(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5105408号
(P5105408)

(45)発行日　平成24年12月26日(2012.12.26)　(24)登録日　平成24年10月12日(2012.10.12)

(51)Int.Cl.			F I		
G09C	1/00	(2006.01)	G09C	1/00	660D
H04L	9/12	(2006.01)	H04L	9/00	631
G06F	21/22	(2006.01)	G06F	21/22	114B
			G06F	21/22	114C

請求項の数 4　(全 12 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)
(65)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)
審査請求日　平成22年5月19日 (2010.5.19)

特許法第３０条第１項適用　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

(73)特許権者　503360115
独立行政法人科学技術振興機構
埼玉県川口市本町四丁目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

審査官　石田　信行

最終頁に続く

(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)【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、
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、

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】
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、
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】
【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。

【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。

【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。

【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ら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か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。

【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。

【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。

【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。

【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～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～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。

【００１４】

量子プログラムu_1～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～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】

引き続いて、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。

【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、量子秘密鍵に応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。

【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。

【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。

【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_{M1}，A_{M2}に応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。

【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入力させないためのものである。

【００２３】

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】

$$(I \otimes L)U'\left(I \otimes R^{\dagger}\right)$$

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。

【００２４】

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＞を生成する秘密鍵生成手段である。量子秘密鍵Ｒ｜ｋ＞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＞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。

【００２５】

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＞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＞に対して、当該量子秘密鍵Ｒ｜ｋ＞に対応する（当該量子秘密鍵Ｒ｜ｋ＞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になる。なお、以下の式において、u_k｜input＞は、実行させたい量子計算を示す。

【数２】

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

【００２６】

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。

【００２７】

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】

引き続いて、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～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～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～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＞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＞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＞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＞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＞を入力し、入力量子ビット空間２１に任意の量子情報｜input＞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】

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

これにより、以下の式のように任意の量子情報｜input＞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＞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＞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。

【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＞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。

【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～A_k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。

【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（QuantumMerlin-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）。

【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量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。

【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。

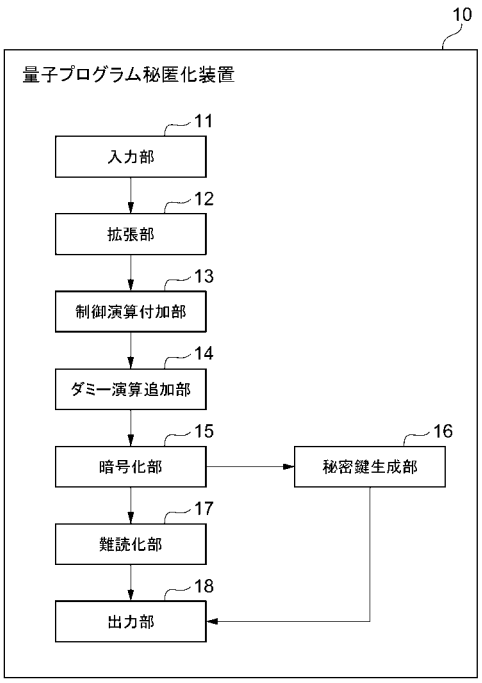
【符号の説明】

【００４３】

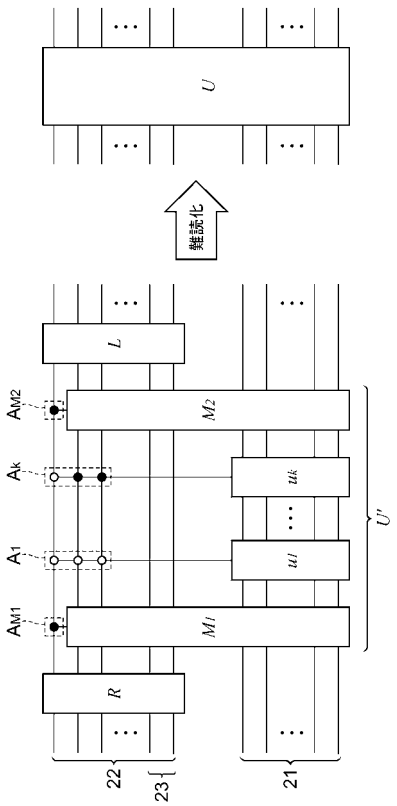
１０…量子プログラム秘匿化装置、１１…入力部、１２…拡張部、１３…制御演算付加

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。

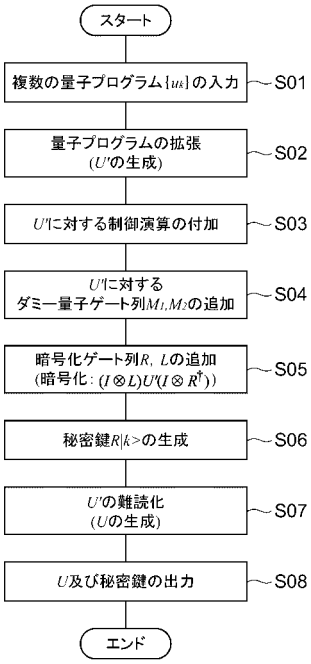
【図１】



【図２】



【図３】


スタート
複数の量子プログラム{u_k}の入力
S01
量子プログラムの拡張
(U'の生成)
S02
U'に対する制御演算の付加
S03
U'に対する
ダミー量子ゲート列M_1,M_2の追加
S04
暗号化ゲート列R, Lの追加
(暗号化：$(I\otimes L)U'(I\otimes R^{\dagger})$)
S05
秘密鍵$R|k>$の生成
S06
U'の難読化
(Uの生成)
S07
U及び秘密鍵の出力
S08
エンド

フロントページの続き

(56)参考文献 特表２００６－５２２９６２（ＪＰ，Ａ）
特開２００６－３３１２４９（ＪＰ，Ａ）
特開２００６－３９４８（ＪＰ，Ａ）
特表２００５－５１３６８０（ＪＰ，Ａ）
特開２００２－４２１０４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　　１／００
Ｇ０６Ｆ　２１／２２
Ｇ０６Ｎ　９９／００
Ｈ０４Ｌ　　９／１２