第 36 卷 第 8 期 计 算 机 工 程 2010 年 4 月
Vol.36 No.8 Computer Engineering April 2010
·安全技术· 文章编号：1000—3428(2010)08—0165—02 文献标识码：A 中图分类号：TP393.08

基于实时控制网络的 RFID 系统认证方案

冯 广
(广东工业大学网络信息与现代教育技术中心，广州 510006)

摘 要：针对射频识别(RFID)应用信息在实时控制网络和拥塞通信网络传输中的安全性与实时性问题，根据 RFID 的非对称结构特点，提出一个基于公钥密码技术的身份认证方案，该方案充分利用 Rabin-PSS-MR 签名方案和改进的 ElGamal 签名方案中签名与验证计算量的非对称性，能保证传输安全并节省通信带宽。

关键词：实时控制网络；无线射频识别；认证；Rabin-PSS-MR 体制；ElGamal 体制

Authentication Scheme for RFID System Based on Real-time Control Network

FENG Guang
(Center of Campus Network & Modern Education Technology, Guangdong University of Technology, Guangzhou 510006)

【Abstract】Aiming at the security and real-time problem of Radio Frequency Identification(RFID) application information while transferring on the real-time control network and congestion communication network, this paper proposes an identity authentication scheme based on public key technology according to the non-symmetry structure feature of RFID. This scheme takes full advantage of signature and verification calculation non-symmetry of Rabin-PSS-MR signature scheme and improved ElGamal signature scheme. It can ensure the transfer security and reduce communication bandwidth.

【Key words】 real-time control network; Radio Frequency Identification(RFID); authentication; Rabin-PSS-MR system; ElGamal system

1 概述

无线射频识别(Radio Frequency Identification, RFID)已得到广泛应用，它是一种利用射频通信实现的非接触式自动识别技术。但 RFID 中存在一些急需解决的问题，例如，拥塞控制网络上的传输实时性，公共网络安全与隐私保护问题等。已有许多用于解决此类问题的 RFID 安全协议[1]，如 Hash-Lock 协议[2]、随机化 Hash-Lock 协议[3]等。

由于 RFID 通信一般需要使用实时控制网络或拥塞通信网络，因此会降低 RFID 应用的安全性和实时性。本文的目标是设计一个适用于高安全保密机制 RFID 安全的认证方案，实现会话密钥的分配并节省带宽。针对 RFID 技术计算资源和存储资源的非对称结构特点，为 Tag 配置计算量少的 Rabin-PSS-MR 签名的验证操作、Rabin-OAEP 加密操作和改进型 ElGamal 签名操作，为后端数据库 BD 配置计算量较大的 Rabin-OAEP 解密操作和改进型 ElGamal 签名的验证操作，以达到降低响应时延、提高网络效率的目的。为进一步节省通信带宽，将“发送公钥及相应证书”的传统公钥认证过程缩短为“仅发送公钥证书(而不发送公钥)”的精简模式，具体方法是采用具有消息恢复功能的 Rabin-PSS-MR 签名方案。认证结束后，双方将同时得到一个共享的会话密钥以确保随后通信的保密性，实现认证功能与密钥分配功能的巧妙结合。

2 RFID 系统认证结构

RFID 系统一般由 4 大部分构成：电子标签(tag)，读写器，通信网络和后端数据库(Back-end Database, BD)，见图 1。

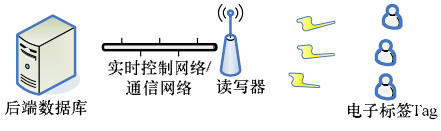

图 1 RFID 系统模型

本文做如下基本假设：Tag 与读写器之间的通信信道是不安全、无拥塞的，读写器与后端数据库之间的通信信道是安全、有拥塞的。

要实现实体间的安全通信，要求标签 Tag 在接入网络之前，通过读写器与后端数据库 BD 进行双向认证，具体如下：(1)证书认证中心(Certficate Authority, CA)负责为 BD 和 Tag 颁发公钥证书。证书是用消息恢复型 Rabin-PSS-MR 签名方案生成的。(2)后端数据库 BD 负责处理所有 Tag 在任何时刻的接入认证请求。(3)标签 Tag 在接入网络前必须向 BD 证明其公钥证书及身份的合法性，并验证 BD 的公钥证书及身份。

BD 的计算资源较充足，但 Tag 的存储和计算能力较弱。所以，本文的设计原则如下：由 BD 承担认证过程中计算量较大的工作，尽量减少 Tag 的工作量。

3 基础密码算法

为 Tag 和 BD 的双向认证配置不同的签名算法和加密算法，以适应 RFID 的非对称结构。本节介绍认证方案中采用的密码算法：改进型 ElGamal 签名算法，Rabin-OAEP 加密算法，Rabin-PSS-MR 签名算法和 SMS4 分组加密算法。

