修 士 論 文

秘密量子信号処理

令和 5年度 修了

三重大学　大学院工学研究科　情報工学専攻
コンピュータソフトウェア研究室

西窪 勇人

概 要

量子計算は古典計算と比較して，特定の問題について優位に計算を行うことができることが様々な研究で立証されており，現在注目を集めている．中でも，量子信号処理 (QSP) という Low と Chuang によって提案された，1 量子ビットの回転行列の回転角を変換する技術は一際注目が集められている．この技術は元来，核磁気共鳴における信号強度を増幅するための手法であったが，量子情報科学における重要な問題の一つであるハミルトニアンシミュレーションに対して最適なアルゴリズムを提供することなども証明されており，その応用可能性について広く研究が行われている．具体的には Maslov らによる 1 量子ビットメモリ上での対称ブール関数の計算などがある．古典計算では 1 ビットメモリ上で対称ブール関数を計算することは不可能であることが知られており，この結果は量子計算の優位性を示していることが分かる．この計算プロトコルにおいて，QSP は 1 量子ビットメモリで計算するための核を担っている．

本研究では QSP について暗号理論の観点からその応用可能性について検討し，その結果，新たな応用として秘密量子信号処理 (PQSP) を提案する．PQSP は秘密同時通信 (PSM) と呼ばれる計算モデルにおいて QSP を実行するプロトコルである．具体的には，それぞれが QSP の回転角に関する秘密の入力をもつ n 人の参加者が，一人の独立した評価者を通じて QSP の出力ユニタリ行列を計算するというものである．PQSP では評価者に対して各参加者が持つ秘密の入力が，出力から洩れる情報以上に洩れることがないことを保証しつつ，参加者から評価者へ送信されるメッセージの通信量が無限の場合は完全に正しい計算結果を得ることができる．ただし，通信量を有限とするためには各参加者の送信するメッセージを有限精度で表現する必要があり，その際には PQSP が最終的に出力する行列に誤りが発生する．よって，本研究ではこの精度と誤りのトレードオフについての評価も行う．

PQSP の応用例として，先述の Maslov らによる 1 量子ビットメモリ上での対称ブール関数の計算が挙げられる．本研究では，Maslov らの手法で使用されている QSP を PQSP と置換することで，1 量子ビットメモリ上で対称ブール関数を計算することができるという優位性はそのままに，PSM モデルにおいて評価者に対して出力情報以上を洩らさずに計算が可能であることを示した．

また，本研究では Cosentino らによって提案された 1 量子ビットプロトコルに対して PQSP で用いる秘匿化手法を適用することで，PSM モデルにおいて 1 量子ビットメモリ上で任意のブール関数を計算することが可能なプロトコルである秘密 1 量子ビットプログラム (P1QP) を提案する．P1QP は PQSP の応用で計算可能な対称ブール関数より大きな関数クラスに属する任意のブール関数を計算可能であることから，より一般的であるといえる．

目 次

第1章　はじめに

1.1　研究背景

現代の様々なサービスはインターネットなどを介した通信を行うことで維持，提供されている．これらがある日突然すべて使用不可能になったとしたらどのようなことが想定できるだろうか．おそらく多くの人々が今までの生活を維持できなくなり，大きな社会問題に発展することは容易に想像がつくだろう．現在，通信を暗号化する手法として，素因数分解問題や離散対数問題などの計算が難しい問題を用いた暗号プロトコルを利用することが一般的である．これは，現代の通信は素因数分解問題や離散対数問題を現実的な時間 (多項式時間) で計算可能なアルゴリズムが存在しない限り，安全に実行可能であるということを意味している．しかし，これらの問題は量子計算機上で実行可能な shor のアルゴリズム [Sho97] を用いることで，多項式時間で計算可能であることが知られている．現時点ではこのアルゴリズムを実行できる量子計算機は存在しておらず，直ちに実社会に影響があるというわけではないが，着実にその開発は進んでいるというのが実状である．これらの状況を鑑み，NIST は量子計算を用いても復号することが難しい耐量子暗号の標準化を進めている [NIS17].

このように，量子計算を用いることで特定の問題について現在知られている古典計算における最適なアルゴリズムに対して，ある優位性をもって計算を行うことが可能であることが示されており，量子計算の計算能力について広く研究されている．先の素因数分解を行う Shor のアルゴリズムや，探索を行う Grover のアルゴリズム [Gro96] などが有名である．また，量子状態の特性である量子もつれを利用した暗号プロトコルなども考案されている．Bennett と Brassard により提案された量子鍵配送プロトコル [BB84] は，古典計算における鍵配送プロトコルで達成することが困難であると予想されている情報理論的安全性を達成する．これを利用することで，素因数分解問題の困難性などの仮定を置くことなく安全に実行可能な暗号通信プロトコルを構成することができる．

他にも，Low らによって提案された量子信号処理 (Quantum Signal Processing, QSP) という 1 量子ビット上の量子演算の回転角を変換する技術がある [LC17, LYC16]．QSP は元来，核磁気共鳴における信号強度を増幅するための手法であったが，同時期に量子情報科学における重要な問題の一つであるハミルトニアンシミュレーションに対して最適なアルゴリズムの提供が可能であることも証明されており，その応用技術についても研究されている．応用例として，Gilyén らにより提案された量子特異値変換 (Quantum Singular Value Transformation, QSVT)[GSLW19] と呼ばれる QSP の一般化がある．QSVT を用いることで，先の Grover の探索アルゴリズムや逆行列計算を高速に計算することができる HHL アルゴリズム [HHL09] など，様々な量子アルゴリズムを統一的に記述することが可能であり，現在広く注目を集めている．(解説論文として [MRTC21] が詳しい.)

また，他の応用として Maslov らによる 1 量子ビットメモリを用いた対称ブール関数の計算 [MKB$^+$21] がある．古典計算では対称ブール関数を 1 ビットメモリを用いて計算することが不可能であるということが知られており [AGK$^+$05]，この結果は量子計算の優位性を示

している．この構成において，QSP は対称ブール関数を計算するユニタリ行列を生成する際に使用される．

Maslov らによる 1 量子ビットメモリで対称ブール関数を計算する手法に関連して，Cosentino らによる 1 量子ビットメモリで任意のブール関数を計算する手法 [CKP13] がある．対称ブール関数はブール関数に含まれることから，Cosentino らの結果はより強力なものであるといえる．

1.2 本研究の成果

本研究では暗号理論の観点から QSP の応用を検討する．秘密同時通信 (Private Simultaneous Messages, PSM) と呼ばれる秘密計算のモデルでは，各参加者 $P_1, \ldots, P_n$ は秘密の入力 $x_1, \ldots, x_n$ を持っており，その入力と，入力に依存しない事前共有乱数に基づいて生成されるメッセージを評価者に同時に送信する．評価者は各参加者からのメッセージを基に関数の出力値 $f(x_1, \ldots, x_n)$ を計算できるが，評価者が知り得る情報は出力値 $f(x_1, \ldots, x_n)$ のみであり，出力値から知り得ない各参加者の入力に関する情報などは知ることができない．

本研究では，この PSM モデルにおいて，各参加者の秘密の入力によって決まるユニタリ行列を QSP で変換しつつも，最終的に得られるユニタリ行列以外の情報について評価者は知り得ない，という秘密量子信号処理 (Private QSP, PQSP) を提案する．PQSP では秘匿化のために Haar ランダムユニタリ行列によって送信するユニタリ行列をランダム化するが，通信量を有限にするためには送信するメッセージを有限精度で表現する必要があり，その丸めによって PQSM で得られる最終的なユニタリ行列に誤りが発生する．本研究ではそのユニタリ行列の精度と誤りに対するトレードオフの評価も行う．

PQSP を 1 量子ビットメモリを用いた対称ブール関数の計算で使用される QSP と置き換えることで，[MKB+21] で示されている量子計算の優位性はそのままに，入力情報および関数情報を秘匿化した状態で計算を行うことができるというアドバンテージを付加することが可能となる．つまり，対称ブール関数を複数の古典参加者と独立した量子評価者で計算するモデルの場合，評価者のメモリが 1 量子ビットであったとしても計算が可能であり，かつ，古典参加者の入力情報および関数情報を秘匿することが可能である．

また，PQSP で用いた秘匿化手法を用いることで，Cosentino らの結果を PSM モデルで実行することが可能な，秘密 1 量子ビットプログラム (Private 1-qubit Program, P1QP) というプロトコルについても提案する．このプロトコルを用いることで，上記の対称ブール関数以上の関数である任意のブール関数を PSM モデルにおいて 1 量子ビットメモリで計算することが可能となる．

1.3 関連研究

量子情報に基づいた PSM プロトコルとその亜種については既にいくつか研究が知られている．

河内と西村は PSM モデルの量子版である PSQM(Private Simultaneous Quantum Messages) を提案した [KN21]．PSQM において各参加者は自身の古典入力と事前共有乱数あるいは事前共有エンタングルメントから量子メッセージを評価者に送信し，評価者は量子メッセージから古典出力を計算する．彼らはいくつかの関数について情報理論的安全性をもつ

PSQM プロトコルを示し，古典通信による PSM プロトコルでは達成できない通信複雑度を量子通信によって達成できることを示した．

Brakerski と Yuen は量子分割可能乱択符号化 (Quantum Decomposable Randomized Encoding, QDRE) を提案している [BY22]．乱択符号化 (Randomized Encoding, RE) とは秘密計算の実現技術の一つであり，入力を $x = (x_1, \ldots, x_n)$ とする関数 f について，あるランダムな要素 r を用いて $f(x)$ よりも簡単な $\hat{f}(x, r)$ を計算し，そこからもとの出力 $f(x)$ を得るような技術である．また，符号化 $\hat{f}(x, r)$ を $(\hat{f}_0(r), \hat{f}_1(x_1, r), \ldots, \hat{f}_n(x_n, r))$ と分割できるような RE を分割可能乱択符号化 (Decomposable Randomized Encoding, DRE) という．DRE を応用することで PSM プロトコルを構成することが可能であることが一般的に知られており，よって QDRE から量子版 PSM プロトコルを構成可能である．

PQSP および P1QP の構成と上記 [KN21] および [BY22] の相違点は，各参加者が量子計算能力を持つか，古典計算能力しか持たないかという点と，計算内容が古典関数であるか，量子回路であるかという点である．PQSP および P1QP では各参加者は古典計算能力しか持ちえないが，[KN21, BY22] では量子計算能力を持つ．計算の対象については，PQSP 及び P1QP，[KN21] は古典関数を，[BY22] は量子回路を計算するプロトコルを与えている．

また，PQSP および P1QP は 1 量子ビットメモリで実行可能であるのに対して，既存 2 手法はこれが不可能である．1 量子ビットメモリの量子計算機は既に存在していることを考慮すると，PQSP および P1QP は現時点で実装が可能であるのに対し，既存 2 手法を実装することは困難であるといえる．つまり，PQSP および P1QP は PSM 量子プロトコルの最初のテストケースと成り得る．量子計算における秘密計算の有用性および課題点の評価を行うためにも，PQSP および P1QP は重要なツールであるといえる．

第2章　準備

2.1　代数学

本節では本研究の成果を述べる上で必要となる代数学の前提知識について記述する．

2.1.1　エルミート行列とユニタリ行列

量子情報科学において，エルミート行列とユニタリ行列は非常に重要な行列であり，本研究の説明にあたっても避けては通れない．ここではエルミート行列とユニタリ行列について記述する．

はじめに随伴行列を定義する．

定義 2.1.1 (随伴行列) 行列 $A \in \mathbb{C}^{m\times n}$ について，A の各要素について複素共役をとり，それを転置させた行列を A の随伴行列といい，$A^\dagger$ で表す．ただし，”†”は複素共役転置を表す．

次にエルミート行列およびユニタリ行列を定義する．

定義 2.1.2 (エルミート行列) 正方行列 $A \in \mathbb{C}^{n\times n}$ について，$A = A^\dagger$ を満たすような正方行列 A をエルミート行列という．これは，$A^\dagger = A^{-1}$，つまり逆行列と随伴行列が等しいことを意味している他，正則であることも意味している．

定義 2.1.3 (ユニタリ行列) 正方行列 $U \in \mathbb{C}^{n\times n}$ について，$UU^\dagger = U^\dagger U = \mathbb{I}$ を満たすような正方行列 U をユニタリ行列という．また，$\det U = 1$ となるユニタリ行列を特殊ユニタリ行列という．

ユニタリ行列は $U^\dagger = U^{-1}$，つまり逆行列と随伴行列が等しいので正則である．また，ユニタリ行列の行列式は必ず $|\det U| = 1$ を満たす．エルミート行列 A は $A = A^\dagger = A^{-1}$ なので，ユニタリ行列でもある．

ユニタリ行列は積に関して結合法則が成り立ち，単位元 $\mathbb{I}$ および逆元が存在する．よって，すべてのユニタリ行列からなる集合は積に関して群を成す．この群をユニタリ群といい，$\mathrm{U}(n)$ で表す．同様に，すべての特殊ユニタリ行列からなる集合も積に関して群を成す．この群を特殊ユニタリ群といい，$\mathrm{SU}(n)$ で表す．

2.1.2　行列ノルム

ここでは本研究を解説する際に使用する作用素ノルムおよびフロベニウスノルムについて記述する．一部の記述は本研究で使用することを考慮し，一般的な解釈とは異なる場合があることに注意されたい．

