量子アルゴリズムを用いたディジタル暗号化方式の安全性評価

桑 門 秀 典　　神戸大学大学院工学研究科准教授

1 はじめに

現在の電気通信は，ディジタル情報伝送とディジタル情報処理によって支えられている．一方で，量子情報を伝送・処理する量子通信や量子情報処理の研究 が活発に行われており，将来の通信技術として期待されている．しかし，ディジタル情報と量子情報は，その基本的な性質の違いから，排他的なものではない．したがって，量子情報処理が実用化されたとしても，現在のディジタル情報にすぐに取って代わるとは考えにくく，両者が共存する時期が長く続くと考 えられる．

量子計算機はまだ実現していないが，量子素子の研究開発が盛んに行われているので，現在の共通鍵ブロック暗号とハッシュ関数が使用されているうちに実現する可能性も否定できない． したがって，ディジタル情報を処理するハッシュ関数や共通鍵暗号の安全性を 量子アルゴリズムで評価することには，意義がある．量子アルゴリズ ムに対して，ハッシュ関数や共通鍵暗号が原理的に越えることができない安全性の限界があることを示した先行研究があるが，これは，適切に設計すれば， 量子コンピュータが実現した場合でも，高い安全性を実現できることも示唆している[3][4]．

しかしながら，先行研究は，ハッシュ関数や共通鍵暗号を完全にブラックボックスとして扱っていること，事前に与えられる仮定が現在のハッシュ関数にあわないこと，など現実にそぐわない部分があった．本研究の動機は，この現実に合わない部分を改善し，現在のハッシュ関数や共通鍵暗号がどの程度限界に近いのかを明らかにすることである．

本研究では，ハッシュ関数や共通鍵暗号が小さいプリミティブの繰り返し 構造になっている点に着目する．理論的な安全性解析を行う場合， そのプリミティブが理想的であることを仮定し， ハッシュ関数や共通鍵暗号全体が安全であることを示す方法が一般的である． したがって， プリミティブが理想的であるかどうか，つまり，プリミティブが理想とされているものから識別可能かどうかという点が非常に重要である．そのような識別可能性を議論する際に，ランダム置換とランダム関数の識別可能性が重要な役割を果たすことが これまでの古典暗号の安全性の議論から分かっている． そこで，本研究では，量子アルゴリズムを用いて， ランダム置換とランダム関数の識別可能性の検討を行う

1-1 RP/RF 識別問題

$F_{l,n}$ を $f:\{0,1\}^l \to \{0,1\}^n$ の全ての関数の集合とする． $F_{l,n}$ からランダムに選ばれた関数を ランダム関数(random function: RF)と呼ぶ． $P_{n,n}$ を $p:\{0,1\}^n \to \{0,1\}^n$ の全ての置換の集合とする． $P_{n,n}$ からランダムに選ばれた置換を ランダム置換(random permutation: RP)と呼ぶ． g を $P_{n,n}$ のランダム置換または $F_{n,n}$ のランダム関数のオラクルとし， g がランダム置換なのか，ランダム関数なのか， を決定する問題を RP/RF 識別問題と呼ぶ[1]． g へオラクルアクセスを q 回行い， 0 または 1 を出力するアルゴリズム A を考える． アルゴリズム A がそれらを識別する能力を評価するために， A の rprf-advantage を以下のように定

[1] 古典暗号の安全性の解析を行う場合は， ランダム置換とランダム関数ではなく， 擬似ランダム置換(pseudorandom permutation: PRP)と 擬似ランダム関数(pseudorandom function: PRF) の識別困難さについて議論する場合が多い． したがって，RP/RFではなく， PRP/PRFという言葉が用いられる． 計算量的な仮定である擬似ランダム関数・擬似ランダム置換の方が， 理想的な仮定であるランダム関数・ランダム置換よりも現実の古典暗号のモデル化として妥当である．

義する.

$$Adv_{n,q}^{rprf}(A)=\left|Pr\left[g\leftarrow F_{n,n};A^{g}\Rightarrow 1\right]-Pr\left[g\leftarrow P_{n,n};A^{g}\Rightarrow 1\right]\right|$$

この rprf-advantage が大きいほど， アルゴリズム A の識別能力が高いことを意味する． なお， A の出力は 0 または 1 なので， A は， g がランダム関数である証拠， あるは， g がランダム置換である証拠を出力する必要はないことに 注意しよう.

A が古典アルゴリズムであり， A は古典オラクル g へ q 回のオラクルアクセスをする(クエリをする) と仮定する． このとき， A の rprf-advantage は,

$$Adv_{n,q}^{rprf}(A)\leq\frac{q(q-1)}{2^{n+1}}$$

である[5]． A が古典的であることとクエリ回数が q 回であること以外， A の計算能力については何ら制限をしていないので， いかなる古典アルゴリズム A も RP/RF 識別問題に有意な解を出力するためには, $O(2^{n/2})$ 回のオラクルアクセスが必要である.

