第 34 卷 第 19 期 计 算 机 工 程 2008 年 10 月
Vol.34 No.19 Computer Engineering October 2008
·安全技术· 文章编号：1000—3428(2008)19—0170—04 文献标识码：A 中图分类号：TP309

基于密钥矩阵的 RFID 安全协议

裴友林，杨善林
(合肥工业大学计算机网络系统研究所，合肥 230009)

摘 要：无线射频识别(RFID)作为一种新型的自动识别技术正逐渐得到广泛应用，但 RFID 系统的特点和 RFID 设备的局限性带来了很多安全隐患问题。针对这些问题，讨论并阐明 RFID 的系统组成和安全隐患，分析了几种现有的典型的 RFID 安全协议的特点和缺陷，提出一种基于密钥矩阵的 RFID 安全协议。该协议使用密钥矩阵来加密标签和阅读器之间传输的数据，并在认证后更新标签中密值，能有效抵抗多种攻击。分析表明，该协议具有效率高、成本低、安全性高等特点。
关键词：RFID 系统；安全协议；密钥矩阵

Key Matrix-based Security Protocol for RFID

PEI You-lin, YANG Shan-lin
(Institute of Computer Network System, Hefei University of Technology, Heifei 230009)

【Abstract】 Radio Frequency Identification(RFID) as a new automated identification technology has become popular in many applications. But the features of the RFID systems and the constraints of RFID devices bring about various privacy problems. To address these issues, the structure and privacy problems of RFID systems are discussed and clarified in this paper, and the features and issues pertinent to several current typical RFID security protocols are analyzed. A new security protocol for RFID based on key matrix is proposed. Encrypting the data transported between tags and readers by key matrix and renewing the tag's secret value after each authentication, the protocol efficiently prevents multiple attacks. Analysis shows that this protocol is high efficiency, low-cost and good security.
【Key words】 RFID system; security protocol; key matrix

无线射频识别技术(Radio Frequency Identification, RFID)是一种非接触式的自动识别技术，它通过射频信号来自动识别目标对象并获取相关数据。这种识别技术的优点之一就是无需任何物理接触或者其他任何可见的接触。但在享受RFID技术带来便利的同时，也必须要面对伴随而来的诸如标签信息泄漏、标签易追踪等安全隐患问题。针对这一问题，国内外开展了大量关于RFID隐私安全保密的研究，提出了一系列的安全认证协议，如Hash Lock协议[1-2]，随机化Hash Lock协议[3]、Hash链协议[4]等，但这些协议存在着安全隐患、效率低下或应用成本过高等缺陷。本文针对这些协议的不足，进一步对RFID的安全隐私进行研究。

1 RFID 系统基本构成与安全隐患

1.1 RFID 系统基本构成

RFID 系统由 3 个部分组成：RFID 标签，RFID 标签读写器以及后台数据库，如图 1 所示。

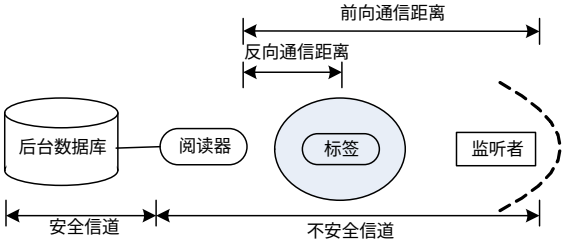

图 1 RFID 系统基本构成

后台数据库是用户根据系统需求进行选择的数据库系统，存储所有标签的信息，如标签序列号、阅读器定位、读取时间以及传感器温度。它通过可信的读写器获得标签发送的信息，具有很强的处理能力和存储空间。RFID 标签读写器是用于读或读/写 RFID 标签的设备，具有较强的处理能力和存储空间。RFID 标签读写器连接后台数据库，一般认为标签读写器至后台数据库的通信通道为安全信道。RFID 标签是 RFID 系统的数据载体，由藕合元件以及微电子芯片组成，通常没有微处理器。标签和标签读写器之间通过无线电进行通信。一般认为，标签和标签读写器之间的通信通道为不安全信道。

