

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2008-294666
(P2008-294666A)

(43) 公開日 平成20年12月4日(2008.12.4)

(51) Int.Cl. F I テーマコード(参考)
H04L 9/12 (2006.01) H04L 9/00 631 5J104

審査請求 未請求 請求項の数 4 O L (全 11 頁)

(21) 出願番号 特願2007-136984 (P2007-136984)
(22) 出願日 平成19年5月23日(2007.5.23)
特許法第30条第1項適用申請有り 研究集会名 修士
論文審査発表会 主催者名 国立大学法人東京大学 開
催日 平成19年1月19日

(71) 出願人 503360115
独立行政法人科学技術振興機構
埼玉県川口市本町4丁目1番8号
(74) 代理人 100088155
弁理士 長谷川 芳樹
(74) 代理人 100124291
弁理士 石田 悟
(74) 代理人 100128107
弁理士 深石 賢治
(72) 発明者 村尾 美緒
東京都文京区本郷7-3-1
(72) 発明者 田中 雄
東京都文京区本郷7-3-1
Fターム(参考) 5J104 AA05 AA16 EA04 EA15 NA02

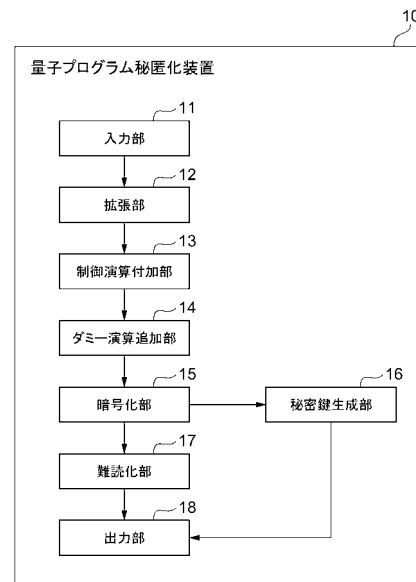
(54) 【発明の名称】 量子プログラム秘匿化装置及び量子プログラム秘匿化方法

(57) 【要約】

【課題】 量子プログラムを、その演算内容を知られずに権限を有する者に対して実行させる。

【解決手段】 量子プログラム秘匿化装置10は、入力された量子プログラムを含み、量子プログラムの入力量子ビット空間に加えて、量子秘密鍵に応じた量子秘密鍵量子ビット空間を有する拡張量子プログラムを生成する拡張部12と、拡張量子プログラムを、量子秘密鍵量子ビット空間が所定の状態である場合に量子プログラムを実行する制御演算を行うように書き換える制御演算付加部13と、拡張量子プログラムに、量子秘密鍵量子ビット空間の状態に対して演算を行う第1の量子ゲート列及び第2の量子ゲート列を追加する暗号化部15と、第1の量子ゲート列の逆演算を行うことによって量子秘密鍵を生成する秘密鍵生成部16と、第1の量子ゲート列が追加された拡張量子プログラムに対して難読化を行う難読化部17とを備える。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

ユニタリ変換を示す量子ゲート列を含む量子プログラムを入力する入力手段と、

前記入力手段により入力された量子プログラムを含み、当該量子プログラムの入力量子ビット空間に加えて、量子秘密鍵に応じた量子ビット空間である量子秘密鍵量子ビット空間を有する拡張量子プログラムを生成する拡張手段と、

前記拡張手段により生成された拡張量子プログラムを、前記量子秘密鍵量子ビット空間が所定の状態である場合に、当該拡張量子プログラムに含まれる量子プログラムを実行する制御演算を行うように書き換える制御演算付加手段と、

前記演算制御付加手段により書き換えられる拡張量子プログラムに、前記制御演算が行われる前の前記量子秘密鍵量子ビット空間の状態に対して演算を行う第 1 の量子ゲート列を追加すると共に当該拡張量子プログラムに、前記制御演算が行われた後の前記量子秘密鍵量子ビット空間の状態に対して演算を行う第 2 の量子ゲート列を追加する暗号化手段と、

10

前記量子秘密鍵量子ビット空間の前記所定の状態に対して、前記暗号化手段により追加された第 1 の量子ゲート列の逆演算を行うことによって量子秘密鍵を生成する秘密鍵生成手段と、

前記暗号化手段により前記第 1 の量子ゲート列が追加された拡張量子プログラムに対して、量子ゲート列の入れ替え及び量子ゲート列の追加の少なくとも何れかを、予め記憶したルールに基づいて行う難読化手段と、

20

前記難読化手段による処理が行われた拡張量子プログラム、及び秘密鍵生成手段により生成された量子秘密鍵を出力する出力手段と、
を備える量子プログラム秘匿化装置。

【請求項 2】

前記量子秘密鍵量子ビット空間には、前記制御演算付加手段による前記拡張量子プログラムの書き換えに係る制御演算に係わらないダミー空間が含まれており、

前記拡張手段により生成された拡張量子プログラムに、前記ダミー空間の状態に対して演算を行うダミー量子ゲート列を追加するダミー演算追加手段を更に備える、
ことを特徴とする請求項 1 に記載の量子プログラム秘匿化装置。

