RFID 标签所有权转换安全协议

陈志德，陈友勤，许力
（福建师范大学 数学与计算机科学学院，福建 福州 350007）

摘 要：针对 RFID 标签所有权转换过程的安全隐私及认证问题，提出一种“一交换两更新”的所有权转换协议。该协议通过先后的 2 次“更新”保证原所有者及新所有者的隐私安全，并且通过一次“交换”达到所有权转换双方不可抵赖及标签确诊的效果。在嵌有 RFID 标签的商品买卖中，该协议不仅保证了买卖双方的隐私安全，还通过不可抵赖的买卖关系保障了售后服务的实现。这对 RFID 现实应用推广具有重大的意义。

关键词：RFID；所有权转换；隐私安全；认证安全
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2010)9A-0202-07

RFID tag ownership transfer secure protocol

CHEN Zhi-de, CHEN You-qin, XU Li
(School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007,China)

Abstract: Aiming at security, privacy and authentication problems during RFID tag ownership transfer, a “one exchange and two update” ownership transfer protocol was proposed. Two “update” could protect both of the previous and new owners’ privacy while “one exchange” was for undeniable ownership transfer and tag verified in one ownership transfer. In the sales of goods with embedded RFID tag, the protocol could ensure the security and privacy for both of two participators and realize after-sales service for the undeniable ownership transfer , which was very valuable for the pervasive application of RFID in reality.

Key words: RFID; ownership transfer; privacy security; authentication security

1 引言

RFID(radio frequency identification)即射频识别技术是自动识别技术的一种，通过无线射频方式进行非接触双向数据通信，对目标加以识别并获取相关数据,具有无线即时读取、大容量和高速数据处理等能力以及高度自动化的特点，已经被广泛应用到零售行业、物流供应链管理、图书馆管理和交通等领域，并成为实现普适计算环境的有效技术之一[1]。但随着 RFID 应用的发展，RFID 的安全隐私问题也受到人们越来越多的关注。而 RFID 标签在其生命周期中进行的所有权转换，又使得这些问题变得更加棘手[2]。

在 RFID 标签生产出来后，制造商将其嵌入到商品中，再将商品出售给批发商，接着批发商又将商品卖给零售商，最后消费者购买了商品[3]。在现实生活中，消费者在使用一段时间后还可能将商品以二手的方式销售给其他消费者。而且在现实交易

收稿日期：2010-08-10
基金项目：福建省自然科学基金资助项目（2008J0014）；福建省教育厅项目（03WA693、JK2010012）；福建省高校服务海西建设重点基金资助项目－基于数学的信息化技术研究；国家自然科学基金资助项目（61072080）
Foundation Items: The Natural Science Foundation of Fujian Province (2008J0014); The Education Bureau of Fujian Province(03WA693,JK2010012); The Key Project of Services for Haixi Construction in Universities of Fujian Province－Information Technology Research Based on Mathematics; The National Natural Science Foundation of China(61072080)

中，若出现不满意的商品，还可以将其退换。在这个期间的每个环节都进行了商品的所有权转换。所谓的 RFID 标签所有权转换，就是有关于原所有者如何把标签上的信息转交给新所有者，而新所有者在转换之后又能实现对标签所有权的控制。

虽然，标签所有权转换定义描述就如此简单，但在实现过程中，如何保证原所有者的隐私信息，如何保证新所有者的隐私信息，如何验证该商品便是新所有者想购买的或是原所有者想销售的，如何保证原所有者不再拥有利用原先的秘密信息对该商品标签进行查询、管理等等操作的权利，又如何保证新所有者完全拥有对商品标签掌控的权利等等都是需要考虑的问题。为何要考虑这些问题呢？我们知道，商品的库存、流通和销售等信息一般都属于商业机密，而用户携带了哪些物品、处于什么位置，这些也都是用户的个人隐私[3]。此外，若不对商品验证，就有可能买到不是自己所需要的产品；消费者需要得到售后服务，就须要有“凭据”，即不可抵赖的交易关系，以此保证消费者能够享有售后服务的权利。