标签读写器至标签的通信信道称为“前向信道”，标签至标签读写器的通信则称为“反向信道”，如图 1 所示。由于读写器的无线功率超过标签的无线功率，导致前向通信范围远大于反向通信范围。标签和标签读写器间的通信受到多个因素的影响。ISO/IEC18000 标准定义的 RFID 系统的通信模型由 3 层组成，依次为物理层、通信层和应用层。物理层主要解决电气信号问题，通信层定义标签读写器与标签之间双向交换数据和指令的方式，而应用层用于解决与最上层应用直接相关的内容，包括认证、识别以及应用层数据的表示、处理逻辑等。通常情况下所说的 RFID 安全协议都属于应用层协议，本文讨论的 RFID 安全协议也属于这个范畴。

基金项目：安徽省 2007 年度重点科研计划基金资助项目(07020303079)
作者简介：裴友林(1982－)，男，硕士，主研方向：嵌入式系统，RFID技术；杨善林，教授、博士生导师
收稿日期：2007-11-18 **E-mail：**flyingsee@126.com

1.2 RFID 安全隐患与安全需求

RFID 系统容易受到攻击，RFID 读写器和 RFID 标签之间通过无线电进行通信，不需要任何物理或者可见接触，使得任何阅读器均可以访问标签并获取其中信息。同时标签中含有唯一序列号，可以唯一地追踪和定位标签获得标签所有者的隐私信息。另外，“前向信道”和“反向信道”的不对称也危及 RFID 系统的安全。

RFID 标签设备本身存在着处理能力有限、存储空间有限(最便宜的标签仅可容纳唯一标识符)、电源供给有限等局限性。尽管采用成熟的公钥算法可以在理论上解决隐私侵犯引起的安全问题，但其所需要的强大处理器能力也势必导致标签成本增加。因此现阶段任何采用公钥体系的算法应用于处理能力有限的被动标签都是不可行的。正因为如此，设计安全、高效、低成本的 RFID 安全协议成为了一个具有挑战性的问题。

一般来说，一个安全的 RFID 系统需要解决下面两方面问题：(1)标签信息泄漏问题，避免未授权读写器或者窃听者获取标签中的敏感数据；(2)标签的可追踪性，避免通过对标签序列号追踪定位获得标签持有者的隐私信息。

2 ID 系统安全机制及相关研究

现有的 RFID 系统安全机制可以分为两类：一类是使用物理方法的硬件安全机制；另一类是基于密码技术的软件安全机制。

2.1 物理安全机制

使用物理方法来保护RFID标签安全性的方法主要有如下几类：Kill 命令机制[3]，静电屏蔽[2]以及Blocker Tag[5]方法等。

Kill 命令机制是由标准化组织 Auto-ID Center 提出，采用从物理上毁坏标签的办法。一旦对标签实施了 Kill 销毁命令，标签便不可能再被重用；此外，一个重要的问题就是难以验证是否真正对标签实施了 Kill 操作。静电屏蔽主要是使用法拉第网罩对标签进行屏蔽，使标签不能接收任何来自标签读写器的信号。这需要一个额外的物理设备，既造成了不便，又增加了系统的成本。Blocker Tag 方案通过采用一个特殊的阻止标签干扰防冲突算法来实现。阅读器读取命令每次总获得相同的应答数据，从而保护标签。此方法需要一个额外的阻止标签，增加了应用成本。

2.2 基于密码技术的安全机制

鉴于物理安全机制存在的种种缺点，在最近的 RFID 系统中，提出了许多基于密码技术的安全机制。

与物理方法的硬件安全机制相比，基于密码技术的软件安全机制主要研究内容则是利用各种成熟的密码方案来设计和实现符合 RFID 安全需求的密码协议。这已经成为当前 RFID 安全研究的热点。但大多数 RFID 安全协议都存在着各种各样的缺陷，下面详细分析下几种典型的 RFID 安全协议。其中，G 和 H 表示 2 个不同的单向 Hash 函数。

