**AKCN-MLWE：基于模格MLWE的通用和模块化的密钥封装机制**

**算法说明书**

赵运磊（复旦大学）

程蕾晓（复旦大学）

金正中（复旦大学）

巩博儒（复旦大学）

吴洪祥（银联商务股份有限公司）

隋光烨（上海扈民区块链科技有限公司）

张振峰（中国科学院软件研究所）

2019 年1月

**摘要**

格密码是目前对抗量子攻击的主要数学方法之一。模格介于一般格和理想格之间，其在灵活性、通用性和在128比特后量子安全级别的效率方面具有独特优势。在本提案中，我们给出了基于MLWE（module learning-with-errors）的通用和模块化的密钥封装协议。基于MLWE的密钥封装协议基于我们所发展的性能几乎达到最优界的AKCN非对称密钥共识机制为基础工具。为了适应不同的目标场景或者在安全性、性能和错误率之间取得更好的平衡，我们做了大量的测试去寻找最适合的具体参数设置。

格基密钥协商和格基密钥封装之间存在着紧密的关系，由其中一者不难构造得到另外一者。在本提案中，我们以介绍我们的基于MLWE和AKCN的密钥封装为主，以介绍与之相对应的基于MLWE和SKCN的密钥协商为辅。特别地，为了描述方便，本提案的部分内容以MLWE-SKCN密钥协商为例进行介绍和分析，由此得到的结论和定量化的结果可以简单推广到MLWE-AKCN的密钥封装。类似的，我们的核心工具AKCN和用于密钥协商的SKCN之间也存在着紧密的关系或简单推广。

据我们所知，我们基于MLWE的密钥协商和密钥封装在128比特后量子安全级别具有优良的性能；其核心工具SKCN既用在密钥协商/公钥加密又是我们基于模格数字签名提案的核心工具，这也很好地体现了模块化和通用性。

特别地，与进入NIST后量子密码竞赛第二轮的明星提案KYBER相比，我们的提案同时提供了密钥协商和密钥封装，而KYBER仅提供了密钥封装；在128比特后量子安全级别，我们的算法在综合性能上优于KYBER（更小的带宽、更低的错误率、削掉更多低位比特所带来的额外安全保障等）；并且KYBER的核心工具也是我们在2016年所公布的AKCN非对称密钥共识机制。

本提案的所有算法实现均是算法提交团队独立自主开发完成，没有使用国际开源代码（比如KYBER的实现代码），具有完全的自主知识产权，不存在代码应用的风险。

**目录**

[1 引言 1](#_Toc9043923)

[1.1 我们的贡献 2](#_Toc9043924)

[2 预备知识 2](#_Toc9043925)

[2.1 LWE问题 3](#_Toc9043926)

[2.2 环的选择 4](#_Toc9043927)

[2.3 MLWE问题 4](#_Toc9043928)

[3 Key Consensus with Noise 5](#_Toc9043929)

[3.1 KC的有效上界 6](#_Toc9043930)

[3.2 SKCN的构造和分析 6](#_Toc9043931)

[4 Asymmetric Key Consensus with Noise 9](#_Toc9043932)

[4.1 AKCN的构造和分析 10](#_Toc9043933)

[4.2 KCvs.AKC的讨论 12](#_Toc9043934)

[5 基于MLWE的密钥协商和密钥封装 13](#_Toc9043935)

[5.1公钥密码体制中基于SKCN-MLWE的KEX算法描述 15](#_Toc9043936)

[5.2公钥密码体制中基于AKCN-MLWE的KEM算法描述 16](#_Toc9043937)

[6 基于MLWE的密钥协商和封装分析 16](#_Toc9043938)

[6.1 安全性分析 16](#_Toc9043939)

[6.2 错误率分析 17](#_Toc9043940)

[7 具体参数、和优缺点声明 18](#_Toc9043941)

[8 算法实现代码及性能测试 20](#_Toc9043942)

[8.1. 基于模格的密钥封装性能分析 21](#_Toc9043943)

[8.1.1 空间消耗 21](#_Toc9043944)

[8.1.2 时间与时钟周期消耗 22](#_Toc9043945)

[9 支持文档 23](#_Toc9043946)

[10 参考文献 24](#_Toc9043947)

[11 原创性声明 28](#_Toc9043948)

[12 未来工作 29](#_Toc9043949)

# 引言

一旦大规模的量子计算机被制造出来，大多数基于普通离散对数、椭圆离散对数或者大整数分解的公钥密码系统都将会被攻破，它们的安全性也就无从谈起。许多科学家认为，这种大规模的计算机的到来目前面临的仅仅是工程实现上的挑战，并且IBM的工程师们预测在未来的二十内将被应用。回顾公钥密码学的发展历史，现代密码学基础设施的部署几乎花费了二十年，因此无论我们是否能够准确预测量子计算时代的到来时间，我们都需要将目前的信息安全系统提升到抗量子级别。此外，如果想要让我们目前所有想要保密的文件等在15年或者更久之后依然具有很高的安全性，就必须从现在开始将所有的密码技术替换为抗量子版本。在非对称密码学领域，最关键的技术就是密钥协商和密钥封装。

格密码是目前对抗量子攻击的主要数学方法之一。在密码学的环境下，和其他古典的格困难问题（例如SVP和CVP）相比，LWE（Learning With Error）问题已经被证明功能更加全面[Reg09]。然而，基于 LWE 的密码系统通常都比较低效，因此学者提出了更高效的ring-LWE (RLWE) 问题[LPR10]和MLWE问题[LS15]。在近些年，许多基于LWE及其变体的优秀工作涌现，其中大多数研究[DXL12，Pei14，BCNS15，ADPS16，BCD+16，Reg09，GPV08，LP10，LPR10，LPR13，PG13，BDK+17，NIST] 集中在基于LWE及其变体的密钥协商和公钥加密协议的设计上。模格介于一般格和理想格之间，并且拥有灵活性、通用性和在构造密码系统时性能有竞争力等优良特性。在本提案中，我们设计了基于MLWE 的密钥协商和密钥封装协议。

