证, 因此攻击者无法通过身份伪装来获取消息实现攻击。

5 仿真实验

本文在 Linux 系统下对该协议进行仿真实验, 实验平台用的 CPU 为 3.60 GHz, 内存为 4 GB。本文进行了 3 次实验, 第 1 次是所有者的权重总和为 4, 参与恢复者权重和为 3; 第 2 次是所有者的权重总和为 8, 参与恢复者权重和为 6; 第 3 次

是所有者的权重总和为 10, 参与恢复者权重和为 8。这 3 次实验主要获取不同权重下进行所有权转换标签来计算所消耗的时间, 如图 3 所示。

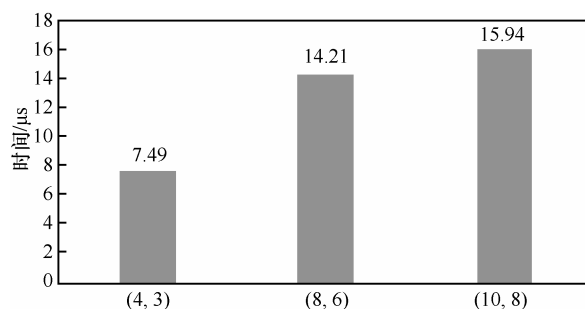


图3 RFID 标签在所有权转换过程中的计算耗时

从图 3 可以看出, 标签所用的计算时间随着需要参与恢复密钥的所有者权重的门限值增多而增大; 所需权重和偏大时标签在所有权转换过程中消耗时间也较少, 因此该协议适合计算能力有限的标签。

6 结束语

本文提出了一种支持标签与多个具有不同权重所有者之间所有权动态转换的协议, 该协议使用了基于拉格朗日公式的密钥共享门限方案。当标签所有者之间权重发生变化或有新的实体成为新所有者时, 该新所有者需要联合原所有者使其权重之和大于门限值, 再根据拉格朗日公式恢复出密钥实现双向的相互认证, 然后更新密钥, 通过密钥共享方案将新密钥分成多份, 再根据所有者新的权重值重新分发子密钥。该协议不仅能保护标签信息的前向安全、后向安全, 而且能抵御中间人攻击和重放攻击。对该协议进行了仿真实验, 实验结果表明该协议中标签的计算耗时较短, 适用于低成本标签。

参考文献:

- [1] RAY B, CHOWDHURY M U, PHAM T. Mutual authentication with malware protection for a RFID system[C]//The International Conference on Advances in Distributed and Parallel Computing ADPC. 2010:24-29.
- [2] SONG B, MITCHELL C J. Scalable RFID security protocols supporting tag ownership transfer[J]. Computer Communications, 2011, 34(4):556-566.
- [3] ERGULER I, ANARIM E. Security flaws in a recent RFID delegation protocol[J]. Personal & Ubiquitous Computing, 2012, 16(3): 337-349.