はじめに，行列ノルムの定義を行う．

定義 2.1.4 (行列ノルム) $A, B \in \mathbb{C}^{n\times n}$ および $c \in \mathbb{C}$ としたとき，以下の 4 つの条件を満たす関数 $\|\cdot\| : \mathbb{C}^{n\times n} \to \mathbb{R}$ を行列ノルムという．

- $\|A\| \geq 0 \quad \text{iff } A = O$
- $\|cA\| \leq |c|\|A\|$
- $\|A + B\| \leq \|A\| + \|B\|$
- $\|AB\| \leq \|A\|\|B\|$

ただし，O は零行列である．

次に，作用素ノルムとフロベニウスノルムの定義を行う．

定義 2.1.5 (作用素ノルム) 行列 $A \in \mathbb{C}^{n\times n}$ を内積空間の線形作用素とする．このとき，

$$\|A\|_{op} := \max_{x\neq 0} \frac{\|Ax\|}{\|x\|} = \max_{\|x\|=1} \|Ax\|$$

を作用素ノルムという．

定義 2.1.6 (フロベニウスノルム) 正則行列 $A \in \mathbb{C}^{n\times n}$ について，

$$\|A\|_F := \sqrt{\sum_{i,j} |a_{ij}|^2} = \sqrt{\mathrm{tr}(AA^\dagger)} = \sqrt{\mathrm{tr}(A^\dagger A)}$$

をフロベニウスノルムという．

最後に，作用素ノルムとフロベニウスノルムの関係についての定理を紹介する．

定理 2.1.7 正則行列 $A \in \mathbb{C}^{n\times n}$ について，

$$\|A\|_{op} \leq \|A\|_F$$

が成り立つ．

定理 2.1.7 を証明するにあたり，二つの補題を証明する．

補題 2.1.8 行列 $A \in \mathbb{C}^{n\times n}$ について，

$$\|A\|_{op} = \sigma_1$$

が成り立つ．ただし，σ_1 は A の最大特異値である．

補題 2.1.8 の証明. 行列 $A \in \mathbb{C}^{n\times n}$ について，特異値分解を行うと，

$$A = U\Sigma V^\dagger$$

となる．ただし，$U, V \in \mathbb{C}^{n\times n}$ はユニタリ行列であり，Σ は A の特異値 $(\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_n)$ の対角行列 $\mathrm{diag}(\sigma_1, \sigma_2, \ldots, \sigma_n)$ である．

これを用いて A の作用素ノルムを表すと，

$$\|A\|_{op} = \max_{\|x\|=1} \|Ax\| = \max_{\|x\|=1} \left\|U\Sigma V^\dagger x\right\| \tag{2.1}$$

となる．U, V はユニタリ行列であり，$x \in \mathbb{C}^n$ について $\|Ux\| = \|x\|$ が成り立つことから，式 (2.1) は，

$$\begin{aligned}
\|A\|_{op} &= \max_{\|x\|=1} \left\|U\Sigma V^\dagger x\right\| \\
&= \max_{\|y\|=1} \|\Sigma y\| \\
&= \max_{\|y\|=1} \sqrt{\sigma_1^2|y_1|^2 + \sigma_2^2|y_2|^2 + \cdots + \sigma_n^2|y_n|^2} \\
&= \sigma_1
\end{aligned}$$

となる．ここで，$y = V^\dagger x$ である． □

補題 2.1.9 正則行列 $A \in \mathbb{C}^{n\times n}$ について，

$$\|A\|_F = \sqrt{\sum_i \sigma_i^2}$$

が成り立つ．ただし，$\sigma_1, \sigma_2, \ldots, \sigma_n$ は A の特異値である．

補題 2.1.9 の証明. 行列 $A \in \mathbb{C}^{n\times n}$ について，特異値分解を行うと，

$$A = U\Sigma V^\dagger$$

となる．ただし，$U, V \in \mathbb{C}^{n\times n}$ はユニタリ行列であり，Σ は A の特異値の対角行列 $\mathrm{diag}(\sigma_1, \sigma_2, \ldots, \sigma_n)$ である．これを用いて A のフロベニウスノルムを表すと，

$$\begin{aligned}
\|A\|_F &= \left\|U\Sigma V^\dagger\right\|_F \\
&= \sqrt{\mathrm{tr}((U(\Sigma V^\dagger))^\dagger U\Sigma V^\dagger)} \\
&= \sqrt{\mathrm{tr}((\Sigma V^\dagger)^\dagger U^\dagger U\Sigma V^\dagger)} \\
&= \sqrt{\mathrm{tr}((\Sigma V^\dagger)^\dagger \Sigma V^\dagger)} \\
&= \sqrt{\mathrm{tr}(\Sigma V^\dagger V\Sigma^\dagger)} \\
&= \sqrt{\mathrm{tr}(\Sigma\Sigma^\dagger)} \\
&= \|\Sigma\|_F \\
&= \sqrt{\sum_i \sigma_i^2}
\end{aligned}$$

となる．ここで，$\|A\|_F = \sqrt{\mathrm{tr}(AA^\dagger)} = \sqrt{\mathrm{tr}(A^\dagger A)}$ を用いた． □

定理 2.1.7 の証明. 正則行列 $A \in \mathbb{C}^{n\times n}$ について $\|A\|_{op} \le \|A\|_F$ が成り立つことは，補題 2.1.8 および補題 2.1.9 からすぐに分かる． □

2.1.3 行列指数関数

量子情報科学において，ユニタリ行列は量子状態を変化させるために使用される．また，この行列は 2 つの回転行列を用いて表現することができる．よって，回転行列を理解することはユニタリ行列を理解する上で非常に有用である．ここでは，回転行列を表す行列指数関数について簡単に記述する．

行列指数関数 $R(\theta) = \exp\left(-i\frac{\theta}{2}A\right)$ とする．ただし，$A \in \mathbb{C}^{2\times 2}$ はエルミート行列である．マクローリン展開を用いることで，$R(\theta)$ を以下のように書くことができる．

$$\begin{aligned}
R(\theta) &= \exp\left(-i\frac{\theta}{2}A\right) \\
&= \sum_n \frac{1}{n!}\left(-\frac{\theta}{2}A\right)^n \\
&= \mathbb{I} + \left(-i\frac{\theta}{2}A\right) + \frac{1}{2!}\left(-i\frac{\theta}{2}A\right)^2 + \frac{1}{3!}\left(-i\frac{\theta}{2}A\right)^3 + \cdots \\
&= \mathbb{I} + \left(-i\frac{\theta}{2}\right)A + \frac{1}{2!}\left(-i\frac{\theta}{2}\right)^2\mathbb{I} + \frac{1}{3!}\left(-i\frac{\theta}{2}\right)^3 A + \cdots \\
&= \sum_n \frac{(-i)^{2n}}{2n!}\left(\frac{\theta}{2}\right)^{2n}\mathbb{I} - i\sum_n \frac{(-i)^{2n}}{(2n+1)!}\left(\frac{\theta}{2}\right)^{2n+1}A \\
&= \sum_n \frac{(-1)^n}{2n!}\left(\frac{\theta}{2}\right)^{2n}\mathbb{I} - i\sum_n \frac{(-1)^n}{(2n+1)!}\left(\frac{\theta}{2}\right)^{2n+1}A \qquad (2.2)
\end{aligned}$$

ここで，$\mathbb{I}$ は 2 次元の単位行列である．式 (2.2) において，$\sum_n \frac{(-1)^n}{2n!}\left(\frac{\theta}{2}\right)^{2n}$ は $\cos\left(\frac{\theta}{2}\right)$ についての，$\sum_n \frac{(-1)^n}{(2n+1)!}\left(\frac{\theta}{2}\right)^{2n+1}$ は $\sin\left(\frac{\theta}{2}\right)$ についてのマクローリン展開になっていることが分かるので，回転行列 $R(\theta)$ は

$$\begin{aligned}
R(\theta) &= \exp\left(-i\frac{\theta}{2}A\right) \\
&= \cos\left(\frac{\theta}{2}\right)\mathbb{I} - i\sin\left(\frac{\theta}{2}\right)A
\end{aligned}$$

と書くことができる．

2.2 量子情報科学

本節では本研究を述べる上で必要となる量子情報科学の前提知識について，[石小河 +12] を参考に記述する．より詳しい内容についてはこの文献を参照されたい．

2.2.1 Dirac の表記法

量子状態は複素ベクトルで表現することが可能であり，量子情報科学ではこれらの複素ユークリッド空間 $\mathbb{C}^d$ を Dirac の表記法で表記することが一般的である．

Dirac の表記法を使用すると $a_1, \ldots, a_d \in \mathbb{C}$ としたとき，列ベクトルはケットベクトル”$|\rangle$”を用いて，共役な行ベクトルはブラベクトル”$\langle|$”を用いてそれぞれ

$$|\psi\rangle := \begin{bmatrix} a_1 \\ \vdots \\ a_d \end{bmatrix}, \quad \langle\psi| := [a_1^*, \ldots, a_d^*]$$

と表記される．ただし，a^* は a の複素共役である．このとき，$\langle\psi|$ は $|\psi\rangle$ の複素共役転置となっている．

また，$|\psi\rangle = (a_1, \ldots, a_d)^T \in \mathbb{C}^d$，$|\phi\rangle = (b_1, \ldots, b_d)^T \in \mathbb{C}^d$ とすると，$\langle\psi|\phi\rangle$ および $|\psi\rangle\langle\phi|$ はそれぞれ

$$\langle\psi|\phi\rangle := [a_1^*, \ldots, a_d^*] \begin{bmatrix} b_1 \\ \vdots \\ b_d \end{bmatrix} = \sum_{i=1}^{d} a_i^* b_i,$$

$$|\psi\rangle\langle\phi| := \begin{bmatrix} a_1 \\ \vdots \\ a_d \end{bmatrix} [b_1^*, \ldots, b_d^*] = \begin{bmatrix} a_1 b_1^* & \cdots & a_1 b_d^* \\ \vdots & \ddots & \vdots \\ a_d b_1^* & \cdots & a_d b_d^* \end{bmatrix}$$

となり，$\langle\psi|\phi\rangle$ は複素ユークリッド内積を，$|\psi\rangle\langle\phi|$ は行列を表す．

上式より，$\langle\psi|\psi\rangle$ は 0 以上であり，等号成立は $|\psi\rangle$ が 0 ベクトルであるときのみである．このことから，ベクトル $|\psi\rangle$ の大きさを定義可能である．

定義 2.2.1 (ユークリッドノルム) $|\psi\rangle \in \mathbb{C}^d$ について，

$$\||\psi\rangle\| := \sqrt{\langle\psi|\psi\rangle} = \sqrt{\sum_i |a_i|^2}$$

をユークリッドノルムと呼ぶ．

2.2.2 量子ビット

現在社会に広く普及している情報科学 (以降，古典情報科学) では，情報の単位としてビット (以降，古典ビット) が用いられている．これに対して，本研究で扱う量子情報科学では情報の単位として量子ビットを用いる．量子ビットは電子のスピンや光子の偏光などの物理量についての状態 (量子状態) であり，これらを複素数ベクトルで表現して古典ビットなどをラベル付けしたものである．単一量子ビットであれば 2 次元の複素ユークリッド空間 $\mathbb{C}^2$ で表現することが可能である．量子ビットは測定と呼ばれる操作において値を判別することが可能であればそのラベルは何でも良いが，ここでは古典ビット 0 と 1 を表現する量子ビットについて記述する．古典ビット 0 および 1 はそれぞれ量子ビット

$$|0\rangle := \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle := \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

で表す．また，$\{|0\rangle, |1\rangle\}$ は $\langle 0|1\rangle = \langle 1|0\rangle = 0$ かつ $\||0\rangle\| = \||1\rangle\| = 1$ であるので，$\mathbb{C}^2$ における正規直行基底となっている．以降，基底 $\{|0\rangle, |1\rangle\}$ を特別に計算基底と呼ぶ．

複素ユークリッド空間 $\mathbb{C}^2$ の任意の量子状態はこの空間における単位ベクトルで記述することが可能である．すなわち，上述の $|0\rangle$，$|1\rangle$ および $\alpha, \beta \in \mathbb{C}$ を用いて，

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.3}$$

と表現することができる．ただし，単位ベクトルである条件をみたすために，$|\alpha|^2 + |\beta|^2 = 1$ となる必要がある．また，量子ビットと単位ベクトルは一対一の対応をとるわけではなく，$|c| = 1$ となる $c \in \mathbb{C}$ について $|\psi'\rangle = c\,|\psi\rangle$ となるとき，$|\psi\rangle$ と $|\psi'\rangle$ は同じ量子ビットを表す．これを位相の不定性と呼び，c をグローバルフェーズと呼ぶ．

式 (2.3) は $|0\rangle$ と $|1\rangle$ のベクトルの和の状態であることが分かる．このような状態を重ね合わせ状態と呼ぶ．これは二値しかとり得ない古典ビットには無いものであり，量子ビット特有のものである．

以上が量子ビットの表現である．しかし，このままでは量子ビットは具体的な情報を得ることができない．量子ビットから具体的な情報を得るためには測定と呼ばれる操作を行う必要がある．

ここでは計算基底による測定を考える．式 (2.3) を例に考えると，量子ビット $|\psi\rangle$ から測定値 0 を得る確率は，

$$|\langle 0|\psi\rangle|^2 = |\alpha\,\langle 0|0\rangle + \beta\,\langle 0|1\rangle|^2 = |\alpha|^2$$

