基于NTRU公钥密码系统的RFID通信安全协议的研究*

蔡庆玲[1,2]，詹宜巨[1]，余松森[1,3]，刘 洋[2]
（1. 中山大学工学院，广东 广州 510275；
2. 中山大学信息科学与技术学院，广东 广州 510275；
3. 华南师范大学计算机工程系，广东 佛山 528225）

摘 要：提出使用NTRU公钥密码系统建立RFID通信安全协议。通过使用构造随机化函数对NTRU公钥密码系统的明文进行动态、随机化映射，使由其映射后的明文具有了动态、随机分布的特性，实现了对明文信息的隐蔽，抵御了对明文信息特性的统计，致使攻击者对所得信息及信息来源无法区分和识别。由此设计的安全协议不仅满足了RFID通信安全协议要求的保密性、认证性等基本功能，而且能够有效地解决流量分析、跟踪攻击、隐私泄漏等RFID系统特殊的安全问题。同时不需要穷尽搜索，不需要密钥同步，密钥存储、密钥管理系统简单，并且具有良好的可扩展性。

关键词：RFID系统；安全协议；NTRU公钥密码系统；认证协议
中图分类号：TP393.04 **文献标识码**：A **文章编号**：0529-6579（2009）05-0006-06

RFID Communication Security Protocol Based on NTRU Public Key Cryptosystem

CAI Qingling[1,2], *ZHAN Yiju*[1], *YU Songseng*[1,3], *LIU Yang*[2]
(1. School of Engineering, Sun Yat-sen University, Guangzhou 510275, China;
2. School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510275, China;
3. Department of Computer Engineering, South China Normal University, Foshan 528225, China)

Abstract: RFID communication security protocol based on NTRU public key cryptography system is established. The plaintexts are randomly mapped by structuring the randomization function, and then the plaintexts mapped possess the properties of dynamic and random distribution. As a result, the plaintext characteristics can be hidden and can't be taken statistics. And that attackers are unable to distinguish from the messages and the message sources. RFID communication security protocol established by the method is not only able to meet the basic confidentiality and authentication requirements, but also effectively solve the special security issues of RFID communication such as traffic analysis、tracking attack、privacy leakage and so on; Moreover, the method has the following advantages: without key synchronization and exhaustive search of ID or key, with simple key storage and key management system, and a good scalability.

Key words: RFID system; security protocol; NTRU public key cryptosystem; authentication protocol

随着射频识别（Radio Frequency Identification，RFID）技术的广泛应用[1]，RFID系统的安全问题也日益突出。RFID系统存在的安全问题主要有保密性、流量分析、跟踪攻击、隐私泄漏等[2]。这

* 收稿日期：2008-10-14
基金项目：国家“985”工程二期资助项目（90013-3272240），广东省自然科学基金资助项目（06023131）
作者简介：蔡庆玲（1966年生），女，博士，讲师；E-mail：caiqingl@mail.sysu.edu.cn

些问题已严重阻碍了 RFID 技术的进一步发展，成为 RFID 技术发展急待解决的关键问题之一。因而，也已吸引了业界众多网络安全学者的关注和投入，并已提出了各种解决方案和策略[3]。目前提出的方案主要有：Hash 函数和对称密钥[4-5]。但前者存在着需要穷尽搜索的问题（在查找标签标识码时，需要在后端数据库中穷尽搜索）[4]；。后者不仅需要服务器为每一个标签分配一对密钥，而且也存在着穷尽搜索密钥问题，此外存储密钥还需要占据大量的空间，更因维持服务器和标签两端密钥同步的算法极其复杂而不易实现[5]，当系统规模巨大时此问题尤为突出。由此可见，上述两种方案均需要耗费系统的大量资源如执行时间和存储空间，因而难以满足仅具有有限资源、又需要高实时响应的 RFID 系统的要求。此外，这些方法大多存在着某种安全漏洞和隐患。至今，业界仍未能提出一个安全、高效、实用、低成本的适合 RFID 系统通信安全问题的解决方案。

