修士論文

(古典) 完全準同型暗号を用いた依頼量子計算法の改良

川野 公誠

主指導教員 藤﨑 英一郎

北陸先端科学技術大学院大学
先端科学技術研究科
（情報科学）

令和 7 年 3 月

Abstract

Fully Homomorphic Encryption (FHE) is a cryptographic scheme that allows arbitrary computations to be performed directly on encrypted data without decryption. The concept of FHE was first proposed by Rivest, Adleman, and Dertouzos in 1978; however, achieving fully homomorphic encryption that supports both multiplication and addition remained an open problem for many years. This problem was first solved in 2009 when Gentry introduced the concept of bootstrapping. However, bootstrapping is computationally expensive, and various improvements have been proposed to enhance its efficiency, such as the GSW scheme and the TFHE scheme, which enables even faster homomorphic computations. Moreover, research has been conducted to extend the framework of FHE to quantum computing, leading to the development of Quantum Fully Homomorphic Encryption (QFHE). Quantum computers are not only expensive but also require advanced expertise for operation and maintenance. As quantum computing technology advances, it is expected that enterprises and individuals will increasingly outsource quantum computations to external quantum computing services. However, outsourcing quantum computations poses a significant privacy risk, as users' confidential data may be exposed to the service provider. As a solution to this issue, QFHE is a promising technology that enables secure quantum computation while preserving data confidentiality, making it highly valuable from the perspective of security and privacy in quantum computing services. A major limitation of conventional QFHE schemes is that the evaluation key is a quantum state, requiring the client to have access to quantum computing resources. To address this limitation, Mahadev (FOCS 2018) proposed a protocol that allows a classical client to delegate encrypted quantum computations to a quantum server via a classical communication channel. This protocol achieves secure delegated quantum computation by utilizing classical fully homomorphic encryption (FHE) to handle Clifford gates and the non-Clifford Toffoli gate. Since Clifford and Toffoli gates together form a universal gate set, this protocol allows a classical client to securely delegate arbitrary quantum computations to a quantum server. However, Mahadev's protocol has certain limitations. Specifically, in the homomorphic evaluation of non-Clifford gates, it requires the encryption and homomorphic computation of classical FHE to be performed on a quantum computer, making it inefficient. Additionally, the protocol remains within the framework of quantum leveled FHE, imposing restrictions on the number of computations. In this study, we aim to enhance the efficiency of Mahadev's protocol by introducing two key modifications. First, we demonstrate that the Toffoli gate used in Mahadev's protocol can be replaced with the simpler non-Clifford gate, the T gate. This modification reduces the number of homomorphic computations required for the non-Clifford

gate evaluation from three to one. Second, we propose replacing the classical FHE scheme used in Mahadev' s protocol with an alternative scheme to improve computational efficiency. These modifications enable the extension of quantum leveled FHE to QFHE, eliminating the need for cryptographic transformations that were previously essential in existing approaches.

目 次

第1章　はじめに

1.1　研究背景

暗号化されたデータを復号することなく、任意の演算を直接計算可能とする暗号方式は完全準同型暗号（Fully Homomorphic Encryption, FHE）と呼ばれる。あらゆるプログラムは加算と乗算の回路として表現可能であるため、これら両方の操作を暗号文上でサポートできる暗号システムは FHE として定義される. 加算のみあるいは乗算のみを可能にする方式は提案されていたものの,FHE の構築は長年未解決の課題だった. この問題は 2009 年に Gentry によるブレイクスルーによって初めて解決された [Gen09].Gentry の方式では、演算を繰り返すたびに増加するノイズをブートストラッピングと呼ばれる手法を用いて提言することで、復号エラーを防ぐ仕組みが導入することで、FHE を実現した. 以降計算コストの高いブートストラッピングの効率化を目指し、様々な改良がおこなわれた. その代表例として Gentry らによる GSW 方式 [GSW13] や、さらに高速な暗号演算を可能にする TFHE[CGGI18] などがあげられる.

FHE の枠組みを量子計算に拡張とした量子完全準同型暗号 (Quantum Fully Homomorphic Encryption, QFHE) が近年注目されている. 量子コンピュータは高コストであることに加え, 運用や管理に高度な専門知識を要するため, 普及が進むにつれ, 企業や個人が量子計算を外部の量子計算サービスへアウトソースする形態が一般化すると予測されている. しかし, このようなサービスを利用する場合、個人的なデータがサーバー側に露見するというプライバシーリスクが伴う. この課題に対する解決策として、QFHE は, データを暗号化したまま量子計算を実行可能であるという特徴を持つ. これにより、データの機密性を維持したまま量子計算を利用できるため、量子計算サービスのセキュリティおよびプライバシーの観点から極めて有望な技術として位置づけられる。

QFHE はユニバーサル量子ゲートセットに基づく準同型評価の実現を目指すが, その中でも特に非クリフォードゲートの評価が主要な課題となる. この問題に対処するため,Broadbent と Jeffery [BJ15] は, 量子ワンタイムパッド（Quantum One-Time Pad, QOTP）[AMTdW00] の鍵を古典的な FHE で暗号化する手法を提案した.Broadbent と Jeffery の手法では次の 2 つのアプローチが提示されている。1 つ目は、暗号文のサイズが非クリフォードゲートの数に対して多項式的に増加する方法である.2 つ目は、非クリフォードゲートの数に応じて量子評価鍵の大きさが指数関数的に増加する方法である. このような方法は非クリフォードゲート評価の可能

性を示す一方で, 計算資源の観点で制約があるとされる. これに対し,Dulek,Schäffer, および Speelman[DSS16] は, 非クリフォードゲートの数に対して量子評価鍵のサイズを多項式的に抑えた手法を新たに提案した. この手法は, 量子計算の効率性と拡張性の向上に寄与し,QFHE の実現可能性をさらに前進させた.