となる．測定値 1 を得る確率についても同様である．

量子計算では量子ビットに対してある操作を行い，最終状態を測定することで計算結果を得るということが一般的である．この操作はユニタリ行列 $U \in \mathbb{C}^{d\times d}$ を用いて表現することができる．実際に式 (2.3) の状態 $|\psi\rangle$ に対して，ユニタリ行列 $U \in \mathbb{C}^{2\times 2}$ で表される操作を行ってできる状態 $|\psi'\rangle$ は

$$\left|\psi'\right\rangle = U\,|\psi\rangle$$

と表現することができる．ここで，操作を行った後の状態 $|\psi'\rangle$ についても $\mathbb{C}^2$ の単位ベクトルとなっていることに注意されたい．

いくつかの有用性の高いユニタリ行列を紹介する．

$$\mathbb{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$\mathbb{I}$ は単位行列，X, Y, Z は Pauli 行列，H は Hadamard 行列と呼ばれるユニタリ行列である．X はビット反転を行う行列であり，$X\,|0\rangle = |1\rangle$，$X\,|1\rangle = |0\rangle$ となる．また，Z は位相反転と呼ばれる操作を行う行列であり，$Z\,|1\rangle = -\,|1\rangle$ となる．これらすべての行列は，自身と自身の複素共役転置をとった行列が等しいため，エルミート行列である．

2.2.3 Bloch 球と回転行列

量子ビットの数式的な表現については上記の通りである．ここでは，量子ビットの幾何学的表現を可能にする Bloch 球について紹介する．Bloch 球を用いることで，Pauli 行列を含む回転行列がどのような操作を行う行列であるかを視覚的に理解することが可能となる．

はじめに，量子ビットの数式表現について改めて考えると，任意の量子ビットの状態 $|\psi\rangle$ は実数パラメータ θ および φ を用いて

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + \exp(i\varphi)\sin(\theta/2)\,|1\rangle$$

と表現することも可能であることが分かる．これは，$0 \leq \theta \leq \pi$，$0 \leq \varphi \leq 2\pi$ とすることで，位相の不定性を除いたすべての量子状態を一対一で表現可能である．この 2 つのパラメータは 3 次元単位球 (2.1) を 3 次元極座標表示を用いて表現する際の，z 軸との角度 θ と x, y 平面の射影と x 軸との角度 φ という角度情報と同じ範囲を動く．このような球を Bloch 球という．

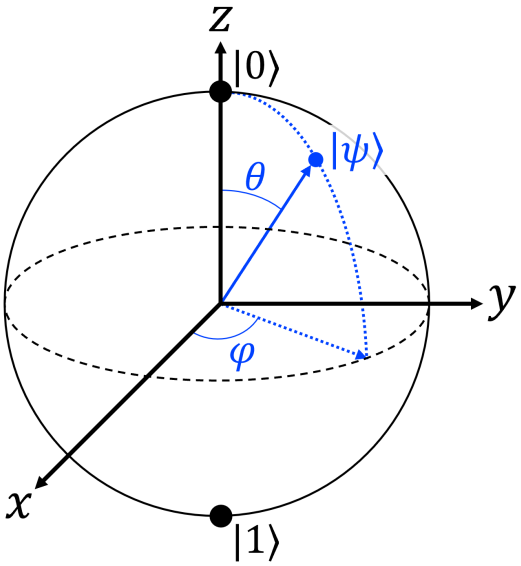

図 2.1: Bloch 球

Bloch 球における各軸を中心として任意の角度分回転させるような操作を行う行列 (回転行列) は以下のように書くことができる．

$$R_x(\theta) = \exp(-i(\theta/2)X) = \cos(\theta/2)\mathbb{I} - i\sin(\theta/2)X = \begin{bmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$$

$$R_y(\theta) = \exp(-i(\theta/2)Y) = \cos(\theta/2)\mathbb{I} - i\sin(\theta/2)Y = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$$

$$R_z(\theta) = \exp(-i(\theta/2)Z) = \cos(\theta/2)\mathbb{I} - i\sin(\theta/2)Z = \begin{bmatrix} \exp\left(-i\frac{\theta}{2}\right) & 0 \\ 0 & \exp\left(i\frac{\theta}{2}\right) \end{bmatrix}$$

これらの回転行列の θ に π を代入すると，Pauli 行列を得ることができる．ここから，Pauli 行列は状態をそれぞれの回転軸について π 回転させるような行列であるということが分かる．

2.2.4 Z-X 分解

1 量子ビットユニタリ行列 U はグローバルフェーズと 3 つの回転行列を用いることで表現が可能である．本論文では Z-X 分解と呼ばれる X, Z の Pauli 行列を用いた分解方法について記述する．

1 量子ビットユニタリ行列は

$$U = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}$$

で表現される．ただし，$u_{11}, u_{12}, u_{21}, u_{22} \in \mathbb{C}$ である．また，各 u は以下の条件を満たす．

- $|u_{11}|^2 + |u_{21}|^2 = 1$
- $u_{12}^* u_{11} + u_{22}^* u_{21} = 0$
- $|u_{22}|^2 + |u_{12}|^2 = 1$

ただし，u^* は u の複素共役である．

これを満たすような U として，

$$\begin{aligned}
u_{11} &= \exp\left(i\left(\alpha - \frac{\beta}{2} - \frac{\delta}{2}\right)\right)\cos\left(\frac{\gamma}{2}\right) \\
u_{12} &= -i\exp\left(i\left(\alpha - \frac{\beta}{2} + \frac{\delta}{2}\right)\right)\sin\left(\frac{\gamma}{2}\right) \\
u_{21} &= -i\exp\left(i\left(\alpha + \frac{\beta}{2} - \frac{\delta}{2}\right)\right)\sin\left(\frac{\gamma}{2}\right) \\
u_{22} &= \exp\left(i\left(\alpha + \frac{\beta}{2} + \frac{\delta}{2}\right)\right)\cos\left(\frac{\gamma}{2}\right)
\end{aligned}$$

が挙げられる．ただし，$\alpha \in [-\pi, \pi)$，$\beta \in [-2\pi, 2\pi)$，$\gamma \in [-2\pi, 2\pi)$，$\delta \in [-2\pi, 2\pi)$ である．実際，この U は $U^\dagger U = UU^\dagger = \mathbb{I}$ となることが確認できる．ただし，$U^\dagger$ は U の複素共役転置である．

この U を変形する．

$$\begin{aligned}
U =& e^{i\alpha}\begin{bmatrix} e^{i(-\beta-\delta)/2}\cos\left(\frac{\gamma}{2}\right) & -ie^{i(-\beta+\delta)/2}\sin\left(\frac{\gamma}{2}\right) \\ -ie^{i(\beta-\delta)/2}\sin\left(\frac{\gamma}{2}\right) & e^{i(\beta+\delta)/2}\cos\left(\frac{\gamma}{2}\right) \end{bmatrix} \\
=& e^{i\alpha}\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}\begin{bmatrix} \cos\left(\frac{\gamma}{2}\right) & -i\sin\left(\frac{\gamma}{2}\right) \\ -i\sin\left(\frac{\gamma}{2}\right) & \cos\left(\frac{\gamma}{2}\right) \end{bmatrix} \\
& \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix} \\
=& e^{i\alpha}\exp\left(-i\frac{\beta}{2}Z\right)\exp\left(-i\frac{\gamma}{2}X\right)\exp\left(-i\frac{\delta}{2}Z\right)
\end{aligned}$$

以降は見やすさを考慮して回転行列 $R_x(\theta), R_z(\theta)$ を用いて，

$$U = e^{i\alpha}R_z(\beta)R_x(\gamma)R_z(\delta)$$

と表現する．

2.3 Haar ランダムユニタリ行列

本節では本研究の成果で使用する Haar ランダムユニタリ行列について，[Ozo09] を参考に記述する．

2.3.1 Haar 測度

関数 f を $\mathbb{R}$ 上で定義された関数とする．このとき，任意の $a \in \mathbb{R}$ に対して

$$\int_{\mathbb{R}} f(x)\mathrm{d}x = \int_{\mathbb{R}} f(x+a)\mathrm{d}x$$

となる．これは，他の多くの並進不変性を持つ群であれば同じことがいえる．群 G の測度 μ を上手く選ぶことで，すべての $g \in G$ について

$$\int_G f(x)\mathrm{d}\mu(x) = \int_G f(gx)\mathrm{d}\mu(x)$$

となる．すべての $S \subseteq G$ と $g \in G$ に対して，非零測度 $\mu : G \to [0, \infty]$:

$$\mu(gS) = \mu(Sg) = \mu(S)$$

を Haar 測度とよぶ．ただし，

$$\mu(S) := \int_{g \in S} \mathrm{d}\mu(g)$$

である．

2.3.2 Haar ランダムユニタリ行列

本研究では 1 量子ビットを操作するユニタリ行列，すなわち，2×2 のユニタリ行列を使用する．よって，ここでは 2×2 の Haar ランダムユニタリ行列について記述する．

はじめに SU(2) を考え，次のようなパラメタライズを行う．

$$\mathrm{SU}(2) = \left\{ \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix} \in \mathbb{C}^{2\times 2} \;\middle|\; |a|^2 + |b|^2 = 1 \right\}$$

次に，$a := \exp(i\psi)\cos(\phi)$ および $b := \exp(i\chi)\sin(\phi)$ と設定し，グローバルフェーズ $\exp(i\alpha)$ を導入することで，次のように U(2) をパラメタライズする．

$$U(\alpha, \phi, \psi, \chi) := \exp(i\alpha) \begin{pmatrix} \exp(i\psi)\cos(\phi) & \exp(i\chi)\sin(\phi) \\ -\exp(-i\chi)\sin(\phi) & \exp(-i\psi)\cos(\phi) \end{pmatrix}$$

ここで，$0 \le \phi \le \frac{\pi}{2}$，$0 \le \alpha, \psi, \chi \le 2\pi$ である．このとき，U(2) 上の一様分布を得るために各パラメータに対してどのような確率分布を用いればよいかは分からない．このような場合，体積要素の式を用いると便利である．

$$\mathrm{d}V = \frac{1}{2}\sin(2\phi)\mathrm{d}\alpha\mathrm{d}\phi\mathrm{d}\psi\mathrm{d}\chi = \frac{1}{2}\,\mathrm{d}\big(\sin^2(\phi)\big)\,\mathrm{d}\alpha\mathrm{d}\psi\mathrm{d}\chi$$

ここから，$\alpha, \psi, \chi \in [0, 2\pi]$ および $\xi \in [0, 1]$ を一様ランダムに選択し，$\phi = \arcsin\big(\sqrt{\xi}\big)$ を計算することで良いことが分かる．

最後に，Haar ランダムユニタリ行列と任意のユニタリ行列の積をとった場合，その結果も Haar ランダムユニタリ行列となることを確認する．

定理 2.3.1 Haar ランダムユニタリ行列を R とすると，任意のユニタリ行列 U について RU は Haar ランダムユニタリ行列である．

2.3.1 の証明. 写像 $\mathcal{R}$ が全単射であることを示す．Haar ランダムユニタリ行列 R について $\mathcal{R}(U) = RU$ とする．ただし，U はユニタリ行列である．このとき，$\mathcal{R}(U_0) = RU_0 = U_0'$, $\mathcal{R}(U_1) = RU_1 = U_1'$ について

$$\begin{aligned} U_0' = U_1' &\longleftrightarrow RU_0 = RU_1 \\ &\longleftrightarrow U_0 = U_1 \end{aligned}$$

であることから単射である．
また，$^{\forall}V$, $^{\exists}U$, $\mathcal{R}(U) = V$ について，$U = R^{\dagger}V$ をとると $\mathcal{R}(R^{\dagger}V) = V$ であることから全射である．よって，写像 $\mathcal{R}$ は全単射であり，R は Haar 測度を保存していることから題意は示される． □

2.4 秘密計算

本節では本研究の成果を述べる上で必要となる暗号理論における秘密計算の前提知識について記述する．

2.4.1 Kilian の乱択化

Kilian の乱択化 [Kil88] とは，乗法群の要素の積を計算する際に要素を秘匿化する技術である．n 個の入力 $x_k \in G$(ただし，G は乗法群) の積を計算する関数 f を例に考える．n 人の参加者 P_k は入力 x_k をもち，独立した評価者は各参加者の入力を送信してもらい，代わりに関数 f の計算を行うものとする．このとき，$r_1, \ldots, r_{n-1}$ をそれぞれ G から一様ランダムに選択した要素とすると，Kilian の乱択化を用いることで，

$$x_k' = r_{k-1}^{-1} \cdot x_k \cdot r_k$$

を生成することが可能である．ただし，$k = 1, \ldots, n$ であり，r_0 および r_n は単位元である．
各参加者は得られた x_k' を x_k の代わりに評価者に送信する．評価者は送信されてきた x_k' について積をとることで $f(x)$ と等しい結果が得られる．また，各参加者から送信されてくる x_k' はランダムな要素により暗号化されているため，元の入力 x_k についての情報を評価者が知ることはできない．

2.4.2 秘密同時通信プロトコル (PSM プロトコル)

秘密同時通信プロトコル (PSM プロトコル)[FKN94, IK97] とは，Feige，Kilian，Naor によって提案され，Ishai，Kushilevitz により拡張された多者間秘密計算 (MPC) の通信パターンを最も単純化したものである．
PSM プロトコルは，入力をもつ n 人の参加者と独立した評価者から構成される．また，各参加者に対しては事前に入力に依存しないランダムネスが共有される．具体的には，始めに

各参加者 P_k は自身の入力 x_k と共有ランダムネス r を用いて関数 Enc_k を計算してメッセージ m_k を生成し，m_k を評価者に送信する．評価者は各参加者から送られてきたメッセージ m_k を入力としてある復号関数 Dec を計算することで，目標とした関数の計算結果を得ることができる．このとき，評価者に対して出力 $f(x)$ から洩れる情報以外の情報は洩れない．

以下に PSM プロトコルの定義を記す．

定義 2.4.1 (PSM プロトコル) $\mathcal{X}_1, \mathcal{X}_2, \ldots, \mathcal{X}_n$，$\mathcal{Z}$ を有限集合とし，$\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_2 \times \cdots \times \mathcal{X}_n$ とする．ただし，$\mathcal{X}_k$ は入力 x_k がとり得る値の集合であり，$\mathcal{Z}$ は出力がとり得る値の集合である．このとき，n 変数関数 $f : \mathcal{X} \to \mathcal{Z}$ を計算する PSM プロトコル $\mathcal{P}$ は以下の要素から構成される．

- 共有ランダムネス r のとり得る有限集合 $\mathcal{R}$ および，$\mathsf{Enc}(x_k, r)$ がとり得る値の集合 $\mathcal{M}_k$.
- メッセージ関数 Enc_k ： $\mathcal{X}_k \times \mathcal{R} \to \mathcal{M}_k$.
- 復号関数 $\mathsf{Dec} : \mathcal{M}_1 \times \mathcal{M}_2 \times \cdots \times \mathcal{M}_n \to \mathcal{Z}$.

