解説

量子コンピュータは公開鍵暗号にとって脅威なのか？

■ 小柴 健史 ■

埼玉大学工学部情報システム工学科
koshiba@tcs.ics.saitama-u.ac.jp

量子コンピュータが実現すると素因数分解等を効率的に解くことができ，RSA 暗号等の公開鍵暗号の解読が可能となってしまうことが知られている．量子暗号として有名な量子鍵配送プロトコルはその性質から，公開鍵暗号にとって変わるものではない．では，量子コンピュータが実現してしまった場合，現在のセキュリティ基盤を支える公開鍵暗号系の技術は崩壊してしまうのであろうか？　本稿では，敵対者として量子コンピュータが存在したとしても安全性が保たれるような公開鍵暗号系の技術の最新動向について紹介する．

はじめに

インターネットが広く普及し社会基盤の1つになり，インターネットバンキングやインターネットショッピングなどの個人レベルの経済活動も盛んになってきている．また，政府高度情報通信ネットワーク社会推進戦略本部が主導するe-Japan重点計画によりネットワークを通じた行政サービスの提供などが本格的になってきている．それに伴い，インターネットセキュリティの重要性がますます大きくなってきているのは言うまでもないだろう．インターネットセキュリティと一言で言っても広範な課題であり，技術的な面から法的な面まで多岐に渡っている．このように広範な課題においては細分化して検討されるのが一般的であり，インターネットセキュリティにおいても同様である．インターネットセキュリティの技術的な面における最も基礎的な技術として公開鍵暗号系の技術がある．ここで「公開鍵暗号系の技術」とは単に公開鍵暗号のことを指すのではなく公開鍵暗号やディジタル署名，認証技術などを含む技術の総称である「公開鍵基盤」の基礎技術のことを指すことにする．

「公開鍵暗号系の技術」はインターネットセキュリティの基盤となる技術であることは述べたが，基盤技術となるからには堅牢であることが要求される．実際に利用されている「公開鍵暗号系の技術」の安全性は素因数分解問題あるいは離散対数問題は効率的に解けないという性質に依拠している．素因数分解問題や離散対数問題に対して厳密な意味で計算が困難であるという証明は与えられていないものの，その困難性は多くの（暗号）研究者によって強く信じられている．

さて，1994年にShorは量子コンピュータを用いることができれば素因数分解問題と離散対数問題が効率的に解けるという驚くべき事実を発見した．現在の公開鍵基盤の基礎技術として広く利用されている公開鍵暗号方式としてRSA暗号が有名であるが，素因数分解が効率的に解けるとRSA暗号は解読されてしまうことが知られている．離散対数問題を利用している方式についても同様に解読されてしまうことになる．つまり，量子コンピュータが実現するかもしれない将来，すなわちPost-Quantum時代には，「現在の」公開鍵基盤は根底から覆されてしまうことになる．公開鍵基盤はもはや社会基盤の1つであり，Post-Quantum時代でも安全であるような公開鍵基盤が必要不可欠であるが，公開鍵基盤の基礎となるようなPost-RSA暗号が存在するのか否かは非常に重要なテーマである．「現在の」公開鍵基盤は素因数分解問題や離散対数問題が効率的に解けないことを安全性の根

拠としているが，公開鍵暗号系の技術は必ずしも素因数分解問題や離散対数問題の難しさに頼る必然性はなかろう．さらに敵対者が量子コンピュータを利用できるのならば暗号システムを構築する上で量子コンピュータを積極的に利用し安全性が保たれるようにするアプローチも可能であろう．本稿では，タイトルにあるように「量子コンピュータは公開鍵暗号にとって脅威なのか？」についてさまざまな視点から見ていきたいと思う．

量子コンピュータと暗号技術

量子コンピュータの1つの特徴として，指数個の状態を量子重ね合わせとして持つことができ，かつ演算操作を同時に適用できることが挙げられる．一方で制約もあり，1つ目の制約として基本的な演算は可逆でなければならない．(R_1, R_2, R_3) をレジスタの3つ組とし，レジスタ R_1 に格納されている値と R_2 に格納されている値の乗算結果をレジスタ R_3 に書き込むことを考えよう．もし，レジスタ R_3 の値を上書きしてしまったら，元の値は何であったか復元することはできない．これに対して，乗算結果を上書きするのではなく，レジスタ R_3 の元の値に対して乗算結果を加算して書き込むことを考えると，R_3 の値に元々どんな値が格納されていたのか復元できる．なぜならば，レジスタ R_1 と R_2 の値は改変されていないので，その乗算結果を R_3 に格納されている値から減じることが可能だからである．現在の計算状況から1つ前の計算状況が一意に決められるという性質のことを計算の可逆性と呼ぶ．2つ目の制約として，並列に重ね合わされた計算結果はどれか1つをランダムに取り出すことしかできないという性質がある．このため高い確率で正解を得るためには多くの計算結果が一致していなければならない．本稿での「量子アルゴリズム」という言葉は，量子計算機上で動作し高い確率で正解を出力するものを指すこととする．

複数の状態を並列的に扱う計算パラダイムとして非決定性計算がある．解の候補ごとに並列的に処理して，1つでも正解であることが多項式時間内で確認できればよいとする計算方式のことを非決定性多項式時間アルゴリズムと呼ぶ．計算量クラスNPとは非決定性多項式時間アルゴリズム存在するような問題のクラスである．NP困難な問題Aとは，仮にAが（決定性）多項式時間で解けると仮定したとき，Aを解くアルゴリズムを利用してすべてのNP問題が多項式時間で解けるようになる問題をいう（問題AがNP困難であることを証明する常套手段は，Aを解くアルゴリズムが存在すると仮定したとき，それを利用してNP困難であることがすでに分かっている問題Bが多項式時間で解けることを示すことであり，これを問題Bから問題Aへの帰着という）．言い換えるならば，NP困難問題とは，任意のNP問題と同等かそれ以上に難しい問題ともいえる．

さて，量子アルゴリズムは指数個の状態に対して同時に演算を適用できるので非常に強力なことができるように思えるかもしれない．しかし，一方でNP計算の場合，正しい答えに1つでも辿り着けばよいので，すべてのNP問題を量子アルゴリズムで解くのは難しそうである．実際にNP困難問題は量子計算を利用しても多項式時間では解けないだろうと予想されている．代表的な量子アルゴリズムとしてGroverアルゴリズムと呼ばれる手法がある．GroverはNP困難な問題を量子コンピュータを利用して多項式時間で解くことを目指して，N個の要素から特定の要素を$O(\log N)$ 時間で見つけようとしていた．この意味では失敗に終わったが，結局$O(\sqrt{N})$時間で見つける方法が得られたという経緯もある．