これらの手法は評価鍵が量子状態であることから, クライアント側が量子計算を実行できる環境を前提とする制約が存在していた. この制約を解消するため,Mahadev [Mah18] は, 古典的な評価鍵を使用して量子計算を準同型的に評価する方法を提案した. この手法により, 完全に古典的なクライアントと量子サーバー間での QFHE が実現が可能となった. 具体的には、Mahadev の手法では, トラップドアクローフリー関数ペアを活用して QOTP の鍵を暗号化する仕組みを採用している. このアプローチにより,Toffoli ゲートの準同型評価を実現し, 量子計算の準同型評価の効率化と拡張性の向上に寄与した.

1.2 本研究の目的

Mahadev が提案した手法では非クリフォードゲートである Toffoli ゲートを評価した際に三回暗号化された CNOT 演算子を作用させる必要がある. 暗号化された CNOT 演算子は重ね合わせ状態で AltHE の暗号化と準同型 XOR を計算する必要があるため, 計算効率の観点から課題が残されている. さらに, 本手法では [GSW13] のスキームが採用されており, このスキームが量子計算において量子 leveledFHE の特性を持つことから, 計算回数に制限がある点もまた課題である. この制約は, 長時間にわたる複雑な量子計算を効率的かつ柔軟に実行する上での障壁となりえる.

本研究では、Mahadev のプロトコルを効率化するため、新たな改良を提案する。具体的には、ユニバーサル量子ゲートセット $\mathsf{X}, \mathsf{Z}, \mathsf{H}, \mathsf{S}, \mathsf{CNOT}, \mathsf{T}$ に基づき、T ゲートの準同型評価を実現する手法を導入する。従来の手法では、非クリフォードゲートである Toffoli の準同型評価において暗号化された CNOT 演算子を三回適用する必要があったが、本手法では T ゲートの準同型評価において、同様の操作を一回の適用で実現可能とした。

第2章　準備

2.1　量子計算

2.1.1　量子ビット

量子計算では, コンピュータのビットに対応して, 量子状態を量子ビット (キュービット) と呼ぶ. 一般に n キュービットは複素ベクトル空間 $\mathbb{C}^{2^n}$ の要素として表現される. 特に,1 キュービットの場合, 状態空間は $\mathbb{C}^2$ であり, 計算基底として以下の 2 つのベクトルが用いられる.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.1}$$

と表現する. この基底は計算基底と呼ばれこれらの記法をディラック (Dirac) 記法と呼ぶ.1 キュービットは計算基底を用いて以下のように表現される:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{2.2}$$

ここで,α, β は確率振幅を表し, 量子力学の正規化条件

$$|\alpha|^2 + |\beta|^2 = 1$$

を満たす必要がある. 状態 $|\psi\rangle$ の複素共役転置は以下のように表られる:

$$\langle\psi| = |\psi\rangle^\dagger = \alpha^* \langle 0| + \beta^* \langle 1|$$

ここで,$\dagger$ は複素共役転置を表す. この記述により, 量子状態を用いた演算や測定の計算が可能となる.

2.1.2　ユニタリ変換

量子力学では量子状態の遷移をユニタリ変換により記述される. この変換はユニタリ演算子 U を用いて以下のように表される:

$$|\psi'\rangle = U |\psi\rangle$$

ここで, ユニタリ演算子は $UU^\dagger = U^\dagger U = I$ を満たす線形演算子である.

2.1.3　多量子ビット

複数のキュービットを扱うとき各キュービットはテンソル積によって結合されると考える.n キュービットは $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$ で表現される. 各キュービットの計算基底を (2.1) とすると n キュービットの計算基底は $\{|b_1\rangle \otimes \cdots \otimes |b_n\rangle\}_{b_1,\ldots,b_n \in \{0,1\}}$ となる. 各ビットに対して $|\phi_i\rangle = U_i |\psi_i\rangle$ と状態が遷移するとき

$$|\phi_1\rangle \otimes \cdots \otimes |\phi_n\rangle = (U_1 \otimes \cdots \otimes U_n) |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$$

と記述される.

キュービットのテンソル積 $|b_1\rangle \otimes \cdots \otimes |b_n\rangle$ は $|b_1\rangle |b_2\rangle \cdots |b_n\rangle$ や $|b_1, \cdots, b_n\rangle$ と略記する.

2.1.4　測定

キュービットから情報を得るためには何らかの物理量の測定をする必要がある. 量子測定は測定演算子 $\{M_n\}$ を用いて記述される. 状態 $|\psi\rangle$ を測定し, 測定結果 m が生じる確率は次式で表される:

$$\Pr[m] = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

で与えられ, また, 測定後のキュー 0 ビットの乗田は次式で与えられる. 測定後のキュービットの状態は次式で与えられる.

$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

本論文では特に計算基底による測定を扱う.1 キュービットを計算基底で測定する場合, 測定演算子 $\{M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|\}$ を使用する.(2.2) の測定結果 0 または 1 を得られる確率はそれぞれ以下のようになる:

$$\Pr[0] = |\alpha|^2, \Pr[1] = |\beta|^2$$

さらに,n キュービットの中で第 1 キュービットのみを測定する場合, 測定演算子 $\{M_0 = |0\rangle\langle 0| \otimes \mathbb{I}^{\otimes n-1}, M_1 = |1\rangle\langle 1| \otimes \mathbb{I}^{\otimes n-1}\}$ を用いる.

2.1.5　量子計算

一般的な量子コンピュータの量子計算の手順は, 以下のように進行する.

1. n キュービットの初期状態 $|0\rangle^{\otimes n}$ を準備する.

2. 初期状態にユニタリ変換 U を作用させ,$U|0\rangle^{\otimes n}$ を生成する.

3. 最終的な状態 $U|0\rangle^{\otimes n}$ を計算基底で測定し, 測定結果を得る.

ユニタリ変換 U は一般に非常に複雑であり, 一度に計算するのは難しい. そのため,$U = U_m U_{m-1} \cdots U_1$ とユニタリ変換の積に分けて複数のユニタリ変換の積として分解される.
ここで, 各 U_i は比較的単純な変換である. 計算はこれらの変換を逐次適用することで進行する. 各ユニタリ変換 U_i は量子演算子と呼ばれ,k じょれを具体的に実現する阻止が量子ゲートである. 量子ゲートは物理的なキュービットに作用し, 量子状態を操作する役割を果たす.

