Takagi's RSA 暗号に対する Small Secret-key Attack

篠原 直行 †　　伊豆 哲也 ‡　　國廣 昇 §

† 情報通信研究機構
〒 184-8795 小金井市貫井北町 4-2-1
shnhr@nict.go.jp

‡ 株式会社富士通研究所
〒 211-8588 川崎市中原区上小田中 4-1-1
izu@labs.fujitsu.com

§ 東京大学大学院 新領域創成科学研究科
〒 277-8561 柏市柏の葉 5-1-5
kunihiro@k.u-tokyo-ac.jp

あらまし Takagi's RSA 暗号は $N = p^r q$ なる合成数を用いた RSA 暗号で, 公開鍵 e と秘密鍵 d の間には $ed \equiv 1(\mathrm{mod}(p-1)(q-1))$ なる関係がある. さらに中国人剰余定理 (CRT) による復号の高速技法が用いられており, $d_q = d \bmod q-1$ なる CRT-exponent d_q が使われる. 同様の高速化技法を用いた通常の RSA 暗号において, CRT-exponent が小さすぎると May's method と Bleichenbacher-May's method (B-M method) で攻撃できることが知られている. 本稿ではこれらの手法を Takagi's RSA 暗号に拡張することで, CRT-exponent が十分小さければ May's method の場合は $p < N^{3/(8r)}$ のときに, また B-M method の場合は $p < N^{(-5+\sqrt{61})/(6r)}$ のときに攻撃できることを示す. これは通常の RSA 暗号の場合の自然な拡張であり, Takagi's RSA 暗号も CRT-exponent が小さいときに本手法で攻撃できることを意味する.

Small Secret-key Attack against a Takagi's RSA

Naoyuki Shinohara†　　Tetsuya Izu‡　　Noboru Kunihiro§

†National Institute of Information and Communications Technology (NICT),
4-2-1, Nukui-Kitamachi, Koganei, 184-8795, Japan
shnhr@nict.go.jp

‡FUJITSU LABORATORIES Ltd.,
4-1-1, Kamikodanaka, Nakahara-ku, Kawasaki,
211-8588, Japan
izu@labs.fujitsu.com

§The University of Tokyo,
5-1-5, Kashiwanoha, Kashiwa,
277-8561, Japan
kunihiro@k.u-tokyo.ac.jp

Abstract Takagi's RSA is a variant of RSA with $N = p^r q$ and $ed \equiv 1(\mathrm{mod}(p-1)(q-1))$. Moreover, via Chinese remainder theorem (CRT), a CRT-exponent d_q s.t. $d_q = d \bmod q-1$ is used for the decryption in Takagi's RSA. For CRT-RSA, if a CRT-exponent is sufficiently-small, then May's method and Bleichenbacher-May's method (B-M method) work well. In this paper, we extend them against Takagi's RSA, and we show that our methods work well in the case of May's method if $p < N^{3/(8r)}$, and by B-M method if $p < N^{(-5+\sqrt{61})/(6r)}$. These conditions are extended results of CRT-RSA, and mean that May's method and B-M method can attack Takagi's RSA when a CRT-exponent is sufficiently-small.

1　はじめに

RSA 暗号では復号の際に整数剰余環における冪乗計算を行うため, その指数が小さいほど計算コストを低減させせることができる. しかし, 指数が小さいと格子理論による攻撃への耐性が弱まってしまう. そこで中国人剰余定理 (CRT) を用いることで冪乗計算の高速化を狙った RSA 暗号 (CRT-RSA 暗号) が提案されている. CRT-RSA 暗号では計算コストを低減するために CRT-exponents と呼ばれる指数が使われており, CRT-exponents が小さくても復号に用いられる指数を大きくとれることがその特徴である. May は CRT-exonents が十分小さいときの CRT-RSA 暗号を攻撃対象とした手法を提案した [5]. またさらにその手法を Bleichenbacher-May が拡張した [1]. これらの手法は small CRT-exonents attack と呼ばれる. 一方で RSA 暗号の自然な拡張として Takagi's RSA 暗号 [6] が知られており, CRT による高速化技法が使われている. Itoh ら [3] によって Takagi's RSA 暗号の解析がなされているが, small CRT-exonents attack による結果は知られていない. 本稿では May's method と B-M mothod を Takagi's RSA 暗号に拡張したときの結果を報告する.

2　準備

この節では解析の対象となる Takagi's RSA 暗号 [6] とその解析手法として使われる格子理論について述べる.

2.1　Takagi's RSA 暗号

Takagi's RSA 暗号は, 二つの奇素数 p, q に対して, $N = p^r q$ なる合成数を用いた RSA 暗号である. また公開鍵 d と秘密鍵 e は $ed \equiv 1 (\bmod\ (p-1)(q-1))$ なる性質を持つ. Takagi's RSA 暗号の利点は通常の RSA 暗号より高速に復号できることである.

