解説

量子計算機に対する暗号の安全性解析

Cryptanalysis on Quantum Computers

國廣　昇

Abstract

量子チューリング機械の下では，Shor のアルゴリズムにより，素因数分解や離散対数問題などの古典計算機では困難であると信じられている問題を多項式時間で解くことが可能である．これにより，大規模で雑音の小さい量子計算機が実現すると，RSA 暗号やだ円曲線暗号などの現在広く利用されている公開鍵暗号が破られることになる．そのため，世界各国で，量子計算機に対しても耐性を持つ耐量子計算機暗号の研究が活発に行われている．更に，Simon のアルゴリズムにより，幾つかの共通鍵暗号における利用モードが破られることも知られている．本稿では，量子計算機による暗号の安全性，特に，共通鍵暗号，公開鍵暗号の両方に対する安全性評価に関して知られている結果を紹介する．

キーワード：量子計算機，安全性評価，Shor のアルゴリズム，Simon のアルゴリズム

1．はじめに：量子計算と暗号

現代暗号は，共通鍵暗号と公開鍵暗号に大別されるが，量子計算機のこの二つの暗号系に対する安全性に関して，その基礎的な結果について説明する(注1)．特に，共通鍵暗号に対する攻撃は，近年，著しく発展しており，その説明も加える．

まず，量子計算による暗号の安全性解析に関して，簡単にその歴史を紹介する．1985 年の Deutsch による量子チューリング機械の提案から歴史は始まる．1994 年に，Simon のアルゴリズム（周期関数の位数発見）[3]，Shor のアルゴリズム（素因数分解，離散対数問題）[4]が提案された．Shor のアルゴリズムは，隠れた位数を発見するアルゴリズムであるが，このアルゴリズムにより，素因数分解，（だ円）離散対数問題を解くことが（量子）多項式時間で可能である．更に，理論的な整備により，可換群上での隠れ部分群問題にまで拡張されている．

研究の別の流れとして，1996 年に Grover によりデータベース探索問題に対する量子アルゴリズム[5]が提案されている．Grover のアルゴリズムは，共通鍵暗号の秘密鍵探索に自明な形で適用可能である．更に，ハッシュ関数の衝突発見にも応用されている．共通鍵，ハッシュ関数の内部構造が一切使えない状況においては，解読の高速化が可能である．

最近になり，Simon のアルゴリズムを適用することによる共通鍵暗号への攻撃も示されている[6],[7]．当初は，特定の暗号構成のみに有効な攻撃であったが，Grover のアルゴリズムと組み合わせることにより，幅広い暗号利用モードに適用可能である[8]．

1.1　量子計算機と暗号を取り巻く環境の変化

素因数分解問題は，広く利用される RSA 暗号の安全性の根拠となる問題である．量子計算機により多項式時間で実行できるという報告は，極めて大きいインパクトをもって受け入れられた．しかし，当時は，実際に動く量子計算機は存在せず，理論的なインパクトの大きさに反して，暗号研究者の中では，それほど重要視されていなかった．

近年になり，様々な要因により，再び，量子計算と暗号の関係は注目されている．一つ目の要因は，NIST による耐量子計算機暗号の募集である．二つ目の要因は，

國廣　昇　正員：シニア会員　筑波大学システム情報系情報工学域
E-mail　kunihiro@cs.tsukuba.ac.jp
Noboru KUNIHIRO, Senior Member (Faculty of Engineering, Information and Systems, University of Tsukuba, Tsukuba-shi, 305-8573 Japan).
電子情報通信学会誌　Vol.105 No.6 pp.516-521 2022 年 6 月

（注 1）　本稿の技術的詳細は，二つの CRYPTREC 外部評価報告書（「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」[1]，CRYPTREC 外部評価報告書「Shor のアルゴリズム実装動向調査」[2]）を参照されたい．共に，最近の話題も含めて詳しく説明がなされている．

Noisy Intermediate-Scale Quantum（NISQ）計算機の開発が進みつつあることである．小さいながらも，実際の量子計算機が登場しつつあり，IBM は 2021 年 11 月に 127 量子ビットを持つ量子計算機を実現したことを公表している．また，IBM が公表しているロードマップ(9)によれば，2023 年中には，1,121 量子ビットを持つ量子計算機を開発する予定である．2021 年現在では，量子雑音が大きいため，暗号の解読に用いるのには不十分であるが，以前の状況から比較すると格段の進歩を遂げている．

