第33卷 第13期 计 算 机 工 程 2007年7月
Vol.33 No.13 Computer Engineering July 2007
·安全技术· 文章编号：1000—3428(2007)13—0179—03 文献标识码：A 中图分类号：TP393.08

基于MYK-NTRUSign签名的用户认证方案

张利华[1,2]，朱成九[2]，郭 强[1]，范晓红[3]，吕善伟[1]
(1. 北京航空航天大学电子信息学院，北京 100083；2. 华东交通大学电气与电子学院，南昌 330013；
3. 北京电子科技学院电子学院，北京 10070)

摘 要：基于修复了延展性缺陷的NTRUSign算法，给出了一个使用智能卡的远程用户认证方案。该方案的安全性是基于单向Hash函数和在有限时间在大维数格计算最短向量的困难性。该方案包括4个阶段：注册阶段，登陆阶段，认证阶段和更改口令阶段。允许用户自主选择并更改口令，实现了双向认证；能够抵御中间人攻击，抗DoS攻击，具备前向安全性、强安全修复性和“黑名单”拒绝服务机制。是一个低开销、强安全性的方案。

关键词：身份认证；口令；智能卡；NTRUSign；延展性

MYK-NTRUSign Signature Based User Authentication Scheme

ZHANG Lihua[1,2], ZHU Chengjiu[2], GUO Qiang[1], FAN Xiaohong[3], LV Shanwei[1]
(1. School of Electronic and Information Engineering, Beijing University of Aeronautics and Astronautics, Beijing 100083;
2. School of Electric and Electronic Engineering, East China Jiaotong University, Nanchang 330013;
3. School of Electronic Engineering, Beijing Electronic Science and Technology Institute, Beijing 10070)

【Abstract】A new remote user authentication scheme using smart cards and a NTRUSign signature scheme against Malleability weak are proposed. The security of the scheme relies on Hash function and the fact that for most lattices, it is very difficult to find extremely short vectors. The scheme has four phases: registration phase, login phase, authentication phase and password change phase. Furthermore, the scheme has many merits: it let users freely choose and change password at their own will; it provides mutual authentication between two entities; it has more lower computational costs; it resists man-in-middle attack and denial of service attack. In addition, it has forward security and strong security reparability, as well as black list eviction mechanism. In a word, the proposed scheme is a better scheme with lower cost and strong security.

【Key words】 authentication; password; smart cards; NTRUSign; malleability

由于网络本身的开放型、网络设计总体构想的安全缺乏性、网络协议的安全不完备性、通信信道的共用性、网络用户的复杂性和网络攻击手段的多样性，用户的个人权益和隐私等受到很大的威胁。远程身份认证是指通过开放的信道如互联网识别和证实远程主体身份，从而授权合法用户访问系统资源的过程。口令认证由于实现简单，是使用比较广泛的远程用户认证方法。智能卡由于存储容量大，具有计算和访问控制功能、安全且便于携带，使用智能卡的口令认证方案是研究的热点。

本文研究了使用智能卡的口令认证方案，构造了一个基于修复了延展缺陷的NTRUSign数字签名算法（MYK-NTRUSign）、使用智能卡的远程身份认证方案。

1 相关研究工作

为改善使用口令表的远程身份认证方案的安全性和认证效率，很多学者进行了深入的研究，给出了不使用口令表的远程用户认证方案。根据使用的密码算法，此类方案主要分为2类：

(1)基于公钥密码体制如ELGamal算法的方案。这类方案以Hwang-Li方案[1]为基础，其安全性基于数学难题。文献[2、3]等针对Hwang-Li方案不能抵御假冒合法用户攻击的安全缺陷，从允许用户自主选择口令、改善用户使用友好性、提供双向认证、增强安全性等方面给出了改进方案。

(2)基于安全单向hash函数的方案。这类方案以以Sun方案[4]为基础，其安全性是基于单向Hash函数的逆向计算的困难性，和基于ElGamal算法的方案相比，计算和通信开销小，认证效率高。2005年，在前人研究的基础上，文献[5]给出了一个能够抵御并行会话攻击的改进方案，文献[6]给出了一个能够抵御重放攻击、内部攻击和弱安全性、能提供双向认证的方案。为避免使用时戳带来的抑制重放攻击的危险性，文献[7]给出了一个基于随机数、低开销的远程用户认证方案。

