高次方程式と対称式を用いた公開鍵暗号

高次対称式暗号

素数を法とする剰余体 K 上の n 次方程式

$$x^n-\sigma_1 x^{n-1}+\sigma_2 x^{n-2}-\cdots+(-1)^n\sigma_n=0\cdots①$$

で，K 上に解を持たないものを考える。このとき，この方程式は K の拡大体を考えれば，その拡大体上に解 α_1，α_2，α_3，…，α_n を持つ。①は

$$x^n-\sigma_1 x^{n-1}+\sigma_2 x^{n-2}-\cdots+(-1)^n\sigma_n=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_n)$$

と変形できる。展開して係数を比較すると，解と係数の関係

$$\sigma_1=\alpha_1+\alpha_2+\cdots+\alpha_n$$

$$\sigma_2=\alpha_1\alpha_2+\cdots+\alpha_{n-1}\alpha_n$$

$$\sigma_3=\alpha_1\alpha_2\alpha_3+\cdots+\alpha_{n-2}\alpha_{n-1}\alpha_n$$

$$\cdots\cdots\cdots\cdots$$

$$\sigma_n=\alpha_1\alpha_2\alpha_3\cdots\alpha_n$$

が得られる。

ここで，p を自然数とし，方程式

$$(x-\alpha_1^p)(x-\alpha_2^p)(x-\alpha_3^p)\cdots(x-\alpha_n^p)=0$$

を考える。展開すると

$$x^n-\sigma(p,1)x^{n-1}+\sigma(p,2)x^{n-2}-\cdots+(-1)^n\sigma(p,n)=0$$

の形になる。このとき

$$\sigma(p,1)=\alpha_1^p+\alpha_2^p+\cdots+\alpha_n^p$$

$$\sigma(p,2)=\alpha_1^p\alpha_2^p+\cdots+\alpha_{n-1}^p\alpha_n^p$$

$$\sigma(p,3)=\alpha_1^p\alpha_2^p\alpha_3^p+\cdots+\alpha_{n-2}^p\alpha_{n-1}^p\alpha_n^p$$

$$\cdots\cdots\cdots\cdots$$

$$\sigma(p,n)=\alpha_1^p\alpha_2^p\alpha_3^p\cdots\alpha_n^p$$

対称式は基本対称式で表されるから

$\sigma(p,1)$，$\sigma(p,2)$，$\sigma(p,3)$，…，$\sigma(p,n)$ は σ_1，σ_2，σ_3，…，σ_n

で表される。さらに，q を自然数とするとき，指数法則

$$\alpha_i^{pq}=(\alpha_i^p)^q=(\alpha_i^q)^p \qquad (i=1,2,3,\cdots,n)$$

が成り立つ。対称式は基本対称式で表されるから

$\sigma(p,1)$，$\sigma(p,2)$，$\sigma(p,3)$，…，$\sigma(p,n)$ は $\sigma(pq,1)$，$\sigma(pq,2)$，$\sigma(pq,3)$，…，$\sigma(pq,n)$

$\sigma(q,1)$，$\sigma(q,2)$，$\sigma(q,3)$，…，$\sigma(q,n)$ は $\sigma(qp,1)$，$\sigma(qp,2)$，$\sigma(qp,3)$，…，$\sigma(qp,n)$

で表される。このとき

$$\sigma(pq,i)=\sigma(qp,i) \qquad (i=1,2,3,\cdots,n)$$

が成り立つ。したがって

σ_1，σ_2，σ_3，…，σ_n から $\sigma(p,1)$，$\sigma(p,2)$，$\sigma(p,3)$，…，$\sigma(p,n)$

が高速に求められれば，Elgamal 暗号が構成できる。

解の累乗和の高速計算法

①の解の 1 つを α とすると

$$\alpha^n=\sigma_1\alpha^{n-1}-\sigma_2\alpha^{n-2}+\cdots+(-1)^{n-1}\sigma_n\cdots②$$

を満たすから，p を n より大きい自然数とするとき，②を繰り返し用いて次数を下げていけば

$$\alpha^{p}=\alpha^{p-n}\alpha^{n}$$
$$=\alpha^{p-n}\{\sigma_1\alpha^{n-1}-\sigma_2\alpha^{n-2}+\cdots+(-1)^{n-1}\sigma_n\}$$
$$=\sigma_1\alpha^{p-1}-\sigma_2\alpha^{p-2}+\cdots+(-1)^{n-1}\sigma_n\alpha^{p-n}$$
$$\cdots\cdots\cdots\cdots$$
$$=c(p,\ 1)\alpha^{n-1}+c(p,\ 2)\alpha^{n-2}+\cdots+c(p,\ n)\cdots③$$

と表すことができる。これを高速に計算する方法を示す。

p を任意の自然数とするとき，p を 2 進法で表す。

$$p=(\cdots(((s_0\cdot 2+s_1)\cdot 2+s_2)\cdot 2+s_3)\cdot 2+\cdots)\cdot 2+s_p$$

ただし，s_i は 0 か 1 の値をとり，$s_0\neq 0$ である。(バイナリー法)

α^{i} から α^{i+1} と α^{i} から α^{2i} が高速に計算できればバイナリー法により α^{p} が高速に計算できる。

α^{i} から α^{i+1}

$$\alpha^{i+1}=\alpha^{i}\alpha=c(i,\ 1)\alpha^{n}+c(i,\ 2)\alpha^{n-1}+\cdots+c(i,\ n)\alpha$$

であるから，②を用いて次数下げをすれば c(i＋1，1)，c(i＋1，2)，…，c(i＋1，n) が求まる。

α^{i} から α^{2i}

$$\alpha^{2i}=(\alpha^{i})^2=\{c(i,\ 1)\alpha^{n-1}+c(i,\ 2)\alpha^{n-2}+\cdots+c(i,\ n)\}^2$$

であるから，これを展開して②を用いて次数下げをすれば c(2i，1)，c(2i，2)，…，c(2i，n) が求まる。

次に，α_1，α_2，α_3，…，α_n の累乗和を求めよう。

③より

$$\alpha_1{}^{p}=c(p,\ 1)\alpha_1{}^{n-1}+c(p,\ 2)\alpha_1{}^{n-2}+\cdots+c(p,\ n)$$
$$\alpha_2{}^{p}=c(p,\ 1)\alpha_2{}^{n-1}+c(p,\ 2)\alpha_2{}^{n-2}+\cdots+c(p,\ n)$$
$$\cdots\cdots\cdots\cdots$$
$$\alpha_n{}^{p}=c(p,\ 1)\alpha_n{}^{n-1}+c(p,\ 2)\alpha_n{}^{n-2}+\cdots+c(p,\ n)$$

