h(x)=f^(-1)(x)\*g(x) mod q

f(x)\*h(x)=f(x)\*f^(-1)(x)\*g(x) mod q=1\*g(x) mod q= g(x) mod q

f(x)\*h(x)= g(x)+u(x)\*q

f(x)\*h(x)- u(x)\*q = g(x)

f(x)\*1-u(x)\*0=f(x)

f(x)\*(h(x), 1)-u(x)\*(q,0) = (g(x),f(x))

N=3; m(x)=x^3-1;

f(x)=f0+f1\*x+f2\*x^2; h(x)=h0+h1\*x+h2\*x^2;

f(x)\*h(x)=( f0+f1\*x+f2\*x^2)\*( h0+h1\*x+h2\*x^2)= f0\*h0+f0\*h1\*x+f0\*h2\*x^2+ f1\*h0\*x+f1\*h1\*x^2+f1\*h2\*x^3+ f2\*h0\*x^2+f2\*h1\*x^3+f2\*h2\*x^4=

rem(f0\*h0+(f0\*h1+ f1\*h0)\*x +(f0\*h2 +f1\*h1+ f2\*h0)\*x^2+(f1\*h2+f2\*h1)\*x^3+f2\*h2\*x^4,m)=

f0\*h0+(f0\*h1+ f1\*h0)\*x +(f0\*h2 +f1\*h1+ f2\*h0)\*x^2+(f1\*h2+f2\*h1)\*1+rem(f2\*h2\*x^4,m)=

(f0\*h0+f1\*h2+f2\*h1)-q\*u0

(f0\*h1+f1\*h0+f2\*h2)\*x-q\*u1\*x

(f0\*h2 +f1\*h1+ f2\*h0)\*x^2 –q\*u2\*x^2

|  |  |  |
| --- | --- | --- |
| dividend | divisor | quotient |
| x^3  -  x^3-1 | x^3-1 | 1 |
| 1 rem |  |  |

|  |  |  |
| --- | --- | --- |
| dividend | divisor | quotient |
| x^4  -  x^4-x | x^3-1 | x |
| X rem |  |  |

f=(f0,f1,f2), h=(h0,h1,h2)

x\*qE=qx



A\*V1=a\*(1,0)=(a,0), v2=(0,1)

V1=(1,0), v2=(0,1)=>v=(a,b)=a\*(1,0)+b(0,1)

V1=(v11,v12, .., v1n); v2=(v21,v22, …, v2n)

(v1,v2)=v1\*v2=v11\*v21+v12\*v22+..+v1n\*v2n

||v||=sqrtt(v\*v)=sqrt(v12+ v22+…+ vn2), v=(v1,v2,…,vn)

V1\*=v1

I=2;

I=3

S=x1;

(For i=2:n){

s=s+xi}