RSA暗号解読における ふるい法について

2008年6月13日

後 保範 (東京工芸大学)

目 次

1. はじめに

(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-200(10進200桁)。2005年5月、ドイツのボン大学、GNFSを使用。

(3) 現在、RSA-1024(1024ビット)の因数分解はスーパーコンで数百年必要と推定。

1.1 暗号化方式

(1) 公開鍵暗号方式(非対称鍵)

公開鍵で暗号化、秘密鍵で復号化

認証やネットワーク通信に都合が良い

RSA暗号：多数桁数因数分解の難しさを利用

(2) 秘密鍵暗号方式(共通鍵、対称鍵)

暗号化と復号化で共通の秘密鍵を使用

代表暗号例：DES(IBM), RC4(Netscape)

1.2 RSA暗号

(1) 鍵の作成(公開鍵:n,e、秘密鍵:d)

素数p,q,e(暗号鍵)を選び、n=p×qを計算

秘密鍵: $d \equiv 1/e \pmod{(p-1)\times(q-1)}$

(2) 暗号化(整数Mを暗号Cに変換)

$C \equiv M^e \pmod{n}$

(3) 復号化(暗号Cを整数Mに変換)

$M \equiv C^d \pmod{n}$

1.3 復号化の数学的理論

(1) オイラーの定理

p,qが素数なら下記が成立。ここでn=p×q

$$M^{(p-1)(q-1)} \equiv 1 \pmod{n}$$

(2) $C^d \pmod{n}$がMになる理由

$d \equiv 1/e \pmod{(p-1)(q-1)}$より$ed = a(p-1)(q-1)+1$

$$C^d \equiv (M^e)^d \equiv M^{a(p-1)(q-1)+1} \equiv (M^{(p-1)(q-1)})^a \cdot M$$

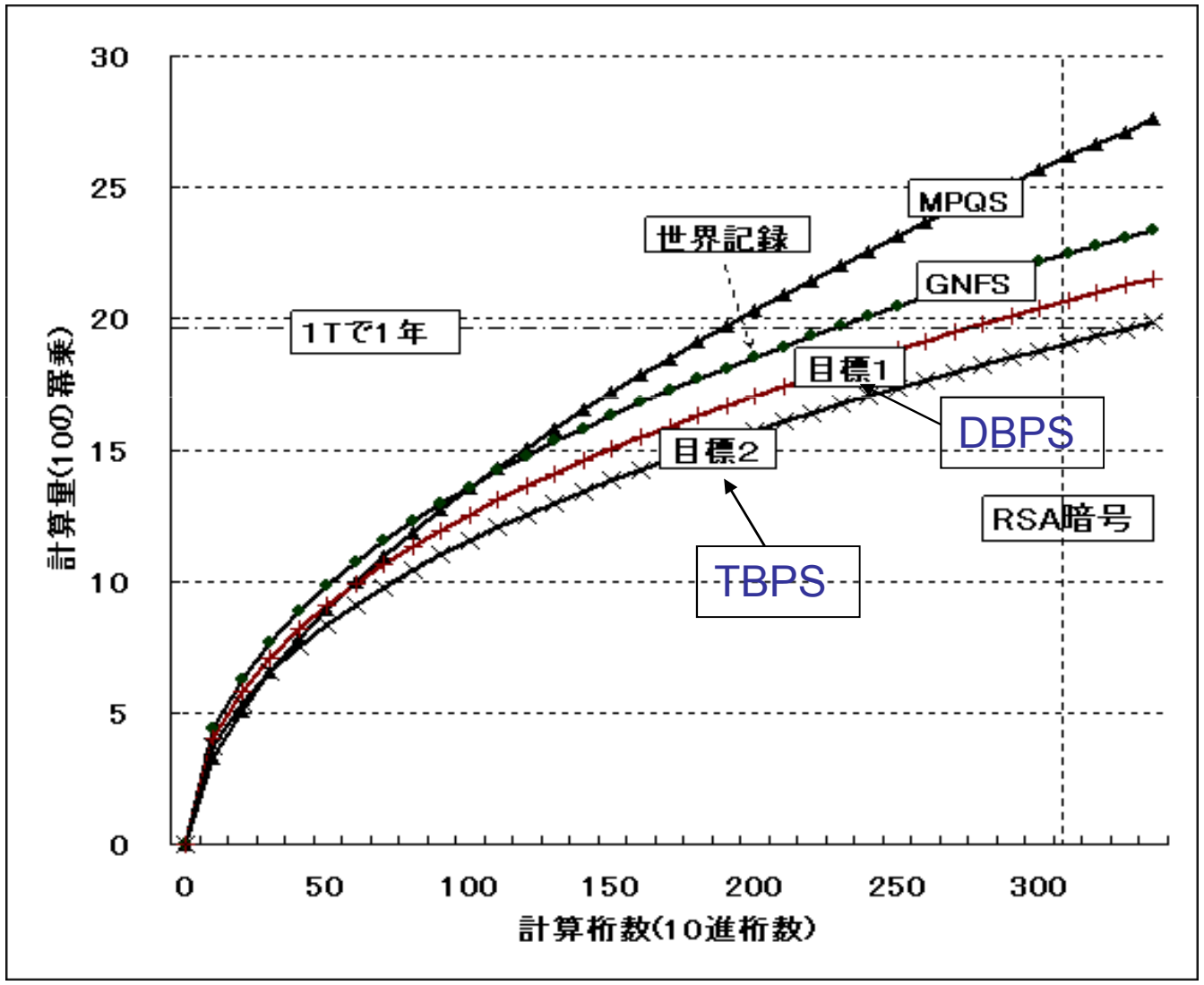
$$\equiv 1^a \cdot M \equiv M \pmod{n}$$