从技术的角度来说，最新的基于LWE及其变体的密钥协商和密钥封装协议（如 [ADPS16，BCD+16，PG13]）的研究工作中的主要的贡献是改善了密钥协商机制（key reconciliation mechanisms）[DXL12，Pei14，LP10，NIST]。但是在之前的研究工作中，密钥协商机制仅以一种非黑盒的形式在KE和PKE中被使用和分析。这也就是说，对于未来用于构建格基密码系统的新的密钥协商机制，我们需要从头开始分析它们的安全性。此外，对于密钥协商机制中的不同的参数，我们仍不清楚这些参数之间需要满足什么样的上界条件。因此，对于如何去评估不同的密钥协商机制以及判断这些不同的机制是否能够进一步改善，我们依然缺乏一个基本的标准。

抽象化和一般化是自然科学（数学、物理）的基础，对于密码学来说尤其重要。例如，在数字签名领域中，Schnorr签名就是首先抽象化协议[CDS94]然后利用Fiat-Shamir转换[FS86]进行一般化而得到的。类似的抽象化和一般化同样在CCA安全的PKE以及在现代密码学的很多领域扮演了重要的角色。抽象化和一般化在格基密码中也是非常有用的，因为格基密码通常更难以被理解和评估，并且也跟NIST后量子密码标准化[NIST]息息相关。

## 1.1 我们的贡献

在本提案中，通过引入和形式化被称为KC（key consensus）和AKC（asymmetric key consensus）的基础工具，我们提炼出已发表的基于LWE及其变体的密钥协商和PKE方案的关键成分。KC和AKC允许通信双方首先通过某种安全的信息交换协议（比如交换LWE样本）得到两个比较接近的值，然后通过这两个接近的值来达到共识。对于任意的KC和AKC，我们给出参数之间的上界。作为概念上的贡献，这大大的简化了未来密码系统的设计和分析。除此之外，我们分别设计和分析了一般化和是实用的KC和AKC方案，为了表述方便，它们分别被称为SKCN（symmetric key consensus with noise）和AKCN（asymmetric key consensus with noise）。SKCN和AKCN都是紧紧贴合被证明的参数上界的方案。特别地，我们的其中一个工作 [CGZ18] 说明了确定版本的SKCN可以作为构造基于格的签名方案的基石。借助SKCN和AKCN，我们设计了基于MLWE的通用的模块化的密钥协商和密钥封装协议。最后，为了适应不同的目标场景或者在安全性、性能和错误率之间取得更好的平衡，我们做了大量的测试去寻找最合适的具体的参数设置。

# 预备知识

对于任意实数，表示小于等于的最大整数，。对于任意的正整数和，用表示和的最小公倍数。对于任意的，并且，用表示整数集合。对于任意的正整数，令表示。中的元素默认表示为，但有时会明确表示为。

如果是一个有限集合，那么表示它的基数，表示均匀随机的从中取一个元素，表示上的一个均匀分布。

在后面的概率相关的算法、实验和交互协议当中，我们使用传统的符号和概念。如果表示一个概率分布，那么表示根据分布选择一个元素。如果是一个概率算法，那么表示将和随机种子作为输入的的运算结果。 表示随机选取并将运行结果赋值给。如果既不是一个算法也不是一个集合，那么就表示简单的赋值操作。用表示事件在一连串有序的随机过程之后发生的概率。

## 2.1 LWE问题

给定正数，对，定义高斯函数。令表示在上的一维离散高斯分布，其概率密度函数为。最后，令表示在上的*n*维球面离散高斯分布，其中每个坐标都从中独立选取。

给定正整数*n*和*q*，它们都是关于安全参数的多项式，并给定整数向量和一个上的概率分布。令是上的分布：随机均匀选择，选取误差项，并输出。这里误差分布通常被认为是离散高斯概率分布；但是，如文献[BCD+16]中所述，也可以采用其他的分布。简而言之，（判定版本的）LWE假设[Reg09]认为，对足够大的安全参数，没有概率多项式时间（PT）算法能以不可忽略的概率来区分和上的均匀分布。即使敌手看到多项式个样本，并且即使私密向量是从随机抽取的[ACPS09]，该结论仍成立。

## 2.2 环的选择

对于正整数，表示阶分圆多项式 (cyclotomic polynomial)。

表示欧拉函数 (Euler's phi function)。下面我们显式地罗列三种类型的环：

* **幂次环**：是2的幂次，是素数且。故且。在这种情形中，。定义环

，。

这是环的特殊情形。

* **安全素数环-1**：是素数，是使得的安全素数。e是使得的最小的整数，是使得)的素数。在这种情形中，，其中。定义环

，。

* **安全素数环-2**：是安全素数。在这种情形中，，模数是2的幂次或者是使得)的素数。定义环

，。

在下文中, 我们不加说明地将多项式（）跟向量（）等同。因此，对于多项式（）和任意（）上的分布，指的是以分布取向量并将该向量对应为相应的多项式。类似地，一个维的多项式向量（）可以按照分布生成。

## 2.3 MLWE问题

令为上节三种环中的任一类环。在本提案中，为了更高效的实现，在实际应用中我们使用幂次环，即，。

令是一个正整数的参数，令表示中满足的所有元素所构成的集合[[1]](#footnote-1)。MLWE问题[LS15]是RLWE问题的推广，我们使用文献[BDK+17]中的定义。

* **MLWE分布**：来自MLWE 分布的样本，其中均匀，，所有样本使用相同的和不同的，。
* **MLWE假设**：MLWE 问题是从多项式个来自MLWE分布的样本中恢复。具体地，对于敌手，定义

我们称-困难性假设成立，如果没有最多运行时间的算法的优势大于。

# Key Consensus with Noise

在介绍密钥共识（Key Consensus, KC）的完整定义之前，我们首先引入一个函数，其中，并且模运算的结果表示在中，例如。在后面的描述中，我们使用来表示两个元素之间的距离。

**定义3.1**一个密钥共识算法的定义如下：

* 表示系统参数，其中为正整数并且满足，表示辅助信息，通常由确定，其值可以设定为表示值为空；
* ：在输入为的条件下，概率多项式算法的输出为，其中并且为共享密钥，并且为提示信号并在后续的过程中公开传输给另一个节点，从而使得双方能达到共识；
* ：在输入为的情况下，确定的多项式时间算法输出为。

**正确性：**一个密钥共识算法满足正确性，如果对于任意的且都有。

**安全性：**一个密钥共识算法满足安全性，如果对任意和是相互独立的，且在上均匀分布。算法中的概率来源于取样的和中使用的随机种子。

### 3.1 KC的有效上界

下面的这个定理提出了关于参数（控制安全性和效率），（共识密钥范围的参数），（带宽参数）和（错误率参数）的上界，有了这个上界，我们就可以根据不同的优先级在这些参数之间取得一个平衡。定理3.1的详细证明参见支持文档所列论文附录A。

