

改进型 RFID 相互认证协议研究

张学军^{1,2}, 陈彦君¹, 常 昆¹

(1. 南京邮电大学 电子科学与工程学院, 江苏 南京 210003;

2. 南京邮电大学 宽带无线通信与传感网技术教育部重点实验室, 江苏 南京 210003)

摘 要:随着射频识别(RFID)技术的发展和广泛应用,RFID 系统的安全性成为了研究的热点,但是由于标签有限的计算能力和存储能力,安全协议的设计成为了保证 RFID 系统安全的关键。文章对 SYK 协议的安全性进行了分析,针对其存在的多个安全漏洞进行改进,提出了一种改进型的 RFID 相互认证协议。安全性能分析表明,改进后的协议通过标签和数据库的信息同步更新和散列函数加密,解决了 SYK 协议的安全隐私问题,满足基本的安全性能,可以抵制跟踪、去同步、重传等多种攻击,提高了 RFID 系统的安全性。

关键词:射频识别技术;相互认证协议;散列函数;安全

中图分类号: TN92

文献标识码: A

文章编号: 1673-629X(2013)08-0129-04

doi:10.3969/j.issn.1673-629X.2013.08.033

An Improved RFID Mutual Authentication Protocol

ZHANG Xue-jun^{1,2}, CHEN Yan-jun¹, CHANG Kun¹

(1. College of Electronic Science and Engineering, Nanjing University of Posts and Telecommunications,
Nanjing 210003, China;

2. Key Laboratory of Broadband Wireless Communication and Sensor Network Technology of Ministry of Education,
Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: With the radio frequency identification (RFID) technology developed and widely used, the safety of the RFID system becomes the focus of research, but the design of security protocols becomes the key to ensure the safety of RFID system because of the limited computing and storage capacity of the tag. In this paper, analyzing the safety performance and improving the security multi-vulnerabilities existed in the SYK protocol, an improved RFID mutual authentication protocol is proposed. Safety performance analysis shows that the proposed protocol solves the privacy problem of the SYK protocol through the synchronous updating of the information and hash function of encryption, meeting the basic safety requirements and overcoming various attacks, such as tracking de-synchronization and replay attack. The security of the RFID system is strengthened.

Key words: radio frequency identification; mutual authentication protocol; hash function; security

0 引 言

射频识别(Radio Frequency Identification, RFID)是一种非接触式的自动识别技术。作为一种快速的、实时的、准确的采集和处理信息的高新技术已广泛地应用于各种领域,尤其是应用于零售业的系统价格标识中,从制造商到仓存再到零售商的整个供应链过程中,RFID 技术能够对整个供应链中的货物进行跟踪^[1,2]。

典型的 RFID 系统由阅读器 R (Reader)、标签 T

(Tag)和后端服务器 DB (DataBase)三部分组成。标签包括主动式、被动式、半被动式。主动式标签使用内置电源来不间断地给标签和射频通信线路提供能量;被动式标签依靠阅读器发出的射频信号给标签提供能量;半被动式标签使用内置电源提供监控环境的变化,但需从阅读器发射的射频信号获取能量,以便标签对阅读器做出响应^[3]。标签与阅读器的信道称为“反向信道”(backward channel),阅读器与标签的信道称为“前向信道”(forward channel)。

收稿日期:2012-11-02

修回日期:2013-01-30

网络出版时间:2013-04-22

基金项目:国家自然科学基金资助项目(60973140,61001077,61170276);南京邮电大学自然科学基金项目(NY211076)

作者简介:张学军(1969-),男,江苏南通人,副教授,硕导,博士,研究方向为无线射频识别技术、通信网络的性能分析、流量控制、QoS 理论与技术等;陈彦君(1987-),女,硕士研究生,研究方向为无线射频识别技术。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20130422.1727.054.html>

文中研究被动式标签的安全认证协议,假设后端服务器与阅读器之间的信道是安全的,阅读器与标签的信道是不安全的。

1 相关工作

RFID 系统常见的安全威胁包括重传攻击、去同步攻击、标签跟踪、不可分辨性、前向安全性、拒绝服务攻击等,能否抵御上述攻击是评价 RFID 系统的重要指标。RFID 系统的安全机制包括物理机制、密码机制及两者相结合的机制三种^[1]。密码机制是当前 RFID 安全研究的热点,例如低成本的加密协议^[4]、Hash-Lock 协议^[5]、随机化 Hash-Lock 协议^[6]、基于 EPC global 标准的协议^[7],其中低成本的安全协议采用简单逻辑加密。

