

# 量子アルゴリズム・量子暗号の研究

## A Study of Quantum Algorithms and Quantum Cryptography

小柴 健史\*

Takeshi Koshihara

埼玉大学 理工学研究科

Graduate School of Science and Engineering, Saitama University

**Abstract**— This report describes properties of basic cryptographic primitives (quantum public-key cryptosystems and quantum one-way functions) in the quantum world where quantum computers are available. Some quantum public-key cryptosystems have already proposed. However, the security requirements for quantum public-key cryptosystems are not studied well. We propose several security notions for quantum public-key cryptosystems and discuss relation among them. In the classical setting, the notion of one-way permutations plays an essential role in cryptology. Even in the quantum setting, quantum one-way permutations are expected to play again an essential role in quantum cryptography. However, we do not have any candidates so far. So, we give a characterization of quantum one-way permutations.

**KeyWords:** Quantum Algorithms, Quantum Cryptography

### 1 はじめに

1994年 Shor により量子計算機を用いた素因数分解アルゴリズムが提案されたことにより量子計算の研究が盛んになったが、一方で素因数分解問題の効率的解法は広く一般に用いられている RSA 公開鍵暗号の解読に繋がるため暗号研究者に大きなインパクトを与えた。この事実は暗号学に対する量子メカニズムの負の側面として語られることもある。これとは対比的に Bennett と Brassard による量子鍵共有プロトコルの成功が一層の脚光を浴びることとなった。敵対者が量子計算を前提にできるからには、正当な暗号の利用者(暗号化および復号アルゴリズムの利用者)が敵対者からの攻撃を防御する手段として量子計算機の利用できる可能性もある。もちろん、敵対者を圧倒的に有利な状況(例えば、適応的選択暗号文攻撃モデルなど)においても安全性が確保できるならばそれに越したことはない。格子に関する問題の困難性を安全性の根拠とする Ajtai-Dwork 公開鍵暗号のようないわゆる格子暗号はその安全性が最短ベクトル問題の計算困難さに依拠しており、たとえ敵対者が量子計算機が利用できたとしても安

全性には影響が少ないということで着目されている。ただし、現在暗号で利用されている最短ベクトル問題は量子計算機を用いても効率的に解けないだろうと強く予想されているわけではなく、一般に格子問題に対する量子アルゴリズム研究も盛んに行われている。

格子暗号が依拠する問題に対して効率的な量子アルゴリズムが知られていないというのは重要な観点であるが、一方で量子計算の能力を積極的に活用した公開鍵暗号方式も存在する。この意味での最初の公開鍵暗号は Okamoto, Tanaka, Uchiyama によるものである。Okamoto-Tanaka-Uchiyama 公開鍵暗号はナップサック公開鍵暗号の延長線上に位置する。OTU 公開鍵暗号では、(鍵生成を行う)受信者に量子計算の能力が必要であるが、送信者や秘密通信に係る情報はすべて古典的である。これに対して、Kawachi, Koshihara, Nishimura, Yamakami による公開鍵暗号は敵対者のみならず受信者も送信者も量子計算機が利用できることが前提で、送信される情報も量子情報であるという設定である。KKNY 暗号は Goldwasser-Micali による確率暗号の量子的な一般化であり、その安全性はグラフ自己同型性判定問題の最悪時間計算量に依存している。Goldwasser-Micali 暗号と同様に、

\* 〒 338-8570 さいたま市桜区下大久保 255. TEL/FAX: 048-858-3494. Email: koshihara@mail.saitama-u.ac.jp

証明可能安全性を持つことが特徴である。

古典暗号の枠組みにおいては様々は用途に応じて安全性概念が様々に定義されていて、その相互関係においても精力的に研究が進められている。量子の枠組みではそれがまだ不十分であり、量子公開鍵暗号の安全性を考慮する上でどのような安全性概念が妥当であるのかを議論する。また、計算の要素が入った暗号系に対する安全性の根本概念は一方向性関数として特徴付けられるが、利便性を考えるとより狭い概念である一方向性置換が用いられることが多い。しかしながら、Shor のアルゴリズムにより、古典的な意味での一方向性置換はもはや量子の意味では一方向性を持たず、量子一方向性置換の候補がないのが現状である。そこで、量子一方向性置換の存在を検討するにあたりその存在性の計算量的な特徴付けを行う。

