NTRU 公开密钥体制及其应用

张晓鹏　何大可
（西南交通大学计算机与通信工程学院国家高性能计算中心，成都 610031）

【摘　要】公开密钥体制 NTRU 算法的安全性取决于从一个非常大的维数格中寻找很短向量的困难性上，它高速、低需求、易实现、密钥产生容易。介绍了这种密钥体制的理论基础和使用方法并与其它密码体系进行了比较。

【关键词】NTRU　加密　解密

NTRU Public Key Cryptosystem and Its Application

Zhang Xiaopeng　He Dake
(College of Computer Engineering, Southwest Jiao Tong University, Chengdu 610031)

【Abstract】NTRU is a new public key cryptosystem . The security of NTRU is based on the hard mathematical problem that of finding very short vectors in lattice of very high dimension. Encryption and decryption with NTRU is extremely fast and key creation is fast and easy to use. This paper introduced the theoretical basis and the implementing method of the NTRU cryptosystem and compared it with other cryptosystems.

【Keywords】NTRU, encryption, decryption

1 引言

NTRU(Number Theory Research Unit) 公开密钥算法是一种新的快速公开密钥体系，它是在 1996 年的美洲密码学会上由布郎大学数学系的三位美国数学家 Hoffstein，Pipher，Silverman 提出的。经过几年的迅速发展与完善，该算法在密码学领域中受到了高度的重视并在实际应用中取得了很好的效果。

2 NTRU 理论基础

NTRU 算法的安全性是基于数论中在一个非常大的维数格中寻找一个很短向量的数学难题，它的正确性是基于随机变量和的群集特性上的。在一个格中找长度最短的非零向量是一个 NP 完全问题。一个格可以被看作在一个向量空间中的特定元素集合中的整系数的线性组合集，在一个 2 维空间中由有整数的坐标的所有点组成的无穷多方格就是一个格的例子，这个格子是由向量(0,1)和(1,0)组成的整线性组合。

基于格的方法被分成两个基本类。实际上，在这两类之间存在着有效的转换。第一类问题是基于所谓的子集和的问题：给定一个数的集合 $S=\{a_1,a_2,\cdots a_t\}$以及另一个数 K，寻找 S 的一个子集，它的值和为 K。Merkle 和 Hellman 的背包问题就是这样的一个例子。20 世纪 80 年代初期 Lovasz 发表了著名的 LLL 算法[2]。这个算法成功地在多项式时间内找到了不超过最短向量的 $2^{(n-1)/2}$ 倍的短的向量，而且往往在实际应用时效果很好。1982 年 4 月，著名密码学家 Shamir 就用该算法的改进算法攻破了 Merkle－Hellmanr 基于背包问题的公钥体制。

另一种基于网格的方法需要寻找在一个网格中的短向量或寻找在向量空间中接近网格顶点的点或接近网格中的向量的点。Ajtai 和 Dwork [AD97] 是这种类型的一个例子。数学家们试图找到‘较短’向量的多项式时间算法。NTRU 算法的提出人研究了一些潜在的攻击方法，并推断它们几乎不可能成功。他们还考虑了标准的基于格的攻击方法，并且指出了攻击者并不能通过 LLL 算法来计算在这个格中的最短向量来找到密钥，因为密钥被一个由许多按指数规律地不相关格向量所组成的‘云’所环绕。

3 NTRU 公钥密码体制操作步骤

3.1 产生参数

在 NTRU 算法中，参数算法需要三个整数参数(N，p，q)和四个 L。首先确定 3 个参数 p，q，N，其中两个是素数 p，

收稿日期：2003－01－06。
张晓鹏：1977 年生，助工，硕士研究生。研究方向为网络安全。
何大可：1944 年生，教授，博士生导师。研究方向为密码学、网络安全、通信保密、并行计算。

q(或者是两个互素的正整数)，N 是 NTRU 要使用的多项式的次数。在 NTRU 中，两个多项式的乘 $f * g$，先进行通常的相乘，然后将各单项式的系数分别模 q，次数模 N。对于 f：$f \in L_f$ 多项式要求其系数为 1 的个数等于 d_r，而系数为 -1 的个数等于 $d_r - 1$，其余系数等于 0。对于 g：$g \in L_g$ 多项式要求其系数为 1 和 -1 的个数相等，并且等于 d_g，其余的系数等于 0。对于 r：$r \in L_r$ 多项式要求其系数为 1 和 -1 的个数相等，并且等于 d_r，其余的系数等于 0。表 1 是 NTRU 技术根据不同的安全级推荐的参数。

表 1 NTRU 中推荐使用的参数

	N	P	q	d	d	d
一般安全	107	64	3	15	12	5
高安全	167	128	3	61	20	18
最高安全	503	256	3	216	72	55

