编者按：公开密钥密码的诞生在现代密码学中具有里程碑式的意义，它的出现极大地推进了现代密码学的发展，使得数字时代的信息安全有了根本性的保障。然而，公钥密码也面临新的安全问题和挑战，首先，随着量子大数分解算法的提出，以 RSA 公钥密码为基石的安全系统在量子计算时代将丧失其安全性。如何寻找能抵御量子计算的密码系统就成为异常紧迫的问题。其次，隐私保护、数据安全等问题在新的网络计算环境如云计算中更为突出，而全同态加密是实现解决这些问题的理想技术手段，但如何实现高效的全同态加密一直是困扰现代密码学的难题。

格(lattice)是 $n$ 维线性空间的离散加法子群，格理论中有许多难解问题，这些难解问题具有很多适合应用于密码学的优良特性。迄今为止，还没有发现求解这些难解问题的多项式时间算法和量子算法，这使得基于格的密码系统成为一种有竞争力的抗量子攻击密码候选方案。此外，格的理论和密码系统也是构建和实现全同态加密的理想工具。然而，目前国内对基于格的密码学意义认识不足，研究人群不多，研究不够深入，相关资料也很缺乏，从事网络信息安全的研究生觉得入门困难，为引起对这一技术领域的广泛关注，提高我校在这一领域的研究基础和水平，我们面向教员、研究生和工程技术人员开设这一讲座。

本讲座主要介绍基于格公钥密码的基本理论、密码原语、公钥密码方案、全同态加密技术及在信息安全上的相关应用等方面的内容，专题共分为以下 6 讲：第 1 讲基于格的密码学概述；第 2 讲基于格的密码函数构造及其应用；第 3 讲基于格的公钥密码方案；第 4 讲基于格的全同态加密实现方案与相关技术；第 5 讲基于格的全同态加密的优化技术；第 6 讲基于格的密码学在信息安全上的应用。

# 基于格的密码学技术专题讲座(一)

## 第 1 讲　基于格的密码学概述

杨　明，王兆丽，韩敬利
(解放军理工大学指挥信息系统学院，江苏 南京 210007)

**摘　要**：文章介绍了基于格的密码学的研究背景和主要内容，阐述了格基本理论，包括基本概念、定义、性质、格问题和特殊格等，从求解算法、格问题归约和最坏情况安全性等方面讨论了格问题的难度假设，概述了基于格的密码函数构造、公钥密码方案、密码分析和发展现状等内容。

**关键词**：基于格的密码学；最短矢量问题；理想格
**中图分类号**：TP309.2　　**文献标识码**：A　　**文章编号**：CN32-1289(2014)01-0067-08

## Overview of Lattice-based Cryptography

*YANG Ming*, *WANG Zhao-li*, *HANG Jing-li*
(College of Command Information System, PLAUST, Nanjing 210007, China)

**Abstract**: The background and contents of lattice-based cryptography were introduced. The basic theory of lattice including basic concepts and definitions, character, lattice problems and

**收稿日期**：2013-07-20；**修回日期**：2013-10-08
**作者简介**：杨　明(1968－)，男，博士，教授.

special lattice was discribed. The hardness assumption of lattice problems was discussed from aspects of lattice algorithms, lattice problem reduction and the worst-case security. Brief surveys about cryptographic funtions, public-key cryptography, cryptanalysis and development using lattice were presented.

Key words: lattice-based cryptography; shortest vector problem; ideal lattice

目前以 RSA 为代表的公钥密码正广泛应用于各种安全应用中，然而，随着计算机技术的发展和计算能力的提高，为确保安全性，密码长度一直在增加，密钥长度的增加意味着现有的公钥密码方案需要在更大的有限域或群内进行指数运算操作，这将加剧这些公钥密码在加密与解密效率方面的问题。为此，研究者开始研究新的公钥密码方案。目前有两类不同的方法：一是寻找具有更高复杂性的难解问题，以此来降低密钥的长度，有代表性的方案是椭圆曲线公钥系统(elliptic curve cryptosystems)，其依赖的数学难题是椭圆曲线的离散对数问题 ECDLP；另一方法是寻找具有更简单运算的数学难题，以此来降低加解密操作的复杂性，有代表性的是基于格的密码系统(lattice-based cryptography)[1,2]，其基本运算为矢量的加法和乘法。表 1 简要比较了这三种有代表性的公钥密码方案。

1994 年，P. Shor 提出因子分解的量子算法[3]，Shor 算法利用量子计算的并行性，对任意大的整数进行快速因子分解，大大降低了目前普遍使用的 RSA 公开密钥加密技术的破解时间。随后还出现了针对基于离散对数问题的量子求解算法。这样，以 RSA 公钥密码为基石的安全系统在量子计算时代将丧失其安全性，寻找能抵御量子计算攻击的密码系统就成为异常紧迫的问题，这就是所谓的后量子计算时代的密码学(post-quantum cryptography)。