本文提出使用公钥密码系统来解决上述问题，但典型的公钥密码系统如：RSA[6]、ElGamal[6] 及 Elliptic 曲线密码系统[6] 时间和空间的耗费都过于庞大无法在 RFID 系统的标签中使用，其它非典型的公钥密码系统也存在着某些问题，经过对现有公钥密码算法多项指标如安全性能，密钥生成、加密解密速度，密钥长度等的综合分析研究发现 NTRU 公钥密码系统具有高安全性、高速性、低耗性等特点[7-8]。尽管 NTRU 公钥密码系统的应用已有报道，但在 RFID 系统使用 NTRU 算法国内外还鲜见公开报道。因而本文提出使用 NTRU 公钥密码系统建立 RFID 通信安全协议。提出利用构造一个具有良好动态、随机变化的函数 $\mathrm{Random}^G(m, R_1, R_2)$，对 NTRU 公钥密码系统的明文进行随机优化使由其映射后的明文具有动态、随机分布的特性，实现对明文信息的隐蔽，抵御对明文信息特性的统计。使得即使是同一标签的标识码，其不同的认证过程所得信息也是动态、随机变化的，致使攻击者对所得信息及信息来源无法区分和识别。以此解决保密性、流量分析、跟踪攻击、隐私泄漏等 RFID 系统特殊的安全问题。

1　NTRU 公钥密码系统的简介

NTRU（Number Theory Research Unit）公钥密码系统是三位美国数学家 Hoffstein，Pipher 和 Silverma[7-8] 于 1996 年提出的一种新的公钥密码系统。其加密使用基于多项式代数和对数 p 和 q 归约模的混合系统，解密使用基于概率论的非混合系统。NTRU 的安全性基于多项式、不同模混合运算的相互作用及基于数论中从一个非常大的维数格中寻找极短向量的数学难题。由于该算法只使用了简单的模乘和模求逆运算，因而具有密钥产生容易，加密、解密迅速，密钥短及安全性能高，对带宽、处理器、存储器的性能要求低，占用系统资源少等特点，NTRU 已在密码学领域中引起了极大的关注，并得到了迅速发展与完善，在实际应用中取得了良好的效果。

一个 NTRU 公钥密码系统建立在三个整数参数 (N, p, q) 和四个整系数的最高次系数为 $N-1$ 的多项式集合 L_f，L_g，L_ω，L_m 之上。p，q 不必为素数，但要求 $gcd(p, q)=1$，并且 q 远大于 p。NTRU 建立于整系数多项式环 $R=Y[X]/(X^N-1)$ 上，一个元素 $A \in R$ 可以表示成一个多项式或一个向量（为了表达形式的统一，本文都使用向量表达形式）：

$$A=\sum_{i=0}^{N-1} A_i x^i = [A_0, A_1, \cdots, A_{N-1}] \tag{1}$$

用 $\otimes$ 来表示环 R 上的乘法，这个乘法可以表示为一个循环卷积：$A \otimes B = C$

$$C_k = \sum_{i=0}^{k} A_i B_{k-i} + \sum_{i=k+1}^{N-1} A_i B_{N+k-i} = \sum_{i+j=k(\mathrm{mod}N)} A_i B_j \tag{2}$$

其中多项式集合 L_f，L_g，L_ω，L_m 满足如下要求：$L_m = \{m \in R$：m 的系数位于区间 $[-(p-1)/2, (p-1)/2]\}$

定义 1　$L(d_1, d_2) = \{F \in R$：F 有 d_1 个系数为 1，d_2 个系数为 -1，其余系数为 $0\}$，再选择三个正整数 d_f，d_g，d_ω，设多项式集合 L_f，L_g，L_ω 分别满足：

$$L_f = L(d_f, d_f-1) \tag{3}$$

$$L_g = L(d_g, d_g) \tag{4}$$

$$L_\omega = L(d_\omega, d_\omega) \tag{5}$$

1.1　密钥生成

NTRU 在生成密钥时，首先随机地选择两个多项式 $f_{key} \in L_f$，$g \in L_g$。要求 f_{key} 关于模 p 和模 q 的逆 F_p，F_q 都存在，也即满足：$F_q \otimes f_{key} \equiv 1 \pmod q$，$F_p \otimes f_{key} \equiv 1 \pmod p$，其中 F_p 和 F_q 可以使用扩展的欧几里德算法来计算。然后计算公钥：

$$h_{key} \equiv F_q \otimes g \pmod q \tag{6}$$

其中，多项式 h_{key} 就是 NTRU 的公钥，而多项式 f_{key} 即为 NTRU 的私钥，同时将 F_p 与 f_{key} 一起秘密保存，共同用作私钥。