【請求項 3】

30

前記入力手段は、複数の前記量子プログラムを入力し、

前記制御演算付加手段は、前記拡張手段により生成された拡張量子プログラムを、前記量子秘密鍵量子ビット空間の状態に応じて、当該拡張量子プログラムに含まれる量子プログラムの何れかを実行する制御演算を行うように書き換える、
ことを特徴とする請求項 1 又は 2 に記載の量子プログラム秘匿化装置。

【請求項 4】

量子プログラム秘匿化装置による量子プログラム秘匿化方法であって、

ユニタリ変換を示す量子ゲート列を含む量子プログラムを入力する入力ステップと、

前記入力ステップにおいて入力された量子プログラムを含み、当該量子プログラムの入力量子ビット空間に加えて、量子秘密鍵に応じた量子ビット空間である量子秘密鍵量子ビット空間を有する拡張量子プログラムを生成する拡張ステップと、

40

前記拡張ステップにおいて生成された拡張量子プログラムを、前記量子秘密鍵量子ビット空間が所定の状態である場合に、当該拡張量子プログラムに含まれる量子プログラムを実行する制御演算を行うように書き換える制御演算付加ステップと、

前記演算制御付加ステップにおいて書き換えられる拡張量子プログラムに、前記制御演算が行われる前の前記量子秘密鍵量子ビット空間の状態に対して演算を行う第 1 の量子ゲート列を追加すると共に当該拡張量子プログラムに、前記制御演算が行われた後の前記量子秘密鍵量子ビット空間の状態に対して演算を行う第 2 の量子ゲート列を追加する暗号化ステップと、

前記量子秘密鍵量子ビット空間の前記所定の状態に対して、前記暗号化ステップにおい

50

て追加された第 1 の量子ゲート列の逆演算を行うことによって量子秘密鍵を生成する秘密鍵生成ステップと、

前記暗号化ステップにおいて前記第 1 の量子ゲート列が追加された拡張量子プログラムに対して、量子ゲート列の入れ替え及び量子ゲート列の追加の少なくとも何れかを、予め記憶したルールに基づいて行う難読化ステップと、

前記難読化ステップにおける処理が行われた拡張量子プログラム、及び秘密鍵生成ステップにおいて生成された量子秘密鍵を出力する出力ステップと、を含む量子プログラム秘匿化方法。

【発明の詳細な説明】

【技術分野】

10

【0001】

本発明は、ユニタリ変換を示す量子ゲート列を含む量子プログラムを秘匿化する量子プログラム秘匿化装置、及び当該量子プログラム秘匿化装置による量子プログラム秘匿化方法に関する。

【背景技術】

【0002】

公開通信路を通じて情報を安全に送るために現在広く用いられている公開鍵暗号は、古典計算機による計算量によって安全が保障されているものである。また、BB84等これまでに提案された量子暗号（量子鍵分配）では、認証が正しく行われていれば無条件安全性が保障される。しかし、上記の方法では、量子計算機が用いられた場合には安全性が保障されない。量子系を用いた公開鍵プロトコルについては、下記の非特許文献 1 に記載されているような研究がある。

20

【非特許文献 1】A. Kawachi et al, Proc.EUROCRYPT 2005, LNCS 3494, 268, 2005

【発明の開示】

【発明が解決しようとする課題】

【0003】

ところで、ユニタリ変換を示す量子ゲートを含む量子プログラムを、作成者を特定（認証）した上で公開して、当該量子プログラムを実行する権限を有する者に対して実行させる態様が考えられる。しかしながら、非特許文献 1 に記載された技術では、量子状態を公開鍵として用いているため、当該量子プログラムを認証して公開するプロトコルとして用いるには困難がある。更に、上記のような態様において、当該量子プログラムの演算内容を実行者に知られずに公開する、即ち、量子プログラムを秘匿化することが必要である場合があると考えられるが、これを実現する技術は提供されていない。

30

【0004】

本発明は、以上の問題点を解決するためになされたものであり、量子プログラムを、その演算内容を知られずに権限を有する者に対して実行させることを可能とする量子プログラム秘匿化装置及び量子プログラム秘匿化方法を提供することを目的とする。