远程身份认证方案要满足以下基本特性[1,6,7]：计算、存储和传输带宽开销小，提供用户和远程主机双向认证，抗DoS(denial of service)攻击，抗中间人攻击，具备前向安全性、安全修复性和“黑名单”拒绝服务机制。使用智能卡的远程用户认证方案需要在智能卡有限资源的情况下提供足够的安全，需要利用能提供同等安全而资源开销小的密码算法来构建用户认证方案。

布朗大学的Jeffrey Hoffstein、Jill Pipher和Joseph H.Silvermanl提出的NTRU (number theory research unit)公钥密码体制[8]是目前公钥密码体制中最优秀、最快速的算法之

基金项目：国家自然科学基金资助项目(6027012)
作者简介：张利华(1972－)，男，副教授、博士研究生，主研方向：网络安全，移动Ad Hoc网络，无线传感器网络；朱成九，副教授；郭 强，硕士研究生；范晓红，硕士、讲师；吕善伟，教授、博士生导师
收稿日期：2006-08-21 **E-mail：**hbzlh@163.com

一。而且，NTRU具有更加良好的特性，和椭圆曲线密码算法ECC相比较，具有数学复杂性简单、容易理解、密钥生成和运行的速度快且容易的优点，需要更少的存储空间，更适合应用在资源严格受限的场合，如嵌入式设备、RFID标签等。这个算法依据的困难问题是Appr-cvp问题。人们先后研究并给出了基于NTRU的算法NSS、R-NSS和NTRUSign[9,10]，NSS和R-NSS算法已经被攻破。在NTRUSign算法中，签名者利用私钥产生明文的接近最近向量，这个向量属于NTRU格，而把这一向量作为明文的签名。敌手在不知道私钥的情况下，想通过其他方法在NTRU格中找到这一最近向量是很困难的[10]。文献[11]给出了一种NTRUSign算法的延展性攻击方法：一个敌手通过主动窃听，在获得一个消息的合法签名的情况下，能够伪造出此消息的多个合法签名；同时给出了一个具备修复延展性缺陷的MYK-NTRUSign数字签名算法。因此，使用MYK-NTRUSign数字签名算法构造使用智能卡的远程身份认证方案，将具有更小的计算开销、更高的认证效率和更强的安全性。

2 符号定义

2.1 环及其运算

设整数环 Z、整数 $N\geq 2$，用 R 表示多项式截断环时，R 可写成：$R=Z[X]/(X^N-1)$。一个多项式 $f(x)\in R$ 可以用一个向量 $\boldsymbol{F}$ 来表示：$\boldsymbol{F}=\sum_{i=0}^{N-1}f_i x^i=(f_0,...,f_{N-1})$

R 上定义了加运算和乘法运算。加运算：环上 2 个多项式 $F=(f_0,f_1,...,f_{N-1})$，$G=(g_0,g_1,...,g_{N-1})$ 的和为 $F+G=(f_0+g_0,f_1+g_1,...,f_{N-1}+g_{N-1})$；乘法运算：环上 2 个多项式 $F=(f_0,f_1,...,f_{N-1})$，$G=(g_0,g_1,...,g_{N-1})$ 的乘积为 $F\otimes G=C$，其中 C 的第 k 个系数 $c_k=\sum_{i=0}^{k}a_i b_{k-i}+\sum_{j=k+1}^{N-1}a_j b_{N+k-j}=\sum_{i+j\equiv k \bmod N}a_j b_j$，$0\leq i,j,k\leq N-1$。

多项式 $f(x)\in R$ 的中心化欧式范数定义为 $\|f(x)\|=\sum_{i=0}^{N-1}a_i^2-\frac{1}{N}(\sum_{i=0}^{N-1}a_i)^2$，且有 $\|F\otimes G\|=\|F\|\bullet\|G\|$。

对于任意正整数 q，令 R_q 代表模 q 的多项式截断环时，R_q 可以写成：$R_q=Z_q[X]/(X^N-1)$。可证明当 q 是素数时，R_q 具有可逆性。即对于 F，有 F^{-1} 满足 $F\otimes F^{-1}\equiv 1 \bmod q$。

2.2 方案参数

NTRUSign公开参数组 $D=(N,q,d_f,d_g,NormBound)$：$N$，维数，是一素数；$q$，模数；$d_f,d_s$ 密钥参数；$NormBound$，验证时使用的限。NTRUSign的推荐参数为 $(251,128,73,71,300)$，具有与 1 024 bit RSA算法同等的安全性[10]。