表 1 不同公钥密码方案的基本比较

| | 大数因子分解问题 | 椭圆曲线离散对数问题 | 格难解问题 |
|---|---|---|---|
| 提出时间 | 70 年代中期 | 80 年代中期 | 90 年代中期 |
| 典型实例 | RSA, DSA | ECDSA | NTRU |
| 实际应用 | 大规模应用 | 推荐应用 | 局部应用 |
| 主要优势 | 深入研究 | 小密钥 | 基于最坏情况复杂性；抗量子攻击；全同态加密 |
| 加/解密操作 | 模 $n$ 的幂运算；$O(n^2)$ | 椭圆曲线上加法运算；$O(n^2)$ | 矢量乘法；$O(n)$ |

## 1 基于格的密码学的主要内容

基于格的密码学的研究内容包括：格的相关理论、格问题的难度证明、密码函数构造、公钥密码和数字签名算法、密码攻击与分析、密码协议及高级密码应用等。基本内容框架如图 1 所示。

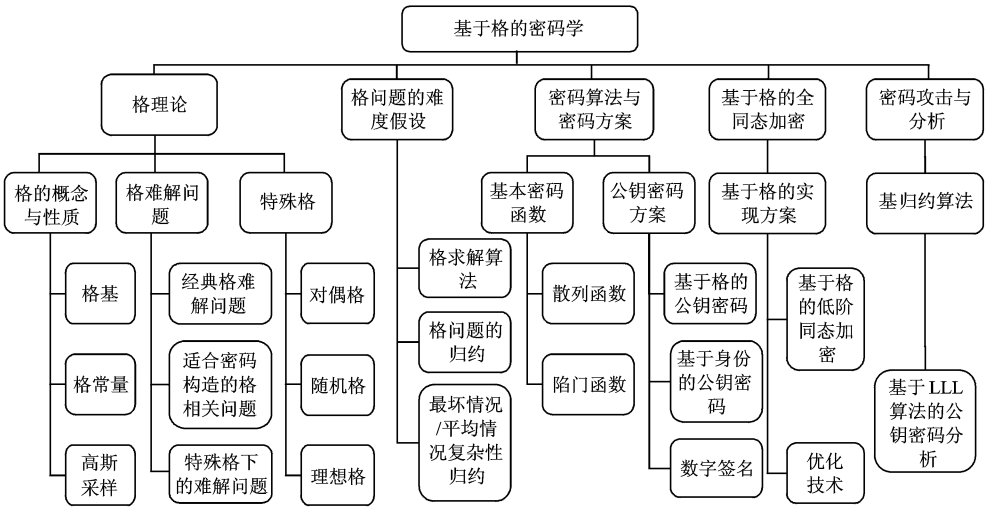


图 1 基于格的密码学内容框

格理论：有关格理论的研究可追溯到两百多年前，对格相关理论研究已取得丰硕的研究成果。在此将格理论的主要内容概括为格的概念和性质、格问题和特殊格

三个部分。重点介绍格的定义、基的性质和格的基本运算等概念；格中有许多难解问题，这些难解问题具有很多适合构建密码函数的独特性质，是格理论中的核心研究内容；特殊格研究在基本格的基础上导出的格和具有特殊结构的格，包括在这些格上格问题的难度和特性，这将是改善现有基于格的密码方案效率的重要手段。

格问题的难度假设：现代密码学将密码系统的安全性建立在某个已知的难解问题之上，问题难度将决定密码系统的安全性。格问题的难度假设是有关格问题及其近似问题的难度猜想，这种难度假设是建立在现有格问题的求解算法、格问题的归约关系以及基于最坏情况复杂性安全性证明的基础上的。除传统的格问题之外，还有针对特殊结构下的格问题，此外也新出现了一些与格相关问题，这些新的难度还需要证明或验证。格问题的难度假设将是整个基于格的密码学安全的基石。

密码算法与密码方案：使用格来构造密码函数和密码方案是基于格的密码学的核心内容，密码函数的构造主要包括基于格问题的散列函数、陷门单向函数、伪随机函数等的构造方法，这类密码函数具有基于格问题难度的可证明安全性。格密码方案主要包括公钥密码方案和数字签名方案等构造情况。基于这些函数和密码方案，又可以构建新的密码协议和密码应用。