これらを足し，α_1，α_2，α_3，…，α_n の累乗和を

$$S_j=\alpha_1{}^{j}+\alpha_2{}^{j}+\cdots+\alpha_n{}^{j}\quad(j=0,\ 1,\ 2,\ \cdots,\ n)$$

とすると

$$S_p=c(p,\ 1)S_{n-1}+c(p,\ 2)S_{n-2}+\cdots+n\cdot c(p,\ n)$$

同様にして S_p，S_{2p}，S_{3p}，…，S_{np} の n 個の値が求まる。これら n 個の値を求めるための計算量は，$O(n^3)$ である。

累乗和と基本対称式の関係

次に，解 α_1，α_2，α_3，…，α_n の基本対称式

$$\sigma_1,\ \sigma_2,\ \sigma_3,\ \cdots,\ \sigma_n$$

と，解の累乗和(n 変数対称式)

$$S_j=\alpha_1{}^{j}+\alpha_2{}^{j}+\cdots+\alpha_n{}^{j}\quad(j=0,\ 1,\ 2,\ \cdots,\ n)$$

の関係を求めよう。

予備定理

$$S_n-\sigma_1S_{n-1}+\sigma_2S_{n-2}-\sigma_3S_{n-3}+\cdots+(-1)^{n}n\sigma_n=0$$

証明

x の多項式の等式

$$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_n)=x^n-\sigma_1x^{n-1}+\sigma_2x^{n-2}-\sigma_3x^{n-3}+\cdots+(-1)^n\sigma_n$$

は恒等式であるから，$x=\alpha_1$，$x=\alpha_2$，　$x=\alpha_3$，　…，$x=\alpha_n$をそれぞれ代入すると

$$\alpha_1{}^n-\sigma_1\alpha_1{}^{n-1}+\sigma_2\alpha_1{}^{n-2}-\sigma_3\alpha_1{}^{n-3}+\cdots+(-1)^n\sigma_n=0$$

$$\alpha_2{}^n-\sigma_1\alpha_2{}^{n-1}+\sigma_2\alpha_2{}^{n-2}-\sigma_3\alpha_2{}^{n-3}+\cdots+(-1)^n\sigma_n=0$$

……

$$\alpha_n{}^n-\sigma_1\alpha_n{}^{n-1}+\sigma_2\alpha_n{}^{n-2}-\sigma_3\alpha_n{}^{n-3}+\cdots+(-1)^n\sigma_n=0$$

これらを足して

$$S_n-\sigma_1S_{n-1}+\sigma_2S_{n-2}+\cdots+(-1)^{n-1}\sigma_{n-1}S_1+(-1)^n n\sigma_n=0$$

証明終

定理　(ニュートンの公式)

α_1，α_2，α_3，…，α_nの対称式σ_i，S_iについて，$k\leqq n$である任意の自然数 k において

$$S_k-\sigma_1S_{k-1}+\sigma_2S_{k-2}+\cdots+(-1)^{k-1}\sigma_{k-1}S_1+(-1)^k k\sigma_k=0$$

証明

対称式

$$S_k-\sigma_1S_{k-1}+\sigma_2S_{k-2}+\cdots+(-1)^{k-1}\sigma_{k-1}S_1+(-1)^k k\sigma_k$$

は，k 次の多項式であるか，　0　である。

この対称式において　$\alpha_{k+1}=\alpha_{k+2}=\alpha_{k+3}=\cdots=\alpha_n=0$　すると，α_1，$\alpha_2\alpha_3$，…，α_kの対称式となるが，これは，予備定理により　0　となる。

ところが，α_1，α_2，α_3，…，α_nの対称式で k 次の多項式であるものの各項は，k 文字以下の異なる文字しか含まないから，α_1，α_2，α_3，…，α_kだけの文字でできた項が必ずある。

したがって，$\alpha_{k+1}=\alpha_{k+2}=\alpha_{k+3}=\cdots=\alpha_n=0$としても，この項は残り，決して　0　にはならない。

ゆえに

$$S_k-\sigma_1S_{k-1}+\sigma_2S_{k-2}+\cdots+(-1)^{k-1}\sigma_{k-1}S_1+(-1)^k k\sigma_k=0$$

証明終

この公式により，累乗和を基本対称式を用いて求めるアルゴリズムができる。

$$S_1=\sigma_1$$

$$S_2=\sigma_1S_1-2\sigma_2$$

$$S_3=\sigma_1S_2-\sigma_2S_1+3\sigma_3$$

……

$$S_n=\sigma_1S_{n-1}-\sigma_2S_{n-2}+\cdots+(-1)^n\sigma_{n-1}S_1+(-1)^{n+1}n\sigma_n$$

変形すると，逆に，基本対称式を累乗和を用いて求めるアルゴリズムができる。

$$\sigma_1=S_1$$

$$\sigma_2=-(S_2-\sigma_1S_1)\cdot 2^{-1}$$

$$\sigma_3=(S_3-\sigma_1S_2+\sigma_2S_1)\cdot 3^{-1}$$

……

$$\sigma_n=(-1)^{n+1}\{S_n-\sigma_1S_{n-1}+\sigma_2S_{n-2}-\cdots+(-1)^{n-1}\sigma_{n-1}S_1\}\cdot n^{-1}$$

いずれも計算量は，$O(n^2)$である。

注　この方法が使えるのはn^{-1}が存在するときであるから，

素体 K の位数$\geqq n+1$

であることが必要である。

$\sigma(p,\ 1),\ \sigma(p,\ 2),\ \sigma(p,\ 3),\ \cdots,\ \sigma(p,\ n)$の高速計算法

ニュートンの公式を用いると

$\sigma_1,\ \sigma_2,\ \sigma_3,\ \cdots,\ \sigma_n$ から $S_1,\ S_2,\ S_3,\ \cdots,\ S_n$

