文章编号:1009-3087(2015)01-0049-05 DOI:10.15961/j.jsuese.2015.01.007

一种基于NTRU新型签名方案的设计

张卷美[1],曹 杰[1,2*],刘年义[3],杨亚涛[1],李子臣[1,2]
(1.北京电子科技学院 基础教学部,北京 100070;2.西安电子科技大学 通信工程学院,陕西 西安 710071;
3.河南省焦作师范高等专科学校,河南 焦作 454150)

摘 要:NSS和NTRUSign是2种典型的基于NTRU格数字签名方案。为了解决安全性问题及提高算法速度,提出一种基于NTRU的新型数字签名方案,分析了本方案的安全性难题、格基规约攻击以及副本分析攻击,对比了NTRUSign、胡予濮提出的改进方案NSS_Hu和本方案3种算法的性能参数,表明本方案在不降低安全性的同时,整体签名验证在复杂度理论程度上速度提升1/7。

关键词:格;NTRU;格基规约;数字签名方案
中图分类号:TP301.4 **文献标志码**:A

A New Design of Digtal Signature Scheme Based on NTRU

ZHANG Juanmei[1], *CAO Jie*[1,2*], *LIU Nianyi*[3], *YANG Yatao*[1], *LI Zichen*[1,2]
(1. Basic Education Dept., Beijing Electronic Sci. and Technol. Inst., Beijing 100070, China;
2. School of Communications Eng., Xidian Univ., Xi'an 710071, China; 3. Jiaozuo Teachers College, Jiaozuo 454150, China)

Abstract: NSS and NTRUSign are two typical digital signature schemes based on NTRU-lattice. For the purpose of solving security problems and speeding up the algorithm, a new scheme based on NTRU was proposed. Its security foundation, lattice reduction attack, and transcript analysis attack were shown. Performances of three schemes of the proposed one, NTRUSign, and its improvement scheme, NSS_Hu, were compared. The result showed that the proposed scheme could accelerate 1/7 without decreasing its security on the degree of complexity theory in total.

Key words: lattice; NTRU; lattice reduction; digital signature scheme

NTRU(number theory research unit)公钥密码密码体制是由Hoffstein等[1]在ANTS'98会议上提出的一种基于环$(\mathbb{Z}[x]/(X^N-1),+,*,)$上运算的密码体制。由于其具有密钥规模小、低数学复杂度和高运行速度的特性使得它适合于安全性要求较高、内存及计算能力受限的电子设备。但是,NTRU不像RSA等公钥密码体制具有自然实用的签名构造方案,因而与NTRU具有类似思想的数字方案成为研究热点。

目前,国际上NTRU数字签名的算法比较有代表性的是NSS[2](NTRU signature scheme)、NTRUSign等。2000年,Hoffstein、Pipher和Silverman利用NTRU格提出了NSS体制,其安全性与在某个格中寻找短的向量(shortest vector problem,SVP)有关,但是Silverman和Mironov[3]分别指出NSS体制由于私钥信息泄漏而导致的一类统计攻击。随后Hoffstein等[4]在Eurocrypt'01提出对NSS的改进体制R-NSS以防止统计攻击,但是Gentry等[5]利用编码方法的弱点,对NSS改进方案进行直接伪造签名攻击,同时Szydlo[5]使用同余条件由

收稿日期:2014-06-25
基金项目:国家自然科学基金资助项目(61370188);北京市支持中央高校共建项目——青年英才计划资助项目;中央高校基本科研业务费专项资金资助项目(2014CLJH09);北京电子科技学院信息安全重点实验室资助项目
作者简介:张卷美(1963—),女,副教授.研究方向:计算数学.E-mail:zhangjuanmei@beisti.edu.cn
*通信联系人 E-mail:caoj1991@163.com
网络出版时间:2014-9-12 9:55:45 **网络出版地址**:http://www.cnki.net/kcms/detail/51.1596.T.20140912.0955.001.html

签名脚本恢复密钥。同年,NTRU 原始设计者与 Nick、Howgrave-graham、William Whyte 合作对 NSS 做较大改动提出 NTRUSign 体制。2003 年,Hoffstein 等[6]在 CTRSA'03 上正式提出的 NTRUSign,并对以前的攻击进行了安全性分析,但是 NTRUSign 并没有用到他们所构造的完全格基,由此带来了安全隐患。

