第 35 卷 第 4 期 计 算 机 工 程 2009 年 2 月
Vol.35 No.4 Computer Engineering February 2009
·安全技术· 文章编号：1000—3428(2009)04—0172—03 文献标识码：A 中图分类号：TP309

RFID 标签组中的可验证门限秘密共享方案

常振华，陈 越，邵 婧
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：无线射频识别(RFID)标签具有隐蔽、方便、高效等优点，可以作为秘密存储的新载体。该文针对如何在 RFID 标签组中实现秘密共享的问题，提出适用于 RFID 系统的可验证门限秘密共享方案，对其进行安全性分析。根据 RFID 系统的特点提出先认证后读取的实现原则。该方案的安全性基于 RFID 阅读器与标签的双向认证以及求解离散对数的困难性。

关键词：无线射频识别；秘密共享；门限方案；离散对数；零知识

Verifiable Threshold Secret Sharing Scheme in RFID Tags Group

CHANG Zhen-hua, CHEN Yue, SHAO Jing
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 Radio Frequency Identification(RFID) tags have the advantages of concealment, convenience and high efficiency, and can be used as new carriers of secret storage. Aiming at implementing secret sharing in RFID tags group, this paper proposes a verifiable threshold secret sharing scheme, which is fit for RFID system, and analyzes its security features. According to characteristics of RFID system, the first authenticating then reading implementing principle is suggested. The security of this scheme is based on the mutual authentication of reader and tags and the difficulty of computing the discrete logarithm modulo for a composite number.

【Key words】 Radio Frequency Identification(RFID); secret sharing; threshold scheme; discrete logarithm; zero-knowledge

1 概述

随着无线射频识别(Radio Frequency Identification, RFID)技术的不断发展，各种 RFID 系统被广泛用于制造业、供应链管理、电子支付、传感通信、身份识别等领域。RFID 标签是一个带天线的微芯片，可以响应阅读器的查询并与阅读器进行数据交换。RFID 可以提高系统效率、节约成本，但带来了安全和隐私问题。研究者提出通过辅助隐私保护设备[1]、安全协议[2-3]或政策法律[4]等手段，在保证商业价值和方便顾客的前提下加强 RFID 的安全性和隐私性。

本文研究如何在一组 RFID 标签中分割并恢复一个组密钥(Group Key, GK)。RFID 标签仅有有限存储空间，但足够存储类似密钥的少量数据。在 RFID 标签组中实现共享秘密是一种新的 RFID 标签应用方式，目前没有相关方案。本文提出的方案可以方便地将 RFID 标签用于密钥托管、多标签同时控制一个设备、高安全性要求的标签组认证等应用。

将 RFID 标签组中的 GK 分段，并将各段保存在该组标签内，可以实现 RFID 标签组之间的秘密共享。上述方法很简单，但存在以下不足：(1)必须对分段进行编号；(2)系统成员数量有变动时必须重新分段；(3)灵活性差，在某些应用(例如，要求当 n 个标签控制同一个设备时，只要 $k(k\leq n)$个以上到场就能开启设备)中无法使用。另一种方法是采用(k, n)门限秘密共享方案，只要有 $k(k\leq n)$个标签同时在场就能恢复 GK。特别地，当 $k=n$ 时，只要所有标签同时在场即可。但一般的门陷方案存在验证者不能对提供的子密钥进行验证的缺点。为增加共享 GK 的安全性、可靠性和灵活性，本文考虑 RFID 标签能提供的计算能力，提出适用于 RFID 系统的标签组可验证(k, n)门限秘密共享方案。子密钥的产生采用 Shamir(k, n)门陷秘密共享方案[5]，GK 和子密钥的隐藏与验证基于离散对数[6]的单向性。