1.2　考慮する量子攻撃モデル

量子計算機自身の詳しい説明は，多くの優れた解説があるため省略する．暗号の安全性解析を議論する上で，考慮すべき攻撃モデルを説明する．

暗号の安全性を考える上で，二つの攻撃モデル：Q1 モデル，Q2 モデルを考える．Q1，Q2 モデルは共に，量子計算機を使う．違いは，Q1 モデルでは古典オラクルのみを用いるのに対して，Q2 モデルは，重ね合わせに対して，量子問合せが可能である点にある．Q2 モデルでは攻撃者が設定した関数 f に対して，

$$\sum\alpha_i|x_i\rangle|y_i\rangle \mapsto \sum\alpha_i|x_i\rangle|y_i \oplus f(x_i)\rangle$$

という状態遷移を 1 ステップで実行する量子オラクルを用いることが可能である．

公開鍵暗号への攻撃，特に，素因数分解や離散対数問題を解く際には，Q1 モデルでの攻撃環境を考える．つまり，量子計算機は利用するものの，量子オラクルは利用しない．その一方で，共通鍵暗号に対する攻撃では，主に Q2 モデルでの攻撃環境を考えている．量子計算機を用いるだけでなく，量子オラクルを利用するため，量子オラクルが想定できない状況では多くの攻撃は有効でないことに注意されたい．

2. 共通鍵暗号の安全性評価

この章では，Grover のアルゴリズムを用いた攻撃，Simon のアルゴリズムを用いた攻撃，更に，この二つを組み合わせた攻撃を説明する．本章の技術的詳細は，文献（1）に詳しい．

2.1　Grover のアルゴリズムによる共通鍵暗号系の攻撃

2.1.1　Grover のアルゴリズム

Grover のアルゴリズムは，データベース探索問題を解くアルゴリズムである．この問題は，次のように定義される．

［定義 1］（データベース探索問題）　関数 $f:\{0,1\}^n \to \{0,1\}$ を考える．$f(x)=1$ となる x がただ一つ存在するとする．f が量子オラクルとして与えられたとき，$f(x)=1$ を満たす x を求めよ．

この問題を一般化して，解が t 個ある場合も考えることができる．つまり，$f(x)=1$ を満たす x が t 個存在するときに，$f(x)=1$ を満たす x を一つ求める問題である．古典計算機では，$\Omega(2^n/t)$ 回の古典クエリが必要であるが，量子計算機の場合，量子クエリ回数はこの平方根の $O(\sqrt{2^n/t})$ 回で十分である．

2.1.2　Grover のアルゴリズムによるブロック暗号への攻撃

送信者と受信者の間で鍵 K を共有しており，平文 m を送信したいとする．暗号化処理を $C=E(K;m)$ と書くことにする．受信者は，暗号文 C を受け取り，$m=D(K;C)$ により平文の復元を行う．攻撃者の目標は，平文と暗号文の組を幾つか保持している状況下で，鍵 K を復元することとする．

ターゲットとする暗号が理想的な暗号であれば，攻撃者は，総当り攻撃，つまり，鍵集合 $\mathcal{K}$ から鍵候補 $K \in \mathcal{K}$ を選び，全ての平文と暗号文の組に対して，$C=E(K;m)$ が成り立つかを確認し，成り立てば正しい鍵であると判定する攻撃が最良である．鍵長が k ビットであれば，平均 2^{k-1} 回の試行により攻撃が成功する．古典計算機を用いる限りにおいては，これより小さくすることはできない．

Grover のアルゴリズムを用いた攻撃を紹介する．鍵が k ビットで，ブロックサイズが n のブロック暗号を考える．$l=\lceil k/n \rceil$ として，平文と暗号文 $C=E(K;M)$ の l 個の組 $(M_1, C_1), \cdots, (M_l, C_l)$ を集める．$k \leq n$ の状況では，$l=1$ で十分である．関数 $f:\{0,1\}^k \to \{0,1\}$ を，「全ての $1 \leq i \leq l$ について $C_i=E(X;M_i)$ が成り立つときのみに限り，$f(X)=1$」と定める．正しい鍵を K とすると，$f(K)=1$ となる．また，暗号が十分によく設計されていれば，$X \neq K$ のとき，$f(X)=0$ となる．Grover のアルゴリズムを素朴に適用することにより，共通鍵 K を時間 $O(2^{k/2})$ で探索可能である．