【課題を解決するための手段】

【0005】

上記目的を達成するために、本発明に係る量子プログラム秘匿化装置は、ユニタリ変換を示す量子ゲート列を含む量子プログラムを入力する入力手段と、入力手段により入力された量子プログラムを含み、当該量子プログラムの入力量子ビット空間に加えて、量子秘密鍵に応じた量子ビット空間である量子秘密鍵量子ビット空間を有する拡張量子プログラムを生成する拡張手段と、拡張手段により生成された拡張量子プログラムを、量子秘密鍵量子ビット空間が所定の状態である場合に、当該拡張量子プログラムに含まれる量子プログラムを実行する制御演算を行うように書き換える制御演算付加手段と、演算制御付加手段により書き換えられる拡張量子プログラムに、制御演算が行われる前の量子秘密鍵量子ビット空間の状態に対して演算を行う第 1 の量子ゲート列を追加すると共に当該拡張量子プログラムに、制御演算が行われた後の量子秘密鍵量子ビット空間の状態に対して演算を行う第 2 の量子ゲート列を追加する暗号化手段と、量子秘密鍵量子ビット空間の所定の状

40

50

態に対して、暗号化手段により追加された第1の量子ゲート列の逆演算を行うことによって量子秘密鍵を生成する秘密鍵生成手段と、暗号化手段により第1の量子ゲート列が追加された拡張量子プログラムに対して、量子ゲート列の入れ替え及び量子ゲート列の追加の少なくとも何れかを、予め記憶したルールに基づいて行う難読化手段と、難読化手段による処理が行われた拡張量子プログラム、及び秘密鍵生成手段により生成された量子秘密鍵を出力する出力手段と、を備えることを特徴とする。

【0006】

本発明に係る量子プログラム秘匿化装置では、量子プログラムから拡張量子プログラムが生成される。生成される拡張量子プログラムは、上記制御演算と第1の量子ゲート列とによって、量子秘密鍵量子ビット空間に量子秘密鍵が入力されなければ、量子プログラムが実行されない。即ち、量子秘密鍵を有した者でなければ、量子プログラムは実行されない。また、上記の拡張量子プログラムは、ゲート列の入れ替え及びゲート列の追加の少なくとも何れかの難読化が行われるため、その演算内容が実行者に知られることはない。また、第2のゲート列の存在により、難読化された拡張量子プログラムによって演算が行われて出力される量子秘密鍵が、制御演算に応じた所定の状態となることがなく、安全性の高い秘匿化を行うことができる。これらにより、本発明に係る量子プログラム秘匿化装置によれば、量子プログラムを、その演算内容を知られずに権限を有する者に対して実行させることを可能とする。

10

【0007】

量子秘密鍵量子ビット空間には、制御演算付加手段による拡張量子プログラムの書き換えに係る制御演算に係わないダミー空間が含まれており、量子プログラム秘匿化装置は、拡張手段により生成された拡張量子プログラムに、ダミー空間の状態に対して演算を行うダミー量子ゲート列を追加するダミー演算追加手段を更に備える、ことが望ましい。この構成によれば、量子秘密鍵量子ビット空間のうちの、どのビットが量子秘密鍵に係るものを分かりにくくするため、更に安全性の高い秘匿化を行うことができる。

20

【0008】

入力手段は、複数の量子プログラムを入力し、制御演算付加手段は、拡張手段により生成された拡張量子プログラムを、量子秘密鍵量子ビット空間の状態に応じて、当該拡張量子プログラムに含まれる量子プログラムの何れかを実行する制御演算を行うように書き換える、ことが望ましい。この構成によれば、本発明に係る量子プログラム秘匿化装置による処理が行われた一つの拡張量子プログラムにより、複数の量子プログラムを実行できるので、ユーザの利便性を向上させることができる。

30

【0009】

ところで、本発明は、上記のように量子プログラム秘匿化装置の発明として記述できる他に、以下のように量子プログラム秘匿化方法の発明としても記述することができる。これはカテゴリが異なるだけで、実質的に同一の発明であり、同様の作用及び効果を奏する。

【0010】

即ち、本発明に係る量子プログラム秘匿化方法は、量子プログラム秘匿化装置による量子プログラム秘匿化方法であって、ユニタリ変換を示す量子ゲート列を含む量子プログラムを入力する入力ステップと、入力ステップにおいて入力された量子プログラムを含み、当該量子プログラムの入力量子ビット空間に加えて、量子秘密鍵に応じた量子ビット空間である量子秘密鍵量子ビット空間を有する拡張量子プログラムを生成する拡張ステップと、拡張ステップにおいて生成された拡張量子プログラムを、量子秘密鍵量子ビット空間が所定の状態である場合に、当該拡張量子プログラムに含まれる量子プログラムを実行する制御演算を行うように書き換える制御演算付加ステップと、演算制御付加ステップにおいて書き換えられる拡張量子プログラムに、制御演算が行われる前の量子秘密鍵量子ビット空間の状態に対して演算を行う第1の量子ゲート列を追加すると共に当該拡張量子プログラムに、制御演算が行われた後の量子秘密鍵量子ビット空間の状態に対して演算を行う第2の量子ゲート列を追加する暗号化ステップと、量子秘密鍵量子ビット空間の所定の状態