所以，在商品交易前，原所有者就要进行一次更新操作即更新 RFID 标签上的秘密信息，使得当新所有者获得商品后，无法知道原先 RFID 标签上的秘密信息，以此保证自己的安全隐私；在商品交易后，新所有者一方面要从原所有者那里得到商品上的 RFID 标签信息，另一方面又要更新 RFID 标签上的秘密信息，使得原所有者无法对 RFID 标签的信息进行查询、管理等等操作，来保障新所有者完全拥有商品的“所有权”及其“使用权”。此外，在现实商品交易过程中，消费者通过对商品标签信息的验证，保证自己将要购买的商品是自己所需要的商品；在商品交易后，消费者通过不可抵赖性的双方交易关系，还可以找到销售者进行享受服务。

2　相关工作

研究者对 RFID 认证问题的研究是比较多的，但是对 RFID 标签的所有权转换问题的研究还不太多。之前我们也做了篇关于 RFID 的认证协议，知道很多文章都是关于这个主题的，而仅有少数文章是关于 RFID 标签的所有权转换问题。下面就现有的几个方案进行简要分析。

Molnar 等人[4,5]所设计的基于密钥树的假名协议第一次用来解决标签的所有权转换问题和 RFID 标签授权的问题。该协议依赖一个可信中心（TC, trust center）操控整棵标签的密钥树，通过“软失效”或“增加标签计数”2 种方式实现标签的所有权转换。当新所有者想获得标签的所有权时，他首先要向可信中心请求授权并询问授权给原所有者还能读取标签的剩余次数。其次，新所有者要么通过“软失效”方式即重复访问标签超过原所有者所能读取标签的剩余次数，要么通过“增加标签计数”方式即直接增加标签的计数值，使得该值超过原所有者还能读取标签的剩余次数，从此原所有者就不能再读取标签，从而实现标签所有权的转换。但是，这 2 种方式本质上都只是限时授权，并没有实现完全的所有权转换，新所有者不能得到标签的完全控制权。而且该协议使用的是假名，因此，在实现所有权转换中，为了获得密钥和解码假名，标签还要进行大量的计算。

Fouladgar 和 Afifi[6~8]使用类似于 Molnar 等人的方案，采用集中式数据库（CDB,centralized database）来操控标签所有权转换过程。每个标签内部都设置了一个计数器，计数器中有个计数参数和当前设定的最大计数次数，每访问一次标签，计数参数就加 1。当计数参数值达到计数器当前设定的最大计数次数时，标签当前的密钥就失效了，CDB 就要重新更新标签的密钥。新所有者通过向 CDB 发出所有权转换请求，通过验证后，CDB 发布标签当前密钥给新所有者，实现授权。并通过更改计数器中设定的最大计数次数，授权给新所有者读取次数。以此实现了所有权转换。

Molnar 和 Fouladgar 等人所提出的所有权转换方案都基于中心设备即 TC 或 CDB，掌控着所有的秘密信息，所以隐私安全随时可能发生。Lim 等人[2]就提出了一个双向认证协议来实现完全的所有权转换。该方案要求原所有者将标签所有的秘密信息发布给新所有者，并允许新所有者秘密地更新标签秘密信息，保障了新所有者的隐私安全。然而该方案的实现是基于标签与阅读器之前的安全信道实现的。此外，Soppera 和 Burbridge[9]也采用了类似于 Molnar 等人的方案，不过，是采用了分布式的管理设备操控所有权转换过程的实现。采用分布式的管理设备，不仅增加额外的耗费，还引出新的可信安全等问题。

Osaka 等人[10]提出了可以高效实现标签所有权转换的方案。该方案首先允许原所有者更改标签秘

密信息，然后再实现所有权转换，最后又允许新所有者更新标签秘密信息，不仅能够保证新所有者的隐私安全，而且能够解决原所有者的隐私问题。但该方案不能抗 Dos 攻击，且用于更新密钥的值也不能防篡改，此外，还能出现标签跟踪问题，一旦标签被入侵敌手就有可能从之前的交互信息中得到原所有者的秘密信息，不具有前向安全。

