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（継続）

桑　門　秀　典　　神戸大学大学院工学研究科准教授

1 はじめに

量子計算機の優れた計算能力は，古典的暗号の安全性に脅かすものとして注目されている．Shor の素因数分解・離散対数問題の量子アルゴリズム[10]を用いれば，公開鍵暗号の RSA 暗号[9]や ElGmal 暗号[3]は，多項式時間で解読可能である．共通鍵暗号に対する最も汎用的な攻撃である鍵探索攻撃に Grover の量子探索アルゴリズム[4]を用いれば，n ビットの鍵を $O(2^{n/2})$ の計算量で発見することができる．また，Brassard ら[2]は，n ビットのハッシュ関数の衝突を $O(2^{n/3})$ で発見する量子アルゴリズムを提案している．Shor のアルゴリズムとは異り，Grover のアルゴリズムや Brassard らのアルゴリズムは，多項式時間アルゴリズムではないが，古典的アルゴリズムより計算量が遥かに少ない．Grover のアルゴリズムや Brassard らのアルゴリズムは，共通鍵暗号・ハッシュ関数の内部構造には全く依存していないので，最も汎用的な攻撃である．

共通鍵暗号は擬似ランダム置換にモデル化できるので，その内部構造の安全性をランダム置換との識別困難性の観点から古典的な評価が行われてきた．そのなかでも，多くの共通鍵暗号が採用している Feistel 構造とよばる内部構造については，最も理論的解析が進んでいる[6,8]．ランダム置換と識別困難であれば，選択平文攻撃または選択暗号文攻撃に対して理論的脆弱性がないことが保証される．

本研究では，共通鍵暗号の内部構造に着目して，量子アルゴリズムによる共通鍵暗号の安全性解析を行う．具体的には，2 ラウンドと 3 ラウンドの Feistel 構造をもつ暗号(Feistel 暗号)のランダム置換との識別困難性を検討する．その結果，いずれの場合においても，量子アルゴリズムを用いれば，識別するための計算量が古典アルゴリズムよりも少なくなることが判明した．2 ラウンド Feistel 暗号の場合，古典アルゴリズムでは，1 回のクエリで両者を識別することはできないが，量子アルゴリズムでは，1 回のクエリでも誤り確率高々0.275 で両者を識別することが可能である．3 ラウンド Feistel 暗号の場合，古典アルゴリズムでは，$O(2^{n/2})$ 回のクエリが必要だが，量子アルゴリズムでは，$O(2^{n/3})$ 回のクエリで両者を識別することが可能である．これらの結果から，量子アルゴリズムが利用可能な状況では，Feistel 暗号のラウンド数を多くする必要がある．

本報告書の構成は下記のとおりである．2 章で定義や従来研究をまとめる．3 章で，2 ラウンド Feistel 暗号に対する識別アルゴリズムを示し，その誤り確率を解析する．4 章で 3 ラウンド Feistel 暗号に対する識別アルゴリズムを示し，その誤り確率を解析する．5 章で，まとめと今後の課題を述べる．

2 準備

2-1 定義

全ての n ビット系列の集合を I_n とおく．I_n から I_n への 全ての関数の集合を F_n，全ての置換の集合を P_n とおく．定義から，$\mathrm{P}_n \subset \mathrm{F}_n$ である．F_n からランダムに選ばれた関数 F をランダム関数と呼び，P_n からランダムに選ばれた置換 P をランダム置換と呼ぶ．

r ラウンド Feistel 暗号は，図 1 のように定義される．図 1 において，$a^{(i)}$ と $b^{(i)}$ は n ビット系列であり，$F_1, F_2, \ldots, F_r$ は F_n の r 個のランダム関数である．r ラウンド Feistel 暗号は，I_{2n} 上の置換である．例えば，以前の米国標準共通鍵暗号 Data Encryption Standard (DES) は，16 ラウンド Feistel 暗号としてモデル化される．Feistel 暗号の変形として，ランダム関数 F_i の代わりに ランダム置換 P_i を用いることができる．この論文では，そのような変形も含めて Feistel 暗号と呼ぶことし，$FS_{T_1,\ldots,T_r}$ と書く．ここで，内部関数 T_i は，F_i または P_i である．