では，量子アルゴリズムで効率的に解けるような問題とはどのような問題であろうか？　前述したように，素因数分解問題と離散対数問題は量子アルゴリズムを用いれば効率的に解ける．離散対数問題についてはなじみのない読者が多いかもしれないので，簡単な例を用いて説明しよう．整数を7で割った余りは0, 1,..., 6であり，余り全体を$\mathbb{Z}_7$と表記する．また，15を7で割った余りは15 mod 7のように表す．余りが1であるというこの事実は$15 \equiv 1 \bmod 7$とも表記する．$\mathbb{Z}_7$には面白い性質があり，$\{3^i \bmod 7 \mid i = 1, 2,..., 6\} = \{1, 2,..., 6\}$ のような関係が成立する．つまり，$\mathbb{Z}_7$に属する0以外の元は3のべきを7で割った余りとして表現できるのである．このような3は$\mathbb{Z}_7^*$ $(= \mathbb{Z}_7 - \{0\})$ の生成元と呼ばれる．生成元を考えると $3^x \equiv 4 \bmod 7$ のような方程式に必ず解が存在することが保証されるのである．一般の素数pについても$\mathbb{Z}_p^*$ $(\mathbb{Z}_p - \{0\})$ には生成元が存在することが分かっている．生成元gを固定して$g^x \equiv y \bmod p$ を考えるとyが与えられた時にxを求める問題を離散対数問題といい，現状では効率的な解法は知られていない．$3^x \equiv 4 \bmod 7$ の例では6通りの可能性をすべてを試すことにより，解 $x = 4$ を現実的な時間内で計算できる．しかし，大きな素数（たとえば100桁の素数p）では離散対数問題を現実的な時間内で解くのは難しくなる．この離散対数問題は量子コンピュータを利用すれば効率的に解けるわけだが，なぜ解けるのか直観的な説明を試みようと思う．Shorの量子アルゴリズムの本質はフーリエ変換が量子コンピュータ上で多項式時間で計算できることにある．今，$f(a, b) = g^a y^{-b} \bmod p$という関数を導入しよう．この関数は$f(a, b) = g^{a-xb} \bmod p$とも書ける．また，$f(a_1, b_1) = f(a_2, b_2) \Longleftrightarrow (a_1, b_1) = (a_2, b_2) + k(x, 1)$ という関係があるのも確かめられる．関数fは周期的な関数であり，そ

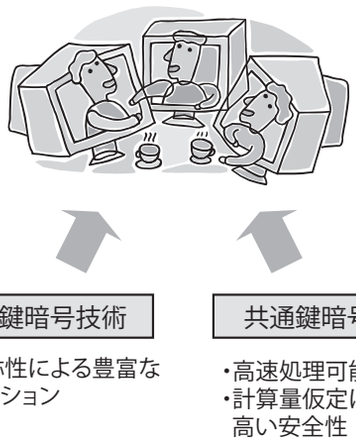

図 -1　共通鍵暗号技術と公開鍵暗号技術の相互補完

の周期は秘密のxに依存しているのである．フーリエ変換は周波数成分に分解する技術であるが，この場合xに依存した周波数しかないので，フーリエ変換によってxが取り出せるという具合である．

上で述べた$\mathbb{Z}_7^*$や$\mathbb{Z}_p^*$は群と呼ばれる数学的構造を持っている．集合Sとその集合上に定義された二項演算を考え，結合法則が成立し，単位元と逆元が存在するならば，その集合（とその演算）は群と呼ばれる．たとえば，$\mathbb{Z}_p^*$は「掛けた後でpで割った余りを取る」演算に関して群である．さて，$\mathbb{Z}_7^*$や$\mathbb{Z}_p^*$には交換法則が成立し，群のなかでも可換群と呼ばれるものである．可換群の場合，フーリエ変換が自然に定義されることを利用して，Shorの量子アルゴリズムをより一般的な問題が解けるように拡張できる．この拡張により，楕円曲線暗号も解読されてしまうことが分かっている．一方で，非可換な群に関しては拡張が容易ではなく，特殊な場合を除いて未解決である．代表的な非可換群として対称群がある．対称群とは，たとえば$\{1, ..., n\}$上の置換写像全体から構成される群である．対称群の演算は写像の合成であり，$n \geq 3$のときにはこの群は非可換になる．対称群への拡張は大きなブレークスルーが必要であると予想されており，量子計算の研究分野における最重要課題の1つである．それでは，非可換な群構造を利用した暗号方式を構築すればよさそうであるが，ことはそれほど単純ではない．暗号には暗号化して復号すると元に戻るという性質が必要である．群構造を利用している暗号方式の場合の多くは，これを実現するための機構として可換性を利用しているのである．

この章では，量子コンピュータと公開鍵暗号技術の関係を見てきた．現在の暗号技術は公開鍵暗号系の技術と共通鍵暗号系の技術に大別されるものの，それぞれ一長一短があり**図-1**にあるように相補的な役割を果たしている．以下に，量子コンピュータと共通鍵暗号技術との関係も簡単に述べておく．共通鍵暗号技術に対する可能な攻撃方法としてGroverの量子アルゴリズムを適用することが考えられる．今，平文サイズが128ビット，暗号文サイズが128ビット，鍵サイズが128ビットの共通鍵を考えよう．さらに，盗聴者が何らかの手段を講じて，ある鍵の元での平文と対応する暗号文を複数組入手している状況を考えよう．盗聴者の目的は，秘密になっている鍵を求め，以降の通信内容を傍受することである．それでは，鍵を求める計算量について考えてみることにする．盗聴者が入手した平文と暗号文との対応関係を満足させるような鍵の候補はおよそ1つ程度であり，共通鍵ブロック暗号の構造を考慮しない場合，通常のコンピュータで鍵を見つけるためには，最悪の場合2^{128}通り試さないといけない．一方，Groverの量子アルゴリズムを利用すると，$2^{64}(=\sqrt{2^{128}})$程度試せば十分であることが導かれる．とはいうものの，鍵サイズを2倍程度に再設定することにより，従来と同程度の安全性を保つことができる．量子アルゴリズムを利用できるという前提があっても，Groverアルゴリズムを用いる以外の共通鍵暗号に対する有効な攻撃方法は知られていないため，共通鍵暗号技術に対する攻撃として量子コンピュータはさほど強力ではないのが現状である．