本研究では, RP/RF 識別問題において， ランダム関数を r 対 1 関数に限定した場合を考察する． ここで, r 対 1 関数とは，1 つの写像に対して原像が常に r 個あるような関数である． つまり，任意の $x\in\{0,1\}^{l}$ の $y=f(x)$ に対して,

$$r=\#\{x\mid y=f(x),x\in\{0,1\}^{l}\}.$$

$F_{l,n}^{r}$ を $f:\{0,1\}^{l}\rightarrow\{0,1\}^{n}$ への全ての r 対 1 関数の集合とする． $F_{l,n}^{r}$ からランダムに選ばれた r 対 1 関数を r 対 1 ランダム関数という． $r=1$ の場合は, 1 対 1 ランダム関数はランダム置換なので， 以後, $r\geq 2$ とする． g を $F_{n,n}^{r}$ の r 対 1 ランダム関数または $P_{n,n}$ のランダム置換のオラクルとし， g が r 対 1 ランダム関数なのか, ランダム置換なのかを 決定する問題を RP/r-RF 識別問題と呼ぶことにする． アルゴリズム A の RP/r-RF 識別能力を評価するために， A の rprrf-advantage を以下のように定義する.

$$Adv_{n,q}^{rprrf}(A)=\left|Pr\left[g\leftarrow F_{n,n}^{r};A^{g}\Rightarrow 1\right]-Pr\left[g\leftarrow P_{n,n};A^{g}\Rightarrow 1\right]\right|$$

本研究では， A が量子アルゴリズムであり， g の計算を行う量子回路にオラクルアクセスする場合, RP/r-RF 識別問題の rprrf-advantage を評価する.

2 従来方式との関係

2-1 Deutsch のアルゴリズム

Deutsch の問題は， 関数値の排他的論理和を計算する問題である． この問題が， RP/RF 識別問題の特殊な場合であることを後で説明する.

Deutsch の問題

1-bit の関数 $f:\{0,1\}\to\{0,1\}$ がオラクルとして与えられる． $f(0)\oplus f(1)$ の値を求めよ．

1-bit の関数 $f:\{0,1\}\to\{0,1\}$ がオラクルとして与えられる． $f(0)\oplus f(1)$ の値を求めよ．

Deutsch のアルゴリズムは， f を計算するオラクルを量子回路の場合， 1 回のクエリ(オラクル呼出)で $f(0)\oplus f(1)$ の値を決定できる． 具体的なアルゴリズムは下記のとおり． f を計算する unitary operator を U_f とする．

$$U_f:|x>|y>\mapsto|x>|f(x)\oplus y>$$

$|x>$ と $|y>$ を

$$|x>=\frac{1}{\sqrt{2}}|0>+\frac{1}{\sqrt{2}}|1>,\ |y>=\frac{1}{\sqrt{2}}|0>-\frac{1}{\sqrt{2}}|1>$$

とする． U_f の出力は，

$$U_f\left(\frac{1}{\sqrt{2}}|0>+\frac{1}{\sqrt{2}}|1>\right)\left(\frac{1}{\sqrt{2}}|0>-\frac{1}{\sqrt{2}}|1>\right)=U_f\frac{1}{2}\left(|0>(|0>-|1>)+|1>(|0>-|1>)\right)$$

$$=\frac{1}{2}\left(|0>(|0\oplus f(0)>-|1\oplus f(0)>)+|1>(|0\oplus f(1)>-|1\oplus f(1)>)\right)$$

$$=\frac{1}{2}\left(|0>(|f(0)>-|1\oplus f(0)>)+|1>(|f(1)>-|1\oplus f(1)>)\right)\qquad(1)$$

となる． ここで， $f(0),f(1)\in\{0,1\}$ なので，下記の等式が成立するので，

$$|0>|f(0)>-|0>|1\oplus f(0)>=(-1)^{f(0)}|0>|0>-(-1)^{f(0)}|0>|1>$$
$$|1>|f(1)>-|1>|1\oplus f(1)>=(-1)^{f(1)}|1>|0>-(-1)^{f(1)}|1>|1>$$

式 (1)に代入すると，

$$U_f\left(\frac{1}{\sqrt{2}}|0>+\frac{1}{\sqrt{2}}|1>\right)\left(\frac{1}{\sqrt{2}}|0>-\frac{1}{\sqrt{2}}|1>\right)=\frac{1}{\sqrt{2}}(-1)^{f(0)}\left(|0>+(-1)^{f(0)\oplus f(1)}|1>\right)\cdot\frac{1}{\sqrt{2}}\left(|0>-|1>\right)$$

最初のキュービットを双対基底で測定すると， アダマール変換を H_2 として，

$$H_2\frac{1}{\sqrt{2}}\left(|0>+(-1)^{f(0)\oplus f(1)}|1>\right)=\begin{cases}|0> & \text{if } f(0)\oplus f(1)=0\\ |1> & \text{if } f(0)\oplus f(1)=1\end{cases}$$

となるので， その測定結果で $f(0)\oplus f(1)$ の値が判明する． この量子アルゴリズムは確定的であり， 必ず正しい値が得られることに注意しよう．

Deutsch の問題が， この研究の対象となっている RP/RF 識別問題の特殊な場合であることを説明しよう．

1 bit から 1 bit への関数全ての集合 $F_{1,1}$ は,

$$F_{1,1} = \{f_0, f_1, f_2, f_3\}$$

ここで，関数 f_i は以下のとおり.

$$\begin{cases} f_0(0) = 0 \\ f_0(1) = 0 \end{cases} \begin{cases} f_1(0) = 0 \\ f_1(1) = 1 \end{cases} \begin{cases} f_2(0) = 1 \\ f_2(1) = 0 \end{cases} \begin{cases} f_3(0) = 1 \\ f_3(1) = 1 \end{cases}$$

1 bit から 1 bit への置換全ての集合 $P_{1,1}$ は,

$$P_{1,1} = \{p_0, p_1\}$$

ここで，置換 p_i は以下のとおり.

$$\begin{cases} p_0(0) = 0 \\ p_0(1) = 1 \end{cases} \begin{cases} p_1(0) = 1 \\ p_1(1) = 0 \end{cases}$$