## 2 量子公開鍵暗号の安全性概念

まず、量子公開鍵暗号の定義は、古典での公開鍵暗号  $(G, M, E, D)$  に対して鍵生成アルゴリズム  $G$  と暗号化アルゴリズム  $E$  を量子多項式時間アルゴリズムに拡張したものとして考える。つまり、暗号化の対象は古典情報であり、ここでは量子情報の暗号化については考慮しない。

量子公開鍵暗号の安全性概念を定める構成要素について、委細に検討してあるがここでは紙面の都合で割愛する。

**定義 2.1** 量子公開鍵暗号  $(G, M, E, D)$  が 識別不可能性を持つとは任意の量子アドバイス付き多項式サイズ量子回路族  $\{C_n, |a_n\rangle\}_{n \geq 1}$ 、任意の  $x, y \in M_n$  で

$$\left| \Pr_{G,E}[C_n(e^{\otimes \text{poly}(n)}, E_e(x), |a_n\rangle) = 1] \right. \\ \left. (e, d) \leftarrow G(1^n) \right. \\ \left. - \Pr_{G,E}[C_n(e^{\otimes \text{poly}(n)}, E_e(y), |a_n\rangle) = 1] \right. \\ \left. (e, d) \leftarrow G(1^n) \right|$$

が  $n$  に対して無視できるときをいう。ただし、上の確率はアルゴリズム  $G$  と  $E$  内のコイントスによる。

識別不可能性については、古典からの単純な類推で妥当な定義を与えることができたが、強秘匿性については考察が必要である。強秘匿性という言葉は “semantic” security の意識であり、秘匿性の意味論をどのように定めるのかに依存して定義

が変化しうるからである。我々の設定では、秘密にしたい情報は古典情報なので「古典的な情報を秘匿する」という意味を付与するのか、量子計算のもとでは古典情報も量子的な情報に変換しうるので「量子的な情報を秘匿する」という意味を付与するのか少なくとも 2 通りの解釈が可能かと思う。ここでは、この 2 通りの解釈にもとづいた定義をそれぞれ与えることにする。

**定義 2.2** 量子公開鍵暗号  $(G, M, E, D)$  が古典情報強秘匿性を持つとはある確率的量子多項式時間一様変換  $T$  が存在し、任意の量子アドバイス付き多項式サイズ量子回路族  $\{C_n, |a_n\rangle\}_{n \geq 1}$ 、平文空間族  $M$  上の任意の確率分布族  $\{X_n\}_{n \geq 1}$ 、任意の多項式限定関数  $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ 、任意の多項式限定量子状態関数  $h : \{0, 1\}^* \rightarrow H^*$ 、において

$$\Pr_{G,E,X_n} \left[ C_n(e^{\otimes \text{poly}(n)}, E_e(\alpha), h(\alpha), |a_n\rangle) = f(\alpha) \mid \right. \\ \left. (e, d) \leftarrow G(1^n); \alpha \leftarrow X_n \right] \\ - \Pr_{T,G,X_n} \left[ C'_n(e^{\otimes \text{poly}(n)}, h(\alpha), |a'_n\rangle) = f(\alpha) \mid \right. \\ \left. (e, d) \leftarrow G(1^n); \alpha \leftarrow X_n \right]$$

が  $n$  に対して無視できるときをいう。ただし  $(C'_n, |a'_n\rangle) = T(C_n, |a_n\rangle)$  は  $T$  に  $C_n$  の記述と  $|a_n\rangle$  を与えて得られる回路と量子アドバイスの対である。また、確率はアルゴリズム  $G$  と  $E$  内のコイントスに加えて分布  $X_n$  と  $T$  内のコイントスによって決まるものである。

