

RSA暗号計算 No.3

MPQS(複数多項式2次ふるい法)

2007年5月
後 保範 (東京工芸大学)

1

目次

1. MPQSの概要
2. SIQS(自己初期化2次ふるい法)の理論
3. SIQSによるふるい
4. SIQSによる因数分解
5. SIQSによるふるい例
6. SIQSによる因数分解例

2

1. MPQSの概要

1. MPQSの概要

QS: $f(x)=x^2 - n$: n は分解対象数

MPQS: $F(x)=(ax+b)^2 - n$, $f(x)=F(x)/a$

a, b の選び方により多数の $f(x)$ が得られる

2. MPQSの種類

- (1) **MPQS**(Multiple Polynomial QS)
複数の a, b をある関係式より求める
- (2) **SIQS**(Self-Initialization QS)
 $b^2 - n \equiv 0 \pmod{a}$ なる関係から a, b を作成

2. SIQSの理論(1/3)

$$F(x) = (ax+b)^2 - n, \quad b^2 \equiv n \pmod{a}$$

$$\rightarrow f(x)=F(x)/a=ax^2+Bx+C, \quad B=2b, \quad C=(b^2 - n)/a$$

証明

$$F(x) = (ax+b)^2 - n \\ = a^2x^2 + 2abx + (b^2 - n)$$

ここで、 $b^2 - n$ は a で割れ、 $C=(b^2 - n)/a$ と表される、従って下記が成立する。

$$f(x) = F(x)/a = ax^2 + Bx + C$$

4

2.1 SIQSの理論(2/3)

$$F(x) = (ax+b)^2 - n, \quad b_k^2 \equiv n \pmod{a_k}, \quad k=1, 2, \dots, h$$

$$a = a_1 \cdot a_2 \cdots a_h, \quad b = \text{CRT}(b_1, b_2, \dots, b_h): \text{剰余乗算}$$

$$\rightarrow f(x)=F(x)/a=ax^2+Bx+C, \quad B=2b, \quad C=(b^2 - n)/a$$

証明 (ただし、 a_k は素数とする)

$$b_k^2 \equiv 0 \pmod{a_k}, \quad k=1, 2, \dots, h$$

$$a = a_1 \cdot a_2 \cdots a_h, \quad b = \text{CRT}(b_1, b_2, \dots, b_h): \text{剰余乗算}$$

に中国剰余定理を利用すると

$$b \equiv n \pmod{a} \text{となり、前ページと同じになる。}$$

5

2.2 SIQSの理論(3/3)

m 個の a_k から h 個で a を構成すると、 (a, b) の個数は約 $2^{h-1} {}_m C_h$ となる。ここで ${}_m C_h = m! / (h! \cdot (m-h)!)$

即ち、**12個の素数 a_k から10個使用**すると、**約3.3万**の多項式 $f(x)$ が得られる。

解説: $b_k^2 \equiv n \pmod{a_k}$ となる b_k は1個の素数 a_k に対して2個(重根のときだけ1個)存在する。従って、 h 個の a_k から構成される a に対応する b は約 2^{h-1} 個できる。また、異なる a_k の組み合わせの a は ${}_m C_h$ 個できる。

6

3. SIQSによるふるい

SIQS(自己初期化2次ふるい法)のふるい手順

- (1) 素数基底 P 及び $b_k^2 \equiv n \pmod{a_k}$ となる m 組の (a_k, b_k) の選定。
- (2) h 個の a_k より a を計算。 b は 2^{h-1} 個できる。
- (3) (a, b) に対応する $f(x)$ を求め、 $|f(x)| < M$ となる範囲で $f(x)$ を素数基底で分解するふるいをおこなう。
- (4) ふるいで得られた分解データが素数基底数以上になればふるいは完了。
足りなければ、(2)で別の a_k の組合せ処理へ

7

3.1 素数基底の選定

分解対象数を n とする。

p を指定数以下の素数として平方剰余

$$s^2 \equiv n \pmod{p}$$

となる、整数 s が存在する素数 p を求める。

上記素数 p に -1 を加えたものを素数基底 P とする。

8

3.2 (a_k, b_k) の選定

- (1) a_k の候補を指定値より大きい素数から順に選ぶ。
- (2) n に対する a_k の平方剰余
 $b_k^2 \equiv n \pmod{a_k}$
となる、整数 b_k が存在する a_k を求める。
このとき、 b_k は重根でない限り2個求まる。
- (3) (a_k, b_k) を m 組求める。
 a_k^m が $n^{1/2}$ 程度となるように整数 m は定める。