RFID 系统中抵制安全攻击方法包括:标志位标识 DB 与 T 同步,密钥等分、分别更新,散列函数加密等。采用标志位方法的协议包括低成本强安全的 RFID 认证协议 (Low-Cost and Strong-Security RFID Authentication Protocol)^[8]在 T 中使用标志位 sync、低成本的相互认证协议 (A Lightweight Authentication Protocol for Low-Cost RFID)^[9]在 DB 中使用标志位。使用密钥等分方法的协议包括 SASI^[10]、EMAP^[4] 协议。使用散列函数加密的协议包括 Song-Mitc hell 认证协议^[11],所有权转移的两个安全问题 (Two Security Problems of RFID Security Method with Ownership Transfer)^[12],对有效认证协议的攻击 (Attacks on an Efficient RFID Authentication Protocol)^[13]等,经过散列函数加密后的信息不能被篡改,增强了系统的安全性。

参考文献[14]中提出了一种低成本相互认证协议(以下简称 SYK 协议)。

SYK 协议采用简单逻辑进行加密,其认证过程如图 1 所示。

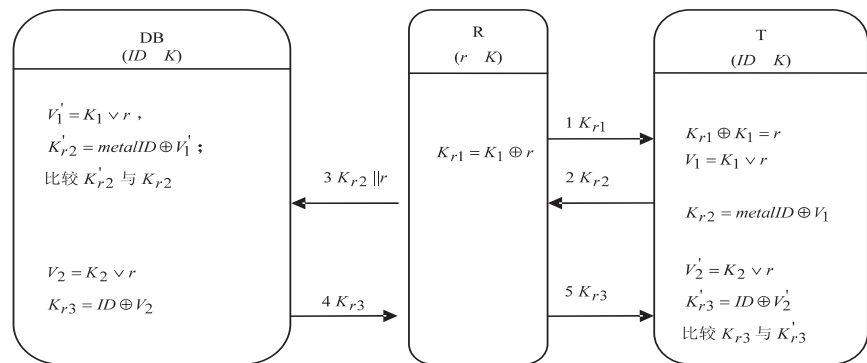


图 1 SYK 协议认证过程

SYK 协议可以实现相互认证,但标签和数据库中的信息没有同步更新,不能满足基本的安全要求。文中第二部分详细分析了 SYK 协议存在的安全漏洞,提出了一种改进型相互认证协议 (An Improved Mutual Authentication Protocol, IMAP),并对 IMAP 协议的安

全性能进行了分析。

2 SYK 协议安全性分析

SYK 协议不能抵制标签跟踪、不可分辨性、前向安全、去同步攻击。具体攻击步骤为:

(1) 标签跟踪。

攻击者窃取标签和阅读器之间的信息 K_{r1} 、 K_{r2} 后通过两种方式实现对标签的跟踪。

方式一:攻击者随机选择两个标签 T_1 、 T_2 ,成功地分辨出标签并实现跟踪,跟踪过程包括学习阶段和挑战阶段。

学习阶段:阅读器与标签 T_1 通信的同时,攻击者窃取阅读器 R 与标签 T_1 之间的信息 K_{r1} 、 K_{r2} ,并保存标签 T_1 的信息 K_{r1} 、 K_{r2} 。通信结束后,阅读器和标签中信息都没有更新,密钥 K 保持不变。如果 K_{r1} 不变,根据 $K_{r1} \oplus K_1 = r$, r 不变,由于 $V_1 = K_1 \vee r$, $K_{r2} = h(\text{metalID} \oplus V_1)$,则 K_{r2} 不变,攻击者将保存的 K_{r1} 发送给攻击的对象,判断接收的 K_{r2} 是否变化实现跟踪。

挑战阶段:攻击者假冒阅读器 R 与标签 T_1 、 T_2 中任意一个标签 T 通信,攻击者将 K_{r1} 发送给标签 T 。标签 T_1 接收到 K_{r1} 后,响应值为 K'_{r2} , $K'_{r2} = K_{r2}$;标签 T_2 接收到 K_{r1} 后,计算 $K_{r1} \oplus K'_1 = r \oplus K_1 \oplus K'_1$, $V_1 = K_2 \vee (r \oplus K_1 \oplus K'_1)$, $K'_{r2} = \text{metalID} \oplus V_1$,响应 K'_{r2} ,每个标签的密钥 K 不同,因此 $K'_{r2} \neq K_{r2}$ 。攻击者根据 K_{r2} 、 K'_{r2} 、 K'_{r2} 判断出 $T = T_1$ 、 $T \neq T_2$,实现了对标签的跟踪。