定義から $P_{1,1} \subset F_{1,1}$ なので， $F_{1,1} \setminus P_{1,1} = \{f_0, f_3\}$ からランダムに選ばれた関数 f と $P_{1,1} = \{p_0, p_1\}$ からランダムに選ばれた関数 p の識別問題になる. さらに， $F_{1,1} \setminus P_{1,1}$ は $F_{1,1}^2$ なので， RP/2-RF 識別問題である. 関数 f は $f(0) \oplus f(1) = 1$， 置換 p は $p(0) \oplus p(1) = 0$ となっているので， f と p の識別問題は Deutsch の問題に帰着する. 故に， 1 bit 入出力の RP/2-RF 識別問題は， 量子アルゴリズムを用いることで 任意の古典アルゴリズムよりも少ないオラクル呼出で， 誤ることなく常に識別可能である.

2-2 Simmons のアルゴリズム

Simmons は，置換と特殊な関数の識別問題(Simmons の問題)を考え， この問題が多項式時間の量子アルゴリズムで解けるが， 多項式時間の古典アルゴリズムでは解けないことを示した. Simmons の問題と RP/RF 識別問題の違いについては， 後で説明する.

Simmons の問題

$f : \{0,1\}^n \to \{0,1\}^n$ がある. この f は，下記のいずれかの性質を満たす.

1. 置換である.
2. 2 対 1 であり，かつ異なる任意の $a, b \in \{0,1\}^n$ に対して,

$$f(a) = f(b) \leftrightarrow b = a \oplus s$$

3. となる s が一つ存在する.

f がどちらの条件を満たすかを決定せよ. もし 2 対 1 の場合， s も求めよ.

この問題を解く確率的量子アルゴリズムを示す. f を計算する unitary operator を U_f とする. 初期状態 $|0^n, 0^n>$ の左側の n キュービットに アダマール変換を適用して,

$$\varphi_1 = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x, 0^n>.$$

を作成する．φ_1 に U_f を適用して，

$$\varphi_2 = U_f \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x,0^n> = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x,f(x)>.$$

を得る．$|x>$ にアダマール変換を適用して，

$$\varphi_3 = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} \sum_{y\in\{0,1\}^n} (-1)^{xy} |y,f(x)>. \tag{2}$$

を得る．そして，φ_3 を観測して，$(y,f(x))$ を得る．これを l 回繰り返して，$(y_1,f(x_1))$，$(y_2,f(x_2))$，…，$(y_l,f(x_l))$ を得る．f が置換の場合，式 (2) は 2^{2n} 通りの全ての状態が等しい振幅で重ね合わさっているので，観測結果 $(y_i,f(x_i))$ はその中から ランダムに選ばれた状態である．一方，f が 2 対 1 の場合，式 (2) において，$|y,f(x)>$ と $|y,f(x\oplus s)>$ は同じ状態になるので，置換の場合とは異なり，2^{2n} 通りの全ての状態が等しい振幅で重ね合わさっているのではない．$|y,f(x)>$ と $|y,f(x\oplus s)>$ の振幅は $(-1)^{xy}/2^n$ と $(-1)^{(x\oplus s)y}/2^n$ であるから，

$$\frac{1}{2^n}\left((-1)^{xy}+(-1)^{(x\oplus s)y}\right) = \begin{cases} \dfrac{1}{2^{n-1}} & \text{if } y\cdot s = 0 \bmod 2 \\ 0 & \text{if } y\cdot s = 1 \bmod 2 \end{cases}$$

ここで，$y\cdot s$ は，y と s を其々2 元の n 次元ベクトルと みなしたときの内積を表す．したがって，観測して得られた $(y_i,f(x_i))$ の y_i は，

$$y_i \cdot s = 0 \bmod 2 \tag{3}$$

を満たす．いずれの場合も，l 個の y_i が入手できているので，

$$\begin{cases} y_1\cdot s = 0 \bmod 2 \\ y_2\cdot s = 0 \bmod 2 \\ \quad\cdots \\ y_l\cdot s = 0 \bmod 2 \end{cases}$$

なる連立方程式をたてることができる．l が n よりも十分に大きいと仮定する．もし f が置換であるならば，y_i はランダムな値なので，この連立方程式を満たす s は存在しない．一方，もし f が 2 対 1 なら

ば， 式 (3)より この連立方程式を満たすsは一意に求まる． なお， lがnよりも十分に大きいという仮定から， y_iをn次元の 2 元ベクトルとみなすと， $y_1, y_2, \ldots, y_l$の中に 線形独立なベクトルがn個以上あることを期待している． しかし， 線形独立なベクトルが必ずn個以上あることは保証できないので， 上記のアルゴリズムは確率的， つまり必ずしも成功は保証されない点が Deutsch の問題のアルゴリズムとは異なる．

Simmons の問題における 2 対 1 関数には制約があるため， 2 対 1 ランダム関数ではない． しかし，$f(a)=f(b)$となるa,bに線形関係がある場合には， 量子アルゴリズムが古典アルゴリズムよりも 効率良くランダム置換と識別できることを示している． なお， 古典アルゴリズムで Simmons の問題を解くためには 指数関数時間を要することが ヤオの最小化原理から導かれる．

2-3 Brassard らのアルゴリズム

Brassard らは， r対 1 関数fが与えられたとき， $f(x_1)=f(x_2)$となるx_1, x_2を計算する 量子アルゴリズムを示した(BHT アルゴリズム)[3]．ランダム置換 p には $p(x_1)=p(x_2)$となるx_1, x_2は存在しないので，BHT アルゴリズムを利用して RP/r-RF 識別問題を解くアルゴリズムが構成できる．