**定理3.1**如果满足正确性和安全性的密钥共识机制，并且，那么。

### 3.2 SKCN的构造和分析

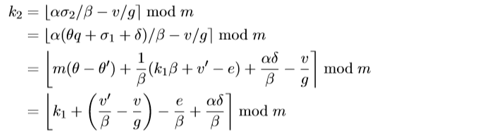
令表示唯一的使得的整数。对于正整数和，有。密钥协商方案 SKCN在算法1中描述。

|  |
| --- |
| **算法1**SKCN：带噪音的对称且四舍五入的密钥共识算法 |
|  |

**事实3.1**对于任意的，其中，如果，那么存在使得。

**定理3.2**若系统参数满足，其中，那么SKCN算法满足正确性。

**证明-定理3.2**假设，由事实3.1可知，存在一个并且，使得。从算法1的第四行到第六行可知，存在，使得。从和的定义中，我们有。将这两个等式代入到（算法1的第十一行）中的等式中可得，



注意到，故

。

由假设的条件，我们可以得到右边是严格小于1/2，因此，在取整之后，有。

**定理3.3**SKCN算法满足安全性。具体来说，当变量之间满足，和是相互独立的，并且均匀分布在中，其中概率取自取样和中使用的随机数。

**证明-定理3.3**在之前的条件中，我们有。我们首先说明是服从中的均匀分布。假设有映射，其中和中元素的表达形式如算法1所示。因为服从均匀分布，并且它们之间相互独立，故也同样服从中的均匀分布。

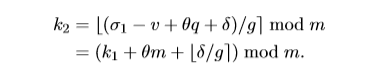
同样，定义，使得，那么显然是个一一映射。从算法1中的第6行我们有。因为服从中的均匀分布，故服从中的均匀分布，因此和是相互独立的。而只依赖于，因此和是相互独立的。

另外，当算法中的参数满足，也就是都是2的幂次时，并且时，SKCN可简化为SKCN Simple，如算法2所示。

|  |
| --- |
| **算法2**SKCN Simple |
|  |

**推论3.1**如果和是2的幂次，并且，那么算法2满足正确性和安全性。

**证明-推论3.1**假设，由事实3.1可知，存在一个并且，使得。将等式将代入到算法2的第八行中的计算中可得，



由假设的条件，有，因此，。

关于安全性的证明，因为算法2是算法1的特殊情形, 故安全性成立。

# Asymmetric Key Consensus with Noise

**定义4.1**一个非对称密钥共识算法定义如下：

* 表示系统参数，其中并且都为正整数，表示由确定的辅助信息，其值可能为空；
* ：在输入为的条件下，概率多项式算法输出公开提示信息；
* ：在输入为的情况下，确定的多项式时间一致算法输出为。

**正确性**：一个非对称密钥共识算法是正确的，如果对于任意的且都有。

**安全性**：一个非对称密钥共识算法满足安全性，如果对于任意的均匀分布在中的，和的分布相互独立。也就是说，对于任意的和任意的，都有，其中概率取自和中使用的随机性。

**定理4.1**令AKC表示一个参数为非对称密钥共识算法，如果AKC满足正确性和安全性，那么。

定理4.1的详细证明参见支持文档所列论文附录B。将定理4.1中的和定理3.1中的相比较，我们可以发现两者之间只相差了一个分子，这表明对于相同的，AKC机制相对于KC机制而言带宽更大。KC/AKC与模糊提取（fuzzyextractor）[DORS08]之间的关系的讨论参见支持文档所列论文附录C。

### 4.1 AKCN的构造和分析

算法3描述了带噪音的非对称密钥共识算法(Asymmetric Key Consensus with Noise, AKCN)。对于AKCN，如果想要加速在线计算的性能，我们可以离线计算并存储和。

|  |
| --- |
| **算法3**AKCN：带噪音的非对称密钥共识算法 |
|  |

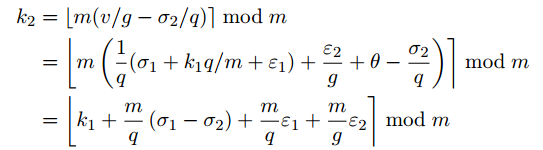
本文所证明的AKC的参数间的上界是AKCN的设计动机。在AKCN的设计中，我们结合了现有文献的优化方法，只为了尽可能满足定理4.1所给出的上界。AKCN是基础的调和机制（reconciliation mechanisms）[LPR10，LP10]的一般化，也受到了SKCN和文献[BPR12,PG13]的启发[[2]](#footnote-2)。特别地，文献[LPR10，LP10]中的调和机制对应着且时特殊的AKCN。

简而言之，AKCN的创新性体现在两个方面：（1）Con程序的设计结合了[LPR10，LP10]中的基础的调和机制以及[BPR12,Pei09]中的四舍五入技巧（rounding technique），而且Rec程序的设计也不是那么直接；（2）参数一般化后允许多比特的共识。据我们所知，现今的工作都不能单独地实例化出AKCN。

**定理4.2**假设AKCN的参数满足，那么算法3描述的AKCN算法满足正确性。

**证明-定理4.2**根据生成的公式，我们知道存在和，其中且，使得

考虑到在Rec中计算的公式，我们有



根据事实3.1，存在和使，因此

由于，故。

**定理4.3** AKCN算法满足安全性。具体来说，当时，和相互独立。

**证明-定理4.3**对任意和任意，我们证明当时，有。对中的任意，事件等价于存在使。注意满足当且仅当存在和，使。也就是说，存在，使得。令。定义映射。显然，是一个一一映射。因此，的基数和无关。具体来说，对于任意的和任意的，都有。故对于任意的和任意的，当时，有。等式右边只依赖于的值，因此和是相互独立的。

