4.3 暗号解読に関係するアルゴリズム

ここでは、暗号解読に関係する量子アルゴリズムとして、素因数分解問題、離散対数問題、及び楕円曲線上の離散対数問題に対する多項式時間アルゴリズムを説明する。

素因数分解問題に対する量子アルゴリズムの説明[17]

問題

整数 $n = pq$（p、q は素数）を素因数分解する

アプローチ

次の２つのステップで素因数分解を行う。量子アルゴリズムは(1)の部分のみ。

(1)量子計算を用いた高速な 周期（period）の計算（Shor のアルゴリズム）

次の関数の周期 r を計算する。 $f_{x,n}(a) = x^a \bmod n$ 。

(2)周期から因数を古典的な高速な手法で計算（Euclid アルゴリズム）

n の因数（i.e. p, q)を、$\gcd(x^{r/2}-1, n)$ と $\gcd(x^{r/2}+1, n)$ を計算して得る

数論的説明

(1)素因数因数分解したい整数 n が与えられたとき、次の関数 $f_{x,n}(a)$ を構成する

$f_{x,n}(a) = x^a \bmod n$

但し、 x は n と互いに素でランダムに選ばれた整数とする。

(2) 周期 r（すなわち $x^r \equiv 1 \bmod n$ なる r ）を見つける

(3) もし 周期 r が偶数の場合、$(x^{r/2}-1)(x^{r/2}+1) \equiv 0 \bmod n$ となる。

この時、もし $x^{r/2} \equiv \pm 1 \bmod n$ でなければ、少なくとも上式の左辺の少なくとも一方は、n の非自明な因数を持たなくてはいけない。

(4)よって、$\gcd(x^{r/2}-1, n)$ and $\gcd(x^{r/2}+1, n)$ を計算することによって n の因数を見つけることができる。

アプローチの(1)のみ量子計算であるため、この部分の量子アルゴリズムを説明する。

量子計算を用いた高速な周期の計算（Shor のアルゴリズム）

周期rを計算する。 即ち $f_{x,n}(a) = x^a \bmod n$ として、 $f(a+r) = f(a)$ なる周期rを計算する。xとnが与えられたとき、上記のような周期rを見つけるため 次のアルゴリズムを実行する。

アルゴリズム

Step1. $2n^2 \le Q < 4n^2$ を満たすスムーズ（smooth）なQを見つける。

スムーズなQを選んだ理由は、あとの step で、多項式時間で構成される量子離散フーリエ変換QFT_Qを使用するため。

Step2 量子離散フーリエ変換QFT_Qを基底状態$|00\rangle$に作用させて、重ね合わせ状態$|\psi_{init}\rangle$を作り出す

ここで離散フーリエ変換は$QFT_Q|a\rangle = \frac{1}{\sqrt{Q}}\sum_{c=0}^{Q-1}\exp(2\pi iac/Q)|c\rangle$で与えられる。

$$QFT_Q:\ |00\rangle \ \rightarrow \quad |\psi_{init}\rangle = \frac{1}{\sqrt{Q}}\sum_{a=0}^{Q-1}|a\rangle|0\rangle$$

Step3 $x^a \bmod n$ の値を計算して、第 2 レジスタに格納する。

（ここで、$f(x) = x^a \bmod n$ と考えればよく、ユニタリ変換U_fを作用させる）

$$U_f|\psi_{init}\rangle = \frac{1}{\sqrt{Q}}\sum_{a=0}^{Q-1}|a\rangle|x^a (\bmod n)\rangle$$

Step4 周期rを取り出すために離散フーリエ変換QFT_Qを作用させる。

$$QFT_Q \cdot U_f|\psi_{init}\rangle == \frac{1}{Q}\sum_{c=0}^{Q-1}\sum_{a=0}^{Q-1}\exp(2\pi iac/Q)|c\rangle|x^a (\bmod n)\rangle$$

Step5 第 1 レジスタの物理量 c を観測する。

このとき、 $\left|c, x^k \pmod n\right\rangle$ の状態を観測する確率 Pr は下記で与えられる。

$$\Pr = \left| \frac{1}{Q} \sum_{\substack{a \\ x^a \equiv x^k \bmod n}} \exp(2\pi i a c / Q) \right|^2$$

この確率は、周期 r が下記の条件のときに大きなピークを持つ。すなわち(1)の条件を満たすか、ほぼその関係を満たす状態しか観測にかからないといえる。

(1) $Q \mid A = \lfloor (Q-k)/r \rfloor$ なら、r_i が $r_i \cdot c = k \cdot Q$ を満たすとき