量子暗号

「量子メカニズム」と「暗号」の2つの単語から「量子暗号」を思い浮かべる人が多いかもしれない．量子暗号とは，光子の偏光を利用したBennettとBrassardの鍵共有方式についての俗称で，彼らが論文題目として利用したことに始まる．いわゆる量子暗号については諸所に解説記事があるので，ここでは彼らのプロトコル（通称BB84プロトコル）の簡単な性質を書くにとどめることにする．量子暗号の詳細については文献6）を参照して欲しい．

BB84プロトコルの目的は互いに離れたところにいる二者が量子通信路を介してランダムなビット列を共有することである．BB84プロトコルは2つのフェーズに分けられ，前半のフェーズでは量子状態と呼ばれる状態を量子通信路を介して伝送する．後半のフェーズでは前半フェーズにおいてどのような量子状態を送ったのかを表す情報をビット列で表現しそれを古典通信路を介して伝送する（量子に対して「古典」と呼ばれるが，通常の通信路のことである）．

BB84プロトコルでは，量子通信路が盗聴されているとすると，盗聴があった事実が判明する仕組みになっている．原理について抽象化して，つまり物理的なこと

図-2　量子メカニズムの従来の位置付け

は省いて，説明しよう．いま，ベクトル空間の直交基底 (a, b) を考える．ここで，ベクトルaとbの大きさは同じとする．このとき，$(a - b, a + b)$ も同じベクトル空間の直交基底となる．これを適当に正規化したものを (c, d) としよう．量子状態とは $v = \alpha a + \beta b$ のようにベクトルの線形結合で表すことができる．また，観測と呼ばれる操作があるが，vを観測するとαに応じた確率でvはaに変化し，βに応じた確率でvはbに変化する．ベクトル空間の基底の選び方には自由度があるので，観測する前に基底を選んでおく必要がある．BB84プロトコルでは (a, b) か (c, d) の2種類の基底だけを利用している．送信者は，まず，基底を選択し，ビット0を送りたい場合は，選んだ基底が (a, b) であればaを送り，選んだ基底が (c, d) であればcを送る．ビット1を送りたい場合は，選んだ基底が (a, b) であればbを送り，選んだ基底が (c, d) であればdを送る．盗聴者は送信者がランダムに選択した基底が分からないので，盗聴者自身でもランダムに基底選択し観測することになる．盗聴者は1/2の確率で基底選択を誤るが，この場合，観測して得られるビットは0かまたは1が等しい割合で得られるだけである．しかも，この場合，送信者が送った量子状態と受信者が受け取る量子状態が異なるものになるので，この事実を利用して盗聴の有無を後で確認できるのである．また，正規の受信者も送信者が選んだ基底は分からないまま観測することになるが，後半のフェーズで選んだ基底に関する情報を交換するので，送受信者の基底が一致しているときに交換した情報のみを利用することにより，ビット列を共有することができる．

BB84プロトコルに関しては，後半フェーズで利用される古典通信路が改竄に対して安全であるという条件の下で情報理論的に安全な鍵共有方式であることが証明されている．つまり，古典通信路は盗聴されていても一向に構わないのである．

古典通信路だけでこのような方式は実現不可能であることを情報理論的に証明できることも，BB84プロトコルが脚光を浴びる要因となっている．BB84プロトコルは共通鍵暗号系の技術として位置付けられ，量子メカニズムが共通鍵暗号系の技術へ貢献する立場となっている．一方で，前章で見たように，量子メカニズムは公開鍵暗号系の技術にとっては破壊者の立場にあり，多くの人にとっての量子メカニズムの位置付けは**図-2**のようなものであろうかと思う．

解読されていない暗号たち

現在，利用されている公開鍵暗号系の技術は素因数分解問題や離散対数問題が効率的に解けないことを前提としている．そのため，Post-Quantum時代には利用できない方式である．一方で，これらの問題に基づかない方式も公開鍵暗号研究の初期段階からいくつか提案されている．すでに解読されて忘れ去られた方式もあるし，改良等を重ねていまだに解読されていない方式もある．解読されていないにもかかわらず実際に利用されていない理由は実装上の効率の悪さにある．とはいえ，Post-Quantum 時代にPost-RSA暗号が存在しないのでは困るので，効率の面はとりあえず目をつむらざるを得ないだろう．あるいは，表舞台に登場することで効率の改善が期待できるかもしれない．

さて，NP困難な問題は量子コンピュータが利用できるとしても効率的に解けないという予想があることを述べた．それでは，NP困難な問題を利用した暗号方式があれば，Post-Quantum時代でも安全性が保たれることが期待できる．しかしながら，現在のところ，そのような暗号方式は実現されていない．ここで紹介する暗号方式はある意味でNP困難問題の緩和問題を利用した方式である．ここでいう緩和問題とは，NP困難問題の部分問題や，求めるべき解の条件を緩めた問題のことを指す．このような緩和問題は，単にNP困難性が証明されていないだけなのかもしれないし，もしかすると効率的に解かれるかもしれない問題でもある．

注意すべき事項として，NP困難性という概念は最悪時を考えた時間計算量評価であるという点がある．一方，暗号の安全性は平均時を考えて評価されるのが一般的であり，暗号の安全性の観点からはベースとなる問題は平均時でも難しいことが望まれる．後述するが，ある種の格子問題について任意の問題を解くことと平均的に問題を解くこととの等価性がAjtaiによって証明され，この事実は格子問題に基づいた暗号方式が有望であることを示唆している．

公開鍵暗号研究の初期段階に提案された方式で，量子計算を前提としても解読されていない方式として，ナップサック暗号方式と符号理論に基づく暗号方式がある．

これらの方式は格子問題に基づく方式のような利点はないものの，背景にあるアイディアは格子問題に基づく暗号方式と通じるものがあり，簡単な紹介をする．そして，近年になって提案されPost-Quantum時代でも有望そうな格子問題に基づく暗号方式を続いて紹介する．

＊ナップサック暗号

MerkleとHellmanによって考案された最初のナップサック暗号はNP困難問題の1つナップサック問題の部分問題を利用した方式である．さて，一般のナップサック問題とは次のような問題である．

入力：正整数 s と正整数のベクトル $a = (a_1,..., a_n)$.
出力：$s = \sum_{i=1}^{n} a_i b_i$ を満たす $b = (b_1,..., b_n)$,
ただし $b_i \in \{0, 1\}$ $(1 \leq i \leq n)$.