1.4 因数分解の方法

(1) 篩(ふるい、Sieve)系解法
計算量は合成数の桁数に依存
RSA暗号の解読に都合が良い
MPQS、GNFSが代表的解法

(2) 楕円曲線法(Elliptic Curve Method,ECM)
計算量は小さい因数の桁数に依存
RSA暗号の解読には不向き

1.5 因数分解の計算量推定



2. 篩(ふるい)法

(1) $A^2-B^2=(A-B)(A+B)\equiv 0 \pmod N$の関係を使用し、Nを因数分解

(2) $A_1^{l1}\cdot A_2^{l2}\cdots A_k^{lk}\equiv B_1^{m1}\cdot B_2^{m2}\cdots B_j^{mj} \pmod N$

なる関係を基底の数より多く集める

(3) 0-1行列を計算し、両辺が平方になるもの(従属関係)のデータを探す

(4) MPQS,GNFS等が代表的なふるい法

2.1 代表的なふるい法

(1) QS (Quadratic Sieve、2次ふるい法)
MPQS (Multiple Polynomial QS,
複数多項式2次ふるい法)が代表的解法

(2) GNFS (General Number Field Sieve、
一般数体ふるい法)。現在、100桁程度
以上で最も高速な解法と言われている。

(3) TBPS (Triple Base Polynomial Sieve、
３重基底多項式ふるい法、提案解法)

2.2 QS(2次ふるい法)

(1) QS (Quadratic Sieve, 2次ふるい法)

Nを分解、XはN$^{1/2}$に最も近い整数

$(X+k)^2 - N = A_k$, k=0,1,2, …

素数基底で分解できるA_kを集める

(2) MPQS (Multiple Polynomial QS)

複数の2次多項式を使用

代表例: $d^2 \equiv N \pmod{c}$なる(c,d)の組で

$(c \cdot x+d)^2 - N = c \cdot f(x)$ と変換しf(x)を分解

2.3 NFS(数体ふるい法)

(1) 分解の違いを利用 (SNFS,特殊数体篩法)

Nを分解、$f(M)\equiv 0 \pmod N$なる多項式

$f(x)=0$の根の一つをθとする。

$a+bM$を素数基底で分解、

$a+b\theta$を生成元(素元と単元)で分解

(2) N=1333の例 ($f(x)=x^3+2$, $M=11$, $\theta^3=-2$)

$2+M=13$, $2+\theta=\theta(1-\theta)(1+\theta)=\theta-\theta^3$

→ $-10\cdot 11\cdot 12\equiv 13 \pmod N$

2.4 GNFS(一般数体ふるい法)

(1) SNFS→GNFS

一般には素元が求まらない。

→ 素元の代わりに素イデアルを使用

問題点：平方の形が明示的に現れない

→ イデアルの積が平方となるようにする

(2) GNFSで新たに必要なこと

(a) 平方剰余の追加：平方の確率を高める

(b) イデアルの平方根を求める

3. TBPSの概要

- TBPS (Triple-Base Polynomial Sieve、3重基底多項式ふるい法)はGNFSとDBPSを合体させたもので、ふるいは下記データを採用

(1) GNFSのふるいで得られたデータ

(2) DBPSのふるいで得られたデータ

(3) イデアル$a\theta+b$の整数倍$G(a\theta+b)$がGNFSのふるいと同様に扱えるデータ
→ 今回着目

3.1 2次式におけるDBPS

- DBPS: 2重基底多項式ふるい法

(1) 対象多項式（分解対象数はN)