2.2.1 Hash-Lock 协议

Hash-Lock协议[1-2]是由Sarma 等人提出的，使用*metaID*来代替真实的标签*ID*以避免信息泄漏和被追踪，协议如图 2 所示。每个标签拥有自己的访问密钥*key*，且*metaID*=H(*key*)。协议的执行过程如下：读写器询问标签，标签发送*metaID*作为响应。读写器将*metaID*发送至后台数据库，数据库系统查询数据库，找到和*metaID*匹配的(*metaID*,*ID*,*key*)记录，并将(*key*,*ID*)发送至读写器。读写器将*key*发送至标签。标签验证H(*key*)和*metaID*是否相同，如果相同，通过验证，将其*ID*发送给阅读器。

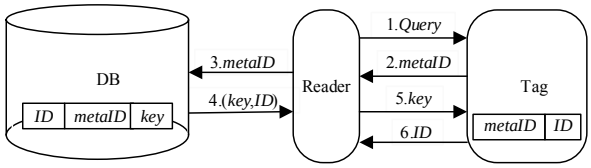

图 2 Hash-Lock 协议

从上述的过程中可以看出，该协议能够提供访问控制和标签数据隐私保护。但是由于 *ID* 没有使用动态刷新机制，*metaID* 保持不变，标签易被跟踪定位。*Key*,*ID* 以明文形式发送，容易被窃听者获取。

2.2.2 随机 Hash-Lock 协议

为了解决Hash-Lock协议[3]中标签跟踪性问题，Weis等人提出了随机Hash-Lock协议，协议如图 3 所示。其中“||”是字符串连接符号。

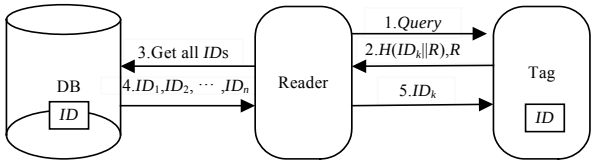

图 3 随机 Hash-Lock 协议

此协议的执行过程如下：读写器请求访问标签，标签生成随机数R，计算$H(ID||R)$，并将$(H(ID_k||R), R)$发送给阅读器。阅读器请求后台数据库，后台数据库将所有标签的标识$(ID_1,ID_2,\cdots,ID_n)$发送给阅读器，阅读器分别计算$H(ID_i||R)$ $(1\leq i\leq n)$，若存在$H(ID_i||R)=H(ID_k||R)$，通过认证，将ID_i发送给标签。标签验证ID_i和ID_k是否相同，相同则通过认证。

此认证协议中，对于阅读器的访问请求，标签的响应是随机的，解决了依据相同响应对标签进行跟踪定位的问题。但是此协议还是有缺陷的，标签认证后的标识ID_k还是以明文发送的，攻击者可以根据ID_k对标签进行追踪定位和据此伪造标签。同时此协议不具有前向安全性，窃听者根据ID_k和R值计算出$H(ID_k||R)$值，因此可追踪到标签历史位置信息。不仅如此，每次认证，数据库都将所有标签的标识发送至阅读器，标签对每个标识进行运算，对于大型的应用来说，这显然是低效的。

2.2.3 Hash-Chain 协议

NTT实验室提出了Hash-Chain协议[4]，保证了前向安全，协议如图 4 所示。

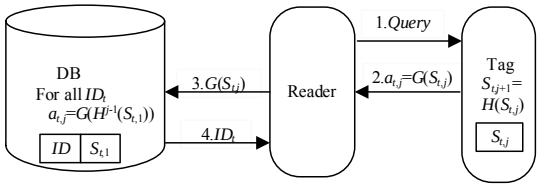

图 4 Hash-Chain 协议

在系统中，每个标签在后台数据库中都有个初始值$S_{t,1}$，G和H是单向的Hash函数。标签和阅读器之间的第j次认证过程如下：阅读器发出请求，标签根据其密值$S_{t,j}$计算$a_{t,j}=G(S_{t,j})$，更新自己的密值$S_{t,j+1}=H(S_{t,j})$，并将$a_{t,j}$发送至阅读器。阅读器将$a_{t,j}$发送至后台数据库，数据库对所有标签记录进行查找并计算是否存在ID_k满足$a_{t,j}=G(H^{j-1}(S_{t,1}))$，若有，认证通过，将

