

# 2023 年全国大学生信息安全竞赛

## 作品报告

作品名称: 后量子时代的 PGP

电子邮箱: 1372322593@qq.com

提交日期: 2023.06.13

## **填写说明**

1. 所有参赛项目必须为一个基本完整的设计。作品报告书旨在能够清晰准确地阐述（或图示）该参赛队的参赛项目（或方案）。
2. 作品报告采用 A4 纸撰写。除标题外，所有内容必需为宋体、小四号字、1.5 倍行距。
3. 作品报告中各项目说明文字部分仅供参考，作品报告书撰写完毕后，请删除所有说明文字。（本页不删除）
4. 作品报告模板里已经列的内容仅供参考，作者可以在此基础上增加内容或对文档结构进行微调。
5. 为保证网评的公平、公正，作品报告中应避免出现作者所在学校、院系和指导教师等泄露身份的信息。

# 目录

<b>摘要</b> .....	1
<b>第一章 作品概述</b> .....	2
1.1 背景分析 .....	2
1.1.1 电子邮件安全与 PGP .....	2
1.1.2 量子计算与后量子密码学 .....	4
1.1.3 密钥分离与密钥复用 .....	6
1.2 本作品的工作 .....	7
1.2.1 实现基于格的 IBE .....	7
1.2.2 基于 IBE 构造 ISE .....	9
1.3 应用前景 .....	10
1.4 特色描述 .....	12
<b>第二章 作品设计与实现</b> .....	13
2.1 准备工作 .....	13
2.1.1 记号 .....	13
2.1.2 高斯采样 .....	13
2.1.3 Kullback-Leibler 距离 .....	14
2.1.4 NTRU 格 .....	14
2.1.5 Module-NTRU 格 .....	15
2.2 PQ-PGP 的设计与实现 .....	16
2.2.1 基于 Module-NTRU 格实现 IBE .....	16
2.2.2 基于 IBE 实现 ISE .....	20
<b>第三章 作品测试与分析</b> .....	24
3.1 测试流程 .....	24
3.2 测试环境 .....	24
3.3 效率测试 .....	25
3.3.1 性能测试 .....	25
3.3.2 功能测试 .....	27
<b>第四章 创新性说明</b> .....	35
4.1 首个后量子安全的 PGP .....	35
4.2 加密方案和签名方案的密钥复用 .....	35
4.3 高效的代码实现 .....	35
4.4 友好的用户界面 .....	36
4.5 广阔的应用范围 .....	36

第五章 总结 .....	37
参考文献 .....	38

## 摘要

信息互联时代，以电子邮件传递为代表的网络通信是人们交流的重要手段，其安全问题也受到重视。现如今流行的电子邮件加密软件 PGP（Pretty Good Privacy）可为数据通信提供机密性和认证性，在保障信息安全传输方面拥有极大优势。然而，随着量子计算机的发展，量子计算能力的提高，世界正在向量子时代前进。Shor 算法、Grover 算法等量子算法的提出，使得现有 PGP 采用的 RSA、ELGamal 公钥密码体制不再安全。也就是说，一旦量子计算机被发明，现有 PGP 为数据通信套上的“护甲”将不再坚固。

针对于此，本作品设计并实现了后量子 PGP 系统：PQ-PGP（Post-Quantum Pretty Good Privacy）。该系统基于后量子密码算法，底层在 MNTRU 上实现了基于 GPV 方案的身份基加密系统（Identity-Based Encryption，IBE），经由 Naor 变换和 Fujisaki-Okamoto 变换转换为集成签名加密系统（Integrated Signature and Encryption，ISE），实现了签名组件和密钥组件共用同一对密钥的 PGP，可以在量子互联网时代为电子邮件的安全传输保驾护航。

本作品的 PQ-PGP 具有以下优势：(1) 强安全：底层 IBE 系统基于格密码算法，可以抵抗量子算法的攻击。(2) 低开销：在满足联合安全性的前提下实现了密钥复用，存储密钥的空间开销降低，减少了密钥的管理成本。传统的密钥分离原则要求用户在加密组件和签名组件中使用不同的密钥对。在本系统中，用户只需要一对密钥——底层 IBE 的主密钥——同时用于加密组件和签名组件。在达到加密方案和签名方案的联合安全性要求的前提下，大大减小密钥存储开销、证书开销以及密码代码的占用空间。(3) 高速度：相较于现有 PGP 最为常用的 RSA-4096 方案，本系统的加解密速度和签名速度约提升 8 倍。(4) 易操作：本系统提供了图形化界面，用户可灵活选择功能，实现了友好的用户交互。(5) 应用广：PQ-PGP 除了可以用于电子邮件加密外，还可以应用于加密聊天软件、加密电子支付等需要为数据传输提供机密性和认证性的场景。

因此，在量子计算时代，本作品具有重要意义和实用价值。

**关键字：**格密码；基于身份的加密系统；集成签名加密系统；密钥复用

# 第一章 作品概述

## 1.1 背景分析

### 1.1.1 电子邮件安全与 PGP

2023 年 1 月 13 日，工信部、网信办、发改委、公安部等十六部门联合发布《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》。《意见》聚焦数据安全保护及相关数据资源开发利用需求，在数据安全保障中，以电子邮件为代表的通信安全依然占据了首要地位。而在现有的互联网时代，电子邮件在日常办公中有着不可或缺的地位。据统计，电子邮件市场规模逐年稳步提升（如图1.1、1.2），在个人、企业、政府等用户通讯、传输文件时，电子邮件扮演了重要的信息传递工具的角色，极大的满足了人们对通信的需求，方便了人们的生活。

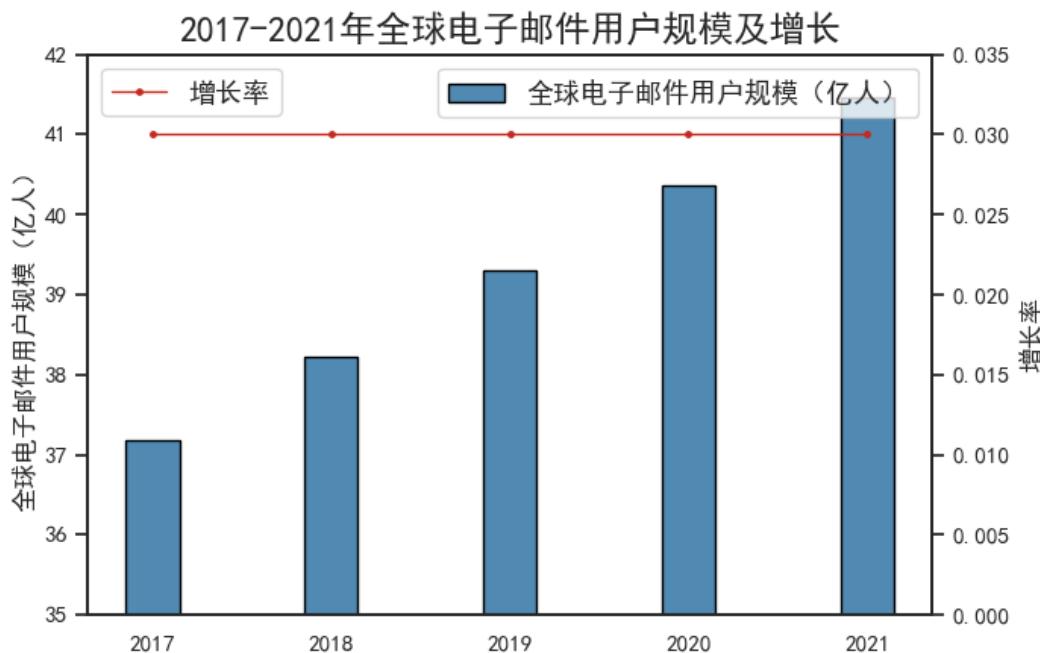


图 1.1 电子邮件市场规模增长

然而与此同时，电子邮件正在成为黑客盗取用户信息，对用户主机进行恶意攻击的突破口。近日，Mimecast 发布《2023 电子邮件安全态势报告》，报告显示电子邮件的使用量呈逐年增长趋势，电子邮件传播造成的安全事件逐年增加、攻击手段日益复杂。根据中国工信部发布的网络安全信息与动态周报（2023.5.1-2023.5.7），境内计算机恶意程序传播次数比上周增长了 3.1%，日攻击频次也持续增加。

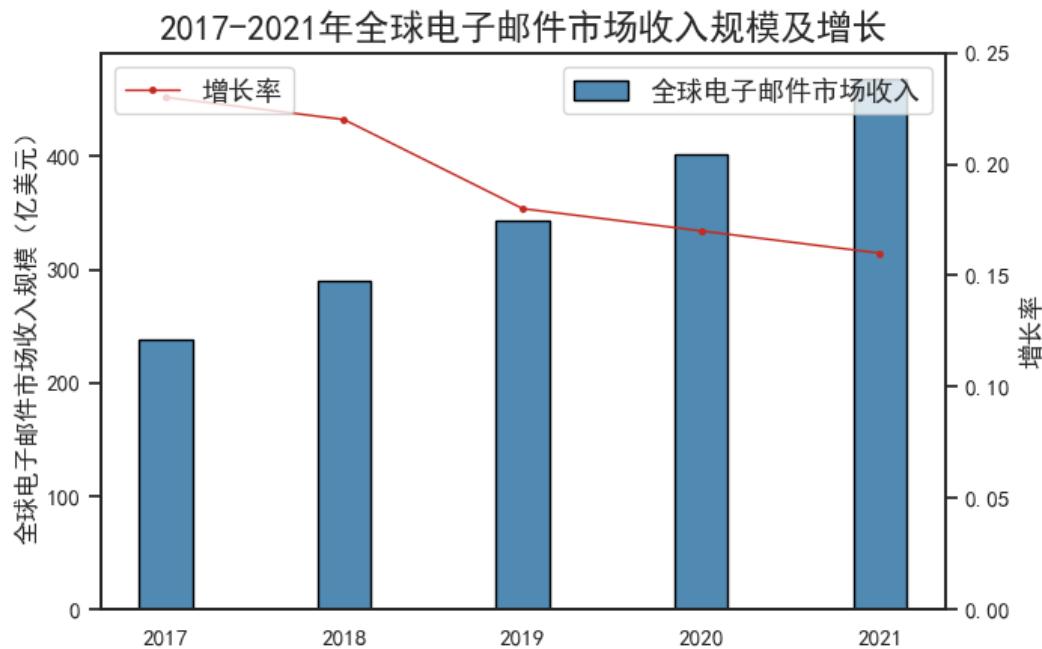


图 1.2 电子邮件市场经济增长

在 SANS 关于电子邮件安全的调查白皮书显示，近 3/4 的网络钓鱼、恶意软件和勒索软件攻击都是通过电子邮件为入口的。诸如 2017 年 9 月 21 日美国得克萨斯州哈里斯县审计署收到了来账单邮件，审计署未经核实邮件地址和发件人便向其转账 88.8 万美元。事后查无此人，实际为钓鱼邮件。2019 年 3 月 11 日起，境外某黑客组织对我国有关部门开展勒索病毒邮件攻击，该勒索病毒版本号为 GANDCRAB V5.2，是 2019 年 2 月升级的勒索病毒版本，运行后将对用户主机硬盘数据全盘加密，并让受害用户通过某种方式支付赎金。如果说这些仅仅是个例，不能代表整个网络邮件环境的话，那么安全情报公司 FireEye 则从大数据统计上给出了一个例子，该公司根据对 2018 年上半年的 5 亿多封电子邮件样本的分析报告指出，在 2018 年上半年的电子邮件流量中，只有不到三分之一的电子邮件流量被认为是“干净的”，并被发送到用户收件箱。由此可见，电子邮件行业在市场规模在稳步增进的同时也隐藏着巨大的隐患，寻找合适的方法来保护电子邮件数据显得尤为重要。

Pretty Good Privacy (PGP) [PGP] 是保障电子邮件安全的最佳解决方案，可以对数据进行加密和数字签名，提供机密性和认证性。使用 PGP 可以较大的提升电子邮件在公开信道上的信息安全。如图1.3[SWR<sup>+</sup>22] 所示，在电子邮件市场规模增长的背景下与人民网络安全意识与日俱增的情况下，使用 PGP 的电子邮件用户越来越多，PGP 的应用也越来越广泛。

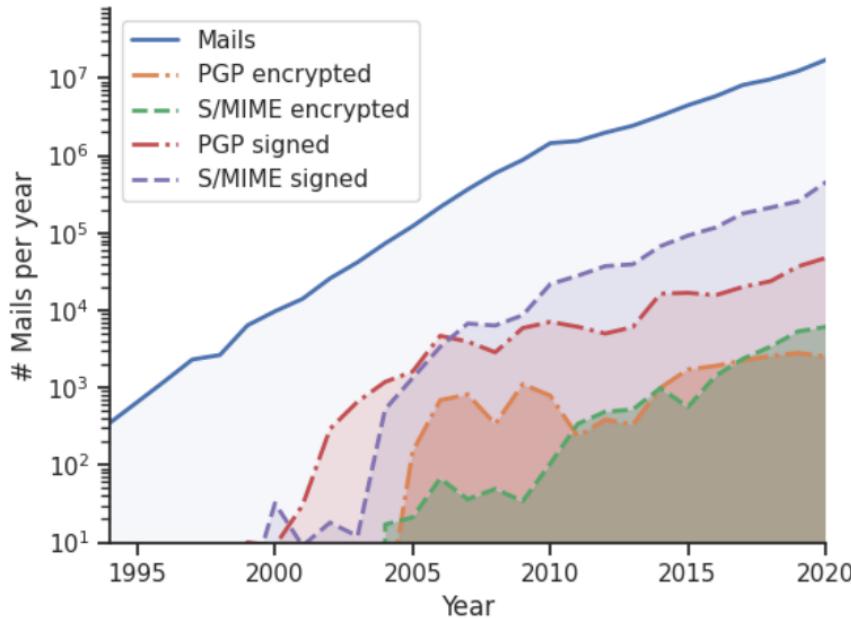


图 1.3 电子邮件与 PGP 使用用户规模 [PGP]

### 1.1.2 量子计算与后量子密码学

自 20 世纪 80 年代初以来，量子计算一直是学术界的热点研究领域。学术界与产业界普遍认为，在未来几十年的时间内，功能完备且可用于各种领域的量子计算机将得以实现。量子计算机可以有效应用于科学研究和其他许多领域，推动人类社会的发展。但是量子计算机的发明实现将带来许多新的问题，其中之一就是数字通信的安全问题。Shor 算法 [LaP21] 与 Grover 算法 [Gro96] 等量子算法的出现，使得循环群上的传统数论假设的不再成立，如大整数分解假设、RSA 假设、离散对数假设及其变体。这意味着在百万比特及加密量子计算机的冲击下，现有的传统公钥密码体制都将被完全破解，这对现有网络协议的安全性产生了极大的威胁。