2.1.6 量子演算子

パウリ演算子 $\mathsf{P} \in \{\mathbb{I}, \mathsf{X}, \mathsf{Y}, \mathsf{Z}\}$ を用いる.

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathsf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \mathsf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \mathsf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

これらのパウリ演算子が生成する群をパウリ群と呼ぶ. また $\mathsf{Y} = i\mathsf{XZ}, \mathsf{XZ} = -\mathsf{ZX}$ が成り立つ.

さらに, クリフォード演算子 C は, パウリ演算子を共役作用の下で別のパウリ演算子を共役作用の下で別のパウリ演算子に変換する演算子であり, 以下の性質を満たす.[Got98]:

$$\mathsf{CPC}^\dagger = \mathsf{P}' \tag{2.3}$$

ここで P, P' はパウリ群の要素である. クリフォード演算子は次のゲートから生成される:

- アダマール変換

$$\mathsf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- 位相ゲート

$$\mathsf{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

- 制御 NOT ゲート CNOT
  2 キュービットに作用し, 状態 $|x, y\rangle$ を $|x, y \oplus x\rangle$ へマッピングする.

$$|x, y\rangle \overset{\mathsf{CNOT}}{\rightarrow} |x, y \oplus x\rangle$$

また, クリフォード演算子には制御 Z ゲート $\hat{\mathsf{Z}}$ も含まれる.$\hat{\mathsf{Z}}$ は 2 キュービットに対して $|x, y\rangle \to (-1)^{xy} |x, y\rangle$ とマッピングするゲートであり,

$$\hat{\mathsf{Z}} = (\mathbb{I} \otimes \mathsf{H})\mathsf{CNOT}(\mathbb{I} \otimes \mathsf{H})$$

を満たす.

クリフォードゲートに対して, 非クリフォードゲートと呼ばれるゲートも存在する. 本論文では以下の非クリフォードを扱う.

- Toffoli ゲート
  Toffoli ゲートは 3 キュービットに対して作用し, 状態 $|x, y, z\rangle$ を $|x, y, z \oplus xy\rangle$ へとマッピングする.
- T ゲート

$$\mathsf{T} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix}$$

2.1.7 ユニバーサル量子ゲートセット

クリフォード演算子の集合に非クリフォードゲートを 1 つ追加することで、任意の量子回路を実現可能なユニバーサル量子ゲートセットを構成できる。この特性により、クリフォードゲートと非クリフォードゲートの組み合わせは、量子計算において基盤となる重要な役割を果たす。ユニバーサル量子ゲートセットとは、任意の量子計算を特定のゲートを用いて任意の精度で近似可能なゲートセットを指す [NC10]。これは量子計算の基本的な構成要素として広く使用されている。

QHE において, ユニバーサル量子ゲートセットが一般的に採用されている:

$$\{\mathsf{X}, \mathsf{Z}, \mathsf{H}, \mathsf{S}, \mathsf{CNOT}, \mathsf{T}\}$$

一方で,Mahadev のプロトコルでは次のユニバーサル量子ゲートセットが使用されている:

$$\{\mathsf{X}, \mathsf{Z}, \mathsf{H}, \mathsf{S}, \mathsf{CNOT}, \mathsf{Toffoli}\}$$

本稿では, これら 2 つのユニバーサル量子ゲートセットを対象に議論を進める.

2.2 量子ワンタイムパッド (QOTP)

量子ワンタイムパッド [AMTdW00] は,ℓ 量子ビットの状態 $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_\ell\rangle$ を暗号化する手法である. この暗号化では, まずランダムに $x, z \in \{0, 1\}^\ell$ を選び, 以下のように量子状態を変換することで暗号化を行う.

$$(\mathsf{X}^{x_1}\mathsf{Z}^{z_1} \otimes \cdots \otimes \mathsf{X}^{x_\ell}\mathsf{Z}^{z_\ell})(|\psi_1\rangle \otimes \cdots \otimes |\psi_\ell\rangle)$$

暗号化された状態は,x と z の情報を持たない者にとっては次のように観測される.

$$\frac{1}{2^{2\ell}} \sum_{x,z\in\{0,1\}^{\ell}} \mathsf{X}^x\mathsf{Z}^z \rho \mathsf{Z}^z\mathsf{X}^x = \frac{\mathbb{I}}{2^{\ell}}$$

ここで,$\rho = |\psi\rangle\langle\psi|$ は元の状態を表す密度行列である. この結果は暗号化された状態が完全混合状態と呼ばれる状態であることを示している. この状態では元の量子状態 $|\psi\rangle$ の情報を一切得ることができない.

2.2.1 古典通信路での QOTP

QOTP を構成する X 演算子と Z 演算子の特性により,X 演算子は測定結果を反転させ,Z 演算子は測定に影響を与えない.[Chi05]. したがって,QOTP された状態を計算機基底で測定すると, 測定結果には QOTP の鍵 x が XOR された状態で出力されることになる. 具体的には, 次のようにあらわされる:

$$\mathsf{X}^x\mathsf{Z}^z \sum_a \alpha_a |a\rangle \overset{\text{測定}}{\to} a' \oplus x$$

さらに, 入力状態を計算基底 $|a\rangle$ とした場合, 暗号化においてはの X のみ影響を与え,Z は測定に影響しないため, 以下のように簡略化される.

$$\mathsf{X}^x\mathsf{Z}^z |a\rangle = |a \oplus x\rangle$$

したがって, 入力状態が計算基底で与えられ, 出力状態も計算基底で測定される場合, 暗号化のプロセスは古典的なワンタイムパッドのみで実現可能となる.

2.3 準同型暗号

準同型暗号は HE.KeyGen,HE.Enc,HE.Eval,HE.Dec の 4 つのアルゴリズムによって構成される. それぞれのアルゴリズムは以下のとおりである.

