带 TTP 的多所有者内部权重变化所有权转换协议

甘 勇 王 凯 贺 蕾
(郑州轻工业学院计算机与通信工程学院 郑州 450002)

摘 要 在实际应用中,多所有者 RFID 标签的所有权不仅是由于标签的所有者发生了变化而改变,每个所有者所占有的权重比例发生变化也会导致标签的所有权发生改变。因此,文中提出了一种带可信第三方(Trusted Third Party,TTP)的多所有者内部权重变化标签所有权协议用以解决该问题,因为存在 TTP 参与所有权的转换,所以所有者完全地将对标签的所有权转移给了权重变化后的所有者,即具备原所有者无关性。该协议采用了 Lagrange 多项式插值法和 Shamir 秘密共享门限方案,并使用 GNY 逻辑进行了安全性分析,结果表明该协议能抵抗转换过程中的多种攻击。同时,仿真实验结果表明标签耗时和计算量都处于可接受的范围之内。

关键词 所有权转换,可信第三方,原所有者无关性,拉格朗日,秘密共享,GNY 逻辑
中图法分类号 TP393.04 **文献标识码** A

Ownership Transfer Protocol for Multi-owners Internal Weight Changes with Trusted Third Party

GAN Yong WANG Kai HE Lei
(School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China)

Abstract In practical application, the ownership of multi-owner RFID tags transfers due to changes not only in owners of the tags, but also in the proportion of weights possessed by each owner. Therefore, in this paper, a tag ownership protocol for multi-owner internal weight changes with trusted third parties (TTP) was put forward to resolve this problem. As there is a trusted third party involved in the conversion of ownership, the original owner completely transfers the tag's ownership to the new owner after the weight changes, which means original owners in the protocol are irrelevant. Lagrange interpolating polynomial and Shamir's threshold secret sharing scheme are used in the protocol, and security analysis is conducted with GNY logic. The results show that the protocol can resist all kinds of attacks in the process of conversion. Meanwhile, the results of simulation experiments indicate the time consumption of tags and the amount of calculation fall within an acceptable range.

Keywords Ownership transfer, Trusted third party, Independence of old owner, Lagrange, Secret sharing, GNY logic

RFID(Radio Frequency Identification) 技术主要依赖于无线电波技术和标签来存储和检索相关实体对象的信息,而不需要与对象物理接触,并且根据获得的数据可以唯一地识别对象[1]。由于超高频 RFID 系统的进步、自动识别中心开发的低成本和基于开放标准的系统、互联网的普及以及其本身所具有的一系列特性等,RFID 被公认为是当前最重要且最炙热的技术之一[2]。随着 RFID 技术的快速发展和广泛应用,RFID 系统中所有权的安全转换也面临新的挑战。单所有者的所有权转换已经不能满足实际应用需求了,在供应链、建筑质量监管等应用领域[3],标签的所有者可能有多个,多个实体共同拥有对标签的所有权,标签与所有者之间会有可信第三方这个通信实体,而且不同所有者所占有的权重份额也可能不同。在这种情况下,一种带 TTP 的多所有者内部权重变化标签所有权转换协议的研究有着重要的价值。RFID 技术的安全和隐私问题是制约其发展和广泛应用的主要障碍,大量研究人员对标签的所有权转换进行了多方面的研究。下面就已存在的几个所有权转换协议进行简要的分析。2010 年,Kulseng 等[4]首先设计了一种轻量级 RFID 安全认证协议,在该协议中只有标签和阅读器之间通过了合法的安全认证后才能进行相互通信。随后,基于该认证协议,他们又设计了一个所有权转换协议。该协议不仅使用了线性反馈位移寄存器和物理克隆技术,而且还使用了可信第三方,因此在提高协议效率的同时也限制了其应用范围。该协议的安全性和可靠性也没有得到认证,对是否能抵抗去同化攻击等都没有详细分析。2011 年,Zhou 等[5]提出了一种用于供应链管理的标签所有权转换方案,该方案包含 5 个通信实体,分别为原所有者、新所有者、标签、可信第三方和第三方物流,但该方案不能抵抗去同步化攻击。金永明等[6]提出了一种基于 SQUASH 方案的轻量级所有权转换协议,但该协议中存在安全漏洞,攻击者可以通过三轮的窃听、重放以及假冒,最终使所有者与标签共享的密钥不相同,使攻击者能够成功地实施拒绝服务攻击和重放攻击。2012 年,Kapoor 等[7]提出了两个所有权转换协