为了抵御量子计算机带来的隐私安全风险和威胁，许多科学家已经开始研究后量子密码学 (Post Quantum Cryptography, PQC)，致力于创造出能够抵抗传统计算机和量子计算机攻击的加密体制。美国国家标准技术研究所 (National Institute of Standards and Technology, NIST) 早在 2012 年就启动了后量子密码的研究工作，并于 2016 年 2 月启动了全球范围内的后量子密码标准征集。NIST 后量子密码团队负责人 Dustin Moody 在 AsiaCrypt 2017 会议上 [Moo17] 对密码学标准的更新做出了图 1.4 的概括：在量子计算时代，对称密码算法的安全性将被显著降低，但可以通过调整参数来解决；而公钥密码算法将被完全破解，亟需后量子密码算法代替。NIST PQC 标准征集工作的候选草案主要包括以下 4 种数学方法构造的后量子密码算法：

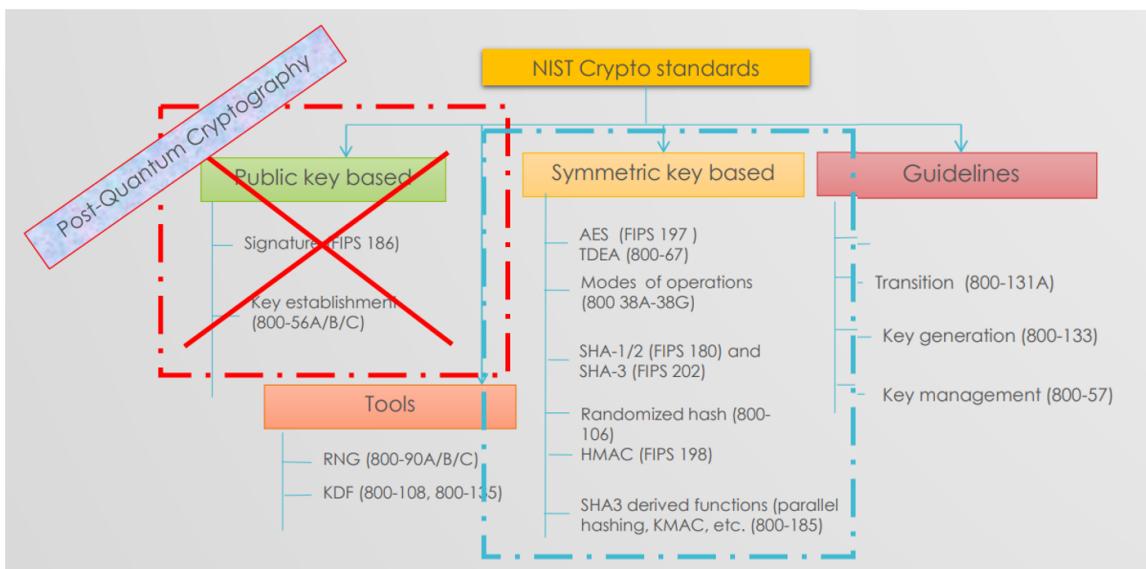


图 1.4 NIST 密码学标准更新概括 [Moo17]

- (1) 格 (Lattice-based);
- (2) 编码 (Code-based);
- (3) 多变量 (Multivariate-based);
- (4) 哈希 (Hash-based);

在提交的 69 个草案中, 有超过三分之一的密码方案都是基于格的密码方案。在经历三轮的严格测试筛选后, NIST 于 2022 年 7 月 5 日公布了首批后量子密码标准 (如图 1.5) 算法: CRYSTALS-KYBER、CRYSTALS-DILITHIUM、FALCON 以及 SPHINCS+ 算法。其中, 前三个密码算法均基于格构造。由此可见, 基于格构造的密码算法是后量子密码学中的研究热点。



图 1.5 NIST 后量子密码学算法

但是，从图1.6[SWR<sup>+</sup>22]可以看出，在现有流通的 PGP 软件中，公钥加密方案依然使用非后量子公钥算法，诸如 RSA 算法、EdDSA 算法等。

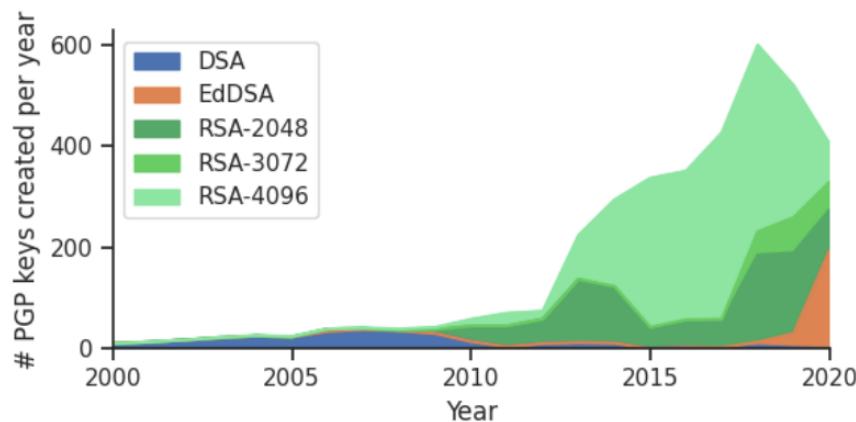


图 1.6 现有 PGP 使用算法统计 [SWR<sup>+</sup>22]

如前文所述，随着量子计算机的逐步发展，上述的公钥密码算法都面临着毁灭性的打击。因此，现有的 PGP 将不再安全。这会对现有的邮件安全造成严重的威胁，尤其在关于国计民生，金融经济领域的通信安全方面更为重要，这关系到国家以及产业体系的健康有序发展。

在目前，还没有一款基于后量子密码算法的 PGP 在流通。如果可以实现抗量子算法攻击的 PGP，就相当于在量子计算时代，为网络数据通信套上了一把安全的锁。这在信息隐私保护，加快安全信息流通，促进经济金融发展等领域都有重要意义。基于此，设计实现后量子的 PGP 是十分必要的。

### 1.1.3 密钥分离与密钥复用

密钥分离是工程实现中的传统原则，它要求在不同的密码学操作中使用不同的密钥对。也就是说，在 PGP 中，每一个用户都需要生成密钥对  $(ek, dk)$  用于公钥加密，生成  $(vk, sk)$  用于数字签名。密钥分离允许人们灵活地选择和组合现成的加密方案和签名方案；并且由于两个密钥对的独立性，联合安全性可以很容易地得到。但是，它有一个明显的缺点：密钥的规模和密钥管理的复杂性增加了一倍。

相比之下，密钥重用原则是指在加密方案和签名方案中使用相同的密钥对，这种系统称为集成签名和加密（Integrated Signature and Encryption, ISE）。正如 Paterson 等人 [PSST11a] 所主张的，采用密钥重用原则有以下优势：(1) 可以减少对于密钥的存储需求；(2) 减少所需的证书数量，进而可以减少证书开销，包括但不限于包括证书的注册、签发、储存、传输、验证等开销 (3) 减少密码代码的占用空间，使开发

工作的代码更加精简。(4) 有助于简化高级协议的设计，使其简洁且安全。



图 1.7 密钥分离原则和密钥复用原则对比

## 1.2 本作品的工作

本作品可以使用以下两种方案来实现后量子安全的 PGP：(1) 采取密钥分离原则：直接用现有的 NIST 后量子密码算法标准代替现有 PGP 中使用的密码算法。(2) 采取密钥复用原则：现有 NIST 后量子密码算法标准中的加密算法 CRYSTALS-KYBER 与签名算法 CRYSTALS-DILITHIUM、FALCON 及 SPHINCS+ 的密钥结构均不同，无法自然地共用同一对密钥。若想实现密码复用原则，需要小心的构造。

为享有密钥复用原则带来的好处，本作品在这里采用第二种方案，设计实现了密钥复用的后量子 PGP：PQ-PGP。本作品采用如图1.8所示的技术路线。主要工作如下：

- (1) 基于 GPV 方案 [GPV08]，在 Module-NTRU (MNTRU) 格上实现了基于身份的加密系统 IBE；
- (2) 基于 PSST 方案 [PSST11b]，由 IBE 实现集成签名加密系统 ISE；
- (3) 基于 QT 开发用户操作友好的后量子 PGP 软件。

接下来，将简要介绍本作品的工作。

### 1.2.1 实现基于格的 IBE

为了实现后量子安全，本作品使用格密码算法作为 PQ-PGP 的底层。在格上实现 IBE 时，本作品以 GPV 方案 [GPV08] 为起点，对比分析了 NTRU 格和 Module-NTRU 格上的 IBE 算法（如图1.9）。

在 2008 年，Gentry 等人在基于格的陷门构造取得重突破，并提出可以在格上构造 IBE[GPV08]。在 [GPV08] 中，陷门生成算法输出矩阵对  $(\mathbf{A}, \mathbf{T}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^{m \times m}$ ，其中  $\mathbf{T}$  是 SIS 方程  $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A} \cdot \mathbf{x} \bmod q$  的陷门。该方案可以得到一对 IBE 的主密钥 ( $mpk = \mathbf{A}, msk = \mathbf{T}$ )，私钥生成中心可以利用  $\mathbf{T}$  为身份信息为  $f_{\mathbf{A}}$  的用户生成用户私钥  $\mathbf{x}$ 。在这里，为确保  $\mathbf{T}$  的保密性， $\mathbf{A}$  的分布需要在统计上接近  $\mathbb{Z}_q^{n \times m}$ ，其中  $m = \Theta(n \log q)$ 。

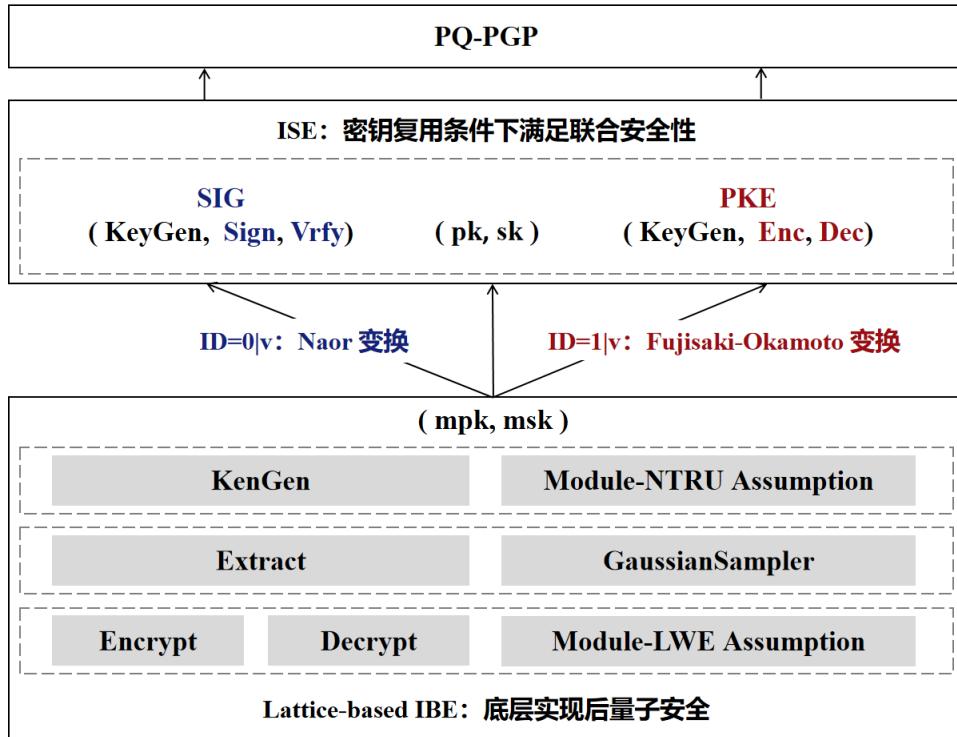


图 1.8 PQ-PGP 技术路线

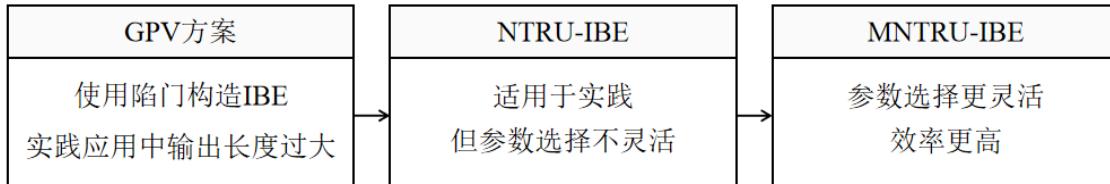


图 1.9 基于格的 IBE 方案对比分析

需要注意的是，GPV 方案中的参数  $m$  较大，使得 IBE 所产生的输出对于实际应用来说太长了。对此，Ducas 等人介绍了一种 GPV 陷门的变体 [DLP14]。该方案利用了 NTRU 格的计算困难性假设，对于多项式环  $\mathcal{R} := \mathbb{Z}[X]/\phi(X)$  (其中首一多项式  $\phi(X) \in \mathbb{Z}[X]$ )，新的陷门生成算法输出一对  $h_{\text{NTRU}} \in \mathcal{R}_q$ ,  $\mathbf{T}_{\text{NTRU}} = \mathcal{R}^{2 \times 2}$ ，在  $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$  上满足  $(1, h_{\text{NTRU}}) \cdot \mathbf{T}_{\text{NTRU}} = 0 \bmod q$ 。由于该方案的陷门生成算法基于多项式环，只需要  $m = 2n$  (而非之前的  $m = \Theta(n \log q)$ )，因此相对于 GPV 的陷门生成更加高效。

尽管在 NTRU 格构造的 IBE 方案已经足够适用于实践，但是在参数的选取上仍然可以改进。出于安全性和高效性的需求， $\phi(X)$  最广泛的选择是  $X^n + 1$ ，其中  $n = 2^k, k \in \mathbb{Z}$ 。当希望获得更高的安全级别，由于  $n$  的特殊形式 (2 的幂次)，参数的选择欠缺灵活性。例如，在 [DLP14] 中分析道当环的维数  $n = 512$  时可以提供 80bits

的安全性，当  $n = 1024$  时可以提供 192bits 的安全性。在这种情况下，当人们希望得到中间级别的安全等级时，比如 128bits，就只能选择  $n = 1024$  的环，从而导致巨大的效率损失。

于是，类似于 Ring-LWE 的广泛概念 Module-LWE[LS15], [CKKS19] 提出了 NTRU 格的广泛概念：Module-NTRU (MNTRU) 格。将  $\mathcal{R}^2$  中的 NTRU 格推广到高维  $\mathcal{R}^d$  中的 MNTRU 格，能够使得 NTRU 陷门的维数选择更加灵活，同时密钥规模更小、比特安全性更强、效率更高（如表1.1所示）。

**表 1.1 NTRU 格与 MNTRU 格的 IBE 实例对比**

	NTRU 格	MNTRU 格
$(d, n, \log_2 q)$	(2,1024,26)	(3,512,19)
Bit-security	87	147
Ciphertext size (bytes)	3328	2432
Master $pk$ size (bytes)	3328	2432
User $sk$ size (bytes)	2048	1152

