様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月 ２２ 日現在

機関番号：３４４１６
研究種目：挑戦的研究（萌芽）
研究期間：2020～2021
課題番号：２０Ｋ２１７９８

研究課題名（和文）量子状態の複製不可能性を利用した秘密情報管理法

研究課題名（英文）Management schemes for secret information using no-cloning property of quantum state

研究代表者

桑門　秀典（Kuwakado, Hidenori）

関西大学・総合情報学部・教授

研究者番号：３０２８３９１４

交付決定額（研究期間全体）：（直接経費）　　4,900,000円

研究成果の概要（和文）：秘密のディジタル情報をユーザが使用するデバイス(装置)に保存しているアプリケーションには、ユーザの内部解析により秘密のディジタル情報が漏洩するリスクがある。本研究では、情報を量子状態で保存することで、情報の漏洩を原理的に防止できる方式を考案した。この方式では、攻撃者に与えられた量子状態に対して一般化Groverアルゴリズムによる振幅増幅を行っても、有益な情報が得られる確率が無視できることを示した。また、ランダムオラクルと非暗号学的置換から成る倍ブロック長圧縮関数の衝突を量子コンピュータを用いて発見しようとするとき、そのクエリ計算量が最大となる非暗号学的置換の十分条件を明らかにした。

研究成果の学術的意義や社会的意義
本研究の社会的意義は、メモリアクセス制限等の既存技術では解決できないデバイスの内部解析による情報漏洩の問題を量子複製不可能定理によって原理的に解決する点にある。そのためには、情報をディジタルビット（古典ビット）ではなく、量子ビットを用いた量子状態に符号化する必要がある。最近、その優れた並列計算能力が注目されている量子コンピュータの実現に向けて研究開発が盛んに行われているが、量子コンピュータが実現できれば、本研究の方式も実現することができる。

研究成果の概要（英文）：Applications that store secret digital information in devices (equipment) used by users have a risk of leakage of the secret due to internal analysis by users. In this research, we proposed a scheme that can prevent information leakage in principle by storing information in a quantum state. We showed that the probability of obtaining useful information is negligible even when amplitude amplification by the generalized Grover algorithm is performed on the quantum state given to the attacker. We also clarified the sufficient conditions for a non-cryptographic permutation that maximizes the query computational complexity when a quantum computer is used to find collisions of a double block-length compression function consisting of the permutation and a random oracle.

研究分野：暗号理論

キーワード：量子複製不可能性定理　対称暗号　Groverアルゴリズム　倍ブロック長圧縮関数

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

著作権保護のために暗号化された Blu-ray Disc のコンテンツは、再生機に内蔵されている「デバイスキー」と呼ばれるユーザには秘密のディジタル情報を用いて、視聴時に復号される。このように、秘密のディジタル情報をユーザが使用するデバイス（装置）に保存しているアプリケーションは少なくない。

そのようなアプリケーションには、デバイスの内部が解析され、その秘密のディジタル情報が漏洩し、不正なデバイスが製造されるリスクがある。このリスクを低減するために、メモリアクセス制限等の機能を有するハードウエアが利用されている。しかし、ディジタル情報の秘匿性を保証することは容易ではない。例えば、Blu-ray 機器の著作権保護機能 AACS やディジタル放送の機器認証用 B-CAS カードは解析され、不正な AACS や B-CAS カードが製造されている。

２．研究の目的

不正デバイスを製造するときには、その秘密のディジタル情報が複製される点に着目する。なぜなら、ディジタル情報を複製できなければ、不正デバイスを製造できないからである。従来は、ディジタル情報が保存されているメモリへのアクセスを制限する等により複製を防止しようとしていた。しかし、不正デバイス製造の採算が見合う場合、メモリアクセス制限等によって、情報漏洩を防止することは難しい。本研究の目的は、メモリアクセス制限等の既存技術では解決できないデバイスの内部解析による情報漏洩の問題を解決することである。