**定義 2.3** 量子公開鍵暗号  $(G, M, E, D)$  が量子情報強秘匿性を持つとはある確率的量子多項式時間一様変換  $T$  が存在し、任意の量子アドバイス付き多項式サイズ量子回路族  $\{C_n, |a_n\rangle\}_{n \geq 1}$ 、平文空間族  $M$  上の任意の確率分布族  $\{X_n\}_{n \geq 1}$ 、任意の多項式限定量子状態関数  $f, h : \{0, 1\}^* \rightarrow H^*$  において

$$\sum_{\substack{(e,d) \in \text{supp}(G(1^n)) \\ \alpha \in M_n}} \langle C_n(e^{\otimes \text{poly}(n)}, E_e(\alpha), h(\alpha), |a_n\rangle) \mid f(\alpha) \rangle \\ \cdot \Pr[G(1^n) = (e, d) \wedge X_n = \alpha] \\ - \sum_{\substack{(e,d) \in \text{supp}(G(1^n)) \\ \alpha \in M_n \\ (C'_n, |a'_n\rangle) \in \text{supp}(T(C_n, |a_n\rangle))}} \langle C'_n(e^{\otimes \text{poly}(n)}, h(\alpha), |a'_n\rangle) \mid f(\alpha) \rangle \\ \cdot \Pr[G(1^n) = (e, d) \wedge X_n = \alpha \wedge \\ T(C_n, |a_n\rangle) = (C'_n, |a'_n\rangle)]$$

が  $n$  に対して無視できるときをいう。ただし  $(C'_n, |a'_n\rangle) = T(C_n, |a_n\rangle)$  は  $T$  に  $C_n$  の記述と  $|a_n\rangle$

を与えて得られる回路と量子アドバイスの対である。

ここで定義した3概念について以下のような結果が導かれる。

**定理 2.1** 量子公開鍵暗号  $(G, M, E, D)$  は選択平文攻撃のもとでは識別不可能性を持つこと、古典情報強秘匿性を持つこと、そして、量子情報秘匿性を持つこととは互いに等価である。

**定義 2.4** 量子公開鍵暗号  $(G, M, E, D)$  が頑健性を持つとはある確率的量子多項式時間一様変換  $T$  が存在し、任意の量子アドバイス付き多項式サイズ量子回路族  $\{C_n, |a_n\rangle\}_{n \geq 1}$ 、平文空間族  $M$  上の任意の確率分布族  $\{X_n\}_{n \geq 1}$ 、任意の多項式限定量子状態関数  $h: \{0, 1\}^* \rightarrow H^*$ 、任意の量子アドバイス付き多項式サイズ量子回路族で計算可能な関係  $R$  において

$$\Pr_{G, E, X_n} \left[ C_n(e^{\otimes \text{poly}(n)}, E_e(\alpha), h(\alpha), |a_n\rangle) = E_e(\alpha') \mid \Lambda(\alpha, \alpha') \in R \mid (e, d) \leftarrow G(1^n), \alpha \leftarrow X_n \right] \\ - \Pr_{T, G, X_n} \left[ C'_n(e^{\otimes \text{poly}(n)}, h(\alpha), |a'_n\rangle) = E_e(\alpha') \mid \Lambda(\alpha, \alpha') \in R \mid (e, d) \leftarrow G(1^n), \alpha \leftarrow X_n \right]$$

が  $n$  に対して無視できるときをいう。ただし  $(C'_n, |a'_n\rangle) = T(C_n, |a_n\rangle)$  は  $T$  に  $C_n$  の記述と  $|a_n\rangle$  を与えて得られる回路と量子アドバイスである。また、確率はアルゴリズム  $G$  と  $E$  内のコイントスに加えて分布  $X_n$  によって決まるものである。

**定理 2.2** 量子公開鍵暗号  $(G, M, E, D)$  は適応的選択暗号文攻撃のもとでは識別不可能性を持つこと、頑健性を持つこととは等価である。

### 3 量子一方向性置換の特徴付け

#### 3.1 関数の計算量クラスとその定義

まず関数の計算量クラスの定義を行う。チューリング機械  $T$  が入力  $x$  に対して受理した時の最終的なテープ内容が  $y$  の時、 $T$  が入力  $x$  に対して  $y$  を計算すると言う。一般的にはチューリング機械は多価関数を計算するが、この論文では一価関数の時に限って議論を進める。