正整数ベクトルaはナップサックベクトルとも呼ばれ，ナップサック暗号の公開鍵に対応する．nビットの平文 $b = (b_1,..., b_n)$ に対して，暗号文cは $c = a_1b_1 + \ldots + a_nb_n$ のように計算される．暗号文cと公開鍵から平文bを求める問題は正にナップサック問題である．このままでは本当にNP困難問題を解かないと復号できないので，復号できるようにナップサックベクトルに条件を追加する必要がある．MerkleとHellmanは $a_i > \sum_{j=1}^{i-1} a_j$を満たす超増加数列の場合はナップサック問題が簡単に解けることに着目し，超増加数列に線形(モジュラー)変換をしたものを公開鍵とした．この線形性のため，Shamirにより，Merkle-Hellman型ナップサック暗号は解読されることになった．その後，ナップサック暗号は改良を繰り返したがBrickellやLagarias-Odlyzkoが考案した低密度攻撃という一般的攻撃手法により，解読されることとなった．最終的に生き残っているナップサック暗号はChorとRivest[2]によるもので，鍵生成に非線形性を取り入れるために，解くのが容易な特殊な離散対数問題を利用した方法である．

＊符号理論に基づく暗号

符号理論に基づく暗号方式を説明する前に簡単に符号理論について説明しよう．ノイズが混入する可能性がある通信路を介した二者間でkビット情報の交換するために，ノイズに対して頑強性を持たせるべく情報に冗長性を持たせn $(n > k)$ ビット情報を交換することを考える．この冗長性を持つ情報を(二元)符号語と呼ぶ．このように冗長性を持たせると誤り訂正が可能になる．たとえば，各符号語が互いに3bit以上異なっていることが分かっているのであれば，nビット情報のうち1bitだけ誤りがあっても元の符号語に戻せる．なお誤り訂正そのものは説明を省く．nビットの符号語wを，要素が0または1からなるn次元のベクトルであると見なそう．符号語（ベクトル）の任意の線形結合がまた符号語であるとき，その符号を(n, k)-線形符号であるという．0または1は$\mathbb{Z}_2$の要素であると考えることもでき，乗算や加算に対して2で割った余りを考えることにする．任意のkビットの情報を正しく伝達するには2^k個の符号語が必要になるが，k個の線形独立な符号語（ベクトル）$w_1,..., w_k$があれば任意の符号語は$w_1,..., w_k$の線形結合で表現されることが知られている．この$w_1,..., w_k$は線形符号の基底と呼ばれる．基底をなす各符号語（ベクトル）を行として並べた$k \times n$行列Gのことをその線形符号の生成行列と呼ぶ．このような設定のもとで，kビットの情報$m = (m_1,..., m_k)$ に対する符号語は $mG = m_1 w_1 + m_2 w_2 + ... + m_k w_k$のようにベクトルと行列の積として計算できる．符号の復号方法や符号の構成方法など，符号理論の詳細については文献5)を参照して欲しい．

さて，符号理論に基づく代表的な方式としてMcEliece暗号[8]を紹介しよう．いま，Gをtビットのエラーまで誤りが訂正可能な(n, k)-線形符号の生成行列とする．Sを逆行列が存在するような$k \times n$の行列とし，Pを$n \times n$の置換行列とする．置換行列Pとはすべての行とすべての列において要素1が現れているのはただ1つで他の要素はすべて0となっている行列のことで，n次元のベクトル $b = (b_1,..., b_n)$ に対してbPを計算すると$b_1,..., b_k$の現れる順番を並び替えたものが得られるという性質がある．McEliece暗号方式を以下に定めよう．

公開鍵：行列の積 $G' = SGP$.
秘密鍵：$\langle S, G, P\rangle$の3つ組.
暗号化：平文 $b = (b_1,..., b_k)$ はkビット．暗号文cは $c = bG' + e$として計算される．ただし，$e = (e_1,..., e_n)$はHamming重み（ビットが1となっている場所の数）がtのランダムなベクトルとする．
復号：暗号文 $c = (c_1,..., c_n)$ はnビット．$\boldsymbol{c}$にP^{-1}を施し，エラー訂正を行い，S^{-1}を施すことにより平文を得る．

置換行列がエラーの位置を替えるだけでノイズのHamming重みは変化しないという性質により上の方法で暗号文の復号が可能となっている．この暗号の安全性の背景には，一般の線形符号の最尤復号（エラーが混入している受信情報から距離の最も近い符号語を求める復号)がNP困難であるという事実がある．

＊格子問題に基づく暗号

格子問題に基づく暗号はナップサック暗号や符号理論に基づく暗号と比較して歴史は浅く，1996年にAjtaiと

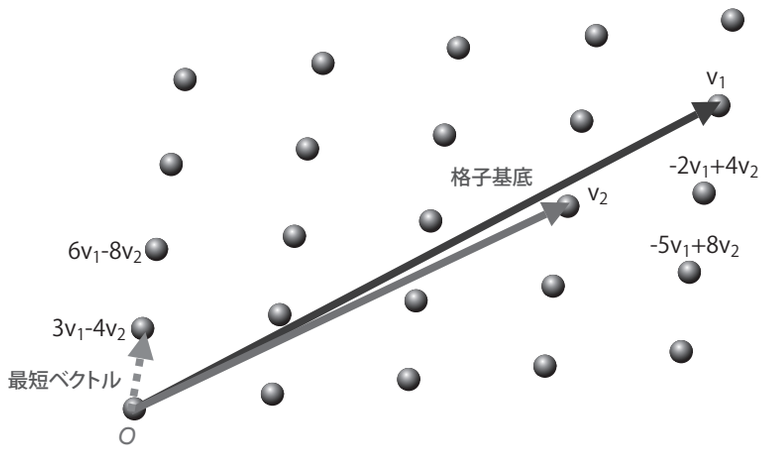

図 -3　最短ベクトル問題

Dwork[1] が格子問題に基づく公開鍵暗号を提案したのが最初である．新しく登場していることもあり，従来にはない性質があるのが特徴的である．前述したように，ベースとなる問題の平均時の難しさが最悪時の難しさに帰着できるという性質である．この性質は暗号の安全性の観点からすると好ましい性質であるが，従来方式では達成し得なかったものである．