が求まり，さらに累乗の計算により

$S_1,\ S_2,\ S_3,\ \cdots,\ S_n$ から $S_p,\ S_{2p},\ S_{3p},\ \cdots,\ S_{np}$

が求まるから，再びニュートンの公式を用いて

$S_p,\ S_{2p},\ S_{3p},\ \cdots,\ S_{np}$ から $\sigma(p,\ 1),\ \sigma(p,\ 2),\ \sigma(p,\ 3),\ \cdots,\ \sigma(p,\ n)$

が求まる。

すなわち

$\sigma_1,\ \sigma_2,\ \sigma_3,\ \cdots,\ \sigma_n$ から $\sigma(p,\ 1),\ \sigma(p,\ 2),\ \sigma(p,\ 3),\ \cdots,\ \sigma(p,\ n)$

を求めることができる。

公開鍵暗号の作成

暗号文受信者の初期設定

1.体 K 上の乱数 $\sigma_1,\ \sigma_2,\ \sigma_3,\ \cdots,\ \sigma_{n-1}$ を生成する。ただし，$\sigma_n=1$ とする。また，乱数 $\sigma_1,\ \sigma_2,\ \sigma_3,\ \cdots,\ \sigma_{n-1}$ は周期が最大となるようにとり，p は周期以下の数とする。

2.乱数 $p \in N$ を生成する。

3. $\sigma_1,\ \sigma_2,\ \sigma_3,\ \cdots,\ \sigma_n$ から $\sigma(p,\ 1),\ \sigma(p,\ 2),\ \sigma(p,\ 3),\ \cdots,\ \sigma(p,\ n-1)$ を求める。

4. $\sigma_1,\ \sigma_2,\ \sigma_3,\ \cdots,\ \sigma_n$ と $\sigma(p,\ 1),\ \sigma(p,\ 2),\ \sigma(p,\ 3),\ \cdots,\ \sigma(p,\ n-1)$ を公開する。

p が秘密鍵であり，$\sigma_1,\ \sigma_2,\ \sigma_3,\ \cdots,\ \sigma_{n-1}$ と $\sigma(p,\ 1),\ \sigma(p,\ 2),\ \sigma(p,\ 3),\ \cdots,\ \sigma(p,\ n-1)$ が公開鍵である。

暗号文送信者の作業

1. 乱数 $q \in N$ を生成する・

2. $\sigma_1,\ \sigma_2,\ \sigma_3,\ \cdots,\ \sigma_{n-1}$ から $\sigma(q,\ 1),\ \sigma(q,\ 2),\ \sigma(q,\ 3),\ \cdots,\ \sigma(q,\ n-1)$を計算する。

3. $\sigma(p,\ 1),\ \sigma(p,\ 2),\ \sigma(p,\ 3),\ \cdots,\ \sigma(p,\ n-1)$ から

$\sigma(pq,\ 1),\ \sigma(pq,\ 2),\ \sigma(pq,\ 3),\ \cdots,\ \sigma(pq,\ n-1)$ を計算する。

4.平文を M とし，$\sigma(pq,\ 1),\ \sigma(pq,\ 2),\ \sigma(pq,\ 3),\ \cdots,\ \sigma(pq,\ n-1)$を共通鍵暗号の秘密鍵として M を暗号化した M'を作る。

5. $\sigma(q,\ 1),\ \sigma(q,\ 2),\ \sigma(q,\ 3),\ \cdots,\ \sigma(q,\ n-1)$ と M'を送信する。

暗号文受信者の復号処理

1. $\sigma(q,\ 1),\ \sigma(q,\ 2),\ \sigma(q,\ 3),\ \cdots,\ \sigma(q,\ n-1)$ から

$\sigma(pq,\ 1),\ \sigma(pq,\ 2),\ \sigma(pq,\ 3),\ \cdots,\ \sigma(pq,\ n-1)$ を計算する。

2. $\sigma(pq,\ 1),\ \sigma(pq,\ 2),\ \sigma(pq,\ 3),\ \cdots,\ \sigma(pq,\ n-1)$を共通鍵暗号の秘密鍵として M'から M を復号する。

注意　$\sigma_n=1$ としたのは，$\alpha_1\alpha_2\alpha_3\cdots\alpha_n$ と $(\alpha_1\alpha_2\alpha_3\cdots\alpha_n)^p$ を共に公開するため，p についての情報を与えるからである。このとき，

$\alpha_1\alpha_2\alpha_3\cdots\alpha_n=1$　から　$\alpha_1{}^p\alpha_2{}^p\alpha_3{}^p\cdots\alpha_n{}^p=1$

となり

$$\sigma(p,\ n)=\sigma(q,\ n)=\sigma(pq,\ n)=1$$

が成り立つ。

周期についての考察

$p\neq 0$ として，任意の整数 k について

$$(\alpha_1{}^{k+p},\ \alpha_2{}^{k+p},\ \alpha_3{}^{k+p},\ \cdots,\ \alpha_n{}^{k+p})=(\alpha_1{}^{k},\ \alpha_2{}^{k},\ \alpha_3{}^{k},\ \cdots,\ \alpha_n{}^{k})$$

を満たすとき，p を周期という。これは

$$(\alpha_1{}^{p},\ \alpha_2{}^{p},\ \alpha_3{}^{p},\ \cdots,\ \alpha_n{}^{p})=(1,\ 1,\ 1,\ \cdots,\ 1)$$

となることと同値である。

ここでは，正の周期だけを考える。

周期のうち最小なものを，基本周期という。このとき，次の定理が成り立つ。

定理

すべての周期は基本周期の倍数である。

証明

基本周期を T とし，T でないある周期を p とすると，$p>T$ より，整数 m を用いて

$$p=Tm+r\quad(0\leqq r<T)$$

と表されるから

$$r=p-Tm$$

となる。T,p は共に周期であるから

$$\begin{aligned}(\alpha_1{}^{k+r},\ \alpha_2{}^{k+r},\ \alpha_3{}^{k+r},\ \cdots,\ \alpha_n{}^{k+r}) &=(\alpha_1{}^{k+p-Tm},\ \alpha_2{}^{k+p-Tm},\ \alpha_3{}^{k+p-Tm},\ \cdots,\ \alpha_n{}^{k+p-Tm})\\ &=(\alpha_1{}^{k+p},\ \alpha_2{}^{k+p},\ \alpha_3{}^{k+p},\ \cdots,\ \alpha_n{}^{k+p})\\ &=(\alpha_1{}^{k},\ \alpha_2{}^{k},\ \alpha_3{}^{k},\ \cdots,\ \alpha_n{}^{k})\end{aligned}$$