经过综合比对后，本作品选择在效率更高的 MNTRU 上实现 IBE 作为底层设计。密钥生成算法 **KeyGen** 中，基于 Module-NTRU 假设，以 MNTRU 实例作为主公钥，接近正交的短格基  $\mathbf{T}_{\text{MNTRU}}$  作为主私钥；用户密钥提取算法 **Extract** 中，在  $\mathbf{T}_{\text{MNTRU}}$  上使用随机化最近平面算法，运行近似高斯采样器得到用户私钥；加密算法 **Encrypt** 和解密算法 **Decrypt** 则基于 Module-LWE 假设实现。具体实现细节将在2.2节中阐释。

MNTRU 格上的 IBE 可以在 512 维的多项上实现 142bits 安全，且相较于基于 NTRU 格 87bits 安全的构造相比，效率也有明显提升：密钥生成效率约提升 1.7 倍，加密和解密约提升 3 倍；与此同时，密钥规模也更小：主公钥规模由 3328bits 缩减为 2432bits，用户私钥规模由 2048bits 缩减为 1152bits。

### 1.2.2 基于 IBE 构造 ISE

为实现密钥复用，本作品将 Paterson 等人提出的基于 IBE 构造 ISE 的方案 [PSST11a] 应用到 MNTRU-IBE[CKKS19] 上（如图1.10），得到支持密钥复用的 PQ-PGP 系统。

本作品对 IBE 中的用户身份空间进行前缀划分，身份 ID 前缀为 0，则通过 Naor 变换，转换为签名组件；身份 ID 前缀为 1，则通过 FO 变换，转换为加密组件。对于

每一个用户，都分别运行 IBE 的密钥生成算法，生成主密钥，用于加密组件和签名组件，实现了密钥复用，同时仍然满足联合安全性。

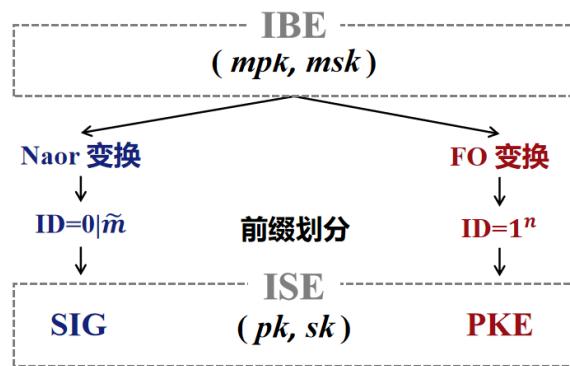


图 1.10 由 IBE 构造 ISE

### 1.3 应用前景

PQ-PGP 有如下的应用场景：

#### 1. 加密电子邮件

本作品的 PQ-PGP 可以用于邮件的加密系统（如图1.11）。由于本作品的后端有极其便捷的接口，可以方便的嵌入到各类前端之中。可以在各大网络邮箱应用，诸如网易邮箱，QQ 邮箱等邮箱之中内嵌。这在量子计算机威胁的不安全信道下有着极其重要的作用，可以在量子信息时代为数据通信提供机密性和认证性。



图 1.11 PQ-PGP 在电子邮件中的应用

#### 2. 加密聊天软件

信息时代人们更加注重数据隐私，全球流行的聊天软件相继启用了端到端加密功能：如 Whatsapp、Signal、Viber 等。用户可以通过加密聊天软件安全私密的收发消息，跨越距离的阻碍，放心地畅所欲言。只有用户本身和与之交流的用户可以读取消息内容，除此之外，其他任何人（包括软件）都无法得知。但现有端到端加密中部署的密码算法同样有着无法抵抗量子算法攻击的缺点，因此可以使用 PQ-PGP 替换其中

的加密算法和签名算法，在量子计算时代为通信内容提供机密性和认证性，让用户隐私有更好的安全保障。



图 1.12 PQ-PGP 在聊天软件中的应用

### 3. 加密电子支付

现如今，电子支付已经成为了人民日常生活的重要组成部分，大大减少了民众出门现金遗失的风险与大规模携带现金的不便，极大方便了人民的生活。在电子支付系统中，网上支付平台、卖家、买家和银行之间的通信需要机密性和认证性。将 PQ-PGP 的加密算法和签名算法嵌入网络支付协议中（如图1.13），可以在金融经济的财产隐私安全上发挥极其重要的作用。

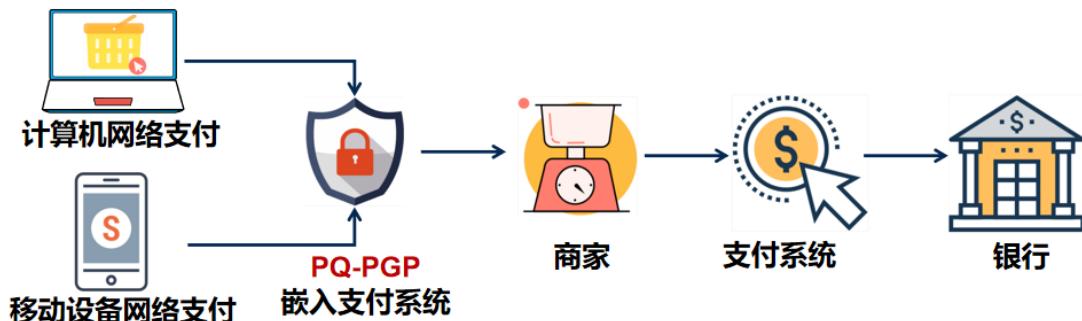


图 1.13 PQ-PGP 在电子支付中的应用模型

总之，本作品的 PQ-PGP 可以适用于一切需要机密性和认证性的应用场景，在量子信息时代具有极强的可用性与拓展性。特别地，采用密钥复用技术下的联合安全性使得密钥存储空间开销大大降低，可以将之用于存储空间较为宝贵的移动通信或支付终端中。在未来量子信息时代的通信场景下具有重要的意义。



图 1.14 PQ-PGP 应用前景分析

## 1.4 特色描述

本作品的 PQ-PGP 平台特色如下：

**1. 强安全：**底层 IBE 在格上实现。格密码算法作为目前后量子领域最受瞩目的算法，其安全性依赖于求解格中问题的困难性，目前尚不能被量子算法破解，达到了抗量子计算攻击的安全性。同时，本作品使用 ISE，在密钥复用前提下达到了加密与签名的联合安全。此外，本作品在底层实现了便捷式接口，可以根据密码学原语的更新迭代实现迅速版本更新，安全性有着与时俱进的保证。

**2. 高速度：**格密码算法主要由矩阵的线性运算组成，算法简单且高度并行。与基于传统数论问题的密码算法构造相比，基于格的算法有着明显提升的计算速度、更高的安全强度，在安全性、公私钥尺寸、计算速度上达到了更好的平衡。本作品基于格密码算法实现的的 PQ-PGP 系统与现有的 PGP 相比，加解密速度和签名速度约提升 8 倍（与现有 PGP 最为常用的 RSA-4096 算法相比）。

**3. 低开销：**加密组件和签名组件密钥复用。密钥的存储需求大大减小；所需的证书数量减少，进而减少了证书开销（包括但不限于包括证书的注册、签发、储存、传输、验证等开销）；开发工作中密码代码的占用空间缩小。

**4. 易操作：**本作品基于 QT 设计了 PQ-PGP 软件的图形 UI 界面屏蔽了后端繁琐的技术细节与底层复杂的安装环境，使用户可以一键式操作，设计相对简单。在这里，本作品提供了三种不同的模式（加密，签名，一次性同时加密签名），使得用户可以灵活选择不同模式进行信息处理，实用度高，易用性强。

**5. 多应用：**本作品的 PQ-PGP 适用于一切需要机密性与认证性的通信场景，在量子信息时代有着广泛的应用。诸如部署在聊天软件，提供端到端加密功能，为用户隐私提供更好的安全保障；以及部署在电子支付系统中，在金融经济的财产隐私安全上发挥重要作用。

## 第二章 作品设计与实现

### 2.1 准备工作

#### 2.1.1 记号

**环**  $\mathbb{Z}[X]/(X^N + 1)$ 。记环  $\mathcal{R} := \mathbb{Z}[X]/(X^n + 1)$ , 并定义  $\mathcal{R}_q := \mathbb{Z}_q[X]/(X^n + 1)$ 。  
 $f := \sum_{i=0}^{n-1} f_i X^i, g := \sum_{i=0}^{n-1} g_i X^i$  是  $\mathcal{R}_q$  上的多项式,  $f_i, g_i \in \mathbb{Z}_q, 0 \leq i \leq n - 1$ 。

$-fg$  表示  $\mathcal{R}_q$  上的多项式相乘。

$-(f)$  表示  $f$  的系数向量,  $f \in \mathcal{R}$ 。

$\|f\|$  表示对于向量  $\mathbf{f} = (f_1, \dots, f_d) \in \mathcal{R}[X]/(X^n + 1)^d$  的欧式距离。

**定义 1 (反循环矩阵)** . 对于  $f = \sum_{i=0}^{n-1} f_i X^i \in \mathcal{R}$ , 定义  $n$  维反循环矩阵如下:

$$\mathcal{A}_n(f) = \begin{pmatrix} f_0 & f_1 & f_2 & \ddots & f_{n-1} \\ -f_{n-1} & f_0 & f_1 & \ddots & f_{n-2} \\ \ddots & \ddots & \ddots & \ddots & \ddots \\ -f_1 & -f_2 & \ddots & \ddots & f_0 \end{pmatrix} = \begin{pmatrix} (f) \\ (x * f) \\ \vdots \\ (x^{n-1} * f) \end{pmatrix}$$

在下文中有时会省略下标  $n$ , 简化写为  $\mathcal{A}(f)$ 。反循环矩阵有如下性质: 对于  $f, g \in \mathcal{R}$ ,  $\mathcal{A}_n(f) + \mathcal{A}_n(g) = \mathcal{A}_n(f + g)$ ,  $\mathcal{A}_n(f) \times \mathcal{A}_n(g) = \mathcal{A}_n(fg)$ 。

**定义 2 (Gram-Schmidt 范数)** . 设  $\mathbf{B} = (\mathbf{b}_i)_{(i \in I)}$  是一个有限基,  $\mathbf{B}^* = (\mathbf{b}_i^*)_{i \in I}$  是它的 Gram-Schmidt 正交化。 $\mathbf{B}$  的 Gram-Schmidt 范数为

$$\|\mathbf{B}^*\| = \max_{i \in I} \|\mathbf{b}_i^*\|$$

#### 2.1.2 高斯采样

**定义 3 (离散高斯分布)** .  $n$  维高斯函数  $\rho_{\sigma, c} : \mathbb{R}^n \rightarrow (0, 1]$  定义如下:

$$\rho_{\sigma, c}(x) \triangleq \exp\left(-\frac{\|x - c\|^2}{2\sigma^2}\right).$$

对于任意格  $\Lambda \subset \mathbb{R}^n$ ,  $\rho_{\sigma, c}(\Lambda) \triangleq \sum_{x \in \Lambda} \rho_{\sigma, c}(x)$ , 在这里将  $\rho_{\sigma, c}(x)$  简记作  $\rho_{\sigma, c}(\Lambda)$ , 并定义  $\mathcal{D}_{\Lambda, \sigma, c}$  为离散高斯分布上的概率重量函数。

**定义 4 (平滑参数 [MR07])** . 平滑参数  $\eta_\varepsilon(\Lambda)$  是使得  $\rho_{1/s, 0}(\Lambda^* \setminus 0) \leq \varepsilon$  成立的最小的的  $s$ , 其中  $\Lambda^*$  为格  $\Lambda$  的对偶格。同时也定义了一个多缩放版本  $\eta_\varepsilon(\Lambda) = \frac{1}{\sqrt{2\pi}} \eta_\varepsilon(\Lambda)$ 。

**高斯采样器**。[GPV08] 提出了一种近似采样离散高斯分布的算法, 在这里将用于 MNTRU 格上的 IBE。算法的细节将在第三章中给出, 这里先简单地定义了语法:

对于格  $L$  的基  $\mathbf{B}$ , 表示 [GPV08] 中近似采样  $\mathcal{D}_{\Lambda, \sigma, c}$  的算法为:

$$\text{GaussianSampler}(\mathbf{B}, \sigma, c).$$

### 2.1.3 Kullback-Leibler 距离

本作品将使用 Kullback-Leibler 距离（或 KL 散度）来测量两个分布的距离。

**定义 5 (Kullback-Leibler 距离).**  $P$  和  $Q$  是在同一个可计数集合  $\Omega$  上的两个分布,  $S \subset \Omega$  是  $P$  的支撑集。 $Q$  和  $P$  的 Kullback-Leibler 距离  $D_{KL}$  定义如下:

$$D_{KL}(P\|Q) = \sum_{i \in S} \ln \left( \frac{P(i)}{Q(i)} \right) P(i).$$

特别的, 对于任意的  $x > 0$ ,  $\ln(x/0) = +\infty$ 。

我们知道, 当两个分布  $P$  和  $Q$  的 KL 距离很小时, 即使将  $P$  的随机谕言机替换为  $Q$  的, 在  $P$  上分任何搜索问题难度都保持不变。

**引理 1 ([PDG14] 中的引理 1).** 设  $\mathcal{A}^P$  是在分布  $P$  上采样的算法, 最多可以询问随机谕言机  $q$  次, 并返回 1bits。设  $\mathcal{A} \geq 0$ , 分布  $Q$  满足  $D_{KL}(P||Q) \leq \varepsilon$ 。设  $x$ (或  $y$ ) 为  $\mathcal{A}^P$ (或  $\mathcal{A}^Q$ ) 输出 1 的概率。那么,

$$|x - y| \leq \sqrt{\frac{q\varepsilon}{2}}.$$

对于理想离散高斯分布和高斯采样器的 KL 散度, 有以下事实:

**定理 1 ([DLP14] 中的定理 2).** 对于任意的  $\varepsilon \in (0, 1/4n)$ , 如果  $\sigma \geq \eta'_\varepsilon \|\mathbf{B}^*\|$ , 那么

$$D_{KL}(\mathcal{D}_{\Lambda(\mathbf{B}), \sigma, c} \| \text{GaussianSampler}(\mathbf{B}, \sigma, \Gamma)) \leq 2 \left( 1 - \left( \frac{1 + \varepsilon}{1 - \varepsilon} \right)^n \right)^2 \approx 8n^2\varepsilon^2$$