1.2 加密

在通信时，假设发送方S要发给接受方R一个消息 m，S首先从明文集 L_m 中选择要发送的消息 m。然后再从 L_ω 中随机选择一个多项式 ω，并用R的公钥 h_{key} 计算：

$$e \equiv p\omega \otimes h_{key} + m \pmod{q} \tag{7}$$

其中，e 就是S发给R的密文。

1.3 解密

当接收方R收到S发来的密文消息 e 后，R用自己的私钥（f_{key}，F_p）对其进行解密。R首先要计算：

$$a \equiv f_{key} \otimes e \pmod{q} \tag{8}$$

然后，在 $[-q/2, q/2]$ 内选择 a 的系数，再对 a 进行 $F_p \otimes a \pmod{p}$ 计算，即可重新得到S发来的明文 m。

2 建立基于NTRU公钥密码系统的RFID通信安全协议

2.1 安全协议的设计思想

RFID通信安全协议不仅要求具有实现信息的保密功能及阅读器和标签双方身份的认证功能，还要能够满足抵御流量分析、跟踪攻击、解决隐私泄漏等特殊的安全要求。本文提出建立基于NTRU公钥密码系统的RFID通信安全协议。使用NTRU公钥算法对RFID系统的通信信息进行加密，使用Challenge-Response机制对读写器和标签双方身份的合法性进行认证。为了解决流量分析、跟踪攻击、隐私泄漏等RFID系统特殊的安全问题，还必须对RFID标签的标识码等重要信息进行随机、动态的隐蔽处理。本文提出利用构造随机化函数 $\mathrm{Random}^G(m, R_1, R_2)$ 对标签的标识码进行随机化映射。通过构造一个具有良好动态、随机变化的函数 $\mathrm{Random}^G(m, R_1, R_2)$，对NTRU公钥密码系统的明文进行随机优化，使由其映射后的明文具有动态、随机分布的特性，实现对明文信息的隐蔽，抵御对明文信息特性的统计。并且由于随机参数的引入也确保了消息（标签的标识码）的新鲜性和主体的活现性。

使用公钥加密方案整个系统只需要配备一对公钥和私钥。其中密钥由服务器产生，并将私钥 f_{key} 连同 F_p 秘密地保存在后端数据库中，同时将公钥 h_{key} 分发给所有的合法标签。标签使用公钥 h_{key} 进行加密，服务器使用私钥 f_{key} 和 F_p 进行解密。使用公钥加密方案解决了需要在后端数据库穷尽搜索密钥或标签标识符问题，也解决了标签和后端数据库密钥同步更新的难题。因而密钥存储、密钥管理系统简单，并且具有良好的可扩展性，易于在RFID系统中实现。

2.2 随机化函数 $\mathrm{Random}^G(m, R_1, R_2)$ 的构造

（1）构造原理

本文根据NTRU公钥密码系统特点及RFID通信安全协议要求构造随机化函数。利用此函数先对NTRU公钥密码系统的明文 m 进行随机化映射，使映射后的明文动态、随机、均匀地分布在整个明文的取值空间 L_m。这样使得即使是同一个标签的标识码，其不同的认证过程所得信息也都是动态、随机变化的，致使攻击者对所得信息及信息来源（来自某一个标签）无法区分和识别也就无法实施流量分析、跟踪及隐私窥探等攻击。

$\mathrm{Random}^G(m, R_1, R_2)$ 的构造直接决定着密文最终的动态化、随机化分布的性能，也即攻击者对明文区分的难度，决定着RFID通信安全协议具有抵抗攻击的能力。受成本限制，RFID标签的资源（计算能力及存储空间）有限、又要求高实时响应，因而本文利用随机数 R_r，R_l 通过截联 $u \amalg v$、截取 $\oint\!\!\oint w$ 和异或⊕等运算来实现对随机化函数 $\mathrm{Random}^G(m, R_1, R_2)$ 的构造。

（2）基本组成

核心组件是一个随机化函数 $\mathrm{Random}^G(m, R_1, R_2)$，通过借助随机数 r、$G(r)$ 对明文 m 进行某种运算，实现对明文 m 信息的隐藏，以达到使明文 m 信息具有随机分布的特性。将随机化函数 $\mathrm{Random}^G(m, R_1, R_2)$ 引入公钥加密算法后其形式变为：$E^G(x) = f(\mathrm{Random}^G(m, R_1, R_2))$。$m$ 是被加密消息，R_1，R_2 是系统产生的随机数，f 是陷门置换函数，本系统为公式（7）NTRU加密算法：$e \equiv p\omega \otimes h_{key} + m \pmod{q}$。