另外，当算法中的参数满足，也就是都是2的幂次，且时，AKCN算法可以简化成AKCN simple，如算法4所示。

|  |
| --- |
| **算法4**AKCN simple |
|  |

**推论4.1**如果都是2的幂次满足，并且满足，那么算法4描述的AKCN-simple满足正确性和安全性。

**证明-推论4.1**对于正确性而言，假设，那么存在一个和使得。由计算的公式可知，存在一个和使得。将这些代入到计算的公式中，可得，

如果，那么，因此。

算法4作为AKCN机制的一个特殊的情况，安全性可以直接根据算法3的安全性证明推导得到。

### 4.2 KCvs.AKC的讨论

基于KC和AKC的密钥协商和密钥封装协议具有以下不同的性能和特点：

* 基于KC的密钥协商对应于格世界中的Diffie-Hellman密钥协商，基于AKC的密钥协商对应于ELGamal密钥传输或密钥封装；
* 当在实际中部署基于AKC的密钥封装时，如果响应者使用的随机性不够随机，那么就会完全破坏整个会话密钥的安全性。与之相比，在基于KC的密钥协商中，双方在整个协商的过程中扮演了同等重要的角色，那么由一方的随机性不够引起的问题可以得到解决。并且对称性通常也是密码学方案中一个必备的特点。
* 对于相同的参数（意味着相同的带宽），基于SKCN的密钥协商比基于AKCN的方案具有更低的错误率。或者说，对于相同的参数（意味着相同的错误率），基于SKCN的密钥协商比基于AKCN的方案具有更小的带宽。这个比较是根据定理3.1和4.1中参数之间的上界不等式所得。
* 基于KC的密钥协商功能更加丰富，一方面它可以直接应用于密钥传输协议中或者CPA安全的PKE机制中；另一方面特定版本的SKCN还可以用于构造基于格密码的签名方案[CGZ18]；
* 基于KC的密钥协商更加适用于目前的很多基于Diffie-Hellman和SIGMA机制[Kra03]的标准例如IKE和TLS。我们注意到在TLS1.3中密钥传输已经明确被弃用了[Res]。

基于以上理由，在本提案中我们更多的关注基于KC（而非AKC）的密钥协商和密钥封装协议（特别是密钥协商）。为了简化系统的复杂性，我们仍然致力于寻找可以同时被KC或AKC实例化统一的协议结构。

# 基于MLWE的密钥协商和密钥封装

令是正确且安全的 KC 方案，或者是的AKC方案。令为一个伪随机生成器 (PRG) ，我们利用输入小种子生成矩阵，的长度是。

基于SKCN和MLWE的密钥协商协议如图1所示，基于AKCN和MLWE 的密钥传输协议如图2所示。第5.1节和5.2节则分别描述了如何在公钥密码体制中应用SKCN和AKCN构造基于MLWE的KEM。为了可证明安全，参数

会被设为 0。但是，为了简单和对称性，我们也会假设和裁剪了相同数目的比特，即令。

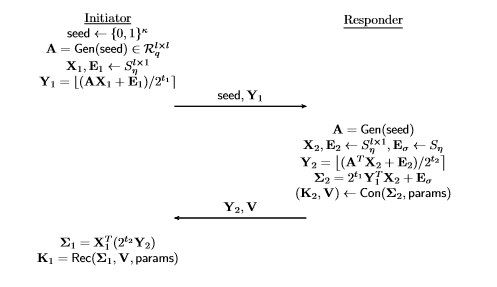
。

图1 SKCN-MLWE的通用构造

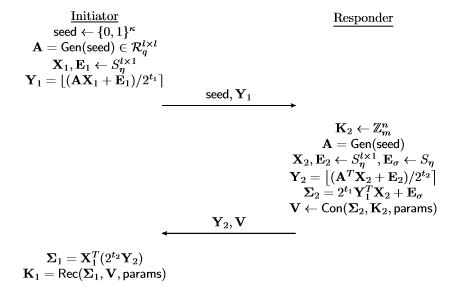


图2 AKCN-MLWE的通用构造，其中

## 5.1公钥密码体制中基于SKCN-MLWE的KEX算法描述

在公钥密码体制中，基于SKCN-MLWE的KEX描述如下。为了简单起见，令。在KEX的实际实现中，共享密钥是由导出的，交互则利用了KDF (key derivation function) (如密码哈希函数或HMAC等) 实现。

到目前为止，所有基于格的密钥交换协议，都是非对称结构的。具体在我们的基于SKCN-MLWE的KEX算法中，

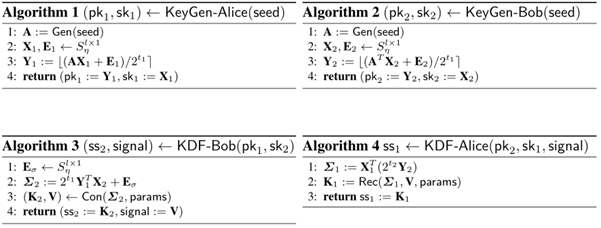
* Alice和Bob在密钥生成的过程中，需要共享一个矩阵。 在调用KeyGen()函数时，通过传递相同的seed参数，来确保两者共享矩阵。

但Alice和Bob在计算各自的共享密钥过程中，分别使用矩阵和的转置矩阵，因此，我们通过两个不同的函数调用(pk1,sk1):=KeyGen\_Alice(seed), (pk2, sk2):=KeyGen\_Bob(seed)来体现它们的区别和相似性。

具体地说，Alice通过调用KeyGen\_Alice(seed)来生成自己的公钥/私钥对(pk1,sk1)，而Bob通过调用KeyGen\_Bob(seed)来生成自己的公钥/私钥对(pk2, sk2)。

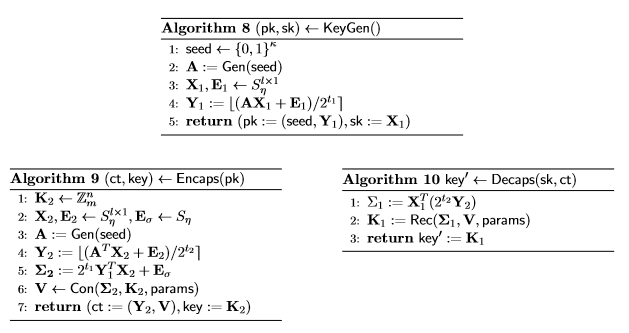
* Alice和Bob需要用两个不同的密钥导出函数，来生成各自的共享密钥。

具体地说，Bob需要使用Alice的公钥pk1和自己的私钥sk2，通过调用KDF-Bob(pk1, sk2)，来生成自己的共享密钥ss2以及发送给Alice、帮助Alice生成共享密钥的启示信息signal；而只有在收到Bob发送的启示信息signal后，Alice才能使用Bob的公钥pk2、自己的私钥sk1，通过调用KDF-Alice(pk2,sk1,signal)，来生成自己的共享密钥ss1。