国内部分学者也对 NTRU 数字签名方案进行了设计和改进。2004 年,文献[7]提出一种基于 NTRU 算法的数字签名方案,其基本原理是签名者在 NTRU 格中用私钥寻找信息摘要的格点,并把格点作为信息摘要的数字签名,但是该方案并没有给出安全性的规约证明。2008 年,胡予濮[8]提出的新型的 NTRU 类数字签名方案 RSS_Hu,其具有与 NSS 相似的结构,并证明由公钥恢复出私钥的困难性是基于若干格上的最小向量问题(SVP),由公钥伪造签名的困难性等价于某个格上的最近向量问题(closest vector problem,CVP),但是该方案的签名值仍然会泄漏私钥的一些信息以至于存在安全隐患。同年一种生成签名速度方面优于 NTRUSign 的新的基于 NTRU 的数字签名方案被提出,但是 2010 年一种伪造签名的攻击方法,证明该方案是不安全的。2009 年,一种基于循环格的 NTRU 数字签名方案被提出,并给出了具体的实例,但是仍然存在签名副本泄漏私钥信息。2010 年,文献[9]基于循环格提出一种 NTRU 类数字签名方案,其基本思想与前述方案的方案基本一致,只是在签名之前对消息摘要进行扰动操作,使得该方案抗 GCD(greatest common divisor)攻击,但是该方案仍然不是零知识的。2012 年,文献[10]提出一种强化 NTRU 的构造方案,并证明了该方案在标准模型下是选择密文攻击(chosen ciphertext attack,CCA)安全的。

在介绍了 NTRU 加密算法后,提出一种新型数字签名方案,依次对方案参数、密钥生成算法、签名验证算法进行了描述,并给出正确性验证,随后从该方案所基于的安全性难题、格基规约攻击和副本分析攻击 3 个方面进行了安全性分析,最后对 NTRUSign 及其改进算法 NSS_Hu 与该签名方案的 3 种算法进行了性能对比,得出在不降低 NTRUSign 安全性的同时,签名验证的整体速度提升 1/7。

1 NTRU 加密算法

NTRU是一种多项式环上的加密系统,其加解密算法基于环上多项式代数运算和模运算,解密的有效性依赖于某些元素的概率。NTRU 的安全性基于复杂性假设:

PFP(polynomial factorization problem):给定一多项式 $h(x) = f_q(x) * g(x) \bmod q$,其中,$\boldsymbol{f}$ 和 $\boldsymbol{g}$ 的系数相对于 q 来说是小的,对适当的参数设置,如果仅知道 $\boldsymbol{h}$,很难恢复出多项式 $\boldsymbol{f}$ 和 $\boldsymbol{g}$,或者是很难找到 2 个具有较小系数的多项式 $\boldsymbol{f}'$ 和 $\boldsymbol{g}'$,满足 $\boldsymbol{f}' * \boldsymbol{h} \equiv \boldsymbol{g}' (\bmod q)$。

1.1 NTRU 参数描述

NTRU 是一种基于多项式环 $R_q = \mathbb{Z}[x]/(X^N - 1)$ 上的加密系统,其中,N 为安全参数,q 为素数。元素 $f(x) = f_0 + f_1 x + \cdots + f_{N-1} x^{N-1} \in R_q$ 视为行向量 $\boldsymbol{f} = [f_0, f_1, \cdots, f_{N-1}]$,$(R_q, *)$ 定义为多项式乘法 $(\boldsymbol{f} * \boldsymbol{g})(x) = \sum_{k=0}^{N-1} \sum_{i+j \equiv k (\bmod N)} f_i \cdot g_j \cdot x^k$,其中,$k \in [0, N)$,$\boldsymbol{f}, \boldsymbol{g} \in R_q$。$L(d_1, d_2) = \{F \in \mathbb{Z}[x]/(X^N - 1) |$ 其中,F 的系数有 d_1 个 1,d_2 个 -1,其余为 0$\}$。p 和 q 为 2 个互素的素数,且 $p > q$,$d_f, d_g, d_r \in (0, N)$,经过一定的编码规则,可以定义明文空间为:

$$M = \{m(x) = a_0 + a_1 x + \cdots + a_{N-1} x^{N-1} \in \mathbb{Z}[x]/(X^N - 1) | -\frac{q}{2} < a_i < \frac{q}{2}, i = 0, \cdots, N-1\}。$$

