

一个新型的 NTRU 类数字签名方案

胡予濮

(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

摘 要 NTRU 类数字签名方案的一个共同缺陷是签名值会泄露私钥的一些信息. 针对这个缺陷, 当前已经有若干有效攻击. 该文提出一个新型的 NTRU 类数字签名方案. 新方案具有与 R-NSS 相似的结构, 但有若干新颖的设计. 文中给出新方案的 3 个结果: (1) 由公钥恢复出私钥的困难性基于若干格上的最小向量问题(SVP); (2) 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(CVP); (3) 每个签名值仍然会泄露私钥的一些信息, 但无限制泄露的最终形式只是关于私钥的一组复杂的非线性方程.

关键词 NTRU; 数字签名; 格上的最小向量问题(SVP); 格上的最近向量问题(CVP)

中图法分类号 TP309

A Novel NTRU-Class Digital Signature Scheme

HU Yu-Pu

(The Ministry of Education Key Laboratory of Computer Networks & Information Security, Xidian University, Xi'an 710071)

Abstract NTRU-class digital signature schemes have a common weakness that signature value will leak information on the private key. According to this weakness, several effective attacks were proposed against these signature schemes. This paper presents a novel NTRU-class digital signature scheme. The new signature scheme has a similar structure to R-NSS, but with several novel designs. This paper has obtained following three results about the new scheme: (1) The hardness of recovering the private key from the public key is based on the hardness of the shortest vector problems(SVP) of several lattices; (2) The hardness of forging a signature is equivalent to the hardness of the closest vector problem(CVP) of some lattice; (3) Each signature will leak information on the private key, but the final shape of the unlimited leakage is just a group of complicated non-linear equations.

Keywords NTRU; digital signature; the Shortest Vector Problem of lattice(SVP); the Closest Vector Problem of lattice(CVP)

1 引 言

NTRU^[1]是已知最快速的公钥密码之一, 其安全基础是格上最小向量问题(SVP)^[2]. 不幸的是, 基于 NTRU 的数字签名方案并不成功. 所有这些签名方案都不是零知识的, 这就是说, 签名值会泄露私钥

的信息. 这种泄露本身并不意味着不安全, 但是针对这个缺陷已经有若干有效的攻击.

NTRU 类签名的两个典型代表是 R-NSS^[3] 和 NTRUSign^[4]. R-NSS 受到 Gentry 和 Szydlo^[5] 的致命攻击, 该攻击结合 GCD(最大公因子)方法和统计方法, 由大量的有效签名值恢复私钥. 该攻击能够成功的原因是: R-NSS 签名值是单个私钥的倍式.

NTRUSign 没有 R-NSS 的这个缺陷, NTRUSign 签名值不是单个私钥的倍式, 而是两个私钥的线性组合式, 但是组合式的系数却大致服从均匀分布. 正因为如此, NTRUSign 受到 Nguyen 和 Oded Regev^[6] 的致命攻击. 该攻击首先利用均匀分布的简单性和可过滤性, 由大量的有效签名值得到了关于私钥的一个二次函数, 然后利用多变量最优化计算程序恢复出私钥. 目前补救 NTRUSign 这种安全性缺陷的唯一方法是搅扰技术^[4]. 搅扰技术能否真正抵抗 Nguyen 和 Oded Regev 的攻击^[6] 还是一个公开问题, 但带有搅扰模块的 NTRUSign 极大地伤害了签名算法的效率. 此外, NTRUSign 的密钥生成过于复杂, 已经失去了简洁性.

本文提出一个新型的 NTRU 类数字签名方案. 提出新方案的基本意图是从签名值中攻击者既不能得到单个私钥的倍式, 也不能得到多个私钥的线性组合式, 而只能得到多个私钥的复杂函数, 因此使得新方案既能抵抗 Gentry 和 Szydlo 对 R-NSS 的致命攻击^[5], 也能抵抗 Nguyen 和 Oded Regev 对 NTRUSign 的致命攻击^[6]. 新方案具有与 R-NSS 相似的结构, 但有若干新颖的设计. 其中一个新设计是私钥与课文的非线性函数, 用来抵抗 Gentry 和 Szydlo^[5] 的攻击. 相比 R-NSS, 新方案保持了简洁的计算. 新方案仍然不是零知识的, 但是本文得到新方案的 3 个结果: (1) 由公钥恢复出私钥的困难性基于若干格上的最小向量问题 (SVP); (2) 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 (CVP); (3) 每个签名值仍然会泄露私钥的一些信息, 但无限制泄露的最终形式只是关于私钥的一组复杂的非线性方程. 具体地说, 那些已知的攻击对于新方案是无效的.