## 5.2公钥密码体制中基于AKCN-MLWE的KEM算法描述

在公钥密码体制中，基于AKCN-MLWE的KEM描述如下。

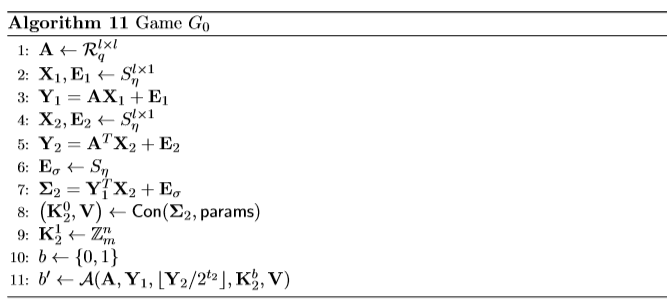


# 基于MLWE的密钥协商和封装分析

## 6.1 安全性分析

**定义6.1**我们称一个基于MLWE以及KC或AKC的密钥协商协议是安全的，若对任意足够大的安全参数和任意PT敌手，在算法11定义的游戏中，绝对值

是可忽略的。

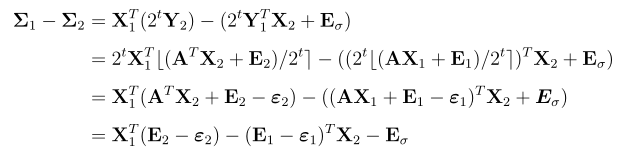


**定理6.1**若是一个正确且安全 KC或AKC方案且，在MLWE假设下，图1和2中的密钥协商协议是安全的。

**证明-定理6.1** 详细的安全证明参考支持文档所列的论文。

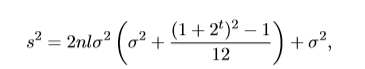
## 6.2 错误率分析

令，记，，则



根据MLWE假设可知，与不可区分，其中服从均匀分布，故非常接近，我们可以把多项式向量中的每个分量看成上的均匀分布。

基于以上分析，对于多项式中的每个系数，我们可以计算它的标准差，即



其中。至此，我们可以通过运行程序脚本得到错误率。

# 具体参数、和优缺点声明

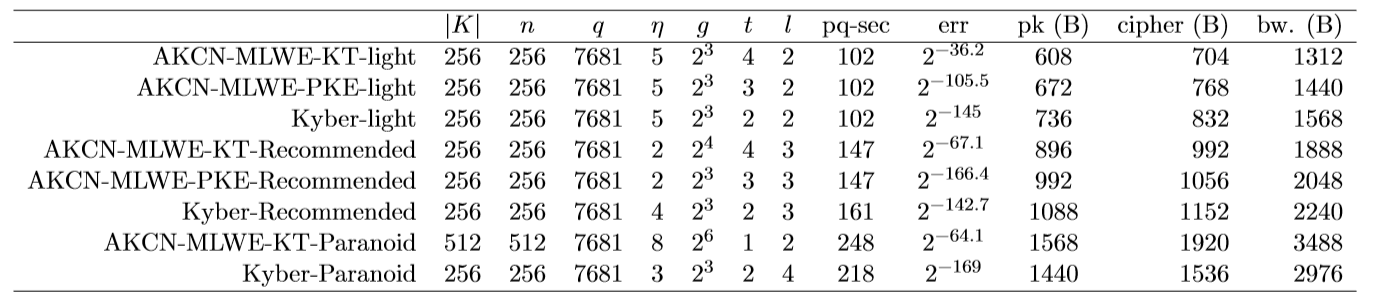
表格7.1给出了AKCN-MLWE的参数和性能。其中，``pq-sec" 指的是时对底层格问题的现有的最好的量子攻击，具体的安全性的值可通过运行文献[BDK+17]中的脚本得到。我们相信在实际中裁剪和最低的个有效比特可以增强安全性 (特别是对一次性的密钥协商和传输而言)。

注意到在安全性证明中我们设置，在实际的实现中却跟Kyber[BDK+17]一样取，理由如下：

* 设置在减少了带宽的同时并没有牺牲实际的安全性 (文献[BDK+17]中给出了详细的解释)。
* 在实际应用中对称性是一个优良的性质。

如果我们强调可证明安全，则在协议实现中令即可。在相同的参数下，若，则错误率减少，带宽 (特别是的大小) 会相应增加。

表7.1 AKCN-MLWE的参数选取以及跟Kyber的对比。KT指一次性密钥传输的参数，PKE是CCA 安全的公钥加密的参数。“|*K***|**”指共识比特的长度，“pq-sec”指量子攻击下的比特安全性，“err”指错误率，“pk”指公钥大小 (字节)，“cipher”指密文大小 (字节)，“bw.”指带宽大小 (字节)。



**与Kyber的对比：**

Kyber [BDK+17] 是基于MLWE和AKC的密钥传输协议，目前进入NIST后量子密码竞赛第二轮。在Kyber中，，，，，其中，是非负整数。Kyber的底层AKC机制是AKCN，一个细微的调整是Kyber中

，

而AKCN 中

。

注意我们的AKCN机制在2016年11月就已经在arXiv公布，并在这之前申请了专利保护。因此，Kyber实际上存在侵权嫌疑。

本提案给出了基于AKCN的密钥传输协议。下面我们简单地对比AKCN-MLWE和Kyber。

* AKCN-MLWE-PKE-light和Kyber-light都达到102比特的后量子安全性，其中AKCN-MLWE-PKE-light（Kyber-light）的带宽是1440 字节（1568 字节），错误率是（）。对于102比特的后量子安全性级别，的错误率已经足够小。AKCN-MLWE-PKE-light（Kyber-light）裁剪了3（2）个最低有效位，故在实际中我们的方案的安全性更高。
* AKCN-MLWE-PKE-Recommended和Kyber-Recommended 都超过了 128比特的后量子安全性，其中 AKCN-MLWE-PKE （Kyber-Recommended）在时有147（161）比特后量子安全性，错误率为（）。AKCN-MLWE-PKE-Recommended（Kyber-Recommended）裁剪了3 （2）个最低有效位，故我们的方案的带宽更低，带宽为2048 字节（2240 字节）。
* AKCN-MLWE-KE-Paranoid和Kyber-Paranoid则不容易比较。前者 AKCN-MLWE-KE-Paranoid是一次性密钥协商的参数，达到了512比特的共识密钥，248比特的后量子安全性，错误率为；Kyber-Paranoid达到了256比特的共识密钥，218 比特的后量子安全性，错误率为。