1.2 NTRU 密钥生成

1)随机地从集合 $L_f(d_f, d_{f-1})$ 中选取一个多项式 $\boldsymbol{f}$,使得 $\boldsymbol{f}_p$ 和 $\boldsymbol{f}_q$ 存在且满足:$\boldsymbol{f}_p * \boldsymbol{f} \equiv 1 (\bmod p)$ 和 $\boldsymbol{f}_q * \boldsymbol{f} \equiv 1 (\bmod q)$,那么私钥 $SK = (\boldsymbol{f}, \boldsymbol{f}_p)$;

2)随机地从集合 $L_g(d_g, d_g)$ 中选取一个多项式 g,计算 $\boldsymbol{h} = p\boldsymbol{f}_q * g (\bmod q)$,$PK = (\boldsymbol{h})$。为了安全起见,$\boldsymbol{g}$ 、$\boldsymbol{f}_q$ 也保密。

1.3 NTRU 加密算法

设明文消息 $m(x) \in M$,随机地从集合 $L_r(d_r, d_r)$ 中选择一个小系数多项式 $r(x)$,通常用于扰动密文信息。加密密文为:$\boldsymbol{e} \equiv \boldsymbol{r} * \boldsymbol{h} + \boldsymbol{m} (\bmod q)$。

1.4 NTRU 解密算法

1)利用私钥 $\boldsymbol{f}$,计算:$\boldsymbol{a} \equiv \boldsymbol{f} * \boldsymbol{e} (\bmod q)$;

2)将多项式进行 mod q 处理,并调整于$(-\frac{q}{2}, \frac{q}{2})$区间之类。

3)利用私钥 $\boldsymbol{f}_p$,计算:$\boldsymbol{d} \equiv \boldsymbol{a} * \boldsymbol{f}_p (\bmod p)$,所得的结果 $\boldsymbol{d}$ 即为解密的明文。

2　新数字签名方案

2.1　参数描述

N 为大素数,p 和 q 为不同的素数且 $p \gg q$,一般的,取 $q = 3$。记 $R = \mathbb{Z}[x]/(X^N - 1)$,那么:

明文空间:

$$M = \{m(x) = a_0 + a_1 x + \cdots + a_{N-1}x^{N-1} \in \mathbb{Z}[x]/(X^N - 1) \mid -\frac{q}{2} < a_i < \frac{q}{2}, i = 0, \cdots, N-1\}$$

,一般当取 $q = 3$,那么明文多项式 $m(x)$ 的系数为 $-1,0,1$,由文献[1]可知,私钥 $\boldsymbol{f}$ 在 L_f 上选取的主要原因是:

1)$\boldsymbol{f}$ 的系数较小;

2)$\boldsymbol{f}$ 以极大的概率模 p 和模 q 可逆。

私钥 $f(x) \in L_f = L(d_f, d_{f-1})$ 和 $g(x) \in L_g = L(d_g, d_g)$,随机多项式 $r(x) \in_R L_r = L(d_r, d_{r-1})$。

密钥空间 $K = \{f(x), g(x), h_1(x), h_2(x)\}$,其中,$h_1(x) = f_p(x) * g(x) \bmod p$,$h_2(x) = f_q(x) * g(x) \bmod q$,签名密钥为 $Ksig = (f(x), g(x))$,验证密钥 $Kver = (h_1(x), h_2(x))$。