2.1.3　ハッシュ関数への攻撃

ハッシュ関数 h の衝突を求める問題を考える．ハッシュ関数の衝突とは，$h(x)=h(x')$ を満たす (x, x')（ただし，$x \neq x'$）の組である．ハッシュ関数の出力が n ビットであるとすると，誕生日のパラドックスから，古典計算機を用いた場合，$O(2^{n/2})$ 回のオラクル呼出しが必要であり，計算時間も $O(2^{n/2})$ となる．

Grover のアルゴリズムを用いたハッシュの衝突探索アルゴリズムを説明する（以下，BHT アルゴリズムと呼ぶ(10)）．このアルゴリズムは，$O(2^{n/3})$ 回の量子オラクル呼出しでハッシュの衝突を発見することが可能であ

る．古典的には $O(2^{n/2})$ 回であることに注意されたい．
BHT アルゴリズムの概略は以下で記述される．

ステップ 1：部分集合 $S\subset\{0,1\}^n$ を選ぶ．ここで，$|S|=2^{n/3}$ とする．全ての $x\in S$ について，$h(x)$ を計算し，$(x,h(x))$ をリスト L に格納する．
ステップ 2：$x'\in\{0,1\}^n S$ と $x\in S$ の組であって，$h(x')=h(x)$ となるものをリスト L を利用し，Grover のアルゴリズムを用いて探索する．
ステップ 3：(x,x') を出力する．

ステップ 1 での h へのクエリ回数は，$O(|S|)$ であり，ステップ 2 での h へのクエリ回数は，$O(\sqrt{2^n/|S|})$ であるため，合計のクエリ回数は $O(|S|+\sqrt{2^n/|S|})$ となる．この値は $|S|=2^{n/3}$ のとき最小となり，このときのクエリ回数は $O(2^{n/3})$ となる．また，量子メモリは，$O(2^{n/3})$ 必要である．h への必要なクエリ回数は，$\Omega(2^{n/3})$ であることが知られているため，h へのクエリ回数という観点では，BHT アルゴリズムが最適である．
BHT アルゴリズムでは，$O(2^{n/3})$ 個の量子メモリが必要である．量子メモリは実質的に量子ビットであり，大量の量子ビットが使える状況は将来にわたっても期待できない．そのため，クエリ回数は増えるものの，必要となる量子メモリが少ないアルゴリズムが提案されている[11]．このアルゴリズムは，クエリ回数は $O(2^{2n/5})$ となり，回数は増加するものの，量子メモリは多項式で収まる．ただし，古典メモリは $O(2^{n/5})$ であり，依然，指数関数個の目盛が必要である．

2.2 Simon のアルゴリズムによる共通鍵暗号に対する攻撃

2.2.1 Simon のアルゴリズム

次の問題を考える．
［定義 2］以下の条件を満たす関数 $f:\{0,1\}^n\to\{0,1\}^n$ を考える．ある $\boldsymbol{r}\in\{0,1\}^n\backslash\{\boldsymbol{0}\}$ が存在して，全ての $\boldsymbol{x}\in\{0,1\}^n$ に対して，$f(\boldsymbol{x}\oplus\boldsymbol{r})=f(\boldsymbol{x})$ が成り立つ．このとき，$\boldsymbol{r}\in\{0,1\}^n$ を求めよ．
表 1 に簡単な例を示す．この例では，$n=3$ で，解は $\boldsymbol{r}=101$ である．
Simon のアルゴリズムは以下で与えられる[3]．Q2 モデル下で動作し，ユニタリ変換 U_f を $U_f:|x\rangle\,|y\rangle\to|x\rangle\,|y\oplus f(x)\rangle$ とする．

ステップ 1：初期状態 $|0\rangle^{\otimes n}\,|0\rangle^{\otimes n}$ を用意する．
ステップ 2：前半の n-qubit に対して，アダマール変換を作用させる．

$$\to\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle^{\otimes n}$$

表 1　関数 f の例

x	000	001	010	011	100	101	110	111
$f(x)$	000	010	001	100	010	000	100	001

ステップ 3：U_f を作用させる．

$$\to\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle$$

ステップ 4：前半の n-qubit にアダマール変換を作用させる．

$$\to\frac{1}{2^n}\sum_{x\in\{0,1\}^n}\sum_{u\in\{0,1\}^n}(-1)^{x\cdot u}|u\rangle|f(x)\rangle$$