9

3.3 (a_k, b_k) から (a, b) 及び $f(x)$ の作成

- (1) m 組の (a_k, b_k) から h 組の (a_k, b_k) を選定
- (2) $a = a_1 \cdot a_2 \cdot \dots \cdot a_h$
- (3) $b = \text{CRT}(b_1, b_2, \dots, b_h)$, CRT: 剰余乗算
このとき、 b_k は各2個あるので、 b_1 以外は2個を使用し、 2^{h-1} 個の b ができる。
- (4) $f(x) = ((ax+b)^2 - n)/a = ax^2 + Bx + C$
 $B=2b$, $C=(b^2-n)/a$
ここで、 b^2-n は a で必ず割り切れる。

10

3.4 中国剰余定理(剰余乗算)

$R_1 \equiv A \pmod{P_1}$, $R_2 \equiv A \pmod{P_2}$ から A を計算
ここで、 $\text{GCD}(P_1, P_2) = 1$ である。

以下に計算方法を示す。

$$w \equiv (R_2 - R_1) \cdot v \pmod{P_2}$$

$$A = w \cdot P_1 + R_1$$

ここで、 $v \equiv P_1^{-1} \pmod{P_2}$

これは、何度でも繰り返し適用でき多数個の剰余から元の値を計算できる。

11

3.5 $f(x)$ の素数基底による分解(1/2)

$f(x)$ の素数基底による分解手順

- (1) $(a \cdot y_k + b)^2 - n \equiv 0 \pmod{p_k}$ となる素数基底の素数 p_k に対応する y_k の計算
- (2) $f(x_k) \equiv 0 \pmod{p_k}$ となる x_k を下記で計算
 $x_k \equiv a^{-1}(y_k - b) \pmod{p_k}$
- (3) $|x| < L$ の範囲の整数 x に対して、 $f(x)$ が素数基底で分解できるかテスト(ふるい)を行う。

12

3.5 $f(x)$ の素数基底による分解(2/2)

$f(x)$ の $|x| < L$ の範囲の整数でのふるい

- (1) $f(x)$ が p_k で割れるのは $x_k + \alpha p_k$
- (2) $|x| < L$ の範囲の整数 x で $g(x)=1$ と初期化
- (3) $|x_k + \alpha p_k| < L$ となる整数 α に対して
 $g(x_k + \alpha p_k) = g(x_k + \alpha p_k) \cdot p_k$ と更新する
- (4) p_k のべき乗に対しても(3)と同様の処理
- (5) $f(x)=g(x)$ となる整数 x なら選定
- (6) 選定した $f(x)$ を素数基底で分解

13

3.6 $f(x)$ の分解による行列作成

$(ax+b)^2 = a \cdot f(x)$ の関係を使用する。

- (1) $f(x)$ が素数基底 P で分解された整数 x を選定する。素数基底の要素数を M とする
- (2) 選定した各 x に対して作成する。
 - (a) 1列目は $f(x)$ が正なら0、負なら1とする。
 - (b) 2~ M 列目(p_k は素数基底の素数)
 $a \cdot f(x)$ を分解する素数 p_k の指数べき
 - (c) $(M+1)$ 列目: $ax+b$ の値

14

4. SIQSによる因数分解

ふるいデータによる因数分解の手順

- (1) 0-1行列の作成
- (2) 0-1行列の従属行の計算
- (3) 従属行より $\alpha^2 \equiv \beta^2 \pmod{n}$ の計算
- (4) $\text{GCD}(|\alpha - \beta|, n)$ の計算
- (5) n の因数分解

15

5. SIQSによるふるい例

- 分解対象数と素数基底の選定
 分解対象数を $n=55751$ とする。
 p を71以下の素数として平方剰余
 $s^2 \equiv n \pmod{p}$
 となる、整数 s が存在する素数 p を求める。
 上記素数 p に-1を加えたものを素数基底 P とする。 P は下記の12要素となる。
 $P = (-1, 2, 5, 11, 17, 19, 29, 41, 43, 47, 61, 71)$