[鍵生成] 二つのランダムな奇素数 p, q を生成し $N = p^r q$ とする. $ed \equiv 1 (\bmod\ (p-1)(q-1))$ かつ $\gcd(e, p) = 1$ なる e, d を求める. さらに $d_p = d \bmod (p-1)$, $d_q = d \bmod (q-1)$ とする. このとき e, N が公開鍵で, d_p, d_q, p, q が秘密鍵となる.

[暗号化] $M \in \mathbf{Z}_N^*$ を平文とすると, それに対応する暗号文は $C = M^e \bmod N$ で定義される.

[復号化] 暗号文 C に対して, $M_p = C^{d_p} \bmod p$ と $M_q = C^{d_q} \bmod q$ を計算し, さらに Hensel lifting で M_p から $M_p^{(r)} \bmod p^r$ を求める. 中国人剰余定理 (CRT) によって $M \equiv M_p^{(r)} (\bmod\ p^r)$ かつ $M \equiv M_q (\mathrm{mod} q)$ なる平文 $0 \le M < N$ をが得られる.

2.2　格子理論による RSA 暗号への攻撃

ここで格子理論を使った RSA 暗号の攻撃手法の概要について説明する. 秘密鍵を得るために, まず, 秘密鍵と公開鍵の関係から得られる shift-polynomial と呼ばれる多項式 $h_1, ..., h_\omega$ を生成する. これらの多項式は, 公開鍵から与えられるある $H \in \mathbf{Z}$ とある整数 m に対して

$$h_i(x_1^{(0)}, ..., x_n^{(0)}) \equiv 0 \pmod{H^m}$$

なる解 $(x_1^{(0)}, ..., x_n^{(0)})$ を持つように定めることができる. さらに h_i の各項の係数から生成されるベクトルを $\boldsymbol{b}_i$ としたときに, $\boldsymbol{b}_1, ..., \boldsymbol{b}_\omega$ は一次独立となるように h_i を定める. このとき秘密鍵は解 $(x_1^{(0)}, ..., x_n^{(0)})$ から与えられ, これを得るために LLL アルゴリズム [4] と Howgrave-Graham's の補題 [2] を用いる. $\boldsymbol{b}_1, ..., \boldsymbol{b}_\omega$ を格子基底に持つ格子 L に属する任意のベクトル $\boldsymbol{b}$ に対して, $\boldsymbol{b}$ に対応する多項式 h は

$$h(x_1^{(0)}, ..., x_n^{(0)}) \equiv 0 \pmod{H^m} \qquad (1)$$

を満たす. そこでノルムがある値で抑えられるようないくつかのベクトル $\boldsymbol{b}'_j \in L$ を LLL アルゴリズムで求め, 各 $\boldsymbol{b}'_j$ に対応する多項式 h'_j が得られる. つまり LLL アルゴリズムは係数がある値より小さく (1) を満たす多項式を求めるために用いられる. 各 $x_i^{(0)}$ と各 h'_j が Howgrave-Graham's の補題で与えらる条件を満たせば, H^m を法とするのではなく $\mathbf{Z}$ 上で h'_j の連立代数方程式を解くことで秘密鍵が得られる.

Howgrave-Graham's の補題について述べる．ベクトル $\boldsymbol{b}$ に対して $||\boldsymbol{b}||$ を $\boldsymbol{b}$ の Euclidean norm とする．多項式 $h(x_1,...,x_n)=\sum h_{i_1,...,i_n} x_1^{i_1},...,x_n^{i_n}$ に対して $||h(x_1,...,x_n)||=\sqrt{\sum h_{i_1,...,i_n}^2}$ とする．

補題 2.1 (Howgrave-Graham's の補題)
$h(x,y,z)\in\mathbf{Z}[x,y,z]$ は高々 ω 個の単項式を持つとする．m を整数とし X,Y,Z,H は正の整数とする．ここで次の条件が成り立つとする．
1. $|x_0|<X$, $|y_0|<Y$, $|z_0|<Z$ かつ $h(x_0,y_0,z_0)=0(\bmod H^m)$.
2. $||h(xX,yY,zZ)||<H^m/\sqrt{\omega}$.
このとき $h(x_0,y_0,z_0)=0$ が $\mathbf{Z}$ 上で成り立つ．

3 May's method と B-M method

この節では May's method [5] と B-M method [1] について説明する．これらの手法は共に CRT-RSA 暗号を攻撃の対象にしている．従ってこの節では平文 M とその暗号文 C に対して，公開鍵 e,N と秘密鍵 d_p,d_q,p,q は以下の性質をもつものとする． $N=pq, ed\equiv 1(\bmod (p-1)(q-1)), d_p=d \bmod (p-1), d_q=d \bmod (q-1), C=M^e \bmod N, M\equiv C^{d_p}(\bmod p), M\equiv C^{d_p}(\bmod p)$. さらに二つの手法はこれらの条件から得られる

$$ed_q\equiv 1(\bmod q-1) \tag{2}$$

に注目した多項式をあつかっている．[5] では $e\approx N$ としているが, [1] ではより詳細な結果を求めるためパラメータ α が導入され

$$e<N^{\alpha}$$

とさだめらる．本稿の第 3.1 節の May's method の解析では α を導入して [5] の結果を再評価したものを示す．また, この節で β,δ は $p<N^{\beta}$, $d_q<N^{\delta}$ を満たすものとする．