HE.KeyGen アルゴリズムアルゴリズムは, セキュリティパラメータ λ を入力として, 公開鍵 pk. 評価鍵 evk. および秘密鍵 sk を生成する. この処理は次式であらわされる:

$$(\mathsf{pk}, \mathsf{evk}, \mathsf{sk}) \leftarrow \mathrm{HE.KeyGen}(1^{\lambda})$$

HE.Enc アルゴリズムは, 平文 $\mu \in \{0,1\}$ を公開鍵 pk で暗号化し暗号文 c を出力する. この処理は次式で記述される:

$$c \leftarrow \mathrm{HE.Enc}_{pk}(\mu)$$

HE.Dec アルゴリズムは, 暗号文 c を復号鍵 sk を用いて復号し, 復号結果である平文 $\mu^* \in \{0,1\}^n$ を出力する. この処理は次式で記述される:

$$\mu^* \leftarrow \mathrm{HE.Dec}_{\mathsf{sk}}(c)$$

HE.Eval アルゴリズムは, 評価鍵 evk を用いて $c_1, ..., c_\ell$ を入力とし、復号後に関数 $f(c_1, ..., c_\ell)$ に一致する暗号文 c' を出力する. この計算は次のようにあらわされる:

$$c' \leftarrow \mathrm{HE.Eval}^f_{evk}(c_1, ..., c_\ell)$$

2.4 トラップドアクローフリー関数ペア

単射の関数 f_0 および f_1 の組について $f_0(x_0) = f_1(x_1)$ を満たす任意の入力ペア (x_0, x_1) を見つけることが計算量的に困難でありながら, 特定のトラップドア情報へのアクセスがある場合には効率的に計算可能な場合, この関数の組はトラップドアクローフリー関数ペアと呼ばれる. また, この場合の入力ペア (x_0, x_1) をクローと呼ばれる. 本論文では関数ペア $f_0, f_1 : \{0,1\} \times \mathcal{R} \to \mathcal{Y}$ を用いる. これらの関数は $f_0(\mu_0, r_0) = f_1(\mu_1, r_1) = y$ を満たすクロー (μ_0, r_0) および (μ_1, r_1) を効率的に見つけることが困難である. 一方で, 適切なトラップドア情報が与えられる場合には,(μ_0, r_0) および (μ_1, r_1) を容易に計算することができる.

第3章　関連研究

3.1　Mahadevの量子 leveled FHEプロトコル

Mahadev のプロトコルは FHE のノイズによる回路の制限があるため量子レベルド FHE である.

3.1.1　暗号化された CNOT 演算子

Mahadev の手法において,Toffoli ゲートを準同型的に評価するためには, 暗号文 $\mathsf{Enc}(s)$ で暗号化されたの古典ビット s を用いて CNOT を制御する必要がある. この暗号化された CNOT 演算子は, 暗号文 $\mathsf{Enc}(s)$ および 2 キュービットの量子状態を入力とし, 以下のように動作する.

$$\mathsf{CNOT}^s \sum_{a,b\in\{0,1\}} \alpha_{ab} |a,b\rangle = \sum_{a,b\in\{0,1\}} \alpha_{ab} |a, b\oplus a\cdot s\rangle$$

暗号化された CNOT 演算子を構築するために, トラップドアクローフリー関数ペア $f_0, f_1 \colon \{0,1\}\times\mathcal{R}\to\mathcal{Y}$ を利用する. この関数ペアは, 任意の $\mu_0,\mu_1\in\{0,1\}$ と $r_0, r_1\in\mathcal{R}$ に対して,$f_0(\mu_0,r_0) = f_1(\mu_1,r_1)$ を満たし, かつ $\mu_0\oplus\mu_1 = s$ という特性を持つ. このトラップドアクローフリー関数ペアをエンタングルすることで, 次の量子状態を構築する.

$$\sum_{a,b,\mu\in\{0,1\},r\in\mathcal{R}} \alpha_{ab} |a,b\rangle |\mu,r\rangle |f_a(\mu,r)\rangle \tag{3.1}$$

ここで, 第三レジスタを測定して結果 $y = f_a(\mu_a,r_a)$ を得ると, 状態は次のようになる.

$$\sum_{a,b,\in\{0,1\}} \alpha_{ab} |a,b\rangle |\mu_a,r_a\rangle \tag{3.2}$$

さらに, この状態においてと μ_a と 2 量子状態のうち 2 番目のキュービットに CNOT を作用させる.$\mu_a = \mu_0 \oplus a \cdot s$ であるため, この操作により次の状態が得られる.

$$\begin{aligned}&\sum_{a,b,\in\{0,1\}} \alpha_{ab} \left|a, b \oplus \mu_a\right\rangle \left|\mu_a, r_a\right\rangle \\ &= (\mathbb{I} \otimes \mathsf{X}^{\mu_0} \otimes \mathbb{I}^{\otimes 2}) \sum_{a,b,\in\{0,1\}} \alpha_{ab} \left|a, b \oplus a \cdot s\right\rangle \left|\mu_a, r_a\right\rangle\end{aligned}$$

最終的に, 第二レジスタをアダマール測定し, 測定結果を d とすると以下の状態が得られる.

$$(\mathsf{Z}^{d\cdot((\mu_0,r_0)\oplus(\mu_1,r_1))} \otimes \mathsf{X}^{\mu_0})\mathsf{CNOT}^{s}_{1,2} \sum_{a,b\in\{0,1\}} \alpha_{ab} \left|a, b\right\rangle \tag{3.3}$$

この状態は古典ビット s をトラップドアクローフリー関数ペアの $\mu_0 \oplus \mu_1 = s$ に隠しておりで,s が暗号化された状態で CNOT を制御していることを示している. さらに,QOTP に暗号化されているため, サーバーは s の値がわからない限り,CNOT を作用させたかどうかを判別することはできない.

準同型暗号を用いて, 以下のようにトラップドアクローフリー関数ペアを構成することで $\mu_0 \oplus \mu_1 = s$ と隠すことが可能である.

$$f_0(\mu_0, r_0) = \mathrm{HE.Enc}(\mu_0; r_0) \tag{3.4}$$

$$f_1(\mu_1, r_1) = \mathrm{HE.Enc}(\mu_0; r_0) \oplus_H \mathrm{HE.Enc}(s) \tag{3.5}$$

ここで,$\oplus_H$ は準同型 XOR を表している.
この暗号化された CNOT 演算子は, 後述する Toffoli ゲートの準同型評価において重要な役割を果たす.