暗号方式について説明する前に格子問題について触れることにする．まず，格子とは n 次元のベクトル $v_1, v_2, \ldots, v_m$ に対して整数係数で線形結合して得られるベクトル全体のことでそれを

$$L = L(v_1, v_2, \ldots, v_m) = \left\{ \sum_{i=1}^{m} a_i v_i \,|\, a_i \in \mathbb{Z} \right\}$$

で表すことにする．格子 L に対して，$(v_1, v_2, \ldots, v_m)$ は格子基底と呼ばれる．また，格子基底は一意的ではなく，1つの格子に対していくつもの格子基底があり得る．格子問題とは単独の問題を指すのではなく，格子に関連した問題の総称である．代表的な格子問題として最短ベクトル問題（Shortest Vector Problem）と最近ベクトル問題（Closest Vector Problem）がある．最短ベクトル問題とは，

入力：格子基底 $v_1, v_2, \ldots, v_m$,
出力：格子 $L(v_1, v_2, \ldots, v_m)$ に属する最短の非ゼロベクトル，

と定められる．問題の記述だけを見た場合，簡単そうに思えるかもしれないので，具体例な例を通してその難しさを考えてみよう．**図-3** は2次元の格子の例であり，その基底が v_1 と v_2 で与えられている．図-3を見れば，最短ベクトルを見つけられるだろう．しかし，問題は与えられた基底を利用して最短ベクトルを達成するような整数係数を求めることである．仮に v_1 と v_2 が直交しているならば，最短ベクトルは v_1 あるいは v_2 である．しかし，一般に与えられるベクトルは非直交であり，最短ベクトルを実現するベクトルの係数は1または0に限定されるわけではない．さらに，n 次元ベクトルの場合は n の指数的な組合せを考えないと最短ベクトルを実現する係数を見つけられそうにない．実際に，最短ベクトル問題はランダム帰着に関してNP困難であることが示されている（ここでランダム帰着とは，NP困難な問題のインスタンスから最短ベクトル問題のインスタンスを構成するのに乱数を利用することを指し，しかも変換された最短ベクトル問題に対する解に対して僅かに誤ることは許容するような特殊な帰着である．通常の意味でNP困難であるかどうかは未解決問題の1つである）．また，最短ベクトル問題はその緩和問題についての難しさについてもさまざまな角度から研究がなされている．ここでは，近似最短ベクトル問題と呼ばれる緩和問題を考えてみよう．近似率として $g(n)$ を導入し，最短ベクトルの大きさの高々 $g(n)$ 倍の範囲のベクトルを出力すればよい，と条件を緩和した問題を $g(n)$-近似最短ベクトル問題と呼ぶ．近似率として $g(n) = \sqrt{2} - \epsilon$ まで許容しても，ランダム帰着に関してNP困難であることが示されている．一方で，近似率 $g(n) = 2^{n/2}$ まで緩めると，近似最短ベクトル問題も多項式時間で解けることが知られている．最短ベクトル問題の異なるタイプの緩和問題としてユニーク最短ベクトル問題と呼ばれる部分問題がある．これは，最短ベクトルと（最短ベクトルとは非平行なベクトルで）次に短いベクトルとの比が一定以上開いていることが保証されている問題である．この比が $f(n)$ であるようなユニーク最短ベクトル問題を以下 $f(n)$-ユニーク最短ベクト

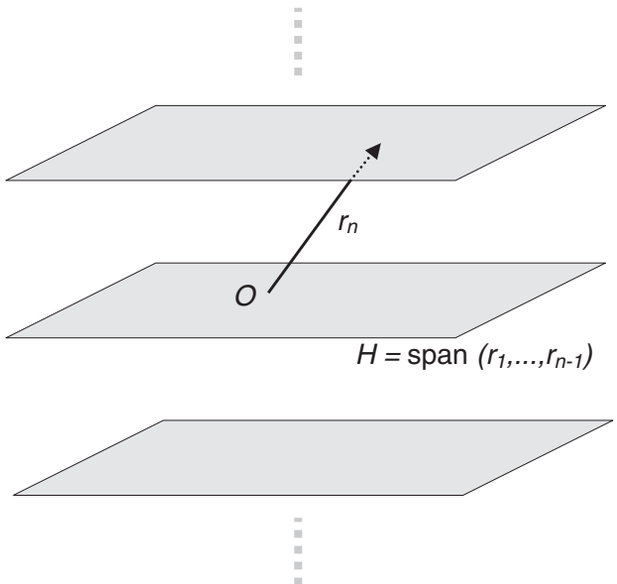

図 -4　Ajtai-Dwork 暗号が利用する格子構造

ル問題と呼ぶ．

次に，最近ベクトル問題を定義しよう．

入力：格子基底 $v_1, v_2,..., v_m$ とベクトル t.
出力：格子 $L(v_1, v_2,..., v_m)$ に属するベクトルで t と最も近いベクトル．

最近ベクトル問題も同様に難しい問題であることが知られており，実際に，通常の意味でNP困難であることが示されている．最短ベクトル問題と同様に近似問題が定義でき，近似率として $g(n) = n^{O(1/\log\log n)}$ まで許容してもNP困難であることが示されている．

Ajtai-Dwork暗号は n^8-ユニーク最短ベクトル問題が(確率的)多項式時間では解けないという仮定の下で強秘匿性(と呼ばれる一方向性よりも高い安全性)が保証されている方式であり，以下にその方式を示す．強秘匿性とは，ある暗号文が平文 m_1 か m_2 のいずれかであるということが分かっている状況で，どちらかであるかを有意に判定できないという性質である．

秘密鍵：ランダムな（線形独立）ベクトル $r_1,..., r_{n-1}$ とこれらの実数係数で線形結合されるベクトル全体 H（部分ベクトル空間あるいは超平面と呼ぶこともある）に対してある程度距離が離れたランダムなベクトル r_n.
公開鍵：格子 $L(r_1, r_2,..., r_n)$ に対するランダムな基底．
暗号化：0を暗号化する場合，ランダムに格子点を選び微小なランダムベクトルを印加する．1を暗号化する場合，ランダムな(格子点に限定しない)ベクトルを選ぶ．