16

5.1 a, b の選定と $f(x)$

説明を容易にするため a は1個の素数とする。

- (1) $a = 11$
- (2) $b^2 \equiv n \equiv 3 \pmod{11}$, $n = 55751$
 $\rightarrow b = 5$
- (3) $f(x) = ((ax+b)^2 - n)/a$
 $= ax^2 + Bx + C$
 $B = 2b = 10$
 $C = (b^2 - n)/a = -5066$

17

5.2 $f(x)$ によるふるいの方針

- (1) $|x|$ が30以下の整数を対象にする
- (2) $f(x)$ が p_k で割れるのは $x = x_k + \alpha p_k$
- (3) p_k に対応する x_k は下記

p_k	2	5	5^2	5^3	11	11^2	17	19
x_k	0	1	4	11	5	-17	0	-3
x_k	---	-1	11	---	---	---	-4	9

p_k	29	29^2	41	41^2	43	47	61	71
x_k	-4	-18	2	12	-6	-5	2	-13
x_k	11	---	12	---	9	-13	-14	25

18

5.3 f(x)によるふるい過程(1/4)

x	f(x)	素数基底												累計 T	f(x) /T
		-1	2	5	11	17	19	29	41	43	47	61	71		
-30	4534	1	2	1	1	1	1	1	1	1	1	1	1	2	2267
-29	3895	1	1	5	1	1	19	1	41	1	1	1	1	3895	1
-28	3278	1	2	1	11	1	1	1	1	1	1	1	1	22	149
-27	2683	1	1	1	1	1	1	1	1	1	1	1	1	1	2683
-26	2110	1	2	5	1	1	1	1	1	1	1	1	1	10	211
-25	1559	1	1	1	1	1	1	1	1	1	1	1	1	1	1559
-24	1030	1	2	5	1	1	1	1	1	1	1	1	1	10	103
-23	523	1	1	1	1	1	1	1	1	1	1	1	1	1	523
-22	38	1	2	1	1	1	19	1	1	1	1	1	1	38	1
-21	-425	-1	1	5 ²	1	17	1	1	1	1	1	1	1	-425	1
-20	-866	-1	2	1	1	1	1	1	1	1	1	1	1	-2	433
-19	-1285	-1	1	5	1	1	1	1	1	1	1	1	1	-5	257

19

5.3 f(x)によるふるい過程(2/4)

-18	-1682	-1	2	1	1	1	1	1	29 ²	1	1	1	1	1	-1682	1	
-17	-2057	-1	1	1	1	11 ²	17	1	1	1	1	1	1	1	-2057	1	
-16	-2410	-1	2	5	1	1	1	1	1	1	1	1	1	1	-10	241	
-15	-2741	-1	1	1	1	1	1	1	1	1	1	1	1	1	-1	2741	
-14	-3050	-1	2	5 ²	1	1	1	1	1	1	1	1	61	1	-3050	1	
-13	-3337	-1	1	1	1	1	1	1	1	1	1	1	47	1	71	-3337	1
-12	-3602	-1	2	1	1	1	1	1	1	1	1	1	1	1	-2	1801	
-11	-3845	-1	1	5	1	1	1	1	1	1	1	1	1	1	-5	769	
-10	-4066	-1	2	1	1	1	19	1	1	1	1	1	1	1	-38	107	
-9	-4265	-1	1	5	1	1	1	1	1	1	1	1	1	1	-5	853	
-8	-4442	-1	2	1	1	1	1	1	1	1	1	1	1	1	-2	2221	
-7	-4597	-1	1	1	1	1	1	1	1	1	1	1	1	1	-1	4597	
-6	-4730	-1	2	5	11	1	1	1	1	1	43	1	1	1	-4730	1	
-5	-4841	-1	1	1	1	1	1	1	1	1	1	47	1	1	-47	103	
-4	-4930	-1	2	5	1	17	1	29	1	1	1	1	1	1	-4930	1	
-3	-4997	-1	1	1	1	1	1	19	1	1	1	1	1	1	-19	263	

20, 263

5.3 f(x)によるふるい過程(3/4)