- [4] TRUJILLO-RASUA R, SOLANAS A, PÉREZ-MARTÍNEZ P A, et al. Predictive protocol for the scalable identification of RFID tags through collaborative readers[J]. *Computers in Industry*, 2012, 63(6):557-573.
- [5] IMRAN E, EMIN A, GOKAY S. A salient missing link in RFID security protocols[J]. *Eurasip Journal on Wireless Communications & Networking*, 2011(1): 5412-5483.
- [6] 周永彬, 冯登国. RFID 安全协议的设计与分析[J]. *计算机学报*, 2006, 29(4):581-589.
ZHOU Y B, FENG D G. Design and analysis of cryptographic protocols for RFID[J]. *Chinese Journal of Computers*, 2006, 29(4): 581-589.
- [7] OSAKA K, TAKAGI T, YAMAZAKI K, et al. An efficient and secure RFID security method with ownership transfer[C]//*Computational Intelligence and Security*. 2006:1090-1095.
- [8] KAPOOR G, PIRAMUTHU S. Single RFID tag ownership transfer protocols[J]. *IEEE Transactions on Systems Man & Cybernetics Part C Applications & Reviews*, 2012, 42(2):164-173.
- [9] FOULADGAR S, AFIFI H. A simple privacy protecting scheme enabling delegation and ownership transfer for RFID tags[J]. *Journal of Communications*, 2007, 2(6): 6-13.
- [10] JÄPPINEN P, HÄMÄLÄINEN H. Enhanced RFID security method with ownership transfer[C]//*International Conference on Computational Intelligence and Security*. 2008: 382-385.
- [11] KAPOOR G, PIRAMUTHU S. Vulnerabilities in some recently proposed RFID ownership transfer protocols[J]. *Communications Letters IEEE*, 2010, 14(14):354-357.
- [12] DIMITRIOU T. RfidDOT: RFID delegation and ownership transfer made simple[C]//*The International Conference on Security and Privacy in Communication Networks*. 2008:1-8.
- [13] KULSENG L, YU Z, WEI Y, et al. Lightweight mutual authentication and ownership transfer for RFID systems[C]//*IEEE Infocom*. 2010:1-5.
- [14] CHEN C L, HUANG Y C, JIANG J R. A secure ownership transfer protocol using EPCglobal Gen-2 RFID[J]. *Telecommunication Systems*, 2013, 53(4):387-399.
- [15] CHEN C L, CHIEN C F. An ownership transfer scheme using mobile RFIDs[J]. *Wireless Personal Communications an International Journal*, 2013, 68(3):1093-1119.
- [16] MUNILLA J, GUO F, SUSILO W. Cryptanalysis of an EPCC1G2 standard compliant ownership transfer scheme[J]. *Wireless Personal Communications*, 2013, 72(1):245-258.
- [17] ZUO Y. Changing hands together: a secure group ownership transfer protocol for RFID tags[C]//*Hawaii International Conference on System Sciences*. 2010:1-10.
- [18] JANNATI H. Cryptanalysis and enhancement of a secure group ownership transfer protocol for RFID tags[J]. *Lecture Notes of the Institute for Computer Sciences Social Informatics & Telecommunications Engineering*, 2011(99):186-193.
- [19] DOSS R, ZHOU W, YU S. Secure RFID Tag ownership transfer based on quadratic residues[J]. *IEEE Transactions on Information Forensics & Security*, 2013, 8(2):390-401.
- [20] YANG M H, HU H Y. Protocol for ownership transfer across authorities: with the ability to assign transfer target[J]. *Security & Communication Networks*, 2012, 5(5):164-177.
- [21] SUNDARESAN S, DOSS R, ZHOU W. Secure ownership transfer in multi-tag/multi-owner passive RFID systems[C]//*Global Communications Conference*. 2013:2891-2896.
- [22] XIN W, GUAN Z, YANG T, et al. An efficient privacy-preserving RFID ownership transfer protocol[M]//*Web Technologies and Applications*. Berlin: Springer, 2013:538-549.
- [23] SUNDARESAN S, DOSS R, ZHOU W, et al. Secure ownership transfer for multi-tag multi-owner passive RFID environment with individual-owner-privacy[J]. *Computer Communications*, 2015, 55:112-124.
- [24] 张学军, 王玉, 王锁萍, 等. 基于循环移位的轻量型相互认证协议研究[J]. *电子学报*, 2012, 40(11):2270-2275.
ZHANG X J, WANG Y, WANG S P, et al. Research on the cyclic shift lightweight mutual authentication protocol[J]. *Acta Electronica Sinica*, 2012, 40(11):2270-2275.
- [25] 贺蕾, 甘勇, 尹毅峰, 等. 基于随机排列函数的 RFID 标签所有权转换协议[J]. *郑州大学学报:工学版*, 2013, 34(6):24-27.
HE L, GAN Y, YIN Y F, et al. Ownership transfer protocol of RFID tags based on random permutation functions[J]. *Journal of Zhengzhou University (Engineering Science)*, 2013, 34(6):24-27.
- [26] 贺蕾, 甘勇, 尹毅峰, 等. 一种 RFID 标签授权访问和所有权转换协议[J]. *合肥工业大学学报*, 2014(2):172-175.
HE L, GAN Y, YIN Y F, et al. A delegation and ownership transfer protocol of tag in RFID system[J]. *Journal of Hefei University*. 2014(2): 172-175.
- [27] 甘勇, 李天豹, 贺蕾, 等. 基于动态重载的 RFID 标签所有权转换协议研究[J]. *轻工学报*, 2016, 31(2): 97-102.
GAN Y, LI T B, HE L, et al. Study of RFID tag ownership transfer protocol based on dynamic overloading[J]. *Journal of Light Industry*, 2016, 31(2): 97-102.
- [28] SHAMIR A. How to share a secret[C]//*Communications of the ACM*. 1976:612-613.
- [29] BLAKLEY G R. Safeguarding cryptographic keys[C]//*The 1979 AFIPS National Computer Conference*. 1979:313-317.

作者简介:



甘勇 (1965-), 男, 湖南株洲人, 博士, 郑州轻工业学院教授、硕士生导师, 主要研究方向为物联网安全。

杨宗琴 (1993-), 女, 河南信阳人, 郑州轻工业学院硕士生, 主要研究方向为物联网安全。

贺蕾 (1983-), 男, 河南三门峡人, 郑州轻工业学院副教授、硕士生导师, 主要研究方向为密码学、物联网安全。

杜超 (1988-), 男, 河南濮阳人, 郑州轻工业学院硕士生, 主要研究方向为物联网安全。

刘思聪 (1985-), 男, 河南郑州人, 郑州轻工业学院硕士生, 主要研究方向为物联网技术与安全。