本文第 2 节描述新方案 and 它的新颖之处; 第 3 节说明由公钥恢复私钥的困难性依赖于若干格上的 SVP 的困难性; 第 4 节证明由公钥伪造签名的困难性等价于某个格上的 CVP 的困难性; 第 5 节说明签名值会泄露私钥的信息, 但大量的签名值对私钥的泄露只得到关于私钥的一组难以求解的非线性方程; 第 6 节是关于本文新方案的若干说明.

2 新方案和它的新颖之处

(N, q, p) 是 3 个公开参数, 其中 $N=251$, q 是 2 的幂. 本文中固定 $q=128$ 或 256 . 基础的数学结构是两个多项式环

$Q[X]/(X^N-1)$ 和 $Z[X]/(X^N-1)$,

其中 Q 是有理数环, Z 是整数环. 多项式 $u = u_0 + u_1X + u_2X^2 + \cdots + u_{N-1}X^{N-1} \in Q[X]/(X^N-1)$ 也可以理解为 N 维向量 $u = (u_0, u_1, u_2, \cdots, u_{N-1})$. 在此基础上得到两个商环 $Z_q[X]/(X^N-1)$ 和 $Z_p[X]/(X^N-1)$. 注意: 模运算 $(\text{mod } q)$ 的结果是在区间 $[-q/2+1, q/2]$ 内, 而不是在区间 $[0, q-1]$ 内; 模运算 $(\text{mod } p)$ 的结果是在 $\{0, 1, -1\}$ 范围内, 而不是在 $\{0, 1, 2\}$ 范围内. $L(a, b)$ 是环 $Z[X]/(X^N-1)$ 中那些多项式的全体, 具有 a 个系数为 1, b 个系数为 -1 , 其它系数为 0. 本文中总是记 EZ 为随机变量 Z 的数学期望.

密钥生成. 随机选取 3 个多项式 $f \in L(37, 36)$, $g^{(1)} \in L(36, 36)$, $g^{(2)} \in L(36, 36)$. 检查 f 是否在 $Z_q[X]/(X^N-1)$ 和 $Z_p[X]/(X^N-1)$ 上都可逆. 检查 $f - g^{(2)}$ 是否在 $Z_p[X]/(X^N-1)$ 上可逆. 如果通过了所有检查, 存储 $\{f, g^{(1)}, g^{(2)}\}$ 作为私钥, 否则重新选择 $f \in L(37, 36)$. 分别记 f_q^{-1} 和 f_p^{-1} 为 f 在 $Z_q[X]/(X^N-1)$ 和 $Z_p[X]/(X^N-1)$ 上的逆. 记 $(f - g^{(2)})_p^{-1}$ 为 $(f - g^{(2)})$ 在 $Z_p[X]/(X^N-1)$ 上的逆. 计算并存储 $h^{(1)} = \{f_q^{-1}g^{(1)}\}(\text{mod } q)$, $h^{(2)} = \{f_q^{-1}g^{(2)}\}(\text{mod } q)$, $H = \{(f - g^{(2)})_p^{-1}g^{(1)}\}(\text{mod } p)$. 公钥为 $\{h^{(1)}, h^{(2)}, H\}$.

签名. 设消息已经经过填充和杂凑, 成为了随机化的消息 m , 其中 $m \in Z_p[X]/(X^N-1)$.

计算 $m^{(1)} = \{f_p^{-1}m\}(\text{mod } p)$.

计算 $m^{(2)} = \{f_p^{-1}Hm\}(\text{mod } p)$.