本文受国家自然科学基金(61572445,61772477),河南省高等学校重点科研项目(16A520075)资助。
甘 勇(1965-),男,博士,教授,CCF 会员,主要研究方向为分布式计算机系统、计算机网络、信息安全;王 凯(1993-),男,硕士生,主要研究方向为无线网络安全、RFID 密码协议安全,E-mail:2403411494@qq.com(通信作者);贺 蕾(1980-),男,讲师,主要研究方向为无线网络安全、密码学、软件安全与保护。

议，一个需要可信第三方参与，另外一个不需要可信第三方参与。这两个协议都需要使用专用密钥密码算法来保护标签与所有者之间的通信信息，标签的计算量较大。Jia 等[8]提出的所有权转换协议采用了公钥加密密码算法，在读写器与后端数据库之间构建一个安全可靠的通信信道，然后在标签与读写器之间进行认证通信，在此基础上进行所有权转换，但该协议存在的问题是不能抵抗跟踪攻击。2013 年，贺蕾等[9]提出了一种基于随机排列函数的 RFID 标签所有权转换协议，其中随机排列函数是在线性反馈移位寄存器和物理不可克隆函数的基础上进行构建的，该协议适用于低成本标签，但不具备原所有者无关性。Doss 等[10]基于数学二次剩余的思想，提出了一种新的标签所有权转换协议，该协议的思想较新颖，但仅能应用于无源标签，在实际应用中具有很大的局限性。2014 年，沈金伟等[11]提出了一种改进的超轻量级 RFID 所有权转换协议，但该协议仍然存在新的安全漏洞和成本花销问题。2015 年，毛雅佼等[12]提出了一种新的 RFID 标签所有权转换协议，该协议采用了挑战响应机制，使标签与新旧所有者分别共享不同的密钥，实现了标签所有权的排他转移，但该协议存在不安全的因素，不能够抵抗中间人攻击和保护标签信息的前向安全。2016 年，苑津莎等[13]设计了基于供应链环境的所有权转移方案，在生产阶段产品处于内部封闭系统中，为保证标签及产品不被跟踪，采用了基于伪 ID 的物联网安全认证方法来认证标签；同时，在销售阶段采用了基于非对称密钥和 Hash 函数的 RFID 双向认证协议认证标签。认证成功后执行对应的所有权转移方法及标签认证数字更新方法。该方案能够实现所有权和标签信息的完全转移，但该方案不能抵抗去同步化攻击。2017 年，苏庆等[14]提出了一种基于密钥共享的超轻量级 RFID 标签所有权转换协议，该协议可以抵御去同步化攻击、拒绝服务攻击、重放攻击、假冒攻击、中间人攻击，且能够保护标签信息的前向安全。但是该协议并不能有效安全地保护标签信息的后向安全，即不具备原所有者无关性。同时，文献[15]提出了一种改进的基于 Rabin 加密算法的 RFID 标签所有权转移协议，该协议采用挑战响应机制，利用 Status 标志位来标志标签当前所有权的归属，虽然该协议具有很好的安全性，但是其计算量、通信量和所占存储空间太大，不适用于低成本标签。文献[16]提出了一种基于 ECC 的支持标签所有权转移的 RFID 认证协议，该协议的结构类似于 Diffie-Hellman 密钥交换算法结构，协议的标签隐私保护基于椭圆曲线上的计算性 Diffie-Hellman 问题的难解性。另外，针对较安全的应用场合，给出了阅读器单向认证标签的简化版协议。但是该协议的成本花销太大，同时不能实现所有权的完全转移。

经过以上分析发现，现已存在的所有权转换协议存在下列问题或者之一：1）没有具备原所有者无关性，即原所有者没有完全地将标签的所有权转移给新所有者，不能保护标签信息的后向安全；2）在现有研究成果中，研究的都是标签具有单一所有者的情况，即标签只具有一个所有者；3）拥有标签不同份额即权重不同的多个所有者进行 RFID 标签所有权转换时的安全隐私问题并没有得到完美的解决。

1　协议描述

标签可以被具有不同权重的多个所有者共同拥有，并且一些所有者可以向其他所有者出售他们或多或少的权重。在标签的生存周期中所有者的权重可能变换，因此需要及时更新密钥以保证所有权的动态更新。本文设计了一个在 TTP 参与转换下的 RFID 标签多所有者内部权重发生变化的所有权转换协议，以实现多个所有者之间权重发生变化后的所有权转换。