ID_k发送至阅读器。

该协议中的标签具有自主更新能力，避免了标签定位隐私信息的泄漏。又由于单向的Hash函数，不可能从$S_{t,j+1}$获得$S_{t,j}$，具有前向安全性。但此协议有缺陷，只对标签进行了身份验证，只要攻击者截获了$a_{t,j}$，就可以伪装标签，通过验证。不仅如此，每次验证时，数据库要对每个标签进行j次运算，应用成本较高。同时，该协议需要 2 个Hash函数，增加了标签成本。

3 基于矩阵密钥的认证协议

RFID 隐私保护与成本之间是相互制约的。因此，需要的 RFID 方案便是平衡隐私保护与成本的最佳方案。本文讨论的是如何在低成本的被动标签上提供确保消费者隐私的隐私安全技术。鉴于上述几种典型的 RFID 安全认证协议在前向安全性、执行效率、应用成本等方面存在着缺陷，本文提出了一种基于密钥矩阵的 RFID 安全认证协议。

3.1 基本原理

定义 1 设$p(p\geq 2)$是给定的正整数，称之为模，正整数r满足$0\leq r<m$，对任意整数a，存在唯一的整数r及唯一的整数q，使等式$a=pq+r$成立。其中，r称为a模p的余数。称全体整数关于模p的全体余数组成的集合为模p的余数集，记作$\boldsymbol{Z}_p$。

定义 2 设 $\boldsymbol{A}$ 是 n 阶整数方阵，若 n 阶方阵 $\boldsymbol{B}$ 满足：

(1)$\boldsymbol{B}$的全部元素属于$\boldsymbol{Z}_p$ ；

(2)$\boldsymbol{AB}\equiv\boldsymbol{BA}\equiv\boldsymbol{I}(\mathrm{mod}\ p)$，$\boldsymbol{I}$ 为 n 阶单位方阵。

称$\boldsymbol{B}$是$\boldsymbol{A}$模p的逆矩阵，记作$\boldsymbol{B}=\boldsymbol{A}^{-1}\mathrm{mod}\ p$。根据可逆矩阵的性质，可以实现加密和解密操作。

设$\boldsymbol{P}$和$\boldsymbol{C}$是长度为n的列向量，分别代表明文和密文，$\boldsymbol{K}$是一个n阶整数方阵，设$\boldsymbol{K}^{-1}$是$\boldsymbol{K}$模p的逆矩阵。则加密的过程可以表示为

$\boldsymbol{C}=E(\boldsymbol{K},\boldsymbol{P})=\boldsymbol{KP}\ \mathrm{mod}\ p$

解密则需要矩阵$\boldsymbol{K}$的逆$\boldsymbol{K}^{-1}$，解密过程可表示为

$\boldsymbol{P}=D(\boldsymbol{K},\boldsymbol{P})=\boldsymbol{K}^{-1}\boldsymbol{C}\ \mathrm{mod}\ p=\boldsymbol{K}^{-1}\boldsymbol{KP}=\boldsymbol{P}$

此方案足以抵抗惟密文攻击[6]。也就是说，在截获密文$\boldsymbol{C}$后，无法根据密文信息来获取明文$\boldsymbol{P}$以及加密密钥$\boldsymbol{K}$。