Shao Jing 等人[3]提出了一种“先授权后更新”的所有权转换模式。该方案分为授权阶段和所有权转换阶段。授权阶段又分为授权请求、密钥协商和信息传输这 3 个阶段，实现标签全部的相关信息秘密传送给新所有者，从而实现完全授权。所有权转换阶段即实现了标签秘密信息的更新，保护新所有者的隐私安全。但该方案并没有保护原所有者的隐私安全。此外，Song 等人[11]提出了可以同时保护新所有者与原所有者的隐私的标签所有权转换方案，并且该方案具有授权恢复的功能。这使现实中售后服务等，得到更完美的实现。

3 方案描述

3.1 主要思想

通过相关工作的描述部分，知道一个完全的所有权转换方案，不仅要考虑所有权的完全转换，新所有者拥有对标签的完全控制权，此外，也要考虑所有权转换过程中新所有的隐私安全和原所有者的隐私安全。而且在现实的应用当中，还要保证交易的商品确实是新旧所有者所要进行交易的。所以，提出了一种“一交换两更新”的所有权转换模式，并为模式的实现设计了 3 个步骤的实现协议。

步骤 1 信息传输与交换。

实现原所有者与标签共享的秘密密钥传输给新所有者，并且实现原所有者与新所有者的签名及其相应的对标签唯一 *ID* 和标签信息 *Info*(*T*)（比如生产日期，地点等）的散列链值的秘密交换。一是实现了新所有者拥有了访问标签的临时秘密密钥，为实现所有权的完全转换提供了条件。二是实现了新所有者对标签的验证，验证了是否是自己所需要交易的商品。三是实现了原所有者与新所有者之间交易关系的不可抵赖，而彼此之间的交易关系，彼此是要保护的，这符合现实的应用。为了保证信息的秘密交换，使用了公钥加密系统（PKC, public key cryptosystem）。原所有者与新所有者都分别拥有一对公私钥，其中，公钥是公开的，私钥只有自己知道。所有者签名是一个所有者对级联信息（标签唯一 *ID* 和标签信息 *Info*(*T*)）的散列链值的签名。 那么所有者与标签共享的秘密密钥是一个对标签唯一 *ID* 的散列值。实现过程当中，结合签名与验证签名的信息，验证信息的有效性。

步骤 2 密钥更新与所有权完全转换。

一是实现对原所有者标签密钥信息的更改，安全地保护自己的秘密信息；二是实现所有权的完全转换。在现实交易当中，商品的库存、流通和销售等信息一般都属于商业机密，所以要对原所有者隐私信息进行保护。出于安全考虑，要求传输的秘密信息是隐藏的，而且每一次传输，其传输的信息形式也要求是变化的，以防止攻击者的追踪。所以传输过程中，需要使用随机生成器生成随机数，将相对固定秘密信息隐藏和改变。最后，标签返回确认信息给当前所有者，验证密钥更改成功。这实际上是一个认证和更改秘密密钥的过程。

步骤 3 新所有者更新信息。

通过以上的步骤之后，新所有者拥有与标签共享的秘密密钥，原所有者都知道。为了保护新所有者自己的隐私安全，务必要再进行一轮标签上秘密密钥的更改，以及标签上相应信息的更改。如果没有相应的更改，新所有者仍拥有对标签的控制权，通过此步骤，可以实现新所有者的隐私安全。当然，此操作过程要在原所有者阅读器读取范围之外的安全环境里完成。

3.2 系统假定

RFID 系统由标签、阅读器、天线和后台数据库等组成[12]。标签(tag，即射频卡)是由耦合元件及芯片组成，含有内置天线，用于和射频天线间进行通信。阅读器（reader）是一个具有读取或写入标签信息功能的设备。天线（antenna）起到传递标签和阅读器间射频信号的作用。这里就将系统简化为标签和阅读器 2 部分。