ステップ 5：最初の n-qubit を観測し，ベクトル $\boldsymbol{u}$ を得る．

観測により，$\boldsymbol{r}$ と直交するベクトル（つまり，$\boldsymbol{r}\cdot\boldsymbol{u}=0$ となるベクトル）が等確率で得られる．この手順を繰返し実行し，$\boldsymbol{r}$ と直交する線形独立なベクトルを $n-1$ 本求める．この繰返し回数は，$n\log n$ 程度で十分である．$n-1$ 本求めることができれば，簡単な線形代数の計算により $\boldsymbol{r}$ を得ることができる．全てのステップが多項式時間で完了するため，アルゴリズム全体として多項式時間である．

2.2.2 Simon のアルゴリズムの暗号解読への応用

ランダム置換を用いる以下の簡単な暗号を考える．K_1,K_2 は n ビットの鍵とし，ランダム置換 P を用いて，

$$E(K_1,K_2;M)=P(M\oplus K_1)\oplus K_2$$

により暗号化を行う．この構成は，Even-Mansour 構成として知られている．
Even-Mansour 構成に対する Simon のアルゴリズムを用いた攻撃を考える．

$$f(x)=E(K_1,K_2;x)\oplus P(x)$$

と定義する．このとき，$f(x\oplus K_1)=f(x)$ が成り立つため，Q2 モデルにおいて，多項式時間で K_1 の復元が可能である．更に，K_1 を求めることができれば，簡単に K_2 を復元することが可能である．
Kuwakado ら[6]の研究に続いて，Kaplan らは，Simon のアルゴリズムを適用することにより，幾つかの共通鍵暗号技術が破られることを示している[7]．

2.3 Grover meets Simon

Grover のアルゴリズムと Simon のアルゴリズムを融合させせることによる改良が提案されている．Even-Mansour 構成におけるランダム置換 P の代わりに，鍵長 k ビットで，n ビットブロック暗号 $F:\{0,1\}^k\times\{0,1\}^n\to\{0,1\}^n$ を考える．この構成は FX 構成と呼ばれる．FX 構成は，鍵長は合計 $k+2n$ ビットの n ビットブロック暗号である．今，暗号化関数 $E:\{0,1\}^{k+2n}\times\{0,1\}^n\to\{0,1\}^n$ は，$E(K_0,K_1,K_2;M)=F(K_0;M\oplus K_1)\oplus K_2$ により定義される．

FX 構成に対する量子攻撃が文献(8)で提案されている．この攻撃では，$O(2^{k/2})$ 回のオラクル呼出しにより攻撃に成功する．以下が，基本的なアイデアである．もし，鍵 K_0 が攻撃者にとって既知であれば，実質的に Even-Mansour 構成と同じになるため，Simon のアルゴリズムにより K_1,K_2 の復元は多項式時間で可能である．そのため，2^k 回の総当り探索を行えば，全ての鍵の復元が可能である．

上の戦略では，K_0 の探索を総当りにより行っている．ここで，K_0 の探索を，Grover のアルゴリズムで行うことにする．このとき，$O(2^{k/2})$ 回のオラクル呼出しにより解を求めることが可能となる．Grover アルゴリズムの内側で Simon アルゴリズムを走らせることがポイントとなる．自明な方法でこの二つを組み合わせることはできないが，観測に工夫を行うことにより融合を可能にしている．詳細は文献(8)を参照されたい．

3. 公開鍵暗号の安全性評価

この章では，公開鍵暗号の安全性評価，特に Shor のアルゴリズムによる素因数分解に対する評価について説明する．本章の技術的内容は，文献(2)，(12)，(13)を参考にしている．