更进一步,攻击者将 K_{r1} 分别发送给多个标签时,所有的标签根据接收到的 K_{r1} 分别响应不同的 K_{r2} 值,攻击者根据响应值与自身的保存的 K_{r2} 比较,若相等,就成功地分辨出标签 T_1 ,并实现跟踪。

方式二:若攻击者窃取了 K_{r1} 、 K_{r2} 、 r ,计算 $K_{r1} \oplus r =$

K_1 ,而 K_1 在相互认证后并没有更新,因此攻击者可以计算 $V_1 = K_1 \vee r$, $K_{r2} \oplus V_1 = \text{metalID}$ 获得 metalID。攻击者虽然不能从 metalID 中获得 ID,但 ID 在相互认证后没有更新,metalID 保持不变,就实现了对标签的跟踪。因此 SYK 协议不满足不可分辨性,标签易被追踪。

(2) 前向安全。

如果攻击者获得了标签和阅读器当前会话的密钥 K ,但 SYK 协议没有密钥更新机制,攻击者也就获得了之前的密钥,因此 SYK 协议不满足前向安全性。

(3) 去同步攻击。

增加密钥更新后的 SYK 协议可以抵制标签跟踪

和前向安全攻击,但是 T 与 R 之间传输的信息 $K_{r2} = \text{metalID} \oplus V_1, K_{r3} = \text{ID} \oplus V_2$,仅使用异或操作,易被篡改,会导致去同步攻击,实施去同步攻击的方法有两种。

方法一:数据库 DB 参数更新后,将 K_{r3} 发送给阅读器 R 和标签 T 。如果攻击者阻止 K_{r3} 从阅读器 R 发送给标签 T ,这时标签 T 无法成功认证数据库 DB,标签中的信息无法更新,数据库 DB 与标签 T 失去同步。下一次会话,数据库 DB 将无法成功地认证标签 T 。

方法二:阅读器 R 将 K_{r3} 发送给标签 T 的过程中被篡改,假设攻击者将 $K_{r3} = \text{ID} \oplus V_2$ 篡改改为 $K'_{r3} = \text{ID} \oplus V_2 \oplus x$,标签 T 接收的信息是 K'_{r3} 。 T 计算 $K'_{r3} \oplus V_2 = \text{ID}' \oplus x$, ID' 与 ID 不相等,标签 T 无法成功地认证数据库 DB,导致数据库 DB 中的信息更新成功,而标签 T 中的信息无法更新,数据库 DB 与标签 T 失去同步。下一次会话时,数据库 DB 就无法认证标签 T 。

3 改进型相互认证协议——IMAP 协议

3.1 IMAP 协议过程

IMAP 协议使用或 (\vee)、异或 (\oplus)、串联 (\parallel)、单向散列 Hash 函数加密,满足基本的安全要求,参数如表 1 所示。

表 1 IMAP 协议参数列表

参数	含义
K_i	第 i 个密钥值, $i = 1, 2$
ID	标签的唯一的识别码
metalID	$h(\text{ID})$, ID 的散列函数
\vee	对应的位进行或操作
r	阅读器产生的随机数
V_1	$K_1 \vee r$ 的值
V_2	$K_2 \vee r$ 的值

DB 中存储 ID_{old} 、 ID_{new} 、 K_{old} 、 K_{new} 、1bit 的标志位 f ;阅读器与标签共享密钥 K ; T 中存储 ID 、 K 。其中 ID_{old} 、 ID_{new} 、 K_{old} 、 K_{new} 、ID 长度是 l bit, K_1 、 K_2 分别是 K 的 $1 - l/2$ bit 和 $l/2 - 2$ bit, IMAP 协议认证过程如图 2 所示。

