BigNumber secret=NTL::to\_ZZ(0), aux, aux1;

for (UInt i = 0; i < shares\_set.size(); i++)

{

aux1 = 1;

for (UInt j = 0; j < shares\_set.size(); j++)

{

if ((shares\_set[j].Get\_X\_Number()) != (shares\_set[i].Get\_X\_Number()))

{

aux = shares\_set[j].Get\_X\_Number() - shares\_set[i].Get\_X\_Number();

while (aux <= 0)

aux += m\_bnPrimeNr;

MulMod(aux1, aux1, ((shares\_set[j].Get\_X\_Number())\*InvMod(aux, m\_bnPrimeNr)) % m\_bnPrimeNr, m\_bnPrimeNr);

}

}

secret = (secret + shares\_set[i].Get\_Shares\_Value()\*aux1) % m\_bnPrimeNr;

}