量子公開鍵暗号とその後の動向

宮澤　俊之

現在，実用的に用いられている公開鍵暗号系の技術は，量子計算機が実用化されると全て破られてしまうため，量子計算機に対して安全な公開鍵暗号を設計することは重要な技術的課題である．このような公開鍵暗号の構成方法として，量子計算機を用いても効率的に解けないと予想されるNP困難問題に基づく構成方法に注目が集まっている．本稿では，この分野が注目を集めるきっかけとなった部分和問題に基づく方式（OTU 2000）と，研究の進展が目覚ましい格子問題に基づく方式の研究動向を紹介する．

キーワード：量子計算機，NP困難問題，公開鍵暗号，ナップザック暗号，格子，SVP

1．はじめに

インターネットが普及している現在において，公開鍵暗号系の技術（公開鍵暗号，デジタル署名，鍵共有，認証技術）は，不特定多数の利用者の間で安全な通信を実現するために中心的な役割を果たしている．例えば，インターネットショッピングにおいてクレジット番号や氏名・住所などの個人情報を安心・安全に送信するためには，鍵配送やデジタル署名など公開鍵暗号系の技術の利用は必須となっている．また，情報漏洩防止の観点から，メールの暗号化を導入している企業も多いのではないだろうか．このように，不特定多数の利用者間で通信する基盤が整っており，また，企業活動における情報の価値が高まりつつある現代社会では，公開鍵暗号系の技術は社会的基盤のひとつといってもよいであろう．

この公開鍵暗号系の技術の安全性を支えているのは，計算量に関する仮定である．例えば，RSA暗号は，現在の計算機では素因数分解問題が効率的に解けない（確率的多項式時間Turing機械では解けない）という仮定を安全性の基盤としている．また，Diffie-Hellmann鍵共有方式や，いわゆる楕円曲線暗号は，離散対数問題が確率的多項式時間Turing機械では解けないという仮定を安全性の基盤としている．これらの計算量に関する仮定は，厳密な意味で計算が困難であることは証明されていないが，多くの研究者によって計算が困難であると信じられている．

ところが，1994年にShorによって，量子Turing機械（いわゆる量子計算機）という計算機モデルを利用すれば，素因数分解問題や離散対数問題を（確率的）多項式時間で解けることが示された[19]．つまり，現在広範に利用されている公開鍵暗号技術であるRSA暗号や，DH鍵交換，楕円曲線暗号は量子計算機が実用化されるとすべて破られることになる．

実用的な鍵サイズの公開鍵暗号を破ることのできる量子計算機が実用化される時期は，かなり先のことと予想されている．しかし，公開鍵暗号が社会基盤となっている現状から考えると，量子計算機が実用化されたときに備え，今からその対策を進めておくことは重要な技術的課題である．

このような背景を踏まえて，2000年に岡本らは，量子計算機の実用化後も安全な公開鍵暗号「量子公開鍵暗号」のパラダイムを示すとともに，量子計算機でも効率的に解けないと予想されるNP困難問題[1]である部分和問題に基づく具体的な構成（OTU 2000）[15]を提案した．この発表をきっかけに，量子計算機では効率的に解けないことが予想されているNP困難問題（厳密に言えば，その緩和問題）に基づく公開鍵暗号方式に関する研究に注目が集まるようになった．NP困難問題に基づく公開鍵暗号方式は，公開鍵暗号の概念が提唱されたのとほぼ同時期から数多くの方式が提案されていたが，RSA暗号や楕円曲線暗号に比べて，鍵サイズや処理速度などの面で効率の悪く，一部の研究者のトピックに過ぎなかった．しかし，量子計算機による公開鍵暗号の危機が示されてから，改め

みやざわ　としゆき
NTT東日本 ITイノベーション部
〒163-8019 新宿区西新宿3-19-2

[1] NP困難問題の厳密な定義については，例えば文献[20]を参照していただきたい．

てこの分野の研究の意義が高まってきたのである．

本稿では，この分野が注目を集めるきっかけとなったOTU 2000と，最近研究の進展が目覚ましい格子を用いた方式，およびその研究動向を紹介する．

2. 部分和問題に基づく方式

2.1 量子公開鍵暗号 OTU 2000

OTU 2000は，量子計算機でも効率的に解くことができないと予想されるNP困難問題の部分和問題の困難さを利用した公開鍵暗号，いわゆるナップザック暗号である．岡本らは，量子計算機を援用することによって，既存の方式の問題点を解消したナップザック暗号を提案している．具体的な方式を示す前に，部分和問題の定義をしておこう．

