問題適合型高精度計算ライブラリの開発

プロジェクト代表:
長谷川秀彦@筑波大学図書館情報メディア研究科

発表者:
後 保範@早稲田大学

プロジェクトの目的

- 計算誤り検証付きライブラリの開発
- RSA 暗号(1024ビット)の強度推定: 発表
- 自動チューニング機構付き線形計算ライブラリの開発
- 精度保証付き線形計算ライブラリの開発
- ４倍精度線形計算ライブラリの開発

RSA 暗号の強度推定の計画

- 初年度

  RSA暗号ふるい処理の高速化と評価
- ２年度

  標数2の線形方程式解法の作成と高速化
- ３年度（発表年度）

  代数平方根の計算とRSA暗号の強度推定

RSA 暗号の強度推定の背景

(1) 現在の暗号 (RSA暗号)や認証システムは多数桁数(1024ビット,10進309桁)の因数分解の困難さを利用している。

(2) 現在の多数桁数の因数分解の世界記録は、RSA-768(10進232桁)。2010年1月、NTT他5カ国共同、GNFSを使用。

(3) 「暗号の2010年問題」:RSA暗号を含む現在の暗号システムの変更が必要

RSA-768(232桁)の計算時間

項目	台数・年	比(%)	対象年
ふるい処理	1500	90	初年度
標数2の線形計算	155	9	昨年度
利用関数の探査	20	1	対象外
代数平方根の計算	1	0	今年度
その他	1	0	今年度

注) AMD64 (2.2Ghz, 1コア換算)
行列サイズ : 192,796,550 * 192,795,550

RSA暗号の解読方法

(1) MPQS (複数多項式2次ふるい法)

$A^2=B^2 \pmod N$を多数の素数から作成

(2) GNFS (一般数体ふるい法)

(a) B^2側を多項式の代数平方根に変更

f(m)=Nで、$f(x)=ax^6+bx^5+cx^4+\ldots+g$

(b) 更にA^2側を1次式の代数平方根に変更

$f(M)=0 \pmod N$, $h(L)=0 \pmod N$

$h(x) = ux+v$

GNFSの計算手順

- 効率の良い多項式f(x)と1次式h(x)を探す
- ふるいでf(x),h(x)が共に分解できる整数s,t (sx+t)を基底要素数以上集める
- Π(sx+t)がf(x)とh(x)の基底要素の2乗となるよう、標数2の線形計算で整数s,tを選択
- $F(x)^2 = \Pi(sx+t) \pmod{f(x)}$, $H(x)^2 = \Pi(sx+t) \pmod{h(x)}$となる、F(x),H(x)を求める
- $A^2 = B^2 \pmod{N}$の形にし、Nを因数分解

代数平方根の規模(RSA-768)

- N(分解対象数) : 10進232桁
- 多項式f(x)の係数(a,b,...g) ：10進15～45桁
- 基底要素(sx+t)の係数(s,t): 10進1～12桁
- Π(sx+t)の(sx+t)の数　　：　1億個
- Π(sx+t) (mod f(x))の係数 :　10進50億桁
- 多項式F(x)の係数　　：　10進25億桁

代数平方根の計算方法

- 1次式の平方根

  剰余は整数なので中国剰余定理で計算

- 多項式(6次式)の平方根

  剰余は5次式

  (a) 中国剰余定理

  桁数は短い。途中の符号の選択が困難

  (b) 多数桁の連立非線形ニュートン法(今回適用)

  方法は単純。50億桁(RSA-768)の計算が必要

多数桁乗算方式(今回適用)

- 1要素(32ビット)に2進32桁で多数桁を表現
- 全て整数(int64,int32)を使用して計算
  (ES2は64ビット整数剰余が高速である)
- 乗算は整数FMT(高速剰余変換)を使用
  (整数MTは容易にベクトル化できる)
- 乗算結果の有効桁数を増やすために、4回の乗算を中国剰余定理で重ね合わせる
- 桁上げ計算のベクトル化に工夫

桁上げ計算のベクトル化対策

- 桁上げ計算は、データ依存性があるため、そのままではベクトル化できない
- 桁上げ(2進32桁単位)要素数が非常に多いため要素数nをLに分割(n=M×L)
- Mに1要素追加し、(M+1)×L要素で表現
- 計算を桁上げ方向から、分割方向に変更し、データ依存性を除きベクトル化

ベクトル化桁上げ計算(主要部)

```
   for (j = 0; j<M; j++) {
#pragma cdir nodep(A,B,C,Cover) on_adb(Cover)
        for (i=0; i<L i++) {
            Apval     = A[i][j] + Cover[i];
            Cover[i]  = (Apval < A[i][j]);
            C[i][j]   = Apval + B[i][j];
            Cover[i] += (C[i][j] < Apval);
      }     }
```

ニュートン法による代数平方根

- $G(x) = Ax^5+Bx^4+...+F = \Pi(sx+t) \pmod{f(x)}$
- $F(x)^2=G(x) \pmod{f(x)}$なる$F(x)$を求める
  ここで、$F(x)=ax^5+bx^4+cx^3+...+f$
- $F(x)^2=g_1(x)x^5+g_2(x)x^4+...+g_6(x) \pmod{f(x)}$なる展開式より$g_1(x)=A,...g_6(x)=F$が成立
- $g_1(x)=A,...g_6(x)=F$から未知数$a,b,...,f$を連立非線形ニュートン法で反復計算

ニュートン法による計算回数

- ニュートン法による初期値の選定
  10進1万桁計算で収束する初期値を探索
  ニュートン法に占める割合は1%以下
- 整数解の選定(6次式)
  平均約3個の解を求める必要がある
- RSA暗号を解読
  解読確率1/2、平均で約2回計算が必要

代数平方根の計算時間(ES2)

- RSA-768(10進232桁)
  6次多項式で、50億桁の計算
  ES2(1ノード)で3時間
- RSA-1024(10進309桁、推定)
  7～8次多項式で、約2000億桁の計算
  ES2(32ノード)で約10時間

まとめ

- RSA暗号解読(ふるい、線形計算、代数平方根)は全て整数演算を使用
- 全てES2でベクトル化可能。工夫は必要
- ふるいは並列化が容易で、台数比例効果
- 標数2の線形計算は並列化に工夫が必要
- RSA-1024解読のES2の必要メモリ量
  ふるい:1ノード、代数平方根:32ノード(推定)
  標数2の線形計算:64ノード(推定)

RSA暗号解読推定時間

- 作成中