復号：超平面 H と平行な超平面は周期的に現れるので，いずれかの超平面との距離を計算する．距離が小さければ0と復号し，そうでなければ1と復号する．

Ajtai-Dwork暗号の秘密鍵も公開鍵もある同一の格子の格子基底になっている．**図-4**はその基底がなす格子を模式的に表したものである．直観的なイメージを捉えるために3次元の場合の例で考えてみよう．ランダムなベクトルとして $r_1 = (2, 3, 0)$ と $r_2 = (3, 4, 0)$ が選ばれたとする．このとき，H は原点を通り z 軸に直交する平面になる（実際には秘密の平面 H の中に格子点が埋まっていることになる）．また H に十分に離れているランダムベクトルとして $r_3 = (1, 1, 10)$ が選ばれたとする．このとき，格子は $L(r_1, r_2, r_3) = \{(i, j, 10k) \mid i, j, k \in \mathbb{Z}\}$ となり，秘密鍵は L の格子基底 (r_1, r_2, r_3) である．秘密の平面 H に水平な格子中の平面はある程度の距離（この例の場合は10）を保って等間隔で現れているという構造になっているが，それが分かるのは秘密鍵を知っている人だけ，という仕組みである．暗号文は，空間全体に一様分布する(格子点とは限らない)ベクトルか，秘密の超平面の周り(正確には格子点の周り)に偏在するベクトルのいずれかである．0の暗号文は，ランダムな格子点を選び微小なランダムベクトルを加えたものなので，たとえば，ランダムな格子点として $(19, 18, 20)$ が選ばれたとし，微小なベクトルとして $(1, 0, 1)$ が選ばれたとすると，暗号文は $c_0 = (20, 18, 21)$ となる．1の暗号文はランダムなベクトルなので，たとえば，$c_1 = (38, 29, 16)$ などがその例である．さて，c_0, c_1 のような暗号文を復号するには，暗号文が秘密鍵から得られる(超)平面の列の近傍にあるか否かを決定すればよい．例ではこの平面は $z = 0, 10, 20,...$ と距離10で等間隔に並んでいるので，暗号文と最も近い平面との距離を求める．c_0 と最も近い平面との距離は1であり，c_1 と最も近い平面との距離は4である．復号において，0と1の暗号文を峻別する閾値を1.5と設定すると，c_0 は0に c_1 は1に正しく復元されることになる．格子点の様子を図示することで H の構造が容易に分かると思われるかもしれないが，図示という作業は n の指数時間的な作業であり，多項式時間内で図示できるのは格子のほんの一部分に過ぎないことを理解する必要がある．さて，Ajtai-Dwork暗号は，本質的に復号時にエラーが発生する可能性がある．つまり，1を暗号化するときにたまたま格子点の近くのベクトルを選んでしまう可能性のことである．この例における設定ではエラーが発生する確率は30% $(=1.5 \times 2/10)$ となる．このエラーに対してはGoldreich, Goldwasser, Haleviが解決法を与えている．

Ajtai-Dwork暗号とはまったく異なる方法に基づいて，1997年にGoldreich, Goldwasser およびHalevi[3] が格子問

題を利用した公開鍵暗号を提案している．最近ベクトル問題は，与えられた基底が直交(に近い)基底であれば簡単に解ける．一方，そうでない場合は，最近ベクトル問題は難しくなるという性質がある．つまり，公開鍵に最近ベクトル問題が難しいような基底を利用し，秘密鍵に最近ベクトル問題が容易に解ける基底を利用するというアイディアである．

秘密鍵：n個のn次元ベクトル$r_1, r_2, ..., r_n$．各r_iはi番目の要素がkでそれ以外の要素が0であるようなベクトルに対して，ランダムな（各要素の絶対値はkと比較して非常に小さい)ベクトルを足したもの．
公開鍵：格子$L(r_1, r_2, ..., r_n)$のランダムな基底$b_1, b_2, ..., b_n$.
暗号化：平文は整数ベクトル$m = (m_1, m_2, ..., m_n)$，暗号文を表すベクトルcは$c = \sum_{i=1}^{n} m_i r_i + e$として計算される，ただし$e$はランダムな微小ベクトル．

復号はBabaiによる最近ベクトル問題近似アルゴリズムを利用して実現されているが，ここでは割愛する．Goldreich-Goldwasser-Halevi暗号は，符号理論に基づく暗号方式の延長線上にあると見ることもできる．というのも，符号理論に基づく暗号方式の章で述べた最尤復号とは，格子問題の文脈では最近ベクトル問題に対応しているからである．Goldreich-Goldwasser-Halevi暗号は，Ajtai-Dwork暗号のような安全性証明は与えられていない従来型の暗号方式である．

対応ついでに付記するならば，ナップサック暗号の解読は最短ベクトル問題の文脈で議論することもできる．低密度攻撃では，ナップサック暗号を解読するのにナップサックベクトルを格子基底に帰着させ，最短ベクトル問題を解くアルゴリズムを呼び出すことにより解読に結び付けている．この議論は一見無意味に思えるかもしれないが，帰着される格子基底は特殊な形をしているため Lenstra-Lenstra-Lovászによる（多項式時間で動作する）格子基底縮約アルゴリズム（通称，LLLアルゴリズム）が最短ベクトル問題を解くアルゴリズムとして機能するのである．LLLアルゴリズムは格子基底を入力とし，与えられた格子基底が定義する格子の基底の中でなるべく直交に近い基底を求めようとするアルゴリズムである．直交基底に近い基底が求められれば最短ベクトルが計算でき，帰着の性質によりナップサック暗号の解読に繋がるのである．

さて，話を格子問題ベースの暗号方式に戻そう．Ajtai-Dwork暗号やGoldreich-Goldwasser-Halevi暗号にはさまざまな拡張（たとえば，Cai-Cusick暗号やMicciancio暗号）がある．特筆すべきは2003年にRegev[12]による$n^{1.5}$-ユニーク最短ベクトル問題をベースにした公開鍵暗号方式の提案であろう．Ajtai-Dwork暗号の延長線上にあり，Ajtai-Dwork暗号と同様にベース問題の最悪時の難しさに安全性の根拠を置くことに成功している．暗号化の方針もAjtai-Dwork暗号と類似しているが，技術的な違いは周期的ガウス分布と一様分布の識別問題を考えている点である．ガウス分布のピークがAjtai-Dwork暗号の超平面に対応しており，ピーク間の距離が超平面間の距離に対応している．このような分布の導入により格子理論（特に双対格子の性質やいわゆるTransference Theorem）との融合に成功し，より難しい問題への帰着を構成している．さらに，Regev[13]は2005年に，同様なアイディアを発展させて別の暗号方式を提案している．新しい方式では，ユニーク最短ベクトル問題ではなく，近似最短ベクトル問題に基づいている点と安全性証明に(だけ)量子計算を利用している点が特徴である．前述したように近似最短ベクトル問題は近似率によってNP困難問題から多項式時間で解ける問題まで定量的に変化させることができる．2005年のRegev暗号方式が利用している近似最短ベクトル問題はNP困難であることは示されていないものの，その安全性を定量的に設定できるNP困難問題の緩和問題に初めて関係付けることに成功したことは大きな意義を持つといえよう．