由于标签计算能力的限制，标签不可能验证分发者提供的子密钥，因此可验证性限于后端服务器对标签所提供子密钥的真实性和所恢复 GK 正确性的验证。

2 方案描述

2.1 主要思想

由于阅读器和标签之间以无线电为通信媒体，因此其通信完全向窃听者和信号分析者暴露。攻击者可以通过监听、假冒、重放等方式来攻击标签和阅读器。为确保会话对象的真实性，会话双方必须采取双向认证机制。为确保子密钥传递的机密性，子密钥在传递过程中必须进行加密。因此，本文提出“先认证后读取”的实现原则。为了保证会话的新鲜性，设置组成员标签认证和组密钥恢复的时间阈值分别为 t_1 和 t_2。本文方案的步骤如下：

(1)在时间 t_1 内完成成员标签的认证。实现标签与阅读器之间的双向认证，并为后续会话传递提供一个一次一换的随机会话密钥(Random Session Key, RSK)和作为会话序号的时间戳(Date Timestamp, DT)。对成员标签的认证具有如下意义：1)组中成员标签退出时只要删除其成员认证信息，使之不再被认证为成员标签，进而不能参加组认证；2)提高安全性，非法阅读器和标签在第(1)步就能被识破，防止了秘密信息的泄露。

(2)在时间 t_2 内完成子密钥的读取和 GK 的恢复。在成员标签认证的基础上，阅读器读取在场标签中的子密钥，恢复

作者简介：常振华(1975－)，男，工程师、硕士研究生，主研方向：网络与信息安全，射频识别技术；陈 越，教授、博士；邵 婧，硕士研究生

收稿日期：2008-07-14 **E-mail：**spring_colorsun@yahoo.com.cn

出 GK，并验证其正确性。如果将该方案应用于标签组认证，GK 可以作为一组标签同时在场的证明。

2.2 标签假设

由于尺寸和成本的限制，标签是很小、无电源的微芯片，它们只能提供数量有限的存储空间和基本计算操作。假设标签有一个单向 hash 函数 $H:\{0,1\}^{*}\rightarrow\{0,1\}^{l}$、一个伪随机数发生器(Pseudorandom Number Generator, PRNG)、一定内存(用于存储 RSK)和非易失性存储器以及基本的运算能力(如 XOR)。文献[7]中指出，实现一个 hash 函数模块，只需要约 1 700 个门，因此，上述假设对低成本标签是合理的。

组内所有标签和数据库系统之间预共享一个组会话密钥(Group Session Key, GSK)。标签和数据库系统有相同的单向 hash 函数。为了简化描述，用 R 代表阅读器，用 B 代表后端数据库系统，用 T_i 代表每个成员标签。

2.3 系统初始化

2.3.1 参数选取

设标签组为 $G=\{T_1,T_2,\cdots,T_n\}$，其中，n 为组中标签的个数。分发者 Dealer 选择一个大的强素数 p，即存在素数 q，使 $p=2q+1$。g 为 $GF(p)$的生成元。p 和 g 在系统中公开。随机生成向量 $\boldsymbol{V}=(v_1,v_2,\cdots,v_n)$，其中，$v_i\neq0(i=1,2,\cdots,n)$。

2.3.2 标签注册和子密钥分发

Dealer 随机选取(k-1)阶多项式，即

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_{k-1}x^{k-1} \tag{1}$$

其中，$a_i\in Z_P^{*}(i=1,2,\cdots,k\text{-}1)$; $a_0=GK$。

对每个标签 $T_i(T_i\in\mathrm{G})$，计算其子密钥 x_i 和相应的公开密钥 y_i，有

$$\begin{cases}x_i=f(v_i)\bmod p\\ y_i=g^{x_i}\bmod p\end{cases} \tag{2}$$

其中，$i=1,2,\cdots,n$。计算

$$y_G=g^{a_0}\bmod p \tag{3}$$

作为 GK 的公开密钥。

Dealer 将 x_i 通过安全信道分发给组中的每个成员标签，将 y_i 存入后台数据库中成员标签对应的记录，并记录 y_G。如果系统中有多个标签组，则对不同的标签组，可以选择不同的多项式和子密钥生成向量，并在标签记录中以不同组标识指示其所属组。