### 2.1.4 NTRU 格

**定义 6(NTRU 格).** 设  $n$  为 2 的幂次形式的整数,  $q$  是一个正整数。对于  $f, g \in \mathcal{R}$ , 设  $h = g/f \pmod q$ 。由  $h, q$  定义的 NTRU 格  $\Lambda_{\text{NTRU}}$  为

$$\Lambda_{\text{NTRU}} = \{(u, v) \in \mathcal{R}^2 : u + vh = 0 \pmod q\}.$$

根据定义,  $\Lambda_{\text{NTRU}}$  能由  $\mathbf{Z}^{2n}$  上的满秩格  $\mathbf{A}_{\text{NTRU}} = \begin{pmatrix} -\mathcal{A}_n(h) & qI_n \\ I_n & O_n \end{pmatrix}$  的列生成。

一些 NTRU 格密码系统的安全性基于 NTRU 问题的困难性假设, 该假设指出, 如果  $f, g \in \mathcal{R}_q$  是随机的小系数多项式, 它们的商  $g/f$  与  $\mathcal{R}_q$  中的随机多项式难以区分。

有趣的是，在 NTRU 格中，只要知道  $f, g$ ，就可以通过计算满足等式  $gF - fG = q$  的  $F, G \in \mathcal{R}$ ，可以找到  $\Lambda_{\text{NTRU}}$  的一组短格基 [HHGP<sup>+</sup>03]：

$$\mathbf{T}_{\text{NTRU}} := \begin{pmatrix} \mathcal{A}_n(g) & \mathcal{A}_n(G) \\ -\mathcal{A}_n(f) & -\mathcal{A}_n(F) \end{pmatrix}$$

### 2.1.5 Module-NTRU 格

Module-NTRU (MNTRU) 是由 [CKKS19] 提出的。类似于 Ring-LWE 到 Module-LWE 的推广，MNTRU 格是  $d \geq 2$  时 NTRU 格的广泛概念 (NTRU 格为  $d = 2$  时的情况)。

**定义 7 (MNTRU 格)** . 给定  $\mathcal{R}_q$  上的满秩随机矩阵

$$\mathbf{S}_{\text{MNTRU}} = (\mathbf{f}_1 \quad \mathbf{f}_2 \quad \dots \quad \mathbf{f}_{d-1}) = \begin{pmatrix} f_{1,1} & f_{2,1} & \dots & f_{1,d-1} \\ f_{2,1} & f_{2,2} & \dots & f_{2,d-1} \\ \dots & \dots & \ddots & \dots \\ f_{d,1} & f_{d,2} & \dots & f_{d,d-1} \end{pmatrix} \in \mathcal{R}^{d \times (d-1)},$$

其中  $f_{i,j} (1 \leq i \leq d, 1 \leq j \leq d-1)$  为小系数多项式，且给定短向量  $\mathbf{h}_{\text{MNTRU}} = (h_1, \dots, h_d) \in \mathcal{R}^{d-1}$ ，满足  $(1, \mathbf{h}_{\text{MNTRU}}) \cdot \mathbf{S}_{\text{MNTRU}} \equiv 0 \pmod{q}$ 。 $dn$  维的 MNTRU 格定义如下：

$$\Lambda_{\text{MNTRU},d} := \left\{ (u_0, \dots, u_{d-1}) \in \mathcal{R}^d : u_0 + \sum_{i=1}^d u_i h_i = 0 \pmod{q} \right\},$$

其基为

$$\mathbf{A}_{\text{MNTRU}} := \begin{pmatrix} -\mathcal{A}(h_1) & -\mathcal{A}(h_2) & \dots & \mathcal{A}(h_{d-1}) & qI_n \\ I_n & O_n & \dots & O_n & O_n \\ O_n & I_n & \dots & O_n & O_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ O_n & O_n & \dots & I_n & O_n \end{pmatrix}.$$

这里的  $\mathbf{h}_{\text{MNTRU}}$  可以由以下方式生成：首先，定义  $\mathbf{S}_i$  为去掉  $\mathbf{S}_{\text{MNTRU}}$  第  $i$  行的  $(d-1) \times (d-1)$  维的矩阵，并定义  $\det_i = (-1)^{i-1} \cdot \det(\mathbf{S}_i)$ ，向量  $\mathbf{det} = (\det_i)_{1 \leq i \leq d}^t$ ，在  $\mathcal{R}$  上满足  $\mathbf{det} \cdot \mathbf{S} = 0$  [CKKS19]，从而可以得到短向量  $\mathbf{h}_{\text{MNTRU}} = \det_1^{-1}(\det_2, \dots, \det_d)$ 。通过该方法生成的  $\mathbf{h}_{\text{MNTRU}}$  可以满足  $(1, \mathbf{h}_{\text{MNTRU}}) \cdot \mathbf{S}_{\text{MNTRU}} \equiv 0 \pmod{q}$ 。

基于 MNTRU 格的密码方案的安全性基于 MNTRU 假设 [CKKS19]，该假设指出， $\mathbf{h}_{\text{MNTRU}} = \det_1^{-1}(\det_2, \dots, \det_d) \in \mathcal{R}^{d-1}$  与  $\mathcal{R}^{d-1}$  中的一个均匀随机变量不可区分。

在生成 MNTRU 陷门时，考虑 MNTRU 方程：给定  $\mathbf{S} \in \mathcal{R}^{d \times (d-1)}$ ，找到多项式  $F_1, \dots, F_d$ ，使得

$$\sum_{i=1}^d \det_i \cdot F_i = q$$

这可以通过推广 [HHGP<sup>+</sup>03] 中的方法实现。对于 MNTRU 方程的解向量  $\mathbf{F} = (F_1, \dots, F_d)$ ，将陷门  $\mathbf{T}_{\text{MNTRU}} \in \mathbb{Z}^{dn \times dn}$  设为  $\mathcal{A}_n(\mathbf{S}_{\text{MNTRU}})$  和  $\mathcal{A}_n(\mathbf{F})$  的级联，即

$$\mathbf{T}_{\text{MNTRU}} := (\mathcal{A}_n(\mathbf{S}_{\text{MNTRU}}) \parallel \mathcal{A}_n(\mathbf{F})).$$

## 2.2 PQ-PGP 的设计与实现

本作品首先基于 GPV 方案在 MNTRU 格上构造 IBE，然后通过 Naor 变换和 FO 变换得到 ISE，从而实现 PQ-PGP。

### 2.2.1 基于 Module-NTRU 格实现 IBE

首先回顾一下 IBE 的概念。一个基于身份的加密 (IBE) 包含以下多项式时间算法：

- **Setup(1)**: 输入安全参数，输出公共参数  $pp$ ，身份空间为  $I$ 。
- **KeyGen( $pp$ )**: 输入公共参数  $pp$ ，输出主密钥  $(mpk, msk)$ 。
- **Extract( $msk, id$ )**: 输入主私钥  $mk$  和身份  $id \in I$ ，输出用户私钥  $sk_{id}$ 。
- **Encrypt( $mpk, id, M$ )**: 输入主公钥  $mpk$ ，身份  $id \in I$ ，消息  $M$ ，输出密文  $C$ 。
- **Decrypt( $sk_{id}, C$ )**: 输入用户私钥  $sk_{id}$ ，密文  $C$ ，输出明文  $M$ 。

基于 GPV 方案的 MNTRU-IBE 流程如图2.1所示。

#### (1) 主密钥生成

首先从主密钥生成算法 **KeyGen** 开始。该算法生成 MNTRU 实例  $\mathbf{h} = (h_1, \dots, h_{d-1}) \in \mathcal{R}^{d \times (d-1)}$  作为主公钥，MNTRU 陷门矩阵  $\mathbf{T}_{\text{MNTRU}}$  作为主私钥。

对于 GPV 框架中的 IBE 方案，用提取用户私钥涉及到在  $\Lambda(\mathbf{T}_{\text{MNTRU}})$  上的离散高斯采样。众所周知，离散高斯采样器样本的大小与  $\|\mathbf{T}_{\text{MNTRU}}^*\|$  成比例，使得  $\mathbf{T}_{\text{MNTRU}}$  的 Gram-Schmidt 范数尽可能的小是非常重要的。[CKKS19] 的 3.2 节中指出，对于 MNTRU 陷门  $\mathbf{T}_{\text{MNTRU}} = [\mathbf{t}_1, \dots, \mathbf{t}_{dn}]$ ，有

$$\|\mathbf{T}_{\text{MNTRU}}^*\| = \max \left\{ \|\mathbf{t}_1^*\|, \|\mathbf{t}_{n+1}^*\|, \dots, \|\mathbf{t}_{(d-1)n+1}^*\| \right\},$$

因此，对于 MNTRU 格，只需要计算  $d$  个 Gram-Schmidt 范数就可以确定  $\|\mathbf{T}_{\text{MNTRU}}^*\|$ 。其中前  $d-1$  个范数取决于  $\mathbf{f}_i \in \mathcal{R}^d$  的选择，在选取  $\mathbf{S}$  时，首先根据等式(3.3)选择前

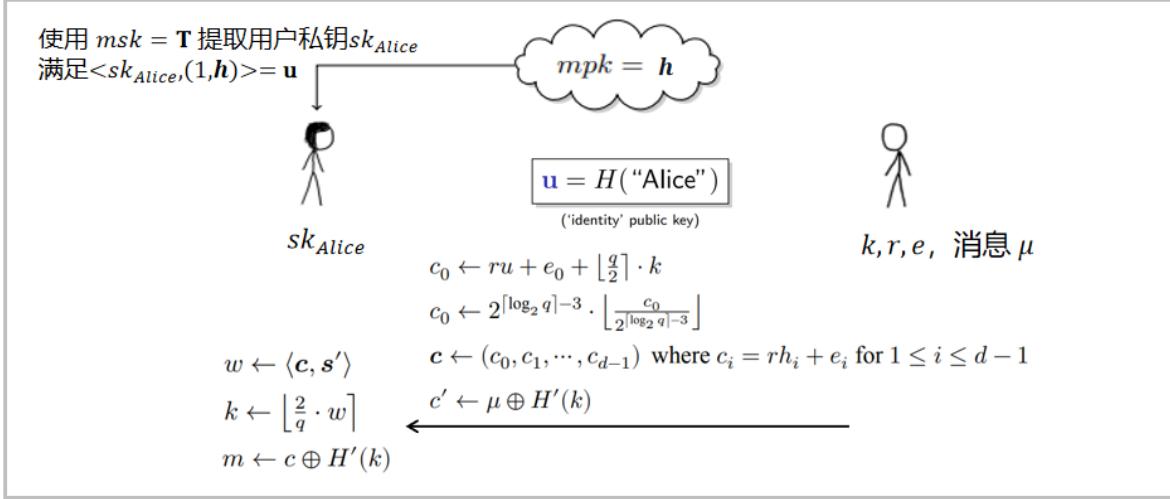


图 2.1 MNTRU 格上的 IBE

$d - 2$  个  $f_{i+1} \in \mathcal{R}^d, 1 \leq i \leq d - 2$ 。

$$\|\mathbf{t}_{in+1}\| = \sqrt{\frac{d}{d-i}} \cdot \|\mathbf{t}_1\|. \quad (2.1)$$

我们知道  $\mathbf{t}_{(i-1)n+1}^*$  是  $\mathbf{t}_{in+1}$  (维度为  $dn$ ) 在  $(d-i)n$  子空间上的投影，因此  $\mathbf{f}_i$  的随机选择意味着

$$\|\mathbf{t}_{(i-1)n+1}^*\| = \sqrt{\frac{d-i+1}{d}} \cdot \|\mathbf{t}_{(i-1)n+1}\|.$$

[CKKS19] 通过实验说明，这样选择的  $f_i$  可以满足等式

$$\|\mathbf{t}_1^*\| = \|\mathbf{t}_{n+1}^*\| = \dots = \|\mathbf{t}_{in+1}^*\|.$$

最后一个范数  $\|\mathbf{t}_{(d-1)n+1}^*\|$  取决于  $\mathbf{S} = [\mathbf{f}_1, \dots, \mathbf{f}_{d-1}]$  的选取，[CKKS19] 指出， $\mathbf{t}_1$  取最佳选择可以表示为  $c_d \cdot q^{1/d}$ ， $c_d$  为由  $d$  决定的常数字，这表明， $\mathbf{T}_{MNTRU}$  的 Gram-Schmidt 范数满足下式

$$\|\mathbf{T}_{MNTRU}^*\| \leq c_d \cdot q^{1/d}.$$

主密钥生成算法的具体步骤由给出算法 1 给出。

**Algorithm 1: KeyGen [CKKS19]**


---

```

input :  $n, q, d$ 
output:  $mpk = \mathbf{h} \in \mathcal{R}_q^{d-1}, msk = \mathbf{T}_{\text{MNTRU}} \in \mathbb{Z}^{dn \times dn}$ 

1 for  $i = q$  to  $d - 1$  do
2    $\sigma_i \leftarrow \sqrt{\frac{d}{d-i+1}} c_d \cdot q^{1/d} / \sqrt{dN}$ 
3    $\mathbf{f}_i \leftarrow (f_{1,i}, \dots, f_{d,i})$  //  $f_{j,i} \in \mathcal{R}$  的系数采样自  $\mathcal{D}_{\mathbf{Z}, \sigma_i}$ 
4 end
5  $\mathbf{S} \leftarrow [\mathbf{f}_1, \dots, \mathbf{f}_{d-1}]$ 
6  $\det \leftarrow (\det_1, \dots, \det_d)$ , 其中  $\det_i = (-1)^{i-1} \cdot \det(\mathbf{S}_i)$ 
7  $\mathbf{h} \leftarrow \det^{-1} \cdot (\det_2, \dots, \det_d) \in \mathcal{R}_q^{d-1}$ 
8 寻找 MNTRU 方程  $\sum_{i=1}^d \det_i \cdot F_i = q$  的解  $\mathbf{F} = (F_1, \dots, F_d) \in \mathcal{R}^d$ 
9  $\mathbf{T} \leftarrow [\mathcal{A}(\mathbf{S}) \| \mathcal{A}(\mathbf{F})]$ 
10 return  $mpk = \mathbf{h}, msk = \mathbf{T}$ 

```

---

**(2) 用户私钥提取**

提取用户  $id$  的用户私钥  $sk_{id}$ , 主要任务是抽样短  $s \in \mathcal{R}^d$  满足

$$\langle s, (1, \mathbf{h}) \rangle = H(id) \mod q$$

其中  $H : \{0, 1\}^* \rightarrow \mathcal{R}_q$  是一种被建模为随机预言机的哈希函数。本作品使用主私钥  $\mathbf{T}_{\text{MNTRU}}$  运行 **GaussianSampler**, 通过在  $\Lambda_{\text{MNTRU}}$  上的高斯采样计算得到向量  $s$ 。为达到 **GaussianSampler**( $\mathbf{T}_{\text{MNTRU}}$ ) 和理想离散高斯分布  $\mathcal{D}_{\Lambda(\mathbf{T}_{\text{MNTRU}}), \sigma}$  的 KL 距离是可忽略的, 标准差  $\sigma$  需要小于  $2^{-\lambda}$ 。这是由以下等式给出的:  $\sigma = \eta'_\varepsilon \cdot \|\mathbf{T}_{\text{MNTRU}}^*\|$ , 其中  $\varepsilon = 2^{-\lambda/2}/(2\sqrt{2} \cdot dn)$ , 更准确地说, 是

$$\sigma \approx \frac{c_d}{\pi} \cdot \sqrt{\frac{\ln 2}{2} \left( \frac{\lambda}{2} + \log_2(4\sqrt{2} \cdot dn) \right)} \cdot q^{1/d}.$$