3.1 位相推定問題，位相推定アルゴリズム

Shor のアルゴリズムの基礎となる位相推定問題とその問題を解くアルゴリズムを説明する．U をユニタリ変換とする．U の固有ベクトルの一つを $|\phi\rangle$ としたとき，ある実数 $0\le\phi<1$ が存在し，

$$U|\phi\rangle=\exp(2\pi i\phi)|\phi\rangle$$

を満たす．ここで，ユニタリ変換の固有値は，その絶対値が 1 であることに注意されたい．

［定義 3］（位相推定問題）U とその固有ベクトル $|\phi\rangle$ が与えられたときに，対応する固有値の位相 ϕ（の近似値）を求めよ．

この問題は，Shor の素因数分解アルゴリズムだけでなく，量子系のエネルギー計算などでも活躍する．

位相推定アルゴリズムは，次のように記述される．基本構成は，Simon のアルゴリズムと同一である．ここで，m を位相 ϕ の近似値の有効ビット数とする．

ステップ 1：初期状態 $|0\rangle^{\otimes m}|\phi\rangle$ を用意する．

ステップ 2：前半の m-qubit に対して，アダマール変換を施す．

$$\to\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|\phi\rangle$$

ステップ 3：ユニタリ変換 $|x\rangle|\phi\rangle\mapsto|x\rangle U^x|\phi\rangle$ を施す．

$$\to\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle U^x|\phi\rangle$$
$$\left(=\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}\exp(2\pi i\phi x)|x\rangle|\phi\rangle\right)$$

ステップ 4：前半の m-qubit に逆 QFT を施す．

$$\to\frac{1}{2^m}\sum_{j=0}^{2^m-1}\sum_{k=0}^{2^n-1}\exp\left(-\frac{2\pi k i}{2^m}(j-2^m\phi)\right)|j\rangle|\phi\rangle$$

ステップ 5：前半の m-qubit を観測し，m ビットの値を得る．

このアルゴリズムは高い確率で $\lfloor 2^m\phi\rceil$ を出力する．ϕ の近似値を m ビットの精度で得られたことになる．

位相推定アルゴリズムの $m=4$ の場合を図 1 に記す．ステップ 3 の演算は，$C-U, C-U^2, C-U^4, C-U^8$ などに分解できることに注意されたい．

3.2 素因数分解アルゴリズム

Shor による素因数分解アルゴリズムは，量子パートと古典パートに大別される．量子パートの目的は，ターゲット合成数 N，N と互いに素な自然数 a に対して，$a^r \bmod N=1$ となる正整数 r を求めることである(注2)．この r は位数と呼ばれる．

古典パートでは，量子パートで求めた r を利用し，N の因数を見つける．素因数分解に失敗した場合は，a の値を変え，量子パートに戻る．

r を求める問題を位相推定問題と関連付け，位相推定アルゴリズムを利用することにより r を求める．ユニタリ変換 U として，$U|y\rangle=|ay \bmod N\rangle$ を考える．このとき，U の固有値は，$j=0,1,2,\cdots,r-1$ に対して，$\exp(2\pi ij/r)$ で与えられ，対応する固有ベクトルは，

(注 2) 実際は，観測値から r を求める際に，古典計算を行っている．

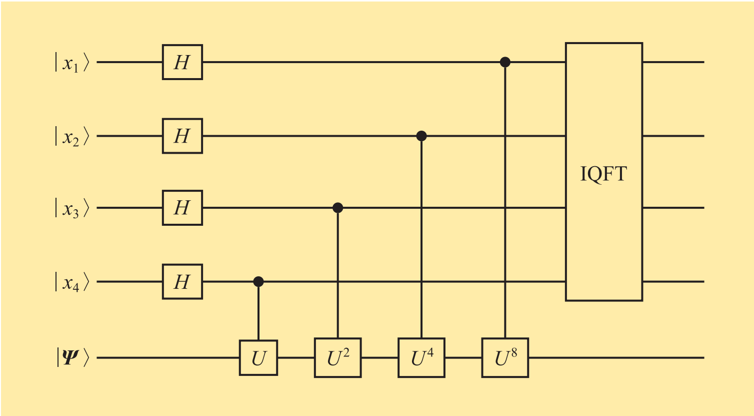

図1　位相推定回路（$m=4$ の場合）

$$|w_j\rangle=\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp(-2\pi kj\mathrm{i}/r)|a^k \bmod N\rangle \qquad (1)$$

であることが知られている．位相推定アルゴリズムを用いることにより，j/r を m ビットの精度で求めることができる．更に，j/r の近似値から，連分数展開を用いることにより r を求めることが可能である．この際，$m=2n+1$ とすれば十分である．

位相推定問題を適用する際には，固有ベクトルを事前に用意する必要がある．式(1)には r が含まれているため，直接的に固有ベクトルを用意することはできないが，全ての固有ベクトルの和が $|1\rangle$ であるという性質を利用することにより，この問題は回避可能である．