40

50

に対して、暗号化ステップにおいて追加された第1の量子ゲート列の逆演算を行うことによって量子秘密鍵を生成する秘密鍵生成ステップと、暗号化ステップにおいて第1の量子ゲート列が追加された拡張量子プログラムに対して、量子ゲート列の入れ替え及び量子ゲート列の追加の少なくとも何れかを、予め記憶したルールに基づいて行う難読化ステップと、難読化ステップにおける処理が行われた拡張量子プログラム、及び秘密鍵生成ステップにおいて生成された量子秘密鍵を出力する出力ステップと、を含むことを特徴とする。

【発明の効果】

【0011】

本発明において生成される拡張量子プログラムは、上記制御演算と第1の量子ゲート列とによって、量子秘密鍵量子ビット空間に量子秘密鍵が入力されなければ、量子プログラムが実行されない。即ち、量子秘密鍵を有した者でなければ、量子プログラムは実行されない。また、上記の拡張量子プログラムは、ゲート列の入れ替え及びゲート列の追加の少なくとも何れかの難読化が行われるため、その演算内容が実行者に知られることはない。また、第2のゲート列の存在により、難読化された拡張量子プログラムによって演算が行われて出力される量子秘密鍵が、制御演算に応じた所定の状態となることがなく、安全性の高い秘匿化を行うことができる。これらにより、本発明によれば、量子プログラムを、その演算内容を知られずに権限を有する者に対して実行させることを可能とする。

10

【発明を実施するための最良の形態】

【0012】

以下、図面と共に本発明に係る量子プログラム秘匿化装置及び量子プログラム秘匿化方法の好適な実施形態について詳細に説明する。なお、図面の説明においては同一要素には同一符号を付し、重複する説明を省略する。

20

【0013】

図1に本実施形態に係る量子プログラム秘匿化装置10の機能的な構成を示す。量子プログラム秘匿化装置10は、ユニタリ変換を示す量子ゲート列を含む量子プログラムを、秘匿化する装置である。この秘匿化は、量子プログラムの演算内容を知られずに権限を有する者に対して量子プログラムを実行させることを可能とするように行われる。図2に本実施形態で処理される処理される量子プログラム $u_1 \sim u_k$ (k は、量子プログラムのインデックスを示す)を示す。図2において、横線は各量子ビットを表し、矩形は量子ゲート列を表す。図2に示す量子プログラムは、通常、左から右に順に実行される。なお、本実施形態では、量子プログラム秘匿化装置10の処理対象は、複数の量子プログラム $u_1 \sim u_k$ である。但し、1つの量子プログラムを処理対象としてもよい。

30

【0014】

量子プログラム $u_1 \sim u_k$ 各々は、量子計算機等の情報処理装置により実行される。具体的には、例えば、イオントラップあるいはNMR (Nuclear Magnetic Resonance: 核磁気共鳴)を用いた量子計算機により実行される。図2に示すように、量子プログラム $u_1 \sim u_k$ 各々は、1以上の量子ビットからなる入力量子ビット空間21を有しており、当該入力量子ビット空間に対する量子情報の入力に対して、量子ゲート列により演算処理を行って、演算処理後の量子情報の出力を行う。

【0015】

引き続き、量子プログラム秘匿化装置10の機能構成について詳細に説明する。図1に示すように、量子プログラム秘匿化装置10は、入力部11と、拡張部12と、制御演算付加部13と、ダミー演算追加部14と、暗号化部15と、秘密鍵生成部16と、難読化部17と、出力部18とを備える。

40

【0016】

入力部11は、複数の量子プログラム $\{u_k\}$ を入力する入力手段である。量子プログラム $\{u_k\}$ の入力は、例えば、量子プログラム秘匿化装置10に接続された外部装置から送信された量子プログラム $\{u_k\}$ を受信することにより行われる。また、量子プログラム秘匿化装置10に格納されている量子プログラム $\{u_k\}$ を、ユーザの操作等をトリガとして読み出すことによって入力することとしてもよい。入力部11は、入力した量子

50

プログラム $\{u_k\}$ を拡張部 12 に出力する。

【0017】

拡張部 12 は、図 2 に示すように、入力部 11 により入力された量子プログラム $\{u_k\}$ を含む拡張量子プログラム U' を生成する拡張手段である。拡張量子プログラム U' は、量子プログラム $\{u_k\}$ の入力量子ビット空間 21 に加えて、量子秘密鍵に依じた量子ビット空間である、1 以上の量子ビットからなる量子秘密鍵量子ビット空間 22 を有する。即ち、拡張部 12 は、量子プログラム $\{u_k\}$ を、量子ビット空間を量子秘密鍵量子ビット空間 22 分増加させた（自由度を増加させた）拡張量子プログラム U' を生成する。具体的には、量子ビット空間の増加は、拡張量子プログラム U' の有する量子ビット空間の定義を上記のように設定することにより行われる。量子秘密鍵は、量子秘密鍵量子ビット空間 22 分の量子ビットの状態を有する量子情報であり、量子プログラム $\{u_k\}$ を実行するためのものである。量子秘密鍵については、より詳しく後述する。なお、量子秘密鍵量子ビット空間 22 には、後述するように量子プログラム $\{u_k\}$ の実行の可否には係わらないダミー空間 23 が含まれている。