签名空间 $S = \mathbb{Z}_p[x] \times \mathbb{Z}_q[x] \times \mathbb{Z}_q[x]$。

2.2　密钥生成

为了清楚说明密钥生成算法实现,将多项式“$*$”模 p 运算用矩阵表示。

设多项式 $f(x) = (a_0, a_1, \cdots, a_{N-1}) = \sum_{i=0}^{N-1} a_i \cdot x^i$,令 $f_p(x)$ 表示 $f(x)$ 模 p 的逆元,用矩阵表示如下:

$$\begin{bmatrix} a_0 & a_{n-1} & a_{n-2} & \cdots & a_1 \\ a_1 & a_0 & a_{n-1} & \cdots & a_2 \\ a_2 & a_1 & a_0 & \cdots & a_3 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{n-1} \end{bmatrix} \bmod p \equiv \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

由矩阵理论可知,$f_p(x)$ 存在的充要条件是:

$$\det(f(x)) \bmod p = \left\| \begin{bmatrix} a_0 & a_{n-1} & a_{n-2} & \cdots & a_1 \\ a_1 & a_0 & a_{n-1} & \cdots & a_2 \\ a_2 & a_1 & a_0 & \cdots & a_3 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \end{bmatrix} \right\| \bmod p \neq 0,$$

且此时逆元 $f_p(x)$ 存在且唯一。

下面给出系统参数生成算法:

1) 随机选取 $\alpha(x) \in_R R$;

2) 计算并判断 $\det(\alpha(x)) \bmod p$ 是否等于 0;

3) 若 $\det(\alpha(x)) \bmod p = 0$ 那么返回第 1) 步,否则继续:

4) 计算并验证 $\det(\alpha(x)) \bmod q$ 是否等于 0;

5) 若 $\det(\alpha(x)) \bmod q = 0$,则返回第 1) 步,否则令 $f(x) = \alpha(x)$。

6) 随机选取多项式 $g(x) \in_R R$,并计算:

$$h_1(x) = f_p(x) * g(x) \bmod p,$$

$$h_2(x) = f_q(x) * g(x) \bmod q。$$

7) 得到的签名密钥 $Ksig = (f(x), g(x))$,验证密钥 $Kver = (h_1(x), h_2(x))$。

2.3　签名算法

假若用户 A 欲向用户 B 发出明文信息 m 及签名,那么 A 首先需要对任意的明文消息 m,经过一定的编码规则编码成 $m(x) \in M$,并计算 $v(x) = m(x) * g(x) \bmod q$。随机选取 $r(x) \in_R R$,定义 $\mathrm{Hash}(\cdot): \{-1,0,1\}^N \mapsto \{\boldsymbol{v} \mid \boldsymbol{v} \in \{-1,0,1\}^k\}$,其中,$k$ 为 $\mathrm{Hash}(\cdot)$ 的输出长度。用户 A 利用签名密钥 $Ksig = (f(x), g(x))$ 计算:

$$s_1(x) = f(x) * (m(x) + r(x)) \bmod p,$$

$$s_2(x) = f(x) * (p - r(x)) \bmod q, s_3(x) = \mathrm{Hash}(v(x)),$$

那么签名结果为:$Sign(m(x)) = (s_1(x), s_2(x), s_3(x))$,那么用户 A 将 $(m(x), Sign(m(x)))$ 发送给用户 B。

2.4　验证算法

当用户 B 收到用户 A 发送过来的信息 $(m(x), Sign(m(x)))$,利用用户 A 的验证密钥 $Kver = (h_1(x), h_2(x))$ 计算:

$$u(x) = (h_2(x) * s_1(x) (\bmod q) + h_1(x) * s_2(x) (\bmod p)) \bmod q,$$

计算并验证 $\mathrm{Hash}(u(x))$ 是否等于 $s_3(x)$,若 $\mathrm{Hash}(u(x)) = s_3(x)$,则签名通过,否则拒绝签名。

2.5　签名正确性验证

$$\begin{aligned} u(x) &= (h_2(x) * s_1(x) (\bmod q) + h_1(x) * s_2(x) (\bmod p)) (\bmod q) = \\ &((f_q(x) * g(x)) (\bmod q) * (f(x) * (m(x) + r(x))) \\ &(\bmod p)) (\bmod q) + ((f_p(x) * g(x) (\bmod p) * (f(x) * \\ &(p - r(x))) (\bmod q))) (\bmod q) = \\ &((g(x) * (m(x) + r(x))) + (g(x) * (p - r(x))) \\ &(\bmod q)) (\bmod q) = (g(x) * m(x)) (\bmod q), \end{aligned}$$