注意到经过Grover搜索算法（Grover's search algorithm）的平方加速，再加上近期对称密码学量子攻击的进展，256比特的共识密钥理论上只能保证大约128比特的量子安全性。

# 算法实现代码及性能测试

算法实现代码在“参考实现文件夹”下。具体来说我们的软件实现分为两个部分。

1. 针对基于模格的AKCN-MLWE-KT-Recommended密钥封装算法给出了软件实现。
2. 针对基于模格的AKCN-MLWE-PKE-Recommended密钥封装算法给出了软件实现。

另外我们还在 测试实例文件夹下提供了测试报告作为本项目的支持文档。 详细给出了程序的安装说明、测试环境、详细的测试用例、测试结果和基于测试结果的性能分析。

另外我们同时在“参考实现”文件夹下给出了算法在Linux和Windows操作系统下的实现，这两份代码在核心算法的实现上基本相同。但是，实验结果表明，两份基本相同的代码在两个不同的操作系统上的运行效率（无论是从运行时间，还是从时钟周期上）相差较大。简单地说，代码在Linux系统下运行，比在Windows系统下运行快5-14倍左右。我们猜测，这可能与以下因素有关：

1. 编译器的优化。对于我们的代码而言，GCC的优化深度应该比Visual Studio要深。
2. 操作系统的调度问题。以Ubuntu系统为例，它的进程调度算法比Windows系统要更为出色。
3. 文件系统的管理。例如，Demand paging和zswap技术的使用，都可以有效降低I/O次数。

一般情况下基于格密码的算法都是在Linux环境下进行实现，主要是因为Linux环境下有更好的随机库以及更高的计算性能，并且在安装编译上也更加简洁，所以我们的算法最开始只提供Linux下的实现，但是由于本次国家密码算法竞赛要求的测试环境为Windows，所以我们同时提供了Windows版本的实现，但是从测试结果来看，Windows下的性能的确是相对较差，更详细的测试数据以及测试环境，安装步骤，以及接口介绍参见“测试实例”文件夹下的测试报告（针对Linux和Windows实现 我们分别给出了测试报告）。

## 8.1. 基于模格的密钥封装性能分析

下面针对我们软件实现的4个部分，给出性能分析总结，首先分析空间消耗，然后分析时间与时钟周期消耗。 具体程序测试环境、测试详细数据、测试过程、测试用例参见测试报告。

### 8.1.1 空间消耗

下面我们将针对AKCN-MLWE-KT-Recommended、AKCN-MLWE-PKE-Recommended两种算法实现给出空间性能分析。

**AKCN-MLWE-KT-Recommended 密钥封装算法的空间消耗**

在表8.1中我们给出了AKCN-MLWE-KT-Recommended算法主要参数一览。

表8.1AKCN-MLWE-KT-Recommended算法主要参数所耗空间一览表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **名称** | **公钥 pk** | **私钥 sk** | **密文ct** | **共享秘密ss** |
| 长度(byte) | 992 | 288 | 1088 | 32 |

对于具体API接口，针对大赛要求实现的kem\_api，一次密钥封装完整过程包括密钥生成函数（kem\_keygen）， 封装函数（kem\_enc）和解封装函数（kem\_dec）。表8.2给出了这三个函数输入输出参数所需要的空间 并对各个参数进行了简要的介绍。

表8.2 AKCN-MLWE-KT-Recommended算法各个接口参数空间性能

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **函数** | **输入** | **长度(byte)** | **含义** | **输出** | **长度(byte)** | **含义** |
| kem\_keygen |  | | | pk | 992 | 用户公钥 |
| sk | 288 | 用户私钥 |
| kem\_enc | pk | 992 | 接收方公钥 | ct | 1088 | 密文 |
| ss | 32 | 共享秘密 |
| kem\_dec | ct | 1088 | 密文 | ss | 32 | 共享秘密 |
| sk | 288 | 接收方私钥 |

**AKCN-MLWE-PKE-Recommended密钥封装算法的空间消耗**

在表8.3中我们给出了AKCN-MLWE-PKE-Recommended算法主要参数一览。

表8.3 AKCN-MLWE-PKE-Recommended算法主要参数所耗空间一览表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **名称** | **公钥 pk** | **私钥 sk** | **密文ct** | **共享秘密ss** |
| 长度(byte) | 1088 | 288 | 1152 | 32 |

对于具体API接口，针对大赛要求实现的kem\_api，一次密钥封装完整过程包括密钥生成函数（kem\_keygen）， 封装函数（kem\_enc）和解封装函数（kem\_dec）。表8.4给出了这三个函数输入输出参数所需要的空间 并对各个参数进行了简要的介绍。

表8.4AKCN-MLWE-PKE-Recommended算法各个接口参数空间性能

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **函数** | **输入** | **长度(byte)** | **含义** | **输出** | **长度(byte)** | **含义** |
| kem\_keygen |  | | | pk | 1088 | 用户公钥 |
| sk | 288 | 用户私钥 |
| kem\_enc | pk | 1088 | 接收方公钥 | ct | 1152 | 密文 |
| ss | 32 | 共享秘密 |
| kem\_dec | ct | 1152 | 密文 | ss | 32 | 共享秘密 |
| sk | 288 | 接收方私钥 |

### 8.1.2 时间与时钟周期消耗

按照大赛要求的测试环境，我们针对算法实现的两个部分，进行不同组数据的测试，最终得到的可收敛的性能耗时统计。

Windows7 + VS2010平台下的性能统计如表8.5所示。

表8.5 Windows7 + VS2010平台下AKCN密钥封装算法API实现的性能统计表

|  |  |  |  |
| --- | --- | --- | --- |
| **算法名** | **接口名** | **平均耗时（微秒）** | **平均CPU周期消耗(万)** |
| AKCN-MLWE-KT-Recommended | 密钥生成 | 370 | 125 |
| 封装 | 510 | 176 |
| 解封装 | 250 | 86 |
| AKCN-MLWE-PKE-Recommended | 密钥生成 | 367 | 125 |
| 封装 | 520 | 177 |
| 解封装 | 253 | 86 |