本研究では、情報をディジタルではなく、量子状態に符号化して保存することを検討する。量子状態に符号化する利点は、量子複製不可能定理にある。この定理は、量子状態が未知ならば、いかなる手段を用いても、その量子状態の完全な複製を作成できないことを保証している。この定理によれば、量子状態を知らない不正デバイス製造者は、多大なコストを費やしても、秘密情報を複製することができない。つまり、情報を量子状態に符号化してデバイスに保存すれば、デバイスの内部解析による不正デバイス製造のリスクを原理的に排除できる。本研究では、量子計算機の優れた並列計算能力だけでなく、量子計算機の量子メモリが有する量子複製不可能定理も利用する点が特徴である。

しかし、情報の複製を防止するだけでは、機能として不十分である。なぜなら、その情報をユーザに秘密にしたままで、所望の処理（コンテンツの復号等）が実行できる必要がある。量子状態の場合、情報を読み込むために量子状態を測定すると、量子状態自身が変化するので、ディジタル情報用の既存の暗号技術を量子状態に符号化された情報に適用することは難しい。

３．研究の方法

本研究では、情報をユーザに秘密にしたままで所望の処理が可能な量子状態に符号化する方法を探索することから始め、量子複製不可能定理に基づく暗号方式を創出する。暗号化・復号に必要な鍵の情報を量子状態に符号化し、それをユーザに秘匿したまま、暗号化・復号処理が可能な暗号方式を検討する。この暗号方式の特徴は、量子的重ね合わせを利用して、指数関数的なビット数が必要な暗号化・復号の表を多項式程度の量子ビット数で符号化することである。平文・暗号文の表と鍵が一対一に対応するならば、その対応表を表す量子状態は鍵を表す量子状態とみなすことができる。鍵が未知ならば、その量子状態も未知なので、量子複製不可能定理を適用できる条件を満たしている。

本方式は、ユーザ間の通信はディジタル情報で行う点がユーザ間で量子状態を通信する量子鍵配送とは異なり、従来の暗号方式とは全く異なるパラダイムの暗号方式となる 。量子状態に符号化された情報に適した暗号化を行い、デバイスの内部解析による情報漏洩を原理的に防止することである。従来のディジタル情報を対象とする暗号技術の安全性が計算量的困難性に基づいているのに対し、本研究の安全性は量子複製不可能定理に基づいている。また、量子状態の通信を必要とする量子鍵配送とは異なり、本研究では、ディジタル情報の通信を想定しており、既存のディジタル通信網を活用できる利点がある。

４．研究成果

(1) 量子複製不可能定理に基づく暗号方式

Bob が Alice に平文を暗号化して送信したい場合を考える。Bob による通信に先立って、Alice は事前に以下の準備を行う。Fを$\{0,1\}^{\lambda} \times \{0,1\}^{L} \to \{0,1\}^{\ell}$の擬似ランダム関数とする。Alice は、$\lambda$ビットの値$\hat{v}$を選び、$\mathsf{f} = \mathsf{F}(\hat{v}, \cdot)$とし、$f$を計算するユニタリ演算子を$U_f$とする。Alice は、$U_f$を用いて、下記の量子状態$|\psi\rangle$を生成し、量子メモリに保存する。そして、Alice はその量子メモリを内蔵するデバイスを Bob に安全な物理的手段（例えば、郵送）を用いて渡しておく。この量子状態は、$\hat{v}$を鍵と考えると、暗号文$f(r)$と平文rの全ての組の重ね合わせ状態になっている。

$$|\psi\rangle = U_f \frac{1}{\sqrt{2^L}} \sum_{r\in\{0,1\}^L} |0^\ell\rangle\,|r\rangle$$
$$= \frac{1}{\sqrt{2^L}} \sum_{r\in\{0,1\}^L} |f(r)\rangle\,|r\rangle$$