10

【0018】

制御演算付加部 13 は、生成された拡張量子プログラム U' を、量子秘密鍵量子ビット空間 22 が所定の状態である場合に、当該拡張量子プログラム U' に含まれる量子プログラム $\{u_k\}$ を実行する制御演算を行うように書き換える制御演算付加手段である。上記の所定の状態は、図 2 に示すように量子プログラム u_1 には状態 A_1 、量子プログラム u_k には状態 A_k のように量子プログラム $\{u_k\}$ 毎に互いに異なるように一意に定められる。即ち、上記の制御演算は、量子秘密鍵量子ビット空間 22 が状態 A_1 であった場合には量子プログラム u_1 が実行されるように、また、量子秘密鍵量子ビット空間 22 が状態 A_k であった場合には量子プログラム u_k が実行されるように制御する演算である。なお、ダミー空間 23 は、量子プログラム $\{u_k\}$ の実行の可否には係わらない。

20

【0019】

所定の状態は、予め一意に定められて、メモリ等に記憶されていてもよいし、プログラム等により一意になるように処理時点で定められるようにしてもよい。制御演算付加部 13 は、書き換えた拡張量子プログラム U' を、ダミー演算追加部 14 に出力する。

【0020】

ダミー演算追加部 14 は、拡張量子プログラム U' に、ダミー空間 23 の状態に対して演算を行うダミー量子ゲート列 M_1, M_2 を追加するダミー演算追加手段である。従って、ダミー量子ゲート列 M_1, M_2 は、拡張量子プログラム U' の量子ビット空間における入力量子ビット空間 21、及びダミー空間 23 以外の量子秘密鍵量子ビット空間 22 の状態には影響を及ぼさない。ダミー量子ゲート列 M_1, M_2 は、上記の条件を満たすようにランダムに選択される。

30

【0021】

追加されるダミー量子ゲート列 M_1, M_2 は、図 2 に示すように拡張量子プログラム U' における量子プログラム $\{u_k\}$ の前後に設けられる。なお、前後の何れか一方に設けられていてもよい。また、ダミー量子ゲート列 M_1, M_2 各々は、制御演算により、拡張量子プログラム U' の量子ビット空間の任意の量子ビットの状態 A_{M_1}, A_{M_2} に依じて実行されるようにしてもよい。ダミー演算追加部 14 は、ダミー量子ゲート列 M_1, M_2 を追加した拡張量子プログラム U' を暗号化部 15 に出力する。

40

【0022】

暗号化部 15 は、拡張量子プログラム U' に、量子プログラム $\{u_k\}$ を実行する制御演算が行われる前の量子秘密鍵量子ビット空間 22 の状態に対して演算を行う第 1 の量子ゲート列である暗号化ゲート列 R を追加する暗号化手段である。暗号化ゲート列 R は、ランダムに選択される。暗号化ゲート列 R は、量子プログラム $\{u_k\}$ に依じた量子秘密鍵量子ビット空間 22 の状態を秘匿するためのものである。即ち、暗号化ゲート列 R は、量子プログラム $\{u_k\}$ を実行する際に、量子プログラム $\{u_k\}$ に依じた量子秘密鍵量子ビット空間 22 の状態を示す量子情報をそのまま入力させないためのものである。

50

【 0 0 2 3 】

また、暗号化部 15 は、拡張量子プログラム U' に、量子プログラム $\{u_k\}$ を実行する制御演算が行われた後の量子秘密鍵量子ビット空間 22 の状態に対して演算を行う第 2 の量子ゲート列である暗号化ゲート列 L を追加するものである。暗号化ゲート列 L は、ランダムに選択される。暗号化ゲート列 L は、量子プログラム $\{u_k\}$ に応じた量子秘密鍵量子ビット空間 22 の状態を秘匿するためのものである。即ち、暗号化ゲート列 L は、量子プログラム $\{u_k\}$ を実行する際に、量子プログラム $\{u_k\}$ に応じた量子秘密鍵量子ビット空間 22 の状態を示す量子情報をそのまま出力させないためのものである。暗号化ゲート列 R, L を拡張量子プログラム U' に追加することを暗号化と呼ぶ。暗号化部 15 により暗号化された拡張量子プログラム U' は以下の式のように示される。

【 数 1 】

$$(I \otimes L)U'(I \otimes R^\dagger)$$

暗号化部 15 は、暗号化した拡張量子プログラム U' を難読化部 17 に出力する。また、暗号化部 15 は、暗号化ゲート列 R を秘密鍵生成部 16 に出力する。