取 $t = (t_0, t_1, t_2, \cdots, t_{N-1})$, $t^{(1)} = (t_0^{(1)}, t_1^{(1)}, t_2^{(1)}, \cdots, t_{N-1}^{(1)})$, $t^{(2)} = (t_0^{(2)}, t_1^{(2)}, t_2^{(2)}, \cdots, t_{N-1}^{(2)})$, 如下:

① 如果 $f_{j_0} = f_{j_1} = \cdots = f_{j_{35}} = -1$, 而对其它下标 j 有 $f_j \neq -1$, 则

$t_{j_0} = m_0^{(1)}, t_{j_1} = m_1^{(1)}, \cdots, t_{j_{17}} = m_{17}^{(1)},$

$t_{j_{18}} = m_0^{(2)}, t_{j_{19}} = m_1^{(2)}, \cdots, t_{j_{35}} = m_{17}^{(2)},$

对其它下标 j 有 $t_j = 0$.

② 如果 $g_{j_0}^{(1)} = g_{j_1}^{(1)} = \cdots = g_{j_{35}}^{(1)} = -1$, 而对其它下标 j 有 $g_j^{(1)} \neq -1$, 则

$t_{j_0}^{(1)} = m_0^{(1)}, t_{j_1}^{(1)} = m_1^{(1)}, \cdots, t_{j_{17}}^{(1)} = m_{17}^{(1)},$

$t_{j_{18}}^{(1)} = m_0^{(2)}, t_{j_{19}}^{(1)} = m_1^{(2)}, \cdots, t_{j_{35}}^{(1)} = m_{17}^{(2)},$

对其它下标 j 有 $t_j^{(1)} = 0$.

③ 如果 $g_{j_0}^{(2)} = g_{j_1}^{(2)} = \cdots = g_{j_{35}}^{(2)} = -1$, 而对其它下标 j 有 $g_j^{(2)} \neq -1$, 则

$t_{j_0}^{(2)} = m_0^{(1)}, t_{j_1}^{(2)} = m_1^{(1)}, \cdots, t_{j_{17}}^{(2)} = m_{17}^{(1)},$

$t_{j_{18}}^{(2)} = m_0^{(2)}, t_{j_{19}}^{(2)} = m_1^{(2)}, \cdots, t_{j_{35}}^{(2)} = m_{17}^{(2)},$

对其它下标 j 有 $t_j^{(2)} = 0$.

计算

$$s^{(1)} = fm^{(1)} + pft^{(1)} + pg^{(2)}t,$$

$$s^{(2)} = fm^{(2)} + pft^{(2)} - pg^{(1)}t.$$

$\{m, s^{(1)}, s^{(2)}\}$ 为有效签名.

验证. 设 $\{m, s^{(1)}, s^{(2)}\}$ 是声称的“有效签名”. 以下 5 个等式是验证方程.

$$(V1) s^{(1)} \pmod{q} = s^{(1)},$$

$$(V2) s^{(1)} \pmod{p} = m,$$

$$(V3) s^{(2)} \pmod{q} = s^{(2)},$$

$$(V4) s^{(2)} \pmod{p} = \{Hm\} \pmod{p},$$

$$(V5) \{s^{(1)}h^{(1)} + s^{(2)}h^{(2)}\} \pmod{q} \pmod{p} = \{Hm\} \pmod{p}.$$

注意到

$$\{s^{(1)}h^{(1)} + s^{(2)}h^{(2)}\} \pmod{q} =$$

$$\{g^{(1)}m^{(1)} + pg^{(1)}t^{(1)} + g^{(2)}m^{(2)} + pg^{(2)}t^{(2)}\} \pmod{q},$$

$$\{g^{(1)}m^{(1)} + pg^{(1)}t^{(1)} + g^{(2)}m^{(2)} + pg^{(2)}t^{(2)}\} \pmod{p} = \{Hm\} \pmod{p}.$$

因此 (V5) 成立当且仅当

$$\{g^{(1)}m^{(1)} + pg^{(1)}t^{(1)} + g^{(2)}m^{(2)} + pg^{(2)}t^{(2)}\} \pmod{q} = g^{(1)}m^{(1)} + pg^{(1)}t^{(1)} + g^{(2)}m^{(2)} + pg^{(2)}t^{(2)}.$$

新方案具有与 R-NSS 相似的结构, 但有若干新颖的设计. 其中一个新设计是 3 个多项式 $\{t, t^{(1)}, t^{(2)}\}$, 它们是私钥与课文的特殊非线性函数. 这种设计的目的是确保攻击者既不能由大量签名值得到任何单一私钥的倍式, 也不能由大量签名值得到多个私钥的任何线性组合式, 因此抵抗 Gentry 和 Szydlo^[5] 的攻击以及 Nguyen 和 OdedRegev 的攻击^[6]. 相比 R-NSS, 新方案保持了简洁的计算.