よって，$r>0$ とすると r は周期となり，$0\leqq r<T$ より T が最小の周期であることに反する。

したがって，$r=0$ となるから，

$$p=Tm$$

ゆえに，p は T の倍数である。

証明終

これより，次の定理が成り立つ。

定理　周期 p が素数であり，1 が周期でないとき，p は基本周期 T である。

さらに，基本周期は任意の周期の約数であるといえる。したがって，1 つの周期が求められれば，その周期を素因数分解することにより，基本周期の候補が見つかる。

異なる$(\alpha_1{}^{k},\ \alpha_2{}^{k},\ \alpha_3{}^{k},\ \cdots,\ \alpha_n{}^{k})$の組の個数は，基本周期である。

体から零元 0 を除けば群をなすから，異なる$(\alpha_1{}^{k},\ \alpha_2{}^{k},\ \alpha_3{}^{k},\ \cdots,\ \alpha_n{}^{k})$の個数は(拡大体の位数－1)の約数であるから，

基本周期は(拡大体の位数－1)の約数

である。

命題

体 K 上の n 次方程式

$$x^n-\sigma_1 x^{n-1}+\sigma_2 x^{n-2}-\cdots+(-1)^n\sigma_n=0\cdots①$$

の解の 1 つを α として

$$\alpha^p=c(p,\ 1)\alpha^{n-1}+c(p,\ 2)\alpha^{n-2}+\cdots+c(p,\ n)$$

と表すとき，①が重解を持たなければ

$$(c(p,\ 1),\ c(p,\ 2),\ c(p,\ 3),\ \cdots,\ c(p,\ n))=(c(q,\ 1),\ c(q,\ 2),\ c(q,\ 3),\ \cdots,\ c(q,\ n))$$

$$\Leftrightarrow(\alpha_1{}^p,\ \alpha_2{}^p,\ \alpha_3{}^p,\ \cdots,\ \alpha_n{}^p)=(\alpha_1{}^q,\ \alpha_2{}^q,\ \alpha_3{}^q,\ \cdots,\ \alpha_n{}^q)$$

証明

$\Rightarrow$は明らか

$\Leftarrow$を示す

$$(\alpha_1{}^p,\ \alpha_2{}^p,\ \alpha_3{}^p,\ \cdots,\ \alpha_n{}^p)=(\alpha_1{}^q,\ \alpha_2{}^q,\ \alpha_3{}^q,\ \cdots,\ \alpha_n{}^q)$$

より

$$c(p,\ 1)\alpha_k{}^{n-1}+c(p,\ 2)\alpha_k{}^{n-2}+\cdots+c(p,\ n)=c(q,\ 1)\alpha_k{}^{n-1}+c(q,\ 2)\alpha_k{}^{n-2}+\cdots+c(q,\ n)\ (k=1,2,3,\cdots,n)$$

よって

$$\begin{pmatrix}\alpha_1^{n-1} & \alpha_1^{n-2} & \cdots & 1\\ \alpha_2^{n-1} & \alpha_2^{n-2} & \cdots & 1\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_n^{n-1} & \alpha_n^{n-2} & \cdots & 1\end{pmatrix}\begin{pmatrix}c(p,1)\\ c(p,2)\\ \vdots\\ c(p,n)\end{pmatrix}=\begin{pmatrix}\alpha_1^{n-1} & \alpha_1^{n-2} & \cdots & 1\\ \alpha_2^{n-1} & \alpha_2^{n-2} & \cdots & 1\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_n^{n-1} & \alpha_n^{n-2} & \cdots & 1\end{pmatrix}\begin{pmatrix}c(q,1)\\ c(q,2)\\ \vdots\\ c(q,n)\end{pmatrix}$$

ここで，$A=\begin{pmatrix}\alpha_1^{n-1} & \alpha_1^{n-2} & \cdots & 1\\ \alpha_2^{n-1} & \alpha_2^{n-2} & \cdots & 1\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_n^{n-1} & \alpha_n^{n-2} & \cdots & 1\end{pmatrix}$ とし，A の行列式を $|A|$ とする。

$|A|$ において，$\alpha_i=\alpha_j\ (i\neq j)$ とおくと 0 になるから，因数定理により $|A|$ は $(\alpha_i-\alpha_j)\ (i\neq j)$ を因数に持つ。

行列式を展開すると $\frac{n(n-1)}{2}$ 次の多項式となるから，行列式は $k\prod_{i<j}(\alpha_i-\alpha_j)$ とおける。(k は定数)

行列式を展開したときの $\alpha_1^{n-1}\alpha_2^{n-2}\alpha_n^{n-3}\cdots1$ の係数は 1

また，$\prod_{i<j}(\alpha_i-\alpha_j)$ を展開したときの $\alpha_1^{n-1}\alpha_2^{n-2}\alpha_n^{n-3}\cdots1$ の係数の絶対値は 1　(Vandermonde)

よって，k の絶対値は 1 であるから，①が重解を持たなければ $k\prod_{i<j}(\alpha_i-\alpha_j)\neq0$

したがって，A は逆行列を持ち

$$(c(p,\ 1),\ c(p,\ 2),\ c(p,\ 3),\ \cdots,\ c(p,\ n))=(c(q,\ 1),\ c(q,\ 2),\ c(q,\ 3),\ \cdots,\ c(q,\ n))$$

証明終

命題

$$(\sigma(p,\ 1),\ \sigma(p,\ 2),\ \sigma(p,\ 3),\ \cdots,\ \sigma(p,\ n))=(\sigma(p,\ 1),\ \sigma(p,\ 2),\ \sigma(p,\ 3),\ \cdots,\ \sigma(p,\ n))$$

⇔集合的に$\{\alpha_1{}^p,\ \alpha_2{}^p,\ \alpha_3{}^p,\ \cdots,\ \alpha_n{}^p\}=\{\alpha_1{}^p,\ \alpha_2{}^p,\ \alpha_3{}^p,\ \cdots,\ \alpha_n{}^p\}$

証明

$(\sigma(p,\ 1),\ \sigma(p,\ 2),\ \sigma(p,\ 3),\ \cdots,\ \sigma(p,\ n))=(\sigma(q,\ 1),\ \sigma(q,\ 2),\ \sigma(q,\ 3),\ \cdots,\ \sigma(q,\ n))$