3.1.2 量子 leveled FHE

量子 leveled FHE においては QHE.KeyGen アルゴリズムを用いて鍵を生成し、QHE.Enc アルゴリズムにより平文を暗号化する. 生成された暗号文と QOTP の鍵はサーバーに送信される. サーバーは受信した暗号文を基に量子状態を生成し,QHE.Eval アルゴリズムを用いて量子計算を実行しつつ,QOTP の鍵を更新する. 更新後, サーバーは量子状態を測定し, 測定結果と更新された QOTP の鍵をクライアントに送信する. クライアントは QHE.Dec アルゴリズムを用いることで復号を行い, 最終的な結果を得る.

- QHE.KeyGen アルゴリズム
  準同型暗号の鍵を生成する. この鍵生成では, 範囲 $1 \leq i \leq L+1$ において $(\mathsf{pk}_i,\ \mathsf{evk}_i,\ \mathsf{sk}_i,\ t_{sk_i})$ を生成する. ここで,t_{sk_i} は Toffoli ゲートの準同型評価に

おける鍵を更新するためのトラップドア情報である. 評価鍵は $1 \leq i \leq L$ の範囲で次のように構成される.

$$\mathsf{evk}\colon (\mathsf{evk}_1, ...\mathsf{evk}_{L+1}), (\mathsf{pk}_{i+1}, \mathsf{HE.Enc}_{\mathsf{pk}_{i+1}}(\mathsf{sk}_i), \mathsf{HE.Enc}_{\mathsf{pk}_{i+1}}(t_{sk_i}))$$

公開鍵は pk_1, 秘密鍵は sk_{L+1} である.

- QHE.Enc アルゴリズム
  まず, クライアントは 入力 $m \in \{0,1\}^\ell$ に対し, をランダムに選んだ鍵 $x \in \{0,1\}^\ell$ を用いてワンタイムパッドを適用し, 暗号文 $c = m \oplus x$ を生成する. その後,x と同様にランダムに選択した鍵 $z \in \{0,1\}^\ell$ を準同型暗号により暗号化し,$\mathrm{HE.Enc}_{\mathsf{pk}_1}(x, z) \to \hat{x}, \hat{z}$ を得る. この暗号化された鍵 $\hat{x}, \hat{z}$ および評価鍵 evk を暗号文 c とともにサーバーへ送信する.

- QHE.Eval アルゴリズム
  量子回路の準同型評価のため, サーバーは QOTP の鍵に対する準同型計算と,QOTP で暗号化された量子状態に対する量子計算の二つを実行する. 具体的には, ユニバーサル量子ゲートセット V に対して以下の操作が実行できることを示す.

$$\mathsf{Enc}(x, z) \to \mathsf{Enc}(x', z')$$
$$\mathsf{X}^x\mathsf{Z}^z |\psi\rangle \to \mathsf{X}^{x'}\mathsf{Z}^{z'}V |\psi\rangle$$

  パウリゲート, クリフォードゲート,Toffoli ゲートそれぞれの場合で, 評価方法が異なる.

  1. パウリゲートの場合
     任意のパウリゲートは XZ で構成されるため,$V = \mathsf{X}^a\mathsf{Z}^b$ を考える.QOTP された状態は以下のように変形できる.

$$\mathsf{X}^x\mathsf{Z}^x |\psi\rangle = \mathsf{X}^{x'\oplus a}\mathsf{Z}^{z'\oplus b} |\psi\rangle = \mathsf{X}^{x'}\mathsf{Z}^{z'}\mathsf{X}^a\mathsf{Z}^b |\psi\rangle$$

     量子計算は行わず, 鍵の更新のみを計算する. このとき, 鍵の更新は準同型的に計算されるため, サーバーは鍵を知らずなくても更新することができる.

$$\mathsf{Enc}(x, z) \to \mathsf{Enc}(x \oplus a, z \oplus b)$$

  2. クリフォードゲートの場合
     まず, サーバーは量子状態に任意のクリフォードゲート C を作用させる. クリフォード群の共役変換の下で, パウリ群の要素を他のパウリ群の要素に変換するという特性 (2.3) を利用する.

$$\begin{aligned}\mathsf{CX}^x\mathsf{Z}^x |\psi\rangle &= \mathsf{CX}^x\mathsf{Z}^z\mathsf{C}^\dagger\mathsf{C} |\psi\rangle \\ &= \mathsf{X}^{x'}\mathsf{Z}^{z'}\mathsf{C} |\psi\rangle\end{aligned}$$

それぞれのクリフォードゲート $\mathsf{H}, \mathsf{S}, \mathsf{CNOT}$ は次のように QOTP を変換する.

$$\begin{aligned}
&\mathsf{H}\mathsf{X}^x\mathsf{Z}^z\mathsf{H} = \mathsf{X}^z\mathsf{Z}^x \\
&\mathsf{S}\mathsf{X}^x\mathsf{Z}^z\mathsf{S}^\dagger = \mathsf{X}^x\mathsf{Z}^{x\oplus z} \\
&\mathsf{CNOT}_{1,2}(\mathsf{X}^{x_1}\mathsf{Z}^{z_1} \otimes \mathsf{X}^{x_2}\mathsf{Z}^{z_2})\mathsf{CNOT}_{1,2} \\
&= \mathsf{X}^{x_1}\mathsf{Z}^{z_1\oplus z_2} \otimes \mathsf{X}^{x_1\oplus x_2}\mathsf{Z}^{z_2}
\end{aligned}$$

したがって, クリフォードゲートに応じて鍵は準同型的に更新される.