IMAP 协议与 SYK 协议相比,增加了标签和数据库的同步更新和标志位 f 。

$f = 1$, 说明 DB 在 K_{new} 域成功地认证了 T , 表明上次会话后, DB 和 T 中的信息都成功地进行了更新, DB 与 T 保持同步。

$f = 0$, 说明 DB 在 K_{old} 域成功地认证了 T , 表明上次会话后, DB 中的信息成功更新而 T 中的信息没有更新, DB 与 T 失去同步。

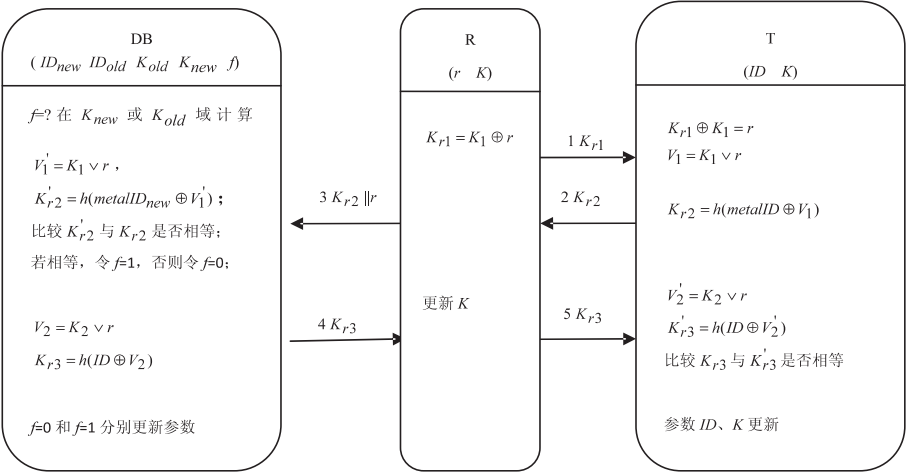


图 2 IMAP 协议的认证过程

阅读器再次与标签通信时, DB 先判断标志位 f , 若 $f = 1$, DB 直接在 K_{new} 域认证标签; 若 $f = 0$, DB 不需要搜索 K_{new} 域, 直接在 K_{old} 域认证 T , 提高了标签的识别效率。

IMAP 协议认证过程为:

(1) 阅读器 R 产生一个随机数 r , 与 K_1 计算 $K_{r1} = K_1 \oplus r$, 阅读器 R 将 K_{r1} 发送给标签 T 。

(2) 标签 T 接收到 K_{r1} 后, 与自身的 K_1 计算 $K_{r1} \oplus K_1 = r$ 获得阅读器的随机数 r , 根据 r 计算 $V_1 = K_1 \vee r$, $K_{r2} = h(\text{metalID} \oplus V_1)$, T 将 K_{r2} 发送给阅读器 R 。

(3) 阅读器 R 将 K_{r2} 、 r 发送给数据库 DB。DB 根据接收到的 K_{r2} 、 r , 验证标签 T , 验证过程包括两步。

第一步: 首先 DB 在 K_{new} 域计算 $V'_1 = K_1 \vee r$, $K'_{r2} = h(\text{metalID}_{\text{new}} \oplus V'_1)$, K'_{r2} 与接收到的 K_{r2} 比较。如果 $K'_{r2} = K_{r2}$, DB 成功认证 T , 此时令 $f = 1$, 否则进行第二步。

第二步: 如果 $K'_{r2} \neq K_{r2}$, 说明上一次会话后, DB 中标签的信息没有成功地更新。DB 重新在 K_{old} 域计算 $V'_1 = K_1 \vee r$, $K'_{r2} = h(\text{metalID}_{\text{old}} \oplus V'_1)$, 再次比较与 K_{r2} 是否相等。如果相等, DB 成功认证 T , 此时令 $f = 0$; 如果不相等, DB 认证 T 失败, 停止通信。

(4) DB 成功认证标签 T 后, 计算 $V_2 = K_2 \vee r$, $K_{r3} = h(\text{ID} \oplus V_2)$, 并将 K_{r3} 发送给 R 。

DB 更新参数: $f = 1$ 时, 更新参数 $K_{\text{old}} = K_{\text{new}}$, $\text{ID}_{\text{old}} = \text{ID}_{\text{new}}$, $K_{\text{new}} = h(K \parallel r)$, $\text{ID}_{\text{new}} = h(\text{ID} \parallel r)$; $f = 0$ 时, 更新参数 $K_{\text{new}} = h(K \parallel r)$, $\text{ID}_{\text{new}} = h(\text{ID} \parallel r)$ 。