まず，BHT アルゴリズムの述べよう． gを$F_{n,n}^{r}$のr対 1 ランダム関数とする． $\{0,1\}^n$から$t=(2^n/r)^{1/3}$個の相異なる要素をランダムに選び， その集合をXとする．

$$X=\{x_1, x_2, \ldots, x_t\},\ x_i \in \{0,1\}^n$$

各x_iに対して， $y_i=g(x_i)$を(古典的に)計算し， y_iの値に従って整列した(x_j, y_j)の(古典的な)表Tを作成する． 次に， 以下のような関数$v:\{0,1\}^n \to \{0,1\}$を計算する unitary operator U_vが与えられたとする．

$$v(x)=\begin{cases}1 & \text{if } x \notin X \wedge (x_j, g(x)) \in T \text{ for } \exists x_j, \\ 0 & \text{otherwise.}\end{cases}$$

このとき， U_vを用いて Grover アルゴリズム [4]を実行して， 出力wを得る．そして， 表Tの中から，$(x_k, g(w))$となる項を探索する． もし発見できれば，(x_k, w)を出力し， 発見できなければ，発見できなかったをことを示す‘⊥’を出力する．

Grover アルゴリズムの出力wは高い確率で$v(w)=1$となるが， $v(w)=0$なwを出力する可能性もあるので， その意味で BHT アルゴリズムは確率的である． BHT アルゴリズムの計算量を 古典的な部分と量子的な部分に分けて評価する． 古典的な部分は，表の作成・整列・探索である． 作成には$O(t)$，整列には$O(t\log t)$，探索には$O(\log t)$の 計算量が必要である． なお，作成の計算量はクエリ回数であるが， 整列と探索はそうではないことに注意しよう． 量子的な部分は，Grover アルゴリズムであり， U_vへのクエリ回数は$O(\sqrt{2^n/t})$である． $t=(2^n/r)^{1/3}$なので， rが2^nに対して十分に小さい定数と仮定すると， 古典的に$O(n2^{n/3})$，量子的に$O(2^{n/3})$となる． 古典アルゴリズムのみで$g(x)=g(x')$となるx, x'を求めるため

には， $O(2^{n/2})$ のクエリ回数が必要であるから， 量子アルゴリズムを用いることで， 計算量が大幅に削減することができる．

g がランダム置換の場合，BHT アルゴリズムの動作を考えよう． $v(w)=1$ になるような $w\in\{0,1\}^n$ が存在しないので， Grover アルゴリズムは， $\{0,1\}^n$ からランダムに選ばれた要素を w として出力する． したがって，表 T の中から $(x_k, g(w))$ なる項目を探索しても 存在しない場合がある．存在した場合， $x_k = w$ である．

BHT アルゴリズムをサブルーチンとする g に関する RP/r-RF 識別問題に対するアルゴリズム A を 以下のように構成できる．

1. g に対して BHT アルゴリズムを実行し，その出力を得る．

2. 出力 (x_k, w) が得られた場合:

もし $g(x_k)=g(w)$ かつ $x_k \neq w$ の場合，1 を出力する．

もし $g(x_k)\neq g(w)$ または $x_k = w$ の場合，0 を出力する．

3. 出力⊥が得られた場合: 0 を出力する．

Grover アルゴリズムの出力 w が $v(w)=1$ となる確率を $P_G(q)$ とおく． ここで， q は U_v へのクエリ回数である． A の rprrf-advantage を評価すると，

$$Pr\left[g \leftarrow F_{n,n}^{r}; A^{g} \Rightarrow 1\right] = P_G(q),\ Pr\left[g \leftarrow P_{n,n}; A^{g} \Rightarrow 1\right] = 0$$

なので，

$$Adv_{n,q}^{rprrf}(A) = P_G(q)$$

となる． Grover アルゴリズムの性質から， $q=O(2^{n/3})$ で $P_G(q)\approx 1$ となる． したがって， BHT アルゴリズムをサブルーチンとして用いれば， RP/r-RF 識別問題は， $2^{n/3}$ 程度のクエリで識別可能である． 古典アルゴリズムでは， $2^{n/2}$ 程度のクエリが必要なので， クエリ回数が大幅に削減されている．

2-4 考察

RP/r-RF 識別問題の特殊な例となる Deutsch の問題や Simmons の問題では，クエリ回数の点で 量子アルゴリズムが古典アルゴリズムよりも 優れていることを示した． 古典アルゴリズムでは取り得る値が複数あった場合， それらが排他的であるのに対し， 量子アルゴリズムでは取り得る値がアダマール変換等により重ね合わされているので， つまり関数 f 全体の様相を作っているので， 関数全体の性質を効率良く決定できている．

一般的な RP/r-RF 識別問題においても， 量子アルゴリズムが古典アルゴリズムより効率が良いことを示した． しかし，BHT アルゴリズムを利用したアルゴリズムでは， 識別問題が要求していない「証拠」（具体的には，ランダム関数の場合の衝突する入力の組）まで求めている． この余計な計算を省略できれば， 効率をさらに改善できる可能性がある．