と仮定すると

$(x-\alpha_1{}^p)(x-\alpha_2{}^p)(x-\alpha_3{}^p)\cdots(x-\alpha_n{}^p)=x^n-\sigma(p,\ 1)x^{n-1}+\sigma(p,\ 2)x^{n-2}-\cdots+(-1)^n\sigma(p,\ n)$

$=x^n-\sigma(q,\ 1)x^{n-1}+\sigma(q,\ 2)x^{n-2}-\cdots+(-1)^n\sigma(q,\ n)$

$=(x-\alpha_1{}^q)(x-\alpha_2{}^q)(x-\alpha_3{}^q)\cdots(x-\alpha_n{}^q)$

よって，n 次方程式

$(x-\alpha_1{}^p)(x-\alpha_2{}^p)(x-\alpha_3{}^p)\cdots(x-\alpha_n{}^p)=0$

の解と，n 次方程式

$(x-\alpha_1{}^q)(x-\alpha_2{}^q)(x-\alpha_3{}^q)\cdots(x-\alpha_n{}^q)=0$

の解は一致する。したがって，集合的に

$\{\alpha_1{}^p,\ \alpha_2{}^p,\ \alpha_3{}^p,\ \cdots,\ \alpha_n{}^p\}=\{\alpha_1{}^q,\ \alpha_2{}^q,\ \alpha_3{}^q,\ \cdots,\ \alpha_n{}^q\}$

逆は明らか

証明終

$(\sigma(p,\ 1),\ \sigma(p,\ 2),\ \sigma(p,\ 3),\ \cdots,\ \sigma(p,\ n))=(\sigma(p,\ 1),\ \sigma(p,\ 2),\ \sigma(p,\ 3),\ \cdots,\ \sigma(p,\ n))$

であるとすると，上記の命題により，$(\alpha_1{}^p,\ \alpha_2{}^p,\ \alpha_3{}^p,\ \cdots,\ \alpha_n{}^p)$ は $(\alpha_1{}^q,\ \alpha_2{}^q,\ \alpha_3{}^q,\ \cdots,\ \alpha_n{}^q)$ の置換となる。

異なる置換は n!個しかなく，

$(\alpha_1{}^k,\ \alpha_2{}^k,\ \alpha_3{}^k,\ \cdots,\ \alpha_n{}^k)\quad (k=1,\ 2,\ 3,\ \cdots,\ T)$

はすべて異なるから，p を固定して考えたとき，1 周期のうちに

$(\sigma(p,\ 1),\ \sigma(p,\ 2),\ \sigma(p,\ 3),\ \cdots,\ \sigma(p,\ n))=(\sigma(q,\ 1),\ \sigma(q,\ 2),\ \sigma(q,\ 3),\ \cdots,\ \sigma(q,\ n))$

となる q は n!個以下である。

よって，T 以下の自然数を暗号化鍵とした場合，暗号鍵長(bit)は最悪 $\log_2(n!)$bit 少なくなると考えられる。したがって，暗号鍵の実質鍵長は最悪

最大鍵長$-\log_2(n!)$ ビット

と考えればよい。

n が十分大きいとき，スターリングの公式により $\log_2(n!)\approx n\log_2 n-n\log_2 e+\frac{1}{2}\log_2(2\pi n)$ であるから，

素体 K の位数≧n+1 とすれば，実質鍵長は $n\log_2 e$ ビット程度確保できる。

C 言語での実装

まず，基本対称式で考えると正負と下付きの数の処理が面倒なので，次のように変形する。

$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_n)=0$

$x^n-\sigma_{n-1}x^{n-1}-\sigma_{n-2}x^{n-2}-\cdots-\sigma_0=0$

$x^n=\sigma_{n-1}x^{n-1}+\sigma_{n-2}x^{n-2}+\cdots+\sigma_0$

$S_j=\alpha_1{}^j+\alpha_2{}^j+\cdots+\alpha_n{}^j\quad (j=0,\ 1,\ 2,\ \cdots,\ n)$

$S_p=c(p,\ n-1)S_{n-1}+c(p,\ n-2)S_{n-2}+\cdots+n\cdot c(p,\ 0)$

このとき，ニュートンの公式は

$S_1=\sigma_{n-1}$

$S_2=(\sigma_{n-1}S_1+2\sigma_{n-2})$

$$S_3=(\sigma_{n-1}S_2+\sigma_{n-2}S_1+3\sigma_{n-3})$$

……

$$S_n=(\sigma_{n-1}S_{n-1}+\sigma_{n-2}S_{n-2}+\cdots+\sigma_1S_1+n\sigma_0)$$

および

$$\sigma_{n-1}=S_1$$
$$\sigma_{n-2}=(S_2-\sigma_{n-1}S_1)\cdot 2^{-1}$$
$$\sigma_{n-3}=(S_3-\sigma_{n-1}S_2-\sigma_{n-2}S_1)\cdot 3^{-1}$$

……

$$\sigma_0=\{S_n-\sigma_{n-1}S_{n-1}-\sigma_{n-2}S_{n-2}-\cdots-\sigma_1S_1\}\cdot n^{-1}$$

となる。ただし，$\sigma_0=1$ である。

体 K の位数を P とするとき，多項式が既約な場合は，拡大体から 0 を除いた群の位数は P^n-1 である。

$$P^n-1=(P-1)(P^{n-1}+P^{n-2}+\cdots+1)$$

であり，n が合成数のときは，$P^{n-1}+P^{n-2}+\cdots+1$ はさらに因数分解できる。実装では $P^{n-1}+P^{n-2}+\cdots+1$ が素数となるようにしたいので，n は素数とする。

なお,

$$(P+1)^{n-1}=P^{n-1}+{}_nC_1P^{n-2}+{}_nC_2P^{n-3}+\cdots+1>P^{n-1}+P^{n-2}+\cdots+1$$

であるから

$$P^{n-1}<P^{n-1}+P^{n-2}+\cdots+1<(P+1)^{n-1}$$

である。

相異なる$(\sigma_1,\ \sigma_2,\ \sigma_3,\ \cdots,\ \sigma_{n-1})$の個数は P^{n-1} 以下であるから，周期が$(P^{n-1}-1)/(P-1)$以上のときは，1 周期のうちに必ず同じ$(\sigma_1,\ \sigma_2,\ \sigma_3,\ \cdots,\ \sigma_{n-1})$が存在する。

