基于格理论公钥密码体制的分析与研究

白 健[1,2] 杨亚涛[2] 李子臣[1,2]

[1](西安电子科技大学通信工程学院 西安 710071)
[2](北京电子科技学院 北京 100070)

摘 要 AD 公钥密码体制，NTRU 公钥密码体制和 Regev 公钥密码体制是基于格理论公钥密码体制中最具代表性的三种公钥密码体制。文章分别从困难问题，安全性和计算复杂性三个角度对三种公钥密码体制进行分析与研究，指出三种公钥密码体制的联系与区别，并将基于格的公钥密码体制与其他公钥密码体制进行比较，指出了基于格理论公钥密码体制的显著优点。

关键词 格；公钥密码体制；NTRU；AD 公钥密码体制；Regev 公钥密码体制

Analysis and Research of Public-Key Cryptosystems Based on Lattice

BAI Jian[1,2] YANG Yatao[2] LI Zichen[1,2]

[1](*Communication Engineering Institute*, *Xidian University*, *Xi'an* 710071, *China*)
[2](*Beijing Electronic Science and Technology Institute*, *Beijing* 100070, *China*)

Abstract In the public-key cryptosystems which are based on lattice, AD's public-key cryptosystem, NTRU and Regev's public-key cryptosystem are the most famous public-key cryptosystems. Through hard problems, security and computational complexity, we analyze and research these three public-key cryptosystems. The connection and difference among these three public-key cryptosystems are given in this paper. We also compare the cryptosystems based on lattice with the cryptosystems based on other hard problems, giving the advantages of the cryptosystems based on lattice.

Keywords lattice; public-key cryptosystem; NTRU; AD' public-key cryptosystem; regev' public-key cryptosystem

1 引 言

1996 年 Ajtai 发表论文称发现了某些著名的格问题的最坏情况复杂性和平均情况复杂性之间存在一种联系。后来 Ajtai 和 Dwork 提出了一种新的密码体制[1]——基于格理论的公钥密码体制，自此便为公钥密码体制开辟了一个新的领域。GGH 公钥密码体制[2]，NTRU 公钥密码体制[3]，Regev 公钥密码体制[4]等基于格理论的公钥密码体制相继被提出。由于它们具有抵抗量子攻击且运算简单的优点，成为众多学者研究和关注的热点。近来，Stehle 和 Steinfeld[5]结合 NTRU 公钥密码体制和 R-LWE 思想，对 NTRU 公钥密码体制进行改进，使得改进后的 NTRU 在理想格上最坏情形下达到 CPA(Chosen-Plaintext attack)安全，Zvika Brakerski 等人在参考参考文献[6]中给出了关于 LWE(Learning With Errors)的困难性规约。

本文主要对格理论公钥密码体制发展过程中三个最重要的公钥密码体制进行分析和研究，分别对三种公钥密码体制的困难问题、安全性和计算复杂性进行分析与研究，指出其困难问题和安全性的联系和区别，同时给出计算复杂性相应的分析比较的结果。

基金项目：国家自然科学基金(61070219)。

作者简介：白健(通讯作者)，硕士研究生，研究方向为密码学、格理论，E-mail：jbai1989@163.com；杨亚涛，博士，研究方向为无线通信安全、密码学等；李子臣，教授，博士生导师，研究方向为信息安全密码学。

2　格背景知识

2.1　格的基础概念

定义 1：设 $v_1,v_2,\cdots,v_m$ 线性无关，m 维格 $L(v_1,v_2,\cdots,v_m)$ 是指由向量 $v_1,v_2,\cdots,v_m$ 生成的一个向量集，它的形式表示如下：

$$L(v_1,v_2,\cdots,v_m)=\sum_{i=1}^{m}a_iv_i,\ a_i\in Z$$

称$\{v_1,v_2,\cdots,v_m\}$为格 L 的一组基，且记 $Dim(L)=m$。m, n 分别为格 L 的维数和秩。当 $m=n$ 时，称格 L 是满维的(Full Dimensional)。

2.2　两种最基本的格困难问题

定义 2(SVP，Shortest Vector Problem)：对于给定格的一组基 $B\in Z^{n\times m}$，找到格中的一个非零向量 $\boldsymbol{\lambda}=B\boldsymbol{x}\ (\boldsymbol{x}\in Z^m)$，使得对于任意的 $\boldsymbol{y}\in Z^m,\boldsymbol{y}\neq 0$，满足$\|\boldsymbol{\lambda}\|\leqslant\|B\boldsymbol{y}\|$。