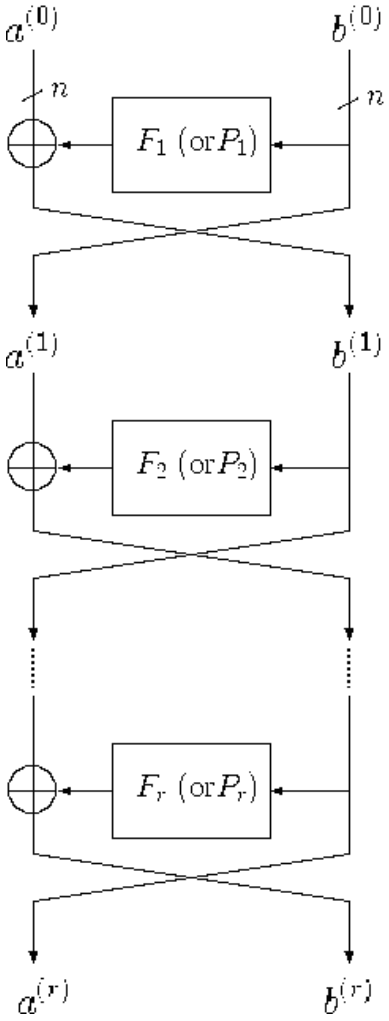

図 1　Feistel 暗号

r ラウンドFeistel暗号 $FS_{T_1,..,T_r}$ の安全性は，I_{2n} 上のランダム置換 RP との識別困難性で評価されてきた．

r ラウンドFeistel暗号またはランダム置換にオラクルとしてアクセスし，0または1を出力する敵 A を考える．Feistel暗号の識別困難性を以下のcpa-advantageで評価する．

$$\mathrm{Adv}^{\mathrm{cpa}}_{FS_{T_1,..,T_r}}(A) = \Pr\left[A^{FS_{T_1,..,T_r}} = 1\right] - \Pr\left[A^{RP} = 1\right].$$

ここで，敵 A は，内部関数 T_i にアクセスできないことに注意しよう．cpa-advantage は，敵 A による選択平文攻撃に対する安全性を評価しているとみなすことができる．[1] もし任意の敵 A に対して cpa-advantage が無視できる程小さいならば，r ラウンド Feistel 暗号はランダム置換と区別できない，つまり，r ラウンド Feistel 暗号は任意の選択平文攻撃に対して安全であることを意味する．

上記の cpa-advantage は，古典的アルゴリズムに基づく定義であるが，量子アルゴリズムに基づく定義に容易に変換できる．つまり，敵は，古典的オラクルの代わりに，ユニタリ演算子を使うことができるとし，二つのユニタリ演算子の識別する．一般的に，I_{2n} から I_{2n} への関数 V は，x, y を $2n$ キュービットとして，以下のユニタリ演算子 U_V として実現される．

$$U_V \mid x, y >= \mid x, y \oplus V(x) >,$$

[1] ‘cpa’ は，chosen plaintext attack(選択平文攻撃)の略である．

可逆性のため，演算子適用後の状態が入力xを含む必要がある．しかし，rラウンドFeistel暗号に対応するユニタリ演算子$U_{FS_{T_1,..,T_r}}$の場合，rラウンドFeistel暗号が置換であるから，演算子適用後の状態は入力xを含む必要はない．

$$U_{FS_{T_1,..,T_r}}|x>=|FS_{T_1,..,T_r}(x)>$$

同じ理由で，ランダム置換に対応するユニタリ演算子U_{RP}も

$$U_{RP}|x>=|RP(x)>.$$

と動作するユニタリ演算子を考えればよい．敵Aは，$U_{FS_{T_1,..,T_r}}$ または U_{RP}である ユニタリ演算子Uをブブラックボックスとして使うことができると仮定する．そのとき，Aのcpa-advantageを

$$\mathrm{Adv}^{\mathrm{cpa}}_{FS_{T_1,..,T_r}}(A)=\Pr\left[A^{U_{FS_{T_1,..,T_r}}}=1\right]-\Pr\left[A^{U_{RP}}=1\right].$$