定義2.1．[部分和問題] $a_1, \cdots, a_n \in \mathbb{N}, (m_1, \cdots, m_n) \in \{0,1\}^n, C=\sum_{i=1}^n m_i a_i$ とする．$a_1, \cdots, a_n, C$ が与えられたとき，$(m_1, \cdots, m_n)$ を求めよ． □

OTU 2000を含むナップザック暗号は，部分和問題を暗号文の生成に利用している．つまり，暗号化に用いる公開鍵は $[a_1, \cdots, a_n]$ と平文 $(m_1, \cdots, m_n) \in \{0,1\}^n$ を用いて，暗号文を $C=\sum_{i=1}^n m_i a_i$ とするのである．

ナップザック暗号は，RSA暗号とほぼ同時期に提案された古くからある暗号であるが，既存の方式は鍵生成に不備があったため，すべて解読されてきた．既存方式の鍵生成では，線形モジュラー変換や，離散対数を用いた非線形変換によって，部分和問題が解きやすいインスタンス（＝秘密鍵）から，ランダムなインスタンス（＝公開鍵）への変換を試みた．しかし，前者は線形性によって解読され，後者は離散対数の計算のために利用した有限体の代数的構造を分析することによって解読された．

OTU 2000は，非線形変換のべき乗/離散対数の関係を用いた変換に着目し，量子計算機を援用して一般の有限体の離散対数を扱うことによって，安全性の課題を解消している．OTU 2000の概略を以下に示す[2]．

鍵生成アルゴリズム システムパラメータ $n, k \in \mathbb{N}$ に対して，以下のようにして，秘密鍵 $SK=(g, N, p_1, \cdots, p_n, k)$ と公開鍵 $PK=(n, k, b_1, \cdots, b_n)$ を計算する：

1. 素数 p と，生成元 $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ をランダムに選択する．
2. 次の条件を満たす n 個の整数 $p_1, \cdots, p_n$ をランダムに選択する．
   - $\forall i, j: i \neq j \Rightarrow \gcd(p_i, p_j)=1$
   - 任意の $\{p_{i_1}, \cdots, p_{i_k}\} \subset \{p_1, \cdots, p_n\}$ に対して，$\prod_{j=1}^k p_{i_j} < p$ を満たす．
3. 各 p_i に対して，$p_i \equiv g^{a_i} \pmod p$ を満たす $a_i \in \mathbb{Z}/(p-1)\mathbb{Z}$ を求める．
4. 公開鍵を $PK=(n, k, a_1, \cdots, a_n)$ とし，秘密鍵を $SK=(g, p, p_1, \cdots, p_n)$ とする． □

暗号化アルゴリズム 公開鍵 PK と $\left\lfloor \log_2 \binom{n}{k} \right\rfloor$ ビットの平文 M から，以下のようにして，暗号文 C を計算する．

1. M を，$\sum_{i=1}^n m_i = k$ となるビット列 $m=(m_1, \cdots, m_n)$ に変換する．
2. $C=\sum_{i=1}^n m_i a_i$ を出力する． □

復号アルゴリズム 秘密鍵 SK と，暗号文 C から，以下のようにして，平文 M を復号する：

1. $u=g^c \bmod p$.
2. $m=(m_1, \cdots, m_n) \in \{0,1\}^n$ を以下のように計算する：
   u が p_i で割り切れるならば $m_i=1$，そうでなければ $m_i=0$ とする．
3. m を $\left\lfloor \log_2 \binom{n}{k} \right\rfloor$ ビットの平文 M に復元する．

□

復号アルゴリズムによって，秘密鍵と暗号文から，$(m_1, \cdots, m_n)$ が復元できることを確認しておこう．u を計算すると以下のようになる：

$$u \equiv g^c \equiv g^{\sum_i m_i b_i} \equiv \prod_i (g^{a_i})^{m_i} \pmod p$$
$$\equiv \prod_i p_i^{m_i} \pmod p.$$