1) 标签：标签本身条件有限制，比如，标签的成本，标签的计算资源和标签的存储空间。所以本系统中，标签拥有一个抗原象和抗强碰撞的散列函数，有一定的存储空间和基本的运算能力。这是符合实际的要求的。由于用于所有权交换的标签的商品一般价值比较高，因此标签的成本高一点也是符合实际的。此外，比较贵的标签一般有较精致的存储设备，就算标签的存储信息被攻击者知道，攻击

者也不具备使标签内存崩溃或伪造信息写回到标签来篡改标签信息的能力。

2) 阅读器：阅读器中拥有一个伪随机数发生器，拥有一个抗原象和抗强碰撞的散列函数，可以进行公钥密码的加解密，可以进行签名与验证签名，也有较大的存储空间和基本的运算能力。一般阅读器的能力都是比较强的，这也符合实际的要求。

3.3 系统初始化

由于商品最初都是在制造商那里制造出来的，因此最初信息的初始化是由产商完成的，接着从一个所有者到另一个所有者的手里。假设进行所有权转换的所有者即原所有者和新所有者在进行交易的时候都知道自己所要交易的标签的信息，包括标签唯一标识 ID 和标签的其他信息 $Info(T)$（比如生产日期，地点等），这符合实际的应用要求。若进行所有权转换的双方是 OWNER_i 和 OWNER_{i+1}，其中 OWNER_i 是原所有者，而 OWNER_{i+1} 是新所有者，那么他们手里的阅读器在所有权转换发生前存储的情况如下。

OWNER_i 阅读器上存储的信息：

1) $ID, Info(T)$：标签唯一标识 ID 和标签的其他信息 $Info(T)$；

2) V_i：标签唯一标识 ID 和标签信息 $Info(T)$ 的第 i 个散列链值 $V_i = H(V_{i-1})$，其中 $V_0 = H(ID, Info(T))$；

3) K_i：与标签共享的秘密密钥 K_i，该密钥为对称密钥；

4) PK_i, SK_i：OWNER_i 的公钥 PK_i 和私钥 SK_i；

5) σ_i：OWNER_i 用私钥 SK_i 对信息 V_i 进行签名得 σ_i，即 $\sigma_i = Sig_{SK_i}(V_i)$，简写为 $\sigma_i = Sig_i(V_i)$；

6) K_t：初值为空；

7) PK_i^*：存储了新所有者的公钥 PK_{i+1} 即 $PK_i^* = PK_{i+1}$；

8) V_i^*：初值为空；

9) σ_i^*：初值为空。

标签上存储的信息：

1) V_i：标签唯一标识 ID 和标签信息 $Info(T)$ 的第 i 个散列链值 $V_i = H(V_{i-1})$，其中 $V_0 = H(ID, Info(T))$；

2) K_i：和当前所有者 OWNER_i 共享的秘密密钥 K_i，该密钥为对称密钥。

OWNER_{i+1} 阅读器上存储的信息：

1) $ID, Info(T)$：OWNER_{i+1} 事先知道的想要转换的标签，存储它的唯一标识 ID 和其他信息 $Info(T)$，用来验证进行所有权转换的标签确实是自己想要的；

2) V_{i+1}：初值为空；

3) K_{i+1}：初值为空；

4) PK_{i+1}, SK_{i+1}：OWNER_{i+1} 的公钥 PK_{i+1} 和私钥 SK_{i+1}；

5) σ_{i+1}：初值为空；

6) K_t：初值为空；

7) PK_{i+1}^*：存储了原所有者的公钥 PK_i 即 $PK_{i+1}^* = PK_i$；

8) V_{i+1}^*：初值为空；

9) σ_{i+1}^*：初值为空。

3.4 标签所有权转换协议

该协议主要通过 3 个步骤来实现的，如上描述的依次是信息传输与交换，密钥更新与所有权完全转换，新所有者更新信息。以下协议中 $Enc_i(m)$ 代表用 OWNER_i 的公钥 PK_i 进行加密，$Dec_i(m)$ 代表用 OWNER_i 的私钥 SK_i 进行解密，$Sig_i(m)$ 代表用 OWNER_i 的私钥 SK_i 进行签名。