古典暗号の安全性の概念の一つに，識別不可能性の概念がある． これは，理想とする関数を最初に決め，

実際に構成した関数がその理想とする関数と識別できる 確率を評価することで， 構成した関数の安全性を示すものである． 例えば，共通鍵暗号では， 鍵が未知のとき暗号化関数はランダム置換と識別不可能である ことを設計目標とする． また，ハッシュ関数では，ランダム関数と識別不可能である ことを設計目標とする． 前節までで示したしたように， 識別不可能性を議論するときには， 古典アルゴリズムより量子アルゴリズムが強力な場合がある． したがって， 古典暗号の識別不可能性を 量子アルゴリズムで評価することは意味がある．

3 RP/２－RF 識別問題

本研究では，まず，RP/2-RF 識別問題について議論する． RP/2-RF 識別問題を具体的に述べると，下記のようになる． RP/2-RF 識別問題は， Simmons の問題と似ているが， Simmons の問題のような線形はないことに注意しよう． また， $n=1$ のときは，Deutsch の問題とほぼ等価である(2.1 節参照)．

RP/2-RF識別問題

$g:\{0,1\}^n \to \{0,1\}^n$ がある． この g は，下記のいずれかの性質を満たす．

4. g はランダム置換である．
5. g は 2 対 1 ランダム関数である．

g がどちらの条件を満たすかを決定せよ．

3-1 クエリ回数が１回の場合

クエリ回数が 1 回の場合の RP/2-RF 識別問題を考える． 古典アルゴリズムの場合， いかなる古典アルゴリズム A も g を識別できない． つまり，

$$Adv_{2,1}^{rp2rf}(A)=0.$$

次に，量子アルゴリズムの場合を考えよう． g の計算を行う unitary operator を U_g とする． U_g を 1 回用いて， g の性質を推定する量子アルゴリズム A を述べる．

1. 下記のような状態 $|\varphi_1>$ を用意する．

$$|\varphi_1>=\frac{1}{2}\sum_{x\in\{0,1\}^n}|x>|00>$$

2. U_g を作用させて，

$$|\varphi_2>=U_g|\varphi_1>$$
$$=\frac{1}{2}\sum_{x\in\{0,1\}^n}|x>|g(x)>$$

第二レジスタの $|g(x)>$ の部分を測定する． 測定後，この部分は固定されるので， 以後この部分の記述を省略する． 測定後の状態は， g の性質によって異なる．

$$|\varphi_3>=\begin{cases} |x_0> & \text{if } g \text{ is RP,} \\ \dfrac{|x_0>+|x_1>}{\sqrt{2}} & \text{if } g \text{ is 2RF.} \end{cases}$$

3. H_nを2^n行2^n列のアダマール行列とする． $|\varphi_3>$にH_nを作用させると，

$$|\varphi_4>=H_2|\varphi_3>$$
$$=\begin{cases} \dfrac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}(-1)^{x_0\cdot z}|z> & \text{if } g \text{ is RP,} \\ \dfrac{1}{\sqrt{2^{n+1}}}\sum_{z\in\{0,1\}^n}\left((-1)^{x_0\cdot z}+(-1)^{x_1\cdot z}\right)|z> & \text{if } g \text{ is 2RF,} \end{cases}$$

ここで，$x_i\cdot z$は，　$x_i=|x_{i,n-1}x_{i,n-2}\cdots x_{i,0}>$，　$z=|z_{n-1}n_{n-2}\cdots z_0>$としたとき，

$$x_i\cdot z=\sum_{j=0}^{n-1}x_{i,j}z_j \bmod 2$$

である．

4. $|\varphi_4>$を測定する． もし$00\cdots0$が測定されれば，1 を出力し， それ以外であれば，0 を出力する

Step 4 の測定において， gがランダム置換の場合，$00\cdots0$が測定される確率は$1/2^n$である． 一方，gが 2 対 1 ランダム関数の場合，　$00\cdots0$が測定される確率は$1/2^{n-1}$である． したがって，

$$Pr\left[g\leftarrow F^2_{n,n};A^g\Rightarrow 1\right]=\frac{1}{2^{n-1}},\ Pr\left[g\leftarrow P_{n,n};A^g\Rightarrow 1\right]=\frac{1}{2^n},$$

となり，

$$Adv^{rp2rf}_{n,1}(A)=\frac{1}{2^{n-1}}$$

である． 古典アルゴリズムの場合， いかなるアルゴリズムでも$Adv^{rp2rf}_{n,1}(A)=0$なので， 量子アルゴリズムの方が優れていることがわかる． 特に，nが小さい場合には(例えば，$n=2,3$)， 上記の量子アルゴリズムの rp2rf-advantage は，無視できない値である．

3-2 クエリ回数が q 回の場合

前節で述べたアルゴリズムは， ビット数nが小さい場合には有効であるが， nが大きくなると， 漸近的に rp2rf-advantage が 0 になるアルゴリズムであった． 本節では，nが大きく，クエリ回数qが多い場合に有効なアルゴリズムを示す．

1. クエリ回数をカウントするためのカウンタc_q， 測定結果の累計をカウントするためのカウンタc_0,c_1を 0 に初期化する．
2. $c_q=q$ならば，Step 12 に行く． そうでなければ，c_qの値を 1 増やす．

3. 状態 $|\psi_0>$ を用意する.

$$|\psi_0>=|0>^{\otimes n}|0>^{\otimes n}|0>.$$

4. 第一レジスタと第三レジスタに Hadamard 変換を施す.

$$\begin{aligned}|\psi_1>&=(H_n\otimes I_n\otimes H_1)|\psi_0>\\&=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x>|0>^{\otimes n}\left(\frac{|0>+|1>}{\sqrt{2}}\right),\end{aligned}$$

ここで, H_n と I_n は, それぞれ $2^n\times 2^n$ Hadamard 行列 と $2^n\times 2^n$ 単位行列である.