需要注意的是, 用户私钥的提取过程应该是有状态的, 也就是说它应该存储以前发布的用户私钥, 否则该方案会因对同一  $id$  重复查询而变得不安全。用户私钥提取算法的具体步骤由算法 2 给出。

**Algorithm 2: Extract [CKKS19]**


---

```

input : 身份  $id$ , 主私钥  $\mathbf{T}$ , 主公钥  $\mathbf{h}$ , 哈希函数  $H : \{0, 1\}^* \rightarrow \mathcal{R}_q$ 
output: 用户私钥  $sk_{id} \in \mathcal{R}^{d-1}$ 

1 if  $id$  之前被查询过 then
2   return 之前存储的  $sk_{id}$ 
3 else
4    $\mathbf{t} \leftarrow (H(id), 0, \dots, 0) \in \mathcal{R}^d$ 
5    $\sigma \leftarrow \frac{c_D}{\phi} \cdot \sqrt{\frac{\ln 2}{2} \left( \frac{\lambda}{2} + \log_2(4\sqrt{2} \cdot dn) \right)} \cdot q_{1/d}$ 
6    $\mathbf{c} \leftarrow \text{GaussianSampler}(\mathbf{T}, \sigma, \mathbf{t})$ 
7    $\mathbf{s} = (s_0, s_1, \dots, s_{d-1}) \leftarrow \mathbf{t} - \mathbf{c} \quad // \langle \mathbf{s}, (1, h) \rangle = t$ 
8   将  $sk_{id} = (s_1, \dots, s_{d-1})$  放入本地存储中
9   return  $sk_{id}$ 
10 end

```

---

**(3) 加密解密**

加密和解密方法与基于 Module-LWE 的加密方法相同。特别地，多项式  $r, e_i$  是从  $\{-1, 0, 1\}^n$  中均匀采样的。此外，如 [DLP14] 中所述，基于 KL 散度的安全参数只适用于搜索问题，这里的 IBE 方案还需结合 KEM 和一次性掩码 (one-time-padding, OTP)。将密钥  $k$  的哈希值  $H'(k)$  用于一次性掩码， $H'$  被建模为随机预言机器，这使得该方案的 CPA 安全性（判定问题）就像精确地找到密钥  $k$ （搜索问题）一样困难。

加密算法和解密算法的具体步骤由算法 3、算法 4 给出。

**Algorithm 4: Decrypt[CKKS19]**


---

```

input : 密文  $C = (\mathbf{c}, c')$ , 用户私钥  $sk_{id} \in \mathcal{R}^{d-1}$ , 哈希函数
       $H : 0, 1^* \rightarrow \mathcal{R}_q, H' : \{0, 1\}^n \rightarrow \{0, 1\}^m$ 
output: 消息  $\mu \in \{0, 1\}^m$ 

1  $\mathbf{s}' = (1, -sk_{id})$ 
2  $w \leftarrow \langle \mathbf{c}, \mathbf{s}' \rangle$ 
3  $k \leftarrow \left\lfloor \frac{2}{q} \cdot w \right\rfloor$ 
4 return  $m \leftarrow c \oplus H'(k)$ 

```

---

对于解密的正确性，观察到

$$w = \langle \mathbf{c}, (1, -sk_{id}) \rangle = \left\lfloor \frac{2}{q} \right\rfloor \cdot m + e_0 + rS_0 - \sum_{i=1}^{d-1} e_i s_i$$

误差多项式  $e_0 + rS_0 - \sum_{i=1}^{d-1} e_i s_i$  的每个系数应当落在区间  $(-q/4, q/4)$  内，因此  $q$  需

**Algorithm 3: Encrypt [CKKS19]**

**input :**身份  $id$ , 消息  $\mu$ , 主公钥  $\mathbf{h}$ , 哈希函数

$$H : 0, 1^* \rightarrow R_q, H' : \{0, 1\}^n \rightarrow \{0, 1\}^m$$

**output:**密文  $C = (\mathbf{c}, c')$ ,  $c \in R_q^{d-1}$ ,  $c' \in \{0, 1\}^m$

- 1  $r, e_i \leftarrow \{-1, 0, 1\}^n$  for  $0 \leq i \leq d - 1$
- 2  $k \leftarrow \{0, 1\}^n$
- 3  $t \leftarrow H(id)$
- 4  $c_0 \leftarrow rt + e_0 + \lfloor \frac{q}{2} \rfloor \cdot k$
- 5  $c_0 \leftarrow 2^{\lceil \log_2 q \rceil - 3} \cdot \left\lfloor \frac{c_0}{2^{\lceil \log_2 q \rceil - 3}} \right\rfloor$
- 6  $\mathbf{c} \leftarrow (c_0, c_1, \dots, c_{d-1})$  where  $c_i = rh_i + e_i$  for  $1 \leq i \leq d - 1$
- 7  $c' \leftarrow \mu \oplus H'(k)$
- 8 **return**  $C = (\mathbf{c}, c')$

要足够大, [CKKS19] 给出的现实条件为:

$$q \geq \frac{32\sqrt{\lambda \ln 2}}{3\sqrt{3}} \cdot \|sk_{id}\|.$$

### 2.2.2 基于 IBE 实现 ISE

集成签密系统是签名系统和加密系统的组合, 其中签名系统和加密系统共享一个密钥生成算法, 即共享同一对密钥  $(pk, sk)$ 。ISE 包含以下算法: (**KeyGen**, **Sign**, **Verify**, **Encrypt**, **Decrypt**), 其中 (**KeyGen**, **Sign**, **Verify**) 组成签名系统, (**KeyGen**, **Encrypt**, **Decrypt**) 组成加密系统。

ISE 的联合安全性规定 [PSST11b], 即使在签名谕言机存在的情况下, PKE 组件也是 IND-CCA 安全的:

$$\Pr \left[ \begin{array}{l} pp \leftarrow \mathsf{Setup}(1^\lambda); \\ (pk, sk) \leftarrow \mathsf{KeyGen}(pp); \\ b = b' : (m_0, m_1) \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{Dec}}, \mathcal{O}_{\mathsf{Sign}}}(pp, pk); \\ b \xleftarrow{R} \{0, 1\}, c^* \leftarrow \mathsf{Enc}(pk, m_b); \\ b' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{Dec}}, \mathcal{O}_{\mathsf{Sign}}}; \end{array} \right] - \frac{1}{2} \leq \mathsf{negl}(\lambda)$$

而签名组件在解密预言机存在的情况下是 EUF-CMA 安全的:

$$\Pr \left[ \begin{array}{l} Vrfy(pk, m^*, \sigma^*) = 1 \\ \wedge m^* \notin \mathcal{Q} \end{array} : \begin{array}{l} pp \leftarrow \text{Setup}(1^\lambda) \\ (pk, sk) \leftarrow \text{KeyGen}(pp) \\ (m^*, \sigma^*) \leftarrow \mathcal{A}^{\mathcal{O}_{\text{Dec}}, \mathcal{O}_{\text{Sign}}}(pp, pk) \end{array} \right] \leq \text{negl}(\lambda)$$

在上一节中已经在 MNTRU 格上构造了 IBE。[PSST11a] 指出，可以基于 IBE 构造集成签名加密系统 ISE。这里的方法是：签名方案组件通过 Naor 变换构建，而 PKE 方案组件通过 FO 变换构建。这里对于底层 IBE 的安全性要求只需要是 OW-ID-CPA 安全，而 ISE 可以在签名加密组件使用同一密钥（即底层 IBE 的主密钥  $(mpk, msk)$ ）时达到联合安全性。

基于 IBE 构造 ISE 的流程如图2.2所示。

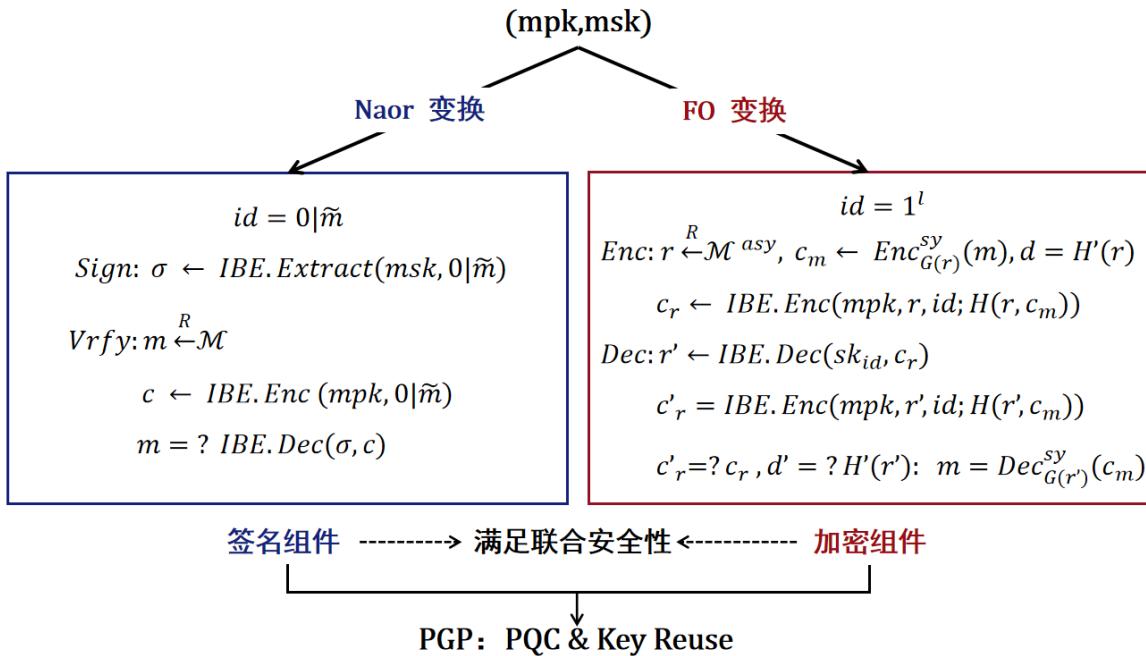


图 2.2 由 IBE 构造 ISE

在这里，本作品使用 1bit 前缀对用户的身份空间进行划分：

- 身份 ID 前缀为 0，使用 Naor 变换 [BF03] 得到 EUF-CMA 安全的签名组件；
- 身份 ID 前缀为 1，使用 Fujisaki-Okamoto 变换 [FO99] 的变体 [TU16] 得到 QROM(Quantum Random Oracle Model) 模型下 IND-CCA 安全的加密组件。

接下来，将详细阐明 Naor 变换和 Fujisaki-Okamoto 变换。

### (1) Naor 变换

使用 Naor 变换 [BF03] 构造签名组件时，将  $id$  设置为  $0|\tilde{m}$ ，其中 “|” 表示级联， $\tilde{m}$  表示需要签名的消息。签名时运行 IBE 的 Extract 算法，得到  $id$  为  $0|\tilde{m}$  对应的用户私钥  $sk_{0|\tilde{m}}$  作为签名。在验证签名时，从消息空间中随机选取一个消息  $m$ ，运行 IBE 的 Encrypt 算法对  $m$  加密得到密文  $c$ ，然后运行 IBE 的 Decrypt 算法，用  $sk_{0|\tilde{m}}$  对  $c$  解密。如果解密结果与  $m$  相同，则验证成功，否则验证失败。

签名组件的具体流程如图2.3所示。

<b>ISE.KeyGen(<math>1^\lambda</math>) :</b>	<b>ISE.Vfry(<math>pk, \tilde{m}, \sigma</math>) :</b>
$pk, sk \leftarrow \text{IBE.KeyGen}(1^\lambda)$	$m \xleftarrow{R} \mathcal{M}$
return $(pk, sk)$	$c \leftarrow \text{IBE.Enc}(pk, 0 \tilde{m})$
<b>ISE.Sign(<math>sk, \tilde{m}</math>) :</b>	if $m = \text{IBE.Dec}(m, \sigma)$
$\sigma \leftarrow \text{IBE.Extract}(sk, 0 \tilde{m})$	then return 1
	else return 0

图 2.3 由 IBE 通过 Naor 变换构造签名组件

## (2) Fujisaki-Okamoto 变换

在构造加密组件时， $id$  固定为  $1^l$ ，将 IBE 退化为 PKE。然后通过 Fujisaki-Okamoto[FO99] 变换将 CPA 安全的 PKE 转变为 CCA 安全。本作品这里采用的是 FO 变换的一个变种 [TU16]，增加一个额外的哈希函数  $H'$ ，可以在量子随机预言机模型（QROM）中达到 IND-CCA 安全性。

对于消息  $m$ ，加密算法  $Enc_{pk}^{hy}$  如下：

$$Enc_{pk}^{hy}(m; \delta) = \left( Enc_{pk}^{asy} \left( \delta; H \left( \delta \| Enc_{G(\delta)}^{sy}(m) \right) \right), Enc_{G(\delta)}^{sy}(m), H'(\delta) \right)$$

其中  $Enc_{pk}^{asy}$  为非对称加密算法（在这里为固定  $id$  为  $1^l$  的 IBE 算法）， $Enc_{sk}^{sy}$  为对称加密算法， $\delta$  为非对称加密算法消息空间中的随即元素， $H, G, H'$  为随机预言机。

加密组件的流程如图2.4所示。

<b> ISE.KeyGen(<math>1^\lambda</math>) :</b>	<b> ISE.Dec(<math>sk, m</math>) :</b>
$pk, sk \leftarrow \text{IBE.KeyGen}(1^\lambda)$	$id = 1^l$
return $(pk, sk)$	$sk_{id} = \text{IBE.Extract}(pk, id)$
	$\delta' = \text{IBE.Dec}(sk_{id}, c_\delta)$
<b> ISE.Enc(<math>sk, \tilde{m}</math>) :</b>	if $\delta' \notin \mathcal{M}^{asy}$
$id = 1^l$	then return $\perp$
$\delta \xleftarrow{R} \mathcal{M}^{asy}$	else $c'_\delta = \text{IBE.Enc}(mpk, \delta', id; H(\delta', c_m))$
$c_m \leftarrow Enc_{G(\delta)}^{sy}(m)$	if $c'_\delta = c_\delta$ and $H'(\delta') = H'(\delta)$
$d = H'(\delta)$	then return $m = Dec_{G(\delta)}^{sy}(c_m)$
return $(c_m, c_\delta, d)$	then return $\perp$