（3）构造方法

由于NTRU公钥密码系统参数的选择具有严格的限制，因而如何将随机化参数引入公式（7）$e \equiv p\omega \otimes h_{key} + m \pmod{q}$，并且还能够确保NTRU系统的所有参数经过随机化映射后仍然在NTRU参数的取值空间，是随机化函数 $\mathrm{Random}^G(m, R_1, R_2)$ 构造的关键和难点。由公式（7）$e \equiv p\omega \otimes h_{key} + m \pmod{q}$ 分析可知：参数 p 和 q 的选择必须满足NTRU的建立条件，而 h_{key} 为NTRU生成的公钥，都已确定不可以随意地进行随机化处理。$\omega \in L_\omega$，由定义1的式（5）可知，其取值空间也有严格的限制。当NTRU的参数 $p = 2$ 时，则 $L_m =$

$\{m \in R$：m 的系数在 $[-1, 1]$ 区间$\}$，其系数选择没有特别限制只需是在 $[-1, 1]$ 区间内，而一般的二进制数都在区间。RFID 标签的标识码可以表示为 64bits 二进制数[1]，以标签的标识码构成的明文空间即可满足 NTRU 明文 L_m 的要求。因而本方案选择对 NTRU 加密算法中的明文 m 进行构造随机化函数，这样既可以实现将随机参数引入 NTRU 加密算法，又可以确保经映射后的明文仍然满足 $\text{Random}^G(m, R_1, R_2) \in L_m$。$\text{Random}^G(m, R_1, R_2)$ 的构造定义如下：

令 $x, y, z \in L_m$，其中 x, y, z 用向量形式（最高次系数为 $N-1$）表示如下：

$$x = [x_0, x_1, \cdots, x_{63}, x_{64}, x_{65}, \cdots, x_{N-1}]$$

$$y = [y_0, y_1, \cdots, y_{63}, y_{64}, y_{65}, \cdots, y_{N-1}]$$

$$z = [z_0, z_1, \cdots, z_{63}, z_{64}, z_{65}, \cdots, z_{N-1}]$$

定义 2 截联运算：

$$x \amalg y = [x_0, x_1, \cdots, x_{63}, y_{64}, y_{65}, \cdots, y_{N-1}] \quad (9)$$

定义 3 截取运算：

$$\oint z = [z_0, z_1, \cdots, z_{63}, 0, 0, \cdots, 0] \quad (10)$$

其中，截取 z 的 $z_0, z_1, \cdots, z_{63}$，其余 $N-(i-1)$ 位补 0。

定义 4 随机化函数：

$$\text{Random}^G(m, R_1, R_2) = m \amalg (R_1 \oplus R_2) \quad (11)$$

其中 $m, R_1, R_2 \in L_m$，$\oplus$为异或运算。

图 1 给出本文提出的使用随机化函数 $\text{Random}^G(m, R_1, R_2)$ 建立的基于 NTRU 公钥密码系统的 RFID 通信安全协议的设计原理，其中 ID_t 和 ID_i 为标签和后端数据库所存储的标签的标识码，$E^{\omega}_{hkey}()$ 和 $D^{Fp}_{fkey}()$ 分别表示 NTRU 公钥密码系统的加密算法和解密算法。

2.3　RFID 通信安全协议的实现

（1）初始条件

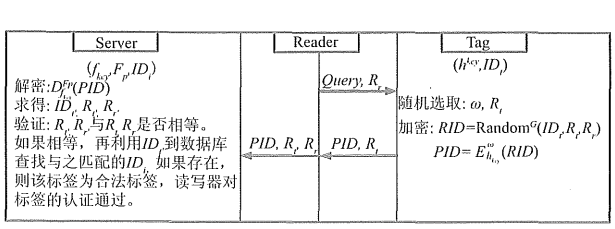

图 1　基于 NTRU 公钥密码系统的 RFID 通信安全协议的设计原理

Fig. 1　the Principle of RFID Communication Security Protocol Based on NTRU Public Key Cryptosystem