(2) (1)でないときは、r_i が $r_i \cdot c = k \cdot Q$ を満たす値の近傍のとき

Step6 観測した値 c から周期 r を得る

このような観測（c を得る）を $\log N$ 回の繰り返すと、周期 r が得られる（$r_i \cdot c \cong k \cdot Q$ なる関係を考慮して求める）

以上が Shor の周期 r を多項式時間で求める量子アルゴリズムである。周期 r を求めると古典計算機上の Euclid アルゴリズムから、多項式時間で n の因数 p, q が確率的に求めることができる。

古典計算機で素因数分解問題を解く場合、計算量が $O(\exp(\log n \log\log n)^{1/2})$ の準指数時間アルゴリズムまでしか知られておらず、量子計算アルゴリズムの方が高速処理できることになる。

離散対数問題に対する量子アルゴリズムの説明[17]

問題

素数 p 、 $F_p^{\times}$ の生成元 g 、 $y(=g^x \bmod p)$ が与えられた時、離散対数 x を求める

但し、これから説明するアルゴリズムは、 $p-1$ がスムーズ（smooth）の時の場合を説明する。この場合を easy case という。

アルゴリズム

Step1 量子離散フーリエ変換 QFT_{p-1} を基底状態 $|0\rangle|0\rangle$ に作用させて、重ね合わせ状態 $|\psi_{init}\rangle$ を作る

ここで、離散フーリエ変換は $QFT_{p-1}|a\rangle = \frac{1}{\sqrt{p-1}}\sum_{a=0}^{p-2}\exp(2\pi iac/(p-1))|c\rangle$,

で与えられる。

$$QFT_{p-1}\otimes QFT_{p-1}:\ |0\rangle|0\rangle\ \rightarrow\ |\psi_{init}\rangle = \frac{1}{p-1}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}|a\rangle|b\rangle$$

Step2 $g^a y^{-b} \bmod p$ の値を計算して、第 3 レジスタに格納する

（ $f(x) = g^a y^{-b} \bmod p$ と考えればよく、ユニタリ変換 U_f を作用させる）

$$U_f:|\psi_{init}\rangle\ \rightarrow\ \frac{1}{p-1}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}|a\rangle|b\rangle|g^a y^{-b} \bmod p\rangle$$

Step3 量子離散フーリエ変換 QFT_{p-1} を第 1 レジスタ、第 2 レジスタに作用させる

その結果下記の状態となる

$$QFT_{p-1}\otimes QFT_{p-1}\otimes I:$$

$$\frac{1}{(p-1)^2}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}\sum_{c=0}^{p-2}\sum_{d=0}^{p-2}\exp(\frac{2\pi i}{p-1}(ac+bd))|c\rangle|d\rangle|g^a y^{-b} \bmod p\rangle$$

Step4 第 1 レジスタの物理量 c、第 2 レジスタの物理量 d を観測する

このとき、$\left|c,d,y\equiv g^{k} \bmod p\right\rangle$ の状態を観測する確率 Pr は下記で与えられる。

$$\Pr=\left|\frac{1}{(p-1)^{2}}\sum_{\substack{a,b\\ a-xb\equiv k \bmod(p-1)}}\exp(\frac{2\pi i}{p-1}(ac+bd))\right|^{2}$$

$$=\left|\frac{1}{(p-1)^{2}}\sum_{b=0}^{p-2}\exp(\frac{2\pi i}{p-1}(kc+b(d+xc)))\right|^{2}$$

Step5 観測すると、 $\left|c\right\rangle\left|-xc(=d)\right\rangle\left|y\right\rangle$ という状態が確率 $\frac{1}{(p-1)^{2}}$ で得られる