但在执行该协议之前，首先完成原所有者对新所有者的授权认证。授权认证原理如下：首先新所有者发出授权请求，然后原所有者利用新所有者的公钥加密一随机数，接着新所有者利用自己的私钥解密出此随机数并用原所有者的公钥加密此随机数，然后将加密消息发送回给原所有者；那么，原所有者就可以利用自己的私钥解密出随机数进行比较来实现授权的认证。

3.4.1 信息传输与交换

本文主要采用了公钥加密保证了能够安全地进行信息交换，采用签名方式验证了标签确实是新所有者想交易的，并保证了新所有者与原所有者之间交易的不可抵赖性，其实现过程如图 1 所示。

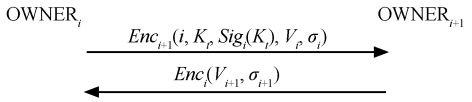

图 1　信息传输与交换

1) OWNER_i 利用伪随机产生器生成一个随机值赋值给 K_t，作为新所有者与标签临时会话的秘密

密钥。为了便于新所有者对标签进行验证，原所有者将自己的转换序号 i， 连同标签唯一标识 ID 和标签信息 $Info(T)$ 的第 i 个散列链值 V_i 及原所有者用其私钥 SK_i 对 V_i 进行签名的 σ_i 一并利用 OWNER_{i+1} 的公钥 PK_{i+1} 进行加密后传送给 OWNER_{i+1}，当然公钥 PK_{i+1} 所加密的信息还包含了 K_t 及原所有者用其私钥 SK_i 对 K_t 的签名 $Sig_i(K_t)$ 部分，即 OWNER_i 将 $Enc_{i+1}(i,K_t,Sig_i(K_t),V_i,\sigma_i)$ 传送给 OWNER_{i+1}。这样有且仅有知道 OWNER_{i+1} 的私钥 SK_{i+1} 才能解密得到其中的秘密信息。

2) OWNER_{i+1} 接收到 OWNER_i 发送来 $Enc_{i+1}(i,K_t,Sig_i(K_t),V_i,\sigma_i)$ 信息。首先利用自己的私钥 SK_{i+1} 对其解密，得到信息 $i,K_t,Sig_i(K_t),V_i,\sigma_i$；其次利用 OWNER_i 的公钥 PK_i 结合签名 σ_i 对 V_i 进行验证；再次利用 $V_0=H(ID,Info(T))$，进行 i 次的散列运算，来进一步验证 V_i，确保彼此进行所有权转换的标签是同一个；最后利用 OWNER_i 的公钥 PK_i 结合签名 $Sig_i(K_t)$ 对 K_t 进行验证。验证成功后，设置 $K_{i+1}=K_t$， $V_{i+1}=H(V_i)$， $\sigma_{i+1}=Sig_{i+1}(V_{i+1})$。至此之后，$\text{OWNER}_{i+1}$ 拥有了 OWNER_i 的 V_i 和 σ_i 信息，可以向可信第三方验证与 OWNER_i 的交易关系。

3) OWNER_{i+1} 利用 OWNER_i 的公钥 PK_i 加密 V_{i+1} 及 σ_{i+1}，并将加密结果发送给 OWNER_i，即 OWNER_{i+1} 将 $Enc_i(V_{i+1},\sigma_{i+1})$ 传送给 OWNER_i。同样利用公钥解密可以保证其过程是安全的。

4) OWNER_i 利用自己的私钥 SK_i 对 $Enc_i(V_{i+1},\sigma_{i+1})$ 解密，得到 V_{i+1} 和 σ_{i+1}。一方面 OWNER_i 可以自己计算出 $H(V_i)$ 和 V_{i+1} 进行比较；另外，可以利用 OWNER_{i+1} 的公钥 PK_{i+1} 结合签名 σ_{i+1} 对 V_{i+1} 再进行验证。至此之后， OWNER_i 拥有了 OWNER_{i+1} 的 V_{i+1} 和 σ_{i+1} 信息，可以向可信第三方验证与 OWNER_{i+1} 的交易关系。