1.1　主要思想

首先运用 Shamir 秘密共享门限方案，将共享密钥分割成若干子密钥，再根据所有者的权重把这些子密钥通过安全信道分发给多个所有者。当所有者的权重发生变化时，该协议将使用拉格朗日多项式插值法，在参与恢复密钥的所有者权重之和等于或大于某一阈值的条件下恢复出原密钥，同时验证原所有者的合法性；当需要进行标签所有权转换时，同意进行所有权转换的所有者权重之和大于或等于先前设定好的阈值，才可以恢复出标签的共享密钥，否则不能恢复密钥，从而保证了所有权转换过程中的可靠性和安全性。

1.2　拉格朗日插值法

对于一个多项式函数，已知 $k+1$ 个取值点，即 $(x_0,y_0),\cdots,(x_k,y_k)$，其中 x_j 是自变量，y_j 就是对应该函数在自变量上的函数值。假设任何一个自变量 x_j 都是互不相等的，根据拉格朗日插值公式得到的多项式为：

$$L(x):=\sum_{j=0}^{k}y_j l_j(x) \tag{1}$$

其中，$l_j(x)$ 是拉格朗日插值基函数，其表达式为：

$$\begin{aligned} l_j(x)&=\prod_{i=0,i\neq j}^{k}\frac{x-x_j}{x_j-x_i}\\ &=\frac{(x-x_0)}{(x_j-x_0)}\cdots\frac{(x-x_{j-1})}{(x_j-x_{j-1})}\frac{(x-x_{j+1})}{(x_j-x_{j+1})}\cdots\frac{(x-x_k)}{(x_j-x_k)} \end{aligned} \tag{2}$$

拉格朗日插值基函数 $l_j(x)$ 的特点就是在 x_j 上取值为 1，在别的点 $x_i(i\neq j)$ 上取值为 0。

1.3　Shamir 秘密共享门限方案

本文主要用的是基于 Lagrange 多项式插值的 Shamir(t,n) 秘密共享门限方案，该方案主要包括 3 个过程，即初始化过程、密钥分发过程以及密钥恢复过程。

（1）初始化过程

假设一个密钥被 $P_1,P_2,\cdots,P_n$ 等多个参与者共同拥有，$x_1,x_2,\cdots,x_n$ 分别为这多个参与者的身份标识，S 就是从有限域中选取的共享密钥。

（2）密钥分发过程

密钥的分发者在有限域 $GF(q)$（q 为大素数）中任意选择 $t-1$ 个元素 $a_1,a_2,\cdots,a_{t-1}$，构造多项式：

$$f(x)=S+\sum_{i=1}^{t-1}a_i x^i \tag{3}$$

然后根据参与者的身份标识为其分配相应的子秘密：

$$y_i=f(x_i),i=1,2,\cdots,n \tag{4}$$

最后经过安全通信信道将 y_i 发送给各个参与者。

（3）密钥恢复过程

当参加恢复密钥的参加者人数大于或者等于 t 时，就可以根据 Lagrange 多项式插值公式算出密钥值。

$$f(0)=\sum_{i=1}^{t}y_i\{\prod_{1\leqslant j\leqslant t,i\neq j}\frac{(0-x_j)}{(x_i-x_j)}\} \tag{5}$$

其中，x_i 和 y_i 分别为参与者的身份标识以及子密钥。

2 协议设计

2.1 系统初始化

设 $P=\{P_1,P_2,\cdots,P_n\}$ 为标签的 n 个权重变化前的所有者，W_i 为所有者 P_i 相应的权重，W_{mij} 为所有者 P_i 向所有者 P_j 购买的权重份额(其中 m 为购买的份额比例)，W_{ni}(上界为 L)为所有者 P_i 权重产生变换后新一轮对应的权重值，L 为参与恢复密钥所有者权重的上界。Tag 表示标签，TID 代表标签的唯一身份标识，S 表示用于与原所有者通信的原密钥，S_{ij}($1\leqslant j\leqslant w_i$)表示不同权重的所有者得到的不同数量的子密钥，$S_{new}$ 表示与所有权发生变化后的所有者通信的密钥，S_{nij}($1\leqslant j\leqslant w_i$)代表不同权重的所有者根据新权重值得到的不同数量的子密钥。R_{pi} 表示所有者 P_i 生成的随机数，R_{ti} 表示标签为所有者 P_i 生成的随机数，R_{pti} 表示后端数据库为所有者 P_i 生成的随机数，R_{ttpi} 表示 TTP 与所有者 P_i 通信过程中生成的随机数，$H(x)$ 为对变量 x 求其 $Hash$ 值，a,b 为变量 a 和 b 的串联，$a\oplus b$ 为变量 a 和 b 的异或。PID_i 代表所有者 P_i 的唯一身份标识，ID_{TTP} 为 TTP 的唯一身份标识，K 代表标签和 TTP 的共享密钥。

