第35卷 第23期 计 算 机 工 程 2009年12月
Vol.35 No.23 Computer Engineering December 2009
·安全技术· 文章编号：1000—3428(2009)23—0144—02 文献标识码：A 中图分类号：TP391

基于混沌序列的RFID安全加密机制

蔡延光，王南生，章 云，周 英
(广东工业大学自动化学院，广州 510006)

摘 要：针对现有RFID系统读写器和标签之间通信安全性低、易受到各种攻击的安全问题，介绍基于Logistic混沌序列的动态实时密钥方法，提出一种基于混沌序列RFID的安全加密机制，采用动态实时密钥对RFID系统中的读写器与电子标签通信消息进行加密。仿真实验结果表明，该方法能够解决RFID系统中非法存取、伪造哄骗、数据泄露、位置跟踪等安全问题。

关键词：消息加密；实时密钥；身份认证

RFID Secure Encryption Mechanism Based on Chaotic Sequence

CAI Yan-guang, WANG Nan-sheng, ZHANG Yun, ZHOU Ying
(College of Automation, Guangdong University of Technology, Guangzhou 510006)

【Abstract】Aiming at secure problem of low communication security and easy to be attacked between reader/writer and labels for existed RFID system, a dynamic real-time key method based on Logistic chaotic sequence is introduced, and a RFID secure encryption mechanism based on chaotic sequence is proposed, which uses dynamic real-time key to encrypt the communication messeges between reader/writer and electronic labels. Simulation experimental results show this method can solve the problems of illegal access, tags forgery, data betray, and position tracking in RFID system.

【Key words】message encryption; real-time key; identity authentication

1 概述

射频识别(Radio Frequency Identification, RFID)技术利用射频方式进行非接触双向通信，以自动识别目标并获取数据。RFID技术解决了无源和免接触两大问题，但是RFID标签具有一些局限性，如有限的计算能力、有限的存储空间、有限的电源供给等。这给RFID系统安全机制的设计带来特殊要求，也使一些高强度的公钥加密机制或认证算法难以在RFID系统中实现。因此，设计安全、高效、低成本的RFID安全协议成为一个新的问题，许多密码学家对此进行研究[1-3]。

RFID系统很容易受到各种攻击，主要由于它的通信过程中没有任何物理或者可见的接触(以电磁波的形式进行)。由于现有读写器和标签之间的无线通信在多数情况下是在不安全信道，以明文方式进行的，未采用任何加密机制，因此攻击者能获取并利用RFID电子标签上的信息[2]。国内外学者提出多种解决方案，旨在解决RFID系统的机密性问题[3-6]。

本文提出一种基于混沌序列的实时密钥对信道加密的安全机制，以解决RFID系统存在的安全隐患，如非法存取、伪造欺骗、数据泄露等。

2 RFID系统存在的安全问题

目前，RFID系统存在的安全隐患有：(1)非法存取：通过未经授权读写器存取标签数据，进行恶意的篡改或非法获取信息。(2)伪造哄骗：通过伪装成合法标签哄骗读写器，为其提供随心所欲数据，达到非授权地出入建筑物或不付费的服务。(3)数据泄露：读写器和标签之间的通信数据被窃听，如泄露ID或其他内容、系统就容易被攻击或者被跟踪、侵犯个人位置隐私与公共安全。

本文提出的RFID安全加密机制，旨在解决以上3个问题。具体措施如下：(1)通过电子标签对读写器的身份认证来防范。(2)通过读写器对电子标签的身份认证来防范。(3)通过对读写器与电子标签的交互消息进行加密(对信道进行加密)。

以上3个措施都需要密钥，密钥用与身份认证和对明文进行加密。要是使用单一的密钥对多次通信进行加密，密钥就容易被分析和攻破。本文提出的安全机制的特点是：读写器与标签之间的通信的每个消息，都采用不用的密钥进行加解密，即动态实时的密钥加密，且这些实时密钥极似随机值，不重复，难于分析攻破(并且实时密钥不在信道中传输，它与消息明文进行叠加形成密文，再发往信道)。这是因为这些实时密钥是一个混沌序列，它们由一个主控密钥(混沌方程的初始值)和一个随机数 R_0 (混沌方程迭代次数)决定的。随机数 R_0 由系统后台数据库提供，这样 R_0 能是真正的随机数，这样做且能节省RFID系统的成本。