**定義 3.1** (1) NPSV とは NPTM によって計算される一価関数の集合。

(2) UPSV とは UPTM によって計算される一価関数の集合。

(3) PSV とは DPTM によって計算される一価関数の集合。

関数  $f$  に対して、

$$\text{graph}(f) = \{(x, y) \mid x \in \text{dom}(f), y = f(x)\}$$

と定め、任意の関数のクラス  $\mathcal{F}$  に対して、集合

$$R_f = \{(x, y) \mid x \in \text{dom}(f), y \leq f(x)\}$$

を関数  $f$  の射影と呼ぶ。Miller は全ての  $x$  に対して  $|f(x)| \leq q(|x|)$  となる全域関数  $f$  に関して、 $R_f \in \mathbf{P}$  と  $f \in \text{PSV}$  は同値であることを示した。  $\text{dom}(f) \subseteq \text{dom}(g)$  かつ  $f$  と  $g$  の挙動が  $\text{dom}(f)$  で一致するとき、部分関数  $g$  は部分関数  $f$  の拡張であるという。全ての  $y \in \text{range}(f)$  に対して  $f(x) = y$ 、 $|x| \leq q(|y|)$  となる  $x$  が存在するような多項式  $q$  が存在する時、関数  $f$  は honest という。

以下に古典、量子、双方における一方向性関数と一方向性置換の正確な定義を示す。

**定義 3.2** 関数  $f$  が honest、 $f \in \text{PSV}$ 、 $f^{-1} \notin \text{PSV}$  のとき  $f$  を一方向性関数と呼ぶ。関数  $f$  が全単射かつ全域な一方向性関数のとき  $f$  を特に一方向性置換と呼ぶ。

**定義 3.3** 関数  $f$  が honest、 $f \in \text{PSV}$ 、 $f^{-1} \notin \text{QPSV}$  のとき  $f$  を c-q 量子一方向性関数と呼ぶ。関数  $f$  が honest、 $f \in \text{QPSV}$ 、 $f^{-1} \notin \text{QPSV}$  のとき  $f$  を q-q 量子一方向性関数と呼ぶ。関数  $f$  が全単射かつ全域な c-q 量子一方向性関数、q-q 量子一方向性関数のときそれぞれ c-q 量子一方向性置換、q-q 量子一方向性置換と呼ぶ。

#### 3.2 c-q 量子一方向性置換

この節では [1, 2] の結果を元にして [5] の結果を拡張させる。量子のセッティングにおいても変わらず以下のことが言える。

**補題 3.1** (1)  $f \in \text{QPSV}$  かつ  $A$  が  $(Q_f, R_f)$  の解言語のとき、 $h \leq_T^P A$  を満たす  $f$  の拡張全域関数  $h$  が存在する。

(2)  $f \in \text{QPSV}$  かつ  $h$  が  $f$  の拡張全域関数のとき、 $A \leq_T^P h$  を満たす  $(Q_f, R_f)$  の解言語  $A$  が存在する。

また、以下のような関数  $\text{comp}_M$  を定義する。

**定義 3.4**  $S \in \text{UP}$ 、そして  $M$  を  $S$  を多項式時間で受理する UTM だとしたとき全ての  $x \in S$  において  $\text{comp}_M(x)$  を  $M$  に  $x$  を入力として与えたときの  $M$  の唯一の受理経路だとする。

この補題と関数  $\text{comp}$  を用いることで以下の定理を示すことができる。

定理 3.1 以下は全て同値である。

- (a)  $\text{EQP} \supseteq \text{UP} \cap \text{coUP}$
- (b)  $\text{range}(f) \in \mathbf{P}$  な  $c$ - $q$  量子一方向性関数  $f$  が存在する。
- (c)  $\text{range}(f) = \Sigma^*$  な  $c$ - $q$  量子一方向性関数  $f$  が存在する。