2.2 所有权出售过程

设一个标签 Tag 有 3 个所有者 P_1,P_2,P_3，每一个所有者的权重分别为 2,1,3，而且 P_1,P_2,P_3 之间的通信信道是安全的，权重值为 2 的所有者 P_1 向权重值为 3 的所有者 P_3 购买一份份额，并且所有者 P_2 也向所有者 P_3 购买了一份份额，同时也向所有者 P_1 购买了一份份额。这时权重值完全发生变化，每一个所有者新的权重值分别变为 2,3,1，具体的购买过程如图 1 所示。

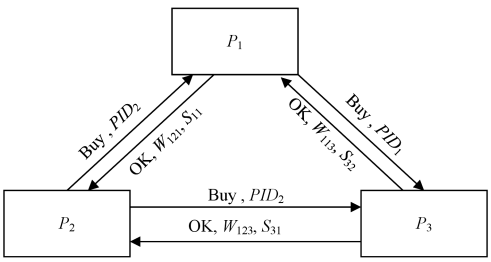

图 1 所有者权重发生变化的过程

从图 1 可以清楚地看到，当所有者 P_2 想要向所有者 P_3 购买权重份额时，它将发送购买请求 Buy 和自己的身份标识 PID_2 给所有者 P_3。当 P_3 同意出售份额给 P_2 时，P_3 将发送同意购买申请 OK、P_2 所购买的权重份额 W_{123}、一份子密钥 S_{31} 给 P_2。同样地，P_2 向所有者 P_1 以及 P_1 向所有者 P_3 购买权重份额的过程类似。

2.3 密钥恢复认证过程

当有标签所有者出售其权重份额后，标签的所有者权重比例发生变化。原所有者即权重比例发生变化前的所有者需与标签完成双向认证，并还原出所有者与标签通信的原密钥 S。此时需要在可信第三方的参与下进行双向认证，以防止有攻击者假冒正常的所有者向标签发送通讯信息，同时也为了具备原所有者无关性这种特性，即所有者完全地将对标签的控制所有权转移给权重变化后的所有者，保护了标签信息的后向安全。具体的恢复认证过程如图 2 所示，为了研究的方便，假设标签与所有者之间的通信信道是不安全的，而其他通信信道是安全的。

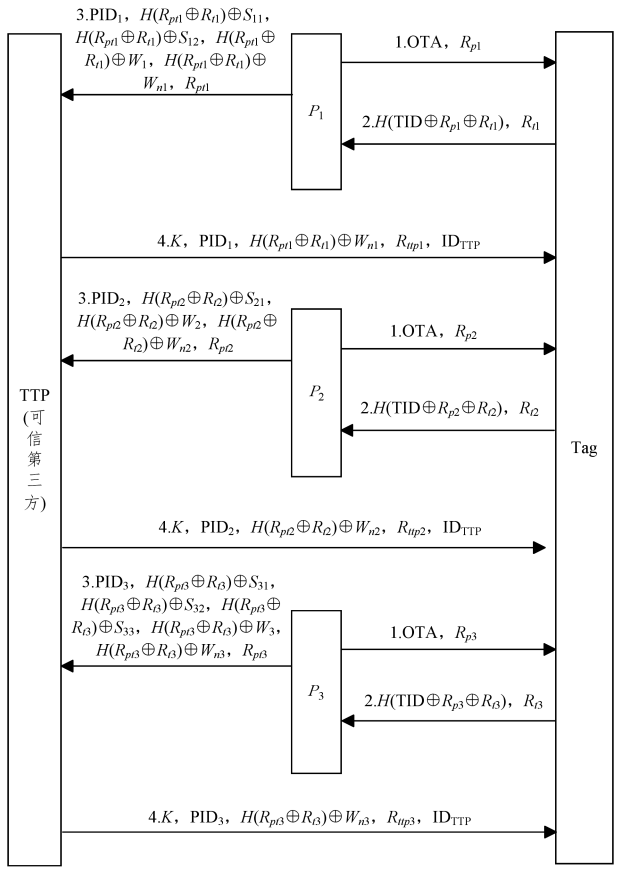

图 2 所有者和标签恢复认证过程

(1)所有者 P_1 向标签 Tag 发送 OTA(Ownership Transfer Allowance)，OTA 为所有权转换许可，并生成随机数 R_{p1}，将 R_{p1} 和 OTA 同时发送给标签。