3 由公钥恢复私钥的困难性

第一个安全性问题是由公钥 $\{h^{(1)}, h^{(2)}, H\}$ 恢复私钥 $\{f, g^{(1)}, g^{(2)}\}$ 的困难性.

3.1 对 $\{h^{(1)}, h^{(2)}\}$ 的 CS 格攻击

CS 格攻击见文献[2]. 对于多项式 $u = u_0 + u_1X + u_2X^2 + \cdots + u_{N-1}X^{N-1} \in \mathbb{Z}[X]/(X^N - 1)$, 记 $M(u)$ 为矩阵

$$M(u) = \begin{bmatrix} u_0 & u_1 & u_2 & \cdots & u_{N-1} \\ u_1 & u_2 & u_3 & \cdots & u_0 \\ u_2 & u_3 & u_4 & \cdots & u_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ u_{N-1} & u_0 & u_1 & \cdots & u_{N-2} \end{bmatrix}.$$

设 $L_{CS}(h^{(1)})$ 为由以下矩阵的行生成的格

$$\begin{bmatrix} \mathbf{I}_N & \mathbf{M}(h^{(1)}) \\ \mathbf{0} & q\mathbf{I}_N \end{bmatrix},$$

其中 \mathbf{I}_N 是 N 阶单位阵, 此格显然包含 $2N$ 维向量 $(f, g^{(1)})$, 因为 $fh^{(1)} = g^{(1)} \pmod{q}$. 此格也包含 $2N$ 维向量 $(X^j f, X^j g^{(1)})$, 因为 $X^j fh^{(1)} = X^j g^{(1)} \pmod{q}$, 其中 $X^j u$ 是 u 的 j -步右旋转, $j = 0, 1, 2, \dots, N-1$. 此外, 以上这些向量极有可能就是此格的最小向量 (见文献[2]). 因此, 恢复私钥 $(f, g^{(1)})$ 就是用格归约算法求解格 $L_{CS}(h^{(1)})$ 的最小向量. 已有的格归约算法包括著名的 LLL 算法^[7] 和 BKZ 算法^[8-11]. Alexander May 提出了两种方法降低格归约的复杂度, Gama Nicolas 等^[12-13] 发表了两篇论文提高格归约的速度. 无论如何, 这种攻击对于充分大的 N 是无效的, 比如 $N = 251$.

类似地设 $L_{CS}(h^{(2)})$ 为由以下矩阵的行生成的格

$$\begin{bmatrix} \mathbf{I}_N & \mathbf{M}(h^{(2)}) \\ \mathbf{0} & q\mathbf{I}_N \end{bmatrix},$$

并且 $(f, g^{(2)})$ 极有可能就是此格的最小向量. 因此, 恢复私钥 $(f, g^{(2)})$ 就是用格归约算法求解格 $L_{CS}(h^{(2)})$ 的最小向量. 这种攻击对于 $N = 251$ 也是无效的.

3.2 对 H 的 CS 格攻击

设 $L_{CS}(H)$ 为由以下矩阵的行生成的格

$$\begin{bmatrix} \mathbf{I}_N & \mathbf{M}(H) \\ \mathbf{0} & p\mathbf{I}_N \end{bmatrix}.$$

此格显然包含向量 $(f - g^{(2)}, g^{(1)})$, 因为 $\{(f - g^{(2)})H\} \pmod{p} = g^{(1)}$. 但是此格包含太多的小向量, 比如矩阵的每一行都是小向量. 另外, $(f - g^{(2)}, g^{(1)})$ 可能远远不是最小向量. 因此, 用格归约算法得到的向量几乎不可能是 $(f - g^{(2)}, g^{(1)})$ 或者其旋转向量.