$\mathrm{Hash}(u(x)) = \mathrm{Hash}(g(x) * m(x) (\bmod q)) = s_3(x)$,显然,当 $\mathrm{Hash}(u(x)) = s_3(x)$,则签名通过,否则拒绝签名。

3　新方案安全性分析

1) 安全性难题。该新型签名算法的安全性是基于安全单向 Hash 函数和基于格理论 CVP 问题。首先由公钥 $h_1(x)$、$h_2(x)$ 求解私钥 $f(x)$ 和 $g(x)$ 来说等价于在有效时间内从大维数格中找到最短向量的困

难问题(CVP),这是一个多项式NP问题,其避免了NTRUSign算法的安全性基础Appr-CVP难题。其次,新方案在签名结果$s_3(x)=\mathrm{Hash}(v(x))$中引入现在公开通用的单向Hash函数,如MD5、SHA-1,SHA-3等高安全性的杂凑算法,伪造签名的困难性等价于恢复对应的单向Hash函数所依赖的代数结构。因此,所设计的新型签名算法具有理论上公认的强安全性。

2)格基规约攻击。目前为止,攻击NTRU加密系统最好的方法是基于格基规约技术。同样的,对于该签名算法的私钥$Ksig=(h_1(x),h_2(x))$来说,其中,$h_i(x)=h_0^{(i)}+h_1^{(i)}x+\cdots+h_{N-1}^{(i)}x^{N-1}\in\mathbb{Z}[X]/(X^N-1)$,$i=1,2$。可以构造一个$2N$维CS格:

$\boldsymbol{L}_{\mathrm{CS}}=\{(F,G)\in\mathbb{Z}^{2N}\mid F\equiv h*G\bmod q,F,G\in R\}$,写成矩阵的形式如下:

$$\boldsymbol{L}_{\mathrm{CS}}=\begin{bmatrix}\alpha&0&\cdots&0&h_0^{(i)}&h_1^{(i)}&\cdots&h_{N-1}^{(i)}\\0&\alpha&&0&h_{N-1}^{(i)}&h_0^{(i)}&\cdots&h_{N-2}^{(i)}\\\vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\cdots&\vdots\\0&0&\cdots&\alpha&h_1^{(i)}&h_2^{(i)}&\cdots&h_0^{(i)}\\0&0&\cdots&0&q&0&\cdots&0\\0&0&\cdots&0&0&q&\cdots&0\\\vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&0&0&0&\cdots&q\end{bmatrix}=\begin{bmatrix}\boldsymbol{I}_N&\boldsymbol{M}(h)\\0&q\boldsymbol{I}_N\end{bmatrix}。$$

签名密钥$Ksig=(h_1(x),h_2(x))$,所以格$\boldsymbol{L}_{\mathrm{CS}}$显然包含$2N$维向量$(\boldsymbol{f},\boldsymbol{g})$,这个向量是格中最小向量。根据文献[11],可以求得一个$\tau(\boldsymbol{f},\boldsymbol{g})$的目标向量,其中,$\tau=\sqrt{2\pi\mathrm{e}}\|\boldsymbol{f}\|_2\cdot\|\boldsymbol{g}\|_2/Nq$。因此,恢复签名密钥$(\boldsymbol{f},\boldsymbol{g})$就是利用格基规约的方法求解格$L$的最小向量,即SVP。当$N$比较大的时候,这是一个多项式的NP问题。

目前为止,已有的格基规约算法包括著名的LLL算法[12]和BKZ算法[13],Gama等[14]提出提高格基规约速度的算法,May等[15]提出2种方法降低格基规约的复杂度的算法,但是都是针对N比较小的时候有效,目前仍然没有一种已知的既快速又有效的格基规约算法。

表1给出在$N=167,263,503$下利用已有的格基规约算法找到NTRU中最小向量的大概时间。

同时,NTRU167、NTRU263和NTRU503至少与RSA512、RSA1024和RSA2048的安全性相当,因此直接寻找签名私钥$(\boldsymbol{f},\boldsymbol{g})$在现有的计算能力情况下几乎是不可能的,因此,基于NTRU的新签名算法也是安全的。