$$\begin{aligned}
\mathsf{H}&\colon \mathsf{Enc}(x,z) \to \mathsf{Enc}(z,x) \\
\mathsf{S}&\colon \mathsf{Enc}(x,z) \to \mathsf{Enc}(x\oplus z, x) \\
\mathsf{CNOT}_{1,2}&\colon \mathsf{Enc}((x_1,z_1),(x_2,z_2) \\
&\qquad \to \mathsf{Enc}((x_1, z_1\oplus z_2),(x_1\oplus x_2, z_2))
\end{aligned}$$

3. Toffoli ゲートのとき
   Toffoli ゲートの共役はパウリ群を以下のようにクリフォードとパウリの積に変換する.

$$\mathsf{Toffoli}(\mathsf{X}^{x_1}\mathsf{Z}^{z_1} \otimes \mathsf{X}^{x_2}\mathsf{Z}^{z_2} \otimes \mathsf{X}^{x_3}\mathsf{Z}^{z_3})\mathsf{Toffoli}^\dagger = C_{xz}P_{xz}$$

ここから

$$\begin{aligned}
&\mathsf{Toffoli}(\mathsf{X}^{x_1}\mathsf{Z}^{z_1} \otimes \mathsf{X}^{x_2}\mathsf{Z}^{z_2} \otimes \mathsf{X}^{x_3}\mathsf{Z}^{z_3})\,|\psi\rangle \\
&= C_{xz}P_{xz}\mathsf{Toffoli}\,|\psi\rangle
\end{aligned} \tag{3.6}$$

となる. このとき,

$$\begin{aligned}
\mathsf{C}_{xz} &= \mathsf{CNOT}^{x_2}_{1,3}\mathsf{CNOT}^{x_1}_{2,3}\hat{\mathsf{Z}}^{z_3}_{1,2} \\
\mathsf{P}_{xz} &= \mathsf{X}^{x_1}\mathsf{Z}^{z_1+x_2z_3} \otimes \mathsf{X}^{x_2}\mathsf{Z}^{z_2+x_1z_3} \otimes \mathsf{X}^{x_1x_2+x_3}\mathsf{Z}^{z_3}
\end{aligned}$$

準同型計算を完了するためには, まず,P_{xz} による鍵の更新を行う.
この状態ではクリフォード演算子 C_{xz} がエラーとして残り, 計算結果に影響を与える. 準同型計算を完了するために,C_{xz} の逆変換を作用させることで打ち消す必要がある. このとき,x_2, x_1, z_3 は準同型暗号で暗号化されている. ここで, サーバーは暗号文から CNOT をコントロールするために暗号化された CNOT を使用する.(3.4) の $\mathsf{Enc}(s)$ に $\mathsf{Enc}(x_2)$ を代入し,(3.6) の 1 キュービット目を制御ビット,3 キュービット目を標的ビットとして作用させると

$$\mathsf{Z}^{d\cdot((\mu_0,r_0)\oplus(\mu_1,r_1))} \otimes \mathsf{X}^{\mu_0}\mathsf{CNOT}^{s}_{1,3}\mathsf{CNOT}^{x_2}_{1,3}\mathsf{CNOT}^{x_1}_{2,3}\hat{\mathsf{Z}}^{z_3}_{1,2}P_{xz}\mathsf{Toffoli}\,|\psi\rangle$$

$s = x_2$ と設定したため $\mathsf{CNOTCNOT} = \mathbb{I}$ より一つ目のクリフォード演算子を打ち消せすことができる. このとき,QOTP による鍵の更新を行うため, 測定結果 y, d を準同型暗号の公開鍵により暗号化し, クライアントから受け取った $\mathsf{HE.Enc}_{\mathsf{pk}_{i+1}}, \mathsf{HE.Enc}_{\mathsf{pk}_{i+1}}(t_{sk_i})$ を用いて y を暗号内でトラップドアクローフリー関数ペアを復号する. 最終的に, 暗号化された CNOT 演算子による QOTP の鍵を以下のように更新する.

$$\mathsf{Enc}((x_c, z_c' = z_c \oplus d \cdot ((\mu_0, r_0) \oplus (\mu_1, r_1)), (x_t' = x_t \oplus \mu_0, z_t)) \tag{3.7}$$

z_c はコントロールビット,x_t はターゲットビットの QOTP の鍵である. 同様に,$s = x_1$ として二つ目のクリフォード演算子も削除する. 三つ目のクリフォード演算子は $\hat{\mathsf{Z}} = (\mathbb{I} \otimes \mathsf{H})\mathsf{CNOT}(\mathbb{I} \otimes \mathsf{H})$ より標的ビットにアダマールゲートを作用させ,$s = z_3$ とし, 暗号化された CNOT 演算子を作用させた後, もう一度アダマールゲートを作用させることで削除することができる. これで Toffoli ゲートの準同型評価が完了する.

- QHE.Dec アルゴリズム
  秘密鍵 sk_{L+1} を使用して QOTP の鍵を復号し,x' および z' を取得する. そして, これらを用いて m' を復元する.

3.1.3 量子可能古典暗号方式 (quantum capable classical encryption scheame)

暗号化された CNOT 演算子を構築するにあたり, トラップドアクローフリー関数ペアとして (3.4)(3.5) が用いられた. 本手法で使用される FHE には二つの特性が要求される. 一つ目は, 準同型 XOR 演算によるノイズの増加が加算的である必要がある. 準同型計算では評価のたびにノイズが増加する特性があるため, 準同型 XOR 演算によるノイズの影響で理想的な状態とは完全に一致しない.FHE では加算によるノイズはほとんど計算に影響しない性質を持つため, 準同型 XOR によるノイズの増加が加算的であることが要求される. 二つ目の特性はランダム性の回復である.FHE の復号アルゴリズムは平文のみ出力するが,Toffoli ゲートによる鍵の更新 (3.7) には平文だけでなく r_0, r_1 が必要となる. したがって, 暗号文 y からランダム性を復元できるトラップドア t_{sk} が存在することが要求される. 一般的にこの二つの特性を満たす FHE 方式はなく,Mahadev はある FHE に以下の条件を満たす AltHE(Alternative Encryption Scheme) が存在する場合, 古典準同型暗号化方式を量子対応準同型暗号と定義した.

