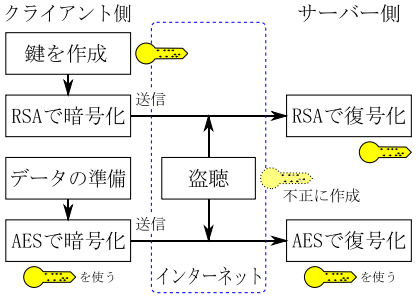
学籍番号		論文題目	スーパーひとし君のコード不思議発見 暗号と量子コンピュータ
氏名	犬飼 仁史		

1　暗号

暗号とは，情報を伝える人以外に内容を知られないように情報を変換する方法である．暗号にはいくつか種類があり，一般的によく利用されるのは RSA 暗号や AES 暗号である．これらには以下の特徴がある．RSA **暗号**は暗号化に必要な鍵を公開しても他者に内容が知られない公開鍵暗号であり，様々な人が使うインターネットと非常に相性が良い．ただし，変換が遅く，1 度に送れるデータ量は少量．AES **暗号**は情報を伝達し合う人同士が同じ鍵を知る必要がある共通鍵暗号であり，比較的近い場所で利用されることが多い．変換が早く，1 度に送れるデータが多い．この 2 つの暗号を用いることで，大量のデータを安全な形で通信することができている．

2　セキュア通信の流れ

RSA 暗号と AES 暗号を組み合わせて通信を行う．まず，AES 暗号に用いる鍵を RSA 暗号で送信して，サーバー側とクライアント側で鍵を共有する．その後，この鍵を用いて AES 暗号で暗号化し通信することで，大量のデータを安全に通信することが可能．しかし，攻撃者はインターネット上の通信を見ることができる可能性があるため，もし，通信を盗聴しデータを解析して不正に鍵が作成可能であれば，この通信方法は安全ではないこととなる．



3　RSA 暗号の安全性・仕組み

RSA 暗号は大きな素数を用いた暗号であり，2 つの大きな素数の積を素因数分解することは一般に難しいとされるため安全とされている．以下は RSA 暗号の仕組みである．

準備　素数 p，q，$(e, pq) = 1$ を満たす $0 \leq e < pq$ を選ぶ．$ed \equiv 1 \pmod{\phi(pq)}$ を満たす $0 \leq d < pq$ を計算する．

暗号化　$a \to a^e \mod pq$　　**復号化**　$A \to A^d \mod pq$

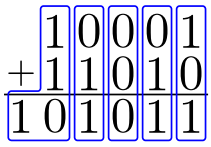
証明 オイラーの定理『$(a, N) = 1$ ならば，$a^{\phi(N)} \equiv 1 \pmod{N}$』を用いれば，$(a,\, pq) = 1$ のとき，

$$a^{ed} = a^{k\phi(pq)+1} = a \cdot a^{k\phi(pq)} \equiv a \pmod{pq}$$

が成り立つ．$(a,\, pq) \neq 1$ のときは簡単に証明できる．

4　演算量

アルゴリズムの性能を表すもの．数を 2 進数としたときの 1 桁同士の足算・引算を 1．すなわち，右の図の四角 1 つの計算を 1 としたときの全体の計算回数を演算量という．この演算量はビッグ O を用いてよく表される．



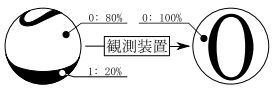
ビッグ O　すべての $N \geq 1$ に対して，$f(N) < kg(N)$ ならば $f(N) = O(g(N))$ と表す．

例　N 以下の数同士の足算の演算量は $O(\ln N + 1)$ である．

正確には $\lfloor \log_2 N \rfloor + 1$ であり，これは，$\lfloor \log_2 N \rfloor + 1 < 2(\ln N + 1)$ である．

5　量子コンピュータ

0 と 1 の両方の状態を持つことができる量子を使ったコンピュータであり，並列計算を行うことができる．0 と 1 の両方の状態を持った量子を**観測**することにより，0 か 1 か確定することができる．例えば，0 が 80%，1 が 20% の状態のときに観測すれば，80% の確率で 0 が 100% の状態または，20% の確率で 1 が 100% の状態となる．この仕組みをうまく使うことで離散フーリエ変換が高速となる．これを用いた素因数分解法が Shor のアルゴリズムである．量子の状態は $\alpha_i \in \mathbb{C}$ を用いて，

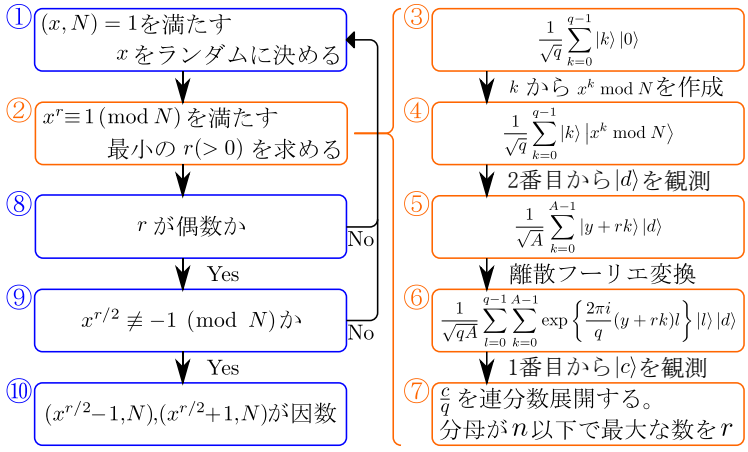


$$\alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle + \alpha_3 |3\rangle + \alpha_4 |4\rangle + \cdots$$