图 2.4 由 IBE 通过 FO 变换构造 IND-CCA 的加密组件

## 第三章 作品测试与分析

### 3.1 测试流程

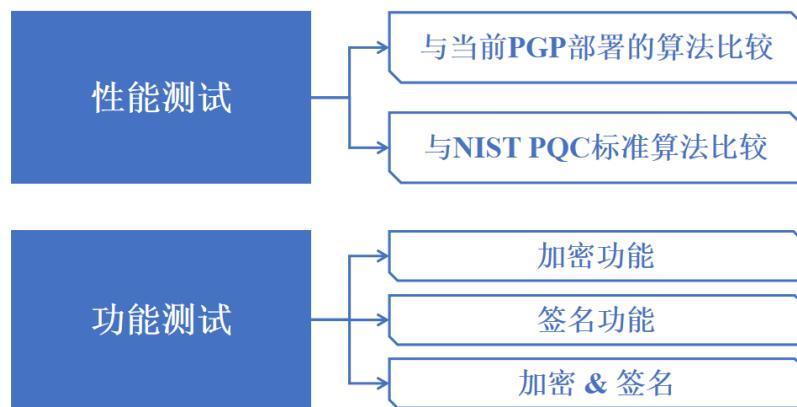


图 3.1 测试流程

### 3.2 测试环境

表 3.1 性能测试的测试环境

操作平台	Ubuntu20.04
CPU	Intel(R) Core(TM) i7-12700H CPU @ 2.30GHz
编译器	GCC 9.4.0
内存	8G

表 3.2 功能测试的测试环境

操作平台	Windows11
CPU	Intel(R) Core(TM) i7-12700H CPU @ 2.30GHz
C++	msvc2019
Qt	6.4.3

### 3.3 效率测试

#### 3.3.1 性能测试

##### (1) 与现有 PGP 算法比较

如表3.3所示，本作品的-PGP 相较于现有的 PGP 而言，可以抵抗量子算法的攻击，同时也可实现密钥复用。

表 3.3 PQ-PGP 与现有 PGP 性能对比 1

	抵抗量子攻击	密钥复用
PQ-PGP	✓	✓
现有的 PGP	✗	✗

在测试 PQ-PGP 效率时，本作品与现有 PGP 中最广泛使用的前三种算法（RSA-4096、RSA-3072、RSA-2048）进行比较。测试单次加密 + 解密的用时，以及单次签名 + 签证的用时，并比较了各个算法的签名长度。测试结果如表3.4所示。

表 3.4 PQ-PGP 与现有 PGP 性能对比 2

	PQ-PGP	现有 PGP		
		RSA-4096	RSA-3072	RSA-2048
单次加密 + 解密用时 (ms)	14.21	114.27	55.43	36.12
单次签名 + 验证用时 (ms)	13.01	109.89	53.24	33.41
签名大小 (bytes)	1152	512	384	256

在加解密速度和签名验签速度方面，本作品的 PQ-PGP 与现有 PGP 流行的算法相比有很好的表现。如图3.2PQ-PGP 加密组件的速度约为 RSA-4096 算法的 8.04 倍，RSA-3072 算法的 3.90 倍，RSA-2048 算法的 2.54 倍；PQ-PGP 签名组件的速度约为 RSA-4096 算法的 8.45 倍，RSA-3072 算法的 4.09 倍，RSA-2048 算法的 2.57 倍。由此可见，加密效率和签名效率均有大幅提升。

在签名规模方面，PQ-PGP 的签名算法相对于现有 PGP 流行的签名算法来说，签名规模较大。

##### (2) 与 NIST 后量子密码标准算法比较

将 PQ-PGP 与 NIST 后量子密码标准算法(CRYSTALS-Kyber、CRYSTALS-Dilithium、Falcon 和 SPHINCS+) 比较，测试结果如表3.5、表3.6所示。

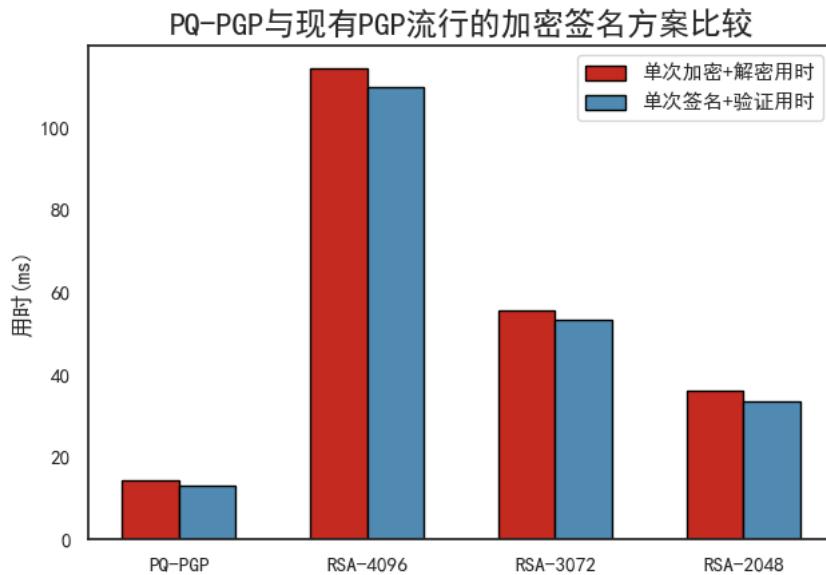


图 3.2 PQ-PGP 与现有 PGP 性能对比

表 3.5 PQ-PGP 的加密组件与 NIST 后量子密码标准算法比较

PQ-PGP	CRYSTALS-Kyber			
		Kyber512	Kyber768	Kyber1024
public key (bytes)	2432	800	1184	1568
secret key (bytes)	12160	1632	2400	3168
Enc+Dec (ms)	14.21	2.07	3.56	4.66

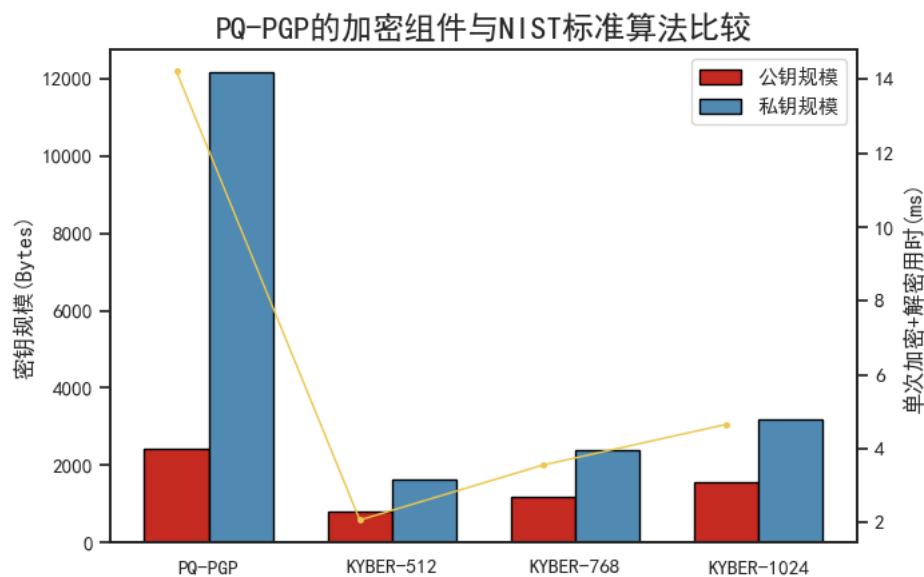


图 3.3 PQ-PGP 加解密组件与 NIST 标准的对比

表 3.6 PQ-PGP 的签名组件与 NIST 后量子密码标准算法比较

	PQ-PGP	CRYSTALS-Dilithium	Falcon	SPHINCS+
public key (bytes)	2432	1312-2592	89-1793	32-64
secret key (bytes)	12160	2528-4860	7553-13953	64-128
signature (bytes)	1152	2020-4595	66-1280	7856-49856
Sign+Vrfy (ms)	13.01	3.21	0.83	26

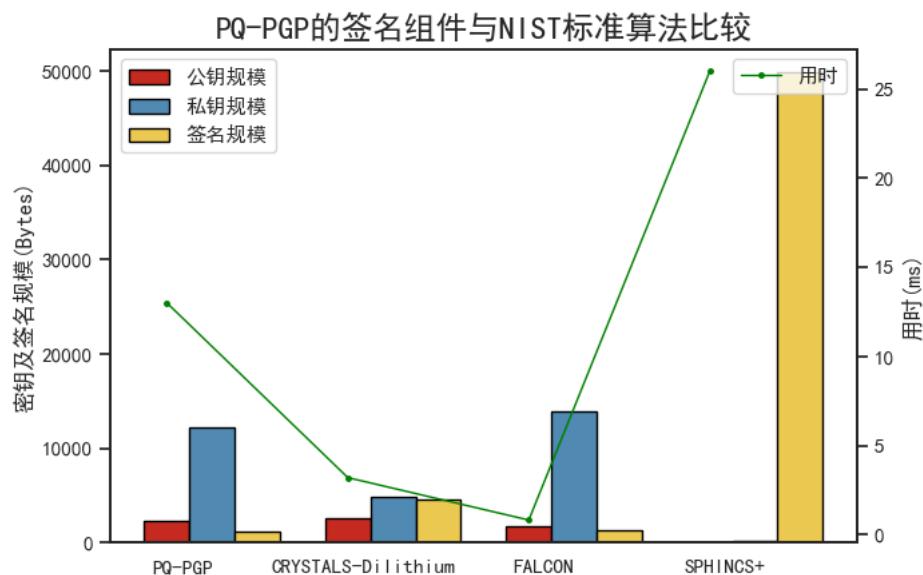


图 3.4 PQ-PGP 签名认证组件与 NIST 标准的对比

如图3.3, PQ-PGP 的加密组件与 NIST 后量子密码标准加密算法 CRYSTALS-Kyber 相比, 密钥规模较大, 加解密速度相较来说稍为逊色。但如图3.4,PQ-PGP 签名算法与 NIST 后量子密码标准签名算法相比, 密钥规模和 Falcon 算法基本相当; 签名尺寸除 Falcon 外, 相较于 CRYSTALS-Dilithium 和 SPHINCS+ 算法均有较好的表现; 签名和签证速度快于 SPHINCS+ 算法, 约为其速度的 2 倍。