3 基于混沌序列实时密钥的产生

由于RFID标签的局限性，因此不可以具有太大的计算能力(标签成本的约束)，本安全机制使用简单的Logistic混沌方程，即

$$X_{n+1} = uX_n(1 - X_n) \tag{1}$$

其中，$u = 4$。

$$X'_{n+1} = uX'_n(1 - X'_n) \tag{2}$$

基金项目：国家自然科学基金资助项目(60374062)；广东省自然科学基金团队资助项目(8351009001000002)；广东省科技计划基金资助项目(2007B010200070)

作者简介：蔡延光(1963－)，男，教授、博士，主研方向：网络控制与优化，组合优化，智能优化，智能决策支持系统；王南生，硕士研究生；章 云，教授、博士、博士生导师；周 英，硕士研究生

收稿日期：2009-07-03 **E-mail：**caiyg99@163.com

其中，$u=4$。式(1)用于读写器方，式(2)用于标签方。

该方程混沌系统迭代产生的时间序列对初始条件敏感，结构复杂难以分析和预测，可以提供具有良好的随机性、相关性、遍历性、复杂性的伪随机序列。混沌时间序列理论上具有类随机性，破坏了相关分析的适用性，保密性得以加强。以 Matlab 仿真为例加以说明该方程的时间序列的随机性和对初始值的敏感性。

当式(1)中的 $X_0=0.1$ 时，混沌序列如图 1 所示。

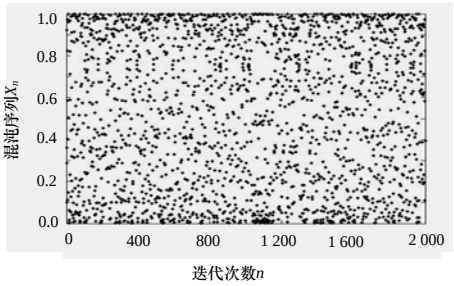

图 1　X_n 的时间序列

从图 1 可以看出，X_n 非常随机地分布在区间[0,1]之间，且具有遍历性。

当式(1)初始值 X_0 取 0.1，式(2)初始值 X_0' 取 0.099 9 时(初始值只具有微小的变化)，X_n 从坐标的 X 轴输出，X_n' 从坐标 Y 轴输出，每迭代一次，显示一个点(X_n, X_n')，如图 2 所示。

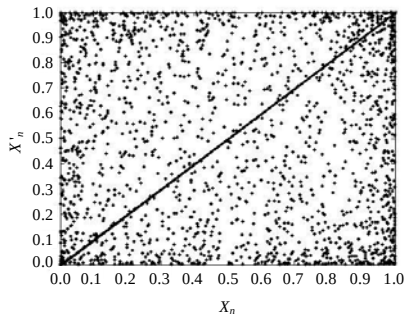

图 2　混沌序列对(X_n, X_n')

从图 2 可以看出，序列对(X_n, X_n')远离对角线 $Y=X$，说明 X_n 与 X_n' 有巨大的差异，即初始值 X_0 的微小变化将导致序列$\{X_n\}$远期行为的巨大差异。由此可知，用 X_0 的初值作为 RFID 系统的主控密钥，混沌序列 X_i 作为加解密时的实时密钥，这样的 RFID 系统的安全性就极高，因为主控密钥 X_0 极其敏感，微小的差别就不能解密，所以它的取值范围极大，不易攻破，且实时密钥 X_i (它的值又主控密钥 X_0 和迭代次数 i 决定)极难分析，迭代次数 i 可由随机数 R_0 决定。

4　基于混沌序列实时密钥的RFID安全机制

4.1　RFID系统的硬件要求

系统中的电子标签要求有安全模块来储存主控密钥、ID 和用户数据，以防对其进行物理攻击。由一个 4 bit 浮点乘法和一个 4 bit 减法电路完成式(2)的运算，而一个 4 bit 伪随机产生器和一个异或电路实现加解密。

