第 38 卷 第 3 期
Vol.38 No.3

计 算 机 工 程
Computer Engineering

2012 年 2 月
February 2012

• 安全技术 •

文章编号：1000—3428(2012)03—0124—02 文献标识码：A 中图分类号：TP309.2

基于二次剩余的增强型 RFID 认证协议

轩秀巍，滕建辅，白 煜

(天津大学电子信息工程学院，天津 300072)

摘 要：分析一种基于二次剩余的认证协议并对其进行改进，提出基于二次剩余的增强型无线射频识别(RFID)安全认证协议。改进协议中的阅读器和标签都产生随机数，并利用 Hash 函数和二次剩余理论对传输的数据进行加密，从而增强系统的安全性。分析结果表明，该协议可满足 RFID 系统对安全和隐私的要求，且计算量和存储量较少。

关键词：无线射频识别；认证协议；Hash 函数；二次剩余；假冒攻击；拒绝服务攻击

Enhanced RFID Authentication Protocol Based on Quadratic Residue

XUAN Xiu-wei, TENG Jian-fu, BAI Yu

(School of Electronic Information Engineering, Tianjin University, Tianjin 300072, China)

【Abstract】This paper analyzes the scheme proposed by Chen et al and presents an improved protocol based on quadratic residue and Hash function. In the improved protocol, random numbers are generated both by reader and tags. The transmitted information is encrypted by quadratic residue and Hash function. Analysis result demonstrates that the improved protocol not only can resist various attacks and ensure privacy, but also needs less computation and storage in the tags and server compared to other improved scheme.

【Key words】Radio Frequency Identification(RFID); authentication protocol; Hash function; quadratic residue; impersonation attack; Denial of Service(DoS) attack

DOI: 10.3969/j.issn.1000-3428.2012.03.042

1 概述

无线射频识别(Radio Frequency Identification, RFID)系统是一种非接触式自动识别系统，该系统包括标签、阅读器和后端数据库。阅读器通过无线信号获得标签中的信息。由于其自动识别特性，RFID 系统在生产、物流管理、门禁系统、交通支付等各领域得到越来越广泛的应用[1]。然而，标签所提供的丰富的数据容易引发用户隐私和安全问题。多数标签因为受成本限制，自身不具有防伪造和抗非法读取的功能，攻击者可以轻易读取或篡改标签信息伪造标签，甚至可以通过标签对所有者进行追踪[2]。

为设计一种高效安全的 RFID 认证协议，文献[3-4]分别引入了公钥加密的方法。文献[4]提出了一种基于二次剩余的认证协议，但文献[5]证明该协议不能提供位置隐私并且易受重放攻击。本文进一步证明该协议易受阅读器假冒攻击和拒绝服务攻击，并提出一种更简单和安全的改进协议。

2 背景知识

2.1 二次剩余理论

假如 n 是一个复合数，在知道 n 的因数分解情况下(k 个素数乘积)，可以分解 $x^2 \equiv a \mod n$，通过解每一个分解方程，从而得到 k 对 x 的值。

解一个二次同余模一个复合数的问题难度在于对模的因数分解。如果 n 是一个非常大的数，对其进行因数分解是不可能的，保证了加密数据的安全性。

二次剩余是一个加密和解密的过程。设加密函数为 $E(n, x)$，解密函数为 $D(p, q, X)$，其运算过程如下，其中，$n = p \times q$；$C(a, b, p, q)$表示中国剩余算法[6]。

E(n, x)
{
$X=x^2 \bmod n$
return X
}
D(p, q, X)
{
$a_1=+(X^{(p+1)/4}) \bmod p$
$a_2=-(X^{(p+1)/4}) \bmod p$
$b_1=+(X^{(q+1)/4}) \bmod q$
$b_2=-(X^{(q+1)/4}) \bmod q$
$x_1=C(a_1, b_1, p, q)$
$x_2=C(a_1, b_2, p, q)$
$x_3=C(a_2, b_1, p, q)$
$x_4=C(a_2, b_2, p, q)$
return x_1, x_2, x_3, x_4
}

2.2 系统条件

本文所用的 RFID 系统由标签、阅读器和后端数据库 3 个部分组成，假设阅读器和数据库之间的通信是安全的，标签和阅读器之间的无线信道容易受到攻击。文中所用符号的含义如表 1 所示。