ここで，$p_1, \cdots, p_n$ の条件から，$\prod_i p_i^{m_i} \in \{0, \cdots, p-1\}$ は一意に定まる．$p_1, \cdots, p_n$ が互いに素である，という条件から，$\prod_i p_i^{m_i}$ は p_i の積に一意に分解される．したがって，u を p_1 から p_n まで試し割りすることによって $(m_1, \cdots, m_n)$ を復元することができる．

鍵生成において，秘密鍵のパラメータ p_j にStep 2の条件があるために，Step 3において，有限体の乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ の離散対数を計算しなくてはならない．離散対数の計算は，現在の計算機でもある程度の大きさであれば，現実的な時間で計算できるが，冒頭で述べたように現在の公開鍵暗号を支える安全性の仮定となる計算困難な問題である．OTU 2000では，この離

[2] OTU 2000では，一般の代数体を利用しているが，ここでは説明の簡略化のため，有理数体に限定する．

散対数の計算に量子計算を援用している．それ以外の処理（暗号化，復号）は，量子計算機を使わずに高速に処理することができる．

その後の展開として，宮澤らによって，量子計算機を使わずに現実的な時間で鍵生成を可能とする改良方式が提案されて[10][11]，OTU 2000は実用的に利用可能な方式となった．

2.2 OTU 2000の安全性

ここでは，部分和問題に対する攻撃方法について解説する．OTU 2000（および，改良方式）固有の安全性については，文献[10][11]を参照されたい．

meet-in-the-middle攻撃 公開鍵と暗号文から秘密鍵を求める方法として，単純な全数探索以外に，meet-in-the-middle攻撃がある．これは，2つのリスト

$$L_1=\left\{\sum_{i=1}^{n} b_i x_i \,\middle|\, \begin{matrix}(x_1,\cdots,x_n)\in\{0,1\}^n \\ \sum_{i=1}^{n} x_i = k/2\end{matrix}\right\},$$

$$L_2=\left\{C-\sum_{i=1}^{n} b_i x_i \,\middle|\, \begin{matrix}(x_1,\cdots,x_n)\in\{0,1\}^n \\ \sum_{i=1}^{n} x_i = k/2\end{matrix}\right\}$$

を作成し，$L_1\cap L_2$を見つけることにより，平文を復元する攻撃である．この攻撃の計算コストは，$O\left(\binom{n}{k/2}\right)$である．また，これを改良した方式を用いることによって$O\left(\sqrt{k}\binom{n/2}{k/2}\right)$のコストで暗号文から平文を求めることができる．

したがって，これらの攻撃に対して安全であるためには，$\binom{n}{k/2}$と$\sqrt{k}\binom{n/2}{k/2}$が十分に大きくなるように，n, kを選択しなくてはならない．

格子を用いた攻撃 ナップザック暗号に対する古くから知られた攻撃として，低密度攻撃がある．この攻撃は，密度$d=\dfrac{n}{\max \log a_i}$が一定の値を下回った場合，暗号文の解読をある$n$次元の格子の最短ベクトル問題（SVP）に帰着するものである．後述するように，SVPもNP困難な問題であるため，SVPを汎用的に解く多項式時間アルゴリズムは知られていない．しかし，密度が低い場合には，LLLなどの格子の基底縮約アルゴリズムによって，暗号文と公開鍵から平文を復元できる．

OTU 2000はパラメータ設定によって低密度攻撃は回避できる．しかし，その後の安全性評価の結果，OTU 2000で扱う平文のHamming重みが低いという性質を利用することにより，部分和問題を格子のSVPに帰着できることが示された[12][14]．つまり，OTU 2000の安全性は，SVPの困難さに関係しているのである．

SVPの困難さについては，3.4節で改めて詳細に述べる．

3. 格子問題に基づく方式

3.1 準備

格子問題に基づく説明をする前に，本節で用いる記号の定義をまとめておく．

$\mathbb{R}^n$をn次元ユークリッド空間とする．$\mathbf{x}=(x_1,\cdots,x_n)$，$\mathbf{y}=(y_1,\cdots,y_n)\in\mathbb{R}^n$の内積を$\langle\mathbf{x},\mathbf{y}\rangle:=\sum_{i=1}^{n} x_i y_i$，$\mathbf{x}\in\mathbb{R}^n$の長さを$\|\mathbf{x}\|:=\sqrt{\langle\mathbf{x},\mathbf{x}\rangle}$とする．