【 0 0 2 4 】

秘密鍵生成部 16 は、量子秘密鍵量子ビット空間 22 の、上記の制御演算における量子プログラム $\{u_k\}$ に応じた所定の状態に対して、暗号化ゲート列 R の逆演算（図 2 における右から左への演算）を行うことによって量子秘密鍵 $R|k\rangle$ を生成する秘密鍵生成手段である。量子秘密鍵 $R|k\rangle$ は、量子秘密鍵量子ビット空間 22 の状態を示す量子情報として生成される。量子秘密鍵 $R|k\rangle$ の生成は、量子プログラム $\{u_k\}$ 毎に行われ、量子プログラム $\{u_k\}$ の数だけ生成される。秘密鍵生成部 16 は、生成した量子秘密鍵を出力部 18 に出力する。

【 0 0 2 5 】

上記のように生成された暗号化された拡張量子プログラム U' の量子秘密鍵量子ビット空間 22 に量子秘密鍵 $R|k\rangle$ を入力すると、入力量子ビット空間 21 に入力される任意の量子情報 $|input\rangle$ に対して、当該量子秘密鍵 $R|k\rangle$ に対応する（当該量子秘密鍵 $R|k\rangle$ が指定する）量子プログラム u_k が実行される。これを式で表すと以下のような。

【 数 2 】

$$(I \otimes L)U'(I \otimes R^\dagger)|input\rangle \otimes R|k\rangle = u_k|input\rangle \otimes L|k\rangle$$

【 0 0 2 6 】

難読化部 17 は、暗号化部 15 により暗号化ゲート列 R, L が追加された拡張量子プログラム U' に対して、難読化を行う難読化手段である。難読化部 17 は、図 2 に示すように、難読化を行うことによって量子プログラム U を生成する。難読化は、量子プログラムを、当該量子プログラムがどのような演算を行うか（どのような量子ゲート列がどのような順番で並んでいるか）を分かりにくくするために、量子ゲート列の表現を変えるものである。従って、難読化は、量子プログラムが行う演算自体を変更するものではない。

【 0 0 2 7 】

プログラムの難読化は、具体的には、量子ゲート列の入れ替え（シャッフル）及び量子ゲート列の追加である。なお、量子ゲート列の入れ替え及び量子ゲート列の両方が必ずしも行われる必要はなく、少なくとも何れかが行われればよい。上記の難読化は、難読化部 17 によって予め記憶されたルールに基づいて行われる。量子ゲート列の入れ替えは、例えば、量子ゲート列を量子力学の交換関係を、上記のルールとして難読化部 17 に予め記憶させておき、当該交換関係に基づいて、拡張量子プログラム U' が行う演算自体が変更されないように行われる。また、量子ゲート列の追加は、拡張量子プログラム U' が行う

10

20

30

40

50

演算自体は変更されない恒等演算子の量子ゲート列を難読化部 17 に予め記憶させておき、当該量子ゲート列を追加することにより行われる。難読化部 17 は、難読化済みの量子プログラム U を出力部 18 に出力する。

【0028】

出力部 18 は、難読化部 17 による難読化が行われた拡張量子プログラム U、及び秘密鍵生成部 16 により生成された量子秘密鍵を出力する出力手段である。この出力は、例えば、量子プログラム秘匿化装置 10 に接続された別の装置に対して行われてもよいし、難読化が行われた拡張量子プログラム U 及び量子秘密鍵を自由に利用できるように、量子プログラム秘匿化装置 10 内のメモリ等に対して行われてもよい。

【0029】

量子プログラム秘匿化装置 10 は、例えば、量子プログラムが実行される装置と同様の量子計算機等の情報処理装置である。具体的には、例えば、イオントラップあるいは NMR を用いた量子計算機である。上記の装置の各ハードウェアがプログラム等によって動作することにより、上記の機能が実現される。以上が、量子プログラム秘匿化装置 10 の構成である。

【0030】

引き続き、図 3 のフローチャートを用いて、本実施形態の量子プログラム秘匿化装置 10 で実行される処理（量子プログラム秘匿化方法）を説明する。この処理は、量子プログラム $\{u_k\}$ の作成者等によって、量子プログラム $\{u_k\}$ が秘匿化される際に行われる。

【0031】

まず、量子プログラム秘匿化装置 10 では、入力部 11 によって量子プログラム $\{u_k\}$ が入力される（S01、入力ステップ）。続いて、入力された量子プログラム $\{u_k\}$ を含み、当該量子プログラム $\{u_k\}$ の入力量子ビット空間 21 に加えて、量子秘密鍵に応じた量子秘密鍵量子ビット空間 22 を有する拡張量子プログラム U' が、拡張部 12 生成される（S02、拡張ステップ）。続いて、制御演算付加部 13 によって、拡張量子プログラム U' が、量子秘密鍵量子ビット空間 22 が所定の状態 $A_1 \sim A_k$ である場合に、当該拡張量子プログラム U' に含まれる量子プログラム $u_1 \sim u_k$ を実行する制御演算が行われるように書き換えられる（S03、制御演算付加ステップ）。