基于格的全同态加密：介绍基于格的全同态加密实现与优化技术。

密码攻击与分析：介绍基于 LLL 格基归约算法的密码攻击与密码分析情况。

本讲将对基于格的密码学进行总体概述性的介绍，重点是格理论和格问题难度，有关内容将在随后的讲座中系统深入地加以介绍。

## 2　格的数学基础

### 2.1　格的基本概念

格是线性空间 $\mathbf{R}^m$ 上的离散加法子群，是具有周期性结构的 $n$ 维空间点的集合。在矢量空间中，子空间可用基来表示，同样，$\mathbf{R}^m$ 上的一个 $n$ 维格可形式化的表示为 $\mathbf{L}(\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n) = \left\{ \sum_{i=1}^{n} x_i \boldsymbol{b}_i \mid x_i \in \mathbf{Z} \right\}$，其中，$\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n \in \mathbf{R}^m$ 为给定 $n$ 个线性无关的向量，也称为格的基 $\boldsymbol{B}=[\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n]$，而格就是由这组基向量产生的系数为整数的的向量集合。格也可使用矢量和矩阵表示，为 $\mathbf{L}(\boldsymbol{B}) = \{\boldsymbol{B}\boldsymbol{x} \mid \boldsymbol{x} \in \mathbf{Z}^n\}$。当 $n=m$，格 $\mathbf{L}(\boldsymbol{B})$ 是满秩的。为方便讨论，本文讨论仅限于 $n$ 维欧几里德矢量空间中满秩格。

格的基并不唯一，格可由不同的基表示，图 2 为一个两维格和不同基的示意图。对于格 $\mathbf{L}(\boldsymbol{B})$，如果 $\boldsymbol{U}$ 为幺模矩阵，则基 $\boldsymbol{B}$ 和 $\boldsymbol{BU}$ 产生相同的格，即 $\mathbf{L}(\boldsymbol{B})=\mathbf{L}(\boldsymbol{BU})$。

格矢量的长度是定义格问题的基本量，可通过范式 $l_p$ 来进行定义，通常使用最多的是 $l_2$。同一格矢量在不同的基下将有不同长度变化。对于不同的基，长度较短的基在格问题中有很重要的作用。格的基本运算就是基本矢量空间中的矢量运算，包括矢量的加法、乘法、点积等。

格的行列式定义 $\det(\mathbf{L}(\boldsymbol{B}))=|\det(\boldsymbol{B})|$，其值与格基的选择无关，是已定义格的一个不变量，从几何意义上看，格行列式的值与格点的密度成反比。

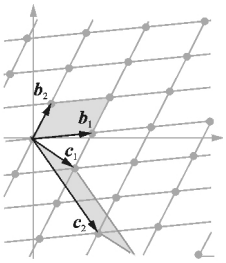


图 2　两维格及其两个不同的基 $(\boldsymbol{b}_1, \boldsymbol{b}_2)$，$(\boldsymbol{c}_1, \boldsymbol{c}_2)$

### 2.2　导出格

给定一个格，可导出与其相关的具有不同结构与性质的格，如对偶格、$q$ -元格等。

(1) 对偶格

给定一个格 $\mathbf{L}\subset\mathbf{R}^n$，其对偶格 $\mathbf{L}^{\times}$ 定义为：$\mathbf{L}^{\times}=\{\boldsymbol{y}\in\mathbf{R}^n \mid \forall \boldsymbol{x}\in\mathbf{L}, <\boldsymbol{x}, \boldsymbol{y}>\in\mathbf{Z}\}$，对偶格还满足 $\mathbf{L}(\boldsymbol{B})^{\times}=\mathbf{L}((\boldsymbol{B}^{-1})^{\mathrm{T}})$，$\det(\mathbf{L}^{\times})=1/\det(\mathbf{L})$。对偶格可用于构建新的基于身份的公钥密码方案。

(2) $q$ -元格

在 Ajtai 提出最坏情况复杂性安全保证的证明中，定义了一种 $q$ -元格，又称为随机格，通过寻找随机格中的最短矢量问题来进行安全性证明。$q$ -元格的基本特性是：如果 $\boldsymbol{x}\equiv\boldsymbol{y} \bmod q$，那么 $\boldsymbol{x}\in\mathbf{L}$，当且仅当 $\boldsymbol{y}\in\mathbf{L}$。

其中，应用最多的是如下形式的随机格：

$\Lambda_q^{\perp}(\boldsymbol{B})=\{\boldsymbol{x}\in\mathbf{Z}^m \mid \boldsymbol{B}\boldsymbol{x}=0(\bmod q)\}$，其中 $\boldsymbol{B}$ 为模 $q$ 的 $n\times m$ 整数矩阵。

$\Lambda_q(\boldsymbol{B})=\{\boldsymbol{x}\in\mathbf{Z}^m \mid \boldsymbol{B}^{\mathrm{T}}\boldsymbol{x}=\boldsymbol{y}(\bmod q),\ \boldsymbol{x}\in\mathbf{Z}^n\}$

这两个 $q$ -元格彼此是对偶格，即 $\Lambda_q^{\perp}(\boldsymbol{B})=q\cdot\Lambda_q(\boldsymbol{B})^{\times}$，$\Lambda_q(\boldsymbol{B})=q\cdot\Lambda_q^{\perp}(\boldsymbol{B})^{\times}$。