上で述べた暗号方式は理論的な側面が強いが，格子問題に基づく暗号方式に分類できる暗号で（高速実装が可能なため）実用的な側面が強い方式としてNTRUと呼ばれる暗号方式がある．Hoffstein, Pipher, Silverman[4]によって考案されたNTRUは多項式環($R = \mathbb{Z}[X]/(X^n-1)$，つまり，係数が$\mathbb{Z}$(整数)であるような$X$についての多項式を$X_n-1$で割った余り全体）上の演算で暗号化が可能であり，NTRU暗号の推奨設定ではRSA暗号等の実用的な方式と比較しても桁違いに高速である．そのため，公開鍵暗号の利用形態を変化させる可能性を秘めている方式でもある．また，多項式環の積として通常の多項式の積ではなく畳込み積と呼ばれる積を利用している点が特徴の1つでもある．多項式$f = \sum_{i=0}^{n-1} a_i x^i$と$g = \sum_{i=0}^{n-1} b_i x^i$において畳込み積は$fg = \sum_{i=0}^{n-1} (\sum_{j=0}^{i} a_j b_{i-j} + \sum_{j=i+1}^{n-1} a_j b_{n+i-j})\, x^i$と定義されるものである．

秘密鍵：小さな係数(−1, 0, 1など)の多項式$f, g \in R$，ただし，fはmod pとmod qで畳込み積に関して逆元を持つようにする．つまり，F_pとF_qが存在して，$F_p f \equiv 1 \bmod p$かつ$F_q f \equiv 1 \bmod q$となる．ここで，多項式についてmod qの演算は各係数に対して適用されるものとする．
公開鍵：互いに素な整数pとq，ただし，pは非常に小

さな数(たとえば3)．多項式 $h = F_q g \bmod q$.

暗号化：平文は小さな係数の多項式m．多項式で表される暗号文cは$c = m + hr \bmod q$と計算される．ただし，rはpの小さな倍数が係数のランダムな多項式.

復号：暗号文cに対して，$a = fc \bmod q$を計算し，$F_p a \bmod p$を計算することにより，平文を得る．

復号できる理由は $a \equiv rg + fm \bmod q$において $rg \equiv 0 \bmod p$であり，$a \equiv fm \bmod p$となるからで，逆元F_pを乗じることにより復号ができる．NTRU暗号は格子問題の文脈で定義できることも知られており格子問題を利用した暗号に分類されるが，演算として畳込み積を利用しているため，通常の格子暗号とは趣が異なり未解明な部分が大きい.

格子問題についてのその他の暗号学的性質については文献10)を参照して欲しい.

量子計算を積極的に

前章では，Post-Quantum時代でも「生き残る」あるいは「有望な」暗号方式で，現在の技術での利用可能な方式について紹介した．Shorの量子アルゴリズムは Post-Quantum時代におけるRSA暗号の可能性を否定することになったが，敵対者が量子コンピュータを使えるという状況では，誰しもが量子コンピュータを利用できるとするのが自然であろう．量子コンピュータであれ通常のコンピュータであれ，コンピュータ技術を悪用できるなら，また，それを防御する手段としてもコンピュータ技術を活用できる．このことを実証するためにも，量子コンピュータを積極的に活用して，Post-Quantum時代の公開鍵基盤の基礎となり得る技術について紹介したいと思う．量子計算に深くかかわる事柄はここでは紹介しないが，量子計算に興味がある方は文献11）を参照して欲しい.

Post-Quantum時代でも解読されないことを目的とし，量子コンピュータの能力を積極的に利用して安全性を高めた方式として2000年に岡本・田中・内山[9]によって最初の量子公開鍵暗号が発表された．彼らの方式はChor-Rivest型ナップサック暗号の延長線上に位置付けられる．Chor-Rivest型ナップサック暗号では，解くのが容易な離散対数問題を利用していたが，量子コンピュータが利用できるという前提の下では，「解くのが容易な」特殊ケースを考えるまでもなく一般の離散対数問題が効率的に解けるのである．Chor-Rivest型ナップサック暗号では，鍵生成の際の非線形性を高める手段として離散対数問題を導入したが，量子コンピュータがこの非線形性をより高めることに貢献しているのである.

さらに，2005年には，河内・小柴・西村・山上[7]によって，従来方式とは異なる量子公開鍵暗号方式が発表された．岡本・田中・内山暗号では，量子コンピュータを活用するのは鍵生成についてであったが，河内・小柴・西村・山上暗号ではより積極的に量子コンピュータを活用する方式である．鍵生成のみならず，暗号化や復号および通信路のすべてに量子メカニズムを前提とした方式となっている．より積極的に量子コンピュータを活用することで，Ajtai-Dwork暗号のようにベース問題の最悪時の難しさと平均時の難しさの間に帰着が存在することを示している．また，ベースとしている問題はグラフ自己同型性判定問題と呼ばれる問題で，従来の暗号方式では利用し得なかった問題である．利用されて来なかった理由の1つは，グラフ自己同型性判定問題が本質的に非可換でもある対称群上の問題とリンクしており暗号方式に組み入れるのが容易でなかったからであろう．もう1つの理由は他の暗号の安全性根拠としている問題と比較してグラフ自己同型性判定問題自身が難しい問題であり，それ以上に解読が難しくなるような暗号方式を設計することは容易でなかったからであろう．従来のコンピュータでは解くのが容易でなかった素因数分解は量子コンピュータ技術を用いることで解けるようになったが，河内・小柴・西村・山上暗号における従来にない性質も量子コンピュータ技術を積極的に利用することで達成されたものである．さて，河内・小柴・西村・山上暗号でベースとなっているグラフ自己同型性判定問題について紹介しよう.