部分一方向性関数の存在と全域一方向性関数の存在の等価性は  $c$ - $q$  量子一方向性関数においても適用でき、以下が言える。

補題 3.2  $g$  を  $\mathbb{N} \rightarrow \mathbb{N}^+$  の非減少関数とする。この時、 $g$ - $to$ -1 で全射な部分  $c$ - $q$  量子一方向性関数が存在する事と  $g$ - $to$ -1 で全射な全域  $c$ - $q$  量子一方向性関数が存在する事は同値である。

これより以下の結果も自然と示される。

定理 3.2 以下は同値である。

- (a)  $\text{EQP} \supseteq \text{UP} \cap \text{coUP}$
- (b)  $c$ - $q$  量子一方向性置換が存在する。

### 3.3 $q$ - $q$ 量子一方向性関数

この節では完全な量子の世界での特徴付けを行う。よって関係性を示す複雑さの理論のクラスは全て量子のクラスを用いる。それにあたり、 $\text{UP}$  の量子版がどういったものになるのかを正確に定義する必要がある。以下のように  $\text{UP}$  の量子版  $\text{UQP}$  を定義した。

定義 3.5 証拠が与えられた時に、多項式時間で確実に認識可能な QTM を  $\text{UQTM}$  と呼び、 $\text{UQTM}$  によって受理される言語の集合を  $\text{UQP}$  と呼ぶ。ただし証拠は古典情報に限る。

この定義を用いると、以下の定理が成り立つ。

定理 3.3 以下は全て同値である。

- (a)  $\text{EQP} = \text{UQP}$
- (b)  $\text{QPSV} = \text{UQPSV}$
- (c)  $\text{QPSV} = \text{UQPSV}_g$

定理 3.4 以下は同値である。

- (a)  $\text{UQP} \neq \text{EQP}$
- (b) 全域な  $q$ - $q$  量子一方向性関数が存在する。

### 3.4 $q$ - $q$ 量子一方向性置換

定理 3.5 以下は全て同値である。

- (a)  $\text{EQP} \neq \text{UQP} \cap \text{coUQP}$
- (b)  $\text{range}(f) \in \mathbf{P}$  な  $q$ - $q$  一方向性関数  $f$  が存在する。
- (c)  $\text{range}(f) = \Sigma^*$  な  $q$ - $q$  一方向性関数  $f$  が存在する。

部分一方向性関数の存在と全域一方向性関数の存在の等価性は  $q$ - $q$  量子一方向性関数においても適用でき、以下が言える。

補題 3.3  $g$  を  $\mathbb{N} \rightarrow \mathbb{N}^+$  の非減少関数とする。この時、 $g$ - $to$ -1 で全射な部分  $q$ - $q$  量子一方向性関数が存在する事と  $g$ - $to$ -1 で全射な全域  $q$ - $q$  量子一方向性関数が存在する事は同値である。

これより、以下の結果も自然と示される。

定理 3.6 以下は同値である。

- (a)  $\text{EQP} \neq \text{UQP} \cap \text{coUQP}$
- (b)  $q$ - $q$  量子一方向性置換が存在する。

### References

- [1] J. Grollmann, A. Selman: Complexity measures for public-key cryposystems, SICOMP 17, pp.309–335, 1988.
- [2] C. M. Homan, M. Thakur: One-way permutation and self-witnessing languages, JCSS 67, pp.608–622, 2003.
- [3] A. Kawachi, H. Kobayashi, T. Koshihara, R. H. Putra: Universal test for quantum one-way permutations, TCS 345, pp.370–385, 2005.
- [4] A. Kawachi, T. Koshihara, H. Nishimura, T. Yamakami: Computational indistinguishability between quantum states and its cryptographic application. Proc. EUROCRYPT 2005, LNCS 3494, pp.268–284, 2005.
- [5] E. Kashefi, H. Nishimura, V. Vedral: On quantum one-way permutations, QIC 2, pp.379–398, 2002.