2.4 成员标签认证阶段

从认证标签组 G 中第 1 个成员标签开始计时，如果在时间 t_1 内完成对组 G 中 k 个以上成员标签的认证，则认为成员标签认证成功，否则停止协议执行。每个成员标签 T_i 的认证过程如图 1 所示。

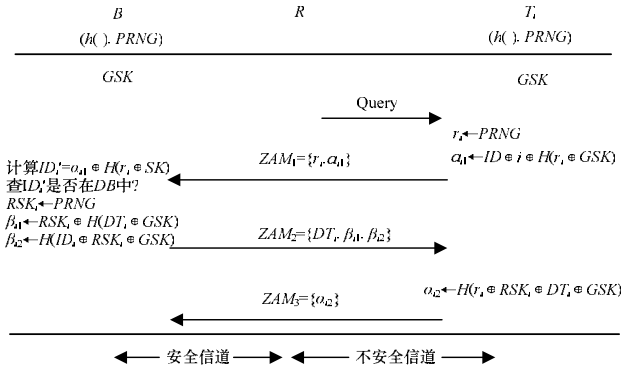

图 1　成员标签的认证过程

成员标签的认证过程描述如下：

(1)R 向 T_i 发送 Query 认证请求。

(2)T_i 产生一个随机数 r_i，使用自己的 ID_i 和 GSK 计算 $\alpha_{i1}=ID_i\oplus H(r_i\oplus GSK)$，形成 $ZAM_1=\{r_i,\alpha_{i1}\}$并发送给 R。

(3)R 将 ZAM_1 转发给 B。

(4)B 计算 $ID_i'=\alpha_{i1}\oplus\mathrm{H}(r_i\oplus GSK)$，在数据库中查找是否有这样的 ID_i'，如果有，则 T_i 通过初步认证，之后 R 产生随机数作为 RSK_i，计算 $\beta_{i1}=RSK_i\oplus H(DT_i\oplus GSK)$，$\beta_{i2}=H(ID_i\oplus RSK_i\oplus GSK)$，形成 $ZAM_2=\{DT_i,\beta_{i1},\beta_{i2}\}$发给 R，其中，DT_i 为时间戳，是 B 的系统时间或具有时间戳功能的随机数，用于防止重放攻击，并作为本次会话的序号，合法的 T_i 可以用 β_{i1} 恢复出 RSK_i，用 β_{i2} 验证 RSK_i 的有效性，并验证 R 的合法性。

(5)R 将 ZAM_2 转发给 T_i。

(6)T_i 收到 ZAM_2 后，先判断 DT_i，如果比以前保存的大，则认为正常，然后 T_i 用自己的 GSK 计算 $H(DT_i\oplus GSK)$，恢复出 RSK_i，并进行验证，如果正确则通过对 R 的认证，并保存 DT_i，计算 $\alpha_{i2}=H(r_i\oplus GSK\oplus RSK_i\oplus DT_i)$，形成再次认证消息 $ZAM_3=\{\alpha_{i2}\}$发送给 R，作为对 ZAM_2 的应答。该应答是零知识的，确认正确收到 RSK_i，且证明 T_i 是整个认证会话的参与者。若 DT_i 不正常或 RSK_i 无效，则忽略 ZAM_2 并保持静默。

(7)R 将 ZAM_3 转发给 B，B 计算 $H(r_i\oplus GSK\oplus RSK_i\oplus DT_i)$，与收到的 α_{i2} 进行比较，如果相等则通过对 T 的认证。