次に，16 ビットの体上で 31 次方程式で実装した結果を示す。

16 ビットの素数を P とするとき，多項式が既約な場合は，拡大体から 0 を除いた群の位数は $P^{31}-1$ であるから，$P^{31}-1$ の素因数がなるべく少ないものを考える。

38783，40127，42683，43223，53267，62507，64007

は，$P^{31}-1$ の素因数は 2，$(P-1)/2$，$(P^{31}-1)/(P-1)$だけである。

このとき，$P-1$ が周期とならないような$(\sigma_1,\ \sigma_2,\ \sigma_3,\ \cdots,\ \sigma_{n-1})$を用いれば，周期は$(P^{31}-1)/(P-1)$以上となる。

注意　$(P^{31}-1)/(P-1)$が素数という条件だけで考えれば，P の候補はもう少し多くなる。

$P=64007$ のとき，100000 個の$(\sigma_1,\ \sigma_2,\ \sigma_3,\ \cdots,\ \sigma_{n-1})$の組で実測したところ，

$P^{31}-1$ が周期でないものが　　96812 個

$(P^{31}-1)/(P-1)$が周期であるものが 3188 個

あり，他の周期のものはなかった。

すなわち、周期が$(P^{31}-1)/(P-1)$であるものは約 3.2%あったことになる。ここで

$$(P^{31}-1)/(P-1)<(2^{16})^{30}$$

である。このとき鍵長は，16bit×(31－1)＝480bit だが，実質鍵長は最悪 16bit×(31－1)－$\log_2(31!)$≒370bit 程と考えられる。

次に，32 ビットの体上で 13 次方程式で実装した結果を示す。

P＝4294957643 のとき，100000 個の(σ_1，σ_2，σ_3，…，σ_{n-1})の組で実測したところ，

$P^{13}-1$ が周期でないものが　　92373 個

$(P^{17}-1)/(P-1)$が周期であるものが 7627 個

あり，他の周期のものはなかった。

すなわち、周期が$(P^{17}-1)/(P-1)$であるものは約 7.6%あったことになる。

ここで $(P^{13}-1)/(P-1)<(2^{32})^{13}$ である。

このとき鍵長は，32bit×(13－1)＝384bit だが，実質鍵長は最悪 32bit×(13－1)－$\log_2(13!)$≒350bit 程と考えられる。

注意

多項式

$$x^n-\sigma_1 x^{n-1}+\sigma_2 x^{n-2}-\cdots+(-1)^n\sigma_n$$

が既約でないとすると，周期が P^{n-1} より大きい素数となることはない。

$$(P^n-1)/(P-1)>P^{n-1}$$

であるから，$(P^n-1)/(P-1)$が素数で，$(P^n-1)/(P-1)$が周期のとき，この多項式は既約である。

注意 2

CPU の剰余の計算は低速であるため，実装にあたっては，剰余の計算をなるべく少なくすることが望ましい。桁あふれの関係上 14bit や 30bit の体上で構成すると剰余の計算の回数が少なくなり，高速に実装できる。

高次対称式暗号におけるデジタル署名

a_1，a_2，a_3，…，a_n および b_1，b_2，b_3，…，b_n に対して，x の n^2 次の多項式の恒等式

(実装時には n は素数とするので，n は 3 以上の奇数とする)

$$(x-a_1b_1)\cdot(x-a_1b_2)\cdot(x-a_1b_3)\cdot\cdots\cdot(x-a_1b_n)\cdot(x-a_2b_1)$$
$$\cdot(x-a_2b_2)\cdot(x-a_2b_3)\cdot\cdots\cdot(x-a_2b_n)\cdot\cdots\cdot(x-a_nb_n)$$
$$=x^{n\hat{}2}-(a_1+a_2+a_3+\cdots+a_n)(b_1+b_2+b_3+\cdots+b_n)x^{n\hat{}2-1}+$$
$$(a_1^2b_1b_2+a_1^2b_1b_3+a_1^2b_1b_4+\cdots+a_n^2b_{n-1}b_n)x^{n\hat{}2-2}+\cdots-(a_1a_2a_3\ldots a_nb_1b_2b_3\ldots b_n)^n \quad \cdots①$$

を考える。

係数は a_1b_1，a_1b_2，a_1b_3，…，a_1b_n，a_2b_1，a_2b_2，a_2b_3，…，a_2b_n，…，a_nb_n の基本対称式であるから，

$$T_k=(a_1b_1)^k+(a_1b_2)^k+(a_1b_3)^k+\cdots+(a_1b_n)^k+(a_2b_1)^k+(a_2b_2)^k+(a_2b_3)^k+\cdots+(a_2b_n)^k+\cdots+(a_nb_n)^k$$

を用いて表すことができる。変形して

$$T_k=(a_1^k+a_2^k+a_3^k+\cdots+a_n^k)(b_1^k+b_2^k+b_3^k+\cdots+b_n^k)$$

ここで，ニュートンのアルゴリズムを用いれば，多項式①の係数はすべて T_k (k＝1，2，3，…，n^2) で表され，T_k は a_1，a_2，a_3，…，a_n と b_1，b_2，b_3，…，b_n の基本対称式で表される。

多項式①の係数を a_1，a_2，a_3，…，a_n と b_1，b_2，b_3，…，b_n の基本対称式から求める計算量は $O(n^4)$ である。

①の x^k の係数を$(-1)^kA_{n\hat{}2-k}$とおくと，①の右辺は

$$x^{n\hat{}2}-A_1x^{n\hat{}2-1}+A_2x^{n\hat{}2-2}+\cdots-A_{n\hat{}2}$$

となる。ただし，A_k はすべて T_k で表される。

また、①の左辺は

$$(x-a_1b_1)\cdot(x-a_2b_2)\cdot(x-a_3b_3)\cdot\cdots\cdot(x-a_nb_n)$$

を因数にもつ。これを展開した式を

$$x^n - B_1x^{n-1} + B_2x^{n-2} + \cdots - B_n \cdots ③$$

とする。このとき，②は③で割り切れる。

特に　$a_k = \alpha_k{}^p$,　$b_k = \alpha_k{}^q$　とすると　$a_kb_k = \alpha_k{}^{p+q}$　$(k = 1, 2, 3, \cdots, n)$