### 2.3 循环格和理想格

(1) 循环格

为改善格在密码学应用中的效率，需要考虑一些具有特殊结构的格，循环格就是这样的格，它在公钥密码方案 NTRU(Number Theory Research Unit)[4] 中有很好的应用。循环格是对格上点的分量进行循环移位后形成的点依然是这个格上的点，即循环格 $\mathbf{L}\subseteq\mathbf{Z}^n$，对于 $\forall(u_1,\ u_2,\ \cdots,\ u_n)\in\mathbf{L}$，必然有 $(u_n,\ u_1,\ \cdots,\ u_{n-1})\in\mathbf{L}$。对于循环格的矢量 $\forall(u_1,\ u_2,\ \cdots,\ u_n)\in\mathbf{L}$ 及 $(u_n,\ u_1,\ \cdots,\ u_{n-1})\in\mathbf{L}$，它们的长度保持不变，即 $\|(u_1,\ u_2,\ \cdots,\ u_n)\|=\|(u_n,\ u_1,\ \cdots,\ u_{n-1})\|$。

循环格与环的理想有密切的联系[5]，将格矢量 $\boldsymbol{u}\in\mathbf{Z}^n$ 进行多项式的系数嵌入，即 $\boldsymbol{u}=(u_1,\ u_2,\ \cdots,\ u_n)$ 对应多项式 $f(x)=u_1+u_2x+\cdots+u_nx^{n-1}$，这样的循环格对应多项式商环 $\mathbf{Z}[x]/<x^n-1>$，其中 $<x^n-1>$ 为多项式环 $\mathbf{Z}[x]$ 的理想。

利用循环格的特殊结构，不仅可以进行更紧凑的表示，减少密钥量，还可利用快速算法如 FFT 实现高效的密码运算。

(2) 理想格

理想格的取名源于所有格矢量的集合构成某种环的一个理想，常见的理想格是对应环 $\mathbf{Z}[x]/<f(x)>$ 中理想的格，其中 $f(x)$ 为首一多项式。循环格也是一种特殊的循环格，由于 $x^n-1$ 是可归约多项式，由其构成的哈希函数不具有抗碰撞性。选择不可归约多项式 $f(x)$ 形成的理想格 $\mathbf{Z}[x]/<f(x)>$ 具有更好的性质。对于理想格矢量，其格矢量长度不再象循环格矢量那样保持不变，其大小变化情况使用膨胀因子来定义。为控制膨胀因子，可选择合适的 $f(x)$，目前常用的选择有：① $f(x)=x^n+1$，$n=2^k$，$k\in\mathbf{N}$；② $f(x)=x^{n-1}+x^{n-2}+\cdots+x+1$，$n$ 为素数。

## 3 格问题的难度假设

### 3.1 格问题

格问题研究的历史悠久，可追溯到 200 多年前，高斯就研究了两维格的最短矢量算法。格问题的主要形式是寻找满足某种最小化特性的格矢量，最为经典的格问题是最短矢量问题(SVP)和最近矢量问题(CVP)。表 2 给出了应用最为广泛的格问题，其中，SVP、CVP、最短独立矢量问题(SIVP)和最短基问题(SBP)问题都是直接的格问题，而其他问题则是与格问题密切相关的问题，如有限距离解码问题(BDD)可形式化为最近矢量问题(CVP)的特例，通过选择合适的误差参数，有误差学习问题(LWE)又可看作是特定格上的 CVP 问题，也可转换后描述为 BDD 问题。

SVP 问题是 NP 难问题，在实际的应用中，通常只需要寻找到“足够短”矢量，因此也出现了近似的格问题。为寻找更适合密码学应用的问题，还会对格问题进行扩展，提出相应的扩展问题，这些扩展包括近似问题、唯一性问题、判定问题等，表 3 给出了 SVP 问题的扩展问题示例。

针对不同格，格问题还可以有不同的难度和性质，为提高密码方案的效率，有研究将普通格上的难解问题延伸到理想格上，具有特殊结构的理想格会导致某些问题的难度发生变化，而有的问题难度还需要重新证明或验证。