3.3 组合攻击

能否由 $\{h^{(1)}, h^{(2)}, H\}$ 的组合来恢复 $\{f, g^{(1)}, g^{(2)}\}$? 一种考虑是“公因子”. 由两个方程 $h^{(1)} = \{f_q^{-1}g^{(1)}\} \pmod{q}$ 和 $h^{(2)} = \{f_q^{-1}g^{(2)}\} \pmod{q}$, f_q^{-1} 很像是 $h^{(1)}$ 和 $h^{(2)}$ 的“公因子”. 然而传统的求解公因子的方法 (如欧几里德算法) 不能借鉴来求解 f_q^{-1} , 因为模运算 \pmod{q} 破坏了大小顺序. 另一种考虑是将 $\{f, g^{(1)}, g^{(2)}\}$ 看作由以下矩阵的行生成的格的最小向量

$$\begin{bmatrix} \mathbf{I}_N & \mathbf{M}(h^{(1)}) & \mathbf{M}(h^{(2)}) \\ \mathbf{0} & q\mathbf{I}_N & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & q\mathbf{I}_N \end{bmatrix}.$$

此格的归约决不比 $L_{CS}(h^{(1)})$ 和 $L_{CS}(h^{(2)})$ 的更容易. 当然攻击者还知道一个新的方程 $\{(f - g^{(2)})H\} \pmod{p} = g^{(1)}$. 但这个方程无法对格归约给出实用的帮助.

3.4 结 论

综上所述, 由公钥恢复私钥的困难性依赖于若干格上的 SVP 的困难性, 而且没有发现其它的简化攻击.

4 伪造签名的困难性

设攻击者知道公钥, 并设由公钥恢复私钥是困难的. 对于消息 $m \in \mathbb{Z}_p[X]/(X^N - 1)$, 攻击者希望构造“签名值” $\{m, s^{(1)}, s^{(2)}\}$, 即构造 $s^{(1)}$ 和 $s^{(2)}$, 使 $\{m, s^{(1)}, s^{(2)}\}$ 满足验证方程 (V1) ~ (V5). 固定消息 m , 并记 $m^* = \{Hm\} \pmod{p}$.

$\{m, s^{(1)}, s^{(2)}\}$ 满足 (V1) 和 (V2), 当且仅当 $s^{(1)} = m + pu^{(1)}$, 且 $\frac{1}{p}m + u^{(1)}$ 的每个分量在区间 $\left[\frac{-q+2}{2p}, \frac{q}{2p}\right]$ 内. $\{m, s^{(1)}, s^{(2)}\}$ 满足 (V3) 和 (V4), 当且仅当 $s^{(2)} = m^* + pu^{(2)}$, 且 $\frac{1}{p}m^* + u^{(2)}$ 的每个分量在区间 $\left[\frac{-q+2}{2p}, \frac{q}{2p}\right]$ 内.

引理 1. 设 $\{m, s^{(1)}, s^{(2)}\}$ 满足 (V1) ~ (V4), $s^{(1)} = m + pu^{(1)}$, $s^{(2)} = m^* + pu^{(2)}$. 则 $\{m, s^{(1)}, s^{(2)}\}$ 满足 (V5) 当且仅当存在多项式 $v \in \mathbb{Z}[X]/(X^N - 1)$, 使得

$$(1) \left(h^{(1)}u^{(1)} + h^{(2)}u^{(2)} - \frac{q}{p}v\right) + \left(\frac{1}{p}h^{(1)}m + \frac{1}{p}h^{(2)}m^*\right) \pmod{p} = 0$$

的每个分量在区间 $\left[\frac{-q+2}{2p}, \frac{q}{2p}\right]$ 内;

$$(2) \left(h^{(1)}u^{(1)} + h^{(2)}u^{(2)} - \frac{q}{p}v\right) + \left(\frac{1}{p}h^{(1)}m + \frac{1}{p}h^{(2)}m^*\right) \pmod{p} = 0$$
$$- \frac{1}{p}m^* \in \mathbb{Z}[X]/(X^N - 1).$$

证明. $\{m, s^{(1)}, s^{(2)}\}$ 满足 (V5) 当且仅当 $\{s^{(1)}h^{(1)} + s^{(2)}h^{(2)}\} \pmod{q} = m^* + p\omega$, 其中 $\omega \in \mathbb{Z}[X]/(X^N - 1)$.