入力：グラフG,

出力：恒等置換以外のGの自己同型置換が存在するか否か？

で定められる問題である．グラフの頂点のラベルに適当な置換を施した後，元のグラフと一致するように並び替えできるか否かを判定する問題である．**図-5**に挙げたグラフは1と5，2と6，3と4を入れ替える置換が自己同型置換となる例である．河内・小柴・西村・山上暗号はグラフ自己同型判定性が量子計算を利用したとしても効率的に解けないという仮定の下で強秘匿性が保証された方式である．暗号方式については，量子計算の知識が必要になるので詳細には説明できないが，その暗号文がどのようなものかを見てみよう．今，グラフGに恒等置換以外の唯一の自己同型置換πが存在するとしよう（この仮定は一般性を失わない仮定であるが詳細は技術的なので割愛する）．また，ランダムに選んだ置換をρとする．各置換に対して基底を構成するベクトルに1対1に対応付けることが可能で，置換ρに対応するベクトルを

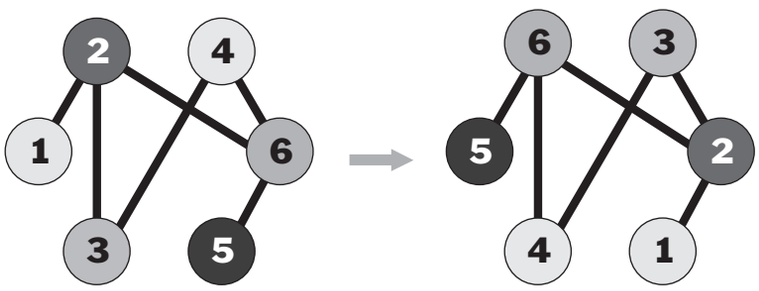

図 -5　非自明な自己同型置換を持つグラフの例

$\bar{\rho}$と表記する．このとき，0の暗号文は量子重ね合わせ状態 $\bar{\rho}+\overline{\rho\circ\pi}$であり，1の暗号文は量子重ね合わせ状態 $\bar{\rho}-\overline{\rho\circ\pi}$である．秘密鍵の$\pi$を知っていると暗号文が復号できるように設計されているが，暗号文である量子状態を単純に観測すると0の暗号文であれ1の暗号文であれランダムな置換が1つ等確率で取り出せるだけで解読には結びつかないようになっている．

Post-Quantum時代の公開鍵基盤の基礎となる技術を目指して，量子コンピュータを積極的に活用している具体的な方式を2つ紹介したが，量子計算を考慮した暗号理論に関してはまだ発展途上にある．現在の暗号技術は情報理論や統計推定などとも関連しているが，量子計算を考慮した暗号技術の場合，量子情報理論や量子統計推定などと関係してくるはずである．これらの研究領域も発展途上にあるが，研究の発展に伴って Post-Quantum 時代に活用できる基礎技術も開発されることであろう．

おわりに

量子計算機を利用するShorの素因数分解アルゴリズムが発見され約10年が過ぎている．「量子コンピュータはどうせ実現できない」と高を括るのは簡単であるが，それは科学的姿勢とは相容れない考えである気がする．ことは社会基盤の問題であり不測の事態に備える必要があるのは当然ではなかろうか．本稿を通じて見てきたように，幸いにも公開鍵暗号は素因数分解問題や離散対数問題に基づくものがすべてではなく現在技術でも動作可能な方式は存在している．とりわけ格子問題に基づいた暗号方式はPost-Quantum時代でも有望そうである．また，Post-Quantum時代では安全性を守る手段としても量子コンピュータが利用でき，積極的に量子コンピュータを利用した具体的な方式についても紹介した．「量子コンピュータが実現してしまった時代に暗号技術はいかにあるべきか?」を考えるきっかけになってもらえれば筆者としても嬉しい限りである．このような問題意識は広がりつつあるようで，2006年にはPost-Quantum Cryptographyに関する国際ワークショップが開催される予定である．これを機に研究が進展し，いつPost-Quantumの時代になっても対応できるような基盤が整備されることを期待したい．

参考文献

1）Ajtai, M. and Dwork, C. : A Public-key Cryptosystem with Worst-case/average-case Equivalence, Proc. STOC 1997, pp.284-293 (1997).
2）Chor, B. and Rivest, R. L. : A Knapsack Type Public Key Cryptosystem based on Arithmetic in Finite Fields, IEEE Trans. Information Theory, Vol.34, No.5, pp.901-909 (1988).
3）Goldreich, O., Goldwasser, S. and Halevi, S. : Public-key Cryptosystems from Lattice Reduction Problems, Proc. CRYPTO 1997, pp.112-131 (1997).
4）Hoffstein, J., Pipher, J. and Silverman, J. H. : NTRU : A Ring-based Public Key Cryptosystem, Proc. ANTS 1998, pp.267-288 (1998).
5）今井秀樹: 符号理論, 電子情報通信学会 (1990).
6）今井　浩, 富田章久, 小林弘忠 : 量子暗号, 情報セキュリティハンドブック, 2編8章, オーム社, pp.123-137 (2004).
7）Kawachi, A., Koshiba, T., Nishimura, H. and Yamakami, T. : Computational Indistinguishability between Quantum States and its Cryptographic Application, Proc. EUROCRYPT 2005, pp.268-284 (2005).
8）McEliece, R. J. : A Public-key Cryptosystem based on Algebraic Coding Theory, The Deep Space Network Progress Report 42-44, Jet Propulsion Laboratory, pp.114-116 (1978).
9）Okamoto, T., Tanaka, K. and Uchiyama, S. : Quantum Public-key Cryptosystems, Proc. CRYPTO 2000, pp.147-165 (2000).
10）Micciancio, D. and Goldwasser, S.: Complexity of Lattice Problems : A Cryptographic Perspective, Kluwer (2002).
11）Nielsen, M. A. and Chuang, I. L. : Quantum Computation and Quantum Information, Cambridge University Press (2000).
12）Regev, O. : New Lattice-based Cryptographic Constructions, J. ACM, Vol.51, No.6, pp.899-942 (2004).
13）Regev, O. : On Lattices, Learning with Errors, Random Linear Codes, and Cryptography, Proc. STOC 2005, pp.84-93 (2005).

（平成18年1月12日受付）