(2)标签从 P_1 接收到 OTA 之后，生成随机数 R_{t1} 并计算 $M=H(TID\oplus R_{p1}\oplus R_{t1})$，将 $H(TID\oplus R_{p1}\oplus R_{t1})$ 和 R_{t1} 发送给所有者 P_1。

(3)当所有者 P_1 接收到来自标签的消息时，后端数据库生成随机数 R_{pt1}，所有者 P_1 将发送 PID_1，$H(R_{pt1}\oplus R_{t1})\oplus S_{11}$，$H(R_{pt1}\oplus R_{t1})\oplus S_{12}$，$H(R_{pt1}\oplus R_{t1})\oplus W_1$，$H(R_{pt1}\oplus R_{t1})\oplus W_{n1}$ 以及 R_{pt1} 给 TTP。

(4)TTP 接到 P_1 的通信信息后，检查其准确性。若其不正确，则认为所有者 P_1 是假冒的，协议停止，即所有者 P_1 没有通过认证。若其正确，则所有者 P_1 认证通过。TTP 生成随机数 R_{ttp1}，并发送 $K,PID_1,H(R_{pt1}\oplus R_{t1})\oplus W_{n1},R_{ttp1}$ 和 ID_{TTP} 给标签。

(5)同样地，TTP 接到 P_2,P_3 的通信信息后，检查其准确性。若其不正确，则认为所有者是假冒的，协议停止，即所有者没有通过认证。若其正确，则所有者认证通过。TTP 生成随机数 R_{ttp2} 和 R_{ttp3}，并发送 $K,PID_2,H(R_{pt2}\oplus R_{t2})\oplus W_{n2}$，$R_{ttp2},ID_{TTP}$ 以及 $K,PID_3,H(R_{pt3}\oplus R_{t3})\oplus W_{n3},R_{ttp3},ID_{TTP}$ 给标签。

(6)标签 Tag 接到 TTP 发送的通信信息后，判定其参加还原密钥的参与者权重之和是否满足要求的阈值(大于或者等于阈值)，若满足条件则标签根据 Lagrange 多项式插值法恢复出密钥 S'，并且用标签的原密钥 K 与 Lagrange 多项式插值法还原出的 S' 进行比较，如果存在 $K=S'$，说明标签经过认证，所有者与标签之间完成了双向认证，并恢复出了权重

值变化前的原密钥 S。

2.4　所有权转换过程

标签对收到的所有者新旧权重值进行对比，以判断权重值是否发生变化，若发生变换，则将标签的密钥更新为 S_{new}，再通过安全信道将所有者权重值变化后的新权重分发给所有者新的子密钥。标签在有限域 GF(q)(q 为大素数)中任意选择 $t-1$ 个元素 $a_1, a_2, \cdots, a_{t-1}$，并构造多项式：

$$f(x)=S_{\text{new}}+\sum_{i=1}^{t-1}a_i x^i \tag{6}$$

然后根据新权重 w_{ni} 为其分配相应的子密钥：

$$S_{nij}=f(x_{ij}),1\leqslant j\leqslant w_{ni} \tag{7}$$

其中，$x_{ij}=(i-1)L+j$，L 为参与恢复密钥所有者权重的上界，然后通过安全信道将 S_{nij} 发给各个所有者，至此便完成了多个所有者内部权重变化的所有权转换过程。

3　性能分析

3.1　安全性分析

本文采用 GNY 逻辑对协议的安全性进行简要的分析。GNY 逻辑是一种常用的形式化分析方法，是第一个对 BAN 逻辑进行增强扩充的类 BAN 逻辑。使用该分析方法进行安全性分析时，在分析过程中进行形式化描述，设定初始化假设，依据推理规则分 3 个步骤进行分析。本文所用的表述方式和推理规则遵守文献[17]中的相应要求和内容。

3.1.1　协议形式化描述

M1：$T \lhd {}^{*} OTA, {}^{*} R_{p1}$

M2：$P_1 \lhd {}^{*} R_{t1}, {}^{*} H(TID \oplus R_{p1} \oplus R_{t1})$

M3：$TTP \lhd {}^{*} PID_1, {}^{*} H(R_{pt1} \oplus R_{t1}) \oplus S_{11}, {}^{*} H(R_{pt1} \oplus R_{t1}) \oplus S_{12}, {}^{*} H(R_{pt1} \oplus R_{t1}) \oplus W_1, {}^{*} H(R_{pt1} \oplus R_{t1}) \oplus W_{n1}, {}^{*} R_{pt1}$