此式成立当且仅当存在多项式 $v \in \mathbb{Z}[X]/(X^N - 1)$, 使得 $ph^{(1)}u^{(1)} + ph^{(2)}u^{(2)} + h^{(1)}m + h^{(2)}m^* - qv = m^* + p\omega$, $\frac{1}{p}m^* + \omega$ 的每个分量在区间 $\left[\frac{-q+2}{2p}, \frac{q}{2p}\right]$ 内, 并且

$\omega \in \mathbb{Z}[X]/(X^N - 1)$. 证毕.

设 $L_{CS}(h^{(1)}, h^{(2)})$ 由以下矩阵的行所生成的格

$$\begin{bmatrix} \mathbf{I}_N & \mathbf{0} & \mathbf{M}(h^{(1)}) \\ \mathbf{0} & \mathbf{I}_N & \mathbf{M}(h^{(2)}) \\ \mathbf{0} & \mathbf{0} & \frac{q}{p}\mathbf{I}_N \end{bmatrix}.$$

容易看出, $3N$ -维向量 $\mathbf{u} = (u^{(1)}, u^{(2)}, u^{(3)}) \in L_{CS}(h^{(1)}, h^{(2)})$ 当且仅当

$$u^{(3)} = h^{(1)}u^{(1)} + h^{(2)}u^{(2)} - \frac{q}{p}v,$$

其中 $u^{(1)}, u^{(2)}$ 和 v 均来自 $\mathbb{Z}[X]/(X^N - 1)$. 取 $3N$ -维向量 $\mathbf{a} \in (Q[X]/(X^N - 1))^3$ 具有如下形状:

$$\mathbf{a} = (a^{(1)}, a^{(2)}, a^{(3)}) = \left(-\frac{1}{p}m, -\frac{1}{p}m^*, -\frac{1}{p}h^{(1)}m - \frac{1}{p}h^{(2)}m^*\right).$$

命题 1. 攻击者能够构造 $\{m, s^{(1)}, s^{(2)}\}$ 满足验证方程 (V1) ~ (V5), 当且仅当存在格 $L_{CS}(h^{(1)}, h^{(2)})$ 中的 $3N$ 维向量 \mathbf{u} , 使得

- (1) $\mathbf{u} - \mathbf{a}$ 的每个分量在区间 $\left[\frac{-q+2}{2p}, \frac{q}{2p}\right]$ 内;
- (2) $u^{(3)} - a^{(3)} + a^{(2)} \in \mathbb{Z}[X]/(X^N - 1)$.

命题 1 说明, 攻击者对消息 m 成功伪造签名等价于找到格 $L_{CS}(h^{(1)}, h^{(2)})$ 中的向量充分接近 \mathbf{a} , 且 $u^{(3)} - a^{(3)} + a^{(2)}$ 的每个分量都是整数. 这是典型的最近向量问题 (CVP). 到目前为止, 只有 $\mathbf{u} = (0, 0, 0) \in L_{CS}(h^{(1)}, h^{(2)})$ 和 $\mathbf{a} = (0, 0, 0)$ 满足命题 1 的条件.

5 抵抗已知攻击的强度

定义 1^[5]. 对于 N -维向量 $\mathbf{u} = (u_0, u_1, u_2, \dots, u_{N-1}) \in Q[X]/(X^N - 1)$, 记

$$\bar{\mathbf{u}} = (u_0, u_{N-1}, u_{N-2}, \dots, u_1).$$

称 $\bar{\mathbf{u}}$ 为 \mathbf{u} 的逆排序.

引理 2^[5]. 积 $\mathbf{u} = (u_0, u_1, u_2, \dots, u_{N-1})$, $\mathbf{u}\bar{\mathbf{u}} = (w_0, w_1, w_2, \dots, w_{N-1})$. 则

- (1) $w_0 = u_0^2 + u_1^2 + u_2^2 + \dots + u_{N-1}^2$,
- (2) $w_j = w_{N-j}$, $j = 1, 2, \dots, N-1$,
- (3) $w_0 + w_1 + w_2 + \dots + w_{N-1} = (u_0 + u_1 + u_2 + \dots + u_{N-1}^2)$.