基金项目：天津市自然科学基金资助项目(09JCYBJC00700)

作者简介：轩秀巍(1984－)，女，博士研究生，主研方向：无线网络安全，RFID 系统；滕建辅，教授、博士生导师；白 煜，讲师、博士

收稿日期：2011-08-08 **E-mail：**xiuweixuan@tju.edu.cn

表 1　符号含义

符号	含义
n	2 个大素数 p 和 q 的乘积
ID	标签的识别码
$h(ID)$	标签识别码的 Hash 值，用作数据库指针
s	阅读器产生的随机数
r	标签产生的随机数
k	标签和服务器之间的当前认证密钥
k_{old}	标签和服务器之间的旧的认证密钥
$PRNG$	伪随机数产生器

3　文献[4]协议

3.1　协议过程

(1)阅读器产生随机数 s，向标签发送认证请求及 s。

(2)标签收到认证请求后，计算 $x=h(ID)\oplus k\oplus s$，并对 x 和 k 进行加密 $X=E(n,x)$ 和 $K=E(n,k)$，将 $X, K, h(x), h(k)$发送给阅读器。

(3)阅读器将 $X, K, h(x), h(k), s$ 发送给后端数据库。

(4)服务器进行解密运算 $(x_1,x_2,x_3,x_4)=D(p,q,X)$ 以及 $(k_1,k_2,k_3,k_4)=D(p,q,K)$，分别得到 x 和 k 的 4 个值。通过比较 $h(x_i)$和 $h(x)$、$h(k_i)$和 $h(k)(i=1, 2, 3, 4)$来确定 x 和 k 的值。从而 $h(ID)=x\oplus k\oplus s$。数据库判断 $h(ID)$的合法性，如果合法则找到对应的密钥 k 和 k_{old}。比较计算所得的密钥是否与 k 或 k_{old} 相等。不相等服务器终止认证过程。如果相等，服务器计算 $x_{ack}=ID\oplus k$，并将 $h(x_{ack})$通过阅读器发送给标签。同时，服务器更新信息 $k_{old}=k$, $k=PRNG(k)$。

(5)收到 $h(x_{ack})$后，标签验证 $h(x_{ack})$是否与 $h(ID\oplus k)$ 相等，相等则更新其密钥 $k=PRNG(k)$；否则，阅读器是非法的，标签保留原来的密钥，认证失败。

3.2　协议不足

(1)阅读器假冒攻击：攻击者通过截取认证信息 $h(x_{ack})$使标签不能进行密钥更新，然后向标签发送认证请求。标签计算并回应<$X, K, h(x), h(k)$>。因为 k 没变，所以 $h(x_{ack})$和上次相同。攻击者将截获的信息 $h(x_{ack})$发送给标签，从而通过标签的认证，造成阅读器假冒攻击。

(2)拒绝服务攻击(Denial of Service, DoS)：在阅读器假冒攻击中，攻击者可以通过标签认证，进而标签更新其密钥。然而服务器中的密钥没有进行更新，导致以后的通信中，标签无法通过服务器的认证，引起拒绝服务攻击。

(3)跟踪攻击：攻击者连续截获或更改认证信息 $h(x_{ack})$，使标签不能进行密钥更新，k 不变。在收到接下来的认证请求后，标签的响应信息 $K, h(k)$始终不变，容易引发跟踪攻击。

4　改进协议

为了抵抗上述攻击，要求标签即使在没有更新密钥的情况下，对认证请求的响应每次都不同。为此，本文提出一种改进的协议，如图 1 所示。认证的具体过程如下：

(1)阅读器产生随机数 s，向标签发送认证请求及 s。

(2)标签收到认证请求后，产生随机数 r，计算 $x=ID\oplus r\oplus s$，并对 x 和 r 进行加密 $X=E(n,x)$，$R=E(n,r)$，同时计算 $M=h(k\,\|\,r)$，并将 $X, R, h(x), h(r), M$ 发送给阅读器。