3.4.2 密钥更新与所有权完全转换

顾名思义，本密钥更新与所有权完全转换就是为了实现标签中秘密密钥的更新，达到所有权完全转换。该实现过程阅读器主要利用到伪随机产生器和散列函数及基本的异或运算，而标签主要是利用到散列函数及基本的异或运算，其实现过程如图 2 所示。

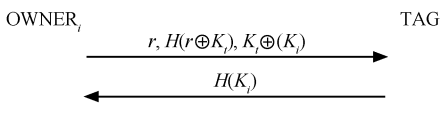

图 2　密钥更新与所有权完全转换

1) OWNER_i 利用伪随机产生器生成一个随机数 r，计算出 $H(r\oplus K_i)$，并利用上一步骤中发送给 OWNER_{i+1} 的 K_t 异或 $H(K_i)$，即得 $K_t\oplus H(K_i)$，将 $r,H(r\oplus K_i),K_t\oplus H(K_i)$ 同时发送给 TAG。此过程中，使用了伪随机数 r 以及 K_t（除 OWNER_{i+1} 知道的 K_t 外，认为是伪随机的），并利用了散列函数，抗原象及强抗碰撞性，保证了传输是安全的。即不仅可以保证传输信息的安全，还可以抵抗重放攻击以及追踪攻击。

2) TAG 首先运算 $r\oplus K_i$，其次再计算出其散列值，对 OWNER_i 发送过来的 $H(r\oplus K_i)$ 进行验证。验证成功后，再次计算 K_i 的散列值，即 $H(K_i)$，并使 $K_t\oplus H(K_i)$，得到与 OWNER_{i+1} 共享的会话秘密密钥 K_t。TAG 更新 K_i 和 V_i 分别为 K_t 和 $H(V_i)$，分别记为 K_{i+1} 和 V_{i+1}，并把计算出的 $H(K_t)$ 返回给 OWNER_i。

3) OWNER_i 将运算得到的 $H(K_t)$ 与传送过来的信息比较，验证 TAG 确实将秘密密钥更改为 K_t。

3.4.3 新所有者更新信息

新所有者为保护自身的隐私，进行了如图 3 所示的秘密信息的更新。

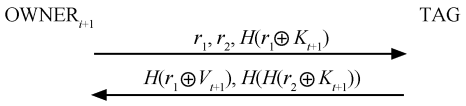

图 3　新所有者更新信息

1) OWNER_{i+1} 利用伪随机产生器生成 2 个随机数 r_1 和 r_2，计算出 $H(r_1\oplus K_{i+1})$，将 $r_1,r_2,H(r_1\oplus K_{i+1})$ 同时发送给 TAG。此过程中，使用了伪随机数 r_1 和 r_2，并利用了抗原象及强抗碰撞性的散列函数。由于操作过程是在 OWNER_i 阅读器读取范围之外，因此可以保证传输是安全的。

2) TAG 首先运算 $r_1\oplus K_{i+1}$，其次再计算出其散列值，对 OWNER_{i+1} 发送过来的 $H(r_1\oplus K_{i+1})$ 进行验证。验证成功后，再次计算 $H(r_2\oplus K_{i+1})$ 和 $H(r_1\oplus V_{i+1})$，并将 $H(r_2\oplus K_{i+1})$ 作为 K_{i+1} 的新值，达到更新秘密密钥的目的。最后，TAG 将 $H(r_2\oplus K_{i+1})$ 再次散列后连同 $H(r_1\oplus V_{i+1})$ 一起发送回给 OWNER_{i+1}。

3) OWNER_{i+1} 将运算得到的 $H(r_1\oplus V_{i+1})$ 与传送过来的信息比较，验证 TAG 确实是自己想要交易的。然后将运算 $H(H(r_2\oplus K_{i+1}))$ 所得信息与传送