$\mathbb{R}^n$内の格子Lとは，互いに独立な$d(\leq n)$個のベクトル$\mathbf{b}_1,\cdots,\mathbf{b}_d\in\mathbb{R}^n$によって$L=\{\sum_{i=1}^{d} n_i\mathbf{b}_i \mid n_i\in\mathbb{Z}\}$で記述できる集合を指し，$\mathbf{b}_1,\cdots,\mathbf{b}_n$を$L$の基底と呼ぶ．また，$\mathbf{B}=(\mathbf{b}_1,\cdots,\mathbf{b}_n)$を基底とする格子を$L(\mathbf{B})$とあらわす．また，格子$L$の双対格子$L^*$を$\{\mathbf{x}\in\mathbb{R}^n \mid \langle\mathbf{x},\mathbf{v}\rangle\in\mathbb{Z} \text{ for } \forall\mathbf{v}\in L\}$とする．$\lambda_1(L):=\min\{\|\mathbf{x}\|\mid\mathbf{x}\in\mathbf{L}\backslash\{\mathbf{0}\}\}$，つまり，$L$の非ゼロベクトルの中で，最短ベクトルの長さとする．また，$\lambda_2(L)$を，Lの最短ベクトルとは並行にならないベクトルの中で，もっとも短いベクトル，つまり，2番目に短いベクトルの長さをあらわすことにする．

定義3.1.［最短ベクトル問題（SVP$_\gamma$: Shortest Vector Problem)］ Lを格子とする．このとき，$\|\mathbf{v}\|\leq\gamma\lambda_1(L)$を満たす$\mathbf{v}\in L\backslash\{\mathbf{0}\}$を求めよ． □

SVP$_1$（つまり，最も短いベクトルを求める問題）はランダム帰着の下，NP困難であることが証明されている．また，γが定数の場合も，NP困難であることが示されている．一方，$\gamma=2^{n/2}$倍以下まで許すと，多項式時間で解けることが知られている．

格子に関する計算問題は複数あるが，SVPの緩和問題のひとつに単一最短ベクトル問題がある．後に用いるので，ここで紹介しておこう．

定義3.2.［単一最短ベクトル問題（f-uSVP: unique Shortest Vector Problem)］ Lを$f\leq\lambda_2(L)/\lambda_1(L)$を満たす格子とする．このとき，$\|\mathbf{v}\|=\lambda_1(L)$を満たす$\mathbf{v}\in L\backslash\{\mathbf{0}\}$を求めよ． □

ここで，SVP$_\gamma$を解くアルゴリズムは，$\gamma'\geq\gamma$となるγ'-uSVPを解くことができることに注意しておこう．

3.2 Ajtai-Dwork暗号

1996年に，Ajtai-Dworkは格子問題に基づく興味

深い特徴を備えた公開鍵暗号（以下AD 96）を提案した．その特徴とは，「AD 96を平均的に破ることができるならば，n^7-uSVPを（最悪時も含めて）すべてを解くことができる」ことである．

RSA，楕円曲線暗号や前述のOTU 2000などの一般の公開鍵暗号は，特定の問題の平均的な難しさを安全性の仮定としている．公開鍵暗号が仮定とする問題は，平均的に難しいことが求められるが，最悪時に帰着できる方式はそれまで知られていなかった．特に，NP困難問題は最悪時の評価であって，簡単なインスタンスもあれば，難しいインスタンスもある．NP困難な問題をもとに構成された公開鍵暗号が解読されたということは，結局，NP困難問題の簡単なインスタンスをもとに構成されていた，ということである．

それに対して，Ajtai-Dworkの方式は，n^7-uSVPの最悪時ケースへの帰着が証明できるため，安全性評価の意味で興味深い方式といえよう．

以下では，AD 96の概略を示す．以下では，$M=n^3$，$N=2^{n\log n}$とする．また，$\mathbf{B}=[\mathbf{b}_1,\cdots,\mathbf{b}_n]$に対して，$\mathcal{P}(\mathbf{B}):=\{\sum_i x_i\mathbf{b}_i : x_i\in[0,1)\}$とする．また，$\mathbf{x} \bmod \mathcal{P}(\mathbf{B})$で，$\mathbf{x}-\mathbf{r}\in L(\mathbf{B})$となる$\mathbf{r}\in\mathcal{P}(\mathbf{B})$とする．