$\mathsf{Enc}(x, r)$ をメッセージ $(\mathsf{Enc}_1(x_1, r), \mathsf{Enc}_2(x_2, r), \ldots, \mathsf{Enc}_n(x_n, r))$ の n タプルとする．このとき，PSM プロトコル $\mathcal{P}$ は以下の二つの性質を満たす．

1. **正当性．** すべての入力 $x \in \mathcal{X}$ とすべての要素 $r \in \mathcal{R}$ に対して，$\mathsf{Dec}(\mathsf{Enc}(x, r)) = f(x)$ となる．
2. **秘匿性．** シミュレータと呼ばれる乱択関数 Sim が存在し，すべての $x \in \mathcal{X}$ について $\mathsf{Sim}(f(x))$ の出力がメッセージ全体の分布と等しくなる．

第3章　先行研究

3.1　量子信号処理 (QSP)

量子信号処理 (Quantum Signal Processing, QSP) とは，[LC17] にて Low と Chuang により提案された量子アルゴリズムである．QSP はもともと核磁気共鳴における信号強度の増幅を目的として提案された技法であるが，同時期にハミルトニアンシミュレーションのような量子計算機上での重要な問題にも応用が可能であることが示されている．

本節では，QSP の定理について Gilyén らの論文 [GSLW19, Gil19] を参考に記す．より詳しい QSP の詳細についてはこれらの論文を参照されたい．

定理 3.1.1 (量子信号処理 (QSP)) $L \in \mathbb{N}$，$\Phi = (\phi_0, \phi_1, \ldots, \phi_L) \in \mathbb{R}^{L+1}$ とする (ただし，$\mathbb{N}$ は 0 を含む)．このとき，すべての $y \in [-1, 1]$ に対して

$$\begin{aligned} &\exp(i\phi_0 Z) \prod_{\ell=1}^{L} (W(y) \exp(i\phi_\ell Z)) \\ &= \begin{bmatrix} P(y) & iQ(y)\sqrt{1-y^2} \\ iQ^*(y)\sqrt{1-y^2} & P^*(y) \end{bmatrix} \end{aligned} \tag{3.1}$$

および

(i) $\deg(P) \leq L$，$\deg(Q) \leq L - 1$

(ii) P のパリティは $L \mod 2$，Q のパリティは $(L-1) \mod 2$

(iii) $\forall y \in [-1, 1] : |P(y)|^2 + (1 - y^2)|Q(y)|^2 = 1$

を満たすような $P, Q \in \mathbb{C}[y]$ が存在する．さらに，$P, Q \in \mathbb{C}[y]$ が (i)-(iii) を満たす場合，式 (3.1) を満たすような $\Phi \in \mathbb{R}^{L+1}$ が存在する．ただし，

$$\begin{aligned} W(y) &= \begin{bmatrix} y & i\sqrt{1-y^2} \\ i\sqrt{1-y^2} & y \end{bmatrix} \\ &= \exp(i \arccos(y) X) \end{aligned} \tag{3.2}$$

である．

定理 3.1.1 の証明.　始めに順方向の証明を帰納法を用いて行う．$L = 0$ とすると，式 (3.1)

の左辺のユニタリ行列は $\exp(i\phi_0 Z)$ となる．

$$\begin{aligned}\exp(i\phi_0 Z) &= \cos(-\phi_0)\mathbb{I} - i\sin(-\phi_0)Z \\ &= \begin{bmatrix} \cos(-\phi_0) - i\sin(-\phi_0) & 0 \\ 0 & \cos(-\phi_0) + i\sin(-\phi_0) \end{bmatrix} \\ &= \begin{bmatrix} \cos(\phi_0) + i\sin(\phi_0) & 0 \\ 0 & \cos(\phi_0) - i\sin(\phi_0) \end{bmatrix} \\ &= \begin{bmatrix} \exp(i\phi_0) & 0 \\ 0 & \exp(-i\phi_0) \end{bmatrix}\end{aligned}$$

であるので，P, Q はそれぞれ $P \equiv \exp(i\phi_0)$，$Q \equiv 0$ となる．また，これらは (i)〜(iii) を満たす．

続いて，$L-1$ について，

$$\exp(i\phi_0 Z)\prod_{\ell=1}^{L-1}(W(y)\exp(i\phi_\ell Z)) = \begin{bmatrix} \tilde{P}(y) & i\tilde{Q}(y)\sqrt{1-y^2} \\ i\tilde{Q}^*(y)\sqrt{1-y^2} & \tilde{P}^*(y) \end{bmatrix},$$

における $\tilde{P}, \tilde{Q} \in \mathbb{C}[y]$ が (i)〜(ii) を満たすことを証明したとする．

$$\begin{aligned}&\exp(i\phi_0 Z)\prod_{\ell=1}^{L}(W(y)\exp(i\phi_\ell Z)) \\ &= \begin{bmatrix} \tilde{P}(y) & i\tilde{Q}(y)\sqrt{1-y^2} \\ i\tilde{Q}^*(y)\sqrt{1-y^2} & \tilde{P}^*(y) \end{bmatrix} \begin{bmatrix} \exp(i\phi_L)y & i\exp(-i\phi_L)\sqrt{1-y^2} \\ i\exp(i\phi_L)\sqrt{1-y^2} & \exp(-i\phi_L)y \end{bmatrix} \\ &= \begin{bmatrix} \exp(i\phi_L)\left(y\tilde{P}(y) + (y^2-1)\tilde{Q}(y)\right) & i\exp(-i\phi_L)\left(y\tilde{Q}(y) + \tilde{P}(y)\right)\sqrt{1-y^2} \\ i\exp(i\phi_L)\left(y\tilde{Q}^*(y) + \tilde{P}^*(y)\right)\sqrt{1-y^2} & \exp(-i\phi_L)\left(y\tilde{P}^*(y) + (y^2-1)\tilde{Q}^*(y)\right) \end{bmatrix}\end{aligned} \tag{3.3}$$

ここで $P(y) = \exp(i\phi_L)\left(y\tilde{P}(y) + (y^2-1)\tilde{Q}(y)\right)$，$Q(y) = \exp(-i\phi_L)\left(y\tilde{Q}(y) + \tilde{P}(y)\right)$ とすると，式 (3.3) は

$$\begin{aligned}&\exp(i\phi_0 Z)\prod_{\ell=1}^{L-1}(W(y)\exp(i\phi_\ell Z)) \\ &= \begin{bmatrix} P(y) & iQ(y)\sqrt{1-y^2} \\ iQ^*(y)\sqrt{1-y^2} & P^*(y) \end{bmatrix}\end{aligned}$$

と書くことができ，多項式 P, Q が (i)，(ii) を満たしていることは容易に理解できる．

最後に (iii) を満たすことを示す．式 (3.1) の右辺について，自身と自身の複素共役転置の積をとると，

$$\begin{aligned}&\begin{bmatrix} P(y) & iQ(y)\sqrt{1-y^2} \\ iQ^*(y)\sqrt{1-y^2} & P^*(y) \end{bmatrix} \cdot \begin{bmatrix} P(y) & iQ(y)\sqrt{1-y^2} \\ iQ^*(y)\sqrt{1-y^2} & P^*(y) \end{bmatrix}^\dagger \\ &= \begin{bmatrix} P(y) & iQ(y)\sqrt{1-y^2} \\ iQ^*(y)\sqrt{1-y^2} & P^*(y) \end{bmatrix} \cdot \begin{bmatrix} P^*(y) & -iQ(y)\sqrt{1-y^2} \\ -iQ^*(y)\sqrt{1-y^2} & P(y) \end{bmatrix} \\ &= \begin{bmatrix} P(y)P^*(y) + Q(y)Q^*(y)(1-y^2) & i(P(y)Q(y) - P(y)Q(y))\sqrt{1-y^2} \\ i(P^*(y)Q^*(y) - P^*(y)Q^*(y))\sqrt{1-y^2} & P(y)P^*(y) + Q(y)Q^*(y)(1-y^2) \end{bmatrix}\end{aligned}$$

となる．ここで，式 (3.1) の左辺はユニタリ行列の積であることから，右辺もユニタリ行列であることが分かる．ユニタリ行列の性質 $UU^\dagger = \mathbb{I}$ を用いることで，

$$\begin{aligned} &P(y)P^*(y) + Q(y)Q^*(y)(1-y^2) = 1 \\ \Leftrightarrow &|P(y)|^2 + (1-y^2)|Q(y)|^2 = 1 \end{aligned} \tag{3.4}$$

となり，(iii) を満たすことが分かる．

次に逆方向の証明を行う．P, Q が (i)〜(iii) を満たすとする．初めに簡単なケースを考える．$\deg(P) = 0$ とすると，(iii) により $|P(1)| = 1$ が得られる．したがって，ある $\phi_0 \in \mathbb{R}$ について $P \equiv \exp(i\phi_0)$ となる．また，これは (iii) から $Q \equiv 0$ であることを意味する．さらに，(ii) より P が偶多項式であることから L は偶数である必要がある．$\Phi = (\phi_0, \frac{\pi}{2}, -\frac{\pi}{2}, \ldots, \frac{\pi}{2}, -\frac{\pi}{2})$ とすると，式 (3.1) は

$$\exp(i\phi_0 Z) \prod_{\ell=1}^{L/2} \Big(W(y) \exp\Big(i\frac{\pi}{2}Z\Big) W(y) \exp\Big(-i\frac{\pi}{2}Z\Big) \Big) \tag{3.5}$$

となる．ここで，

$$\begin{aligned} \exp\Big(i\frac{\pi}{2}Z\Big) &= \cos\Big(-\frac{\pi}{2}\Big)\mathbb{I} - i\sin\Big(-\frac{\pi}{2}\Big)Z \\ &= \begin{bmatrix} \cos\big(-\frac{\pi}{2}\big) - i\sin\big(-\frac{\pi}{2}\big) & 0 \\ 0 & \cos\big(-\frac{\pi}{2}\big) + i\sin\big(-\frac{\pi}{2}\big) \end{bmatrix} \\ &= \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \end{aligned}$$

であり，同様に

$$\exp\Big(-i\frac{\pi}{2}Z\Big) = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}$$

であるので，式 (3.5) は

$$\begin{aligned} &\exp(i\phi_0 Z) \prod_{\ell=1}^{L/2} \begin{bmatrix} y & i\sqrt{1-y^2} \\ i\sqrt{1-y^2} & y \end{bmatrix} \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} y & i\sqrt{1-y^2} \\ i\sqrt{1-y^2} & y \end{bmatrix} \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} \\ &= \exp(i\phi_0 Z) \prod_{\ell=1}^{L/2} \begin{bmatrix} iy & \sqrt{1-y^2} \\ -\sqrt{1-y^2} & -iy \end{bmatrix} \begin{bmatrix} -iy & -\sqrt{1-y^2} \\ \sqrt{1-y^2} & iy \end{bmatrix} \\ &= \exp(i\phi_0 Z) \prod_{\ell=1}^{L/2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \exp(i\phi_0 Z) \end{aligned}$$

となる．よって，$\deg(P) = 0$ としたとき式 (3.1) を満たす $\Phi \in \mathbb{R}^{L+1}$ が存在することが示された．このケースは $L = 0$ のケースの証明となっている．以降の証明は帰納法を用いて行う．

$L-1$ について証明が完了したと仮定する．式 (3.4) について，この式は無限の点で成り立つので，左辺の多項式の定数部分は 1 である必要がある．一般性を損なわずに $1 \leq \deg(P) = k \leq L$ とすると，必然的に $\deg(Q) = k-1$ となり，式 (3.4) において打ち消しあうためにそ