### 3.2 格问题的难度

Ajtai[6,7] 在 1997 年证明了最著名的格问题－最短矢量问题(SVP)是在随机归约下是 NP 难问题，解决

表 2　经典的格问题

| 格 问 题 | 问 题 描 述 |
|---|---|
| 最短矢量问题(SVP) | 给定格 L 的一个基 $\boldsymbol{B}$，找出格 L 中非零的最短矢量。 |
| 最接近矢量问题(CVP) | 给定格 L 的一个基 $\boldsymbol{B}$ 和一个目标矢量 $t$，找出 L 中最靠近 $t$ 的格矢量。 |
| 最短独立矢量问题(SIVP) | 给定格 L 的一个基 $\boldsymbol{B}$，寻找 $n$ 个线性无关的格矢量，使得这 $n$ 个矢量的最长矢量最短。 |
| 最短基问题(SBP) | 给定格 L，寻找长度最短的基。 |
| 小整数解问题(SIS) | 给定模整数 $q$，矩阵 $\boldsymbol{A}\in\mathbf{Z}_q^{n\times m}$，$m\geqslant n$ 和一个实数常量 $c$，要求寻找非零矢量 $\boldsymbol{u}\in\mathbf{Z}^m$，满足 $\boldsymbol{Au}=0 \bmod q$ 且 $\|\boldsymbol{u}\|\leqslant c$。 |
| 有限距离解码问题(BDD) | 给定格 L 的一个基 $\boldsymbol{B}$，一个距离参数 $\alpha$ 和一个目标矢量 $x$，矢量 $x$ 到格的距离小于格最短矢量的 $\alpha$ 倍，找出与 $x$ 距离恰等于 $x$ 到格的距离的格矢量。 |
| 有误差学习问题(LWE) | 已知 $m$ 个相互独立学习样本$(\boldsymbol{a}_i, b_i)$，$i=1, 2, \cdots, m$，其中 $\boldsymbol{a}_i\in\mathbf{Z}_p^n$，$b_i\in\mathbf{Z}_p$，$i=1, 2, \cdots, m$，满足：$b_i=<\boldsymbol{a}_i, s>+e_i$，误差 $e_i$ 服从概率分布 $\chi$，$s\in\mathbf{Z}_p^n$ 为未知量，求解未知量 $s$。 |

表 3　SVP 格问题的扩展问题

| 格 问 题 | 问 题 描 述 |
|---|---|
| 最短矢量问题(SVP) | 给定格 L 的一个基 $\boldsymbol{B}$，找出格 L 中非零的最短矢量。 |
| 近似最短矢量问题(aSVP) | 给定格 L 的一个基 $\boldsymbol{B}$ 和近似因子 $\gamma\geqslant 1$，找出格 L 中非零的矢量 $\boldsymbol{u}$，即 $\boldsymbol{u}\in\mathbf{L}$，满足 $\|\boldsymbol{u}\|\leqslant\gamma\min\|v\|$。 |
| 唯一最短矢量问题(uSVP) | 给定格 L 的一个基 $\boldsymbol{B}$ 和倍数因子 $\gamma\geqslant 1$，找出格 L 中非零的最短矢量 $\boldsymbol{u}\in\mathbf{L}$，对其他的格矢量 $\forall\boldsymbol{v}\in\mathbf{L}$ 满足 $\|\boldsymbol{v}\|\leqslant\gamma\|\boldsymbol{u}\|$。 |
| 最短矢量的判定问题(GapSVP) | 给定格 L 的一个基 $\boldsymbol{B}$，一个实数 $\zeta$ 和近似因子 $\gamma\geqslant 1$，如果 $\lambda_1(\mathbf{L})\leqslant\zeta$，返回 YES；如果 $\lambda_1(\mathbf{L})>\zeta\gamma$，返回 NO。 |

了长期悬而未决的难题。格的最近矢量问题($CVP$)也被证明是 $NP$ 难问题。此外，针对这些问题的近似问题的复杂性也已进行了广泛而深入的研究，当近似因子为指数因子即 $\gamma=2^{n(\log\log n)^2/\log n}$ 时，利用著名的格基归约算法 LLL[8] 及其改进算法可在多项式时间内求解；而当近似因子 $\gamma<c/\log\log n$ 时，$c$ 为一常数，除非 P=NP，否则没有多项式时间求解算法。随着研究的深入，研究成果表明格的 SVP 问题和 CVP 的近似问题因近似因子的不同而具有不同的复杂性，当近似因子 $\gamma>c/\log\log n$，SVP 问题将不再是 NP 难问题。其近似因子对应的复杂性关系图如图 3 所示。其中 P 表示多项式时间易解问题类，BPP 表示有限错误率的概率多项式时间问题类，NP 表示非确定图灵机下多项式时间类，CoNP 为 NP 问题的补问题类，hard 表示等价 CVP 或 SVP 难解问题。