-2	-5042	-1	2	1	1	1	1	1	1	1	1	1	1	1	-2	2521
-1	-5065	-1	1	5	1	1	1	1	1	1	1	1	1	1	-5	1013
0	-5066	-1	2	1	1	17	1	1	1	1	1	1	1	-34	149	
1	-5045	-1	1	5	1	1	1	1	1	1	1	1	1	-5	1009	
2	-5002	-1	2	1	1	1	1	1	41	1	1	61	1	-5002	1	
3	-4937	-1	1	1	1	1	1	1	1	1	1	1	1	-1	4937	
4	-4850	-1	2	25	1	1	1	1	1	1	1	1	1	-50	97	
5	-4741	-1	1	1	11	1	1	1	1	1	1	1	1	-11	431	
6	-4610	-1	2	5	1	1	1	1	1	1	1	1	1	-10	461	
7	-4457	-1	1	1	1	1	1	1	1	1	1	1	1	-1	4457	
8	-4282	-1	2	1	1	1	1	1	1	1	1	1	1	-2	2141	
9	-4085	-1	1	5	1	1	19	1	1	43	1	1	1	-4085	1	
10	-3866	-1	2	1	1	1	1	1	1	1	1	1	1	-2	1933	
11	-3625	-1	1	5 ²	1	1	29	1	1	1	1	1	1	-3625	1	
12	-3362	-1	2	1	1	1	1	41 ²	1	1	1	1	1	-3362	1	
13	-3077	-1	1	1	1	17	1	1	1	1	1	1	1	-17	181	
14	-2770	-1	2	5	1	1	1	1	1	1	1	1	1	-10	277	

21, 277

5.3 f(x)によるふるい過程(4/4)

15	-2441	-1	1	1	1	1	1	1	1	1	1	1	1	1	-1	2441
16	-2090	-1	2	5	11	1	19	1	1	1	1	1	1	1	-2090	1
17	-1717	-1	1	1	1	17	1	1	1	1	1	1	1	1	-17	101
18	-1322	-1	2	1	1	1	1	1	1	1	1	1	1	1	-2	661
19	-905	-1	1	5	1	1	1	1	1	1	1	1	1	1	-5	181
20	-466	-1	2	1	1	1	1	1	1	1	1	1	1	1	-2	233
21	-5	-1	1	5	1	1	1	1	1	1	1	1	1	1	-5	1
22	478	-1	2	1	1	1	1	1	1	1	1	1	1	1	2	239
23	983	-1	1	1	1	1	1	1	1	1	1	1	1	1	1	983
24	1510	-1	2	5	1	1	1	1	1	1	1	1	1	1	10	151
25	2059	-1	1	1	1	1	1	29	1	1	1	1	1	71	2059	1
26	2630	-1	2	5	1	1	1	1	1	1	1	1	1	1	10	263
27	3223	-1	1	1	11	1	1	1	1	1	1	1	1	1	11	293
28	3838	-1	2	1	1	1	19	1	1	1	1	1	1	1	38	101
29	4475	-1	1	5 ²	1	1	1	1	1	1	1	1	1	1	25	179
30	5134	-1	2	1	1	17	1	1	1	1	1	1	1	1	34	151

22

5.4 ふるい結果による行列作成

行列作成の方針

- (1) ふるい過程でf(x)/Tが1のものを選定する
- (2) 選定したデータ数が素数基底の数以下なら、整数xの範囲を拡大する。
- (3) 素数基底の数(12)を超えると行列を作成
- (4) 選定データ毎に下記で行列を作成
 - (a) 1列目: f(x)が正なら0、負なら-1
 - (b) 2~12列目: 素数2,3,...,71の指数ベキ
 - (c) 13列目: 11x+5の値

23

5.5 ふるい結果の行列(1/2)

0	0	1	1	0	1	0	1	0	0	0	0	0	314
0	1	0	1	0	1	0	0	0	0	0	0	0	237
1	0	2	1	1	0	0	0	0	0	0	0	0	226
1	1	0	1	0	0	2	0	0	0	0	0	0	193
1	0	0	3	1	0	0	0	0	0	0	0	0	182
1	1	2	1	0	0	0	0	0	0	1	0	0	149
1	0	0	1	0	0	0	0	0	1	0	0	0	138
1	1	1	2	0	0	0	0	1	0	0	0	0	61

24

5.5 ふるい結果の行列(2/2)