定义 3(CVP，Closest Vector Problem)：对于给定格的一组基 $B\in Z^{n\times m}$ 和一个任意的目标向量 $\boldsymbol{t}\in Z^n$，找到格中的一个非零向量 $\boldsymbol{\lambda}=B\boldsymbol{x}\ (\boldsymbol{x}\in Z^m)$，使得对于任意的非零向量 $\boldsymbol{y}\in Z^m$，满足$\|\boldsymbol{\lambda}-\boldsymbol{t}\|\leqslant\|B\boldsymbol{y}-\boldsymbol{t}\|$。

2.3　三种格公钥密码体制的介绍

2.3.1 AD 公钥密码体制

密钥选取：如果 u 是 u-SVP 格 L 中的最短向量，那么由 u 可以确定一组超平面(隐藏平面组)$\{H_i\,|H_i=\{x|<u,x>=1\}\}$，$i\in Z$。AD 系统将这组超平面作为 AD 的私钥。通过一些特殊的方法，生成一个与这组超平面很接近的空间点，这个点就是公钥。根据这个点来推测超平面的难度等价于最坏输入情况下的 u-SVP 问题。

加密过程：AD 密码算法进行加密是按照逐比特方式来进行的。加密比特“0”时，通过公钥找到超平面附近的一个随机向量 $v\in R^n$，向量 v 就是该“0”比特对应的密文。加密比特“1”的时候，随机均匀地从空间 R^n 中选择一个向量 w，向量 w 就是该“1”比特对应的密文。

解密过程：解密时利用私钥(超平面)检查密文对应的点是否足够靠近超平面。如果是，则解密为比特“0”，否则，解密比特为“1”。

2.3.2 NTRU 公钥密码体制

密钥选取：NTRU 的 3 个公开参数为(N,p,q)，通常情况下 $p=3$，$q=2^k$，N−1 是多项式的最高次数。它构建在商环 $Z[x]/(x^N-1)$ 上。$L(a,b)$ 表示环中具有 a 个系数为 1，b 个系数为−1，其余系数均为 0 的全体整系数多项式。随机选取两个多项式 $f=1+pF$ 和 $g\in L(d_g,d_g)$，其中保证 f 存在逆元 f_p 和 f_q，使得 $f*f_p=1(\mathrm{mod}\,p)$，$f*f_q=1(\mathrm{mod}\,q)$。计算 $h=f_q*g(\mathrm{mod}\,q)$，则 NTRU 的公钥为(N, p, q, h)，私钥为 f。

加密过程：用户选取随机多项式 $r\in L(d_r,d_r)$，对于明文消息 m，计算 $c=pr*h+m(\mathrm{mod}\,q)$ 得到密文。

解密过程：解密者得到密文 $c=pr*h+m(\mathrm{mod}\,q)$后，

(1)计算　$a\equiv c*f(\mathrm{mod}q)$；

(2)计算　$m'=a*f_p$；

(3)计算　$m\equiv m'(\mathrm{mod}\,p)$。

2.3.3 Regev 公钥密码体制

密钥选取：随机均匀选取 $\boldsymbol{s}\in\mathbb{Z}_p^n$ 作为私钥，从独立均匀分布中选取 m 个向量 $a_1,\cdots,a_m\in\mathbb{Z}_p^n$，$i=1,\cdots,m$，从分布 χ 中独立地选取元素 $e_1,\cdots,e_m\in\mathbb{Z}_p$，公钥便是$(\boldsymbol{a}_i,b_i)_{i=1}^m$，其中 $b_i=<\boldsymbol{a}_i,\boldsymbol{s}>+e_i$。

加密过程：当需要加密一比特时，从 $[m]$ 的 2^m 的子集中的一个集合 S。如果该比特是 0，加密为 $(\sum_{i\in S}a_i)$，如果该比特是 1，加密为 $(\sum_{i\in S}a_i,\left\lfloor\frac{p}{2}\right\rfloor+\sum_{i\in S}b_i)$。

解密过程：密文$(\boldsymbol{a},b)$进行解密，如果 $b-<\boldsymbol{a},\boldsymbol{s}>$ 接近 0，我们就解密为 0，如果接近$\left\lfloor\frac{p}{2}\right\rfloor$，就解密为 1。

3　三种公钥密码体制的困难问题研究分析

下文将对 AD 公钥密码体制基于 u-SVP 问题，NTRU 基于 PFP 困难问题，Regev 基于 LWE 困难问题进行简单描述。

u-SVP：如果一个 n 维格 L 中仅有唯一短向量 v，并且其他长度至多是它的 n^c 倍的向量都平行于 v，那么从格中找到这个最短的向量 v 是困难的，并且称这种格为 u-SV 格。