M4：$T \lhd K, {}^{*} R_{tp1}, {}^{*} PID_1 \sim > P_1 \sim OTA, {}^{*} H(R_{pt1} \oplus R_{t1}) \oplus W_{n1}, {}^{*} ID_{TTP}$

M5：$T \lhd {}^{*} OTA, {}^{*} R_{p2}$

M6：$P_2 \lhd {}^{*} R_{t2}, {}^{*} H(TID \oplus R_{p2} \oplus R_{t2})$

M7：$TTP \lhd {}^{*} PID_2, {}^{*} H(R_{pt2} \oplus R_{t2}) \oplus S_{21}, {}^{*} H(R_{pt2} \oplus R_{t2}) \oplus W_2, {}^{*} H(R_{pt2} \oplus R_{t2}) \oplus W_{n2}, {}^{*} R_{pt2}$

M8：$T \lhd K, {}^{*} R_{tp2}, {}^{*} PID_2 \sim > P_2 \sim OTA, {}^{*} H(R_{pt2} \oplus R_{t2}) \oplus W_{n2}, {}^{*} ID_{TTP}$

M9：$T \lhd {}^{*} OTA, {}^{*} R_{p3}$

M10：$P_2 \lhd {}^{*} R_{t3}, {}^{*} H(TID \oplus R_{p3} \oplus R_{t3})$

M11：$TTP \lhd {}^{*} PID_3, {}^{*} H(R_{pt3} \oplus R_{t3}) \oplus S_{31}, {}^{*} H(R_{pt3} \oplus R_{t3}) \oplus S_{32}, {}^{*} H(R_{pt3} \oplus R_{t3}) \oplus S_{33}, {}^{*} H(R_{pt3} \oplus R_{t3}) \oplus W_3, {}^{*} H(R_{pt3} \oplus R_{t3}) \oplus W_{n3}, {}^{*} R_{pt3}$

M12：$T \lhd K, {}^{*} R_{tp3}, {}^{*} PID_3 \sim > P_3 \sim OTA, {}^{*} H(R_{pt3} \oplus R_{t3}) \oplus W_{n3}, {}^{*} ID_{TTP}$