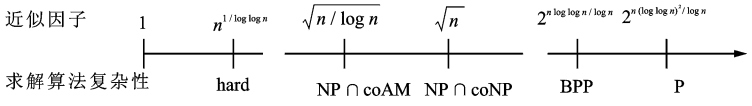


图 3　格问题的难度

目前，已知的求解 SVP 问题最好的算法时间复杂性为 $O(2^n)$，空间复杂性也为 $O(2^n)$；而当空间复杂性为 $O(n^k)$ 时，算法复杂性则上升为 $O(2^{n\log n})$。此外，自从 Shor 量子因子分解提出以来，针对求解格问题的量子算法研究和尝试就一直不断，然而，到目前为止，几乎没有任何进展。为此，对近似格问题有如下两个难度猜想：①难度猜想 1：不存在近似因子为多项式的求解近似格问题的多项式时间算法；②难度猜想 2：不存在近似因子为多项式的求解近似格问题的多项式时间量子算法。

问题归约(reduction)方法是证明问题复杂性的基本方法，通过不同问题的归约，可建立归约问题之间复杂性的联系。图 4 为目前已证明的不同格问题之间的归约关系，其中 A→B 表示问题 A 可在多项式时间归约为问题 B。归约是一种映射，A→B 表示存在一种映射，将问题 A 的实例转化为问题 B 的实例，同时表明问题 B 的难度不低于问题 A 的难度。图中的 $\star$ 表示这种归约还依赖于这些问

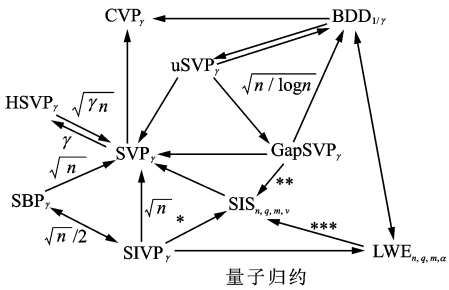


图 4　不同格问题的归约关系

题的参数选择。通过格中的基本问题如 SVP、CVP 和 SIVP 可以和更多的相关问题建立归约关系图，这样从理论上证明了这类问题的难解性，为格问题的难度假设提供了理论依据。

### 3.3 基于最坏情况的安全保证

尽管现代密码学采用难解问题来提供可证明安全性，然而，问题的这种难解性通常是基于最坏情况的，在密码系统实际实现和应用过程中，采用的难解问题实例并不总是难解的，因此密码系统的安全性通常是基于难解问题的平均情况复杂性。

对于基于格问题密码系统来说，其安全性可建立在最坏情况复杂性上。Ajtai 提出一个近似 SVP 问题的单向函数构造方法，近似因子 $n^c$，$c>0$，其安全性基于最坏情况复杂性。该单向函数是基于随机格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 上的短矢量问题，其中 $\boldsymbol{A}$ 为从 $\mathbf{Z}_q^{n\times m}$ 随机选取元素构造的随机矩阵。通过选择合适的参数 $m$，$n$，$q$，随机格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 上的短矢量问题与最坏情况下的格问题如 aSVP 具有同等的难度。随着研究的深入，这种基于最坏情况的安全性保证还可出现在其它的格相关问题中[9]。目前，绝大多数公钥密码系统都是基于平均情况复杂性的，基于最坏情况复杂性是格密码系统所特有的。

## 4 密码函数与公钥密码方案的构造

### 4.1 散列函数

基于效率原因，当前散列函数的实现主要基于 Ad-Hoc 的设计原则，类似分组密码的构造方法，然而，这类构造方案缺乏可证明安全性保证，其安全性缺乏保障，如 MD5 就已经被破解。因此，更为理想的构造方法转向基于某些难解问题的可证明安全性的构造方法。然而，这样的构造方法还存在不尽人意的地方：效率比分组密码方式低，无法抵御量子计算的攻击。

基于格问题的抗攻击散列函数的构造始于 Ajtai 的工作，Ajtai 提出了一个基于 SIS 问题的单向散列函数，其基本构造为 $f_A(x)=\boldsymbol{A}\boldsymbol{x} \bmod q$，其中 $\boldsymbol{A}$ 为取自 $\mathbf{Z}_q$ 的随机矩阵，通过选取合适的参数，该散列函数取得了最坏情况的安全保证。基于特殊格如循环格或理想格还可获得更高效的实现方式。事实上，基于格的散列函数具有如下优势：可证明安全性，基于最坏情况复杂性假设；能抵御量子攻击；实现效率可与传统的类分组密码方式相比。目前，最新的方案是 SWIFFT[10]，这是一个高效的散列函数族，基于理想格上的难解问题，是一个极有竞争力的可证安全性抗攻击散列函数方案。

### 4.2 公钥密码系统

基于格的公钥密码系统构造是基于格的密码学的重要内容，目前，沿着两条不同的路线向前迈进，一条路线是从效率和实用出发，另一条路线则优先考虑构建可证明安全性。

基于效率和实用路线的典型公钥密码系统包括 GGH[11] 和 NTRU 公钥密码系统，不足的是这些密码系统还缺乏可证明安全性的难解问题支持。GGH 公钥密码方案是完全利用格理论和问题构建的，其单向陷门函数是基于最近矢量问题，使用不同基作为密钥，其中由较短且几乎正交的基矢量组成的“好”基作为私钥，而“坏”基作为公钥。NTRU 公钥密码方案是一个基于环的密码系统，NTRU 公钥密码方案可看作基于理想格而构建的，它充分利用了理想格的结构性，具有很高的效率，但缺乏可证明安全性支持，利用 NTRU 密钥上的格结构特性，已有使用格基归约算法对其进行攻击的尝试。