### 3.3.2 功能测试

本作品的 PQ-PGP 可以实现加密解密、签名验证以及同时签名加密功能, 如图3.5所示。



图 3.5 作品功能概览图

首先，用户可以通过界面左下方的查询 MPK 来随时查询自己的 MPK



图 3.6 MPK 查询

其次，需要用户生成密钥，输入邮箱，输出用户的公钥。A 和 B 生成密钥的界面如图3.7, 3.8所示。

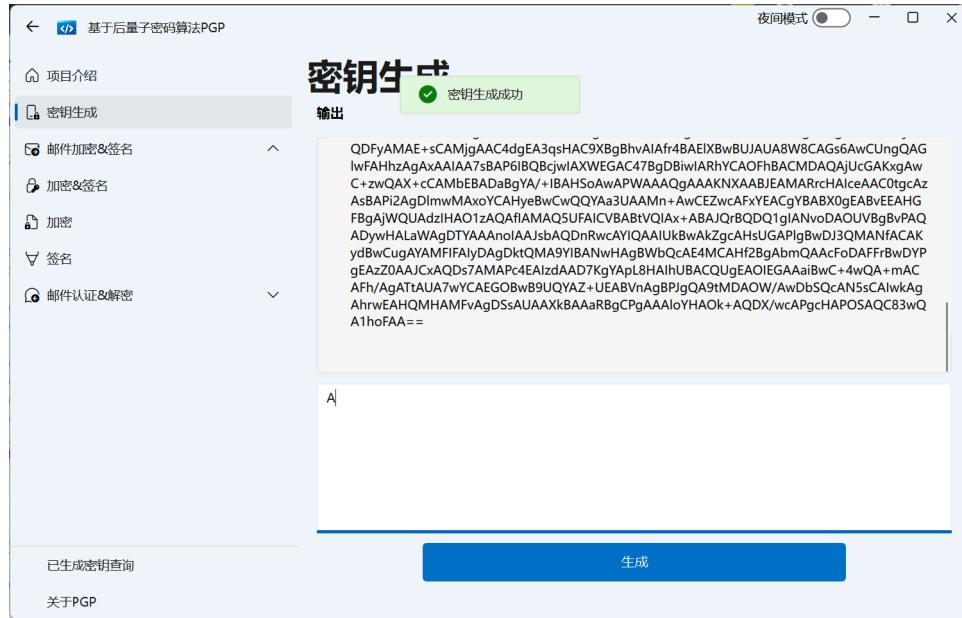


图 3.7 A 生成公钥

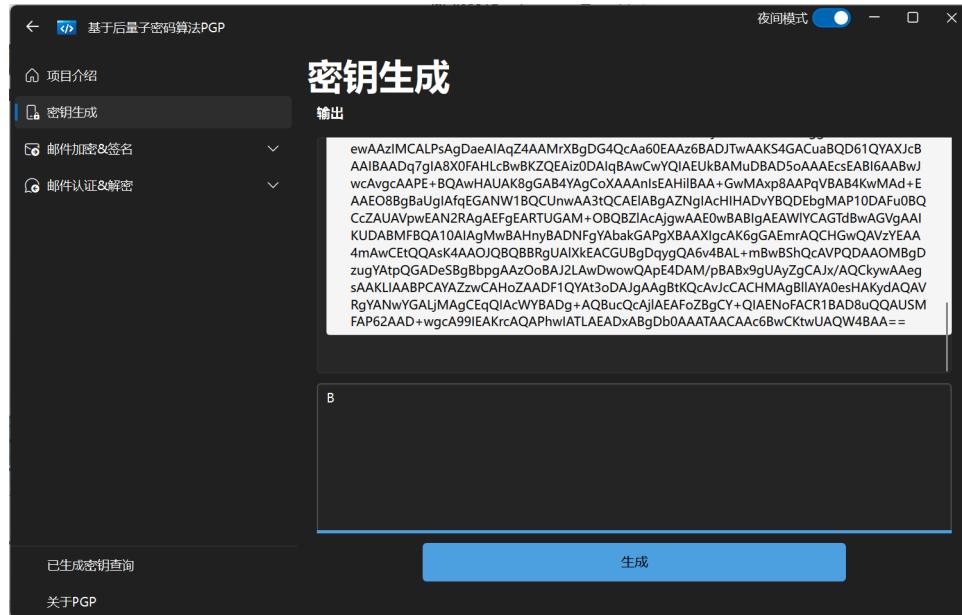


图 3.8 B 生成公钥

## (1) 加密功能

可以实现加密功能，提供保密性。

加密时，输入接收者的公钥和明文；输出加密后的密文。加密功能如图3.9所示。

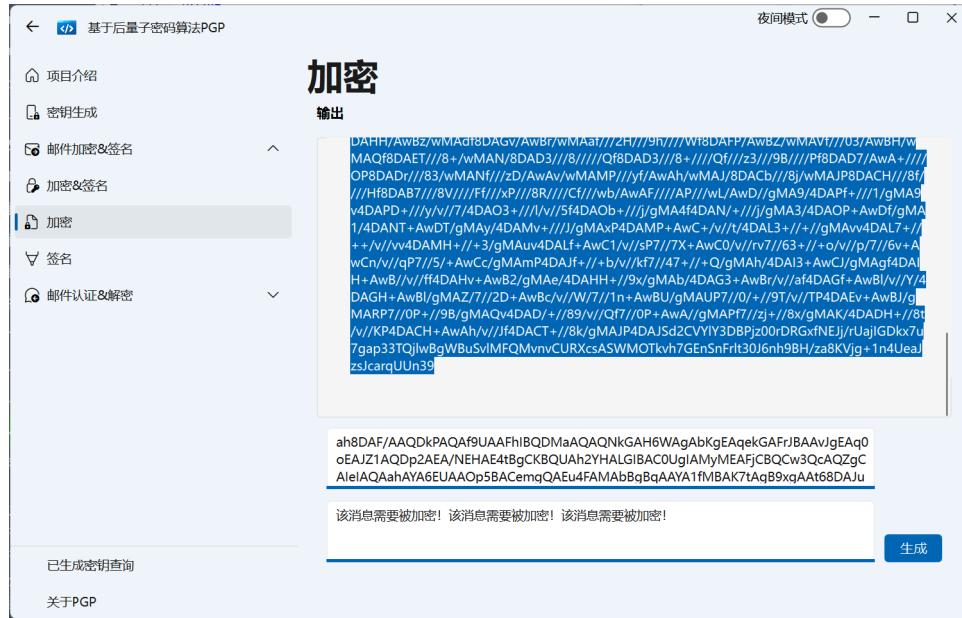


图 3.9 加密

解密时，输入加密后的密文；如果密文合法，则输出解密后的明文（如图3.10），如果密文不合法，则返回解密失败（如图3.11）。

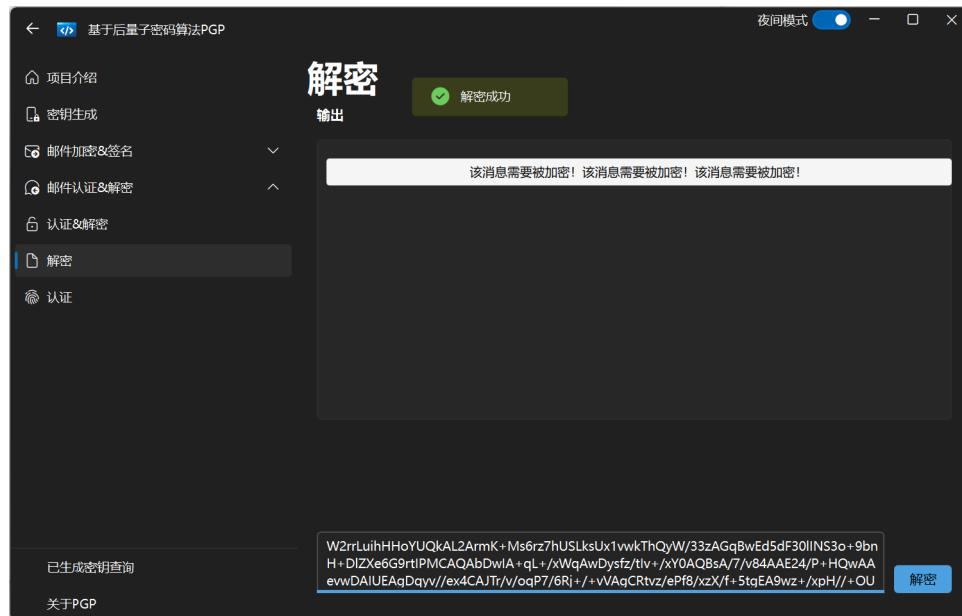


图 3.10 解密成功

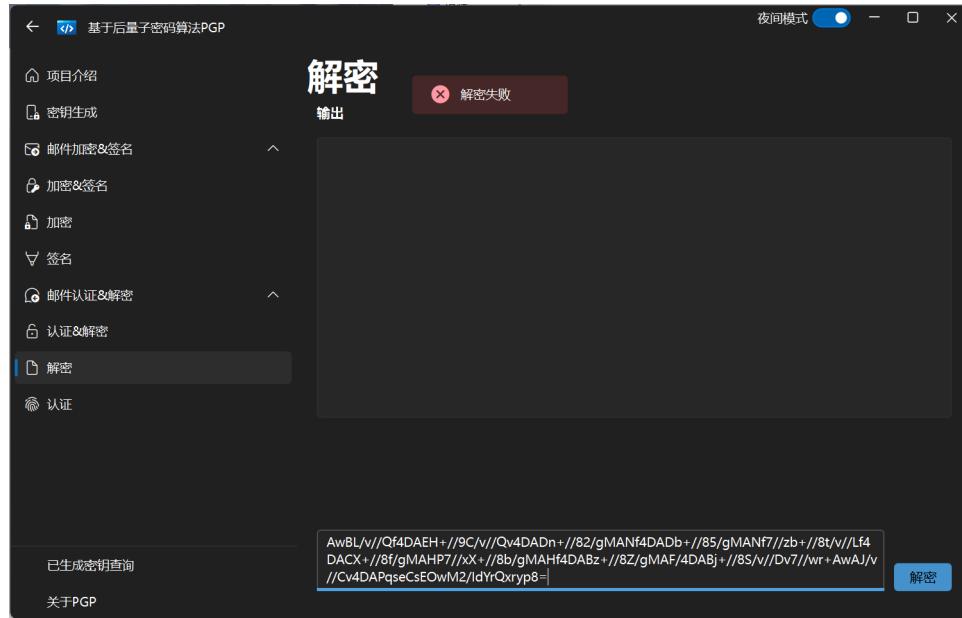


图 3.11 解密失败

## (2) 签名功能

可以实现签名认证功能，提供完整性。

签名时，输入需要被签名的消息，输出签名，如图3.12所示。

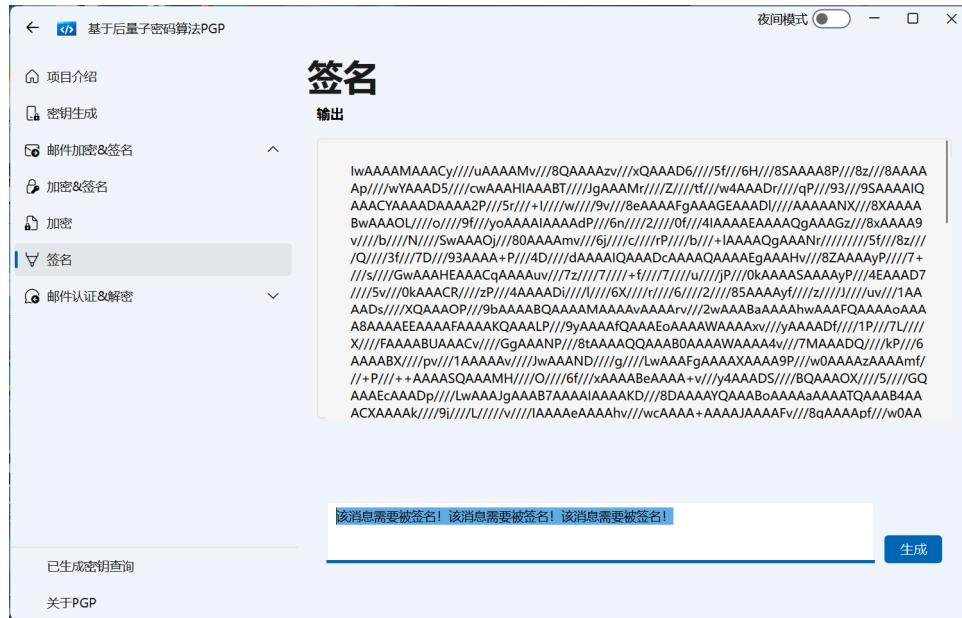


图 3.12 签名

验证签名时，输入发送者的公钥，被签名的消息和签名。如果签名合法，则显示认证成功（如图3.13），反之，显示认证失败（如图3.14）。

## (3) 一次性签名和加密

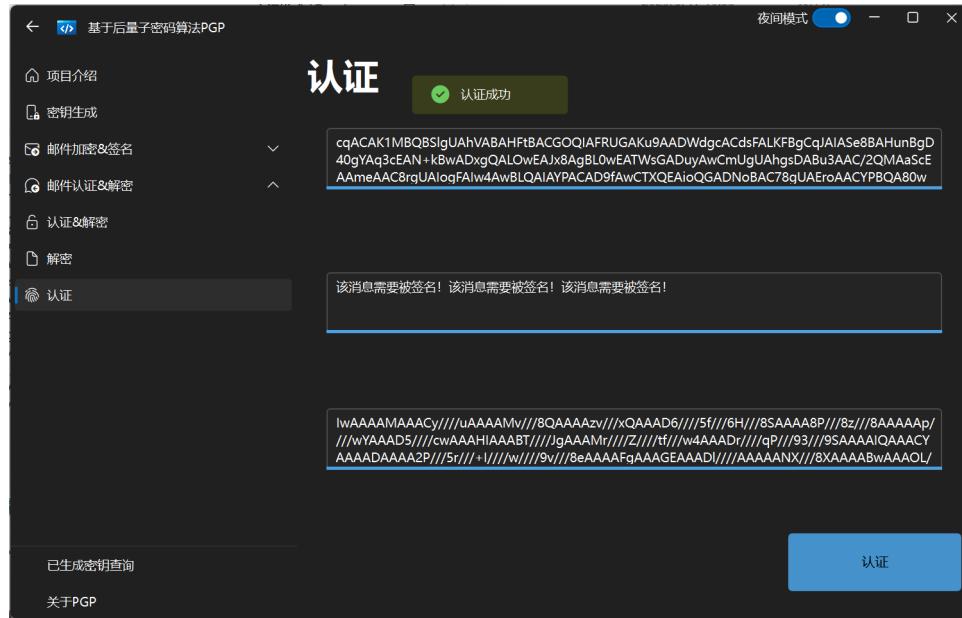


图 3.13 验证签名成功

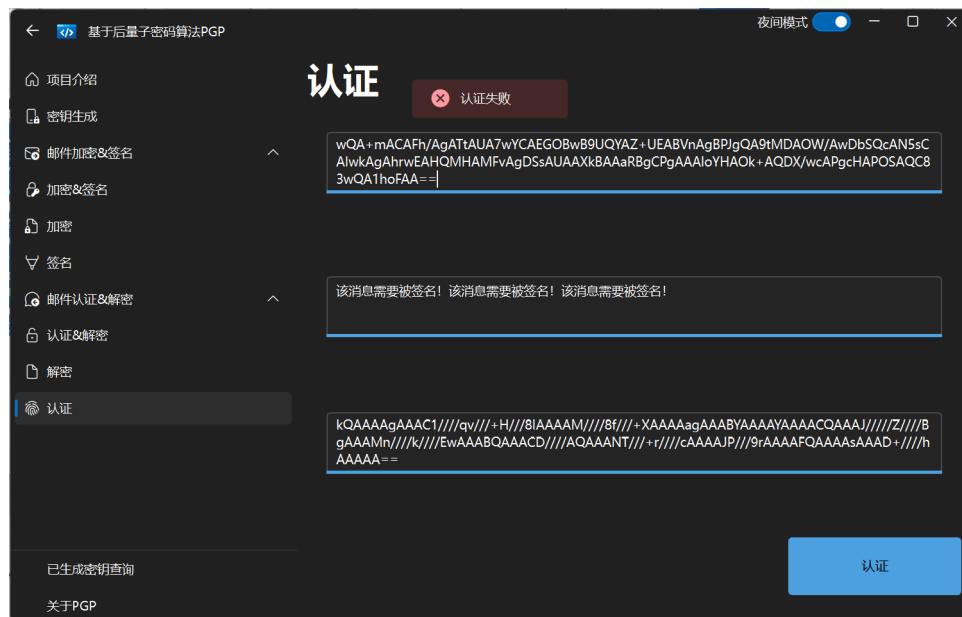


图 3.14 验证签名失败

可以一次性实现签名和加密功能，同时提供保密性和完整性。

采用“Sign-and-Encrypt”策略。发送者 A 输入接收者 B 的公钥和需要被加密和签名的消息  $m$ ，首先对消息  $m$  签名，得到  $\sigma = \text{ISE.Sign}(sk_A, m)$ ；然后对消息  $m$  和签名  $\sigma$  进行加密，得到密文  $C = \text{ISEEnc}(pk_B, m||\sigma)$ （如图3.15）。接收者 B 收到  $C$  后，首先解密得到  $m, \sigma$ ，如果密文不合法，则返回解密失败（如图3.16），如果密文合法，验证签名  $\sigma$  是否正确，如果验证签名时失败，则返回认证失败（如图3.17），如