如果取 u 为私钥 f , 则 $w_0 = 73$, $w_0 + w_1 + w_2 + \dots + w_{N-1} = 1$.

如果取 u 为私钥 $g^{(1)}$ 或私钥 $g^{(2)}$, 则 $w_0 = 72$, $w_0 + w_1 + w_2 + \dots + w_{N-1} = 0$.

设 $\{(m^{(j)}, s^{(1j)}, s^{(2j)})\}, j = 1, 2, \dots, n$ 是攻击者获

得的 n 个有效签名, 且 n 足够大. 攻击者因此能计算 $s^{(3j)} = \{s^{(1j)}h^{(1)} + s^{(2j)}h^{(2)}\}(\text{mod } q)$. 由 $\{(s^{(1j)}, s^{(2j)}, s^{(3j)})\}$, $j=1, 2, \dots, n\}$ 攻击者能够近似地计算出各种数学期望值, 如 $\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{j=1}^n s^{(1j)} = Es^{(1)}$, $\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{j=1}^n s^{(1j)} \overline{s^{(2j)}} = E\{s^{(1)} \overline{s^{(2)}}\}$ 等等. 注意到这些数学期望都是私钥的已知函数. 如果这些私钥的已知函数是简单函数 (比如二次函数等), 则攻击者就得到了关于私钥的简单方程 (比如二次方程等), 可以用比较简单的方法求解私钥. Gentry 和 Szydlo 的攻击^[5]、Nguyen 和 Oded Regev 的攻击^[6], 都是利用了签名方案的这一弱点.

因为 $E(s^{(1)}, s^{(2)}, s^{(3)}) = (0, 0, 0)$, 所以一阶数学期望的表达式不含有私钥. 然后观察二阶数学期望, 一共有 15 个二阶数学期望, 如下所述.

$$\begin{aligned} &E\{s^{(1)} \overline{s^{(1)}}\}, E\{s^{(2)} \overline{s^{(2)}}\}, E\{s^{(3)} \overline{s^{(3)}}\}, \\ &E\{s^{(1)} \overline{s^{(2)}}\}, E\{s^{(1)} \overline{s^{(3)}}\}, E\{s^{(2)} \overline{s^{(3)}}\}, \\ &E\{s^{(2)} \overline{s^{(1)}}\}, E\{s^{(3)} \overline{s^{(1)}}\}, E\{s^{(3)} \overline{s^{(2)}}\}, \\ &E\{s^{(1)} s^{(1)}\}, E\{s^{(2)} s^{(2)}\}, E\{s^{(3)} s^{(3)}\}, \\ &E\{s^{(1)} s^{(2)}\}, E\{s^{(1)} s^{(3)}\}, E\{s^{(2)} s^{(3)}\}. \end{aligned}$$

15 个二阶数学期望中, 每个都是私钥的极为复杂的非线性函数, 因此 Gentry 攻击^[5] 和 Nguyen 攻击^[6] 在针对本文的新方案时, 没有求解私钥的算法.

6 关于新方案的若干说明

作者设计的新方案具有 R-NSS 结构, 而不具有 NTRUSign 结构. 这是因为作者希望避免 NTRUSign 结构的庞大的密钥生成算法.

新方案不是零知识的, 即签名值会泄露私钥的一些信息, 这是所有基于 NTRU 的签名方案的共同缺陷. 但是新方案力图保证对私钥信息的泄露只能得到难以求解的方程.

新方案暂时还无法建立可证明安全的理论系统, 这也是所有基于 NTRU 的签名方案的共同问题.

尽管基于 NTRU 的签名方案有诸多缺陷, 但它们还有着无比的优越性. 比如, 基于大数分解困难性或以离散对数困难性的签名方案在未来量子计算环境下已经被证明是不安全的^[14], 而基于格上最小向量困难性或格上最近向量困难性的签名方案是未来的可能选择.