Linux平台下的性能统计如表8.6所示。

表8.6 Linux平台下AKCN密钥封装算法API实现的性能统计表

|  |  |  |  |
| --- | --- | --- | --- |
| **算法名** | **接口名** | **平均耗时（微秒）** | **平均CPU周期消耗(万)** |
| AKCN-MLWE-KT-Recommended | 密钥生成 | 65 | 20.30 |
| 封装 | 78 | 24.29 |
| 解封装 | 19 | 5.89 |
| AKCN-MLWE-PKE-Recommended | 密钥生成 | 66 | 20.57 |
| 封装 | 77 | 24.70 |
| 解封装 | 18 | 5.89 |

关于测试的详细数据请参见“测试实例”文件夹下的测试报告。

# 支持文档

Practical Key Establishment from Module Lattice

# 参考文献

[AGKS05] M. Abe，R. Gennaro，K. Kurosawa and V. Shoup. Tag-KEM/DEM: A New Framework for Hybrid Encryption and A New Analysis of Kurosawa-DESmedt KEM. EUROCRYPT 2005: 128-146.

[A17] M. R. Albrecht. On dual lattice attacks against small-secret LWE and parameter choices in HElib and SEAL. EUROCRYPT 2017: 103-129.

[APS15] M. R. Albrecht，R. Player and S. Scott. On the Concrete Hardness of Learning with Errors. Journal of Mathematical Cryptology，Volume 9，Issue 3，pages 169-203，2015.

[ADPS16] E. Alkim，L. Ducas，T. P¨oppelmann，and P. Schwabe. Post-quantum Key Exchange — A New Hope. 25th USENIX Security Symposium (USENIX Security 16)，pages 327–343.

[ADPS16b] E. Alkim，L. Ducas，T. Pppelmann，and P. Schwabe. NewHope without Reconciliation. Cryptology ePrint Archive，Report 2016/1157，2016.

[AJS16] E. Alkim，P. Jakubeit，and P. Schwabe. A New Hope on ARM Cortex-M. Cryptology ePrint Archive，Report 2016/758，2016.

[ACPS09] B. Applebaum，D. Cash，C. Peikert，and A. Sahai. Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems. CRYPTO 2009: 595-618.

[BLL+15] S. Bai，A. Langlois，T. Lepoint，D. Stehl´e，and R. Steinfeld. Improved Security Proofs in Lattice-Based Cryptography: Using the R´enyi Divergence rather than the Statistical Distance. ASIACRYPT 2015: 3-24.

[BPR12] A. Banerjee and C. Peikert and A. Rosen. Pseudorandom Functions and Lattices. EUROCRYPT 2012: 719-737.

[BGL+18] S. Bhattacharya，O. Garcia-Morchon，T. Laarhoven，R. Rietman，M. Saarinen，L. Tolhuizen，and Z. Zhang. Round5: Compact and Fast Post-Quantum Public-Key Encryption. Cryptology ePrint Archive，2018/725.

[BBG+17] H. Baan，S. Bhattacharya，O. Garcia-Morchon，R. Rietman，L. Tolhuizen，J.L. Torre-Arce，and Z. Zhang. Round2: KEM and PKE based on GLWR. Cryptology ePrint Archive，2017/1183.

[BGM+16] A. Bogdanov，S. Guo，D. Masny，S. Richelson，and A. Rosen. On the Hardness of Learning with Rounding over Small Modulus. TCC 2016: 209-224.

19

[BCD+16] J. Bos，C. Costello，L. Ducas，I. Mironov，M. Naehrig，V. Nikolaenko，A. Raghunathan，and D. Stebila. Frodo: Take oﬀ the Ring! Practical，Quantum-Secure Key Exchange from LWE. ACM CCS 2016: 1006-1018.

[BCNS15] J.W. Bos，C. Costello，M. Naehrig，and D. Stebila. Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem. IEEE Symposium on Security and Privacy 2015，553-570.

[BDK+17] J. W. Bos，L. Ducas，E. Kiltz，T. Lepoint，V. Lyubashevsky，J. M. Schanck，P. Schwabe，D. Stehl´e. CRYSTALS-Kyber: a CCA-Secure Module-lattice-based KEM. Available from: https://pq-crystals.org/ Preliminary version appears at Euro S&P 2018.

[CZZ18] R. Chen，Z. Zhang and Z. Zhang. On the Hardness of the Computational Ring-LWR Problem and its Applications. ASIACRYPT 2018. Available from Cryptology ePrint Archive，2018/536.

[CN11] Y. Chen and P.Q. Nguyen. BKZ 2.0: Better Lattice Security Estimates. ASIACRYPT 2011: 1-20.

[CGZ18] L. Cheng，B. Gong，and Y. Zhao. Lattice-Based Signature from Key Consensus. Cryptology ePrint Archive，Report 2018/1180. https://eprint.iacr.org/2018/ 1180

[CKLS16] J.H. Cheon，D. Kim，J. Lee，and Y. Song. Lizard: Cut Oﬀ the Tail! Practical PostQuantum Public-Key Encryption from LWE and LWR. Cryptology ePrint Archive，Report 2016/1126，2016.

[CW90] D. Coppersmith and S. Winograd. Matrix Multiplication via Arithmetic Progressions. Journal of Symbolic Computation，volume 9，issue 3，pages 251-280，1990.

[CDS94] R. Cramer，I. Damgrd and B. Schoenmakers. Proofs of Partial Knowledge and Simpliﬁed Design of Witness Hiding Protocols. CRYPTO 1994: 174187.

[DKRV17] J. D’Anvers，A. Karmakar，S.S. Roy，and F. Vercauteren. SABER: Mod-LWR based KEM. Proposal to NIST PQC Standardization.

[DXL12] J. Ding，X. Xie and X. Lin. A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem. Cryptology ePrint Archive，Report 2012/688，2012.

[DORS08] Y. Dodis，R. Ostrovsky，L. Reyzin，and A. Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. SIAM Journal on Computing，volume 38，issue 1，pages 97-139，2008.

[DD12] L. Ducas and A. Durmus. Ring-LWE in Polynomial Rings. PKC 2012: 34-51.

[DTV15] A. Duc，F. Tram`er，and S. Vaudenay. Better Algorithms for LWE and LWR. EUROCRYPT 2015: 173-202.

[FS86] A. Fiat and A. Shamir. How to Prove Yourself: Practical Solutions to Identiﬁcation and Signature Problems. CRYPTO 1986: 186194.