4.2　RFID安全机制步骤

如果读写器和标签都合法，那么读写器的主控密钥 K_m 应该等于标签的主控密钥 K_m'。通过验证主控密钥可以鉴别双方的合法身份，读写器的实时密钥用 K_n 表示，其中，$n=i,i+1,\cdots$；i 为常数。K_n 表示读写器第 n 密钥。标签的实时密钥用 K_n' 表示，其中，$n=i,i+1,\cdots$，i 为常数。K_n' 表示标签第 n 密钥。基于混沌序列实时密钥的 RFID 安全加密的工作原理如图 3 所示。

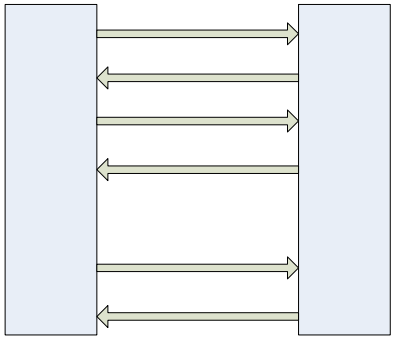

图 3　读写器与电子标签间的身份认证与保密通信

对图 3 的说明如下：

步骤 1　对于读写器方：读写器发一个查询命令 *Query* 和一个随机数 R_0 (这个随机数由后台数据库提供)给标签。接着对读写器取出储存在安全模块中的主控密钥 K_m，作为迭代式(1)中的初始值，即 $X_0=K_m$，然后让方程迭代 (R_0+C) 次，此时式(1)的迭代值为 X_i，此时初始化读写器实时密钥，$K_i=X_i$。其中，$C=50$；$i=R_0+C$，迭代 (R_0+C) 次目的是确保式(1)进入混沌状态。对于电子标签方：电子标签收到随机数 R_0 时，从它的安全模块取出主控密钥 K_m'，作为迭代式(2)中的初始值，即 $X_0'=K_m'$，让方程迭代 (R_0+C) 次，其中，$C=50$，目的是确保式(2)进入混沌状态。此时式(2)的迭代值为 X_i'，初始化电子标签实时密钥，$K_i'=X_i'$。

步骤 2　对于电子标签方：把从读写器发过来的 R_0 与此时密钥 K_i' 异或得到 $E_i'(R_0)$，即 $E_i'(R_0)=R_0\oplus K_i'$，然后产生一个伪随机数 R_1，把 $E_i'(R_0)$ 和 R_1 发往读写器。

对于读写器方：读写器收到 $E_i'(R_0)$ 和 R_1，把 $E_i'(R_0)$ 与读写器此时的密钥 K_i 异或后得到 R_0'，也即 $R_0'=E_i'(R_0)\oplus K_i$，若 $R_0'=R_0$ (步骤 1 发给标签的随机数)，那就证明 $K_i=K_i'$，证明如下：

$$\left.\begin{aligned}R_0'&=E_i'(R_0)\oplus K_i=\\&R_0\oplus K_i'\oplus K_i=\\&R_0'\oplus K_i'\oplus K_i=\\&K_i'\oplus K_i\oplus R_0'\\0&=K_i'\oplus K_i\end{aligned}\right\}\Rightarrow\quad R_0'\oplus R_0'=K_i'\oplus K_i\oplus R_0'\oplus R_0'\quad\Rightarrow$$

即 $K_i'=K_i$，这就证明了标签的主控密钥 K_m' 等于读写器的主控密钥 K_m，若 R_0' 不等于 R_0，则说明该标签为非法标签，读写器不予处理，并报警。这个步骤完成读写器对电子标签的身份认证。解决了标签伪造哄骗的安全问题。

步骤 3　对于读写器方：读写器让式(1)再迭代一次，得到迭代值 X_{i+1}，此时更新读写器的实时密钥，$K_{i+1}=X_{i+1}$。把标签发过来，R_1 与此时密钥 K_{i+1} 异或得 $E_{i+1}(R_1)$，即 $E_{i+1}(R_1)=R_1\oplus K_{i+1}$，把 $E_{i+1}(R_1)$ 发往电子标签。对于电子标签方：电子标签收到 $E_{i+1}(R_1)$，让迭代式(2)再迭代一次，得到迭代值 X_{i+1}'，更新标签的实时密钥，$K_{i+1}'=X_{i+1}'$，然后 $E_{i+1}(R_1)$ 与此时的密

(下转第 148 页)