なり，このときも②は③で割り切れる。

このことを用いれば ElGamal 署名や Schnorr 署名の変形版のデジタル署名が実装可能になる。

その方法を示す。

デジタル署名 1　(デジタル署名 2 に対して，高速で，署名長が短い)

(1) $g = \sigma(1)$，$t = \sigma(p)$ を送信者の公開鍵とする。p が秘密鍵である。

(2) 送信者は，文書 M に対して，文書 M のハッシュ値 $e = h(M)$を求め，さらに $\lambda = \sigma(p+e)$ を求める。
λ が M の署名である。(安全のため，文書 M にはパディングをする。)
このとき，$\sigma(p)$ と $\sigma(e)$から作られる②式が $\lambda = \sigma(p+e)$ による③式で割り切れる。
送信者は，受信者に文書 M とその署名 λ を送る。

(3) 受信者は，ハッシュ値 $e = h(M)$ を求める。
さらに，g と e から $\sigma(e)$を求め，$\sigma(e)$と t から②式を作る。
このとき，②式を λ による③式で割った余りが 0 となれば，文書 M の署名が確認されたと考える。

デジタル署名 2　(Elgamal 署名や Schnorr 署名の変形版のデジタル署名)

(1) $g = \sigma(1)$，$t = \sigma(p)$を送信者の公開鍵とする。p が秘密鍵である。

(2) 送信者は，文書 M に対して秘密の乱数 q を選び，次の計算をする。

$\gamma = \sigma(q)$

$e = h(M, \gamma)$(文書 M と γ を結合した文書のハッシュ値)

$\delta = q - pe$

このとき，$pe + \delta = q$ であるから，$\sigma(pe)$と $\sigma(\delta)$から作られる②式が $\gamma = \sigma(q)$による③式で割り切れる。
送信者は，受信者に文書 M とその署名(γ, δ)を送る。

(3) 受信者は，ハッシュ値 $e = h(M, \gamma)$を求める。
さらに，t と e から $\sigma(pe)$，g と δ から $\sigma(\delta)$を求め，$\sigma(pe)$と $\sigma(\delta)$から②式を作る。
このとき，②式を γ による③式で割った余りが 0 となれば，文書 M の署名が確認されたと考える。

注　方程式

$$x^n - \sigma_1x^{n-1} + \sigma_2x^{n-2} - \sigma_3x^{n-3} + \cdots + (-1)^{n-1}\sigma_{n-1}x + (-1)^n = 0$$

の両辺を x^n で割り，$1/x = t$ と置くと

$$t^n - \sigma_{n-1}t^{n-1} + \sigma_{n-2}t^{n-2} - \sigma_{n-3}t^{n-3} + \cdots + (-1)^{n-1}\sigma_1t + (-1)^n = 0$$

元の方程式と係数の並びが逆になる。
よって，ニュートンのアルゴリズムにおいて，σ_0，σ_1，σ_2，…，σ_{n-1}，σ_nをσ_n，σ_{n-1}，σ_{n-2}，…，σ_1，σ_0に置き換え，S_1，S_2，S_3，…をS_{-1}，S_{-2}，S_{-3}，…に置き換えた等式が成り立つ。
σ_{n-1}，σ_{n-2}，…，$\sigma_{(n+1)/2}$についてはこれを用いて求めると，デジタル署名において計算量は約 1/2 となる。

付録

3 次方程式の場合

$$c(p,\ 1)=s,\quad c(p,\ 2)=s,\quad c(p,\ 3)=u$$
$$\sigma_1=a,\quad \sigma_2=b,\quad \sigma_3=1$$

とおき

$$f(x)=sx^2-tx+u$$

とおくと

$$\alpha_1+\alpha_2+\alpha_3=a,\quad \alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1=b,\quad \alpha_1\alpha_2\alpha_3=1$$

であるから

$$\sigma(p,\ 1)=f(\alpha_1)+f(\alpha_2)+f(\alpha_3)$$
$$=s(a^2-2b)+ta+3u$$
$$\sigma(p,\ 2)=f(\alpha_1)f(\alpha_2)+f(\alpha_2)f(\alpha_3)+f(\alpha_3)f(\alpha_1)$$
$$=s^2(b^2-2a)+t^2b+3u^2+st(ab-3)+2tua+2us(a^2-2b)$$

が得られる。
特に，GL(2)の拡大体上では

$$\sigma(p,\ 1)=sa^2+ta+u$$
$$\sigma(p,\ 2)=(sb)^2+t^2b+u^2+st(ab+1)$$

と簡単になり，高速に計算ができる。

行列を用いた計算法
行列を用いて高次方程式暗号を再構成すると，見通しがよくなる。しかし，計算量は増えるため，実装する際には，行列を用いない方がよい。

命題
n 次の正方行列

$$A=\begin{pmatrix}\sigma_1 & -\sigma_2 & \sigma_3 & \cdots & (-1)^{n-1}\sigma_n\\ 1 & 0 & 0 & \cdots & 0\\ 0 & 1 & 0 & \ddots & 0\\ \vdots & \ddots & \ddots & \ddots & \vdots\\ 0 & 0 & \cdots & 1 & 0\end{pmatrix}$$

の固有方程式は

$$x^n-\sigma_1x^{n-1}+\sigma_2x^{n-2}-\sigma_3x^{n-3}+\cdots+(-1)^n\sigma_n=0$$

である。
証明
A の固有方程式は

$$\begin{vmatrix} \sigma_1 - x & -\sigma_2 & \sigma_3 & \cdots & (-1)^{n-1}\sigma_n \\ 1 & -x & 0 & \cdots & 0 \\ 0 & 1 & -x & \ddots & 0 \\ \vdots & \ddots & \ddots & -x & \vdots \\ 0 & 0 & \cdots & 1 & -x \end{vmatrix} = 0$$