3.2 协议描述

在基于双矩阵密钥的RFID双向认证协议中，每个标签的认证过程中需要使用 2 个矩阵密钥，记为$\boldsymbol{K}_1$和$\boldsymbol{K}_2$，$\boldsymbol{K}_1$和$\boldsymbol{K}_2$是n阶可逆方阵。$\boldsymbol{K}_1^{-1}$, $\boldsymbol{K}_2^{-1}$分别是他们的逆。标签中存储密值$\boldsymbol{S}$和 2 个矩阵$\boldsymbol{K}_1$及$\boldsymbol{K}_2^{-1}$。密值$\boldsymbol{S}$是长度为q的向量，$q=m\times n$，m是正整数。

后台数据库为每个标签存储$(\boldsymbol{X},\boldsymbol{S},\boldsymbol{K}_1^{-1},\boldsymbol{K}_2)$这样的记录，$\boldsymbol{X}$表示该标签记录在数据库中的索引。$\boldsymbol{X}$是长度为$q$的向量，其值可通过对$\boldsymbol{K}_1$和$\boldsymbol{S}$进行下列运算得到：将$\boldsymbol{S}$划分成$m$个长度为$n$的向量，$\boldsymbol{S}=(\boldsymbol{s}_1,\boldsymbol{s}_2,\cdots,\boldsymbol{s}_i,\cdots,\boldsymbol{s}_m)^{\mathrm{T}}$，则$\boldsymbol{X}=(\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_i,\cdots,\boldsymbol{x}_m)^{\mathrm{T}}$，其中$\boldsymbol{x}_i$和$\boldsymbol{s}_i$是长度为$n$的向量且$\boldsymbol{x}_i=\boldsymbol{K}_1\boldsymbol{s}_i(1\leq i\leq m)$。

初始化时，为每个标签随机选择可逆方阵$\boldsymbol{K}_1$和$\boldsymbol{K}_2$。选择唯一的$\boldsymbol{X}$，并根据$\boldsymbol{X}$值，计算$\boldsymbol{K}_1{}^{-1}\boldsymbol{X}$，得密值$\boldsymbol{S}$。将这些信息按照图 5 所示存储进标签和数据库；(1)阅读器向标签发送Query认证请求。(2)标签计算$\boldsymbol{X}\leftarrow\boldsymbol{K}_1\boldsymbol{S}$，将$\boldsymbol{X}$发送给阅读器。(3)阅读器将$\boldsymbol{X}$转发给后台数据库。(4)数据库搜索数据库，找到相应的$\boldsymbol{X}$。计算$\boldsymbol{K}^{-1}\boldsymbol{X}$，并验证此值与$\boldsymbol{S}$是否相同。不同，认证不通过；相同，选择使$\boldsymbol{X}_{\mathrm{new}}$唯一的$\boldsymbol{S}_{\mathrm{new}}$，计算$\boldsymbol{Y}\leftarrow\boldsymbol{K}_2\boldsymbol{S}$，$\boldsymbol{Z}\leftarrow\boldsymbol{K}_2\boldsymbol{S}_{\mathrm{new}}$，更新$\boldsymbol{S}$。将$\boldsymbol{Y},\boldsymbol{Z}$发送给读写器。(5)读写器将$\boldsymbol{Y},\boldsymbol{Z}$转发给标签。(6)标签计算$\boldsymbol{K}_2^{-1}\boldsymbol{Y}$，验证此值是否与$\boldsymbol{S}$相同。不同，认证不通过；相同，计算$\boldsymbol{K}_2^{-1}\boldsymbol{Z}$，并将$\boldsymbol{S}$更新为此值。