参 考 文 献

- [1] Hoffstein J, Pipher J, Silverman J H. NTRU: A new high speed public key cryptosystem//Proceedings of the Algorithm Number Theory (ANTS III). LNCS 1423. Springer-Verlag, 1998: 267-288
- [2] Coppersmith D, Shamir A. Lattice attacks on NTRU//Proceedings of the Eurocrypt'97. LVCS-IACR. Springer-Verlag, 1997
- [3] Hoffstein J, Pipher J, Silverman J H. Enhanced encoding and verification methods for the NTRU signature scheme. Version 2, May 30, 2001. <http://www.ntru.com>
- [4] Hoffstein J, Howgrave-Graham N, Pipher J, Silverman J H, Whyte W. NTRUSign: Digital signatures using the NTRU lattice//Proceedings of the CT-RSA'03. LNCS 2612. Springer-Verlag, 2003: 122-140
- [5] Gentry C, Szydlo M. Cryptanalysis of the revised NTRU signature scheme//Proceedings of the Advances in Cryptology-Eurocrypt'02. LNCS 2332. Springer-Verlag, 2002: 299-320
- [6] Nguyen P Q, Oded R. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures//Proceedings of the Advances in Cryptology-EUROCRYPT'06. LNCS 4004. Springer-Verlag, 2006: 215-233
- [7] Lenstra A K, Lenstra H W, Lovasz L. Factoring polynomials with integer coefficients. Mathematische Annalen, 1982, 261: 513-534
- [8] Schnorr C P. A hierarchy of polynomial time lattice basis reduction algorithm. Theoretical Computer Science, 1987, 53: 201-224
- [9] Schnorr C P. Block reduced lattice basis and successive minima. Combinatorics, Probability and Computing, 1994, 3: 507-522
- [10] Schnorr C P, Euchner M. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. Mathematical Programming, 1994, 66: 181-199
- [11] Schnorr C P, Hoerner H H. Attacking the Chor Rivest cryptosystem by improved lattice reduction//Proceedings of the Advances in Cryptology-Eurocrypt'95. LNCS 921. Springer-Verlag, 1995: 1-12
- [12] Gama Nicolas, Howgrave-Graham Nick, Nguyen Phong Q. Symplectic lattice reduction and NTRU//Proceedings of the Advances in Cryptology-EUROCRYPT'06. LNCS 4004. IACR and Springer-Verlag, 2006: 233-253
- [13] Gama Nicolas, Howgrave-Graham Nick, Koy Henrik, Nguyen Phong Q. Rankin's constant and blockwise lattice reduction//Proceedings of the Advances in Cryptology-CRYPTO'06. LNCS 4117. Springer-Verlag, 2006: 112-130
- [14] Shor P W. Polynomial-time algorithm for prime factorization and discrete logarithm on a quantum computer. SIAM Journal on Computing, 1997, 26(5): 1484-1509



HU Yu-Pu, born in 1955, professor, Ph. D. supervisor. His major research interest is in cryptology, including stream cipher, block cipher, public key cipher, etc.

Background

NTRU is one of the fastest public-key-ciphers known. The security of NTRU is based on the hardness of the shortest vector problem (SVP) of some lattice, called NTRU lattice or CS lattice (named by D. Coppersmith and A. Shamir). Unfortunately, from the point of the security, digital signature schemes following the NTRU design have not been successful enough. Most of them have been broken. The reasons why such attacks are effective are the follow.

Reason 1. Each signature value is a multiple of a single private key (without the protection by the modular operations), with the secret combination coefficients. So that the GCD method can be used to recover the private key.

Reason 2. Each signature value is a linear combination of the private keys (without the protection by the modular operations), with the secret combination coefficients. The

combination coefficients have a public distribution (for example, uniform distribution). By a large number of signatures, the attacker can filter off the combination coefficients, and obtain the value of some simple function of the private keys. Such function can be taken as the function of real number variables. Those methods of the continuous mathematics (for example, the optimization method) can be used for computing the private keys.

Although the digital signature schemes following the NTRU design have so many security weaknesses, they may be the candidates in the future computation environment, because RSA and DSA have been broken in the quantum computation environment. So that it is worth to take an advanced research for the digital signature schemes following the NTRU design.