(3)阅读器将 $X, R, h(x), h(r), M, s$ 发送给后端数据库。

(4)服务器分别对 x 和 r 进行解密，得到 $(x_1,x_2,x_3,x_4)=D(p,q,X)$，$(r_1,r_2,r_3,r_4)=D(p,q,R)$，通过比较 $h(x_i)$和 $h(x)$、$h(r_i)$和 $h(r)(i=1, 2, 3, 4)$来确定 x 和 r 的值，从而 $ID=x\oplus r\oplus s$。数据库判断 ID 的合法性，合法则找到对应的密钥 k 和 k_{old}。比较计算 $h(k\,\|\,r)$ 或 $h(k_{old}\,\|\,r)$ 是否与 M 相等。不相等说明标签是非法的，终止此次认证；有一个相等，服务器则根据相等的密钥值计算 $x_{ack}=ID\oplus k\oplus r$ 或 $x_{ack}=ID\oplus k\oplus r_{old}$，并将 $h(x_{ack})$通过阅读器发送给标签。同时，服务器更新信息 $k_{old}=k$, $k=PRNG(k)$。

(5)收到 $h(x_{ack})$后，标签验证 $h(x_{ack})$是否与 $h(ID\oplus k\oplus r)$ 相等。若相等，标签更新其密钥 $k=PRNG(k)$；否则，阅读器是非法的，标签保留原来的密钥，认证失败。

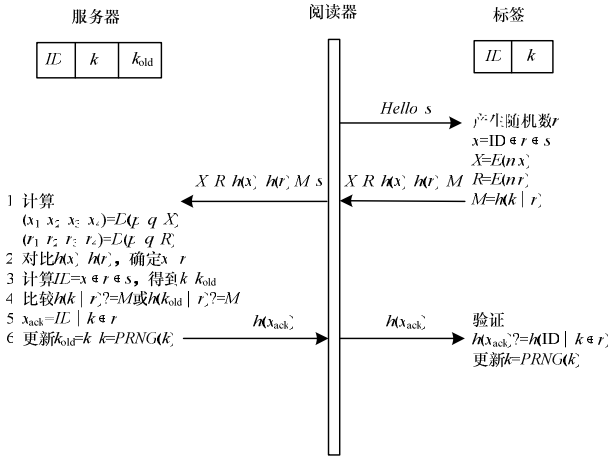

图 1　改进协议

5　改进协议的安全性分析

(1)阅读器假冒攻击

本文所提出的改进协议中，标签产生随机数，阅读器的认证信息 $h(x_{ack})=h(ID\oplus k\oplus r)$ 即使被攻击者截获，并再次发送给标签，因为下次通信中 r 改变，攻击者不能通过标签认证。可见本协议有效阻止了阅读器假冒攻击。

(2)DoS：由于攻击者不能通过标签认证，不能导致标签更新其密钥，这样标签中的密钥始终与服务器中的密钥保持一致，避免了拒绝服务攻击。

(3)跟踪攻击：标签响应的计算<$X, R, h(x), h(r), M$>都含有随机数 r，即使攻击者截获或更改认证信息 $h(x_{ack})$，导致标签不能进行密钥更新，对于每次的认证请求，标签的响应仍然不同，进而阻止了跟踪攻击。

(4)重放攻击：改进协议中，阅读器和标签都产生随机数，即使攻击者截获以前通信的数据，重放给阅读器或标签，因为每次通信的内容都不同，攻击者不能通过认证。

(5)前向安全：本协议中通信数据的计算包含随机数和密钥，具有不可预测性。即使标签发生泄密，攻击者仍不能根据标签现在的信息推测标签以前的行为，具有前向安全性。

(6)窃听攻击：通信过程中所传输的数据采用 Hash 函数和二次剩余加密的方法，保证了数据安全性，可以预防窃听攻击。

改进协议与其他协议的安全性对比如表 2 所示，与其他改进协议的计算量和存储数据对比如表 3 和表 4 所示。其中，E 表示二次剩余加密函数；D 表示二次剩余解密函数；H 表示 Hash 运算；PRNG 表示伪随机数产生器。

表 2　安全性对比

协议	窃听攻击	跟踪攻击	Dos	假冒攻击	前向安全	重放攻击
文献[4]协议	√	×	×	×	√	×
文献[5]协议	√	√	√	√	√	√
本文协议	√	√	√	√	√	√

(下转第 129 页)