と定義する．

2-2 古典的アルゴリズムによる識別困難性

Patarin［8］は，古典的アルゴリズムによるI_{2n}上のrラウンドFeistel暗号とランダム置換の識別困難性の結果を網羅的にまとめている．ここでは，2ラウンドFeistel暗号と3ラウンドFeistel暗号の結果を述べる．これら以上のラウンド数のFeistel暗号はこの論文では扱わない．

（1）2ラウンドFeistel暗号

Cを2ラウンドFeistel暗号またはランダム置換のオラクルとする，つまり，$C\in\{FS_{F_1,F_2},RP\}$．Cに質問を1回する敵Aを考える．このとき，Cは，どちらのオラクルであっても，I_{2n}の要素をランダムに一つ返すだけなので，任意の敵Aのcpa-advantageは，

$$\mathrm{Adv}^{\mathrm{cpa}}_{FS_{F_1,F_2}}(A)=\Pr\left[A^{FS_{F_1,F_2}}=1\right]-\Pr\left[A^{RP}=1\right]=0.$$

である．したがって，1回しか質問をしない場合，いかなる敵もランダムに0,1を出力する敵よりも 高い確率でそれらを識別することはできない．なお，内部関数をランダム置換に置き換えたとしても，敵Aのcpa-advantageは変わらない．

しかし，もし敵が質問を2回するならば，敵は2ラウンドFeistel暗号とランダム置換を非常に高い高い確率で 識別することができる[8]．

（2）3ラウンドFeistel暗号

Cを3ラウンドFeistel暗号またはランダム置換のオラクルとする，つまり，$C\in\{FS_{F_1,F_2,F_3},RP\}$．$C$に$O(2^{n/2})$回の質問をする敵$A$を考える．このとき，下記のcpa-advantageを持つ敵Aが存在する．

$$\mathrm{Adv}^{\mathrm{cpa}}_{FS_{F_1,F_2,F_3}}(A)=\Pr\left[A^{FS_{F_1,F_2,F_3}}=1\right]-\Pr\left[A^{RP}=1\right]=O(1).$$

このcpa-advantageは，3ラウンドFeistel暗号とランダム置換を高い確率で識別できる敵が存在することを意味する．そして，3ラウンドFeistel暗号とランダム置換を有意な確率で識別するためには，いかなる敵も$O(2^{n/2})$回以上の質問が 必要であることが証明されている[6,7]．

次に，3ラウンドFeistel暗号で二番めの内部関数がランダム置換の Feistel暗号 FS_{F_1,P_2,F_3}を考える．この場合，FS_{F_1,P_2,F_3}に対するcpa-advantageは，もう少し精密に評価することができる．AをCにq回質問する任意の敵とする．Aのcpa-advantageは，

$$\mathrm{Adv}^{\mathrm{cpa}}_{FS_{F_1,P_2,F_3}}(A)=\Pr\left[A^{FS_{F_1,P_2,F_3}}=1\right]-\Pr\left[A^{RP}=1\right]\le\frac{q(q-1)}{2^{n+1}}.$$

である．

2-2 古典的アルゴリズムによる識別困難性

本節では，4章でサブルーチンとして用いる Grover アルゴリズム[4]と Brassard らのアルゴリズム[2]を簡単に述べる．

（1）Groverアルゴリズム

Grover アルゴリズムは，I_n から $\{0,1\}$ への関数 $W(x)$ に対して，$W(x)=1$ となる x を発見する量子アルゴリズムである．関数 $W(x)$ に対応するユニタリ演算子を U_W とし， 平均値反転のためのユニタリ演算子を U_A とする．

$$U_A = H_n\left(2\,|0_n><0_n|-I_n\right)H_n,$$

ここで，H_n は n 次元アダマール変換行列，$|0_n>,<0_n|$ は n 次元の 0 に対応するケット，ブラベクトル，I_n は n 次元単位行列である．Grover アルゴリズムは，下記のとおり．