将上述设计思想及原理应用于本方案，具体实现如下：

RFID 系统初始时，由服务器使用 NTRU 公钥密码系统生成公钥 h_{key} 和私钥 (f_{key}, F_p)；并为每一个标签分配一个唯一的标识码（可由制造商完成）。服务器将标识码以及物品（贴有该标签的物品）的相关信息同时存储于标签和后端数据库，分别用 ID_t 和 ID_i 表示；将公钥 h_{key} 和私钥 (f_{key}, F_p) 也分别存储于标签和后端数据库。由于公钥 h_{key} 和私钥 (f_{key}, F_p) 是系统建立时由服务器产生的，并且服务器将其中的私钥 (f_{key}, F_p) 和 ID_i 秘密地保存，将公钥 h_{key} 分发给每一个标签；同时通过安全信道将标签的标识码 ID_t 存储到相应的标签。故私钥 (f_{key}, F_p) 和标识码 ID_i、ID_t 在本系统中都被认为是安全保密的。

令 $R_r, R_t, O \in L_m$，$\omega \in L_\omega$，其中 O 为零向量（$O = [0, \cdots, 0]$）。选择 $p=2$，则 $L_m = \{m \in R$：m 的系数在 $[-1, 1]$ 区间$\}$，由于标签的标识码可以用二进制数表示，因而可设 $ID_t \in L_m$。但由于标签的标识码为 64bits，因而其仅占用 ID_t 的 $[ID_0, ID_1, \cdots, ID_{63}]$，其余的 $[ID_{64}, ID_{65}, \cdots, ID_{N-1}]$ 初始化时赋值为 0。

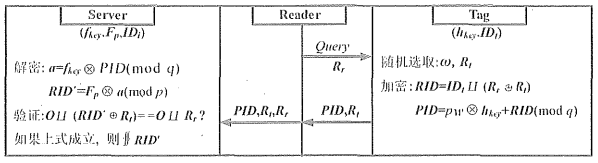

图 2　基于 NTRU 公钥密码系统的 RFID 通信安全协议

Fig. 2　RFID Communication Security Protocol Based on NTRU Public Key Cryptosystem

（2）认证过程

RFID 通信认证协议如图 2，认证步骤如下：

① Reader→Tag：读写器从 L_m 中选取一随机数 R_r，并向标签发送认证请求 $Query$，同时将 R_r 发送给标签。

② Tag→Reader→Server：标签接到读写器发来的认证请求（$Query$，R_r）后，首先也从 L_m 中选取一随机数 R_t 计算出 $RID = ID_t \amalg (R_r \oplus R_t)$，再从 L_ω 中选取一随机数 ω，利用公钥 h_{key} 和公式（7）对 RID 进行加密运算 $PID \equiv p\omega \otimes h_{key} + RID \pmod q$，然后将（$PID$，$R_t$）发送给读写器，读写器再将（$PID$，$R_t$，$R_r$）转发给服务器。

③ Server：服务器收到（PID，R_t，R_r）后，

首先利用私钥（f_{key}，F_p）和公式（8）对 PID 进行解码运算：$a \equiv f_{key} \otimes PID \pmod{q}$ 和 $RID' \equiv F_p \otimes a \pmod{p}$ 获得 RID'，因为 $RID' = ID_t' \amalg (R_r' \oplus R_t')$（用 RID'，ID_t'，R_r'，R_t'分别表示为 RID，ID_t，R_r，R_t 解码所得）。然后再验证 $O \amalg RID' = = O \amalg (R_r \oplus R_t)$ 是否成立，如果等式成立则认证通过。再利用公式（10）截取 $\oint RID'$，即可得到标签的标识码 ID_t。利用 ID_t 就可直接在后端数据库中读取该标识码 ID_t 对应的标签信息，如果后端数据库中查不到该标识码 ID_t，认证失败，则认为其为非法标签拒绝接受而停止操作。实现了读写器对标签的认证。

④ Server：如果服务器不是合法的，则该服务器将不具有私钥（f_{key}，F_p），也就无法对标签发送的（PID，R_t，R_r）进行解密，无法获得 ID_t，因而也无法得到标签的 ID_t 及相关信息，其身份的合法性也可以得到验证，实现了标签对读写器的认证，由此可以实现读写器和标签的双向认证。