AS：远程主机；$h(\cdot)$：安全 Hash 函数；ID_i：用户 U_i 的身份标识；PW_i：用户 U_i 的口令；N：随机数；U_a：敌手；T_*：当前时戳；$\Rightarrow$：安全信道；$\rightarrow$ 一般信道。

3 MYK-NTRUSign 算法

MYK-NTRUSign算法是 2004 年由SungJun Min等人在分析NTRUSign数字签名算法的延展性缺陷的基础上，给出的一种修复延展性缺陷的NTRUSign的数字签名算法改进算法。其和NTRUSign一样，具有同样的计算特性[11]。因此，可以认为算法是安全的。算法包括密钥生成、签名和验证 3 个部分，其运算建立在环 $R=Z[X]/(X^N-1)$ 上。

3.1 密钥生成

(1)输入参数组 $D=(N,q,d_f,d_g,NormBound)$，随机选取 $f,g\in R$，满足 f,g 的系数分别只有 d_f,d_g 个 1，其余为 0；

(2)寻找较小的 $f,g\in R$，满足 $f\otimes G-F\otimes g=q$；

(3)计算公钥 $h\equiv f^{-1}\otimes g(\bmod q)$，输出公钥 h，私钥 (f,g,F,G)。

3.2 签名过程

(1)输入参数组 $D=(N,q,d_f,d_g,NormBound)$，私钥 (f,g,F,G)，消息 m，计算 $H(m)$，然后对 $H(m)$ 进行模 q 运算，获得多项式 (m_1,m_2)；

(2)计算 $G\otimes m_1-F\otimes m_2=A+q\otimes B$，$-g\otimes m_1+f\otimes m_2=a+q\otimes b$；

其中 $-q/2\leq A,a\leq q/2$；

(3)计算 $s'\equiv f\otimes B+F\otimes b(\bmod q)$；

(4)计算 $t'=s'\otimes h(\bmod q)$，如果 $\|s'-m_1\|^2+\|t'-m_2\|^2>Normbound^2$，令 $s=s'+\sum_{i=0}^{N-1}x^i(\bmod q)$，否则，则令 $s=s'-s'_{N-1}\sum_{i=0}^{N-1}x^i(\bmod q)$

(5)返回 (s)。

3.3 验证过程

(1)输入参数组 $D=(N,q,d_f,d_g,NormBound)$，公钥 h，签名 (s)，消息 m，计算 $H(m)$，然后对 $H(m)$ 进行模 q 运算，获得多项式 (m_1,m_2)；

(2)计算 $t=s\otimes h(\bmod q)$；若 $\|s-m_1\|^2+\|t-m_2\|^2>Normbound^2$，则返回拒绝该签名；

(3)如果 $s_{N-1}\neq 0$，令 $s'=s-\sum_{i=0}^{N-1}x^i(\bmod q)$，如 $\|s'-m_1\|^2+\|t'-m_2\|^2\leq Normbound^2$，则返回拒绝该签名。

(4)返回接收该签名。

4 基于 MYK-NTRUSign 算法的远程用户认证方案

4.1 注册阶段

AS 生成如下参数：$h(\cdot)$；系统密钥 x_s，随机数 N_1，NTRUSign 公开参数组 $D=(N,q,d_f,d_g,NormBound)$。$U_i$ 是请求 AS 注册的第 i 个用户，通过安全信道向 AS 提交其身份标识 ID_i 和 PW_i。

R1：AS 计算 $K_i=h(ID_i\oplus x_s)\oplus N_1$，$R_i=K_i\oplus PW_i$，$L_i=K_i\oplus x_s$，AS 将 ID_i，L_i 存入用户数据库中；

R2：$AS\Rightarrow U_i$：$(ID_i,h(\cdot),K_i,R_i)$ 及参数组 $D=(N,q,d_f,d_g,NormBound)$。智能卡按密钥生成算法生成公钥 h，私钥 (f,g,F,G)。并将 $(ID_i,h(\cdot),K_i,R_i)$ 及参数组 $D=(N,q,d_f,d_g,NormBound)$、私钥 (f,g,F,G) 存在用户的智能卡中，通过安全信道向 AS 公布公钥 h，存入用户数据库中。