1. 状態 $|\varphi>=\frac{1}{2^{n/2}}\sum_{i\in\{0,1\}^n}|i>$ を用意する．
2. $|\varphi>$ に，U_AU_W を $O((2^n/r)^{1/2})$ 回適用する．ここで r は，$W(x)=1$ となる x の個数である．

$$|\psi>=U_AU_WU_AU_W\ldots U_AU_W\,|\varphi>$$

3. $|\psi>$ を測定し，その結果 z を出力する．

出力された z が $W(z)=1$ を満たす確率は，約 $1/2$ である．したがって，$O((2^n/r)^{1/2})$ 回 U_W を使用すれば，$W(x)=1$ を満たす x を発見することができる．

（２）Brassard らのアルゴリズム

F を F_n の関数とする．Brassard らのアルゴリズムは，$F(a)=F(x)$ となる a,x を発見する量子アルゴリズムである．このアルゴリズムは，Grover アルゴリズムをサブルーチンとして用いる．

1. $2^{n/3}$ 個の入力 x_i をランダムに選び，$y_i=F(x_i)$ を古典的に計算する．集合 S を
$$\mathrm{S}=\{(x_i,y_i)\,|\,i=1,2,\ldots,2^{n/3}\}$$
とする．
注意：この古典的計算によって，$F(x_i)=F(x_j)$ となる x_i,x_j が発見できる可能性はあるが，ここではそれは無視する．
2. I_n から $\{0,1\}$ への関数 $W(x)$ を下記のように定義する．
$$W(x)=\begin{cases}1 & \text{もし } y\in\mathrm{B} \text{ここで} y=F(x),\\ 0 & \text{上記以外}\end{cases}$$
3. 関数 $W(x)$ に対応するユニタリ演算子 U_W を考え，Grover アルゴリズムによって，$W(a)=1$ となる a を発見する．
4. $F(a)=F(x_i)$ となる x_i を集合 B の中から探し，a,x_i を出力する．

ステップ 1 で F の $2^{n/3}$ 回の計算が必要である．ステップ 3 で Grover アルゴリズムを使用するとき，ユニタリ演算子 U_W を $O(2^{n/3})$ 回使用することになる．

3 2 ラウンド Feistel 暗号の量子的識別困難性

この章では，量子アルゴリズムを用いれば，2 ラウンド Feistel 暗号とランダム置換が一回の質問で識別可能であることを示す．U_C を $U_{FS_{F_1,F_2}}$ または U_{RP} の ユニタリ演算子とする．このとき，下記のアルゴリズムの敵 A を考える．

1. 状態 $|a^{(0)}>|b^{(0)}>$ を準備する．

$$|a^{(0)}>|b^{(0)}>=\frac{1}{2^{(n+1)/2}}\left(\sum_{i\in\{0,1\}^n}|i>\right)\left(|0^{n-1}0>+|0^{n-1}1>\right),$$

ここで，$0^{n-1}=\overbrace{00\ldots0}^{n-1}$である．

2. $|a^{(0)}>|b^{(0)}>$にU_Cを作用させる．作用させた後の状態を$|a^{(2)}>|b^{(2)}>$とおく．

$$|a^{(2)}>|b^{(2)}>=U_C\,|a^{(0)}>|b^{(0)}>$$

3. $|a^{(2)}>|b^{(2)}>$の最も右側にあるキュービットを除いて，残りの$2n-1$キュービットを測定する．測定されたキュービットは固定されるので，今後は表記しない(測定結果は必要ない)．測定後の状態，つまり最も右側にあるキュービットの状態 を$|\varphi>$とおく．

4. アダマール基底$\{|+>,|->\}$を用いて，$|\varphi>$ を測定する．ここで，

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

である．

5. もし測定結果が$|+>$ならば，1 を出力し，そうでなければ，0 を出力する．
注意: ‘1’は，Cが 2 ラウンドFeistel 暗号であると推定したことを意味し，‘0’は，Cがランダム置換であると推定したことを意味する．