20

[FO99] E. Fujisaki and T. Okamoto. How to Enhance the Security of Public-Key Encryption at Minimum Cost. IEICE Transactions on Fundamentals of Electronics，Communications and Computer Sciences Volume 83，Issue 1，pages 24-32，1999.

[FO13] E. Fujisaki and T. Okamoto. Secure Integration of Asymmetric and Symmetric Encryption Schemes. Journal of Cryptology，Volume 26，Issue 1，pages 80-101，2013.

[GPV08] C. Gentry，C. Peikert，and V. Vaikuntanathan. Trapdoors for Hard Lattices and New Cryptographic Constructions. ACM STOC 2008: 197-206.

[GS16] S. Gueron and F. Schlieker. Speeding Up R-LWE Post-Quantum Key Exchange. Cryptology ePrint Archive，Report 2016/467，2016.

[KLL15] M. Kaplan，G. Leurent，A. Leverrier and M. Naya-Plasencia. Quantum Diﬀerential and Linear Cryptanalysis. ArXiv Preprint: 1510.05836，2015.

[Kra03] H. Krawczyk. SIGMA: The ‘SIGn-and-MAc’ Approach to Authenticated DiﬃeHellman and Its Use in the IKE Protocols CRYPTO 2003: 400-425.

[KM10] H. Kuwakado and M. Morii. Quantum Distinguisher between the 3-round Feistel Cipher and the Random Permutation. IEEE ISIT 2010: 2682-2685.

[LP10] R. Lindner and C. Peikert. Better Key Sizes (and Attacks) for LWE-Based Encryption. CT-RSA 2011: 319-339. Also available from http://eprint.iacr.org/2010/ 613.

[LS15] A. Langlois and D. Stehl´ e. Worst-case to Average-case Reductions for Module Lattices. Des. Codes Cryptography，75(3): 565-599，2015.

[LPR10] V. Lyubashevsky，C. Peikert，and O. Regev. On Ideal Lattices and Learning with Errors over Rings. EUROCRYPT 2010: 1-23.

[LPR13] V. Lyubashevsky，C. Peikert，and O. Regev. A Toolkit for Ring-LWE Cryptography. EUROCRYPT 2013: 35-54.

[FrodoKEM] Michael Naehrig，ErdemAlkim，Joppe Bos，Leo Ducas，Karen Easterbrook，Brian LaMacchia，Patrick Longa，Ilya Mironov，Valeria Nikolaenko，Christopher Peikert，Ananth Raghunathan，and Douglas Stebila. Supporting documentation: Frodokem. Technical report，National Institute of Standards and Technology，2017. https://csrc.nist.gov/CSRC/media/Projects/ Post-Quantum-Cryptography/Round-1-Submissions.

[NIST] NIST. Post-Quantum Cryptography Standardization. https: //csrc.nist.gov/Projects/Post-Quantum-Cryptography/ Post-Quantum-Cryptography-Standardization

[Pei09] C. Peikert. Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem. STOC 2009: 333-342.

[Pei14] C. Peikert. Lattice Cryptography for the Internet. PQCrypto 2014: 197-219.

21

[Pei16] C. Peikert. A Decade of Lattice Cryptography. In Foundations and Trends in Theoretical Computer Science，Volume 10，Issue 4，pages 283-424，2016.

[PVW08] C. Peikert，V. Vaikuntanathan，and B. Waters. A Framework for Eﬃcient and Composable Oblivious Transfer. CRYPTO 2008: 554-571.

[Pop16] A.V. Poppelen，Cryptographic Decoding of the Leech Lattice. Cryptology ePrint Archive，Report 2016/1050，2016.

[PG13] T. P¨oppelmann and T. Gu¨neysu. Towards Practical Lattice-Based Public-Key Encryption on Reconﬁgurable Hardware. SAC 2013: 68-85.

[Reg09] O. Regev. On Lattices，Learning with Errors，Random Linear Codes，and Cryptography. Journal of the ACM (JACM)，Volume 56，Issue 6，pages 34，2009.

[Res] E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. IETF RFC 8846. https://datatracker.ietf.org/doc/rfc8446/.

[SBG+18] M. Saarinen，S. Bhattacharya，O. Garcia-Morchon，R. Rietman，L. Tolhuizen，and Z. Zhang. Shorter Messages and Faster Post-Quantum Encryption with Round5 on Cortex M. Cryptology ePrint Archive，2018/723.

[SE94] C. P. Schnorr and M. Euchner. Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems. Mathematical Programming，Volume 66，Issue 2，pages 181-199，Springer，1994.

[Sim02] M.K. Simon. Probability Distributions Involving Gaussian Random Variables : A Handbook for Engineers and Scientists. Springer，2012.

[SM16] D. Stebila and M. Mosca. Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project. Cryptology ePrint Archive，Report 2016/1017，2016.

[Str69] V. Strassen. Gaussian Elimination is not Optimal. NumerischeMathematik，Volume 13，Issue 4，pages 354-356，Springer，1969. Cryptology ePrint Archive: Report 2018/309

[ZWXZ18] Z. Zheng，X. Wang，G. Xu and C. Zhao. Error Estimation of Practical Convolution Discrete Gaussian Sampling with Rejection Sampling. Cryptology ePrint Archive: Report 2018/309.

# 原创性声明

本报告所提交的研究工作，除已明确标注和致谢的地方外，所有的观点、文字、图表及数据等均为自己的研究成果。他人研究对本研究工作的启发和贡献均已作了明确的说明和致谢。除文中已经注明引用的内容外，本报告不包含任何其他个人或集体已经发表或撰写过的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

作者签名：

时间：年月日

# 未来工作

本算法提案聚焦基于MLWE的CPA-安全的密钥封装。由于CCA安全的密钥封装和公钥加密可以从CCA-安全的密钥封装基于公开的成熟的技术转换而得到，在本提案中我们没有提供相应的转换。在未来的版本中，我们将增加相应的CCA安全的密钥封装及其实现。另外，我们注意到最新版本的Kyber使用了更小的模数q = 3329和优化的NTT技巧；Kyber的这些技巧也同样可以应用到SKCN-MLWE。我们计划在未来版本中应用这些技巧。

1. 通常基于文献[BDK+17] 给出的中心二项分布：选取，再输出。该分布的标准差是。 [↑](#footnote-ref-1)
2. AKCN和[PG13]的底层调和机制大体上可以看成是不兼容的。 [↑](#footnote-ref-2)