$d+xc\neq 0 \bmod(p-1)$ のとき、確率 Pr は 0、即ち観測されない

$d+xc\equiv 0 \bmod(p-1)$ のとき、確率 Pr は 0 でない値となり観測される

Step6 c と $p-1$ が互いに素のとき、x は観測値 c と d より、それらの逆元演算と乗算で求められる。

すなわち x、c、d は、$d\equiv -xc \bmod(p-1)$ なる関係式を満たしているため、

$x\equiv(-d)\cdot c^{-1} \bmod(p-1)$ の計算をすることで離散対数 x が求まる。

なお Step6 では、観測値 c が $p-1$ と互いに素のとき逆元 $c^{-1} \bmod(p-1)$ が存在して、離散対数 x が求まる。観測値 c が $p-1$ と互いに素となるような確率は、Euler 関数 Φ 及びその性質から次のように評価できる。

$$\Phi(p-1)/(p-1)\cong e^{-\gamma}/(\log\log p)>1/\log p$$

すなわち、$\log p$ 回操作を繰り返すと、c が $p-1$ と互いに素となり x が求まる。

但し上記のアルゴリズムは easy case の説明である。この時、古典計算機上でも多項式アルゴリズムが存在する(Pohlig-Hellman 法)。easy case ではなく、一般の場合も Shor により同様にして多項式時間アルゴリズムが示されている[17]。

古典計算機では、離散対数問題を解くアルゴリズムの計算量のオーダとしては、$O(\exp(\log p\log\log p)^{1/2})$ の準指数時間要し、量子アルゴリズムの方が高速である。

Boneh-Lipton の論文[27]より、容易に一般の群の離散対数問題にも量子アルゴリズムは適用可能である。すなわち例えば楕円曲線暗号に関しても多項式時間で解読が可能であることが言える[27]。次に示す。

楕円曲線上の離散対数問題に対する量子アルゴリズムの説明[27,29]

問題

E を下記で定義される楕円曲線とする。

$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ （$a_1, a_2, a_3, a_4, a_6 \in F_q$）

F_q（但し、$q = p^m$、p は素数）は有限体である。またここで、$P \in E(F_q)$ を大きな素数 n を位数にもつ base point として、R を $R = rP$ なる楕円曲線上の r 倍点とする。このとき、楕円曲線上の離散対数問題とは、R と P が与えられたとき、$R = rP$ なる r を求める問題である。

アルゴリズム

Step1 $n \le Q < 2n$ を満たすスムーズ（smooth）な Q を見つける

但し、n は位数で $n = \#< P >$ である。また、スムーズな Q を選んだ理由は、あとで多項式時間で構成される量子離散フーリエ変換 QFT_Q を使用するため。

Step2 第 1 レジスタと第 2 レジスタのそれぞれに重ね合わせ状態 $|\psi_{init}\rangle$ を作り出す

$$|\psi_{init}\rangle = \frac{1}{n}\sum_{a=0}^{n-1}\sum_{b=0}^{n-1}|a\rangle|b\rangle$$

但し P は basepoint。

Step3 $aP - bR$ の値を計算して、第 3 レジスタに格納する

（$f(x) = aP - bR$ と考えればよく、ユニタリ変換 U_f を作用させる）

$$\frac{1}{n}\sum_{a=0}^{n-1}\sum_{b=0}^{n-1}|a\rangle|b\rangle|aP - bR\rangle \qquad \text{但し } R = rP$$

Step4 量子離散フーリエ変換 QFT_Q を第 1 レジスタ、第 2 レジスタに作用させる

ここで、離散フーリエ変換は

$QFT_Q|a\rangle = \frac{1}{\sqrt{Q}}\sum_{a=0}^{n-1}\exp(2\pi iac/Q)|c\rangle$ で与えられる。

$$QFT_Q \otimes QFT_Q \otimes I : \frac{1}{qn}\sum_{a=0}^{n-1}\sum_{b=0}^{n-1}\sum_{c=0}^{Q-1}\sum_{d=0}^{Q-1}\exp(\frac{2\pi i}{Q}(ac+bd)|c\rangle|d\rangle|aP-bR\rangle$$

Step4 第 1 レジスタの物理量 c、第 2 レジスタの物理量 d を観測する

このとき、$|c,d,K=kP\rangle$ の状態を観測する確率 Pr は下記で与えられる。

$$\Pr = \left|\frac{1}{nQ}\sum_{\substack{a,b \\ a-rb\equiv k}}\exp(\frac{2\pi i}{Q}(ac+bd))\right|^2$$

以下 Shor の離散対数問題アルゴリズムの議論と同様にこの値を評価し、$R=rP$ なる r を多項式時間で得ることができる。

また暗号解読に関連して Grover のデータベース検索アルゴリズムを秘密鍵暗号に適用することを考えると、全数探索の平方根の計算量で解読できる。すなわち例えば鍵が 64bit のブロック暗号の場合は、2^{32} の探索で解読できる。128bit ブロック暗号の場合は、2^{64} の探索で解読できることになる。