上記のアルゴリズムにおいて，Cが 2 ラウンドFeistel 暗号ならば，敵Aは常に 1 を出力する．なぜなら，$|a^{(2)}>|b^{(2)}>$ は，上記のアルゴリズムにおいて，

$$|a^{(2)}>|b^{(2)}>=\frac{1}{2^{(n+1)/2}}\sum_{i\in\{0,1\}^n}|i\oplus F_1(0^{n-1}0)>|0^{n-1}0\oplus F_2(i\oplus F_1(0^{n-1}0))>$$
$$+\frac{1}{2^{(n+1)/2}}\sum_{i\in\{0,1\}^n}|i\oplus F_1(0^{n-1}1)>|0^{n-1}1\oplus F_2(i\oplus F_1(0^{n-1}1))>.$$

であるから，ステップ 3 の測定後の状態は，常に

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

である．もしCがランダム置換ならば，Aが 1 を出力する確率は高々0.55 である(付録 A 参照)．よって，cpa-advantage は，

$$\mathrm{Adv}^{\mathrm{cpa}}_{FS_{F_1,F_2}}(A)=\Pr\left[A^{FS_{F_1,F_2}}=1\right]-\Pr\left[A^{RP}=1\right]\geq 0.45.$$

となる．Aの誤り確率を評価すると，

$$P_{err}=\Pr\left[1\,|\,C=RP\right]\Pr\left[C=RP\right]+\Pr\left[0\,|\,C=FS_{F_1,F_2}\right]\Pr\left[C=FS_{F_1,F_2}\right]$$
$$\leq\frac{1}{2}\cdot 0.55+0\cdot\frac{1}{2}=0.275.$$

となる．したがって，ユニタリ演算子を一回使用するだけで，敵は 2 ラウンドFeistel 暗号とランダム置換を誤り確率高々0.275で識別することができる．この誤り確率が良い近似値になっていることを計算機実験により確認した．

4 3 ラウンド Feistel 暗号の量子的識別困難性

この章では，$O(2^{n/3})$ 回のユニタリ演算子を使用すれば，3 ラウンド Feistel 暗号がランダム置換と識別可能であることを示す．この識別アルゴリズムは，Brassard らの衝突発見量子アルゴリズム[2]を利用している．C を FS_{F_1,P_2,F_3} または RP のオラクルとし，下記の敵 A を考えよう．

1. $a_i^{(0)}\ (i=1,2,\ldots,2^{n/3})$ をランダムに選び，$(a_i^{(2)},b_i^{(2)})=C(a_i^{(0)},0^n)$ を古典的に計算する．集合 B を
$$\mathrm{B}=\{b_i^{(2)}\mid i=1,2,\ldots,2^{n/3}\}$$
と定義する．
2. もしある i,j に対して，$b_i^{(2)}=b_j^{(2)}$ ならば 0 を出力する．
注意: 上式が成立する確率は非常に低いため，以下の解析では，任意の i,j に対して，$b_i^{(2)}\neq b_j^{(2)}$ を仮定する．
3. I_n から $\{0,1\}$ への 関数 $W(x)$ を下記のように定義する．
$$W(x)=\begin{cases}1 & \text{もし } z\in \mathrm{B} \text{ここで} (a,z)=C(x,0^n),\\ 0 & \text{上記以外.}\end{cases}$$
4. $r=0$ とする．r の最大値 q を定める．
5. Grover アルゴリズムを用いて，$W(u)=1$ なる u を見つける．もし Grover アルゴリズムが出力した u に対して $W(u)\neq 1$ ならば，つまり Grover アルゴリズムが失敗したならば，このステップを繰り返す．
6. $r\leftarrow r+1$.
7. もし任意の i に対して $u\neq a_i^{(0)}$ ならば，0 を出力する．もし $r<q$ ならば，ステップ 5 に戻り，そうでなければ 1 を出力する．
注意: ‘1’は，C が 3 ラウンド Feistel 暗号であると推定したことを意味し，‘0’は，C がランダム置換であると推定したことを意味する．