1. HE の暗号文 c, サーバは c を AltHE の暗号文 $\hat{c}$ に変換できなければならない.
2. AltHE の準同型 XOR 演算のノイズが加算的である.

3. AltHE で暗号化された分布 $f_0(D)$ が存在し,$\hat{c}$ の準同型 XOR によるシフト後も同じままであり, 重ね合わせを効率的に構築可能である. さらに適切な秘密鍵 sk とトラップドア情報 t_{sk} により AltHE に基づく暗号文の復号とランダム性の回復の両方が可能である.

Mahadev は [Reg05] の dual を [GSW13] により FHE に拡張した,DualHE が量子可能であることを示した.

第4章　提案手法

MahadevはCNOTを暗号化することでToffoliゲートの準同型評価を実現した.Mahadevが提案した手法では非クリフォードゲートであるToffoliゲートを評価した際に三回暗号化されたCNOT演算子を作用させる必要がある.暗号化されたCNOT演算子は重ね合わせ状態でAltHEの準同型XORを計算する必要があるため効率的とは言えない.

本研究ではMahadevのプロトコルを効率的にするため,別のユニバーサル量子ゲートセット$\{\mathsf{X},\mathsf{Z},\mathsf{H},\mathsf{S},\mathsf{CNOT},\mathsf{T}\}$のTゲートの準同型評価を実現した.従来の手法では非クリフォードゲートの準同型評価に暗号化されたCNOT演算子が3回行う必要があったが,1回作用するだけで評価が可能になった.

4.1　Tゲートの準同型評価

Tゲートの準同型評価の手法を示す.QPTPされた量子状態にTゲートを作用したとき量子状態は

$$\mathsf{T}(\mathsf{X}^x\mathsf{Z}^z)\left|\psi\right\rangle = \mathsf{T}(\mathsf{X}^x\mathsf{Z}^z)\mathsf{T}^\dagger\mathsf{T}\left|\psi\right\rangle \tag{4.1}$$

でありTゲートは共役の下でパウリを以下のようにクリフォードとパウリの積に変換する.

$$\mathsf{T}(\mathsf{X}^x\mathsf{Z}^z)\mathsf{T}^\dagger = \mathsf{S}^x\mathsf{X}^x\mathsf{Z}^z$$

Tゲートの操作を完了するためにはToffoliゲートの時と同様に$\mathsf{S}^\dagger$ゲートを$\mathsf{Enc}(s)$のsで制御する必要がある.$\mathsf{S}^\dagger$ゲートは

$$\left|a\right\rangle \to (-i)^a\left|a\right\rangle$$

と変換するゲートであるため$\mathsf{S}^\dagger$ゲートをsで制御すると

$$\left|a\right\rangle \to (-i)^{a\cdot s}\left|a\right\rangle$$

$\mathsf{S}^\dagger$の暗号化はトラップドアクローフリー関数ペアを使って次のようにできる.まず(3.1)を1量子ビットで作る.

$$\sum_{a,\mu\in\{0,1\},r\in\mathcal{R}} \alpha_a\left|a\right\rangle\left|\mu,r\right\rangle\left|f_a(\mu,r)\right\rangle$$

この状態で第三レジスタを測定し、結果を $y = f_a(\mu_a, r_a)$ とすると

$$\sum_{a\in\{0,1\}} \alpha_a |a\rangle |\mu_a, r_a\rangle$$

第二レジスタに S ゲートを作用させる.

$$\sum_{a\in\{0,1\}} i^{\mu_a}\alpha_a |a\rangle |\mu_a\rangle |r_a\rangle$$

$s = 0$ のとき $\mu_0 = \mu_1$ となるためこの変換で変化も起きない.$\mu_0 = 1, \mu_1 = 0$ のとき $i|0\rangle|\mu_0\rangle|r_0\rangle + |1\rangle|\mu_1\rangle|r_1\rangle$ となる. これは 1 量子ビット目に $\mathsf{S}^\dagger$ ゲートを作用させたことと等価であり、S ゲートのエラーを打ち消せる.$\mu_0 = 0, \mu_1 = 1$ のとき $|0\rangle|\mu_0\rangle|r_0\rangle + i|1\rangle|\mu_1\rangle|r_1\rangle$ となり 1 量子ビット目に S ゲートを作用させたことと等価になる.
よって

$$((\mathsf{S}^\dagger)^{\mu_0}\mathsf{S}^{\mu_1} \otimes \mathbb{I}^{\otimes 2}) \sum_{a\in\{0,1\}} \alpha_a |a\rangle |\mu_a, r_a\rangle$$

ここで $\mathsf{ZS}^\dagger = \mathsf{S}, (\mathsf{S}^\dagger)^2 = \mathsf{Z}$ より

$$\begin{aligned}&(\mathsf{Z}^{\mu_1}(\mathsf{S}^\dagger)^{\mu_0}(\mathsf{S}^\dagger)^{\mu_1} \otimes \mathbb{I}^{\otimes 2}) \sum_{a\in\{0,1\}} \alpha_a |a\rangle |\mu_a, r_a\rangle \\ =&(\mathsf{Z}^{\mu_1\oplus\mu_0\cdot\mu_1}(\mathsf{S}^\dagger)^s \otimes \mathbb{I}^{\otimes 2}) \sum_{a\in\{0,1\}} \alpha_a |a\rangle |\mu_a, r_a\rangle\end{aligned}$$

2,3 キュービット目をアダマール測定し、測定結果が d だったとき

$$\mathsf{Z}^{d\cdot((\mu_0,r_0)\oplus(\mu_1,r_1))}\mathsf{Z}^{(\mu_1\oplus\mu_0\cdot\mu_1)}(\mathsf{S}^\dagger)^s \sum_a \alpha_a |a\rangle \tag{4.2}$$

よって T ゲートを作用させた (4.1) の状態に (4.2) を作用させ

$$(\mathsf{Z}^{d\cdot((\mu_0,r_0)\oplus(\mu_1,r_1))}\mathsf{Z}^{(\mu_1\oplus\mu_0\cdot\mu_1)}(\mathsf{S}^\dagger)^s\mathsf{S}^x\mathsf{X}^x\mathsf{Z}^z |\psi\rangle$$

$s = x$ とすることでクリフォード演算子を削除する. その後、CNOT のときと同様に鍵を

$$z' = z \oplus ((\mu_1 \oplus \mu_0\cdot\mu_1) \oplus (d\cdot((\mu_0, r_0)\oplus(\mu_1, r_1))))$$

と更新する.