4.2 登录阶段

L1：当 U_i 登录AS时，将智能卡插入读写器，输入 ID_i 和 PW_i^*，计算 $C_1=R_i\oplus PW_i^*$，如果 $C_1\neq K_i$，拒绝登录；

L2：智能卡计算 $M=h(C_1\oplus T_A)$，计算 $H(m)$，然后对 $H(m)$ 进行模 q 运算，获得多项式 (m_1,m_2)；

L3：计算 $G\otimes m_1-F\otimes m_2=A+q\otimes B$，$-g\otimes m_1+f\otimes m_2=a+q\otimes b$；

其中，$-q/2\leq A,a\leq q/2$；

L4：$s'\equiv f\otimes B+F\otimes b(\bmod q)$；

L5：计算 $t'=s'\otimes h(\bmod q)$，如果 $\|s'-m_1\|^2+\|t'-m_2\|^2$

$Normbound^2$，令 $s=s^{'}+\sum_{i=0}^{N-1}x^i(\mathrm{mod}\,q)$，否则，令 $s=s^{'}-s_{N-1}^{'}\sum_{i=0}^{N-1}x^i(\mathrm{mod}\,q)$；

L6：$U_i \rightarrow AS$ ：(ID_i,T_A,s)。

4.3 认证阶段

A1：AS 收到信息 (ID_i,T_A,s) 后，验证 ID_i,T_A 是否合法，如检验失败，则拒绝登录请求。

A2：计算 $L_i^{'}=L_i\oplus x_s.$，$M^{'}=h(L_i^{'}\oplus T_A)$，计算 $H(m^{'})$，然后对 $H(m^{'})$ 进行模 q 运算，获得多项式 $(m_1^{'},m_2^{'})$；

A3：计算 $t=s\otimes h(\mathrm{mod}\,q)$，若 $\|s-m_1^{'}\|^2+\|t-m_2^{'}\|^2>Normbound^2$，则拒绝登录请求；

如果 $s_{N-1}\neq 0$，令 $s^{'}=s-\sum_{i=0}^{N-1}x^i(\mathrm{mod}\,q)$，如 $\|s^{'}-m_1\|^2+\|t^{'}-m_2\|^2\leq Normbound^2$，则返回拒绝登录请求。否则，$U_i$ 的合法性得到认证；

A4：计算 $C_2=h(L_i^{'}\oplus T_S)$，$AS\rightarrow U_i$ ：(T_S,C_2)；

A5：U_i 收到 (T_S,C_2) 后，U_i 验证 T_S 的合法性，如否，拒绝登录请求；

A6：计算并判断 $C_2?=h(C_1\oplus T_s)$，如果成立，远程主机 AS 的合法性得到认证。

4.4 口令更改阶段

当 U_i 要将口令 PW_i 改为 PW_{new}，用户将卡插入合法终端的读写器，输入 PW_i，智能卡和终端之间完成相互认证后，用户选择进行口令更改，并根据提示输入新口令：

C1：智能卡计算 $K_i^{'}=R_i\oplus PW_i$，比较 $K_i^{'}?=K_i$，如否，拒绝更改口令；

C2：计算 $R_{new}=R_i\oplus PW_i\oplus PW_{new}$，用 R_{new} 取代 R_i，并存入卡中。

5 方案的安全性分析

方案的安全性是基于安全单向 Hash 函数和有效时间内不可能从大维数格中找到最短向量的困难问题，方案能够抵御中间人攻击，抗 DoS 攻击，具备前向安全性、强安全修复性和“黑名单”拒绝服务机制。

(1)抵御中间人攻击。敌手的攻击分为 5 种情况，敌手偶然得卡后，任意输入口令攻击；敌手伪造 (ID_i,T_A,s) 信息进行攻击；敌手截获 U_i 和 AS 的通信信息后，进行重放攻击；敌手截获 U_i 和 AS 的通信信息后，伪造合法用户进行攻击；敌手截获 U_i 和 AS 的通信信息后，伪造合法主机进行攻击。

假设敌手偶然获得智能卡后，在登录阶段的第 1 步，任意输入口令进行攻击。因为 $C_1\neq K_i$，敌手不能登录。敌手的攻击不能成功。

假设敌手欲伪造 (ID_i,T_A,s) 信息进行攻击。因为 C_1 未知，以及单向 Hash 函数逆向计算的困难性和有效时间内不可能从大维数格中找到最短向量的困难问题，不能伪造出合法的签名。