敵 A は，Grover アルゴリズムを 1 回実行するためにユニタリ演算子を $O(2^{n/3})$ 回使用する．ステップ 4 では，Grover アルゴリズムを平均 2 回使用するので，敵 A は，ユニタリ演算子を $O(2q2^{n/3})$ 回使用し，古典的計算を $2^{n/3}+2q$ 回行う．

C を 3 ラウンド Feistel 暗号 FS_{F_1,P_2,F_2} と仮定する．第二内部関数が置換 P_2 なので，ある i に対して $u=a_i^{(0)}$ が常に成立する．したがって，敵 A は必ず 1 を出力する．次に，C がランダム置換と仮定する．$RP(x,0^n)$ の右側の出力はランダム関数のように振る舞うので，$W(u)=1$ となる u は，平均で 2 個ある．従って，敵 A は確率 0.5 で 1 を出力する．以上より，敵 A の cpa-advantage は，

$$\mathrm{Adv}^{\mathrm{cpa}}_{FS_{F_1,P_2,F_3}}(A)=\Pr\left[A^{FS_{F_1,P_2,F_3}}=1\right]-\Pr\left[A^{RP}=1\right]\leq 1-2^{-q}.$$

となり，A の誤り確率 P_{err} of A は，

$$\begin{aligned}P_{err}&=\Pr[1\mid C=RP]\Pr[C=RP]+\Pr\left[0\mid C=FS_{F_1,P_2,F_3}\right]\Pr\left[C=FS_{F_1,P_2,F_3}\right]\\&\leq 2^{-(q+1)}.\end{aligned}$$

となる．繰り返し回数の上限 q に対して，誤り確率 P_{err} は指数関数的に小さくなるが，ユニタリ演算子の使用回数と古典的計算回数は 線形的にしか大きくならないことに注意しよう．

5 まとめ

2 ラウンド・3 ラウンド Feistel 暗号とランダム置換は，量子アルゴリズムを用いれば，古典的アルゴリズムよりも効率よく識別できることを示した．これらの結果は，量子的な選択平文攻撃は 古典的な選択平文攻撃よりも強力であること示している．

本論文で述べた 3 ラウンド Feistel 暗号に対する識別アルゴリズムは，Brassard らのアルゴリズムに基づ

いている．しかし，置換と関数の識別問題に関する Aaronson の解析[1]に従う量子アルゴリズムがあれば，3 ラウンド Feistel 暗号の識別に必要な計算量はさらに削減できる見込みがある．また，古典的な安全性解析によって 7ラウンドFeistel暗号まで識別可能性が定量的に評価されている.量子的アルゴズムを用いて，より多くのラウンドの Feistel 暗号とランダム置換の 識別可能性を検討することは，重要である．

謝辞　本研究を援助を頂きました 財団法人電気通信普及財団に深く感謝いたします.

付録 A　ランダム置換のときの確率

この付録では，I_{2n} 上のランダム置換からの 2^n 個の出力のうち，$2n-1$ ビットが等しくなる出力の組の確率を評価する．2^n 個の出力のうち，$2n-1$ ビットが等しくなる出力の組が k 組存在する事象を表す 確率変数を np とおき，その確率を $\Pr[\mathrm{np}=k]$ と書く．まず，$2n-1$ ビットが等しくなる出力の組が全くない確率 $\Pr[\mathrm{np}=0]$ は,

$$\Pr[\mathrm{np}=0]=\prod_{i=1}^{2^n-1}\left(1-\frac{i}{2^{2n}-i}\right)$$

である．両側不等式[2]を用いて，式(1)の上限と下限を評価する．

$$\Pr[\mathrm{np}=0]>\exp\left(-\sum_{i=1}^{2^n-1}\frac{i}{2^{2n}-2i}\right)>\exp\left(-\frac{1}{2^{2n}-2^{n+1}}\sum_{i=1}^{2^n-1}i\right)$$

$$>\exp\left(-\frac{1}{2}-\frac{1}{2(2^n-2)}\right)\to\exp\left(-\frac{1}{2}\right)\ (n\to\infty)$$

$$\Pr[\mathrm{np}=0]<\exp\left(-\sum_{i=1}^{2^n-1}\frac{i}{2^{2n}-i}\right)<\exp\left(-\frac{1}{2^{2n}}\sum_{i=1}^{2^n-1}i\right)$$

$$<\exp\left(-\frac{1}{2}+\frac{1}{2^{n+1}}\right)\to\exp\left(-\frac{1}{2}\right)\ (n\to\infty)$$