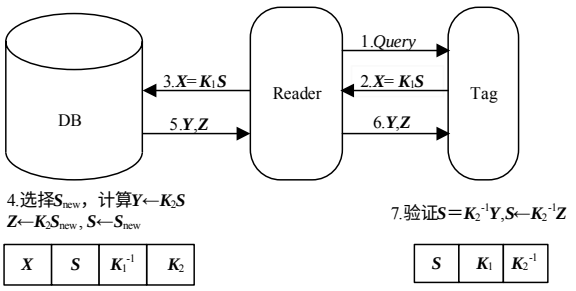

图 5 双矩阵密钥认证协议

3.3 数值实验

在实验中，密钥矩阵为 3×3 的整数方阵。电子标签中的信息以十六进制形式存储，故取模 $\boldsymbol{P}=16$，密值和序列号长度均为 6。

设数据库中存储了n条标签记录，现有一个标签T_1，进行初始化操作：选择唯一的序列值$\boldsymbol{I}_1$=302 164，随机选择 2 对密钥矩阵$(\boldsymbol{K}_{1,1},\boldsymbol{K}^{-1}{}_{i,1}),(\boldsymbol{K}_{1,2},\boldsymbol{K}^{-1}{}_{1,2})$，其中：

$$\boldsymbol{K}_{1,1}=\begin{bmatrix}1&3&4\\1&3&5\\3&8&7\end{bmatrix},\ \boldsymbol{K}^{-1}{}_{i,1}=\begin{bmatrix}13&11&3\\8&11&15\\15&1&0\end{bmatrix},$$

$$\boldsymbol{K}_{1,2}=\begin{bmatrix}2&1&3\\1&3&5\\3&6&11\end{bmatrix},\ \boldsymbol{K}^{-1}{}_{1,2}=\begin{bmatrix}3&7&12\\4&13&9\\13&7&5\end{bmatrix}$$

验证如下：

$$\boldsymbol{K}_{1,1}\,\boldsymbol{K}^{-1}{}_{i,1}=\begin{bmatrix}97&48&48\\112&49&48\\208&128&129\end{bmatrix}\mathrm{mod}16=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

同理也能验证$\boldsymbol{K}^{-1}{}_{1,2}$是$\boldsymbol{K}_{1,2}$模 16 的逆矩阵；再计算密值$\boldsymbol{S}_1$，将$\boldsymbol{I}_1$划分成 2 个长度为 3 的列向量：$\boldsymbol{I}_{1,1}=\begin{bmatrix}3&0&2\end{bmatrix}^{\mathrm{T}}$，$\boldsymbol{I}_{1,2}=\begin{bmatrix}1&6&4\end{bmatrix}^{\mathrm{T}}$，则

$$\boldsymbol{S}_1=\boldsymbol{K}^{-1}{}_{1,1}\,\boldsymbol{I}_1=\begin{bmatrix}\boldsymbol{K}_{1,1}^{-1}\boldsymbol{I}_{1,1}\\\boldsymbol{K}_{1,1}^{-1}\boldsymbol{I}_{1,2}\end{bmatrix}=\begin{bmatrix}45\\54\\45\\91\\134\\21\end{bmatrix}\mathrm{mod}\ 16=\begin{bmatrix}13\\6\\13\\11\\6\\5\end{bmatrix}$$

转化为十六进制表示则为D6DB65。将$(\boldsymbol{I}_1,\ \boldsymbol{S}_1,\boldsymbol{K}_{1,2},\ \boldsymbol{K}^{-1}{}_{1,1})$存入数据库，如表 1 所示。同时将$(\boldsymbol{S}_1,\ \boldsymbol{K}_{1,1},\ \boldsymbol{K}^{-1}{}_{1,2})$存入标签$T_1$。

表 1 数据库中初始化标签认证信息

序列号$\boldsymbol{I}_i$	密值$\boldsymbol{S}_i$	密匙$\boldsymbol{K}^{-1}{}_{i,1}$	密钥$\boldsymbol{K}_{i,2}$
302164	D6DB65	$\begin{bmatrix}13&11&3\\8&11&15\\15&1&0\end{bmatrix}$	$\begin{bmatrix}2&1&3\\1&3&5\\3&6&11\end{bmatrix}$