5. $U_g\otimes I_1$ を $|\psi_1>$ に適用する.

$$\begin{aligned}|\psi_2>&=U_g\otimes I_1|\psi_1>\\&=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x>|g(x)>\left(\frac{|0>+|1>}{\sqrt{2}}\right).\end{aligned}$$

6. 第二レジスタ $|g(x)>$ を測定する. 第二レジスタの測定値は重要ではなく, これ以降固定値になるので, 第二レジスタの表記を省略する. 測定後の状態は, 下記のように書ける.

$$|\psi_3>=\left(\alpha_0|x_0>+\alpha_1|x_1>\right)\left(\frac{|0>+|1>}{\sqrt{2}}\right),$$

ここで, α_i は実数であり, $\alpha_0^2+\alpha_1^2=1$ を満たす.

7. $|\psi_3>$ に Hadamard 変換を施す.

$$\begin{aligned}|\psi_4>&=(H_n\otimes I_1)|\psi_3>\\&=\left(\frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}\alpha_0(-1)^{x_0\cdot z}+\alpha_1(-1)^{x_1\cdot z}|z>\right)\left(\frac{|0>+|1>}{\sqrt{2}}\right),\end{aligned}$$

ここで, $x_i\cdot z$ は, x_i と z の法 2 の内積である. つまり, $x_i=x_{i,n-1}x_{i,n-2}\ldots x_{i,0}$ $z=z_{n-1}z_{n-2}\ldots z_0$ に対して,

$$x_i\cdot z=\sum_{j=0}^{n}x_{i,j}\cdot z_j \bmod 2.$$

と計算される.

8. $|z>$ の $n-1$ qubit $|z_{n-1}z_{n-2}\ldots z_1>$ を測定する. 測定値は重要ではなく, このレジスタの部分は, これ以降固定されるので, 表記を省略する. 測定後の状態は, 下記のように書ける.

$$|\psi_5>=(\beta_0|0>+\beta_1|1>)\left(\frac{|0>+|1>}{\sqrt{2}}\right)$$
$$=\frac{\beta_0}{\sqrt{2}}|00>+\frac{\beta_0}{\sqrt{2}}|01>+\frac{\beta_1}{\sqrt{2}}|10>+\frac{\beta_1}{\sqrt{2}}|11>.$$

ここで，β_i は実数であり，$\beta_0^2+\beta_1^2=1$を満たす.

9. 4 次の DCT 行列 C_2 を $|\psi_5>$に作用させる.

$$|\psi_6>=C_2|\psi_5>$$
$$=\gamma_0|00>+\gamma_1|01>+\gamma_3|11>.$$

ここで,γ_iは実数であり，$\gamma_0^2+\gamma_1^2+\gamma_3^2=1$ を満たす. なお,4 次の DCT 行列 C_2は，下記のような unitary 行列である.

$$C_2=\frac{1}{\sqrt{2}}\begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \cos\left(\frac{\pi}{8}\right) & \cos\left(\frac{3\pi}{8}\right) & \cos\left(\frac{5\pi}{8}\right) & \cos\left(\frac{7\pi}{8}\right)\\ \cos\left(\frac{2\pi}{8}\right) & \cos\left(\frac{6\pi}{8}\right) & \cos\left(\frac{10\pi}{8}\right) & \cos\left(\frac{14\pi}{8}\right)\\ \cos\left(\frac{3\pi}{8}\right) & \cos\left(\frac{9\pi}{8}\right) & \cos\left(\frac{15\pi}{8}\right) & \cos\left(\frac{21\pi}{8}\right)\end{pmatrix}$$

10. $|\psi_6>$の左側の qubit を測定する． 測定結果が 1 ならば，Step 2 へ戻る． そうでなければ，以下の Step を続ける． これ以降，左側の qubit は固定されるので， その表記を省略すると， 測定後の状態は下記のようになる.

$$|\psi_7>=\delta_0|0>+\delta_1|1>.$$

ここで，δ_iは実数であり，$\delta_0^2+\delta_1^2=1$を満たす.

11. $|\psi_7>$を測定する． 測定結果が 0 ならば，カウンタ c_0の値を 1 増やし， 測定結果が 1 ならば，カウンタ c_1の値を 1 増やす． そして，Step 2 へ戻る.

12. 最後に,

$$\frac{c_0}{c_1}\le-\frac{\log\left(\frac{1}{2}+\frac{\cos^2\left(\frac{\pi}{8}\right)}{1+\cos^2\left(\frac{\pi}{8}\right)}\right)}{\log\left(\frac{1}{2}+\frac{1}{1+\cos^2\left(\frac{\pi}{8}\right)}\right)}\approx 1.04031,$$

であるならば，0 を出力し， そうでなければ，1 を出力して終了する.

gがランダム置換である事象をRP， gが 2 対 1 ランダム関数である事象を$2RF$と表記する.

$$Pr\left[RP\right]=\frac{1}{2},\ Pr\left[2RF\right]=\frac{1}{2}$$

である． Step 6 の$|\psi_3>$を場合分けして書くと，

$$|\psi_3>=\begin{cases} |\psi_{3,0}>=|x_0>\left(\dfrac{|0>+|1>}{\sqrt{2}}\right), \\ |\psi_{3,1}>=\left(\dfrac{1}{\sqrt{2}}|x_0>+\dfrac{1}{\sqrt{2}}|x_1>\right)\left(\dfrac{|0>+|1>}{\sqrt{2}}\right). \end{cases} \tag{4}$$