したがって，n が十分に大きいときには,

$$\Pr[\mathrm{np}=0]=\exp\left(-\frac{1}{2}\right)\approx 0.606$$

である.

[2] $0<t<1$ なる任意の t に対して，$\exp\left(-\frac{t}{1-t}\right)<1-t<\exp(-t)$ が成立する.

次に，$2n-1$ビットが等しくなる出力の組が一組存在する確率$\Pr[\mathrm{np}=1]$を評価する．その一組がa番目の出力とb番目の出力であると仮定し，その確率を$P_{a,b}$とおく．

$$
\begin{aligned}
P_{a,b} = 1\cdot\left(1-\frac{1}{2^{2n}-1}\right)\left(1-\frac{2}{2^{2n}-2}\right)\cdots\left(1-\frac{a-2}{2^{2n}-(a-2)}\right) \\
\left(1-\frac{a-1}{2^{2n}-(a-1)}\right)\left(1-\frac{a}{2^{2n}-a}\right)\cdots\left(1-\frac{b-2}{2^{2n}-(b-2)}\right) \\
\frac{1}{2^{2n}-(b-1)}\left(1-\frac{b-2}{2^{2n}-b}\right)\cdots\left(1-\frac{(2^n-1)-2}{2^{2n}-(2^n-1)}\right) \\
=\prod_{i=0}^{b-2}\left(1-\frac{i}{2^{2n}-i}\right)\frac{1}{2^{2n}-(b-1)}\prod_{i=b}^{2^n-1}\left(1-\frac{i-2}{2^{2n}-i}\right) \\
=\frac{1}{2^{2n}-1}\prod_{i=2}^{2^n-1}\left(1-\frac{i-2}{2^{2n}-i}\right)
\end{aligned}
$$

上式より，確率$P_{a,b}$は，その一組の出現位置a,bに依存しないことがわかる．その一組の取り方は$2^n(2^n-1)/2$通りあるので，確率$\Pr[\mathrm{np}=1]$は，

$$
\begin{aligned}
\Pr[\mathrm{np}=1] &= \frac{2^n(2^n-1)}{2}\frac{1}{2^{2n}-1}\prod_{i=2}^{2^n-1}\left(1-\frac{i-2}{2^{2n}-i}\right) \\
&= \frac{1}{2}\left(1-\frac{1}{2^n+1}\right)\prod_{i=2}^{2^n-1}\left(1-\frac{i-2}{2^{2n}-i}\right) \qquad (2)
\end{aligned}
$$

となる．式(2)を両側不等式を用いて評価する．

$$
\begin{aligned}
\prod_{i=2}^{2^n-1}\left(1-\frac{i-2}{2^{2n}-i}\right) &> \exp\left(-\sum_{i=2}^{2^n-1}\frac{i-2}{2^{2n}-2i+2}\right) \\
&> \exp\left(-\frac{1}{2^{2n}-2^{n+1}}\sum_{i=2}^{2^n-1}(i-2)\right) \\
&> \exp\left(-\frac{1}{2}+\frac{3}{2^{n+1}}\right)\to\exp(-\frac{1}{2})\ \ (n\to\infty)
\end{aligned}
$$

$$
\begin{aligned}
\prod_{i=2}^{2^n-1}\left(1-\frac{i-2}{2^{2n}-i}\right) &< \exp\left(-\sum_{i=2}^{2^n-1}\frac{i-2}{2^{2n}-i}\right) < \exp\left(-\frac{1}{2^{2n}}\sum_{i=2}^{2^n-1}(i-2)\right) \\
&< \exp\left(-\frac{1}{2}+\frac{5\cdot 2^n-6}{2^{2n+1}}\right)\to\exp\left(-\frac{1}{2}\right)\ \ (n\to\infty)
\end{aligned}
$$