R 更新参数: $K_{\text{new}} = h(K \parallel r)$ 。

(5) R 将 K_{r3} 发送给 T , T 接收到 K_{r3} 后, 认证数据库 DB。

T 计算 $V'_2 = K_2 \vee r$, $K'_{r3} = h(\text{ID} \oplus V'_2)$, 将 K'_{r3} 与接收到的 K_{r3} 比较。如果相等, 标签 T 成功地认证数据库

DB,相互认证成功, T 更新参数 $ID_{new}=h(ID\parallel r),K_{new}=h(K\parallel r)$;若不相等,相互认证失败,标签不更新参数。

3.2 IMAP 协议的安全性分析

相互认证:数据库通过 K_{r_2} 实现了对标签的认证,而标签通过 K_{r_3} 实现了对数据库的认证,因此IMAP协议实现了数据库与标签的相互认证。

不可分辨性:攻击者窃取阅读器与标签 T_1 之间的通信信息 K_{r_1},K_{r_2} 。攻击者随机选择两个标签 T_1,T_2 发送 K_{r_1} ,试图根据接收到 K_{r_2} 的值与自身的 K_{r_2} 比较分辨标签 T_1 是不可能的。因为 K_{r_1},K_{r_2} 与ID、 K,r 有关,ID、 K 每次会话后都会更新,每次会话 K_{r_1},K_{r_2} 值会不同,因此IMAP协议满足标签的不可分辨性。

前向安全性:假设攻击者获得了某一次会话的随机数 r ,并窃取了 K_{r_1},K_{r_2} ,计算 $K_{r_1}\oplus r=K_1$ 得到 K_1 ,而攻击者无法得到 K_2 ,因此无法得到密钥 K ,根据 $K_{new}=h(K\parallel r)$,攻击者无法获得 K_{new} 和标签之前的密钥值 K_{old} ,实现了前向安全。

抵制标签跟踪:如果攻击者获得了一些信息和密钥值 K ,想要推测标签的相关信息实现跟踪是不可能的。由于DB与 T 相互认证后,ID、 K 都进行更新,并且更新后 ID_{new},K_{new} 值与随机数 r 有关,因此每次会话的ID、 K 都是随机的,攻击者通过窃取信息 $K_{r_1},K_{r_2},K_{r_3},K_{old}$ 无法实现对标签的跟踪。

假设攻击者获得本次会话的密钥 K 后,通过计算 $V_1=K_1\vee r,K_{r_2}\oplus V_1=metalID$,获得 $metalID$,由于相互认证后标签的ID更新为 $ID_{new}=h(ID\parallel r)$,而 $metalID=h(h(ID\parallel r))$ 与 r 相关是随机的,攻击者无法实现对标签的跟踪。

抵制重传攻击:阅读器与标签之间传输的信息 K_{r_1},K_{r_2},K_{r_3} 每次会话都会更新,并且都是与随机数 r 相关的,因此攻击者伪装成阅读器或标签都不能重传原来的值认证成功。

抵制去同步攻击:包括两种情况。

情况一: $K_{r_3}=h(ID\oplus V_2)$ 使用散列函数加密不易被篡改,攻击者想通过篡改 K_{r_3} 是不容易的。如果 K_{r_3} 被篡改导致标签的信息无法更新,数据库和标签失去同步,由于DB中保存了 ID_{old},K_{old} ,下一次会话,数据库会通过 ID_{old},K_{old} 成功地认证标签,数据库中的信息不再更新,标签中的信息更新,数据库和标签重新保持同步。

情况二:如果攻击者阻止 K_{r_3} 从阅读器发送给标签,标签无法成功认证数据库,数据库和标签信息失去同步,会采用与第一种情况相同的方法保持同步。

IMAP协议,通过增加信息的更新、 K_{r_2},K_{r_3} 加密方法改进、数据库中增加 ID_{old},K_{old},f 来加强安全性。满

足了相互认证、不可分辨性、前向安全、抵制跟踪、抵制重传攻击、防止去同步等基本要求。IMAP协议与其他协议的安全性能比较如表2所示。

表 2 各个协议的安全性比较

协议 \ 安全性	SASI	SM	YL	HC	IMAP
隐私性					
相互认证					
不可跟踪性					
抵制去同步攻击					
抵制重传攻击					
前向安全					