PFP(Polynomial Factorization Problem)[7]：给定多项式 $h=f_q^{-1}*h\equiv g'(\mathrm{mod}\,q)$，其中 f 和 g 的系数相对于 q 来说是较小的。对适当的参数设置，如果仅知道 h，很难恢复出多项式 f 或 g，或者很难找到两个具有较小系数的多项式 f' 和 g' 满足 $f'*h\equiv g'(\mathrm{mod}\,q)$。

LWE(Learning With Errors)问题[8]：设 n，p 是整数，$\boldsymbol{s}\in Z_p^n$，$\boldsymbol{a}\in Z_p^n$，错误向量 $e\in\chi$，其中 χ 是 Z_p 上的高斯概率分布，输入 $(\boldsymbol{a},<\boldsymbol{a},\boldsymbol{s}>+e)$，计算 $\boldsymbol{s}$。

格密码中两类最基本的困难问题是 SVP 和 CVP，

在讨论上述两个 NP 问题时，可将其转换为其他三种不同的问题：(1)搜索问题，(2)优化问题，(3)判定问题。上面的三种问题是可以实现相互规约的，即判定 SVP≤p、优化 SVP≤p、搜索 SVP 和判定 CVP≤p、优化 CVP≤p、搜索 CVP [9]，所以在实际情况中，针对具体的应用，选择其中一种问题讨论即可。AD 密码体制依据的 u-SVP 等同于特殊格 u-SV 格中的 SVP 问题。NTRU 的 PFP 问题建立在基于 CS 格中的 SVP 问题[10]，要寻找到由公钥 h 生成的 $2n$ 维 CS 格中长度较小的向量，即解决 γ-SVP问题，就有可能破解 NTRU。虽然 CS 格具有一定的特殊性，但到目前为止还没有理论证明特殊格中的 SVP 问题、CVP 问题或是近似 NP 困难问题的计算难度相比于普通格中的困难问题容易。而 LWE 问题则是等同于 GAPSVP 问题，也就是判定版本的 SVP 问题，这个在参考文献[4]中给出了相关的定理和说明。

4 安全性比较分析

AD 密码体制是第一个建立在格困难问题的公钥密码算法，现在已经被淘汰了，其被淘汰的主要原因有三个：解密错误现象较高、工作效率较低问题以及实用性不强问题，但它的安全性还是相对较高的。Ajtai 和 Dwork 在参考文献[1]中证明：如果存在概率算法能够区别 AD 加密的“1”和“0”，那么该算法就能用于解决所有 $\lambda_2(L)/\lambda_1(L)>n^8$ 的 SVP 问题。而目前的研究表明，SVP 问题是 NP 问题，因此不存在多项式时间算法能够区别 AD 加密的“1”和“0”。Nguyen 和 Stern[5]还证明了，如果存在能够解决近似因子小于 $n^{0.5-\varepsilon}$ 的 app-SVP 算法，或者是存在能够解决近似因子小于 n^{133} 的 app-CVP 算法，那么攻击者能够在多项式时间内以较高的概率恢复明文。

NTRU 密码体制是现在公认较好的基于格理论的密码体制，从加解密过程中我们可以看出参与加密的隐私信息有 f，g 和 r，所以攻击 NTRU 的两种途径为：一是恢复 f 和 g；二是找到加密消息用的随机多项式 r。然而需要注意的是多项式 r 只能恢复到明文 m，但却无法得到私钥 f 和 g，因此找到 r 对恢复出其他用同一公钥 h 加密的明文是没有帮助的。NTRU 常用攻击方法主要有强力攻击，中间相遇攻击，多次发送攻击和格基规约算法攻击。但在复杂性上这些攻击方法还都未达到要求，因此 NTRU 目前仍然被认为是比较安全的，表 1 给出了 NTRU 与 RSA 的安全性对比。

表 1 NTRU 与 RSA 安全性对比

系统	密钥长度 (bits)	安全性 (MIPS yrs)
RSA 1024	1024	3.00×10^{12}
NTRU263	1841	4.61×10^{14}
RSA2048	2048	3.00×10^{21}
RSA4096	4096	2.00×10^{33}
NTRU503	4024	3.38×10^{38}

对于 Regev 公钥密码体制，在参考文献[4]中提到：对于任意 $\varepsilon>0$，$m\geqslant(1+\varepsilon)(n+1)\log p$，如果存在一个多项式时间算法可以区分 Regev 公钥密码体制中加密的“0”和“1”，则存在一个区分器，可以区分 $A_{s,\chi}$ 和 $\boldsymbol{Z}_q^n\times Z_q$，其中 $A_{s,\chi}$ 是变量 $(\boldsymbol{a},\boldsymbol{a}^T\boldsymbol{s}+x)$ 所形成的在 $\boldsymbol{Z}_q^n\times Z_q$ 上的分布。详细的安全性证明过程请参考文献[4]。