表1 破解NTRU体制求解SVP的大概时间

Tab.1 Approximate time to solve SVP in breaking NTRU

安全等级	公开参数N	时间T(MIPS-year)
NTRU167	167	2.077×10^6
NTRU263	263	4.607×10^{14}
NTRU503	503	3.375×10^{35}

3)副本分析攻击。对于一般的NTRU格,10^4个签名副本就会泄漏私钥第2个矩的信息,10^8个签名副本会泄漏私钥的第4个矩的信息。当知道私钥的第4个矩的信息,结合Gentry和Szydlo的方法[5],就可以在多项式时间内恢复出私钥。提出的新型NTRU数字签名算法,在签名结果$s_1(x)$和$s_2(x)$的计算中引入随机向量$\boldsymbol{r}(x)$作为扰动因子,从而增加敌手副本分析攻击的难度,例如当$N=251$时,需要的签名副本的数量至少为10^{18}个,从而有效的增加了敌手副本分析攻击的难度[1]。

4 新方案算法性能分析

"$*$"模p运算是NTRU、NTRUSign算法及其改进算法的主要耗时运算,将直接影响加解密和签名运算的速度。下面将对NTRUSign、NSS_Hu[8]及本方案进行性能分析与比较(N为公开参数):

1)NTRUSign算法

签名密钥$Ksig=(\boldsymbol{f}_i,\boldsymbol{f}_i',\boldsymbol{h}_i)$,验证密钥$Kver=\boldsymbol{h}$,签名结果$Sign(\boldsymbol{m})=(\boldsymbol{m},\boldsymbol{r},\boldsymbol{s})$,签名算法的时间复杂度为$O(6N^2)$,验证算法的时间复杂度为$O(N^2)$。

2)NSS_Hu算法

签名密钥$Ksig=(\boldsymbol{f},\boldsymbol{g}_1,\boldsymbol{g}_2)$,验证密钥$Kver=(\boldsymbol{h}_1,\boldsymbol{h}_2,\boldsymbol{h}_3)$,签名结果$Sign(\boldsymbol{m})=(\boldsymbol{m},\boldsymbol{s}_1,\boldsymbol{s}_2,\boldsymbol{s}_3)$,签名算法的时间复杂度为$O(4N^2)$,验证算法的时间复杂度为$O(3N^2)$。

3)新签名算法

签名密钥$Ksig=(\boldsymbol{f},\boldsymbol{g})$,验证密钥$Kver=(\boldsymbol{h}_1,\boldsymbol{h}_2,\boldsymbol{H})$,签名结果$Sign(\boldsymbol{m})=(\boldsymbol{m},\boldsymbol{s}_1,\boldsymbol{s}_2)$,签名算法的时间复杂度为$O(4N^2)$,验证算法的时间复杂度为$O(2N^2)$。

以上3种算法的性能参数对比列于表2。由表2的性能参数比较可知,NTRUSign及胡予濮的改进体制NSS_Hu的签名验证过程需要的总步数为$7N^2$,而本研究构造的签名验证过程的总步数为$6N^2$,在计算复杂度理论程度上与经典的NTRUSign相比,签名速度约提升1/3,整体速度约提升1/7。

表 2　3 种算法的性能参数比较

Tab. 2　Performance comparison on three algorithms

签名算法	公钥长度/bit	私钥长度/bit	签名长度/bit	签名速度/步	验证速度/步
NTRUSign	$N \cdot \mathrm{lb}\, q$	$3N \cdot \mathrm{lb}\, q$	$3N \cdot \mathrm{lb}\, q$	$6N^2$	N^2
NSS_Hu[8]	$3N \cdot \mathrm{lb}\, q$	$3N \cdot \mathrm{lb}\, q$	$3N \cdot \mathrm{lb}\, q$	$4N^2$	$3N^2$
新方案	$2N \cdot \mathrm{lb}\, q$	$2N \cdot \mathrm{lb}\, q$	$3N \cdot \mathrm{lb}\, q$	$4N^2$	$2N^2$