2.5 子密钥读取和 GK 恢复阶段

如果成员标签认证成功，则开始读取每个标签的子密钥。子密钥读取和验证过程如图 2 所示。

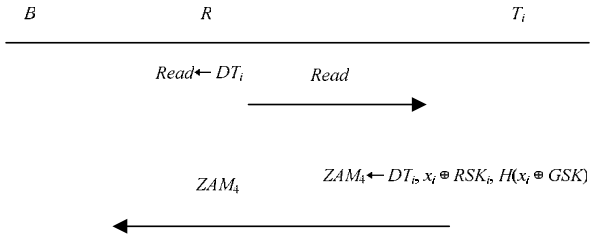

图 2　子密钥读取和验证过程

子密钥读取和验证过程描述如下：

(1)R 以 $Read=\{DT_i\}$作为读取标签 T_i 子密钥的读消息。

(2)T_i 以 $ZAM_4=\{DT_i,\ x_i\oplus RSK_i,\ H(x_i\oplus GSK)\}$作为对 $Read$ 消息的响应发送给 R。消息的第 2 部分 $x_i\oplus RSK_i$ 用于恢复 x_i，第 3 部分 $H(x_i\oplus GSK)$用于对 x_i 的验证。

(3)R 将 ZAM_3 转发给 B，由 B 恢复出 x_i 并验证。如果通过验证，则验证 $g^{x_i}\bmod p$ 是否与保存的 y_i 相等，若不等，则认为该标签提供的子密钥为非法子密钥。

(4)B 获得 k 个以上合法子密钥后，恢复出 GK 并验证 $g^{GK}\bmod p=y_G$ 是否成立，如果通过验证则说明恢复成功。

3 安全性分析

3.1 机密性

本文协议基于零知识思想，在完成认证和子密钥传递时，确保不泄露标签 ID、共享密钥和子密钥等信息。单向 hash 函数确保了从成员标签的认证消息和子密钥读取消息中无法获得标签的 GSK 等敏感信息。协议采用共享 GSK，使阅读器和标签对收到的信息可以进行正确性和完整性验证，从而保证认证信息和交换 RSK 的机密性。

当攻击者想从数据库直接获取 GK 或各子密钥时，将面

对求解 $GF(p)$上离散对数的难题，可见，离散对数体制确保了对 GK 和子密钥的可验证性并保证了它们的安全性。

采用门限秘密共享方案，保证对于任意 $r(r \geq k)$个合法标签在场，很容易恢复 GK。而任意 $r(r < k)$个标签在场时，对恢复 GK 没有任何帮助。

3.2 可认证性

在成员标签的认证阶段采用双向身份认证机制，有效防止了未授权的阅读器和假冒标签参与会话，增加了认证的可靠性。子密钥的传递由 RSK 进行加密保护，并提供相应认证。可验证的门限秘密共享机制提供了对成员标签子密钥的合法性和来源的认证，认证结果可以用于审计。

3.3 可用性

针对不同攻击，对本文方案的可用性分析如下：

(1)假冒 RFID 阅读器攻击，即攻击者假装成有效阅读器。此攻击会被 DT, RSK 和 GSK 的组合击败，因为只有合法阅读器才能提供一个有效认证消息，所以假冒阅读器采用重放或篡改等方式向标签作认证时会被标签识破。

(2)假冒 RFID 标签攻击。攻击者假装成有效标签的攻击包括 2 种情况：

1)攻击者发出假的 ZAM_1，在没有 GSK 的情况下，此攻击在对标签的初次认证时就会被 B 识破；

2)攻击者对阅读器重放某次有效标签的 ZAM_1 进行攻击，该攻击虽然能使 B 产生 ZAM_2，但在再次认证时，由于攻击者没有正确的 GSK，不可能恢复 RSK_i，因此不能构造出正确的 ZAM_3，无法通过系统对其的再次认证。

