论文“Fully-Homomorphic Encryption from Lattice Isomorphism”的分析报告

叶力天 PB23151830

2025 年 6 月 8 日

1 研究背景与目标

1.1 研究背景

全同态加密（FHE）是一种突破性的密码学技术，允许在密文上执行任意计算并获得与明文计算相同的结果。传统 FHE 方案主要基于学习带噪声问题（LWE），其安全性被认为能抵抗量子计算攻击。然而，随着量子计算技术的快速发展，LWE 的安全性可能面临威胁，因此，探索新的硬度假设以支持 FHE 成为密码学研究的重要方向。

格同构问题（LIP）涉及判断两个格是否通过正交线性变换同构。LIP 作为一种潜在的密码学硬度假设，因其数学结构和抗量子攻击的潜力而受到关注。论文“Fully-Homomorphic Encryption from Lattice Isomorphism”探索了 LIP 是否可以作为 FHE 的新基础，扩展经典和量子密码学的工具集。

1.2 研究目标

基于上述背景，本篇论文希望利用 LIP 的变体（论文中称其为区分-LIP）构建经典和量子 FHE 方案，从而减少对 LWE 的依赖，并为密码学提供新的硬度假设。

具体而言，作者旨在：

1. 证明区分-LIP 的强度可以支持线性同态加密，并通过循环安全假设扩展为全同态加密。
2. 探索 LIP 在量子 FHE 中的应用，特别是在 OSP 协议中的潜力。

3. 解决格基加密中的技术挑战，如噪声增长和空间不匹配，以实现高效的 FHE 方案。

2 主要研究贡献

论文方案的核心思想是利用区分型 LIP 问题的安全性，并据此构建了 FHE 和 QFHE 方案。

2.1 基于区分 LIP 的经典 FHE 方案

基于[Dv22]的加密方案，作者引入线性随机性提取器以支持同态属性，提出了如下方案：

- **密钥生成**：生成二次型 $P = U^T QU$（U 为随机单模矩阵）和向量 $\mathbf{r} \in \mathbb{Z}_p^n$，公钥为 $(\mathbf{P}, \mathbf{r})$，私钥为 U。
- **加密**：对消息 $m \in \{0,1\}$，从二次型 P 上的离散高斯分布 $\mathcal{D}_{\boldsymbol{P},\sigma}$ 采样格点 x，计算 $y = \frac{1}{q} \cdot x (\mathrm{mod}\ \mathbb{Z}^n)$ 和 $z = \frac{1}{q} \cdot x - y$，密文为 $c_0 = y, c_1 = r^T z + m \ (\mathrm{mod}\ p)$。
- **解密**：通过 Uy 计算格点 Uz，利用 $s^T Uy$（$s^T = r^T \ (\mathrm{mod}\ p)$）恢复消息 m。

上述加密方案在概念上实现了对位消息的封装，其中密文包含格点信息 $c_0 = y$ 和一个加密掩码 $c_1 = r^T z + m$。由于公开信息只是一个等构晶格的基（P），攻击者无法区分这是源自 Λ_Q 还是 Λ_L 的晶格，从而无法区分加密对应的 m 值。

2.2 技术构造与同态运算

在上述基础加密方案的框架上，作者进一步引入了同态运算，实现线性同态和最终的全同态加密功能。主要设计包括以下几点：

- **线性同态加法**：给定两个密文 (c_0, c_1) 和 (c_0', c_1') 对应消息 m, m'，可以直接对密文分量进行加法：$(c_0 + c_0',\ c_1 + c_1') = \left(y + y',\ r^T(z + z') + (m + m')\right)$. 解密时，这相当于对原消息进行模 p 的加法。论文证明只要噪声增长仍在可控范围，解密能够正确返回 $m + m'$。因此方案天然支持任意多次同态加法。
- **常数乘法及位移**：更一般地，对于整数常数乘法也可以高效实现。论文指出，

通过对消息取二进制分解，将加密拓展到对模 pq 中的任意消息（q 取较大幂2）进行操作。其中，乘以 2^k 的操作只需将密文的二进制表示向左平移 k 位即可实现同态乘法。更一般地，对任意常数的乘法可以通过二进制加权和的方式组合加法与移位来完成。

总体而言，方案支持对密文进行任意线性变换，这使得它是**线性同态加密**的。

- **同态乘法和全面同态**：要实现任意乘法运算，论文在上述线性同态基础上引入了循环安全性假设，允许公钥中包含私钥的加密版本，从而在同态运算时能评估到秘密参数。利用已有的"短整数同态"，论文采用类似于 Gentry 引导加密的思路，并进一步论证了该方案的解密电路属于 NC^1，满足引导加密的必要条件，从而实现了从可计算任意电路深度扩展到可计算任意多项式大小电路的全同态性能。