【0032】

続いて、ダミー演算追加部 14 によって、拡張量子プログラム U' に、量子秘密鍵量子ビット空間 22 に含まれるダミー空間 23 の状態に対して演算を行うダミー量子ゲート列 M_1, M_2 が追加される（S04、ダミー演算追加ステップ）。続いて、暗号化部 15 によって、拡張量子プログラム U' に、暗号化ゲート列 R, L が追加される（S05、暗号化ステップ）。なお、S03 ~ S05 の処理に関して、図 2 に示すような各処理完了後の拡張量子プログラム U' となっていればよいのでそれらの順番は必ずしも上記の順番でなくてもよい。

【0033】

続いて、秘密鍵生成部 16 によって、量子秘密鍵量子ビット空間 22 の上記の所定の状態 $A_1 \sim A_k$ に対して、暗号化ゲート列 R の逆演算を行うことによって量子秘密鍵 $R|k\rangle$ が生成される（S06、秘密鍵生成ステップ）。続いて、難読化部 17 によって、図 2 に示すように、拡張量子プログラム U' に対して難読化が行われ、難読化済みの拡張量子プログラム U が生成される（S07、難読化ステップ）。なお、S06 及び S07 の処理はそれぞれ独立に行われるので、順序が逆になっていてもよい。続いて、出力部 18 によって、難読化済みの拡張量子プログラム U 及び量子秘密鍵 $R|k\rangle$ が出力される（S08、出力ステップ）。以上が、量子プログラム秘匿化装置 10 で実行される処理である。

【0034】

量子プログラム秘匿化装置 10 によって、生成された難読化済みの拡張量子プログラム U 及び量子秘密鍵 $R|k\rangle$ は、例えば、以下のように利用される。難読化済みの拡張量子プログラム U は、認証局等でプログラムの作成者が認証された上で、古典公開鍵として公

10

20

30

40

50

開される。当該拡張量子プログラムUは、任意の者によって取得することができる。当該拡張量子プログラムUに含まれる量子プログラム $\{u_k\}$ を実行する者は、プログラムの作成者からの供給を受けること等により、実行したい量子プログラム u_k に応じた量子秘密鍵 $R|k\rangle$ を取得する。実行者は、以下の式のように、拡張量子プログラムUの量子秘密鍵量子ビット空間22に量子秘密鍵 $R|k\rangle$ を入力し、入力量子ビット空間21に任意の量子情報 $|input\rangle$ を入力して、難読化済みの拡張量子プログラムUを実行する。

【数3】

$$U(|input\rangle \otimes R|k\rangle)$$

10

これにより、以下の式のように任意の量子情報 $|input\rangle$ に対して、量子プログラム u_k が実行される。

【数4】

$$u_k|input\rangle \otimes R|k\rangle$$

【0035】

上記のように本実施形態に係る量子プログラム秘匿化装置10により生成される難読化済み拡張量子プログラムUは、上記の制御演算と暗号化ゲート列Rとによって、量子秘密鍵量子ビット空間22に量子秘密鍵 $R|k\rangle$ が入力されなければ、量子プログラム $\{u_k\}$ が実行されない。即ち、量子秘密鍵 $R|k\rangle$ を有した者でなければ、量子プログラム $\{u_k\}$ は実行されない。

20

【0036】

また、難読化済み拡張量子プログラムUの実行者は、上記の難読化の効果により、量子計算機を用いても難読化済み拡張量子プログラムU（古典公開鍵）の情報から多項式時間で量子プログラム $\{u_k\}$ （ユニタリ演算）を特定することができない。また、量子秘密鍵 $R|k\rangle$ の量子状態の特定も、多項式時間の量子計算によっては不可能となる。上記の処理（秘匿量子計算）を用いると、量子秘密鍵を用いずに多項式時間で量子計算を実行することが可能であるのは、難読化済み拡張量子プログラムUの作成者だけとなる。従って、本実施形態によれば、量子プログラム $\{u_k\}$ をその演算内容を知られずに権限を有する者に対して実行させることを可能とする。

30

【0037】

また、暗号化量子ゲート列Lの存在により、難読化済みの拡張量子プログラムUによって演算が行われて出力される量子秘密鍵が、上記の制御演算に応じた所定の状態 $A_1 \sim A_k$ となることなく、安全性の高い秘匿化を行うことができる。