:表示满足该安全性 :表示不满足 :部分满足

4 结束语

RFID系统以及自身的许多特殊性和局限性带来各种安全问题,基于密码技术的RFID安全协议是一种实现和保护RFID系统安全性的重要方法,也是当前该领域研究的热点问题。设计安全、高效、低成本的实用RFID安全协议具有很大的挑战性,既有应用环境与RFID设备的特殊性和局限性(如:标签成本),也有与已有国际相关标准的兼容性问题。随着可证明安全理论和分析技术的进一步完善,RFID系统的安全性得到进一步的完善。

参考文献:

[1] 丁振华,李锦涛,冯波.基于Hash函数的RFID安全认证协议研究[J].计算机研究与发展,2009,46(4):583-592.

[2] 赵云青,徐文军,张晓华,等.射频识别系统中读写器的设计[J].计算机技术与发展,2012,22(7):238-241.

[3] 杜治国,杨波,欧阳国帧,等.安全的RFID认证协议研究设计[J].计算机工程和设计,2009,30(3):561-565.

[4] 赵跃华,王益维,李晓聪.一种适合于低成本标签的RFID双向认证协议[J].计算机应用研究,2010,27(5):1885-1888.

[5] 白煜,滕建辅,张立毅,等.基于Hash锁的同步强化RFID验证协议[J].计算机工程,2009,35(21):138-139.

[6] Lee K. A Two-Step Mutual Authentication Protocol Based on Randomized Hash - Lock for Small RFID Networks [C]//Proc. of 2010 Fourth International Conference on Network and System Security. Melbourne:[s. n.],2010:527-533.

[7] 尹平,李群祖.基于EPC标准的认证及所有权转移协议[J].电子设计工程,2012,20(2):38-41.

[8] Ha J, Moon S, Nieto J M G, et al. Low-Cost and Strong-Security RFID Authentication Protocol[J]. IFIP International Federation for Information,2007,48(9):795-807.

化抑制作用减小,相电流的变化率变大,电流上升变快,脉冲值更高。根据公式(2)

$$T_e = \frac{1}{2} i^2 \frac{\partial L}{\partial \theta} \quad (2)$$

可知,由于相电流幅值更大,小极宽具有更高的合成转矩,定子齿宽越小,对电机出力就会越有利。但是,这只是考虑了电机出力,没考虑效率、起动转矩以及转矩脉动等问题。

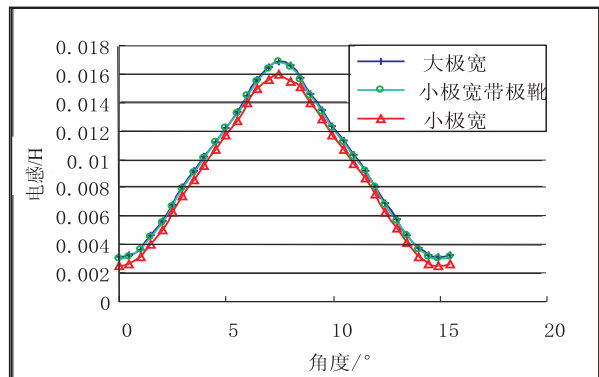


图 5 三种不同齿结构电感曲线

3 结束语

通过起动转矩及过载能力比较,以及电机额定工作点效率比较和效率曲线比较,可以看出,三相 18/24 结构方案相比于三相 36/24 结构方案,综合性能更具有优势。在选择 18/24 结构方案基础上,对电机结构进行定子齿形优化,最后采用带极靴的定子齿结构,此种结构具有起动能力、电机出力、效率等方面的综合优势。文中采用的轮毂电机轴长较短,端部电阻占据比较大,造成铜耗过大,系统效率下降。此外,此电机端部电感对电机性能有较大影响,暂未考虑。综上所述,文中采用三相 18/24 结构 SRM 作为样机方案。

参考文献:

[1] Kalan B A, Lovatt H C, Prout G. Voltage control of switched

reluctance machines for hybrid electric vehicles [C]//PESC Record-IEEE Annual Power Electronics Specialists Conference. [s. l.]: [s. n.], 2002: 1656-1660.

[2] Uematsu T, Wallace R S. Design of a 100 kW switched reluctance motor for electric vehicle propulsion [C]//Proceedings of IEEE Applied Power Electronics Conference and Exposition. [s. l.]: [s. n.], 1995: 411-415.