ここで，gがランダム置換ならば，$|\psi_3>$は必ず$|\psi_{3,0}>$であり，gが2対1ランダム関数ならば，$|\psi_3>$は必ず$|\psi_{3,1}>$である． つまり，

$$Pr\left[|\psi_3>=|\psi_{3,0}>|RP\right]=1,\ Pr\left[|\psi_3>=|\psi_{3,1}>|RP\right]=0,$$
$$Pr\left[|\psi_3>=|\psi_{3,0}>|2RF\right]=0,\ Pr\left[|\psi_3>=|\psi_{3,1}>|2RF\right]=1.$$

Step 8 の $|\psi_5>$ を考えよう． 式 (4)から $|\psi_5>$は，以下のいずれかの状態になる．

$$|\psi_5>=\begin{cases} |\psi_{5,0}>=\left(\dfrac{1}{\sqrt{2}}|0>+\dfrac{1}{\sqrt{2}}|1>\right)\left(\dfrac{|0>+|1>}{\sqrt{2}}\right), \\ |\psi_{5,1}>=\left(\dfrac{1}{\sqrt{2}}|0>-\dfrac{1}{\sqrt{2}}|1>\right)\left(\dfrac{|0>+|1>}{\sqrt{2}}\right), \\ |\psi_{5,2}>=|0>\left(\dfrac{|0>+|1>}{\sqrt{2}}\right), \\ |\psi_{5,3}>=|1>\left(\dfrac{|0>+|1>}{\sqrt{2}}\right). \end{cases}$$

gをランダム置換と仮定する． このとき，$|\psi_5>$は， $|\psi_{5,0}>$または$|\psi_{5,0}>$であり， それぞれの確率は1/2である． $|\psi_5>$が$|\psi_{5,2}>$または$|\psi_{5,3}>$になることはない． つまり，

$$Pr\left[|\psi_5>=|\psi_{5,0}>|RP\right]=Pr\left[|\psi_5>=|\psi_{5,1}>|RP\right]=\frac{1}{2},$$
$$Pr\left[|\psi_5>=|\psi_{5,2}>|RP\right]=Pr\left[|\psi_5>=|\psi_{5,3}>|RP\right]=0.$$

gを2対1ランダム関数と仮定する． $|\psi_5>$は上記の四つのいずれかの状態になるが， その確率は，nに依存する． nが十分に大きくなると， それぞれの状態になる確率は，1/4に近くなる．

$$Pr\left[|\psi_5>=|\psi_{5,0}>|2RF\right]\approx Pr\left[|\psi_5>=|\psi_{5,1}>|2RF\right]$$
$$\approx Pr\left[|\psi_5>=|\psi_{5,2}>|2RF\right]\approx Pr\left[|\psi_5>=|\psi_{5,3}>|2RF\right]\approx\frac{1}{4}.$$

Step 8 の測定は 原像$|x_0>$あるいは$|x_0>+|x_1>$に関する ほとんどの情報を破壊するので， この時点で Step 2 で得られた測定結果に対する原像の情報はほとんど失われる． このときに測定されなかった 1

qubit を用いて，g の性質を特定する． Step 9 で DCT 変換を作用させた後の状態は，

$$|\psi_6>=\begin{cases}|\psi_{6,0}> &= C_2|\psi_{5,0}> \\ &= |00>, \\ |\psi_{6,1}> &= C_2|\psi_{5,1}> \\ &= \cos\left(\frac{\pi}{8}\right)|01>-\cos\left(\frac{3\pi}{8}\right)|11>, \\ |\psi_{6,2}> &= C_2|\psi_{5,2}> \\ &= \frac{1}{\sqrt{2}}|00>+\frac{1}{\sqrt{2}}\cos\left(\frac{\pi}{8}\right)|01>-\frac{1}{\sqrt{2}}\cos\left(\frac{3\pi}{8}\right)|11>, \\ |\psi_{6,3}> &= C_2|\psi_{5,3}> \\ &= \frac{1}{\sqrt{2}}|00>-\frac{1}{\sqrt{2}}\cos\left(\frac{\pi}{8}\right)|01>+\frac{1}{\sqrt{2}}\cos\left(\frac{3\pi}{8}\right)|11>. \end{cases}$$

Step 10 において， 測定結果 w が 0 の確率を求めると，

$$Pr[w=0]=Pr[w=0|RP]Pr[RP]+Pr[w=0|2RF]Pr[2RF]$$

$$=\frac{5}{8}+\frac{3}{8}\cos^2\left(\frac{\pi}{8}\right)-\frac{1}{8}\cos^2\left(\frac{3\pi}{8}\right)\approx 0.9267. \tag{5}$$

測定結果が 0 として次のステップに進むと， 測定後の状態 $|\psi_7>$ は，下記のいずれかになる．

$$|\psi_7>=\begin{cases}|\psi_{7,0}> &= |0>, \\ |\psi_{7,1}> &= |1>, \\ |\psi_{7,2}> &= \frac{1}{\sqrt{1+\cos^2\left(\frac{\pi}{8}\right)}}|0>+\frac{\cos\left(\frac{\pi}{8}\right)}{\sqrt{1+\cos^2\left(\frac{\pi}{8}\right)}}|1>, \\ |\psi_{7,3}> &= \frac{1}{\sqrt{1+\cos^2\left(\frac{\pi}{8}\right)}}|0>-\frac{\cos\left(\frac{\pi}{8}\right)}{\sqrt{1+\cos^2\left(\frac{\pi}{8}\right)}}|1>. \end{cases}$$