Shor のアルゴリズムの回路構成を考える．ステップ4の量子フーリエ変換の構成法は，既によく知られており，ここでは考察しない．ステップ3はべき乗剰余計算であり，様々な構成法が提案されている．ここでは，多くの方式で基本となる考え方を紹介する．前述のように，ステップ3は，$C-U^{2^k}$ を実装すれば十分である．素朴な実装では 2^k 回 $C-U$ を適用しないといけない．しかし，素因数分解を行う状況では，U^{2^k} は，$U^{2^k}|x\rangle=|a^{2^k}x \bmod N\rangle$ と記述できることに着目すると，$A_k:=a^{2^k} \bmod N$ を古典的に計算し，乗算剰余 $|x\rangle\mapsto|A_k x \bmod N\rangle$ を行う回路を構成すれば十分である．

3.3 Shor のアルゴリズムの回路構成

3.3.1 リソース評価

素因数分解を行う際に，どの程度の量子計算機が必要となるかを議論する．ここでは，量子回路をゲートレベルで書き下すことにより，素因数分解を行うのに必要なリソース評価が行われている．

べき乗剰余計算は，制御乗算剰余計算により構成させる．乗算剰余計算の方法は幾つか提案されているが，最も素朴なものは加算を組み合わせる方法である．加算の構成は，古典での加算の適用（半加算器と桁上がり），量子加算などがある．量子加算は量子フーリエ変換を行い，周波数領域で加算を行うことにより，桁上がりに必要な量子ビットが不要である．回路のサイズ及び深さの増大を招くものの，少ない量子ビットで構成が可能である．

まず，量子誤りが全くないという理想的な環境を考える．素朴な方法では，$3n+2$ 量子ビット必要であり，必要な Toffoli ゲート数は $270n^3$ で見積もられる[12]．2,048 ビット合成数の場合では，6,146 量子ビット，3.04×10^{12} 個のゲートが必要となる．量子加算を用いた構成では，$2n+3$ 量子ビット必要[注3]であり，必要なゲート数は，$97n^4$ で見積もられる．量子誤りがある場合には，これより多くの量子ビット及び量子ゲートが必要である．実際に素因数分解を行うことを考えた場合，少なくともこの程度の量子ビットは最低限必要であり，量子計算機ハードウェア構成の一つの目標とみなすことができる．

表2　誤りがあるときのリソース評価

ビット長	Qubit 数	計算時間（h）	回路の深さ
1,024	8.05×10^6	3.58	6.4×10^{10}
2,048	8.56×10^6	28.63	51.5×10^{10}
4,096	11.2×10^6	229	412.2×10^{10}

表2は，誤りがあるときのリソース評価を示している[15]．この評価では，誤り率は 10^{-5} と仮定し，ゲート演算は，クロック周波数は 5 MHz（1 サイクルは 0.2 μs）としている．量子ビットは，二次元格子上で配置され，最近傍でのみ計算が可能であるとしている．誤り訂正は，表面符号を利用している．

文献(16)では，誤り率が 10^{-3} というより現実的な環境下での回路構成，評価を与えている．この論文中で

（注3）　量子ビットは，$2n+2$ まで削減されている[14]．

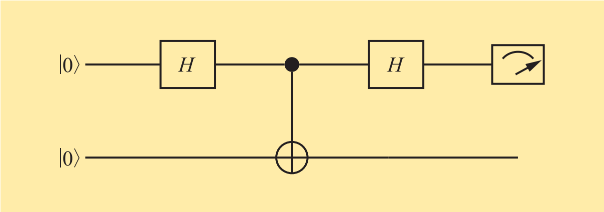

図2　Oversimplifying Quantum Factoring Circuit

は，20×10^6 量子ビットを用いて，2,048ビットの素因数分解が5.1時間で実行可能であると主張している．

3.3.2　実際の量子計算機を使った素因数分解

実際の量子計算機上での実験を紹介する．これまでに，15, 21の素因数分解実験が行われている．しかし，いずれの実験も，(i)ターゲットとなる合成数に特化している，若しくは，(ii)素因数が既知の下で，素因数分解を行っている．特に，素因数，若しくはそれと等価の情報を用いた場合，どのような大きい値を素因数分解を行ったとしても意味がない．詳細は，文献(13)を確認されたい．