从总体上来看，AD 公钥密码体制和 Regev 公钥密码体制具有较高的安全性，但是由于其加密方式都是针对逐比特进行的，所以其公私钥以及明密文的长度较长，不适合实际应用，而 NTRU 的安全性还存在质疑，这些方面都严重制约的格公钥密码体制的大范围的应用。

5 计算复杂性比较分析

在这节我们主要对三种公钥密码体制的相关计算复杂性进行研究分析。

AD 公钥密码体制(AD97，AD07)公钥长度为 $O(n^4)$，加密后密文扩展 $O(n)$，而 Regev 公钥密码体制(Reg04)的公钥长度为 $O(n^4)$，加密后密文扩展 $O(n^2)$。

NTRU 避免了大指数求模运算和离散对数运算，只涉及多项式环上的乘法和小整数求模运算，这使得它的运算速度远快于现在广泛使用的 RSA，ECC，ElGamal 等公钥密码体制。这个优点使得 NTRU 可以降低对带宽、处理器、存储器的性能要求，扩大了它的应用范围。NTRU 的相关计算复杂性见下表 2[3]。

采用参数 N＝107 的 NTRU 程序在 CPU 为 Intel(R)Core(TM)i5-2410M 2.30GHz 环境下针对文件加解密速率进行测试得到的相关数据如下表 3。

表 2 NTRU 相关计算复杂性

明文大小	密文大小	加密速度	解密速度	加密扩展	私钥长度	公钥长度
$N\log_2 q$ bits	$N\log_2 q$ bits	$O(N^2)$次	$O(N^2)$次	$\log_p q$-to-1	$2N\log_2 p$ bits	$N\log_2 q$ bits

表 3　采用 N=107 的 NTRU 对文件加解密时间

密文文件大小	加密时间	解密时间
2 KB	15 ms	32 ms
5 KB	31 ms	141 ms
10 KB	62 ms	204 ms

6　小　结

本文通过对格理论发展过程中产生的三种里程碑式的公钥密码体制进行分析和研究，指出了三种公钥密码体制所依据的格困难问题以及与格理论的联系，同时阐述了三种公钥密码体制的安全性和相关的计算复杂性。在以后的研究过程中，我们旨在创新，重点将会放在基于格的密码体制的研究和设计中去。由于基于格的密码体制具有抵抗量子攻击和运算量小的优点，研究和设计新的更加安全的基于格的密码体制已经成为大家研究的热点问题。相信在不久的将来，基于格的公钥密码体制一定会有广泛的应用，进而对人类社会的生产和生活产生巨大的推动作用。

参 考 文 献

[1] Ajtai M, Dwork C. A publie-key cryptosystem with worst-ease/average-ease equivalence [C] // Proceedings of the 29th Annual ACM Symposium on Theory of Computing, 1997: 284-293.

[2] Bellare M, Rogaway P. Optimal asymmetric encryption [C] // Proceedings of Workshop on the Theory and Application of Cryptographic Techniques Perugia, 1995: 92-111.

[3] Hoffstein J, Pipher J, Silverman JH. NTRU: a ring-based public key cryptosystem [C] // Proceedings of Algorithmic Number Theory Symposium, 1998: 267-288.

[4] Regev O. On lattices, learning with errors, random linear codes, and cryptography [J]. Journal of the Association for Computing Machinery, 2009, 56(6): 1-40.

[5] Stehlé D, Steinfeld R. Making NTRU as secure as worst-case problem over ideal lattices [C] // Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2011: 27-47.

[6] Brakerski Z, Langlois A, Peikert C, et al. Classical hardness of learning with errors [C] // Proceedings of the 45th Annual ACM Symposium on Theory of Computing, 2013: 575-584.

[7] 黄琼, 赵一鸣. 基于格的公钥密码系统及其安全性分析 [J]. 计算机工程, 2005, 31(10): 60-65.

[8] 潘平, 王励成, 何万生. 基于格的公钥加密体制的研究 [J]. 天水师范学院学报, 2012, 32(5): 30-34.

[9] 李德龙, 王绪安. 基于格的公钥密码体制研究 [J]. 武警工程学院, 2009, 4: 44-48.

[10] Coppersmith D, Shamir A. Lattice attacks on NTRU [C] // Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, 1997: 52-61.