过来的信息比较，验证 TAG 确实将秘密密钥更改为 $H(r_2 \oplus K_{i+1})$。最后 OWNER $_{i+1}$ 将 K_{i+1} 更新为 $H(r_2 \oplus K_{i+1})$。

4　系统架构分析

通过以上协议的描述过程，除了原来的 RFID 系统的基本架构，还需要一个可信的第三方。例如当新所有者所有权转换的标签出现问题的时候或需要售后服务的时候，如何找到原所有者呢？即出现此类纠纷时候，该怎么解决呢？本协议借助可信第三方进行仲裁。这个可信第三方只有在标签所有权转换出现纠纷的时候才出现。只要原所有者和新所有者分别向可信第三方出示彼此的信息，如上面的V_i、σ_i和V_{i+1}、σ_{i+1}信息，就可进行裁决。

另外，本系统并不基于中心设备，也就是说，嵌有标签的商品从产商出厂，产商后台数据库中存有商品所有的信息，当商品从产商传到零售商，零售商后台数据库中也存有商品所有的信息，最后商品从零售商到各个消费者手中，消费者的阅读器也可以作为一个类似的小型后台数据库存储信息。如果用户需要验证或获取一些简单的信息，无需到零售商或者是产商那里进行信息验证或获取相关的信息，即信息的存储和处理不具有集中化，它可以小化到各个用户的手里。所以，本系统具有很强的实用性。

5　安全性分析

5.1　原所有者隐私安全

通过协议中步骤 2，原所有者将标签中先前的秘密密钥信息更改，从而达到了保护自己隐私的目的。当发生所有权转换后，即使当新所有者的秘密密钥泄露，即标签上当前秘密密钥泄露，它也不能够得到标签之前的秘密密钥信息。因为前后实现过程中，都是用到了伪随机数及抗原象和强抗碰撞的散列函数，即使得到伪随机数及散列函数值，也很难求出原象信息。若可以的话，本身便和散列函数抗原象和强抗碰撞矛盾。

5.2　新所有者隐私安全和所有权转换的完全性

通过协议中步骤 3，新所有者将标签中秘密密钥信息进行更改。如果没有这一步，原所有者仍然拥有标签的秘密信息，仍然拥有控制权，这样，新所有者不但没有完全授权，而且还暴露隐私问题。但是，经过步骤 3 后，结合伪随机数和散列函数的性质，使得新所有者能够在原所有者阅读器读取范围之外的安全环境里面，秘密而又安全地更改信息，保护自己的隐私，并且拥有了标签的控制权。

5.3　标签确诊

通过协议中步骤 1 和步骤 3，可以实现对标签的确诊。该系统中可以存在不诚实的交易方，这也是符合实际情况的。通过步骤 1，保证了原所有者拥有新所有者想要交易的标签，即商品。另外，通过步骤 3，利用标签发送过来的V_{i+1}再次验证了标签，即商品，是新所有者想拥有的。而且步骤 3 实际上是进行了标签和阅读器之间的一个双向认证协议，此过程实现了彼此的验证。所以，这个过程当中，既可以防止非法的所有者从中夺取，也可以防止非法的标签（主要是不符合新所有者要求的标签）冒充。

5.4　交易关系的不可抵赖

交易关系的不可抵赖是本协议的特色，这也符合实际情况。通过步骤 1，新所有者与原所有者拥有了对方的散列链值及对应的签名，即V_i、σ_i和V_{i+1}、σ_{i+1}。只要一出示彼此的信息，便可进行验证。