3.1 改进型 ElGamal 签名算法

3.1.1 参数设置

取 p 为一个大素数，g 是 Z_p^* 的一个本原元，$x \in Z_{p-1}$ 为私钥，$y = g^x \bmod p$ 为公钥，$m \in Z_{p-1}$ 是待签名的消息。

基金项目：国家自然科学基金资助项目(U0735003)；教育部博士点基金资助项目(20070562005)；广东省科技攻关计划基金资助项目(2007A010300016)；广东省自然科学基金资助项目(06021498)
作者简介：冯 广(1973－)，男，工程师、博士研究生，主研方向：控制系统，密码学
收稿日期：2009-12-26 **E-mail：**von@gdut.edu.cn

3.1.2　签名生成

签名生成过程如下：(1)选取一个随机数 $r \in Z_{p-1}$。(2)计算 $V = g^r \pmod p$，$W = x(m+V) - r \pmod{p-1}$，$(W,V)$ 作为消息 m 的签名。

3.1.3　签名验证

收到签名 (W,V) 后，判断 $y^{(m+V)} = Vg^W \bmod p$ 是否成立。若成立，则确认签名 (W,V) 有效，否则认定签名无效。

本文采用此改进型 ElGamal 签名算法的原因是签名过程中的模幂运算 g^r 可以预先计算，实时进行的只有模加和模乘运算，而无原始 ElGamal 方案[4]中的模逆运算，可以加快 Tag 的运算速度。

3.2　Rabin-OAEP 加密算法

Rabin 原始算法无法抵抗自适应选择密文攻击。因此，加入的最优非对称加密填充(Optimal Asymmetric Encryption Padding, OAEP)算法采用随机化消息填充技术，引入无碰撞的哈希函数，提供了可证明的安全性。

3.2.1　参数设置

运行密钥产生算法 $Gen(1^k)$ 得到($N = pq, p, q, G, H, n, k_0, k_1$)，其中，$N = pq$ 是公钥，$p = q = 3 \pmod 4$ 是私钥；$|N| = k = n + k_0 + k_1$；2^{-k_0} 和 2^{-k_1} 可忽略；$H: \{0,1\}^{k-k_0} \to \{0,1\}^{k_0}$，$G: \{0,1\}^{k_0} \to \{0,1\}^{k-k_0}$ 是 2 个哈希函数；n 是明文消息 m 的长度。

3.2.2　加密过程

加密过程如下：(1)对消息 $m \in \{0,1\}^n$ 进行加密。(2) $r \leftarrow_U \{0,1\}^{k_0}$; $s \leftarrow (m \| 0^{k_1}) \oplus G(r)$; $t \leftarrow r \oplus H(s)$。(3) $c \leftarrow (s \| t)^2 \bmod N$。

3.2.3　解密过程

收到密文 c 后，进行如下计算：(1)利用私钥 p 和 q 计算 $s \| t \leftarrow q(q^{-1} \bmod p)c^{\frac{p+1}{4}} + p(p^{-1} \bmod q)c^{\frac{q+1}{4}} \pmod N$，其中，$|s| = n + k_1 = k - k_0$；$|t| = k_0$。(2) $u \leftarrow t \oplus H(s)$，$v \leftarrow s \oplus G(u)$。(3) $v = m \| 0^{k_1}$ 输出消息 m，否则密文无效。

Rabin-OAEP 加密机制引入了哈希函数 G 和 H，其计算量相对于模幂和模逆等运算来说可以忽略，且具有可证明安全性。Tag 实施加密操作时，只要进行模平方运算和简单的哈希、异或运算，而将相对复杂的求平方根运算留给计算资源相对充裕的 BD，符合上述配置原则。

3.3　Rabin-PSS-MR 签名算法

Rabin 原始签名函数属确定性算法，无法抵抗自适应选择消息攻击。概率签名方案(Probability Signature Scheme, PSS)能实现消息恢复功能，形成 PSS-MR 方案。

3.3.1　密钥设置

运行密钥产生算法 $Gen(1^k)$，得到($N = pq, p, q, G, H, n, k_0, k_1$)，其中，$N = pq$ 是公钥，$p = q = 3 \pmod 4$ 是私钥；$|N| = k = n + k_0 + k_1 + 1$；$2^{-k_0}$ 和 2^{-k_1} 可忽略；$G: \{0,1\}^{k_1} \to \{0,1\}^{k-k_1-1}$，$H: \{0,1\}^* \to \{0,1\}^{k_1}$ 是哈希函数，将 G 拆分成 $G_1 \| G_2$，即 $G_1: \{0,1\}^{k_1} \to \{0,1\}^{k_0}$，$G_2: \{0,1\}^{k_1} \to \{0,1\}^n$；$n$ 是 m 的长度。

3.3.2　签名生成

若要对消息 $m \in \{0,1\}^n$ 进行签名，则必须执行以下计算：(1) $r \leftarrow_U \{0,1\}^{k_0}$; $w \leftarrow H(m \| r)$; $r^* \leftarrow G_1(w) \oplus r$; $m^* = G_2(w) \oplus m$。(2) $y \leftarrow 0 \| w \| r^* \| m^*$。(3)利用私钥 p 和 q 计算 $u \leftarrow q(q^{-1} \bmod p)y^{\frac{p+1}{4}} + p(p^{-1} \bmod q)y^{\frac{q+1}{4}} \pmod N$。