れぞれの最高次係数は $|p_k| = |q_{k-1}|$ である必要がある．$\phi_L \in \mathbb{R}$ を $\exp(2i\phi_L) = \frac{p_k}{q_{k-1}}$ を満たすようなものであるとし，$\tilde{P}, \tilde{Q}$ を以下の計算を通して定義する．

$$
\begin{aligned}
&\begin{bmatrix} \tilde{P}(y) & i\tilde{Q}(y)\sqrt{1-y^2} \\ i\tilde{Q}^*(y)\sqrt{1-y^2} & \tilde{P}^*(y) \end{bmatrix} \\
&:= \begin{bmatrix} P(y) & iQ(y)\sqrt{1-y^2} \\ iQ^*(y)\sqrt{1-y^2} & P^*(y) \end{bmatrix} \exp(-i\phi_L Z) W^\dagger(y) \\
&= \begin{bmatrix} P(y) & iQ(y)\sqrt{1-y^2} \\ iQ^*(y)\sqrt{1-y^2} & P^*(y) \end{bmatrix} \begin{bmatrix} \exp(-i\phi_L)y & -i\exp(-i\phi_L)\sqrt{1-y^2} \\ -i\exp(i\phi_L)\sqrt{1-y^2} & \exp(i\phi_L)y \end{bmatrix} \\
&= \begin{bmatrix} \exp(-i\phi_L)yP(y) + \exp(i\phi_L)(1-y^2)Q(y) & i(\exp(i\phi_L)yQ(y) - \exp(-i\phi_L)P(y))\sqrt{1-y^2} \\ i(\exp(-i\phi_L)yQ^*(y) - \exp(i\phi_L)P^*(y))\sqrt{1-y^2} & \exp(i\phi_L)yP^*(y) + \exp(-i\phi_L)(1-y^2)Q^*(y) \end{bmatrix}
\end{aligned}
\tag{3.6}
$$

つまり，

$$
\begin{aligned}
\tilde{P}(y) &= \exp(-i\phi_L)yP(y) + \exp(i\phi_L)(1-y^2)Q(y) \\
&= \exp(-i\phi_L)\left(yP(y) + \frac{p_k}{q_{k-1}}(1-y^2)Q(y)\right)
\end{aligned}
\tag{3.7}
$$

かつ，

$$
\begin{aligned}
\tilde{Q}(y) &= \exp(i\phi_L)yQ(y) - \exp(-i\phi_L)P(y) \\
&= \exp(-i\phi_L)\left(\frac{p_k}{q_{k-1}}yQ(y) - P(y)\right)
\end{aligned}
\tag{3.8}
$$

となる．式 (3.7) および式 (3.8) から，最上位項が相殺されることが分かるので，$\deg(\tilde{P}) \leq k-1 \leq L-1$，$\deg(\tilde{Q}) \leq k-1 \leq L-2$ となることは容易に理解できる．また，式 (3.7) および式 (3.8) から $L-1$ に対して $\tilde{P}, \tilde{Q}$ が (i)，(ii) を満たすことが確認でき，$\exp(-i\phi_L Z)W^\dagger(y)$ がユニタリ行列であることから (iii) についても満たすことが分かる．

よって，帰納法により，式 (3.6) はある $\tilde{\Phi} \in \mathbb{R}^L$ に対して $\exp\left(i\tilde{\phi}_0 Z\right)\left(\prod_{\ell=1}^{L-1} W(y)\exp\left(i\tilde{\phi}_\ell Z\right)\right)$ に等しいことが分かり，$\Phi := (\tilde{\phi}_0, \tilde{\phi}_1, \ldots, \tilde{\phi}_{L-1}, \phi_L) \in \mathbb{R}^{L+1}$ が解であることが分かる． □

3.2 Maslov らの手法

本節では Maslov らによって提案された量子信号処理を用いた 1 量子ビットメモリ上での対称ブール関数の計算手法について記述する．

はじめに [Haa19] の論文を参考に QSP の多項式表現について記述する．$U(\theta)$ を QSP の出力行列とする．このとき，実数値関数 A, B, C, D を用いて，$U(\theta) = A(\theta)\mathbb{I} + iB(\theta)X + iC(\theta)Y + iD(\theta)Z$ と書くことができる．事実，$R_x(\theta) = \frac{1}{2}\exp(-i\theta/2)(\mathbb{I}+X) + \frac{1}{2}\exp(i\theta/2)(\mathbb{I}-X)$ は A, B, C, D が $t = \exp(i\theta/2)$ の関数であることが分かる．これらは $A(t) = \sum_{j=-L}^{L} a_j t^j$ のような次数 L の t についてのローラン多項式である．参考文献 [Haa19] より，このような式が成り立つのは以下の条件を満たすときである．

(i) $A(t)^2 + B(t)^2 + C(t)^2 + D(t)^2 = 1$

(ii) A, B, C, D は最大次数が L のローラン多項式であり，少なくとも一つの多項式は次数が L である．

(iii) A, B, C, D は L の値が偶数であれば遇関数，奇数であれば奇関数となる．

(iv) $A(t) = A(1/t)$ および $D(t) = D(1/t)$ が成り立ち，$B(t) = -B(1/t)$ および $C(t) = -C(1/t)$ が成り立つ．

ここで，対称性より $\theta \in [0, \pi)$ の範囲外の A, B, C, D の値は領域内の値と等価であることに注意する．例えば，$A(\theta) = A(-\theta) = -A(2\pi - \theta) = -A(2 - \pi - \theta)$ である．また，参考文献 [Haa19] より，A, B が (ii-iv) の条件を満たす対称性を持つローラン多項式であり，すべての θ に対して $0 \leq A(\theta)^2 + B(\theta)^2 \leq 1$ を満たすとき，A, B, C, D が条件 $(i - iv)$ を満たすような関数 $C(t)$ と $D(t)$ が存在することが分かる．

次に，QSP を用いて対称ブール関数を計算する方法について記述する．最終的なゴールは，$f(x) = 0$ のときに $U(\theta) = \mathbb{I}$ となり，$f(x) = 1$ のときに $U(\theta) = iX$ となるような $U(\theta)$ を構成することである．一般性を損なわない範囲で $f(0^n) = 0$ と仮定し，入力ビット列 $x \in \{0, 1\}^n$ に対して $\theta = \Delta|x| - \delta$ を定義する．一般に，関数 f について何も分からない場合は $\Delta = \pi/(n + 1)$ および $\delta = 0$ とする．これにより，$|x| = 0, 1, \ldots, n$ に対する θ の範囲は $[0, \pi)$ となる．つまり，目標の $U(\theta)$ を構成するためには，条件 (ii-iv) および，$0 \leq A(\theta)^2 + B(\theta)^2 \leq 1$,

$$A(\theta) = \begin{cases} 0, & f(x) = 1 \\ 1, & f(x) = 0 \end{cases}, \tag{3.9}$$

$$B(\theta) = \begin{cases} 0, & f(x) = 0 \\ 1, & f(x) = 1 \end{cases} \tag{3.10}$$

を満たす A, B を構成する必要があることが分かる．また，$A(\theta)^2 + B(\theta)^2 \leq 1$ を議論する際に，すべての $x \in \{0, 1\}^n$ について，

$$\frac{\mathrm{d}}{\mathrm{d}\theta} A(\theta) = 0 \ \text{ かつ } \ \frac{\mathrm{d}}{\mathrm{d}\theta} B(\theta) = 0 \tag{3.11}$$

を必要とすることに注意する．

L が奇数であると仮定する．このとき，A は j が奇数の場合は $a_j = a_{-j}$，偶数の場合は $a_j = 0$ となるローラン多項式になる．本手法のアプローチは，式 (3.9) および (3.11) から得られる $2(n+1)$ 個の線形系を使用して，$a_1, a_3, \ldots, a_L$ の $(L+1)/2$ 個の変数を解くというものである．$\frac{\mathrm{d}}{\mathrm{d}\theta} A(0) = 0$ より，一つの方程式は自動で満たされるため，残りの $2n + 1$ を考える．方程式と変数の数を等しくすることを考えると，必要な L の長さはせいぜい $L = 4n + 1$ であることが分かる．B についても同様の議論を行うことが可能であり，同じ結論に到達する．以後，A および B は線形系を解く最小次数のローラン多項式であると仮定する．

次に，$P(\theta) = 1 - A(\theta)^2 - B(\theta)^2$ が必ず 0 以上であることを示す．はじめに，すべての θ に対して 1 に等しい和 $E(\theta) = A(\theta) + B(\theta)$ を考える．このとき，A および B は上記の制約を満たす最小次数ローラン多項式であるため，$E(\theta) = 1$ はこの一点のみで成り立つ．よって，すべての x に対して $\frac{\mathrm{d}}{\mathrm{d}\theta} E(\theta) = 0$，$\theta \in [0, \pi]$ について $E(\theta) < 1$ であるので，すべての

$\theta \in [0,\pi]$ に対して $0 \le E(\theta) \le 1$ が成り立つことが分かる．A および B は対称性を持つため，

$$\begin{aligned}
A(\theta)+B(\theta) \le 1,\ A(\theta)B(\theta) \ge 0,\ (\theta \in [0,\pi]),\\
A(\theta)-B(\theta) \le 1,\ A(\theta)B(\theta) \le 0,\ (\theta \in [-\pi,0]),\\
-A(\theta)+B(\theta) \le 1,\ A(\theta)B(\theta) \le 0,\ (\theta \in [\pi,2\pi]),\\
-A(\theta)-B(\theta) \le 1,\ A(\theta)B(\theta) \ge 0,\ (\theta \in [-2\pi,-\pi])
\end{aligned}$$

となることに注意する．これらは，すべての θ に対して $P(\theta) \ge 0$ であることを意味している．例えば，$\theta \in [0,\pi]$ であれば $P(\theta) = 1-(A(\theta)+B(\theta))^2 + 2A(\theta)B(\theta) \ge 0$ となる．

以上より，対称ブール関数 f を計算する $U(\theta)$ を構成することができた．

3.3 1 量子ビットモデル (1-qubit model)

1 量子ビットモデル (1-qubit model) とは，[CKP13] にて Cosentino と Kothari，Paetznick により提案された，1 量子ビットを操作する行列のみで任意のブール関数を計算することが可能な量子アルゴリズムである．Maslov らによる QSP の応用 [MKB+21] で計算することが可能な関数は対称ブール関数であるので，1 量子ビットモデルはこれ以上の能力を持っていることが分かる．本節では，この 1 量子ビットモデルについて，[CKP13] を参考に解説する．

定義 3.3.1 (1 量子ビットモデル) 1 量子ビットを操作するユニタリ行列を $U_\ell (\ell = 0,\dots,L)$，古典ビット $x_k (k = 1,\dots,n)$ によって制御されるパウリ行列 X を X^{x_k} とする．このとき，これらを用いて構成される図 3.1 のような量子回路を 1 量子ビットモデルと呼ぶ．ただし，量子回路の出力は計算基底による測定によって決定される．

また，ある関数 $f : \{0,1\}^n \to \{0,1\}$ について，x を入力としたとき量子回路が確率 1 で $f(x)$ を出力するものを 1 量子ビットプログラムと呼ぶ．1 量子ビットプログラムでは，プログラムの長さを X^{x_k} の総数として定義する．

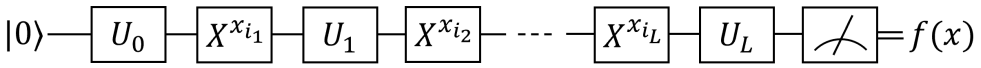

図 3.1: 1 量子ビットモデル

定理 3.3.2 (1 量子ビットモデル) 2 入力の AND と OR，および NOT ゲートを用いて深さ d の古典回路で計算可能な任意の関数は，長さ 4^d の 1 量子ビットプログラムで計算することが可能である．

定理 3.3.2 の証明． C を関数 $C(x)$ を計算する深さ d の古典回路とする．また，F を関数 $C(x)$ を計算する長さ 4^d の 1 量子ビットプログラムとする．つまり，$F = X^{C(x)}$ は $F|0\rangle = |C(x)\rangle$ と同じことを意味する．

証明は古典回路の構造に対する帰納法を用いて行う．古典回路 C は入力変数を木の葉，ゲートを内部ノードとする二分木として捉えることが可能である．古典回路のルートにゲー

ト (AND または NOT) があるとき，そのゲートの入力を生成する部分回路について帰納仮説が成り立つと仮定して進める．

はじめに，C が単一の変数 x_i のみである，すなわち木の葉のみの木である場合を考える．このとき，対応する 1 量子ビットプログラムはビット x_i によって制御される X^{x_i} であり，$F = X^{x_i}$ となる．

次に 2 つのケースを考える．一つ目は C が NOT ゲートと部分回路 C' から構成されている場合である．F' を古典回路 C' を長さ 4^d で計算する 1 量子ビットプログラムであるとする．このとき，C を計算する長さ 4^d の 1 量子ビットプログラムは次のように得ることができる．

$$F = XX^{C'(x)} = X^{\bar{C}'(x)} = X^{C(x)}.$$

ここで，NOT ゲートは回路の深さに寄与しないため，C と C' の回路の深さは同じであり，また，1 量子ビットを操作するユニタリ行列はプログラムの長さに寄与しないので，プログラム F と F' の長さについても同じであることに注意されたい．

二つ目は C が AND ゲートと二つの部分回路 C' と C'' から構成されている場合である．F' と F'' をそれぞれ C' と C'' を計算する長さ 4^{d-1} の 1 量子ビットプログラムとし，次の 1 量子ビットプログラムを考える．

$$\begin{aligned} F &= VX^{C'(x)}H^{C''(x)}X^{C'(x)}H^{C''(x)}V \\ &= V(-iY)^{C'(x)\wedge C''(x)}V \\ &= -iX^{C(x)}. \end{aligned}$$