5　结　论

在介绍了 NTRU 公钥密码体制后,提出一种新的数字签名方案,并对其安全性基于的难题进行分析,讨论了格基规约和副本分析 2 种攻击方法,并对 NTRUSign、胡予濮提出的 NSS_Hu 体制和新数字签名方案进行性能对比,得出在不降低签名方案安全性的同时,整体签名验证速度提高 1/7 的结论。

下一步工作是将新型数字签名方案应用到具体的协议设计中。

参考文献:

[1] Hoffstein J, Pipher J, Silverman J H. NTRU: A ring-based public key cryptosystem[C]//Proceedings of the 3rd International Symposium on Algorithmic Number Theory. London: Spinger-Verlag, 1998.

[2] Hoffstein J, Silverman J H. NSS: An NTRU lattice-based signature scheme[C]//Proceedings of Eurocrypt'01. Berlin: Springer-Verlag, 2000, 2045: 211 – 228.

[3] Mironov I. A note on cryptanalysis of the preliminary version of the NTRUSignature scheme[J]. IACR Cryptology ePrint Archive, 2001(5): 1 – 6.

[4] Hoffstein J, Pipher J, Silverman J H. NSS: An NT-RU lattice-based signature scheme[C]//Advanced in Cryp-tology—Eurocrypt' 01. Berlin: Springer-Verlag, 2001: 123 – 127.

[5] Gertry C, Szydlo M. Cryptanalysis of the revised NTRU signature scheme [C]//Advances in Cryptology—Eurocrypt'02. Berlin: Springer-Verlag, 2002: 299 – 320.

[6] Hoffstein J, Pipher J, Silverman J H, et al. NTRUSign: Digital signatures using the NTRU lattice[C]//Proceedings of CTRSA'03. San Francisico: LNCS, 2003, 2612: 122 – 140.

[7] Bu Shanyue, Wang Chonghui, Yan Yunyang. The signature scheme based on NTRU arithmetic[J]. Computer Engineerging and Applications, 2004, 40(1): 86 – 87. [步山岳,王崇辉,严云洋. 一种基于 NTRU 算法的数字签名方案[J]. 计算机工程与应用,2004,40(1):86 – 87.]

[8] Hu Yupu. A novel NTRU-class digital signature scheme [J]. Chinese Journal of Computers, 2008, 31(9): 1661 – 1665. [胡予濮. 一个新型 NTRU 类数字签名方案[J]. 计算机学报,2008,31(9):1661 – 1665.]

[9] Zhang Rufeng, Ma Chunbo, Ao Jun. A NTRU-class digital signature scheme based on cyclic lattice[J]. Ship Electronic Engineering, 2010, 30(12): 120 – 125. [张如丰,马春波,敖珺. 一个基于循环格的 NTRU 类数字签名方案[J]. 舰船电子工程,2010,30(12):120 – 125.

[10] Steinfeld R, Ling S, Pieprzyk J, et al. NTRUCCA: How to strengthen NTRU enryptto chosen-ciphertext seurity in the standard model[C]//Proceedings of the Advances in Public Key Cryptography 2012, PKC2012. Darmstadt: LNCS, 2012: 353 – 371.

[11] Coppersmith D, Shamir A. Lattice attacks on NTRU [C]//Proceedings of the Eurocrypt'97, LVCS-IACR. Santa Barbara: Springer-Verlag, 1997.

[12] Lenstra A K, Lenstra H W, Lovasz A K. Factoring polynomials with Rational coefficients[J]. Mathematische Annalen, 1982, 261: 515 – 534.

[13] Schnorr C P. Block reduced lattice bases and successive minima [J]. Combinatories, Probability and Computing, 1994(3): 503 – 522.

[14] Gama N, Howgrave-Graham N, Nguyen P Q. Symplectic lattice reduction and NTRU [C]//EUROCRYPT'06. St Petersburg: Springer-Verlag, 2006, 4004: 233 – 253.

[15] May A, Silverman J H. Dimension reduction methods for convolution modular lattices[C]//CaLC 2001. Rhode Island: Springer-Verlag, 2001, 2146: 110 – 125.

(编辑　杨　蓓)