5.5　被动攻击与主动攻击

标签所有权转换的成功与否，也要考虑转换的过程中的被动与主动攻击。被动攻击即窃听，可分为获取消息的内容和进行业务流分析 2 类。由于本标签所有权转换协议的实现过程中，都添加了一些随机变化的消息部分，因此本转换协议可以抵御被动攻击。然而对于中断、篡改或伪造等主动攻击者来说，由于在协议的 3 个步骤中，步骤 1 主要用到公钥加密，步骤 2 和 3 分别用到了散列函数，因此根据公钥加密的特点及散列函数的单向性和强抗碰撞性，再加上一些随机变化的参数，使得协议实现过程中，即使交互的消息被知道，也只能知道表面的加密信息或是散列值而无法得到被加密的秘密信息或是散列函数的原象，如果消息被篡改或伪造，只要交易双方通过验证，也可知道交易的信息被攻击，如果消息被中断，那交易就无法进行，一般这种情况不会发生，可以假设即使受到主动攻击，系统也不会因此中断。因此本协议可以抵御主动攻击。

6　结束语

本文提出了一个实现 RFID 标签所有权完全转换的有效方案。通过“一交换两更新”的 3 步骤实

现协议。通过“交换”和“两更新”达到了标签所有权完全转换的要求，保护了原新所有者的隐私，抵御了一些不法参与方的恶意行为，保障了交易方尤其是新所有者的权益。该研究既有理论意义，又符合实际需求。

参考文献：

[1] CHEN Y Q, CHEN Z D, XU L. Rfid system security using identity-based cryptography[A]. 3rd International Symposium on Intelligent Information Technology and Security Informatics(IITSI 2009)[C]. Jinggangshan, China, 2010.

[2] LIM C H, KWON T. Strong and robust rfid authentication enabling perfect ownership transfer[A]. 8th International Conference on Information and Communications Security (ICICS)[C]. Raleigh, NC, USA, 2006.

[3] SHAO J, CHEN Y, CHANG Z H. Design of rfid tag ownership transfer mode and protocols[J]. Computer Engineering, 2009,35(15): 143-145.

[4] MOLNA D, SOPPERA A, WAGNER D. A scalable, delegatable pseudonym protocol enabling ownership transfer of rfid tags [A]. 12th International Workshop on Selected Areas in Cryptography (SAC) [C]. Kingston, ON, Canada, 2005.

[5] MOLNA D, SOPPERA A, WAGNER D. A scalable, delegatable, pseudonym protocol enabling ownership transfer of rfid tags [A]. Workshop on RFID and Light-Weight Crypto[C]. Graz, Austria, 2005.

[6] FOULADGAR S, AFIFI H. A simple delegation scheme for rfid systems (SiDeS)[A]. IEEE RFID[C]. Grapevine, TX, USA, 2007.

[7] FOULADGAR S, AFIFI H. A simple privacy protecting scheme enabling delegation and ownership transfer for rfid tags[J]. Journal of Communications, 2007,2(6):6-13.

[8] FOULADGAR S, AFIFI H. An efficient delegation and transfer of ownership protocol for rfid tags[A]. 1st International EURASIP Workshop on RFID Technology[C]. Vienna, Austria, 2007.

[9] SOPPERA A, BURBRIDGE T. Secure by default: the RFID acceptor tag (RAT)[A]. 2nd Workshop on RFID Security(RFIDSec)[C]. Graz, Austria, 2006.

[10] OSAKA K, TAKAGI T, YAMAZAKI K, *et al*. An efficient and secure RFID security method with ownership transfer[A]. Computational Intelligence and Security(CIS)[C]. Guangzhou, China, 2006.

[11] SONG B. RFID tag ownership transfer[A]. 4th Workshop on RFID Security(RFIDSec)[C]. Budapest, Hungary, 2008.

[12] 张晴翔, 王伟驎. 无线视频辨识系统 RFID[M]. 中国台湾: 沧海书局, 2008.
ZHANG Q X, WANG W L. Wireless Radio Frequency Identification System RFID[M]. Taiwan, China: Canghai Publishing, 2008.

作者简介：

陈志德（1976-），男，福建泉州人，博士，福建师范大学副教授，主要研究方向为网络安全与密码学、分布式计算。

陈友勤（1986-），女，福建莆田人，福建师范大学硕士生，主要研究方向为网络安全与分布式计算。

许力（1970-），男，福建福州人，博士，福建师范大学教授，主要研究方向为无线网络与通信、信息安全和智能信息处理。