ここで，$V = \frac{1}{\sqrt{2}}(X+Y)$ は $VYV = X$ および $VXV = Y$ を満たすエルミート行列である．帰納仮説より，C' を計算する 1 量子ビットプログラム F' が存在するするので，$X^{C'(x)}$ は計算可能である．また，$H^{C''(x)}$ については，$KXK = H$，$KHK = X$，$KX^aK = (KXK)^a = H^a$ を満たすようなエルミート行列

$$K = \begin{bmatrix} \frac{1}{2}\sqrt{2-\sqrt{2}} & (\frac{1}{2}+\frac{1}{\sqrt{2}})\sqrt{2-\sqrt{2}} \\ (\frac{1}{2}+\frac{1}{\sqrt{2}})\sqrt{2-\sqrt{2}} & -\frac{1}{2}\sqrt{2-\sqrt{2}} \end{bmatrix}$$

を用いることで，$X^{C''(x)}$ から $H^{C''(x)}$ を導出可能である．帰納仮説より，C'' を計算する 1 量子ビットプログラム F'' が存在するので，$X^{C''(x)}$ は計算可能である．よって，1 量子ビットプログラム F はいくつかの 1 量子ビットを操作するユニタリ行列および F' の二つのコピー，F'' の二つのコピーから構成可能であることが分かる．また，F' と F'' の長さは最長でも 4^{d-1} であり，1 量子ビットを操作するユニタリ行列は長さに寄与しないため，F の長さは 4^d となる．

□

第4章　提案手法

本研究では，2 つのプロトコルを提案する．一つ目は秘密量子信号処理 (PQSP) である．これは，1 量子ビット上の回転角 θ の 2×2 ユニタリ行列から回転角 $\mathrm{poly}(\theta)$ の 2×2 ユニタリ行列を生成するような PSM モデルに基づく QSP について，各参加者が保持する角度情報を秘匿化しつつ，2×2 ユニタリ行列を生成することができるようなプロトコルである．二つ目は秘密 1 量子ビットプログラム (P1QP) である．これは，PSM モデルにおいて，各参加者が保持するビット情報を秘匿化しつつ，それらを入力とした任意のブール関数を計算するプロトコルである．

これら二つのプロトコルでは，各参加者から送信されるメッセージはそれぞれが生成するユニタリ行列について Z-X 分解などの分解を行った際に得られる回転行列の軸と角度の情報である．評価者は図 4.1 古典ビットにより制御される 1 量子ビット回転行列を 1 量子ビットメモリ上に適用し，計算を行うものとする．

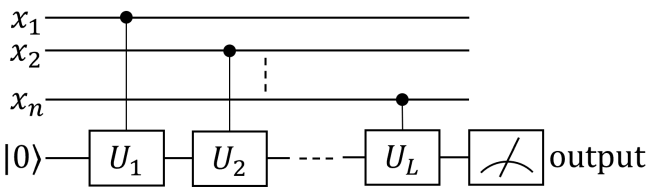

図 4.1: 1 量子ビットモデル (PSM)

4.1　秘密量子信号処理 (PQSP)

本研究で扱う PSM モデルに基づく QSP は，入力情報 (角度情報)θ_k をもつ n 人の古典参加者と独立した量子評価者によって構成される．具体的には，はじめに入力 θ_k を持つ各参加者 P_k は事前に共有される入力に依存しない 1 量子ビットに対する Haar ランダムユニタリ行列 R を用いて独立した計算 $\mathsf{Enc}_k(\theta_k, R)$ を行い，その結果 (メッセージ m_k) を評価者に送信する．評価者は各参加者から送られてきたメッセージ m_k を入力とした復号関数 Dec を計算することで，目的の 2×2 ユニタリ行列を得る．

PQSP を構成するにあたり，各参加者が保持している入力情報を秘匿化するメッセージを生成する必要がある．本研究では，この秘匿化を Kilian の乱択化手法を用いて行う．ただ

し，$\theta = \theta_1 + \theta_2 + \cdots + \theta_n$ である．

$$\begin{aligned} W(y) &= \exp(i\theta X) \\ &= \exp(i(\theta_1 + \theta_2 + \cdots + \theta_n)X) \\ &= \prod_{k=1}^{n} \exp(i\theta_k X) \end{aligned} \tag{4.1}$$

に対して，$n-1$ 個の 1 量子ビットに対する Haar ランダムユニタリ行列を用いて Kilian の乱択化を適用する．

$$\begin{aligned} W'(y) =& \exp(i\theta_1 X) R_1 \cdot R_1^\dagger \exp(i\theta_2 X) R_2 \\ & \cdot \cdots \cdot R_{n-1} \cdot R_{n-1}^\dagger \exp(i\theta_n X) \end{aligned} \tag{4.2}$$

式 (4.2) の 1 量子ビットに対する Haar ランダムユニタリ行列 R_k は自身の複素共役転置行列 $R_k^\dagger$ と打ち消しあうため，

$$\begin{aligned} W'(y) =& \exp(i\theta_1 X) R_1 \cdot R_1^\dagger \exp(i\theta_2 X) R_2 \cdot \cdots \cdot R_{n-1} \cdot R_{n-1}^\dagger \exp(i\theta_n X) \\ =& \exp(i\theta_1 X) \cdot \exp(i\theta_2 X) \cdot \cdots \cdot \exp(i\theta_n X) \\ =& \exp(i(\theta_1 + \theta_2 + \cdots + \theta_n)X) \\ =& W(y) \end{aligned}$$

となり，最終的な出力は Kilian の乱択化を適用する前と等しいことが分かる．

上述のようにすることで，各参加者は独立してメッセージを作成することが可能である．しかし，この方法では評価者は $W(y)$ を復元することができてしまい，角度 $\theta = \theta_1 + \theta_2 + \cdots + \theta_n$ の情報が洩れてしまうという問題がある．

本研究ではこの問題を解決するべく，位相列に関する部分にも Kilian の乱択化手法を適用する．

$$\begin{aligned} U'(\theta) =& \exp(i\phi_0 Z) R_0 \cdot R_0^\dagger W(y) \exp(i\phi_1 Z) R_1 \cdot R_1^\dagger W(y) \exp(i\phi_2 Z) R_2 \cdot R_2^\dagger \\ & \cdot \cdots \cdot R_{L-1} \cdot R_{L-1}^\dagger W(y) \exp(i\phi_L Z) \\ =& \exp(i\phi_0 Z) \prod_{\ell=1}^{L} W(y) \exp(i\phi_\ell Z) \\ =& U(\theta) \end{aligned} \tag{4.3}$$

ただし，R_ℓ は 1 量子ビットに対する Haar ランダムユニタリ行列である．

得られた $U'(\theta)$ の $W(y)$ を $W'(y)$ に置換することで，角度 θ を秘匿化した状態で $U(\theta)$ を計算することが可能となる．各参加者が生成するメッセージおよび評価者が計算する復号関数については構成 (PQSP) を参照せよ．

以下に PQSP の構成を示す．

構成 (PQSP Π_{PQSP})

n 人の古典参加者 P_k はそれぞれ入力 θ_k を持っており，独立した量子評価者を通じて QSP を実行するとする．このとき，PQSP Π_{PQSP} は以下のような手順で実行される．

Step 1.
各参加者 P_k は事前に入力に依存しない独立な 1 量子ビットに対する Haar ランダムユニタリ行列の列 $R = (R_{k,\ell} :\ k = 1, \ldots, n;\ \ell = 1, \ldots, L)$ を共有しておく.
Step 2.
各参加者 P_k は自身の入力 θ_k に基づいて以下の操作を行う.

- P_1 は以下のメッセージ m_1 を評価者に送信する.
  - $m_{1,0} = \exp(i\phi_0 Z) \cdot R_{n,L}$
  - $m_{1,1} = R_{n,L}^{\dagger} \cdot \exp(i\theta_1 X) \cdot R_{1,1}$
  - $m_{1,\ell} = R_{n,\ell-1}^{\dagger} \cdot \exp(i\theta_1 X) \cdot R_{1,\ell}$
    $(\ell = 2, \ldots, L)$
  - $m_1 = (m_{1,0}, m_{1,1}, \ldots, m_{1,L})$
- P_k $(k = 2, \ldots, n-1)$ は以下のメッセージ m_k を評価者に送信する.
  - $m_{k,\ell} = R_{k-1,\ell}^{\dagger} \cdot \exp(i\theta_k X) \cdot R_{k,\ell}$
    $(\ell = 1, \ldots, L)$
  - $m_k = (m_{k,1}, \ldots, m_{k,L})$
- P_n は以下のメッセージ m_n を評価者に送信する.
  - $m_{n,\ell} = R_{n-1,\ell}^{\dagger} \cdot \exp(i\theta_n X) \cdot \exp(i\phi_\ell Z) \cdot R_{n,\ell}$
    $(\ell = 1, \ldots, L-1)$
  - $m_{n,L} = R_{n-1,L-1}^{\dagger} \cdot \exp(i\theta_n X) \cdot \exp(i\phi_L Z)$
  - $m_n = (m_{n,1}, \ldots, m_{n,L})$

Step 3.
評価者は各参加者から送られてきたメッセージをもとに，以下の復号関数 Dec を計算する.

$$\mathsf{Dec}(m) = m_{1,0} \cdot \prod_{\ell=1}^{L} \prod_{k=1}^{n} m_{k,\ell} = U(\theta) \tag{4.4}$$

次に，PQSP が以下の正当性および秘匿性についての定理を満たすことを証明する.

定理 4.1.1 (正当性 (PQSP)) すべての入力 $\theta \in [-\pi, \pi)$ およびすべての 1 量子ビット上のユニタリ行列 R から生成されるメッセージ $m = (m_1, \ldots, m_n)$ について，$\mathsf{Dec}(m) = U(\theta)$ となる.

定理 4.1.1 の証明. PQSP の構成で用いられる式 (4.4) から，復号関数 Dec を計算することで，評価者はすべてのメッセージ m について確率 1 でユニタリ $U(\theta)$ を出力することができることは明らかである. □

定理 4.1.2 (秘匿性 (PQSP)) 各参加者から送られてくるメッセージ $m = (m_1, \ldots, m_n)$ が従う分布を $\mathcal{M} = (\mathcal{M}_1, \ldots, \mathcal{M}_n)$ とする．このとき，$\mathsf{Sim}(U(\theta))$ の出力の分布が $\mathcal{M}$ と同一分布となるような乱択関数 Sim が存在する．

定理 4.1.2 の証明. はじめに各参加者から送られてくるメッセージの分布を考える．PQSP の構成より，この分布は独立な $nL+1$ 個の 1 量子ビット上の Haar ランダムユニタリ行列をとる確率変数について，PQSP の復号関数で計算される計算結果が $U(\theta)$ となる条件を満たす確率分布になっていることは容易に理解できる．一般性を損なわずに最終要素以外をそれぞれが独立な 1 量子ビット上の Haar ランダムユニタリ行列とした場合，最終要素 $m_{n,L}$ は

$$m_{n,L} = \prod_{k=n-1}^{1} m_{k,L}^{\dagger} \cdot \prod_{\ell=L-1}^{1} \prod_{k=n}^{1} m_{k,\ell}^{\dagger} \cdot m_{1,0}^{\dagger} \cdot U(\theta)$$

で決定されることが分かる．次にシミュレータ $\mathsf{Sim}(U(\theta))$ の分布を考える．

$$\mathsf{Sim}(U(\theta)) = (S_{1,0}, S_{1,1}, \ldots, S_{1,L}, S_{2,1}, \ldots, S_{2,L}, \ldots, S_{n,1}, \ldots, S_{n,L})$$

とし，$S_{k,\ell}$ の分布を $\mathcal{S}_{k,\ell}$ とする．最終要素を除いたすべての要素について，それぞれが独立な 1 量子ビット上の Haar ランダムユニタリ行列をとり，最終要素を

$$S_{n,L} = \prod_{k=n-1}^{1} S_{k,L}^{\dagger} \cdot \prod_{\ell=L-1}^{1} \prod_{k=n}^{1} S_{k,\ell}^{\dagger} \cdot S_{1,0}^{\dagger} \cdot U(\theta)$$

とする．これらを PQSP の復号関数の入力として計算すると $U(\theta)$ となることは容易に理解できる．よって，$\mathsf{Sim}(U(\theta))$ の分布は PQSP の復号関数で計算される計算結果が $U(\theta)$ となる条件付確率になっていることが分かる．以上より，$\mathsf{Sim}(U(\theta))$ と $\mathcal{M}$ の分布が同一となる乱択関数 Sim が存在することが分かる． □

上記のプロトコル Π_{PQSP} は無限精度の理想的なユニタリ行列を利用しており，プロトコルの通信量は無限大である．しかし，この設定は現実的なものではなく，実装のためには通信量を制限する必要がある．ただし，制限を行う場合は Π_{PQSP} で得られる行列は理想的な行列から乖離した誤りのあるものとなる．

本研究では Π_{PQSP} における正当性誤りと通信量のトレードオフについて評価を行う．各参加者から送られてくるメッセージは本章冒頭で述べた通り，回転軸と角度の情報である．各回転行列 $R_a(\theta)(a \in \{x, y, z\})$ を，θ を 2 進数 k 位で切り捨てて角度 $\theta \in [0, 2\pi)$ で近似する．$\tilde{\theta}$ を θ の近似された角度であるとし，$R_a(\tilde{\theta})$ を $R_a(\theta)$ の k ビット近似であるとする．誤差の尺度として，理想的なユニタリ行列と近似したユニタリ行列それぞれで得あれる最終出力行列の最大トレース距離とする．