(3)跟踪标签位置攻击。因为标签每次发出的认证消息都不同，所以跟踪者无法判定跟踪的是否是同一个标签。

(4)中间人攻击。假定协议在长距离下工作，由中间人转发认证消息，而认证和响应都是加密且零知识的，因此，会话的消息对于中间人是透明的，通过直接读取消息，攻击者只能得知阅读器和标签在通信，而不能得到任何秘密信息。即使攻击者通过转发标签的请求认证消息和再次认证消息而通过阅读器的认证，仍然不可能获得 RSK，因此，无法得到标签的子密钥。

4 结束语

在 RFID 标签组中实现秘密共享是标签作为一种新数据载体的应用。该应用发挥了标签体积小、防复制和伪造、便于携带和读取、抗恶劣环境使用等优点。本文结合 RFID 系统特点，提出一种适用于标签计算量且安全可靠的实现方案，具有一定借鉴和参考意义。

参考文献

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

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

[3] Henrici D, Müller P. Hash-based Enhancement of Location Privacy for Radio-frequency Identification Devices Using Varying Identifiers[C]//Proceedings of the 2nd IEEE Annua1 Conf. on Pervasive Computing and Communications. Washington D. C., USA: IEEE Press, 2004: 149- 153.

[4] Garfinkel S. An RFID Bill of Rights[Z]. Massachusetts Institute of Technology, 2002.

[5] Shamir A. How to Share a Secret[J]. Communication of the ACM, 1979, 24(11): 612-613.

[6] Odlyzko A M. Discrete Logarithms in Finite Fiends and Their Cryptographic Significance[C]//Proceedings of EUROCRYPT. [S. l.]: Springer-Verlag, 1985: 224-314.

[7] Yüksel K. Universal Hashing for Ultra-low-power Cryptographic Hardware Applications[D]. Worcester, USA: Worcester Polytechnic Institute, 2004.

(上接第 171 页)

3.4 抗攻击性实验

将图像旋转 45°，检测得到的角点如图 1(b)所示。先确定参照三角形 ABC 和 CDE 的位置，根据式(4)确定仿射变换的系数，对图像进行重建后，再检测水印。可以看到在 u_1 =34 和 u_2 =67 处出现较强的冲激特征。将图像分别放大 0.8 倍和 1.8 倍后，检测到的角点分别如图 1(c)和图 1(d)所示，可以精确地定位 2 个参考三角形，并与原始三角形的位置进行比较，就能确定缩放倍数，重建后的检测结果与图 2 所示结果相同。

对图像进行质量系数为 6%的 JPEG 压缩，或加入信噪比为 31.13 dB 的高斯噪声时，在 u_1 =34 和 u_2 =67 处仍然可以看到较强冲激，表明算法能很好地抵抗常见信号处理操作。

4 结束语

本文利用角点抵抗几何攻击的特性，实现对几何攻击后的图像进行重建。本文算法对 JPEG 压缩、加噪等信号处理操作有很好的抵抗力，且对旋转、缩放等几何攻击具有较高鲁棒性。

参考文献

[1] Barni M, Bartolini F, Cappellini V, et al. A DCT-domain System for Robust Image Watermarking[J]. Signal Processing, 1998, 66(3): 357-372.

[2] Lin Chingyung, Ingemar J C. Rotation, Scale, and Translation Resilient Watermarking for Image[J]. IEEE Transactions on Image Processing, 2001, 10(5): 767-782.

[3] Djurovic I, Stankovic S, Pitas I. Digital Watermarking in the Fractional Fourier Transformation Domain[J]. Journal of Network and Computer Applications, 2001, 24(1): 167-173.

[4] He Xiaochen, Yung N H C. Curvature Scale Space Corner Detector with Adaptive Threshold and Dynamic Region of Support[C]// Proceedings of the 17th International Conference on Pattern Recognition. Cambridge, USA: [s. n.], 2004: 791-794.

[5] Almeida L B. The Fractional Fourier Transform and Time-frequency Representations[J]. IEEE Transactions on Signal Processing, 1994, 42(11): 3084-3091.