次に、Bob は、受け取ったデバイスの量子メモリ上の量子状態$|\psi\rangle$を測定する。測定結果を$(\hat{c},\hat{r})$とおく。そして、平文をmとしたとき、Bob は$(\hat{c}\oplus m,\hat{r})$を Alice に暗号文として Alice に送信する。ここで、この暗号文は量子ビットではなく、古典ビット（通常のビット）なので、現在のディジタル通信網で送信することができる。なお、Bob は量子状態$|\psi\rangle$を測定して重ね合わせ状態を破壊しているので、このデバイスは再利用できない、つまり使い捨てにする必要がある。

また、量子状態$|\psi\rangle$は、Bob にとって未知の量子状態である。なぜなら、$f(r)$の値を知るためには$\hat{v}$の値を必要とするが、$\hat{v}$は Alice のみが知る値である。したがって、量子複製不可能定理により、Bob は量子状態$|\psi\rangle$を複製することができない。

Alice は受信した暗号文から第 2 成分$\hat{r}$を取り出し、下記の式によって平文mを得る。

$$m = (\hat{c}\oplus m)\oplus F(\hat{v},\hat{r})$$

ここで、$\hat{v}$の値は Alice のみが知る値なので、この計算ができるのは Alice のみである。

この例では、Alice の通信相手として Bob のみを考えたが、Alice は Bob に渡したデバイスと同じデバイス、つまり同じ$|\psi\rangle$を内蔵するデバイスを Bob 以外のユーザに渡しても Bob の平文mの機密性が損なわれないことを示した。

(2) 倍ブロック長圧縮関数の衝突困難性の量子的解析

上述の提案方式で用いる擬似ランダム関数Fを倍ブロック長圧縮関数から構成することを考えよう。$\{0,1\}^m \to \{0,1\}^n$のランダムオラクルhと不動点がない非暗号学的置換πから下記のように定義される倍ブロック長圧縮関数h^πを考える。

$$h^\pi(x) = (h(x), h(\pi(x)))$$

現在のコンピュータを用いた場合、倍ブロック長圧縮関数h^πの衝突（出力が同じになる異なる入力）を発見するクエリ計算量（衝突困難性）は$\Omega(2^n)$であることが知られている。衝突困難性は、Fが擬似ランダム関数であるための必要条件であるから、衝突困難性を明らかにすることは重要である。今回、量子コンピュータを用いた場合の倍ブロック長圧縮関数h^πの衝突困難性を明らかにした。

まず、置換πが involution の場合、Grover アルゴリズムを用いることにより衝突困難性は$O\left(2^{n/2}\right)$であることがわかった。次に、衝突困難性が$\Omega\left(2^{2n/3}\right)$になるための置換$\pi$の十分条件を明らかにし、その十分条件を満たす$\pi$の例をいくつか示すことができた。

5．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　1件）

1．著者名 Hidenori Kuwakado and Shoichi Hirose and Masahiro Mambo	4．巻 589
2．論文標題 White-Box Encryption Scheme Using a Quantum Memory	5．発行年 2021年
3．雑誌名 Cryptology ePrint Archive	6．最初と最後の頁 1-16
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Shoichi Hirose and Hidenori Kuwakado	4．巻 13129
2．論文標題 A Note on Quantum Collision Resistance of Double-Block-Length Compression Functions	5．発行年 2021年
3．雑誌名 The 18th IMA International Conference on Cryptography and Coding, (IMACC 2021), Lecture Notes in Computer Science	6．最初と最後の頁 161-175
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-92641-0_8	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計0件

〔図書〕　計0件

〔産業財産権〕

〔その他〕

－

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	廣瀬　勝一 (Hirose Shoichi) (20228836)	福井大学・学術研究院工学系部門・教授 (13401)	
研究分担者	満保　雅浩 (Mambo Masahiro) (60251972)	金沢大学・電子情報通信学系・教授 (13301)	

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関