3.2 产生密钥

首先选取两个互素的整数 p，q(如 256，3)，两个次数为 N 的多项式 f，g，并且这两个多项式的系数都是小整数 (如 0～255)。接着，计算 $F_p \equiv f^{-1} \bmod p$ 和 $F_q \equiv f^{-1} \bmod q$。再计算 $h \equiv p(f_q * g) \bmod q$。将多项式 h 作为公钥，而将一对多项式 f 与 F_p 作为自己的私钥，在 NTRU 算法中，私钥和公钥不可交换使用。

3.3 加密过程

在 NTRU 中，一个消息 m 就是一个次数为 N 的多项式，它的系数也是小整数。首先根据参数 d_r 随机选取一个多项式 r，系数取自 $\{1,0,-1\}$。接着，计算 $e \equiv (r * h + m) \bmod q$，$e$ 就是加密后的消息。NTRU 保密性就在于多项式 r 的随机选取，然后模 q 运算上。

3.4 解密过程

得到 e 以后，先计算 $a \equiv e * f \bmod q$，再计算 $a * F_p \bmod p$，其结果就是消息 m。

4 NTRU 的安全性分析和比较

NTRU 体制中有两种运算：“加”和“乘”，因此是基于环上运算的。而基于大数分解困难的 RSA 体制和基于离散对数困难的 ECC 体制只是在群上运算。数论上的传统观点认为，基于环的问题比基于群的一般要困难得多。NTRU 体制中 N 选的较大时，L 的维数也大，从而使得寻找 L 的最短向量相当困难。另一方面，L 越接近一个随机的格，就越难找到最短向量。就目前来说，NTRU 的安全性和目前最有影响的 RSA 算法、椭圆曲线加密体制 ECC 等算法是一样安全的。NTRU 算法设计非常巧妙，整个算法只包括小整数的加、乘、模运算，在相同安全级的前提下，NTRU 算法的速度比要比其它公开密钥体制的算法快的多，用 NTRU 算法产生密钥的速度也很快，NTRU 密钥的位数也较小。NTRU 算法的优点意味着可以降低对带宽、处理器、存储器的性能要求，这也扩大了 NTRU 公开密钥体制的应用范围。表 2 所示即为 NTRU 的安全特性。表 3 为 NTRU 与 RSA 在加、解密及密钥产生时间上的比较。

表 2 NTRU 的安全特性

	私钥长度 (位)	公钥长度 (位)	估计破解所需时间
一般安全	340	642	25.7 天
高安全	530	1169	541～610 年
最高安全	1595	4024	$5.4 * 10^{13}$ 年

表 3 NTRU 与 RSA 的性能比较

	四密等极	加密速度(块/秒)	解密速度(块/秒)	密钥产生时间 (s)
NTRU	一般	16666	2273	0.0079
	高	4762	724	0.0184
	极高	730	79	0.1528
RSA	512	1020	125	0.26
	768	588	42	0.59
	1024	385	23	1.28

在表 3 中 NTRU 的性能是在 200MHz Pentium, Linux 系统下测得，RSA 的性能则是在 225MHz Digital Alpha Station 下测得。

由上述对比可看出，在大致相同的等级下，NTRU 体制比 RSA 体制在加密、解密、以及密钥产生速度方面都要快。

5 NTRU 密码体制的应用

5.1 PASS 多项式认证与签名方案)

安全和密码算法面临许多的挑战，特别是约束系统中，许多算法的计算代价是昂贵的，但是要在高数据速率下确保适当的系统响应时间或吞吐量，算法的实现必须小心的保证安全的操作并防止任何缺陷。而 NTRU 提供了一个适宜于在强限制环境中如：智能卡、无线应用等中使用的多项式认证与数字签名方案 PASS (Polynomial Authentication and Signature Scheme)。它基于的算法 NTRU 以高速和小的占用而著称。

5.2 NSS

NSS (NTRU 签名方案，NTRU Signature Scheme) 补充了 NTRU 公开密钥体制的论证/签名方法。NSS 建立所依赖的数学难题是与 NTRU 建立所依赖的数学难题是相似的并且 NSS 相似的拥有高速、低需求以及易于产生密钥的特点。

6 结束语

NTRU 算法被认为公开密钥体制中最快的算法。它高速、低需求、易实现、密钥产生容易，快速而安全，必将在诸如：智能卡、移动通信系统、保密数据网、电子商务、电子现金和微型支付系统及认证系统等业务方面发挥重要作用。NTRU 完全有可能在公开密钥体制中占有主导地位，它将是一个大有作为的密码体制。

参考文献

1 Hoffstein J, Pipher J, Silverman J H. NTRU: A new high speed public key cryptosystem. Crypto'96, 1996: 471

2 Lenstr A K. Factoring Polynonials with Interger Coefficients. Math Ann, 1982; 261: 513

3 步山岳. 快速安全的 NTRU 公开密钥体制. 淮阴工学院学报, 2002; 11(1): 67

4 肖鸿, 赵惠文. 格基归约在密码上的应用. 西安电子科技大学学报, 2000; 27(6): 736