【0038】

即ち、本実施形態は、量子計算機でも計算量的に安全性が保障されるQMA（Quantum Merlin-Arthur）困難問題に基づく、量子暗号要素技術（暗号プリミティブ）としての秘匿量子計算を可能にするものである。なお、秘匿量子計算の概念は、本願発明者によって見出されたものであり、以下に示すものである。秘匿量子計算は、AとBとの二者間量子プロトコルである。Aが量子プロトコル（量子計算におけるユニタリ変換）を決定し（即ち、本実施形態における量子プログラム $\{u_k\}$ の作成者）、Bが入力量子情報を準備する（即ち、量子プログラム $\{u_k\}$ の実行者）。

40

【0039】

Aが量子プログラムを暗号化及び難読化して古典公開鍵とし、復号を行う量子秘密鍵と共にBに送信する。量子秘密鍵は未知量子状態のため同定が不可能であり、量子プログラムはQMA困難である難読化によって計算的に解読が不可能であるため、AはBに量子プログラムの内容を知らせることなく、Bが準備する任意の入力量子情報に対して量子プログラムを実行させることができある。以上が、秘匿量子計算である。

【0040】

また、本実施形態のようにダミー量子ゲート列 M_1, M_2 を拡張量子プログラムU'に

50

追加することとすれば、量子秘密鍵量子ビット空間 22 のうちの、どのビットが量子秘密鍵に係るものかを分かりにくくするため、さらに安全性の高い秘匿化を行うことができる。

【0041】

また、本実施形態のように複数の量子プログラム { u_k } を入力して、難読化済み拡張量子プログラム U にそれらを含ませることとすれば、一つの難読化済み拡張量子プログラム U により、複数の量子プログラム { u_k } を実行できるので、ユーザの利便性を向上させることができる。但し、必ずしも複数の量子プログラムを難読化済み拡張量子プログラム U に含ませる必要はなく、秘匿量子計算に用いられる量子プログラムが1つである場合等は1つの量子プログラムのみを難読化済み拡張量子プログラム U に含ませてもよい。

10

【図面の簡単な説明】

【0042】

【図1】本発明の実施形態に係る量子プログラム秘匿化装置の構成を示す図である。

【図2】量子プログラム秘匿化装置により秘匿化される量子プログラム及び生成される拡張量子プログラムを概念的に示す図である。

【図3】本発明の実施形態に係る量子プログラム秘匿化装置によって実行される処理（量子プログラム秘匿化方法）を示すフローチャートである。

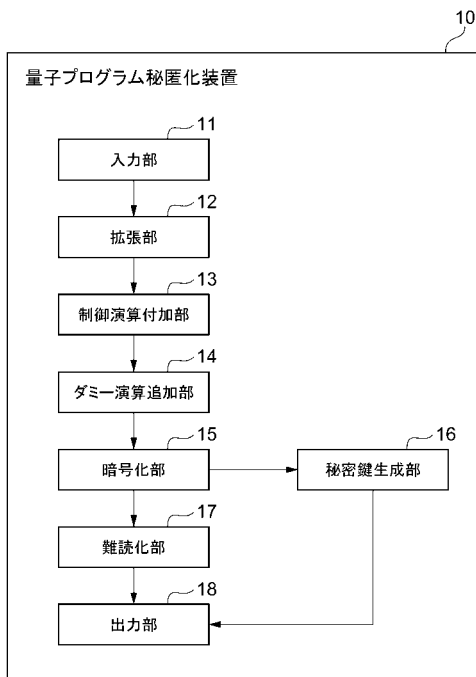
【符号の説明】

【0043】

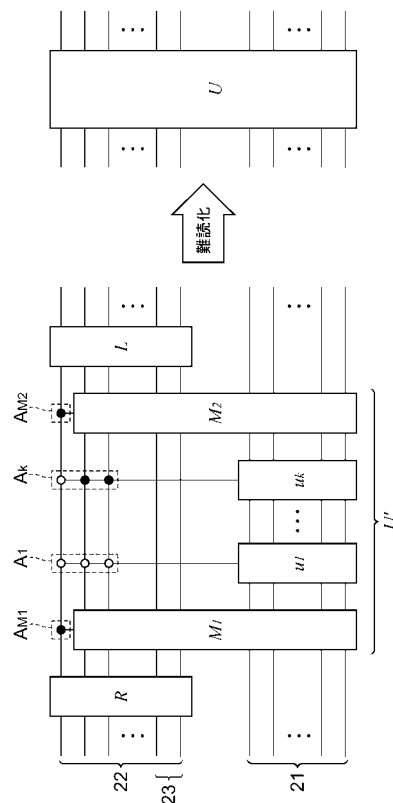
10 ... 量子プログラム秘匿化装置、 11 ... 入力部、 12 ... 拡張部、 13 ... 制御演算付加部、 14 ... ダミー演算追加部、 15 ... 暗号化部、 16 ... 秘密鍵生成部、 17 ... 難読化部、 18 ... 出力部。

20

【図1】



【図2】



【 図 3 】