と表され，k が観測される確率は α_k^2 となる．

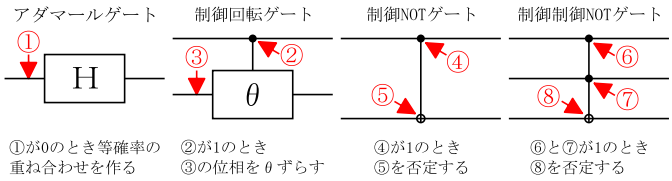
6　Shor のアルゴリズム

素因数分解する数を N とすれば，Shor のアルゴリズムは右図のようになる．左の列は上から 2 番目を除いて古典的コンピュータで行い，それ以外を量子コンピュータで計算する．古典的コンピュータではこの部分の計算に時間がかかるが，量子コンピュータで離散フーリエ変換をうまく使うことで演算量が少なくなる．素因数分解が完了するまでに量子コンピュータが行う演算量は $O((\ln N)^3(\ln\ln N))_q$ である．



7　量子コンピュータの演算量

量子状態を変化させる基本ゲート 1 個を演算量 1 として考える．基本ゲートは全部で 4 種類あり，右図のようになっている．$|0\rangle$ をアダマルゲートに通すことで $\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$ の等確率の量子状態を作ることができる．



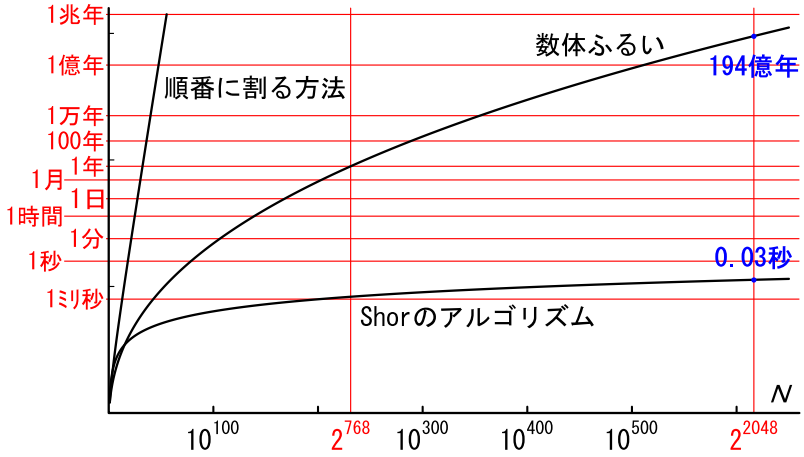
8　RSA 暗号を解く時間

N を素因数分解する時間を 3 つのアルゴリズム，単純に順番に 1 つずつ割る方法．古典的コンピュータで現在最速の数体ふるい．そして，量子コンピュータを用いた Shor で比較する．これらのアルゴリズムの演算量はそれぞれ

順番に割る方法　$K_1\sqrt{N}\left(\ln\sqrt{N}\right)^2$　　数体ふるい　$\exp\left(K_2(\ln N)^{1/3}(\ln\ln N)^{2/3}\right)$

Shor のアルゴリズム　$K_3(\ln N)^3(\ln\ln N)_q$

である．2005 年から 2010 年にかけて NTT が中心となり行われた実験をもとに係数を決定する．2^{768} 程度の数を数体ふるいを用いて計算に 1 年，1 秒間に 10^{12} 回計算可能であるとすれば，$K_2=1.6279734078$ である．そこで，K_1，K_3 もこの値であるとする．このとき，RSA-2048 を解く時間は数体ふるいで 194 億年，Shor のアルゴリズムで 0.03 秒である．



参考文献

[1] J.H.Silverman, J.Tate, 楕円曲線論入門, シュプリンガー・ジャパン株式会社，2012.
[2] Neal Koblitz, 櫻井 幸一, 数論アルゴリズムと楕円暗号理論入門, シュプリンガー・フェアラーク東京，1997.
[3] 西野 哲朗, 情報科学セミナー 量子コンピュータ入門, 東京電気大学出版局，1997.
[4] NIST, FIPS 197, 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
[5] 橋本 竜太, 実数の有理数近似と連分数展開, 詫間電波工業高等専門学校, 2006.
[6] James J. Tattersall, 小松 尚夫 初等整数論 9 章 (第 2 版), 森北出版, 2008.
[7] 青空学園数学科, 数論初歩, http://aozoragakuen.sakura.ne.jp/suuron/node24.html.
[8] NTT, 公開鍵暗号の安全性の根拠である「素因数分解問題」で世界記録を更新, http://www.ntt.co.jp/news2010/1001/100108a.html.
[9] 徳永 裕己, 長井 歩, 今井 浩, 量子計算機シミュレーションシステム, http://www.kurims.kyoto-u.ac.jp/ kyodo/kokyuroku/contents/pdf/1120-13.pdf
[10] Eric Bach, Jeffrey Shallit, Algorithmic Number Theory, Vol. 1: Efficient Algorithms, The MIT Press, 1996.