分析：在本协议中，R_r 和 R_t 不仅是引入的随机化参数，而且也是认证参数。R_r 和 R_t 如何实现两种功能分析如下：由 $RID = ID_t \amalg (R_r \oplus R_t)$ 可知，本文利用公式（9）截联运算 $\amalg$ 将 RID 分为 ID_t 和（$R_r \oplus R_t$）两个独立部分作为明文填充，而不是直接使用 $RID = ID_t \oplus (R_r \oplus R_t)$。其目的是在认证过程中 R_r 和 R_t 必须能够相互认证。也即是：当（$R_r \oplus R_t$）与 R_r进行异或时，R_t 必须能够独立出来，才能利用解密所得到的、独立的 R_t'与接收到的 R_t进行验证，进而才能有效得到确认。如果使用 $ID_t \oplus (R_r \oplus R_t)$，那么有 $ID_t \oplus (R_r \oplus R_t) \oplus R_r = ID_t \oplus R_t$，$R_t$ 仍不能够独立出来，无法有效确认，也就无法实现对其的认证功能。$(R_r \oplus R_t) \oplus R_t$ 也同理。

3 RFID 通信安全协议安全性能分析

本系统的安全性能取决于 NTRU 公钥密码系统及 RFID 通信安全协议两部分。

3.1 NTRU 公钥密码系统安全性能分析

NTRU 的安全性可以划分为三个等级[7-8]，其安全性能如下：

（1）一般安全等级 $N = 107$，适合一些对安全性能要求不高的较低等级的 RFID 标签使用。

密钥安全级别为：2^{50}　信息安全级别为：$2^{26.5}$。

（2）高安全等级 $N = 167$，适合一些对安全性能要求较高的中高等级的 RFID 标签使用。

密钥安全级别为：$2^{82.9}$　信息安全级别为：$2^{77.5}$。

（3）最高安全等级：$N = 503$，适合一些对安全性能要求极高的特殊的 RFID 标签使用。

密钥安全级别为：2^{285}　信息安全级别为：2^{170}。

在本通信协议中 ID_t，R_r，$R_t \in L_m$，其中 ID_t 为 64bits 仅占用 ID_t 的［ID_0，ID_1，…，ID_{63}］位，其余的［ID_{64}，ID_{65}，…，ID_{N-1}］位用于传输 $R_r \oplus R_t$。

当 $N = 107$ 时，$R_r \oplus R_t$ 使用 43bits，两次选择随机数 R_r 或 R_t 相等的概率为 $1/2^{43}$；

当 $N = 167$ 时，$R_r \oplus R_t$ 使用 103bits，两次选择随机数 R_r 或 R_t 相等的概率为 $1/2^{103}$；

当 $N = 503$ 时，$R_r \oplus R_t$ 使用 439bits，两次选择随机数 R_r 或 R_t 相等的概率为 $1/2^{439}$。

3.2 RFID 通信安全协议安全性能分析

本文通过使用构造随机化函数 $\mathrm{Random}^G(m, R_1, R_2)$，对 NTRU 公钥密码系统的明文进行随机优化使由其映射后的明文具有动态、随机分布的特性，确保了 RFID 传输信息的保密，并有效地解决了流量分析、跟踪攻击、隐私泄漏的 RFID 系统特殊的安全问题。同时能够阻止伪装攻击、重放攻击。具体分析如下：

（1）抵抗伪装攻击

攻击者 A 伪装成合法标签对读写器进行攻击：

① 攻击者 A 首先伪装为合法读写器向某合法标签发送（$Query$，R_r）进行认证请求，攻击者 A 从标签处接收到应答（PID，R_t，R_r），其中 $PID \equiv p\omega \otimes h_{key} + RID \pmod{q}$，$RID = ID_t \amalg (R_r \oplus R_t)$。

② 在下一次认证时段中，当某合法读写器向标签发送认证请求（$Query$，R_r'）时，攻击者 A 再伪装成合法标签，利用在①中获得的（PID，R_t）应答该合法读写器，但由于此时读写器发送的认证请求为（$Query$，R_r'），则 $PID' \equiv p\omega \otimes h_{key} + RID' \pmod{q}$，$RID' = ID_t \amalg (R_r' \oplus R_t)$。因而要使读写器对标签的认证能够通过，$R_r$ 和 R_r'必须相同。但 R_r 和 R_r'是合法读写器两次产生的随机数，两者相同的概率最多只有 $1/2^{103}$（NTRU 为中等安全等级时），因而本协议能够有效抵抗伪装攻击。