具体例として，素因数と等価な情報を用いて素因数分解を行うことの問題点を指摘したOversimplifying quantum factoring[(17)]について説明する．特殊な a の値[(注4)]を用いれば，図2で示される簡単な量子回路で，どのような大きな合成数でも素因数分解ができることを示している．このような a を求めることと素因数分解は等価な問題であり，そのような特殊な a を用いれば，古典計算機でも瞬時に素因数分解が可能である．実際に，論文中では，2万ビットの素因数分解を示している．

4. ま　と　め

本稿では，量子計算機を用いた場合の共通鍵暗号及び公開鍵暗号の安全性に関する研究の紹介を行った．共通鍵暗号に対しては理論的進展が大きく，公開鍵暗号に対しては誤りを考慮した実装に関して進展が大きい．また，量子計算機にも耐性があると期待される耐量子計算機暗号も，古典計算機，量子計算機に対する安全性評価が進んでいる．多くの未解決な問題が残されており，更に多くの研究者の参画を期待する．

(注4)　$a\equiv1 \bmod p, a\equiv-1 \bmod q$ を満たす a．

文　　献

(1) 細山田光倫，“CRYPTREC外部評価報告書「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」.” https://www.cryptrec.go.jp/exreport/cryptrec-ex-2901-2019.pdf
(2) 高安　敦，“CRYPTREC外部評価報告書「Shorのアルゴリズム実装動向調査」.” https://www.cryptrec.go.jp/exreport/cryptrec-ex-3005-2020.pdf
(3) D.R. Simon, “On the power of quantum computation,” FOCS 1994, pp. 116-123, 1994.
(4) P.W. Shor, “Algorithms for quantum computation : Discrete logarithms and factoring,” FOCS 1994, pp. 124-134, 1994.
(5) L.K. Grover, “A fast quantum mechanical algorithm for database search,” STOC 1996, pp. 212-219, 1996.
(6) H. Kuwakado and M. Morii, “Security on the quantum-type Even-Mansour cipher,” Proc. ISITA 2012, pp. 312-316, 2012.
(7) M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, “Breaking symmetric cryptosytems using quantum period finding,” Proc. CRYPTO 2016, Lect. Notes Comput. Sci., vol. 9815, pp. 207-237, 2016.
(8) G. Leander and A. May, “Grover meets Simon-quantumly attacking the FX-construction,” Proc. ASIACRYPT 2017, Lect. Notes Comput. Sci., vol. 10625, pp. 161-178, 2017.
(9) IBM's roadmap for scaling quantum technology. https://research.ibm.com/blog/ibm-quantum-roadmap（2021年11月27日確認）
(10) G. Brassard, P. Høyer, and A. Tapp, “Quantum cryptanalysis of hash and claw-free functions,” SIGACT News, vol. 28 , no. 2, pp. 14-19, 1997.
(11) A. Chailloux, M. Naya-Plasencia, and A. Schrottenloher, “An efficient quantum collision search algorithm and implications on symmetric cryptography,” Proc. ASIACRYPT 2017, Lect. Notes Comput. Sci., vol. 10625, pp. 211-240, 2017.
(12) N. Kunihiro, “Exact analysis of computational time for factoring in quantum computers,” IEICE Trans. Fandamentals, vol. E88-A, no. 1 pp. 105-111, Jan. 2005.
(13) N. Kunihiro, “Quantum factoring algorithm : Resource estimation and survey of experiments,” Proc. MQC 2019, pp. 39-55, 2020.
(14) Y. Takahashi and N. Kunihiro, “A quantum circuit for Shor's factoring algorithm using 2n+2 qubits,” Quantum Information and Computation, vol. 6, no. 2, pp. 184-192, 2006.
(15) Quantum Computing : Progress and Prospects, 2019. https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects
(16) C. Gidney and M. Ekerå, “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits.” https://arxiv.org/abs/1905.09749
(17) J. Smolin, G. Smith, and A. Vargo, “Oversimplifying quantum factoring,” Nature, vol. 499, pp. 163-165, 2013.

（2021年12月28日受付）

國廣　昇（くにひろ　のぼる）（正員：シニア会員）
平6東大・工・計数卒．平8同大学院修士課程了．同年日本電信電話株式会社入社．電通大，東大に在籍の後，現在，筑波大システム情報系教授．博士（工学）．暗号理論，情報セキュリティ，量子計算の研究に従事．平21年度本会論文賞受賞．著書「代数学」「ほんとうに安全？現在の暗号」など．