$f(x) = Ax^2+Bx+C, \quad f(M) \equiv 0 \pmod N$

(2) DBPSの計算式

$(A_1x+a)(A_2x+b) - f(x) = Sx+T = G(sx+t)$

$S=A_1b+A_2a - B, \quad T=ab - C, \quad A_1A_2=A$

$G=\mathrm{sign}(G)\cdot \mathrm{GCD}(|S|,|T|), \quad s=S/G, \quad t=T/G$

(3) ふるいによる得られるデータ

(a) A_1M+a, A_2M+b及び$sM+t$が基底分解できるもの

(b) $A_1x+a, A_2x+b, sx+t$で一致するもの

3.2 3次式におけるDBPS

(1) 対象多項式（分解対象数はN)

$f(x) = Ax^3+Bx^2+Cx+D, \quad f(M) \equiv 0 \pmod N$

(2) DBPSの計算式

$(A_1x+a)(A_2x+b)(A_3x+c) - f(x) = Sx+T = G(sx+t)$

$A_1A_2A_3=A, \quad A_1A_2c+A_1A_3b+A_2A_3a=B,$

$S=A_1bc+A_2ac+A_3ab-C, \quad T=abc - D$

$G=\mathrm{sign}(G)\cdot \mathrm{GCD}(|S|,|T|), \quad s=S/G, \quad t=T/G$

(3) ふるいによる得られるデータ

(a) A_1M+a, A_2M+b, A_3M+c及び$sM+t$が基底分解

(b) $A_1x+a, A_2x+b, A_3x+c, sx+t$で一致するもの

4. 2次式TBPSの関係式(1/2)

- TBPS: 2重基底多項式ふるい法

(1) 対象2次多項式（分解対象数はN)

$f(x) = Ax^2+Bx+C, \quad f(M) \equiv 0 \pmod N$

(2) TBPS(DBPSと同じ)の計算式

$(A_1x+a)(A_2x+b) - f(x) = Sx+T = G(sx+t)$

$S=A_1b+A_2a - B, \quad T=ab - C, \quad A_1A_2=A$

$G=\mathrm{sign}(G)\cdot GCD(|S|,|T|), \quad s=S/G, \quad t=T/G$ – (4.1)

(3) イデアルaθ+bのノルム(N(a,b))

$N(a,b) = a^2\cdot f(-b/a) = | Ab^2 - Bab + Ca^2 |$

4. 2次式TBPSの関係式(2/2)

- TBPSの関係式

(1) ノルムの関係式

$$N(A_1,a)\cdot N(A_2,b) = A\cdot N(S,T) \qquad -(4.2)$$

(2) ノルム関係式にGが現れるケース

(4.1)式で|G|が2以上なら下記が成立する。

$$N(A_1,a)\cdot N(A_2,b) = A\cdot G^2\cdot N(s,t) \qquad -(4.3)$$

(3) TBPSの計算式(前頁の(4.1)式の再掲)

$$(A_1x+a)(A_2x+b) - f(x) = Sx+T = G(sx+t)$$

$$S=A_1b+A_2a - B,\ \ T=ab - C,\ \ A_1A_2=A$$

$$G=\mathrm{sign}(G)\cdot \mathrm{GCD}(|S|,|T|),\ \ s=S/G,\ \ t=T/G \qquad -(4.1)$$

4.1 ふるいでの利用(2次多項式)

(1) $N(A_1,a)\cdot N(A_2,b) = A\cdot N(S,T)$

$(A_1x+a)(A_2x+b) \equiv Sx+T \pmod{f(x)}$

から、$S\theta+T$の素イデアル分解は、$A_1\theta+a$及び$A_2\theta+b$ の素イデアル分解で生成される。

(2) $N(A_1,a)\cdot N(A_2,b) = A\cdot G^2\cdot N(s,t)$

$(A_1x+a)(A_2x+b) \equiv G(sx+t) \pmod{f(x)}$

から、異なる Gを使用すれば、$s\theta+t$と$G(s\theta+t)$は共にGNFSのふるいデータとして利用可能

←$G(s\theta+t)$ のノルムが$(A_1\theta+a)(A_2\theta+b)$で可能

5. 3次式TBPSの関係式(1/2)

(1) 対象2次多項式（分解対象数はN)