秘密鍵　n次元単位球体からランダムに選択した$\mathbf{u}\in\mathbb{R}^n$を秘密鍵とする．□

公開鍵　$PK=(\mathbf{V},\mathbf{W})$を，以下のように生成する．

1. $\mathbf{V}:(\mathbf{v}_1,\cdots,\mathbf{v}_M)$を以下のようにサンプルする．
   (a) $\mathbf{v}_i'\in\{\mathbf{x}\in[0,N)^n|\langle\mathbf{x},\mathbf{u}\rangle\in\mathbb{Z}\}$をランダムに選択する．
   (b) $\delta_1,\cdots,\delta_n\in\{\mathbf{x}\in\mathbb{R}^n|\|\mathbf{x}\|\le n^{-8}\}$をランダムに選択する．
   (c) $\mathbf{v}_i=\mathbf{v}_i'+\sum_{i=1}^n\delta_i$
2. $\mathcal{P}(\mathbf{v}_{i_0+1},\cdots,\mathbf{v}_{i_0+n})$の幅が$n^{-2}N$以上となる最小のインデックス$i_0$をとり，$\mathbf{W}=(\mathbf{v}_{i_0+1},\cdots,\mathbf{v}_{i_0+n})$とする．□

暗号化アルゴリズム　AD 96は1ビットの平文mを暗号化する方式である．（複数ビットの場合は，各ビットごとに以下の処理を実施する．）mの値に応じて，公開鍵を用いて暗号文$\mathbf{c}$を以下のように計算する：

- $m=0$の場合，ランダムに$b_1,\cdots,b_M\in\{0,1\}$を選択し，$\mathbf{c}=\sum_{i=1}^M b_i\mathbf{v}_i \bmod \mathcal{P}(\mathbf{W})$を暗号文とする．
- $m=1$の場合，$\mathbf{c}\in\mathcal{P}(\mathbf{W})$をランダムに選択し，$\mathbf{c}$を暗号文とする．□

復号アルゴリズム　暗号文$\mathbf{c}$と秘密鍵$\mathbf{u}$を用いて，以下のように平文mを復号する：

1. $\tau=\langle\mathbf{c},\mathbf{u}\rangle$を計算する．
2. τがある整数と$1/n$以内の距離にあれば$m=0$，そうでなければ$m=1$を出力する．□

復号アルゴリズムの正当性について簡単に説明しよう．$H_0\subset\mathbb{R}^n$を$\mathbf{u}$の直行補空間とし，$k\in\mathbb{Z}$に対して$H_k:=H_0+k\mathbf{u}$とする．このとき，$\mathbf{v}_1,\cdots,\mathbf{v}_M$は，ある超平面$H_k$の近いベクトルとなるため，0の暗号文は，ある超平面H_k'の近いベクトルとなる．また，1の暗号文はある領域からランダムに選んだベクトルなので，H_kに近いとは限らない．したがって，$\mathbf{u}$を知っていれば，0の暗号文は必ず0に復号される．しかし，およそ$2/n$の確率で1の暗号文は0と復号されてしまう．この問題はGoldreich-Goldwasser-Haveriによって，1の暗号文を$\{H_k+1/2\}$付近にとることによって解消されている[6]．

AD 96の安全性　一見するとAD 96は，uSVPとあまり関係ないように思えるが，uSVPは双対格子を用いて，隠れ超平面問題（Hidden hyperplane problem）に変換することができる．隠れ超平面問題とは，大まかに言えば，$\mathbb{R}^n$内の一様分布と，上記$\{H_i\}$付近に集中した分布を識別する問題である．つまり，AD 96における1の暗号文と0の暗号文を識別する問題である．詳しくは文献[1]を参照していただきたいが，AD 96の0の暗号文と，1の暗号文を識別できるアルゴリズムが存在すれば，任意のn^7-uSVPを解くことができることが証明できる．つまり，AD 96の平均的な安全性が，特定のuSVPの最悪時の困難さに帰着している．

しかし，AD 96は効率が悪く，それを利用した攻撃がNguyenらによって示されている[13]．AD 96の安全性を確保するには，公開鍵の長さは$O(n^5\log n)$となり，例えば，$n=32$としても，公開鍵は20メガバイト，1ビットあたりの暗号文は6144ビットとなる．AD 96の現実的な利用を想定すれば，nは小さな値となり，その場合AD 96の公開鍵から秘密鍵を求めることができることを示唆している．これは，AD 96が現実的な意味で利用できる公開鍵暗号ではないことも意味している．