当标签读写器询问标签时，标签进行运算$\boldsymbol{I}=\boldsymbol{K}_{1,1}\boldsymbol{S}_1$=302 164，将$\boldsymbol{I}$发送给读写器。读写器将$\boldsymbol{I}$发送至后台数据库。数据库搜索到相关的数据库记录$(\boldsymbol{I}_1,\boldsymbol{S}_1,\boldsymbol{K}_{1,2},\boldsymbol{K}^{-1}{}_{1,1})(\boldsymbol{I}=\boldsymbol{I}_1)$。数据库验证密值$\boldsymbol{S}_1=\boldsymbol{K}^{-1}{}_{1,1}\boldsymbol{I}$= D6DB65，通过验证后数据库选择新的唯一的序列值$\boldsymbol{I}_{\mathrm{new}}$=301009，计算$\boldsymbol{S}_{\mathrm{new}}=\boldsymbol{K}^{-1}{}_{1,1}\boldsymbol{I}_{\mathrm{new}}$=A7DB70。计算$\boldsymbol{Y}=\boldsymbol{K}_{1,2}\boldsymbol{S}_1$＝70AB6C, $\boldsymbol{Z}=\boldsymbol{K}_{1,2}\boldsymbol{S}_{\mathrm{new}}$=207D0B。更新数据库后将$\boldsymbol{Y},\boldsymbol{Z}$通过读写器转发给标签。标签$T_1$根据$\boldsymbol{Y}$计算出$\boldsymbol{S}_1=\boldsymbol{K}^{-1}{}_{1,2}\boldsymbol{Y}$=D6DB65，通过验证。再通过运算$\boldsymbol{S}_{\mathrm{new}}=\boldsymbol{K}^{-1}{}_{1,2}\boldsymbol{Z}=$A7DB70 得到新的密值，更新标签中存储的密值为$\boldsymbol{S}_{\mathrm{new}}$。认

证一次后数据库中标签T_1记录如表 2 所示。

表 2　认证一次后数据库中标签认证信息

序列号$\boldsymbol{I}_i$	密值$\boldsymbol{S}_i$	密匙$\boldsymbol{K}^{-1}_{i,1}$	密钥$\boldsymbol{K}_{i,2}$
301009	A7DB70	$\begin{bmatrix}13 & 11 & 3\\ 8 & 11 & 15\\ 15 & 1 & 0\end{bmatrix}$	$\begin{bmatrix}2 & 1 & 3\\ 1 & 3 & 5\\ 3 & 6 & 11\end{bmatrix}$

通过实验，可验证该协议实现了标签和后台数据库之间的双向认证，并在每次认证后同时更新后台数据库与标签中密值。

3.4　安全和性能分析

使用矩阵密钥的加密方案能够有效地抵抗密文攻击，攻击者无法从密文中获得加密密钥和明文。并且每次认证通过后，标签将更新密值，使攻击者无法进行明密文攻击，使本方案的安全性大大提高。使用了双矩阵密钥进行了双向身份验证。本协议的特点主要有下面几点：

(1)标签匿名性。由于每次通过认证后，标签都将密值$\boldsymbol{S}$更新为$\boldsymbol{S}_{\text{new}}$。标签对于阅读器的认证请求的响应次次都不一样。避免窃听者根据响应信息来跟踪定位标签，实现了标签的匿名性。

(2)前向安全性。本协议中更新的密值$\boldsymbol{S}_{\text{new}}$是通过$\boldsymbol{K}^{-1}{}_1\boldsymbol{I}_{\text{new}}$运算获得的，$\boldsymbol{I}_{\text{new}}$是随机选择的唯一序列值，故$\boldsymbol{S}_{\text{new}}$值也是随机的。即使被当前密值$\boldsymbol{S}_{\text{new}}$被窃取，也无法根据$\boldsymbol{S}_{\text{new}}$推算出之前密值$\boldsymbol{S}$，无法获取标签的历史活动记录。

(3)执行效率高，应用成本低。设数据库中有 n 条标签记录，那么本协议在一次认证过程中需要执行 n 次记录搜索，执行 3 次矩阵运算和一次值比较。相对于 Hash-Chain 协议的 n 个记录搜索，2n 次 Hash 函数计算，n 次值比较，本协议大大提高了执行效率，减少了应用成本。此协议比较适合标签较多的大型应用中。