$f(x) = Ax^3+Bx^2+Cx+D, \quad f(M) \equiv 0 \pmod N$

(2) TBPS(DBPSと同じ)の計算式

$(A_1x+a)(A_2x+b)(A_3x+c) - f(x) = Sx+T = G(sx+t)$

$A_1A_2A_3=A, \quad A_1A_2c+A_1A_3b+A_2A_3a=B,$

$S=A_1bc+A_2ac+A_3ab - C, \quad T=abc - D$

$G=\mathrm{sign}(G)\cdot \mathrm{GCD}(|S|,|T|), \quad s=S/G, \quad t=T/G$ – (4.4)

(3) イデアルaθ+bのノルム(N(a,b))

$N(a,b) = a^3\cdot f(-b/a) = | Ab^3 – Bab^2 + Ca^2b – Da^3 |$

5. 3次式TBPSの関係式(2/2)

(1) ノルムの関係式

$$N(A_1,a)\cdot N(A_2,b)\cdot N(A_3,c) = A\cdot N(S,T) \quad -(4.5)$$

(2) ノルム関係式にGが現れるケース

(4.1)式で|G|が2以上なら下記が成立する。

$$N(A_1,a)\cdot N(A_2,b)\cdot N(A_3,c) = A\cdot G^3\cdot N(s,t) \quad -(4.6)$$

(3) TBPSの計算式(前頁の(4.4)式の再掲)

$$(A_1x+a)(A_2x+b)(A_3x+c) - f(x) = Sx+T = G(sx+t)$$

$$A_1A_2A_3=A,\quad A_1A_2c+A_1A_3b+A_2A_3a=B,$$

$$S=A_1bc+A_2ac+A_3ab-C,\quad T=abc - D$$

$$G=\mathrm{sign}(G)\cdot GCD(|S|,|T|),\ s=S/G,\ t=T/G \quad -(4.4)$$

5.1 ふるいでの利用(3次多項式)

(1) $N(A_1,a)\cdot N(A_2,b)\cdot N(A_3,c) = A\cdot N(S,T)$

$(A_1x+a)(A_2x+b)(A_3x+c) \equiv Sx+T \pmod{f(x)}$

から、$S\theta+T$の素イデアル分解は、$A_1\theta+a$, $A_2\theta+b$ 及び$A_3\theta+c$の素イデアル分解で生成される。

(2) $N(A_1,a)\cdot N(A_2,b)\cdot N(A_3,c) = A\cdot G^3\cdot N(s,t)$

$(A_1x+a)(A_2x+b)(A_3x+c) \equiv G(sx+t) \pmod{f(x)}$

から、異なる Gを使用すれば、$s\theta+t$と$G(s\theta+t)$ は共にGNFSのふるいデータとして利用可能

←$G(s\theta+t)$ のノルムが$(A_1\theta+a)\ldots(A_3\theta+c)$で可能

6. TBPSのふるい検討事項

- TBPSのふるいを高速化するには、整数倍のイデアルG(aθ+b)がGNFSのふるいで採用されればよい。それに必要な条件は下記。

(1) 異なるGで下記が成立する。

$(A_1x+a)(A_2x+b) - f(x) = G(sx+t)$:2次式

$(A_1x+a)(A_2x+b)(A_3x+c) - f(x) = G(sx+t)$: 3次式

(2) 上記の関係が無くても
aθ+bとG(aθ+b)が共に可能な条件
→ 現在調査中(異なるGは条件)

6.1 G(aθ+b)が利用できる利点

- GNFSのふるいデータとして有効な条件

(1) (aθ+b)だけふるいに利用(従来のGNFS)
aM+b、aθ+bが共に因子基底で分解要

(2) G(aθ+b)もふるいに利用(TBPS)
aM+b、aθ+bの一方が因子基底で分解要

注) Mは整数でθは代数根で下記が成立
$f(M)\equiv 0 \mod N$, $f(\theta)=0$
整数aM+bは素数基底で分解
イデアルaθ+bは素イデアル基底で分解

7. おわりに

(1) 異なるGで下記ならsθ+t及びG(sθ+t)をふるいデータとして採用可能なことが判明。

$(A_1x+a)(A_2x+b) - f(x) = G(sx+t)$:2次式

$(A_1x+a)(A_2x+b)(A_3x+c) - f(x) = G(sx+t)$: 3次式

(2) 2,3次多項式のTBPSでaθ+bとG(aθ+b)が共にふるいデータとして採用できる条件を明確にする。

(3) 高次(4～7次)多項式で(2)の条件を明確にする。

(4) RSA-768(10進232桁)の因数分解に挑戦する。