果合法，则输出消息  $m$ （如图 3.18）。

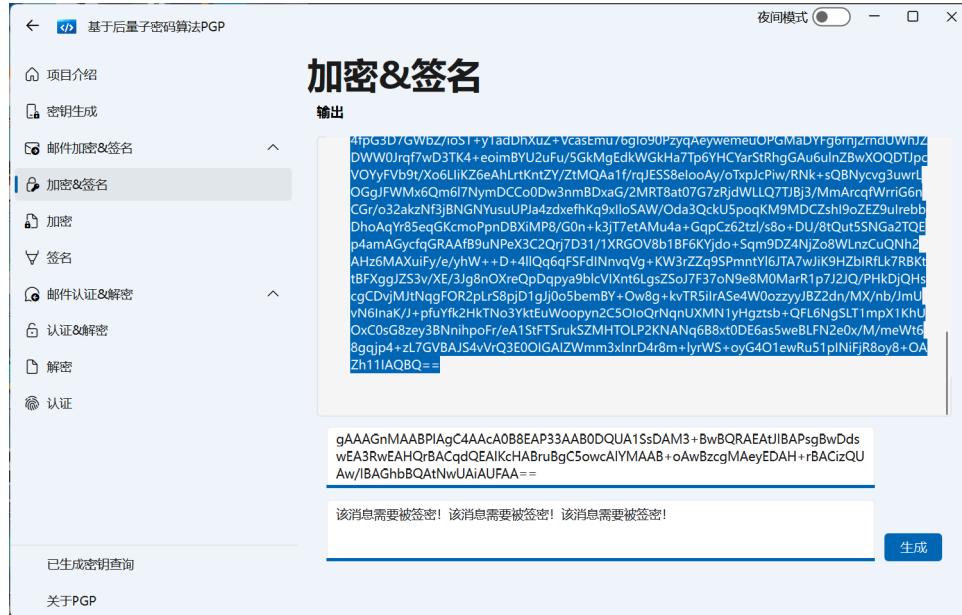


图 3.15 既签名又加密

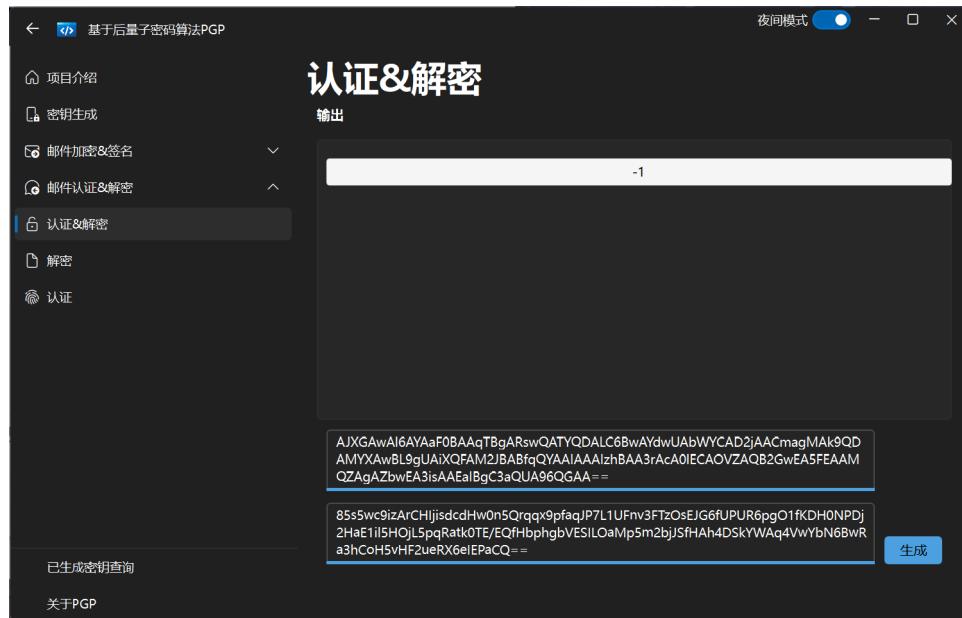


图 3.16 验证签名失败

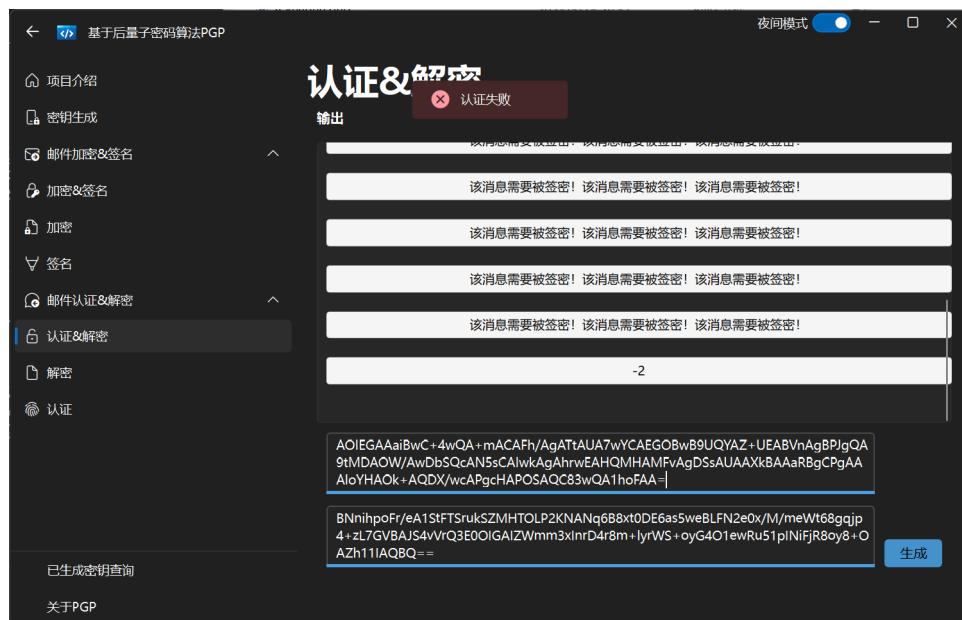


图 3.17 解密失败

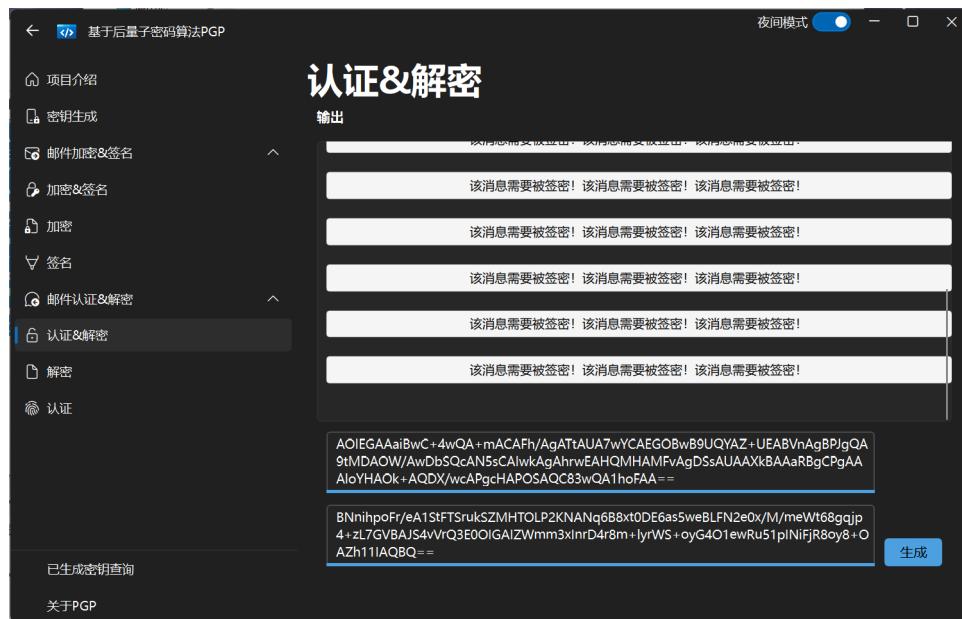


图 3.18 解密成功且验证签名成功时返回消息

## 第四章 创新性说明

### 4.1 首个后量子安全的 PGP

现有的 PGP 标准主要基于 RSA、ELGamal、椭圆曲线密码（ECC）公钥密码体制设计，其安全性基于传统数论假设，不能抵御量子计算机的攻击。一旦量子计算机被发明，现有的 PGP 将不再安全。

本作品的 PQ-PGP 基于格密码算法，是首个达到后量子安全性的 PGP。本作品底层的 IBE 方案基于 Module-NTRU 假设和 Module-LWE 假设，在 Module-NTRU 格上实现，可抵御量子攻击。

### 4.2 加密方案和签名方案的密钥复用

现有 NIST 后量子密码算法标准中的加密算法 CRYSTALS-KYBER 与签名算法 CRYSTALS-DILITHIUM、FALCON 及 SPHINCS+ 的密钥结构均不同，无法自然的共用同一对密钥。为享有密钥复用原则带来的好处，本作品底层采用 IBE 方案，对身份空间进行前缀划分，分别利用 Naor 变换和 Fujisaki - Okamoto 变换，将 IBE 转换为集成签名加密系统 ISE。其中，加密方案在签名预言机下有选择密文攻击下不可区分性 (IND-CCA)；签名方案在量子预言机模型 (QROM) 下，当加密预言机存在时有选择详细攻击下的不可伪造性 (EUF-CMA)。

相较于采用传统的密钥分离原则，本作品可以实现密钥复用，有如下优势：密钥的存储需求大大减少；证书注册、签分、存储、传输等开销大大降低；缩小了密码代码的占用空间，开发工作更加精简。

### 4.3 高效的代码实现

本作品的底层基于 GPV 方案，在 MNTRU 格上实现了高效的 IBE 方案。与基于传统数论问题的密码算法相比，基于格的算法有着明显提升的计算速度、更高的安全强度和略微增加的通信开销，在安全性、公私钥尺寸、计算速度上达到了更好的平衡。

本作品基于格密码算法实现的的 PQ-PGP 系统与现有 PGP 最为常用的 RSA-4096 方案相比，加解密速度和签名速度约提升 8 倍。与 NIST 的后量子密码算法标准相比，签名速度优于 SPHINCS+ 算法，签名尺寸优于 Dilithium 和 SPHINCS+ 算法。

## 4.4 友好的用户界面

本作品基于 QT 设计了 PQ-PGP 软件的图形 UI 界面屏蔽了后端繁琐的技术细节与底层复杂的安装环境，使用户可以一键式操作，设计相对简单。本系统提供了三种不同的模式（加密，签名，一次性同时加密签名），使得用户可以灵活选择不同模式进行信息处理，实用度高，易用性强。

## 4.5 广阔的应用范围

本作品的 PQ-PGP 不仅适用于电子邮件加密，更适用于一切需要机密性与认证性的通信场景，在量子信息时代有着广泛的应用。诸如部署在聊天软件，提供端到端加密功能，只有用户本身和与之交流的用户可以读取消息内容，除此之外，其他任何人（包括软件）都无法得知，为用户隐私提供更好的安全保障；或部署在电子支付系统中，在金融经济的财产隐私安全上发挥重要作用。

## 第五章 总结

随着量子计算技术的发展，现有 PGP 中部署的密码算法已无法抵抗量子算法的攻击。为应对出现的新型威胁，本作品设计实现了首个可以抵抗量子算法攻击且支持密钥复用的 PGP：PQ-PGP，可在量子计算时代为数据通信提供机密性和认证性。

本作品的研究成果主要包括以下几个方面：

**1. 基于格实现 IBE，底层算法上实现后量子安全。**本作品对比分析了基于格的 IBE 算法，选择在实现高效，参数选取灵活的 Module-NTRU 格上进行实例。底层 IBE 可以实现 147 比特安全性。

**2. 基于 IBE 构造 ISE，实现签名组件和加密组件的密钥复用。**本作品基于底层的 IBE，对用户身份空间进行前缀划分，ID 前缀为 0 则使用 Naor 变换得到 EUF-CMA 安全的签名组件，ID 前缀为 1 则使用 FO 变换得到 QROM 模型下 IND-CCA 安全的加密组件。加密组件和签名组件都使用底层 IBE 的主密钥作为密钥对，在满足联合安全性的前提下实现了密钥复用，大大减少了密钥存储需求、证书开销以及密码代码的占用空间。

**3. 高效的代码实现。**本作品的底层基于 GPV 方案，在 MNTRU 格上实现了高效的 IBE 方案。上层对 IBE 的用户身份空间进行前缀划分，分别利用 Naor 变换和 Fujisaki - Okamoto 变换，将 IBE 转换为 ISE。最后，基于 Qt 搭建了用户操作平台，并将开发的 PQ-PGP 发布至开源社区，为开源社区贡献了平台的成果和经验。

**4. 对加密组件和签名组件进行测试和效率分析。**本作品将 PQ-PGP 与现有 PGP 部署的算法进行效率比较，相较于最广泛使用的 RSA-4096 算法相比，本系统的加密速度和签名速度均提升了 8 倍，效率大幅提升。同时，也与国际最先进的 NIST PQC 标准算法比较，加密效率略逊于 Kyber 算法，但签名速度优于 SPHINCS+ 算法，签名尺寸优于 Dilithium 和 SPHINCS+ 算法。通过分析说明了本系统的高效性。

**5. 使用 Qt 搭建用户操作平台，实现友好的用户界面。**软件的图形 UI 界面屏蔽了后端繁琐的技术细节与底层复杂的安装环境，使用户可以一键式操作，设计相对简单。本作品提供了三种不同的模式：加密，签名，一次性同时加密与签名。用户可以自由灵活的选择方案，易于操作，保证了用户的使用体验。

总之，本作品设计的 PQ-PGP 可以抵抗量子算法的攻击，同时实现了签名组件和加密组件的密钥复用，具有高安全，高性能，低开销，易操作等特点。在量子计算时代，PQ-PGP 可以为数据传输提供机密性和认证性，具有重要意义和实用价值。

## 参考文献

- [BF03] Dan Boneh and Matthew Franklin. Identity-based encryption from the weil pairing. *SIAM journal on computing*, 32(3):586–615, 2003.
- [CKKS19] Jung Hee Cheon, Duhyeong Kim, Taechan Kim, and Yongha Son. A new trapdoor over module-ntru lattice and its application to id-based encryption. Cryptology ePrint Archive, Paper 2019/1468, 2019. <https://eprint.iacr.org/2019/1468>.
- [DLP14] Léo Ducas, Vadim Lyubashevsky, and Thomas Prest. Efficient identity-based encryption over ntru lattices. In *International Conference on the Theory and Application of Cryptology and Information Security*, 2014.
- [FO99] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *International Cryptology Conference*, pages 80–101, 1999.
- [GPV08] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*, 2008.
- [Gro96] L. K. Grover. A fast quantum mechanical algorithm for database search. 1996.
- [HHGP<sup>+</sup>03] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte. Ntrusign: Digital signatures using the ntru lattice. In *The Cryptographer’s Track at RSA Conference*, 2003.
- [LaP21] Ray LaPierre. *Shor Algorithm*, pages 177–192. Springer International Publishing, Cham, 2021.
- [LS15] A. Langlois and D Stehlé. Worst-case to average-case reductions for module lattices. *Designs Codes Cryptography*, 75(3):565–599, 2015.
- [Moo17] D Moody. The ship has sailed: the nist post-quantum cryptography “competition” (invited talk). In *Advances in Cryptology—ASIACRYPT*, 2017.

- [MR07] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measure. *SIAM Journal on Computing*, 37(1):267–302, 2007. Preliminary version in FOCS 2004.
- [PDG14] Thomas Pöppelmann, Léo Ducas, and Tim Güneysu. Enhanced lattice-based signatures on reconfigurable hardware. Cryptology ePrint Archive, Paper 2014/254, 2014. <https://eprint.iacr.org/2014/254>.
- [PGP] Why I Wrote PGP. Philip zimmermann.
- [PSST11a] Kenneth G. Paterson, Jacob C. N. Schuldt, Martijn Stam, and Susan Thomson. On the joint security of encryption and signature, revisited. Cryptology ePrint Archive, Paper 2011/486, 2011. <https://eprint.iacr.org/2011/486>.
- [PSST11b] Kenneth G Paterson, Jacob CN Schuldt, Martijn Stam, and Susan Thomson. On the joint security of encryption and signature, revisited. In *Advances in Cryptology–ASIACRYPT 2011: 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings* 17, pages 161–178. Springer, 2011.
- [SWR<sup>+</sup>22] Christian Stransky, Oliver Wiese, Volker Roth, Yasemin Acar, and Sascha Fahl. 27 years and 81 million opportunities later: Investigating the use of email encryption for an entire university. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 860–875, 2022.
- [TU16] Ehsan Ebrahimi Targhi and Dominique Unruh. Post-quantum security of the fujisaki-okamoto and oaep transforms. In *Theory of Cryptography: 14th International Conference, TCC 2016-B, Beijing, China, October 31–November 3, 2016, Proceedings, Part II* 14, pages 192–216. Springer, 2016.