[3] 刘迪吉. 开关磁阻调速电动机 [M]. 北京: 机械工业出版社, 1994.

[4] Ahn Jin-Woo, Oh Seok-Gyu, Moon Jae-Won, et al. A three-phase switched reluctance motor with two-phase excitation [J]. IEEE Trans. on IA, 1999, 35(5): 1067-1074.

[5] 吴建华. 开关磁阻电机设计与应用 [M]. 北京: 机械工业出版社, 2000: 110-112.

[6] 樊小明, 朱学忠, 刘迪吉. 新型四相关关磁阻电机主电路研究 [J]. 电力电子技术, 1997(2): 6-8.

[7] 詹琼华, 吴莹, 郭伟. 开关磁阻电机绕组连接方式的研究 [J]. 电机与控制学报, 2002, 6(2): 93-95.

[8] Zhang Dong, Dong Lei, Qin Ming, et al. Winding Structure of Switched Reluctance Motor Based on Three-Phase Bridge Converter and Its Influence on Torque Ripple [C]//Proceedings of the 2nd IEEE International Symposium on Power Electronics. [s. l.]: [s. n.], 2010: 626-630.

[9] 周涛, 詹琼华, 王双红. 电动自行车用经济型开关磁阻电动机驱动系统 [J]. 微特电机, 2006(5): 24-26.

[10] Krishnan R. Switched Reluctance Motor Drives: Modeling, Simulation, Analysis, Design, and Applications [M]. [s. l.]: CRC Press, 2001.

[11] 曹志亮, 冬雷, 朱学忠. 电动摩托车用开关磁阻电机控制策略研究 [J]. 微电机, 2000, 33(6): 13-15.

[12] 王长华, 王秩雄, 宋爱民. 一种超宽带天线的分析设计 [J]. 计算机技术与发展, 2009, 19(3): 193-195.

[13] Wang Xilian, Zhang Yihuang, Wang Xudong. Optional-angle Controller of Switched Reluctance Motor Based on EPROM [C]//Proceedings of the Fifth International Conference on Electrical Machines and Systems. [s. l.]: [s. n.], 2001: 600-603.

(上接第 132 页)

[9] Chien Hung-Yu, Huang Chenwei. A Lightweight Authentication Protocol for Low-Cost RFID [J]. Journal of Signal Processing Systems, 2010, 59(1): 95-102.

[10] Phan R C W. Cryptanalysis of a New Ultralightweight RFID Authentication Protocol-SASI [J]. IEEE Transactions on Dependable and Secure Computing, 2009, 6(4): 316-320.

[11] Rizomiliotis P, Rekleitis E. Security Analysis of the Song-Mitchell Authentication Protocol for Low-cost RFID Tags [J]. IEEE Communications Letters, 2009, 13(4): 274-276.

[12] Yoon Eun-Jun, Yoo Kee-Young. Two Security Problems of RFID Security Method with Ownership Transfer [C]//Proc. of

IFIP International Conference on Network and Parallel Computing. China, Shanghai: [s. n.], 2008: 68-73.

[13] Erguler I, Anarim E. Attacks on an Efficient RFID Authentication Protocol [C]//Proc. of 10th IEEE International Conference on Computer and Information Technology. Bradford: [s. n.], 2010: 1065-1069.

[14] Kang Soo-Young, Lee Im-Yeong. A Study on New Low-Cost RFID System with Mutual Authentication Scheme in Ubiquitous [C]//Proc. of IEEE International Conference on Multimedia and Ubiquitous Engineering. Busan: [s. n.], 2008: 527-530.

改进型RFID相互认证协议研究

作者:

张学军, 陈彦君, 常昆, ZHANG Xue-jun, CHEN Yan-jun, CHANG Kun

作者单位:

张学军, ZHANG Xue-jun(南京邮电大学 电子科学与工程学院, 江苏 南京 210003; 南京邮电大学 宽带无线通信与传感网技术教育部重点实验室, 江苏 南京 210003), 陈彦君, 常昆, CHEN Yan-jun, CHANG Kun(南京邮电大学 电子科学与工程学院, 江苏 南京, 210003)

刊名:

计算机技术与发展

ISTIC

英文刊名:

Computer Technology and Development

年, 卷(期):

2013 (8)

本文链接: http://d.g.wanfangdata.com.cn/Periodical_wjtz201308033.aspx