（2）抵抗重放攻击

攻击者 A 伪装成合法读写器对某标签进行重放攻击，在本协议中没有意义。因为攻击者 A 伪

装成合法读写器向标签发送（*Query*，R_r）请求认证，标签应答为（*PID*，R_t）。由于读写器是非法的，没有办法得到私钥，因而也无法对 *PID* 进行解密，无法获得 ID_t，攻击无效。

（3）抵抗流量分析和跟踪攻击

攻击者 A 为了对某标签进行流量分析和跟踪必须不断地获得该标签的应答信息。其具体方法如下：

① 攻击者 A 可以伪装成合法读写器不断地向该标签发送（*Query*，R_r）认证请求或监听其它读写器与该标签的通信信息。

② 当标签接到连续的认证请求后，标签的一次应答信息为（*PID*，R_t），其中 $PID \equiv p\omega \otimes h_{key} + RID \pmod q$，$RID = ID_t \amalg (R_r \oplus R_t)$；而另一次应答信息为（*PID'*，$R_t'$），其中 $PID' \equiv p\omega \otimes h_{key} + RID' \pmod q$，$RID' = ID_t \amalg (R_r \oplus R_t')$。两次应答的信息分别为（*PID*，$R_t$）和（*PID'*，$R_t'$），由于 R_t 和 R_t'是由标签两次认证时段产生的随机数，因而即使同一标签两组应答的信息（*PID*，R_t）和（*PID'*，R_t'）两者相同的概率最多只有 $1/2^{103}$（NTRU 为中等安全等级时），无法判断该信息是否来源于同一标签（即同一个物品），也就无法进行流量分析和实现跟踪攻击，因而本协议能够有效地抵抗流量分析和跟踪攻击。

4 结　论

本文提出建立基于 NTRU 公钥密码系统的 RFID 通信安全协议。使用 Challenge-Response 机制实现对读写器和标签的双向认证；使用构造随机化函数 Random^G（m，R_1，R_2）对标签的标识码进行随机化映射，实现了对明文信息的隐蔽，抵御了对明文信息特性的统计，致使攻击者对所得信息及信息来源无法区分和识别，解决了流量分析、跟踪攻击、隐私泄漏等 RFID 系统特殊的安全问题。

此外，使用公钥加密方案整个系统只需要配备一对公钥和私钥，解决了需要在后端数据库穷尽搜索密钥或标签标识码问题，也解决了标签和后端数据库密钥同步更新的难题。因而密钥存储、密钥管理系统简单，并具有良好的可扩展性，易于在 RFID 系统中实现。满足了安全、高效、实用、低成本的 RFID 通信安全协议的要求。

对于本文提出的 RFID 通信安全协议的安全性验证，本人在另一篇名为《RFID 通信安全协议及其可证明安全性理论与方法的研究》的文章中进行了深入地研究，并给出了详细地分析和论证。

参考文献：

[1] EPCglobal tag data standards version 1.3[S], http://www.epcglobalinc.org.

[2] SARMA S E, WEIS S A, ENGELS D W. Radio-frequency identification: secure risks and challenges[J]. RSA Laboratories Cryptophytes, 2003, 6(1): 2-9.

[3] 周永彬，冯登国. RFID 安全协议的设计与分析[J]. 计算机学报，第 29 卷，第 4 期，2006：581-589.
ZHOU Y B, FENG D G. Design and analysis of cryptographic protocols for RFID[J]. Chinese Journal of Computers, 2006,29(4): 581-589.

[4] RHEE K, KWAK J, KIM S. Challenge-response based RFID authentication protocol for distributed database environment[J]. Lectures Notes in Computer Science 3450, Berlin: Springer-Verlag, 2005: 78-84.

[5] MARTIN F, SANDRA D, JOHANNES W S. Strong authentication for RFID systems using the AES algorithm[J]. International Associations for Cryptology Research 2004, CHES 2004, LNCS 3156, 2004: 357-370.

[6] MAO W B. Modern cryptography: theory and practice[M]. 北京：电子工业出版社，2004：165-190.

[7] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: A ring-based public key crypto-system[C]. In Proc of ANTS-Ⅲ, LNCS 1423, 1998: 267-288.

[8] The NTRU public key cryptosystem-a tutorial[J]. http://www.ntru.com.