第5章　おわりに

Mahadev の暗号化された CNOT 演算子の手法を応用し,$\mathsf{S}^\dagger$ を暗号化することで T ゲートの準同型評価が可能であることを示した. この結果, 従来の Toffoli ゲートでは三回必要とされた非クリフォードゲートの準同型評価によるクリフォードのエラー修正を,T ゲートでは一回での修正で達成可能となった. 本研究では,$\{\mathsf{X}, \mathsf{Z}, \mathsf{H}, \mathsf{S}, \mathsf{CNOT}, \mathsf{T}\}$ に基づくの準同型評価の実現を示したが,Mahadev の暗号化された CNOT と $S^\dagger$ の暗号化を組み合わせることで別のユニバーサル量子ゲートの準同型評価を可能にできると考えられる. 例えば Zhen-Wen Chen らは QHE における非クリフォードとして $\{\mathsf{CV}, \mathsf{CV}^\dagger\}$ を挙げている [CCX+24]. ここで,V ゲートは $\mathsf{V}^2 = \mathsf{X}$ を満たし,CV は制御 V を表す.QOTP で暗号化された状態に非クリフォードゲート $\{\mathsf{CV}, \mathsf{CV}^\dagger\}$ を作用させるとそれぞれ以下のようになる.

$$
\begin{aligned}
&\mathsf{CV}_{1,2}(\mathsf{X}^{x_1}\mathsf{Z}^{z_1} \otimes \mathsf{X}^{x_2}\mathsf{Z}^{z_2}) \left|\psi\right\rangle \\
&= (\mathsf{S}^{z_2} \otimes \mathsf{V}^{x_1})\mathsf{CNOT}_{1,2}^{x_1 \oplus z_2}(\mathsf{X}^{x_1}\mathsf{Z}^{z_1 \oplus x_1 z_2} \otimes \mathsf{X}^{x_2 \oplus x_1 \oplus x_1 z_2}\mathsf{Z}^{z_2})\mathsf{CV}_{1,2} \left|\psi\right\rangle \\
&\mathsf{CV}^\dagger{}_{1,2}(\mathsf{X}^{x_1}\mathsf{Z}^{z_1} \otimes \mathsf{X}^{x_2}\mathsf{Z}^{z_2}) \left|\psi\right\rangle \\
&= (\mathsf{S}^{z_2} \otimes \mathsf{V}^{x_1})\mathsf{CNOT}_{1,2}^{x_1 \oplus z_2}(\mathsf{X}^{x_1}\mathsf{Z}^{z_1 \oplus x_1 z_2 \oplus z_2} \otimes \mathsf{X}^{x_2 \oplus x_1 z_2}\mathsf{Z}^{z_2})\mathsf{CV}^\dagger{}_{1,2} \left|\psi\right\rangle
\end{aligned}
$$

ここで,$\mathsf{V} = \mathsf{HSH}$ を満たすため,S および,CNOT ゲートを暗号化可能であればば $\{\mathsf{CV}, \mathsf{CV}^\dagger\}$ によるクリフォードエラーを削除することができる. このことは,Mahadev の手法を他の非クリフォードゲートにも適用できることを示唆している.

今後の課題として,Mahadev の量子 leveledFHE を他の非クリフォードゲートでもできることを明確に示すことが必要である. これにより, 量子計算の内容に応じて最適なユニバーサル量子ゲートセットの組み合わせを選択することが可能となり,QHE による量子計算の効率性がさらに向上するものと期待される.

謝辞

本研究を進めるにあたり、研究や論文の添削をはじめ、終始適切な助言を賜り、丁寧にご指導くださった藤﨑 英一郎先生に、心より感謝申し上げます。先生のご指導と励ましがなければ、本研究を完成させることはできませんでした。

また、藤﨑研究室のメンバーの皆様には、輪講での議論をはじめ、日々の何気ない会話を通じて支えられ、研究を続ける活力を得ることができました。皆様のおかげで最後まで研究をやり遂げることができ、心より感謝申し上げます。

参考文献

[AMTdW00] Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald de Wolf. Private quantum channels. In *41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12-14 November 2000, Redondo Beach, California, USA*, pages 547–553. IEEE Computer Society, 2000.

[BJ15] Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low t-gate complexity. In *Annual Cryptology Conference*, pages 609–629. Springer, 2015.

[CCX+24] Zhen-Wen Cheng, Xiu-Bo Chen, Gang Xu, Li Ma, and Zong-Peng Li. Quantum one-time pad-based quantum homomorphic encryption schemes for circuits of the non-clifford gates. *Physica A: Statistical Mechanics and its Applications*, 637:129529, 2024.

[CGGI18] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. TFHE: Fast fully homomorphic encryption over the torus. Cryptology ePrint Archive, Paper 2018/421, 2018.

[Chi05] Andrew M. Childs. Secure assisted quantum computation. *Quantum Inf. Comput.*, 5(6):456–466, 2005.

[DSS16] Yfke Dulek, Christian Schaffner, and Florian Speelman. Quantum homomorphic encryption for polynomial-sized circuits. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III*, volume 9816 of *Lecture Notes in Computer Science*, pages 3–32. Springer, 2016.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In Michael Mitzenmacher, editor, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 169–178. ACM, 2009.

[Got98] Daniel Gottesman. The heisenberg representation of quantum computers. *arXiv preprint quant-ph/9807006*, 1998.

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 75–92. Springer, 2013.

[Mah18] Urmila Mahadev. Classical homomorphic encryption for quantum circuits. In Mikkel Thorup, editor, *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, pages 332–338. IEEE Computer Society, 2018.

[NC10] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 84–93. ACM, 2005.