其中，T 为标签，P_1, P_2, P_3 分别为标签拥有的 3 个所有者，TTP 为可信第三方。

3.1.2　协议初始化假设

A1：$P_1 \mid \equiv P1 \overset{S_{11}, S_{12}}{\longleftrightarrow} T$

A2：$P_1 \mid \equiv \sharp R_{p1}$

A3：$P_1 \ni S_{11}, S_{12}$

A4：$P_2 \mid \equiv P2 \overset{S_{21}}{\longleftrightarrow} T$

A5：$P_2 \mid \equiv \sharp R_{p2}$

A6：$P_2 \ni S_{21}$

A7：$P_3 \mid \equiv P_3 \overset{S_{31}, S_{32}, S_{33}}{\longleftrightarrow} T$

A8：$P_3 \mid \equiv \sharp R_{p3}$

A9：$P_3 \ni S_{31}, S_{32}, S_{33}$

A10：$\mathrm{T} \mid \equiv T \overset{K}{\longleftrightarrow} TTP$

A11：$T \mid \equiv \sharp R_{t1}, \sharp R_{t2}, \sharp R_{t3}$

A12：$T \ni K$

A13：$T \mid \equiv TTP \mid \Rightarrow TTP \mid \equiv *$

A14：$\mathrm{T} \mid \equiv \mathrm{TTP} \mid \Rightarrow \mathrm{P}_1 \sim OTA$

A15：$\mathrm{T} \mid \equiv \mathrm{TTP} \mid \Rightarrow P_2 \sim \mathrm{OTA}$

A16：$T \mid \equiv TTP \mid \Rightarrow \mathrm{P}_3 \sim OTA$

3.1.3　协议安全性分析

G1：$P_1 \mid \equiv T \ni S_{11}, S_{12}$（由 M2，A1，A2，A3，I3，I6 可得）

G2：$P_2 \mid \equiv T \ni S_{21}$（由 M6，A4，A5，A6，I3，I6 可得）

G3：$P_3 \mid \equiv T \ni S_{31}, S_{32}, S_{33}$（由 M10，A7，A8，A9，I3，I6 可得）

G4：$T \mid \equiv P_1 \ni S_{11}, S_{12}$（由 M1，A10，A11，A12，I3，I6 可得）

G5：$T \mid \equiv P_2 \ni S_{21}$（由 M5，A10，A11，A12，I3，I6 可得）

G6：$T \mid \equiv P_3 \ni S_{31}, S_{32}, S_{33}$（由 M9，A10，A11，A12，I3，I6 可得）

G7：$T \mid \equiv TTP \ni K$（由 M4，A10，A11，A12，I3，I6 可得）

G8：$T \mid \equiv P_1 \sim \mathrm{OTA}$（由 M4，A10，A11，A12，I3，A13，J2，A14，J1 可得）

类似地，可以得到 G9，G10。

G9：$T \mid \equiv P_2 \sim \mathrm{OTA}$

G10：$T \mid \equiv P_3 \sim \mathrm{OTA}$

G11：$T \ni S_{\text{new}}$（由 M8，A12，P6 可得）

从分析过程可以发现，该协议能提供所有者与标签之间的双向认证，当有攻击者假冒所有者向标签发送消息时，标签需先验证发送者的身份，由于所有者的身份标识唯一，攻击者不可能假冒合法的所有者，因此攻击者的攻击无效，该协议可以抵抗假冒攻击。在此基础上，当所有者的权重值产生变化时，该协议能够立即地更新标签密钥值，以确保权重变化前的所有者完全不再对标签具有控制所有权，即具备了原所有者无关性；权重变化后，所有者也不知道标签原来的密钥，不能获得标签之前的信息，保护标签信息的前向安全和后向安全。此外，协议中并未发送标签的身份信息或其他机密信息，可以避免受到跟踪攻击。

协议中采用随机数保证了协议执行的新鲜性，能够抵抗重放攻击。由于在 TTP(可信第三方)的参与下进行双向认证过程，不合法攻击者不能通过冒充中间人获得通信信息的方式来完成攻击，因此协议能够抵抗中间人攻击。

由于该协议在更新密钥之前，需先恢复出权重值变化前的原密钥 S，因此在遭受去同步化攻击时，可以通过原密钥值重新同步，以抵抗去同步化攻击。表 1 列出了本文协议与现有部分研究成果的对比结果，由表 1 以发现本文所提出的协议具有较好的安全性。

表 1 所有权转换协议的安全性对比

攻击类型	文献[4]	文献[5]	文献[7]a	文献[7]b	文献[9]	文献[12]	本文协议
抗去同步化攻击	√	×	√	√	√	√	√
抗重放攻击	√	√	√	√	√	√	√
抗假冒攻击	√	×	×	×	×	√	√
抗中间人攻击	√	√	√	√	√	×	√
不可跟踪性	×	√	√	√	√	×	√
前向安全	√	√	√	√	√	×	√
后向安全	√	√	√	√	√	√	√
原所有者无关性	×	×	√	×	×	√	√

注:a 表示含 TTP,b 表示不含 TTP,√ 表示满足安全性,×表示不满足安全性

3.2 仿真实验

实验在 CPU 为 3.60GHz 并且存储器为 4GB 的 Linux 系统环境中实现了该协议和部分现有的其他协议,主要获取了标签在执行协议时所消耗的时间等数据,并进行了对比。结果如图 3 所示,横轴代表各个协议,纵轴代表各个协议标签的计算时间。从图中可以看出,与现有的其他协议相比,本文所提出的所有权转换协议中标签的计算耗时较短,并且计算量在可接受的范围内,适用于低成本的标签。

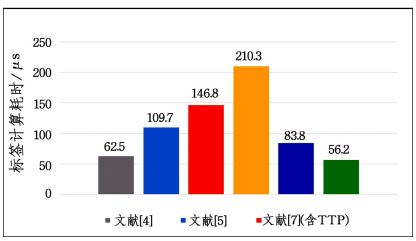

图 3 标签计算耗时对比

结束语 本文依据带有不同权重的多个所有者之间的权重值发生改变时,所有者本身没有变化的情况,提出了一种带 TTP 的多所有者内部权重变化所有权转换协议。多个所有者在可信第三方的参与下通过恢复出密钥与标签进行双向认证,保证了所有者的合法性;标签更新密钥,然后根据新的权重值将新密钥分割成多份子密钥,再将其分发给各个所有者。采用 GNY 逻辑对协议的安全性进行分析,结果表明该协议不仅能提供所有者与标签之间的双向认证,抵抗去同步化攻击、重放攻击、假冒攻击、跟踪攻击和中间人攻击,还能保护标签信息的前向安全和后向安全,并具备原所有者无关性。仿真实验结果表明,标签的计算耗时较短,适用于低成本标签。下一步的研究目标是在不降低安全性的前提下,研究如何进一步降低标签的计算量和所消耗的计算时间。

参 考 文 献

[1] 张帆,孙璇,马建峰,等. 供应链环境下通用可组合安全的 RFID 通信协议[J]. 计算机学报,2008,31(10):1754-1767.