したがって，nが十分に大きいときには，式(2)と上式より，

$$
\Pr[\mathrm{np}=1]=\frac{1}{2}\exp\left(-\frac{1}{2}\right)\approx 0.303
$$

となる．以上の結果を用いると，nが十分に大きいとき，ランダム置換で敵Aが1を出力する確率は，

$$
\begin{aligned}
\Pr\left[A^{RP}=1\right] &= \sum_{i=0}^{2^{n-1}} \Pr\left[A^{RP}=1 \mid \mathrm{np}=i\right]\Pr\left[\mathrm{np}=i\right] \\
&\le \Pr\left[A^{RP}=1 \mid \mathrm{np}=0\right]\Pr\left[\mathrm{np}=0\right] \\
&+\Pr\left[A^{RP}=1 \mid \mathrm{np}=1\right]\Pr\left[\mathrm{np}=1\right] \\
&+ \max_{i=2,..,2^{n-1}} \Pr\left[A^{RP}=1 \mid \mathrm{np}=i\right](1-\Pr\left[\mathrm{np}=0\right]-\Pr\left[\mathrm{np}=1\right]) \\
&\le \frac{1}{2}\cdot\exp\left(-\frac{1}{2}\right) \\
&+\left(\frac{1}{2^{n-1}}\cdot 1+\left(1-\frac{1}{2^{n-1}}\right)\frac{1}{2}\right)\frac{1}{2}\exp\left(-\frac{1}{2}\right) \\
&+1\cdot\left(1-\exp\left(-\frac{1}{2}\right)-\frac{1}{2}\exp\left(-\frac{1}{2}\right)\right) \\
&\to 1-\frac{3}{4}\exp\left(-\frac{1}{2}\right)\approx 0.545 \ \ (n\to\infty)
\end{aligned}
$$

よって, n が十分に大きいと仮定すると, ランダム置換のとき, 敵 A が 1 を出力する確率は高々0.55 である. 56 ビットの擬似ランダム置換を作成し, 確率 $\Pr\left[\mathrm{np}=k\right]$ を計算機実験により求めた結果を表 1 に示す. この表から, 上記の解析結果と実験値がよく一致していることがわかる. 実験値によれば, ランダム置換で敵 A が 1 を出力する確率は, 0.5 と推定される.

表 1　計算機実験による組数と確率

k	確率 $\Pr\left[\mathrm{np}=k\right]$
0	0.61008
1	0.30236
2	0.07359
3	0.01261
4	0.00117
5	0.00011
6	0.00005

【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] G. Brassard , P. H?yer , and A. Tapp , “Quantum algorithm for the collision problem,” quant-ph/9705002, 1997.

[3] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Transactions on Information Theory, vol. IT-31, no. 4, pp. 469–472, July 1985.

[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] A. Klimov and A. Shamir, “Cryptographic applications of T-functions,” Selected Area in Cryptography, SAC 2003, Lecture Notes in Computer Science, vol. 3006, pp. 248–261, 2004.

[6] M. Luby and C. Rackoff, "How to construct pseudorandom permutations from pseudorandom functions," SIAM Journal on Computing, vol. 17, no. 2, April 1998.
[7] U. M. Maurer, "A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generators," Advances in Cryptology - EUROCRYPT '92, Lecture Notes in Computer Science, vol. 658, pp. 239–255, 1993.
[8] J. Patarin, "Generic attacks on Feistel schemes," Cryptology ePrint Archive, Report 2008/036, 2008.
[9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, pp. 120–126, 1978.
[10] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, pp. 124–134, 1994.

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
量子アルゴリズムによる Feistel 暗号の安全性解析	電子情報通信学会情報理論研究会	2009 年 7 月