定理 4.1.3 (通信量評価) U を Π_{PQSP} を実行して得られる最終出力ユニタリ行列とし，$\tilde{U}$ を各参加者から送信される角度が k ビットで近似されているプロトコルを実行して得られる最終出力ユニタリ行列であるとする．このとき，正当性誤りは

$$\max_{|\psi\rangle} \left\| U |\psi\rangle\langle\psi| U^{\dagger} - \tilde{U} |\psi\rangle\langle\psi| \tilde{U}^{\dagger} \right\|_{\mathrm{tr}} = O(2^{-k} nL)$$

となり，通信量は $O(nLk)$ となる．

定理 4.1.3 の証明. $O(nL)$ は U を構成する回転行列の個数から決定されるため，Π_{PQSP} とその k ビット近似 $\tilde{V}$ で利用されるすべての回転行列 V に対して $\max_{|\psi\rangle} \left\| V|\psi\rangle\langle\psi|V^\dagger - \tilde{V}|\psi\rangle\langle\psi|\tilde{V}^\dagger \right\|_{\mathrm{tr}} = O(2^{-k})$ を求めることができれば，トレースノルムについて [NC10] の Box 4.1 で与えられる hybrid argument から正当性誤りを得ることは容易である．また，メッセージサイズは近似から明らかである．

任意の $|\psi\rangle$ を固定する．トレースノルムと忠実度の関係から，

$$\left\| V|\psi\rangle\langle\psi|V^\dagger - \tilde{V}|\psi\rangle\langle\psi|\tilde{V}^\dagger \right\|_{\mathrm{tr}} = \sqrt{1 - \left|\langle\psi|V^\dagger\tilde{V}|\psi\rangle\right|^2} \leq \sqrt{1 - \left|\mathrm{Re}\Big\{\langle\psi|V^\dagger\tilde{V}|\psi\rangle\Big\}\right|^2}. \tag{4.5}$$

が得られる．よって，$\left|\mathrm{Re}\Big\{\langle\psi|V^\dagger\tilde{V}|\psi\rangle\Big\}\right|$ の下界証明を行うことで良いことが分かる．ここで，

$$\left\| V|\psi\rangle - \tilde{V}|\psi\rangle \right\|_2 = \sqrt{(\langle\psi|V^\dagger - \langle\psi|\tilde{V})(V|\psi\rangle - \tilde{V}|\psi\rangle)} = \sqrt{2 - 2\,\mathrm{Re}\Big\{\langle\psi|V^\dagger\tilde{V}|\psi\rangle\Big\}}. \tag{4.6}$$

に注意する．

V は回転行列であり，$\tilde{V}$ はその k ビット近似であるため，$A \in \{X, Y, Z\}$ について $V = \cos(\theta) + i\sin(\theta)A$ および $\tilde{V} = \cos(\theta - \varepsilon) + i\sin(\theta - \varepsilon)A$ となる．誤差 ε について，

$$\varepsilon \leq \sum_{m=k+1}^{\infty} 2^{-m} < 2^{-k}$$

となることは容易に理解できる．$W := V - \tilde{V}$ とする．ここで，マクローリン展開により，

$$W = \sum_{k=0}^{\infty} \frac{\theta^{2k} - (\theta-\varepsilon)^{2k}}{(2k)!} I + i\frac{\theta^{2k+1} - (\theta-\varepsilon)^{2k+1}}{(2k+1)!} A = i\varepsilon A + \left(\theta\varepsilon - \frac{\varepsilon^2}{2}\right) I + \cdots.$$

である．W の各要素 w について，ある定数 $c > 0$ に対して $|w| \leq c\varepsilon < c \cdot 2^{-k}$ であることが分かる．

以上より，$\left\| V - \tilde{V} \right\|_{\mathrm{F}} < c \cdot 2^{-(k-1)}$ となり，式 (4.6) および

$$\left\| V|\psi\rangle - \tilde{V}|\psi\rangle \right\|_2 \leq \left\| V - \tilde{V} \right\|_{\mathrm{op}} \leq \left\| V - \tilde{V} \right\|_{\mathrm{F}}$$

から，

$$\left|\mathrm{Re}\Big\{\langle\psi|V^\dagger\tilde{V}|\psi\rangle\Big\}\right| > 1 - c^2 \cdot 2^{-2k+1} \tag{4.7}$$

となる．式 (4.5) および式 (4.7) から，

$$\left\| V|\psi\rangle\langle\psi|V^\dagger - \tilde{V}|\psi\rangle\langle\psi|\tilde{V}^\dagger \right\|_{\mathrm{tr}} < c \cdot 2^{-k+1} = O(2^{-k})$$

となる．

□

4.1.1 PQSP を用いた対称ブール関数の計算

[MKB+21] で提案されている 1 量子ビットメモリで対称ブール関数を計算する構成は QSP を用いたものである．この QSP 利用部分を PQSP に置き換えることで，それぞれが古典入力をもつ n 人の参加者が量子評価者を通じて関数を計算するモデルについて，評価者に計算結果以外の関数情報および入力情報を秘匿した状態で計算を行うことが可能となる．

定理 4.1.4 (PQSP を用いた 1 量子ビットメモリ対称ブール関数計算) PQSP を用いることで，PSM モデルにおいて 1 量子ビットメモリを用いて対称ブール関数を計算可能である．

定理 4.1.4 の証明. はじめに対称ブール関数の入力を 1 ビット単位で分解可能であり，PQSP で計算可能であることを示す．Maslov らの手法を参考に，$\forall x \in \{0,1\}^n, \theta = \frac{\pi}{n+1}|x|$ とする．ただし，n は参加者数である．このとき，QSP で使用される $W(\theta)$ は

$$\begin{aligned}
W(\theta) &= \exp(i\theta X) \\
&= \exp\left(i(\frac{\pi}{n+1}|x|)X\right) \\
&= \exp\left(i(\frac{\pi}{n+1}x_1 + \frac{\pi}{n+1}x_2 + \cdots + \frac{\pi}{n_1}x + n)\right) \\
&= \exp\left(i\frac{\pi}{n+1}x_1 X\right) \cdot \exp\left(i\frac{\pi}{n+1}x_2 X\right) \cdot \cdots \cdot \exp\left(i\frac{\pi}{n+1}x_n X\right) \\
&= \exp(i\theta_1 X) \cdot \exp(i\theta_2 X) \cdot \cdots \cdot \exp(i\theta_n X)
\end{aligned}$$

ただし，$\theta_k = \frac{\pi}{n+1}x_k$ である．よって，対称ブール関数の入力を 1 ビット単位で分解可能であり，PQSP で計算可能である． □

次にこれが正当性および秘匿性を満たすことを示す．

定理 4.1.5 (正当性) すべての入力 $x_1, \ldots, x_n \in \{0,1\}^n$ およびすべての 1 量子ビット Haar ランダムユニタリ行列から生成されるメッセージ $m_1, \ldots, m_n$ について，$\mathsf{Dec}_{\mathrm{SBF}}(m_1, \ldots, m_n) = \mathsf{Dec}(m)\,|0\rangle$ の出力を計算基底で測定した結果は必ず $f(x)$ と等しくなる．ただし，Dec は PQSP の構成で使用される復号関数である．

定理 4.1.5 の証明. PQSP の性質より，$\mathsf{Dec}(m)$ は必ず QSP の出力行列 $U(\theta)$ と同じ行列を出力することおよび，[MKB+21] より QSP を用いて $f(x) = 0$ のとき $\mathbb{I}$，$f(x) = 1$ のとき iX を出力するような計算が可能であることから評価者は確率 1 で $f(x)$ を手に入れることができることは明らかである． □

定理 4.1.6 (秘匿性) 各参加者から送られてくるメッセージ $(m_1, \ldots, m_n)$ が従う分布を $(\mathcal{M}_1, \ldots, \mathcal{M}_n)$ とする．このとき，$\mathsf{Sim}(f(x))$ の出力分布が $(\mathcal{M}_1, \ldots, \mathcal{M}_n)$ と同一分布となるような乱択関数 Sim が存在する．

定理 4.1.6 の証明. はじめに各参加者から送られてくるメッセージの分布を考える．PQSP の構成より，この分布は独立な $nL+1$ 個の 1 量子ビット上の Haar ランダムユニタリ行列をとる確率変数について，PQSP の復号関数で計算される計算結果が $(iX)^{f(x)}$ となる条件を

満たす確率分布になっていることは容易に理解できる．一般性を損なわずに最終要素以外をそれぞれが独立な 1 量子ビット上の Haar ランダムユニタリ行列とした場合，最終要素 $m_{n,L}$ は

$$m_{n,L} = \prod_{k=n-1}^{1} m_{k,L}^{\dagger} \cdot \prod_{\ell=L-1}^{1} \prod_{k=n}^{1} m_{k,\ell}^{\dagger} \cdot m_{1,0}^{\dagger} \cdot (iX)^{f(x)}$$

で決定されることが分かる．次にシミュレータ $\mathsf{Sim}(f(x))$ の分布を考える．

$$\mathsf{Sim}(f(x)) = (S_{1,0}, S_{1,1}, \ldots, S_{1,L}, S_{2,1}, \ldots, S_{2,L}, \ldots, S_{n,1}, \ldots, S_{n,L})$$

とし，$S_{k,\ell}$ の分布を $\mathcal{S}_{k,\ell}$ とする．最終要素を除いたすべての要素について，それぞれが独立な 1 量子ビット上の Haar ランダムユニタリ行列をとり，最終要素を

$$S_{n,L} = \prod_{k=n-1}^{1} S_{k,L}^{\dagger} \cdot \prod_{\ell=L-1}^{1} \prod_{k=n}^{1} S_{k,\ell}^{\dagger} \cdot S_{1,0}^{\dagger} \cdot (iX)^{f(x)}$$

とする．これらを PQSP の復号関数の入力として計算すると $(iX)^{f(x)}$ となることは容易に理解できる．よって，$\mathsf{Sim}(f(x))$ の分布は PQSP の復号関数で計算される計算結果が $(iX)^{f(x)}$ となる条件付確率になっていることが分かる．以上より，$\mathsf{Sim}(f(x))$ と $\mathcal{M}$ の分布が同一となる乱択関数 Sim が存在することが分かる． □

定理 4.1.3 より，有限精度の近似による対称ブール関数の計算誤りについても桁数 k に対して誤り確率が $O(nL2^{-k})$ で押さえられる．このときの参加者が評価者に送る通信ビット数は $O(nLk)$ となる．

4.2 秘密 1 量子ビットプログラム (P1QP)

秘密 1 量子ビットプログラム (P1QP) は Cosentino らによって提案された 1 量子ビットモデル [CKP13] を PSM モデルにおいて定義し，それを基に構成したプロトコルである．P1QP では PSM モデルにおいて，秘密の 1 ビット入力を持つ複数の参加者と一人の独立した評価者が共同であるブール関数を計算することが目的である．

はじめに，定理 3.3.2 を少し拡張する．これは本研究の成果を述べる上で必要不可欠ではないため，読み飛ばしても構わない．その場合は以下で出現する定理 4.2.1 を定理 3.3.2 に置き換えてもらいたい．

定理 4.2.1 (拡張 1 量子ビットモデル (+XOR)) 2 入力の AND と OR, NOT, および XOR を用いて深さ d の古典回路で計算可能な任意の関数は，長さ 4^d の 1 量子ビットプログラムで計算することが可能である．

定理 4.2.1 の証明. 証明は帰納法を用いて行う．定理 3.3.2 より，OR，AND，NOT ゲートを用いた深さ d の古典回路で計算可能な任意の関数については証明されているため，追加で考えるゲートは XOR のみである．定理 3.3.2 の証明の「2 つのケース」に XOR のケースを追加する．

C が XOR ゲートと二つの部分回路 C' と C'' から構成されている場合を考える．F' と F'' をそれぞれ C' と C'' を計算する長さ 4^{d-1} の 1 量子ビットプログラムとし，次の 1 量子ビットプログラムを考える．

$$F = X^{C'(x)}X^{C''(x)} = X^{C'(x)\oplus C''(x)} = X^{C(x)}.$$

帰納仮説により，C' および C'' を計算する 1 量子ビットプログラム F' および F'' が存在するので，$X^{C'(x)}$ および $X^{C''(x)}$ は計算可能である．また，F' と F'' の長さは 4^{d-1} であるので，F の長さは 4^d となる． □

定理 3.3.2 では XOR を一つのゲートとみなした 1 量子ビットプログラムの長さが 16^d であるのに対して，定理 4.2.1 では 1 量子ビットプログラムの長さが 4^d で押さえることができる．一般的な算術回路では XOR をビット和，AND をビット積と考えるため，定理 4.2.1 の方が一般的であるといえる．

次に，PSM モデルにおける 1 量子ビットプログラムを構成する．構成にあたって，はじめに秘匿性を考慮しない PSM モデルにおける 1 量子ビットプログラムを構成する．

定理 4.2.1 より，それぞれが入力ビット x_k を持つ n 人の参加者が評価者を通してブール関数 $C(x_1,\ldots,x_n)$ を計算するとする．このとき，1 量子ビットプログラム F は以下のようにあらわされる．

$$F = U_0 \prod_{\ell=1}^{L} X^{x_{i_\ell}} U_\ell$$

ここで，$U_\ell(\ell = 0,\ldots,L)$ は 1 量子ビットプログラムで使用される 1 量子ビットを操作するユニタリ行列であり，$i_\ell(\ell = 1,\ldots,L)$ は入力ビットのインデックス列である．パラメータ L はブール関数 $C(x_1,\ldots,x_n)$ を計算する回路の深さ d について最大 4^d である (定理 4.2.1 より)．

これらを基に秘密 1 量子ビットプログラムを構成する．

構成 (P1QP $\Pi_{\mathbf{P1QP}}$)

n 人の古典参加者 P_k はそれぞれ入力ビット x_k を持っており，独立した量子評価者を通じてブール関数 $C(x_1,\ldots,x_n)$ を計算するとする．また，関数を計算する回路における 1 量子ビットプログラムは参加者および評価者に公開されているとし，各参加者の入力に依存する行列 $X^{x_{i_\ell}}(\ell = 1,\ldots,L)$ の入力インデックス列 i_ℓ についても参加者および評価者に公開されているものとする．以降出現する Enq と Deq，Pop について，m.Enq(A) はリスト m の末尾に要素 A を追加する操作 (enqueue) であり，m.Deq はリスト m の先頭要素を取り出す操作 (dequeue) であり，m.Pop はリスト m の末尾要素を取り出す操作 (pop) である．このとき，P1QP Π_{P1QP} は以下のような手順で実行される．

Step 1.