(4)标签成本低。据 Auto-ID 中心实验的试验数据，低成本被动标签用于安全操作的门电路数量不能超过 2 500~5 000。本协议中，标签只需要执行简单的矩阵运算，实现矩阵运算操作只需要很少的门电路，大大减少了标签的成本。

4　结束语

本文提出了基于密钥矩阵的安全认证协议，在保证标签隐私安全的前提下，提高了认证的执行效率及应用成本。但此协议还有不足之处，标签中存储信息量较大。再者，需要做到标签中信息和后台数据库的同步更新，不适用于分布式环境，还需要对其进行进一步研究。

参考文献

[1] Sarma S E, Weis S A, Engels D W. RFID Systems and Security and Privacy Implications[C]//Proc. of the 4th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer-Verlag, 2003: 454-469.

[2] Sarma S E, Weis S A, Engels D W. Radio Frequency Identification: Secure Risks and Challenges[J]. RSA Laboratories Cryptobytes, 2003, 6(1): 2-9.

[3] Weis S A, Sarma S E, Rivest R L, et al. Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems[C]//Proc. of the 1st International Conference on Security in Pervasive Computing. Berlin, Germany: Springer-Verlag, 2004: 201-212.

[4] Ohkubo M, Suzuki K, Kinoshita S. Hash-chain Based Forward-secure Privacy Protection Scheme for Low-cost RFID[C]//Proc. of Symposium on Cryptography and Information Security. Sendai, Japan: [s. n.], 2004: 719-724.

[5] Juels A, Rivest R L, Szydlo M. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy[C]//Proc. of the 10th ACM Conference on Computer and Communications Security. Washington D. C., USA: [s. n.], 2003: 103-111.

[6] Stallings W. Cryptography and Network Security: Principles and Practice[M]. 2nd ed. Englewood Cliffs, USA: Prentice-Hall, 1999.

（上接第 169 页）

通过实验，验证了系统的实际效果，能够达到网站系统对入侵的事后及时发现和恢复，实现了网站系统的可生存性。

4.2　系统性能分析

数据库保护部分利用了 DBMS 自带的触发器机制，当网站程序访问数据库时，相应的触发器自动被调用，不会对网站的性能产生影响。文件保护的轮询机制，文件备份恢复的时间很短，能够保证用户浏览到正常的网页。

下面着重分析 NDIS 的数据包过滤技术的性能情况：2 台 PC 全速通信，安装 PASSTHRU 前网卡的平均速率为 80.6 Mb/s，安装 PASSTHRU 后网卡的平均速率为 79.1 Mb/s，这证明了 PASSTHRU 对网络吞吐量影响很小，几乎不会影响到网站系统的性能，不会因为开启了包过滤保护而影响用户浏览网页的速度。

5　结束语

本文提出了一种基于可生存性的网站保护系统的设计方案，把数据库保护和网页文件保护相结合，采取数据库触发器机制，多线程轮询机制和开发 Windows 网络中间层驱动 3 种不同的保护策略，比较彻底地实现了网站的安全保护，对于网站的入侵容忍和事后恢复有很好的效果。

参考文献

[1] 高延玲, 张玉清, 白宝明, 等. 网页保护系统综述[J]. 计算机工程, 2004, 30(10): 113.

[2] Scoff D, Sharp R. Abstracting Application-level Web Security[C]//Proc. of the 11th International Conference on World Wide Web. Honolulu, Hawaii, USA: [s. n.], 2002: 396-407.

[3] Knight J C, Strunk E A, Sullivan K J. Towards a Rigorous Definition of Information System Survivability[C]//Proc. of DARPA Information Survivability Conference and Exposition. [S. l.]: IEEE Press, 2003: 78-89.

[4] 梁　旦, 徐国华, 朱良根. 基于网页监控与保护的安全数据库系统[J]. 计算机应用研究, 2004, 21(8): 116-118.

[5] 刘大勇. 校园网站网页防篡改技术研究与应用[J]. 电脑知识与技术, 2005, (7): 73.