3.3　その後の展開

AD 96の後，Regevによって，ガウス分布とフーリエ解析を用いて，$n^{1.5}$-uSVPの最悪時に帰着させる方式（Regev 04）が提案されている[17]．その後，Regevは，量子計算を用いて$\mathrm{SVP}_{n^{1.5}}$の最悪時に帰着させる方式（Regev 05）を提案している[18]．AD 96とRegev 04がSVPの緩和問題であるuSVP

の最悪時へ帰着させているのに対し，Regev 05は，量子計算を用いた帰着ではあるものの，SVPそのものの最悪時に帰着させているという点で興味深い．また，Regev 05は，OTU 2000の改良方式と同様に，通常の計算機で実行可能であり，方式自体に量子計算機は用いない．量子計算機を利用するのは，困難性の帰着時に使うのみである．

これまでに挙げたAD 96，Regev 04，Regev 05は，すべて最悪時への帰着が証明可能である点で理論的には興味深い方式ではある一方で1ビット暗号であるため実用的な方式とは言い難い．しかし，この問題を解決する方式として，草川らによって，1ビットの格子暗号を$O(\log n)$ビットの格子暗号へ汎用的に変換できる方式[7]が提案され，効率面での改良もすすんでいる．

上記に挙げた方式のほかにも，最悪時への帰着はないが，格子のSVPの困難性を安全性の仮定する効率的な方式も存在する．そのなかでもNTRU[4]は，近年標準化を進めつつあるが，攻撃と改良が提案されて続けており，安全性に関する議論は現在も盛んに続けられている．

3.4 格子問題の難しさ

本節で述べた格子に基づく暗号の安全性や，前節で示したOTU 2000の安全性は，SVPおよびその緩和問題の難しさに関係している．では，SVPは実際にどの程度難しい問題なのであろうか．

一般にSVPはNP困難であるため，多項式時間で汎用的なSVPを厳密に解くアルゴリズムは知られていない．実際，現在知られているSVPを解く最良のアルゴリズムの計算量は$2^{O(n)}$である[2]．

一方，LLLやBKZなどの基底縮約アルゴリズムは，近似SVPアルゴリズムとして機能するが，理論的に保証されている最悪の近似精度に比べてかなり短いベクトルを出力し，入力する基底によっては最短ベクトルを出力することもある．これらの基底縮約アルゴリズムは，決定性のアルゴリズムであるものの，出力に関する挙動は明確にわかっていない．

しかし，その挙動を解析しようとする研究も盛んに行われている．Gamaら[5]は，計算機実験を通じて，現状の基底縮約アルゴリズムによって出力されるベクトルの長さを評価し，次元$n \geq 500$のとき，一般のランダムな格子では$\|\mathbf{v}\| \leq (1.005)^n \cdot \mathrm{vol}(L)^{1/n}$を満たす$\mathbf{v}$を求めることはできないだろうという見解を示している．また，SVP_γについては$\gamma \geq 1.01^n$，uSVPについてはλ_2/λ_1が1.01^nの定数倍以上であれば現実的な時間で解くことが可能だろう，という見通しを示している．

このような研究は，格子問題と関連する公開鍵暗号の設計や実用的なパラメータを決める上で非常に重要であり，より厳密な評価を与えていくことは今後の重要な研究課題である．

4. おわりに

本稿では，量子計算機が実用化した後も安全と考えられる公開鍵暗号としてOTU 2000と格子に基づく暗号に絞って，方式と研究動向を紹介した．本稿では枚数の都合上紹介できなかったが，量子計算機が実用化した後も安全と考えられる公開鍵暗号の構成方法としては，ハッシュ関数に基づく方式，符号問題に基づく方式，多変数2次連立方程式に基づく方式などがある．それらについては，文献[3]を参考にしていただきたい．

本稿で紹介したような公開鍵暗号は新しい提案も多く，数多くの課題が残っている．理論面では，格子に関する問題以外のNP困難問題（または，その緩和問題）の最悪時に帰着できる方式の構成が挙げられる．また，現実の使用を想定すれば，3.4節で示したような解析も含めた安全性評価・解析はまだ不十分であり，信頼性を高める上では更なる解析が必要である．NP困難な問題に基づく公開鍵暗号は，現在使われている公開鍵暗号に比べて鍵長が長く，効率性の改良も重要な研究課題である．また，本稿で触れることのできなかったデジタル署名方式・認証方式など，他の方式も同様の課題がある．

本稿が日本における「量子公開鍵暗号」の研究の活性化につながれば幸いである．

謝辞 本稿をまとめるにあたり，貴重なコメントをいただいた，NTT情報流通プラットフォーム研究所の小林鉄太郎さんに感謝いたします．

参考文献

[1] M. Ajtai and C. Dwork, "A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence," In Proc. 28th STOC, pp. 284-293, ACM (1996).