完成上述计算后，将 u 作为消息 m 的签名。

3.3.3　签名验证

收到签名 u 后，执行下列计算：(1) $y \leftarrow u^2 \bmod N$，将 y 分段解释为 $b \| w \| r^* \| \gamma$，其中，b 是 k 位 y 中的第 1 位；w 是后续的 k_1 位；r^* 是接下来的 k_0 位；γ 是其余 n 位。(2) $r \leftarrow G_1(w) \oplus r^*$，$m \leftarrow G_2(w) \oplus \gamma$。(3)若 $H(m \| r) = w$ 且 $b = 0$，则返回消息 m，并确认签名 u 有效，否则认定签名无效。

用 Rabin-PSS-MR 签名算法产生的公钥证书可以在公钥认证过程中只发送证书而无须同时发送公钥。接收方仅利用证书(签名)就可以恢复出公钥消息，极大减少了对通信带宽的要求。且证书的验证只须做模平方运算，可进一步减少 Tag 的工作量。另外，计算量几乎可忽略不计的哈希函数的引入能提供可证明的安全性。

3.4　SMS4 分组加密算法

SMS4[5]分组密码算法主要采用了异或、移位、查表等操作，运行速度比公钥密码算法快，适用于海量数据的加解密。本文用它来提供会话的保密性，关键问题是如何为通信双方分配共享的会话密钥。本文设计的认证方案能在成功认证的同时巧妙实现会话密钥的分配。

4　RFID 认证方案

根据设计原则，给出 3 个认证实体的参数设置及其在认证过程中采用的密码算法，具体参数设置如表 1、表 2 所示。图 2 给出了本文设计的 RFID 认证方案的交互过程。

表 1　认证实体参数设置 1

实体	私钥	公钥
CA	Rabin 私钥：(p_{CA},q_{CA}) p_{CA}=q_{CA}=3 mod 4 $\| p_{CA} \|$=$\| q_{CA} \|$=l_{CA}	Rabin 公钥：N_{CA} $\| N_{CA} \|$=2l_{CA}
Tag	ElGamal 私钥：x_{Tag} $\| x_{Tag} \|$= l_{Tag}	ElGamal 公钥：y_{Tag}=g^(x_{Tag}) mod p_{Tag} $\|y_{Tag}\|$= l_{Tag}
BD	Rabin 私钥：(p_{BD},q_{BD}) P_{BD}=q_{BD}=3 mod 4 $\|p_{BD}\|$=$\|q_{BD}\|$=l_{BD}	Rabin 公钥：N_{BD} $\| N_{BD} \|$= 2l_{BD}

表 2　认证实体参数设置 2

实体	证书	密码运算
CA		Rabin-PSS-MR 签名
Tag	C_{Tag}={Tag, y_{Tag}, T_{Tag}, h_{Tag}} h_{Tag}=Y_{Tag} $^{1/2}$ mod N_{CA} $\|Tag\|$=l_{Tag1},$\|T_{Tag}\|$=l_{Tag2},$\|h_{Tag}\|$=2l_{CA}	Rabin-PSS-MR 签名的验证、Rabin-OAEP 加密、SMS4 解密、改进型 ElGamal 签名、SMS4 加密
BD	C_{BD}={BD，N_{BD}，T_{BD}，h_{BD}} h_{BD}=Y_{BD} $^{1/2}$ mod N_{CA} $\|BD\|$=l_{BD1},$\|T_{BD}\|$=l_{BD2},$\|h_{BD}\|$=2l_{BD}	Rabin-OAEP 解密、SMS4 加密、SMS4 解密、Rabin-PSS-MR 签名的验证、改进型 ElGamal 签名的验证

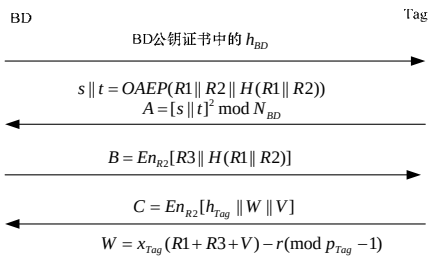

图 2　RFID 认证方案

本文认证方案主要包括以下步骤：(1)BD 把公钥证书 h_{BD} 发送给 Tag。(2)Tag 利用 Rabin-PSS-MR 验证算法验证 BD 公钥证书的合法性，若认证成功，则 Tag 选择随机数 $R1$ 和 $R2$，计算其哈希函数值 $H(R1 \| R2)$，并利用 Rabin-OAEP 方案加密 $R1$, $R2$ 和 $H(R1 \| R2)$，将结果 A 发送给 BD。(3)BD 利用

(下转第 169 页)