[2] 邵婧,陈越,常振华. RFID 标签所有权转换模式及协议设计[J]. 计算机工程,2009,35(15):143-145.

[3] 邵婧,陈越,甄鸿鹄. 供应链环境下的 RFID 标签所有权转换方案[J]. 计算机工程与设计,2009,30(24):5618-5621.

[4] KULSENG L,YU Z,WEI Y,et al. Lightweight mutual authentication and ownership transfer for RFID systems[C]// Proc of the 29th Conf on Computer Communications—IEEE INFOCOM 2010. Piscataway NJ:IEEE,2010:1-5.

[5] ZHOU W,YOON E J,PIRAMUTHU S. Varying levels of RFID tag ownership in supply chains[C]// On the move to meaningful internet systems. Berlin:Springer,2011:228-235.

[6] 金永明,孙惠平,关志,等. RFID 标签所有权转移协议研究[J]. 计算机研究与发展,2011,48(8):1400-1405.

[7] KAPOOR G,PIRAMUTHU S. Single RFID tag ownership transfer protocols [J]. IEEE Transactions on Systems,Man,and Cybernetics, Part C: Applications and Reviews, 2012, 42(2):164-173.

[8] JIA H,WEN J. A novel RFID authentication protocol with ownership transfer[C]// International conference on automation and robotics. Berlin:Springer,2012:599-606.

[9] 贺蕾,甘勇,尹毅峰,等. 基于随机排列函数的 RFID 标签所有权转换协议[J]. 郑州大学学报(工学版),2013,34(6):24-27.

[10] DOSS R,ZHOU W L,YU S. Secure RFID tag ownership transfer based on quadratic residues[J]. IEEE Trans on information Fo-rensics and Security,2013,8(2):390-401.

[11] 沈金伟,凌捷. 一种改进的超轻量级 RFID 所有权转移协议[J]. 计算机科学,2014,41(12):125-128.

[12] 毛雅佼,孙达志. 一种新的 RFID 标签所有权转移协议[J]. 计算机工程,2015,41(3):147-150.

[13] 苑津莎,陈琳,张路路. 基于供应链环境的所有权转移方案设计[J]. 计算机工程与设计,2016,37(7):1770-1776,1981.

[14] 苏庆,李倩,张俊源,等. 基于共享密钥的超轻量 RFID 标签所有权转移协议[J/OL]. http://kns.cnki.net/kcms/detail/11.2127.TP.20170227.1544.042.html,[2017-02-27].

[15] 吴伟民,陈超雄,蓝炯江,等. 基于 Rabin 加密算法的 RFID 标签所有权转移协议[J]. 计算机应用研究,2017,34(5):1531-1535.

[16] 杨兴春,许春香,李朝荣. 基于 ECC 的支持标签所有权转移的 RFID 认证协议[J]. 计算机应用,2017,37(8):2275-2280.

[17] 李建华,张爱新,薛质,等. 网络安全协议的形式化分析与验证[M]. 北京:机械工业出版社,2010:27-33.

(上接第 357 页)

[2] KORNBLUM J D. Using JPEG quantization tables to identify imagery processed by software[J]. Digital Investigation,2008,5(Suppl):S21-S25.

[3] FARID H. Digital image authentication from thumbnails[C]// Media Forensics and Security II. DBLP,2009:75410.

[4] KEE E,JOHNSON M K,FARID H. Digital Image Authentication From JPEG Headers[J]. IEEE Transactions on Information Forensics & Security,2011,6(3):1066-1075.

[5] 卢启萌,施少培. Exif 信息在数码照片真实性鉴定中的应用[J]. 中国司法鉴定,2012(5):86-90.

[6] 邢赛鹏,平西建,詹杰勇. JPEG 图像数据格式简明分析[J]. 微计算机信息,2005(26):166-168.

[7] HAMILTON E. JPEG File Interchange Format[M]. Fer Publishing,2004.