各参加者 P_k は事前に入力に依存しない独立な 1 量子ビットに対する Haar ランダムユニタリ行列の列 $R = (R_\ell :\ \ell = 1,\ldots,L)$ を共有しておく．また，各参加者は事前に空のリスト m_k を作成しておく．

Step 2.

各参加者 P_k は自身の入力 x_k に基づいて以下の操作を行う．

- P_1 は以下の操作後，リスト m_1 を評価者に送信する．
  - $m_1.\mathsf{Enq}(U_0 \cdot R_1)$
  - $\ell \in [L-1]$ について，$i_\ell = 1$ であるならば，$m_1.\mathsf{Enq}(R_\ell^\dagger \cdot X^{x_1} \cdot U_\ell \cdot R_{\ell+1})$ を行う．
  - $i_L = 1$ であるならば，$m_1.\mathsf{Enq}(R_L^\dagger \cdot X^{x_1} \cdot U_L)$ を行う．
- $P_k (k = 2, \ldots, n)$ は以下の操作後，リスト m_k を評価者に送信する．
  - $\ell \in [L-1]$ について，$i_\ell = k$ であるならば，$m_k.\mathsf{Enq}(R_\ell^\dagger \cdot X^{x_k} \cdot U_\ell \cdot R_{\ell+1})$ を行う．
  - $i_L = k$ であるならば，$m_k.\mathsf{Enq}(R_L^\dagger \cdot X^{x_k} \cdot U_L)$ を行う．

Step 3.
評価者は以下の復号関数 Dec を計算し，その結果を計算基底で測定する．

$$\begin{aligned}\mathsf{Dec}(m_1, \ldots, m_n) &= m_1.\mathsf{Deq}\left(\prod_{\ell=1}^{L} m_{i_\ell}.\mathsf{Deq}\right)|0\rangle \\ &= |C(x_1, \ldots, x_n)\rangle \end{aligned} \tag{4.8}$$

次に，P1QP が以下の正当性および秘匿性についての定理を満たすことを証明する．

定理 4.2.2 (正当性 (P1QP)) すべての入力 $x_1, \ldots, x_n \in \{0,1\}^n$ およびすべての 1 量子ビット Haar ランダムユニタリ行列から生成されるリスト $m_1, \ldots, m_n$ について，$\mathsf{Dec}(m_1, \ldots, m_n)$ の出力を計算基底で測定した結果は必ず $C(x_1, \ldots, x_n)$ と等しくなる．

定理 4.2.2 の証明. P1QP の構成で用いられる式 (4.8) から，復号関数を計算した結果を計算基底で測定することで，評価者はすべてのリスト $m_1, \ldots, m_n$ について確率 1 で $C(x_1, \ldots, x_n)$ を出力することができることは明らかである． □

定理 4.2.3 (秘匿性 (P1QP)) 各参加者から送られてくるリスト $(m_1, \ldots, m_n)$ が従う分布を $(\mathcal{M}_1, \ldots, \mathcal{M}_n)$ とする．このとき，$\mathsf{Sim}(C(x_1, \ldots, x_n))$ の出力分布が $(\mathcal{M}_1, \ldots, \mathcal{M}_n)$ と同一分布となるような乱択関数 Sim が存在する．

定理 4.2.3 の証明. はじめに各参加者から送られてくるメッセージリストの分布を考える．P1QP の構成より，この分布は独立な $L+1$ 個の 1 量子ビット上の Haar ランダムユニタリ行列をとる確率変数について，P1QP の復号関数で計算される行列積が $X^{C(x_1,\ldots,x_n)}$ となる条件を満たす確率分布になっていることは容易に理解できる．一般性を損なわずにリスト m_{i_L} の最終要素以外をそれぞれが独立な 1 量子ビット上の Haar ランダムユニタリ行列とした場合，m_{i_L} の最終要素は

$$m_{i_L} = \left(\prod_{\ell=L}^{1} (m_{i_\ell}.\mathsf{Pop})^\dagger\right) \cdot (m_1.\mathsf{Pop})^\dagger \cdot X^{C(x_1,\ldots,x_n)}$$

で決定されることが分かる．次にシミュレータ $\mathsf{Sim}(C(x_1, \ldots, x_n))$ の分布を考える．
$\mathsf{Sim}(C(x_1, \ldots, x_n)) = (S_1, \ldots, S_n)$ とし，S_k の分布を $\mathcal{S}_k$ とする．ただし，S_k はリストである．$S_1.\mathsf{Enq}(HR)$ を実行した後，$\ell = 1, \ldots, L-1$ について順に $S_{i_\ell}.\mathsf{Enq}(HR)$ を実行する．

ただし，HR はその都度一様ランダムに選ばれる独立した Haar ランダムユニタリ行列である．また，S_{i_L} の最終要素を

$$S_{i_L} = \left(\prod_{\ell=L}^{1} (S_{i_\ell}.\mathsf{Pop})^\dagger \right) \cdot (S_1.\mathsf{Pop})^\dagger \cdot X^{C(x_1,\ldots,x_n)}$$

とすると，これらを P1QP の復号関数の入力として計算するとその行列積部分が $X^{C(x_1,\ldots,x_n)}$ となることは容易に理解できる．よって，$\mathsf{Sim}(C(x_1,\ldots,x_n))$ の分布は PQSP の復号関数で計算される計算結果が $X^{C(x_1,\ldots,x_n)}$ となる条件付確率になっていることが分かる．以上より，$\mathsf{Sim}(C(x_1,\ldots,x_n))$ とリスト $(m_1,\ldots,m_n)$ の分布が同一となる乱択関数 Sim が存在することが分かる． □

第5章　まとめ

本研究では，暗号理論の観点から QSP の応用の検討を行い，その結果，PSM モデルにおいて各参加者の入力情報および計算内容を秘匿した状態で QSP の出力ユニタリ行列を計算することが可能な秘密量子信号処理 (PQSP) を提案した．また，参加者 n 人で位相列長が $L+1$ であり，行列の要素の実部と虚部がそれぞれ k ビットであるとき，正当性の誤り確率が $O(nL2^{-k})$，通信量は $O(nLk)$ となることを示した．PQSP の応用例として，PSM モデルにおいて 1 量子ビットメモリ上での対称ブール関数の計算が可能であることを示した．これは，[MKB+21] のプロトコルで用いられている QSP と PQSP を置換することで実現可能である．この手法は 1 量子ビットメモリ上での対称ブール関数の計算が可能であるという量子の優位性と秘匿性を両立させたものとなっている．

また，PSM モデルにおいて 1 量子ビットメモリで任意のブール関数を計算可能なプロトコルである秘密 1 量子ビットプログラム (P1QP) を提案した．これは [CKP13] を PSM モデルで動作するように PQSP で用いた秘匿化手法を適用したプロトコルであり，PQSP を用いた対称ブール関数の計算よりも大きな関数である任意のブール関数を計算可能であることからこちらの方がより一般的である．

5.1　今後の課題

今後の課題としては大きく三つある．

一つ目は，PQSP を用いたより一般的な関数の計算の可否である．PQSP を用いることで，PSM モデルにおいて対称ブール関数の計算が可能であることは以上の通りである．これは，対称ブール関数を入力情報のハミング重みのみで計算することが可能であることを利用している．ハミング重みのみを使用していることから，X 軸回転行列 $W(y)$ を分解することが可能となり，入力情報の秘匿化を行うことが可能となる．つまり，入力情報のハミング重みのみを利用して QSP で計算することが可能な関数であれば，PQSP の構成を適用することが可能であるといえる．ハミング重み以上の情報を用いる場合については，より一般的な QSP の構成が必要であると考えられるため，本構成を適用することが可能であるかは不明である．

二つ目は，QSVT への応用である．QSVT は Grover の探索アルゴリズムや逆行列計算を行う HHL アルゴリズムなど，様々な量子アルゴリズムを統一的に記述可能な技術である．QSVT は QSP の一般化であり，QSP を含めた様々な技術が構成要素となっている．つまり，QSVT で使用されている QSP を PQSP と置換することで，PSM モデルにおける Grover の探索アルゴリズムや HHL アルゴリズムを実現することができる可能性がある．ただし，QSVT では上述の通り様々な技術が使用されているため，PQSP を適用した際に正当性および秘匿性に問題が無いことを証明することが必要不可欠である．また，PSM モデルにおける Grover の探索や HHL がどのような意味を成すかを考察する必要がある．

三つ目は，PQSP，P1QP の実装である．QSP は 1 量子ビットの量子回路で実現可能なア

ルゴリズムであり，その性質はPQSPでも引き継がれている．論文執筆時点で1量子ビットの量子回路を実際に実行することが可能な量子計算機が存在し，これを用いてPQSPを実装することが可能である．また，PQSPでは入力情報を持つ参加者は古典計算機および古典通信を用いて評価者に情報を伝送可能である．これは，参加者の人数分の量子計算機を用意することが難しい現代でもPQSPを実現することが容易であるということを示唆している．PQSPの実装・評価を行うことは，量子技術を利用した秘密計算の有用性および課題点を導き出すにあたり非常に有益であると考えられる．P1QPについても同様である．

謝辞

本研究，論文執筆を進めるにあたり，多くのご指導ご鞭撻を賜りました河内亮周教授，研究活動における様々な場面でお世話になりました小野寺香里事務員，森岡幸音元事務員，研究の如何を問わず多くの助言や意見を頂戴いたしましたコンピュータソフトウェア研究室の皆様に深く御礼申し上げます.

参考文献

[AGK+05] Farid Ablayev, Aida Gainutdinova, Marek Karpinski, Cristopher Moore, and Christopher Pollett. On the computational power of probabilistic and quantum branching program. *Information and Computation*, 203(2):145–162, 2005.

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *International Conference on Computer System and Signal Processing, IEEE*, pages 175–179, 1984.

[BY22] Zvika Brakerski and Henry Yuen. Quantum garbled circuits. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing(STOC 2022)*, pages 804–817, 2022.

[CKP13] Alessandro Cosentino, Robin Kothari, and Adam Paetznick. Dequantizing read-once quantum formulas. In *8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013)*, volume 22 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 80–92, 2013.

[FKN94] Uriel Feige, Joe Kilian, and Moni Naor. A minimal model for secure computation (extended abstract). In *Proceedings of the 26th Annual ACM Symposium on Theory of Computing(STOC 1994)*, pages 554–563, 1994.

[Gil19] András Gilyén. *Quantum Singular Value Transformation & Its Algorithmic Applications*. PhD thesis, University of Amsterdam, 2019.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, 1996.

[GSLW19] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 193–204. ACM, 2019.

[Haa19] Jeongwan Haah. Product Decomposition of Periodic Functions in Quantum Signal Processing. *Quantum*, 3:190, 2019.

[HHL09] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Phys. Rev. Lett.*, 103:150502, 2009.

[IK97] Yuval Ishai and Eyal Kushilevitz. Private simultaneous messages protocols with applications. In *Proceedings of the 5th Israeli Symposium on Theory of Computing and Systems (ISTCS1997)*, pages 174–183, 1997.

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 20–31. Association for Computing Machinery, 1988.

[KN21] Akinori Kawachi and Harumichi Nishimura. Communication complexity of private simultaneous quantum messages protocols. In *2nd Conference on Information-Theoretic Cryptography (ITC 2021)*, volume 199 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 20:1–20:19. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

[LC17] Guang Hao Low and Isaac L. Chuang. Optimal hamiltonian simulation by quantum signal processing. *Phys. Rev. Lett.*, 118:010501, 2017.

[LYC16] Guang Hao Low, Theodore J. Yoder, and Isaac L. Chuang. Methodology of resonant equiangular composite quantum gates. *Phys. Rev. X*, 6:041067, 2016.

[MKB+21] Dmitri Maslov, Jin-Sung Kim, Sergey Bravyi, Theodore J. Yoder, and Sarah Sheldon. Quantum advantage for computations with limited space. *Nature Physics*, 17(8):894–897, 2021.

[MRTC21] John M. Martyn, Zane M. Rossi, Andrew K. Tan, and Isaac L. Chuang. Grand unification of quantum algorithms. *PRX Quantum*, 2:040203, 2021.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2010.

[NIS17] NIST. Post-Quantum Cryptography. `https://csrc.nist.gov/projects/post-quantum-cryptography`, 2017. 2024 年 1 月 29 日閲覧.

[Ozo09] Maris A. Ozols. How to generate a random unitary matrix. 2009.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[石小河 +12] 石坂智, 小川朋宏, 河内亮周, 木村元, and 林正人. **量子情報科学入門**. 共立出版株式会社, 2012.