基于可证安全性路线的公钥密码方案包括 AD 公钥密码系统和基于有误差的学习问题(LWE)的公钥密码方案[12]。目前，这类公钥密码方案存在的最大问题是效率较低。为使公钥密码系统达到兼顾可证明安全性和效率的目标，Regev 提出了 LWE，证明了格问题 GapSVP 和 SIVP 在量子条件下可归约为 LWE 问题。基于 LWE 问题难度假设，LWE 问题展现其惊人的多才多艺，成为构建新型密码学的利器，在 Regev 提出基于 LWE 的公钥密码方案的第一个应用后，又出现了以 LWE 问题为基石的密码学函数、算法、方案和协议，其中包括有损失的陷门函数、基于身份的加密 IBE、不经意传输 OT 协议、CCA 安全密码系统和全同态加密方案等，开创了基于格的密码学研究和发展的新篇章。尽管基于 LWE 的公钥密码方案的效率已有

所改进，但其密钥量、加解密的运算量仍然很大。因此，已开始考虑利用定义于环上的 LWE 问题来改善其效率[13]。

## 5　基于格基归约算法的密码分析

最初对格理论的研究主要集中在基归约算法上，其目标是如何寻找性质更好的基。1982 年由 Lenstra，Lenstra 和 Lovasz 发表著名的 LLL 格基归约算法，同时应用 LLL 格基归约算法解决了有理多项式分解的难题。LLL 算法的巨大价值不仅体现在数学和计算机领域，还立即成为密码分析中的利器，特别是针对公钥密码方案分析的重要工具。Shamir 使用 LLL 算法破解了基于背包问题的 Merkle-Hellman 公钥密码方案；此外，基于格基归约算法的成功密码学攻击还包括：Blum 秘密交换协议、小指数 RSA 分析、截断线性同余产生器、基于有理数或模背包的密码系统。鉴于 LLL 算法在公钥密码分析中的巨大成功和影响，早期，格理论在密码学中的应用始终是“负面的”。

目前，LLL 算法依旧是求解 SVP 问题的理想方法，也自然成为攻击基于格密码系统的首选工具。LLL 算法也出现了新的改进技术，这一方面使基于格的密码系统面临更严厉的攻击，另一方面，也通过这样的攻击挑战来验证格密码系统的安全性，增强人们对其安全性的信心。

## 6　基于格的全同态加密实现方案

与全同态加密的概念相近的隐私同态在 RSA 算法不久就提出了，同态加密是指具有能直接对密文进行函数运算而解密后其结果与明文直接函数运算的结果相同的性质。现有的很多公钥密码方案都具有一种或两种同态运算的功能，但进行任意函数同态加密的全同态方案的构造和实现则很困难，从提出后的三十多年时间里，一直没有进展。直到 2009 年，C. Gentry[14] 提出了构建全同态加密的方案，并且提出了一个基于理想格的全同态加密实现方案。此后，基于格的全同态加密方案成为研究的主流，出现了一些基于 LWE 问题的公钥密码构建低阶同态加密的方案，这也是构建 Gentry 全同态加密方案的第一步。当然，现有的全同态加密方案效率还很低，因此，有关全同态加密实现方案优化技术的研究很多，这些优化技术涉及大量格的理论。尽管全同态加密技术取得了突破性的进展，但距离实用化还有较长的路要走。

## 7　基于格的密码学应用

随着量子计算技术的快速进展，网络信息安全必须面对量子计算攻击的现实，而基于格的密码系统是抗量子攻击密码很有竞争力候选方案，其意义和作用将不言而喻。基于格的公钥密码成为实现全同态加密方案的基石与核心，全同态加密能实现对密文进行有效操作而不泄漏明文信息，因此在隐私保护、多方安全计算、数据与服务外包等方面有诸多的应用，也将成为解决云计算环境中安全与信任问题的强有力技术手段。

## 8　结束语

随着量子计算的进展，针对抗量子计算密码学的研究变得很迫切，一种公钥密码方案从提出到能大规模部署应用，其间需要经过大量的研究、改进和验证等工作，特别是安全性要经过长期持久地考验，人们对其安全性才能逐步建立起信心。此外，效率也是影响实用化的重要因素，密码系统的成熟需要大量的研究和工作。

事实上，基于格的密码学正是这样一块有待深耕沃土和有待雕琢的美玉。基于格的密码学的安全性是建立在格问题的最坏情况复杂性上，许多格问题是 NP 难问题，迄今也还没有发现有效的量子求解算法，加/解密操是简单的矢量运算，易于构建更复杂的密码函数等。当然，基于格的密码学也还远未成熟，对其安全

性的信任度还不高，接受攻击考验的时间还不够长，密钥量很大，效率还需进一步改进。然而，这些不足和挑战正是我们进行更深入研究的源泉和动力。

## 参考文献：


[1] Micciancio D，Regev O. Lattice-based cryptography[C]// Post Quantum Cryptography. Berlin-Heidleberg：Springer，2009：147-191.