假设敌手 U_a 截获 U_i 和 AS 的通信信息 (ID_i,T_A,s)，重新开始一个登录过程，直接将 (ID_i,T_A,s) 通过不安全的信道发给 AS，T_A 的合法性不能得到验证，因此，敌手不能有效实施重放攻击。

假设敌手 U_a 截获 U_i 和 AS 的通信信息 (ID_i,T_A,s)，获得 ID_i，然后重新开始登录过程，由于 N_1 未知，U_a 无法得到正确的 K_i。即使 U_a 同时获得 PW_i，也不能计算出正确的 R_i，因而不能发起攻击，敌手无法有效实施假冒合法用户攻击。

假设系统密钥 x_s 不慎泄漏或被盗，在登录阶段的第 2 步，U_a 截获 U_i 发送给 AS 的 (ID_i,T_A,s)，N_2 未知，U_a 不能计算出 C_1；同时由于 PW_i 未知，U_a 也不能获得 R_i；而且 L_i 未知，敌手 U_a 不能计算出正确的 (T_S,C_2)，因而在认证阶段的第 5 步不能通过认证。即使 U_a 同时获得 PW_i、x_s，由于 N_2 未知，U_a 不能计算出 C_1；同样，由于 L_i 未知，敌手 U_a 不能计算出正确的 (T_S,C_2)，因而在认证阶段的第 5 步不能通过认证。因此敌手无法有效实施假冒合法远程主机攻击。

(2)抗DoS攻击。在系统密钥 x_s 泄漏的情况下，即使敌手 U_a 偶然获得合法用户的智能卡，和内部人员一起通过假冒合法读写器更改用户口令时[15]，因为 $K_i^{'}\neq K_i$，智能卡终止口令更改过程，敌手 U_a 不能更改用户的口令，因此敌手不能发起 DoS攻击。

(3)前向安全性。在系统密钥 x_s 泄漏的情况下，由于每个用户注册阶段 N_1 未知，敌手不能计算出合法的 k_i；又由于 PW_i 未知，敌手不能计算 $R_i=K_i\oplus PW_i$，因此 x_s 泄漏不会影响到合法用户的登录和使用，方案具备前向安全性。

(4)强安全修复性。在敌手 U_a 获得合法用户的智能卡和口令，假冒合法用户攻击远程主机系统时，远程主机更改对应的 N_1 值，计算新的 K_i、L_i 值，并将新的 L_i 值存入用户数据库，在认证阶段第 2 步，不能获得认证授权，从而拒绝特定的假冒用户登录，有效修复系统安全。

(5)“黑名单”拒绝服务机制。对于一些在使用过程中因为各种原因进入“黑名单”，限制登录远程主机系统的用户，远程主机通过更改对应的 N_1 值，计算新的 K_i、L_i 值，并将新的 L_i 值存入用户数据库，限制这些用户登录，有效保护系统安全。

6 结束语

基于 MYK-NTRUSign 的用户认证方案基于单向 Hash 函数和有限时间内在大维数格上计算最短向量的困难性，充分利用了 NTRU 优良的计算、存储、带宽开销小、安全性好的特性，满足了远程用户认证方案的基本特性，具有低开销、高安全性的特点，是一个有发展前途的方案，可以运用在电子商务、远程资源服务等需要用户身份认证的领域。

参考文献

1 Hwang M S, Li L H. A New Remote Authentication Scheme Using Smart Cards[J]. IEEE Transactions on Consumer Electronics, 2000, 46(1): 28-30.

2 Leung K C, Cheng L M, Fong A S, et al. Cryptanalysis of a Modified Remote User Authentication Scheme Using Smart Cards[J]. IEEE Transactions on Consumer Electronics, 2003, 49(4): 1 243-1 245.

3 Amit K, Awasthi, Sunder L. An Enhanced Remote User Authentication Scheme Using Smart Cards[J]. IEEE Transactions on Consumer Electronics, 2004, 50(2): 583-586.

4 Sun H M. An Efficient Remote Use Authentication Scheme Using Smart Cards[J]. IEEE Transactions on Consumer Electronics, 2000, 46(4): 958-961.

5 Yoon E J, Ryu E K, Yoo K Y. An Improvement of Hwang-Lee-Tang's Simple Remote User Authentication Scheme[J]. Computers & Security, 2005, 24(1): 50-56.

（下转第 184 页）