であり，変形すると

$$\begin{vmatrix} -x & -\sigma_2 & \sigma_3 & \cdots & (-1)^{n-1}\sigma_n \\ 0 & -x & 0 & \cdots & 0 \\ 0 & 1 & -x & \ddots & 0 \\ \vdots & \ddots & \ddots & -x & \vdots \\ 0 & 0 & \cdots & 1 & -x \end{vmatrix} + \begin{vmatrix} \sigma_1 & -\sigma_2 & \sigma_3 & \cdots & (-1)^{n-1}\sigma_n \\ 1 & -x & 0 & \cdots & 0 \\ 0 & 1 & -x & \ddots & 0 \\ \vdots & \ddots & \ddots & -x & \vdots \\ 0 & 0 & \cdots & 1 & -x \end{vmatrix} = 0$$

となる。これを展開すればよい。

証明終

命題

行列 A の固有方程式の解を α_1， α_2， α_3，…， α_n とすると， A^p の固有方程式の解は $\alpha_1{}^p$， $\alpha_2{}^p$， $\alpha_3{}^p$，…， $\alpha_n{}^p$ である。

証明

行列 A は，適当な行列 P を用いると PAP^{-1} はジョルダン標準形になる。よって， A^p の固有方程式は

$$\left|A^p - xE\right| = 0$$

$$\left|P(A^p - xE)P^{-1}\right| = 0$$

$$\left|(PAP^{-1})^p - xE\right| = 0$$

したがって

$$(x-\alpha_1{}^p)(x-\alpha_2{}^p)\cdots(x-\alpha_n{}^p) = 0$$

ゆえに， A^n の固有方程式の解は $\alpha_1{}^p$， $\alpha_2{}^p$， $\alpha_3{}^p$，…， $\alpha_n{}^p$ である。

証明終

命題

A^p の固有方程式を

$$\mathrm{x^n - s_1x^{n-1} + s_2x^{n-2} - s_3x^{n-3} + \cdots + (-1)^n s_n = 0}$$

とする。このとき，

$$B = \begin{pmatrix} s_1 & -s_2 & s_3 & \cdots & (-1)^{n-1}s_n \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

とすると， B^q の固有方程式と A^{pq} の固有方程式は一致する。

証明

A の固有方程式の解を α_1， α_2， α_3，…， α_n とすると， A^p の固有方程式の解は

α_1^p，α_2^p，α_3^p，…，α_n^p

よって，B の固有方程式の解も α_1^p，α_2^p，α_3^p，…，α_n^p である。

したがって，B^q の固有方程式の解は α_1^{pq}，α_2^{pq}，α_3^{pq}，…，α_n^{pq} となり，これは A^{pq} の固有方程式の解と一致する。

ゆえに，B^q の固有方程式と A^{pq} の固有方程式は一致する。

証明終

ハミルトン・ケーリーの定理により

$$A^n=s_1A^{n-1}-s_2A^{n-2}+s_3A^{n-3}-\cdots+(-1)^{n-1}s_n$$

が成り立つ。バイナリー法を用いるとき，この等式を用いて次数下げをすれば

$$A^p=c_1A^{n-1}+c_2A^{n-2}+c_3A^{n-3}+\cdots+c_n$$

の形に表すことができ，A^p を高速に求めることができるので，A^p の固有方程式を求めればよい。

$A^p=B$ とするとき，B の固有多項式

$$|xE-B|=x^n+b_1x^{n-1}+b_2x^{n-2}+b_3x^{n-3}+\cdots+b_n$$

はフレーム(Frame)法により高速に求められる。フレーム法は以下のアルゴリズムである。

```
X＝E
for i＝1 to n
    X＝BX
    b_i＝－tr(X)・i^(－1)  (「tr」はトレースを表し，対角要素の和である)
    X＝X＋b_iE
next i
```

フレーム(Frame)法の証明

tr(AB)＝tr(BA)が成り立つから

$$tr(P^{-1}AP)=tr((P^{-1}A)P)=tr(P(P^{-1}A))=tr((PP^{-1})A))=tr(EA)=tr(A)$$

よって，フレーム法において，B を予めジョルダン標準形に変形しておいても b_i の値は変わらない。

このとき，B の対角成分には B の固有値が並ぶから，ニュートンの公式の「基本対称式を累乗和を用いて求めるアルゴリズム」により，フレーム法のアルゴリズムが成り立つ。

証明終

注意 1

フレーム法は，GL(2)の拡大体では使えない。(偶数の逆元がないから)。また，計算量は $O(n^4)$ である。

逆行列による方法

フレーム法やニュートンの公式を用いない方法を示す。

$$x^n=\sigma_1x^{n-1}-\sigma_2x^{n-2}-\cdots+(-1)^{n-1}\sigma_n$$

これを繰り返し用いると，x^{p-1}，x^{2p-1}，x^{3p-1}，…，x^{np-1} は x の n－1 次式で表される。このように得られた等式に x をかけて

$$\begin{pmatrix} x^{np} \\ x^{(n-1)p} \\ \vdots \\ x^{p} \end{pmatrix} = \begin{pmatrix} s_{11} & s_{12} & \cdots & s_{1n} \\ s_{21} & s_{22} & \cdots & s_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ s_{n1} & s_{n2} & \cdots & s_{nn} \end{pmatrix} \begin{pmatrix} x^{n} \\ x^{n-1} \\ \vdots \\ x \end{pmatrix}$$

の形に表すことができる。

$$X = \begin{pmatrix} x^{n} \\ x^{n-1} \\ \vdots \\ x \end{pmatrix}, \quad Y = \begin{pmatrix} x^{np} \\ x^{(n-1)p} \\ \vdots \\ x^{p} \end{pmatrix}, \quad S = \begin{pmatrix} s_{11} & s_{12} & \cdots & s_{1n} \\ s_{21} & s_{22} & \cdots & s_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ s_{n1} & s_{n2} & \cdots & s_{nn} \end{pmatrix}$$ とおくと

$$Y=SX$$

よって，S^{-1}が存在するとき

$$X=S^{-1}Y$$

となる。

ここで，$P=(1, -\sigma_1, \sigma_2 \cdots, (-1)^{n-1}\sigma_{n-1})$とすると

$$PX=PS^{-1}Y$$

$x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \cdots + (-1)^n \sigma_n = 0$ であるから

$$PX=(-1)^{n-1}\sigma_n$$

よって，

$$PS^{-1}Y=(-1)^{n-1}\sigma_n$$

$$PS^{-1}Y+(-1)^n\sigma_n=0$$

となり，$t = x^p$ と置くと，t についての n 次方程式が得られる。

S^{-1}を計算するのに，掃き出し法を用いた場合，計算量は $O(n^3)$となる。