[2] Peikert C. Public-key cryptosystems from the worst-case shortest vector problem[C]// ACM Symposium on Theory Of Computing(STOC). Bethesda：ACM Press，2009：333-342.

[3] Shor P. Algorithms for quantum computation：discrete logarithms and factoring[C]// Annual Symposium on Foundations of Computer Science. Santa Fe：IEEE Press，1994：124-134.

[4] Hoffstein J，Pipher J，Silverman J. NTRU：a ring-based public key cryptosystem[C]// Algorithmic Number Theory，Portland：Springer，1998：267-288.

[5] Micciancio D. Generalized compact knapsacks，cyclic lattices，and efficient one-way functions[J]. Computational Complexity，2007，16(4)：365-411.

[6] Ajtai M. Generating hard instances of lattice problems[C]// ACM Symposium on Theory Of Computing(STOC). New York：ACM Press，1996：99-108.

[7] Ajtai M，Dwork C. A public-key cryptosystem with worst-case/average-case equivalence[C]// ACM Symposium on Theory Of Computing(STOC). EI Paso：ACM Press，1997：284-293.

[8] Lenstra A，Lenstra H，Lovasz L. Factoring polynomials with rational coefficients[J]. Mathematicsche Annalen，1982，261(4)：515-534.

[9] Micciancio D，Regev O. Worst-case to average-case reductions based on gaussian measures[J]. SIAM Journal on Computing，2007，37(1)：267-302.

[10] Lyubashevsky V，Micciancio D，Peikert C，et al. SWIFFT：a modest proposal for FFT hashing[C]// Fast Software Encryption(FSE 2008). Lausaanne：Springer，2008：54-72.

[11] Goldreich O，Goldwasser S，Halevi S. Public-key cryptosystems from lattice reduction problems[C]// Crypto'97. Santce Barbara：Springer，1997：112-131.

[12] Regev O. On lattices，learning with errors，random linear codes，and cryptography[C]// ACM Symposium on Theory Of Computing(STOC). Baltimore：ACM Press，2005：84-93.

[13] Lyubashevsky V，Peikert C，Regev O. On ideal lattices and learning with errors over rings[C]// Eurocrypt 2010. French Riviera：Springer，2010：1-23.

[14] Gentry C. Fully homomorphic encryption using ideal lattices[C]// ACM Symposium on Theory Of Computing(STOC). Bethesda：ACM Press，2009：169-178.


（上接第 63 页）


[4] 孙 腾，孙安健. 基于 XML 数据交换的电子政务系统集成[J]. 计算机应用与软件，2012，29(5)：188-190.

[5] 谷宁静. 基于 IPSec 和 XML 的电子政务数据交换系统的设计[J]. 科技通报，2012，28(10)：40-42.

[6] 章 玥，邱雪松，孟洛明. 基于 Web Services 的网络管理业务流程管理系统交互接口[J]. 电子与信息学报，2008，30(6)：1470-1474.

[7] 彭 营. 基于 XML 和本体的 Web 数据集成的研究与应用[D]. 大连：大连海事大学，2008.

[8] 叶枝平，李振坤，刘竹松，等. 基于 XML 的数据交换平台的研究与设计[J]. 微计算机信息，2008，24(9)：229，243-244.

[9] 邵秀丽，韩建彬，阎仲蹼. 基于 XML 的异构数据源间数据交换的实现研究[J]. 南开大学学报：自然科学版，2007，40(3)：9-14.

[10] 王 沛. 一种基于 XML 的异构数据库数据转换方法[J]. 西安邮电学院学报，2011，16(3)：73-76.

[11] 董永峰，侯向丹，袁 超，等. 分布式异构数据库同步集成的研究与应用[J]. 计算机应用与软件，2012，29(6)：122-124.

[12] 王淑蓉，赵晋松，黄文泉. 基于 XML 技术的异构数据库集成方案设计[J]. 西安工程大学学报，2011，25(4)：551-554.

[13] 郭亚琴. 数据链消息处理技术[J]. 电讯技术，2009，49(3)：87-91.

[14] 何 赞. 战术数据链消息通用表示方法研究[J]. 舰船电子工程，2011，31(1)：7-9.