综上，论文通过巧妙结合基于格点采样的加密机制和线性同态运算，引入循环安全性来支持同态乘法，最终构造了一个理论上的 FHE 方案。方案的安全性归约表明，只要区分 LIP 够难（即对应 Λ_Q, Λ_L 晶格族不可区分），那么该加密方案的 CPA 安全性成立；在附加循环安全性假设下，该方案就能支持任意电路的同态评估。

2.3 基于区分 LIP 的 QFHE 方案

论文进一步构建了支持量子电路的 QFHE 方案，核心是通过两消息无知状态准备（OSP）协议：

- **OSP 定义**：OSP 允许经典客户端指示量子服务器准备计算基态（$\mu = 0$，如 $|b\rangle$）或 Hadamard 基态（$\mu = 1$，如 $|0\rangle + (-1)\hat{}b\,|1\rangle$），确保两种模式在计算上不可区分。
- **OSP 协议**：客户端生成二次型 P（对应 $\mu = 0$ 时同构于 Q_0，$\mu = 1$ 时同构于 Q_1），服务器准备高斯叠加态并通过测量和过滤生成目标状态。量子状态过滤技术确保 Hadamard 基态的正确性。
- **QFHE 构建**：结合 OSP 和经典 FHE（解密在 NC^1 中），根据最新的[GV24, BK25]成果，实现 QFHE，支持量子电路的同态评估。

2.4 创新技术与贡献

综合分析，论文的贡献体现在以下几个方面：

1. **提出 FHE 的新基础假设**

本文首次将晶格同构问题（LIP）用于构造全同态加密（FHE），拓展了 FHE 的安全基础。尽管当前方案在参数上仍可能隐含 LWE，但提供了一条有望脱离 LWE 的独立路径，对密码学理论是一项重要推动。

2. **拓展 LIP 的应用范围**

论文显著扩展了 LIP 工具箱，不仅实现 FHE 和 QFHE，还构造了碰撞抗哈希函数和无交互状态准备协议，表明 LIP 可支撑更复杂的密码功能，超越原先用于签名、零知识等基本原语的局限。

3. **揭示几何难题与功能加密的联系**

工作展示了晶格几何结构（如同构性）也能承载代数意义上的同态运算，丰富了密码学中“难题驱动设计”的理论框架，推动了从结构性质构建高级原语的研究方向。

4. **为后量子加密提供新路径**

作为格问题的 LIP 预期对量子攻击具有天然抵抗力，若未来可优化为纯 LIP 安全，将成为后量子 FHE 的有力候选。论文中的 OSP 协议也可能促进跨越经典与量子的加密方案设计。

3 个人思考与启发

3.1 对 LHE 和 LIP 的理解加深

首先，FHE 的本质在于：在加密状态下仍能对数据进行任意计算，并保证解密结果与明文计算一致。这要求加密方案不仅满足语义安全，还要具备可组合的同态结构。我意识到，真正实现 FHE 的关键挑战不在于加密本身，而在于如何在不破坏安全性的前提下，支持复杂函数的逐步同态评估，同时控制噪声增长以保持解密正确性。这使得 FHE 成为密码学中最复杂、最结构化的原语之一。

其次，对 LIP 问题的理解也显著加深。LIP 关注的是两个高维晶格是否存在正交变换使其等构，属于一种结构不可区分性问题。它不同于 LWE 的“解方程难”，而是更类似于图同构问题的“辨结构难”。这一问题难以通过传统代数手段求解，因为即使知道两

个晶格等构，寻找具体变换也是计算上极难的。正因如此，LIP 为构造加密方案提供了“结构隐藏性”的天然基础。

3.2 对密码学发展的进一步思考

在该论文中，作者广泛借鉴并整合了前人的研究成果，例如 Gentry 的全同态加密框架、基于 LWE 的方案中所采用的噪声管理技术，以及量子密码学中的状态准备协议。在此基础上，作者首次将概率性验证技术成功应用于全同态加密及量子全同态加密领域，取得了具有重要意义的突破。这一研究使我深刻认识到，现代密码学是一个持续演进、不断积累与创新的学科体系。它建立在一代又一代研究者长期努力的基础之上，每一次理论上的进展和技术上的突破，都离不开对已有成果的深入理解，以及对新挑战的敏锐洞察和勇于探索的精神。

3.3 该方向的未来研究方向

论文指出，当前经典 FHE 方案仍依赖 LWE 硬度，未来的研究需要优化参数以实现完全独立于 LWE。此外，比较 LIP-basedFHE 与现有 LWE-basedFHE 的效率和实用性将是一个有价值的方向。OSP 协议的进一步应用，如在量子多方计算中的实现，也是一个值得探索的领域。这些开放问题为密码学研究提供了清晰的方向。

3.4 总结和感悟

综上，阅读这篇论文是一次宝贵的学习经历。论文结合了格理论、同态加密和量子密码学的先进概念，展示了如何将数学严谨性应用于实际问题。其清晰的结构和对技术挑战的系统性解决方法，激发了我进一步学习格基密码学和量子计算的兴趣，感受到了密码学的强大。