[2] M. Ajtai, R. Kumar and D. Sivakumar, "A Sieve Algorithm for the Shortest Lattice Vector Problem," In Proc. 33rd STOC, pp. 601-610, ACM (2001).

[3] D. Bernstein, J. Buchmann and E. Dahmen (ed.), "Post Quantum Cryptography," Springer (2009).
[4] J. Hoffstein, J. H. Silverman and W. White, "Estimated Breaking Times for NTRU Lattices," NTRU Cryptosystems, NTRU Report 012, Version 2, available at http://www.ntru.com (2003).
[5] N. Gama and P. Q. Nguyen, "Predicting Lattice Reduction," In Proc. Eurocrypt '08, LNCS 4965, pp. 31-51, Springer-Verlag (2008).
[6] O. Goldreich, S. Goldwasser and S. Halevi, "Eliminating Decryption Errors in the Ajtai-Dwork Cryptosystem," CRYPTO 1997, LNCS 1294, pp. 105-111, Springer (1997).
[7] A. Kawachi, K. Tanaka and K. Xagawa, "Multibit Cryptosystems Based on Lattice Problems," In PKC 07, LNCS 4450, pp. 315-329, Springer-Verlag (2008).
[8] D. Micciancio, "Cryptographic functions from worstcase complexity assumptions," http://www-cse.ucsd.edu/daniele/papers/LLL25.html (2007).
[9] D. Micciancio and S. Goldwasser, Complexity of Lattice Problems: a cryptographic perspective, Kluwer Academic Publishers (2002).
[10] T. Miyazawa, T. Kobayashi, S. Oda, I. Nakamura and A. Kanai, "Implementation of improved "Quantum public-key cryptosystem," Proc. of PQCrypto 2006, pp. 181-191, available at http://postquantum.cr.yp.to/ (2006).
[11] 宮澤, 小林, 小田, 金井, "量子公開鍵暗号の実装方式," In Proc of SCIS 2007, 3 A 3-5 (2007).
[12] P. Q. Nguyen and J. Stern, "Adapting Density Attacks to Low-Weight Knapsacks," Proc. of Asiacrypt 2005, LNCS 3788, pp. 41-58, Springer-Verlag (2005).
[13] P. Q. Nguyen and J. Stern, "Cryptanalysis of the Ajtai-Dwork Cryptosystem," Proc. of CRYPTO '98, LNCS 146, pp. 223-242, Springer-Verlag (1998).
[14] K. Omura and K. Tanaka, "Density Attack to the Knapsack Cryptosystems with Enumerative Source Encoding," IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E87-A, No. 6, pp. 1564-1569 (2004).
[15] T. Okamoto, K. Tanaka and S. Uchiyama, "Quantum Public Key Cryptosystems," Proc. of CRYTPTO 2000, LNCS 1880, pp. 147-165, Springer-Verlag (2000).
[16] 岡本, 田中, "量子公開鍵暗号," 量子情報科学とその展開—量子コンピュータ・暗号・情報通信—, 別冊・数理科学 2003 年 4 月, pp. 154-159, サイエンス社 (2003).
[17] O. Regev, "New lattice-based cryptographic constructions," J. ACM 51 (6), pp. 899-942 (2004).
[18] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," In 37th STOC, pp. 84-93, ACM (2005).
[19] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," Proc. 35nd Annual Symposium on Foundations of Computer Science (Shafi Goldwasser, ed.), IEEE Computer Society Press, pp. 124-134 (1994).
[20] M. Sipser, "Introduction to the Theory of Computation (Second edition)," Course Technology, 2005. 太田和夫, 田中圭介監訳『計算理論の基礎 原著第 2 版』, 共立出版 (2008).