Step 11 の測定結果を z とおくと， z が 0 または 1 の確率は，

$$Pr[z=0|RP]=\frac{1}{2},$$

$$Pr[z=1|RP]=\frac{1}{2},$$

$$Pr[z=0|2RF]=\frac{1}{2}\left(\frac{1}{2}+\frac{1}{1+\cos^2\left(\frac{\pi}{8}\right)}\right)\approx 0.5198,$$

$$Pr[z=1|2RF]=\frac{1}{2}\left(\frac{1}{2}+\frac{\cos^2\left(\frac{\pi}{8}\right)}{1+\cos^2\left(\frac{\pi}{8}\right)}\right)\approx 0.4802.$$

となる． g がランダム置換の場合，測定結果の分布は確率 $1/2$ の二項分布であり， g が 2 対 1 ランダム関数の場合，測定結果の分布は確率約 0.5198 の二項分布になる． Step 12 で行っていることは，これら二

つの二項分布の識別を行っている．

例として，$c_0 + c_1 = 1000$ の場合を考える． このとき，Step 11 の判定条件は， $c_0 \le 509$ ならば 0 を出力し， $c_0 \ge 510$ ならば 1 を出力することになる． したがって，

$$Pr\left[g \leftarrow F_{n,n}^2; A^g \Rightarrow 1 \right] = Pr\left[c_0 \ge 510 \,|\, 2RF \right],\ Pr\left[g \leftarrow P_{n,n}; A^g \Rightarrow 1 \right] = Pr\left[c_0 \ge 510 \,|\, RP \right],$$

となる． それぞれについて，計算すると，

$$p = \frac{1}{2}\left(\frac{1}{2} + \frac{1}{1+\cos^2\left(\frac{\pi}{8}\right)} \right) \approx 0.5198,$$

とおいて，

$$Pr\left[c_0 \ge 510 \,|\, 2RF \right] = \sum_{i=510}^{1000} \binom{1000}{i} p^i (1-p)^{1000-i}$$
$$\approx 0.741869$$

そして，

$$Pr\left[c_0 \ge 510 \,|\, RP \right] = \sum_{i=510}^{1000} \binom{1000}{i} \left(\frac{1}{2}\right)^{1000}$$
$$\approx 0.273986$$

である． したがって，rp2rf-advantage は，

$$Adv_{n,q}^{rp2rf}(A) \approx 0.741869 - 0.273986 = 0.467883$$

となる． ここで，$c_0 + c_1 = 1000$ となるために必要なクエリ数 q は， 式 (5) より，平均 1079 である．

次に，$c_0 + c_1 = 10^5$ の場合を考えよう． この場合， Step 11 の判定条件は， $c_0 \le 50987$ ならば 0 を出力し， $c_0 \ge 50988$ ならば 1 を出力することになる． したがって，

$$Pr\left[g \leftarrow F_{n,n}^2; A^g \Rightarrow 1 \right] = Pr\left[c_0 \ge 50988 \,|\, 2RF \right],\ Pr\left[g \leftarrow P_{n,n}; A^g \Rightarrow 1 \right] = Pr\left[c_0 \ge 50988 \,|\, RP \right],$$

となる． 上記と同様の計算により，

$$Pr\left[c_0 \ge 50988 \,|\, 2RF \right] \approx 1$$
$$Pr\left[c_0 \ge 50988 \,|\, RP \right] \approx 2.10958 \times 10^{-10}$$

なので，

$$Adv_{n,q}^{rp2rf}(A) \approx 1$$

4 まとめ

量子アルゴリズムは， 古典暗号の安全性を評価するツールとして有効である． 本研究では， 古典暗号の安全性解析において重要な ランダム置換とランダム関数の識別問題をとりあげ， ランダム関数が 2 対 1 に限定される場合のそれらの識別困難性を検討した． その結果， クエリ回数が 1 回の場合， 古典アルゴリズムでは，両者を識別することは不可能であるが， 量子アルゴリズムでは，可能であることを示した．

本研究をまとめている段階で，本研究と関連ある先行研究結果をある国際会議の査読者から御指摘頂いた [1][2]． これら先行研究結果の比較・検討を今後行っていきたい．

謝辞

本研究にご援助頂いた財団法人 電気通信普及財団に感謝します.

【参考文献】

[1] S. Aaronson, “Quantum lower bound for the collision problem,” Proceedings of the 34th ACM Symposium on the Theory of Computing, pp. 635–642, 2002.

[2] S. Aaronson and Y. Shi, “Quantum lower bounds for the collision and the element distinctness problems,” Journal of the ACM, vol. 51, no. 4, pp. 595–605, July 2004.

[3] G. Brassard, P. Hoyer, and A. Tapp, “Quantum algorithm for the collision problem,” quant-ph/9705002, 1997.

[4] L. K. Grover, “A fast quantum mechanical algorithm for database search,” Proceedings of The 28th ACM Symposium on the Theory of Computing, pp. 212–219, 1996.

[5] S. Lucks, “The sum of PRPs is a secure PRF,” Advances in Cryptology - EUROCRYPT 2000, Lecture Notes in Computer Science, vol. 1807, pp. 470–484, 2000.

〈発 表 資 料〉

題 名	掲載誌・学会名等	発表年月
Indifferentiable Double-Block-Length Compression Function	2007 Hawaii and SITA Joint Conference on Information Theory	2007 年 5 月
Query Complexity for Distinguishing r-to-One Random Functions	Proceedings of The 2008 Symposium on Cryptography and Information Security	2008 年 1 月