1	1	1	1	1	0	1	0	0	0	0	0	39
1	1	0	1	0	0	0	1	0	0	1	0	27
1	0	1	1	0	1	0	0	1	0	0	0	104
1	0	3	1	0	0	1	0	0	0	0	0	126
1	1	0	1	0	0	0	2	0	0	0	0	137
1	1	1	2	0	1	0	0	0	0	0	0	181
1	0	1	1	0	0	0	0	0	0	0	0	236
0	0	0	1	0	0	1	0	0	0	0	1	280

25

6. SIQSによる因数分解例

分解手順

- (1) 0-1行列の作成(最後の列を除き(mod 2))
- (2) 左に単位行列を置き、ガウス消去
- (3) 消去結果から従属行の取り出し
- (4) $\alpha^2 \equiv \beta^2 \pmod{n}$ の算出
- (5) $\text{GCD}(|\alpha - \beta|, n)$ の計算
- (6) nの因数分解結果

26

6.1 0-1行列

$$A = \begin{matrix} & & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ & & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ & & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ & & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ & & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ & & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ & & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix}$$

27

6.2 消去後の行列

A	E
1 0 0 1 1 0 0 0 0 0 0 0 0 0 0	0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0	0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 1 1 0 1 0 1 0 0 0 0 0 0 0 0	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 1 1 0 1 0 0 0 0 0 0 0 0 0 0 0	0 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0
1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0	0 0 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0
1 1 0 1 0 0 0 0 0 0 0 0 0 0 1 0	0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0
1 0 0 1 0 0 0 0 0 0 0 0 0 1 0 1	1 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0
1 1 1 0 0 0 0 0 0 0 0 1 0 0 0 0	0 0 0 0 0 0 1 1 0 0 0 0 1 0 0 0 0 0
1 1 1 1 1 0 0 0 0 0 1 0 0 0 0 0	0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0
1 1 0 1 0 0 0 0 1 0 0 0 0 1 0 0	0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 1
1 0 1 1 0 0 1 0 0 0 1 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0
1 0 1 1 0 0 0 1 0 0 0 0 0 0 0 0	Eの列番号 --> 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
1 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 1 1 0 0 0 1 0 0 0 0 0 0 0 0 0	0 0 1 1 0 0 0 0 0 1 0 0 0 1 0 0 0 0
1 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0
0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

6.3 従属行

- (1) 従属行1: 2, 8, 11
- (2) 従属行2: 3, 4, 9, 12
- (3) 従属行3: 4, 13
- (4) 従属行4: 1, 4, 6, 10, 14
- (5) 従属行5: 1, 2, 4, 6, 10, 15
- (6) 従属行6: 3, 5

29

6.4 $\alpha^2 \equiv \beta^2 \pmod{n}$ の計算

- (1) 従属行1: 2, 8, 11の例
 左辺: $(ax+b)^2$ の項: 最後の列
 $(237*61*104)^2$
 右辺: 対応素数のベキ
 $(2*5*11^2*19*41)^2$
 等号
 $54202^2 \equiv 40803^2 \pmod{55751}$

30

6.5 $\alpha^2 \equiv \beta^2 \pmod{n}$ の結果

- (1) $54202^2 \equiv 40803^2 \pmod{55751}$
- (2) $32008^2 \equiv 23743^2 \pmod{55751}$
- (3) $26441^2 \equiv 26158^2 \pmod{55751}$
- (4) $46855^2 \equiv 28140^2 \pmod{55751}$
- (5) $46855^2 \equiv 28140^2 \pmod{55751}$
- (6) $41132^2 \equiv 10285^2 \pmod{55751}$

31

6.6 $\text{GCD}(|\alpha - \beta|, n)$ の結果

- (1) $\text{GCD}(54202-40803, 55751) = 197$
- (2) $\text{GCD}(32008-23743, 55751) = 1$
- (3) $\text{GCD}(26441-26158, 55751) = 283$
- (4) $\text{GCD}(46855-28140, 55751) = 197$
- (5) $\text{GCD}(46855-28140, 55751) = 197$
- (6) $\text{GCD}(41132-10285, 55751) = 283$

32

6.7 n の因数分解結果

- (1) $55751 = 197 \cdot 283$ と因数分解
- (2) 自明解で分解できない
- (3) $55751 = 283 \cdot 197$ と因数分解
- (4) $55751 = 197 \cdot 283$ と因数分解
- (5) $55751 = 197 \cdot 283$ と因数分解
- (6) $55751 = 283 \cdot 197$ と因数分解

33