3.1 May's method

式 (2) より, ある整数 k が存在して $(k+1)(q-1)-q=-ed_q$ を得る．この式の両辺に p をかけることで $(k+1)(N-p)-N=-ed_q p$ が得られ, $(k+1)(N-p)-N\equiv 0 \pmod e$ が成り立つ．そこで

$$f(x,y)=x(N-y)-N \tag{3}$$

とすると, $f(x,y)=0$ は e を法として $(x_0,y_0)=(k+1,p)$ を解に持つ．$|x_0|,|y_0|$ の大きさが問題となる． $|k+1|=|(ed_q-q)/(q-1)|<ed_q/(q-1)<N^{\alpha+\beta+\delta-1}$ と $p<N^{\beta}$ であることから, x_0,y_0 の上限値 X,Y を

$$X=N^{\alpha+\beta+\delta-1}, Y=N^{\beta}$$

と定めることができる．

Shift-polynomial $g_{i,j}(x,y), h_{i,j}(x,y)$ は以下のように定める．但しパラメータ τ は後で最適化されるものとする．

$$\begin{aligned} g_{i,j}(x,y) &= e^{m-i}x^j f(x,y)^i \quad (4)\\ &\quad (0\le i\le m, 0\le j\le m-i),\\ h_{i,j}(x,y) &= e^{m-i}y^j f(x,y)^i \quad (5)\\ &\quad (0\le i\le m, 1\le j\le \tau m). \end{aligned}$$

また項順序を

$$\begin{aligned} &1\prec x\prec xy\prec x^2\prec x^2y\prec x^2y^2\prec x^3\prec\cdots\\ &\prec x^m y^m\prec y\prec\cdots\prec y^{\tau m}\prec xy^2\prec\cdots\\ &\prec xy^{1+\tau m}\prec\cdots\prec x^m y^{m+1}\prec\cdots\prec x^m y^{m+\tau m} \end{aligned}$$

のように定めれば, $g_{i,j}(x,y)$ と $h_{i,j}(x,y)$ の最高次の項はそれぞれ $e^{m-i}x^{i+j}y^i$ と $e^{m-i}x^i y^{i+j}$ になる．これらの shift-polynomial によって, 下三角行列の対角成分にそれぞれの最高次の項が対応するような基底行列 B を作ることができる．B に対応する格子 L の次元は shift-polynomial の総数なので次の式を得る．

$$\dim L=\frac{m^2}{2}(2\tau+1+o(1)). \tag{6}$$

ここで $\det L$ について考える．B は下三角行列でその対角成分には, (x,y) に (xX,yY) を代

入したときの各 shift-polynomial の最高次の項の係数が並ぶ. よって

$$\det L = e^{\frac{m^3}{6}(2+3\tau+o(1))}X^{\frac{m^3}{6}(2+3\tau+o(1))} Y^{\frac{m^3}{6}(1+3\tau+3\tau^2+o(1))} \tag{7}$$

となる. また, ある c が存在して

$$\det L < cN^{\alpha m \dim L} \tag{8}$$

が成り立つときに LLL で得られるベクトルが補題 2.1 の条件を満たすことが保証されている [5].

X, Y と N の関係式を式 (7) に導入し, (6) と (8) から

$$\begin{aligned} F(\tau) &= 3\beta\tau^2 + (6\beta + 3\delta - 3)\tau \\ &\quad +\alpha + 3\beta + 2\delta - 2 \\ &= 3\beta\left(\tau + \frac{2\beta+\delta-1}{2\beta}\right)^2 \\ &\quad -\frac{3(2\beta+\delta-1)^2}{4\beta} + \alpha + 3\beta + 2\delta - 2 \\ &< 0 \end{aligned}$$

を得る. $F(\tau)$ は $\tau_0 = \frac{-2\beta'-\delta+1}{2\beta}$ のとき最少となり

$$\begin{aligned} F(\tau_0) &= \frac{-3\delta^2 + (-4\beta+6)\delta + 4\alpha\beta + 4\beta - 3}{4\beta} \\ &< 0. \end{aligned}$$

よって

$$\delta < 1 - \frac{2}{3}\left(\sqrt{\beta^2 + 3\alpha\beta} + \beta\right) \tag{9}$$

を得る. ここで May's method で RSA 暗号を解読するための p の条件 N^β について考える. 公開鍵 $e \in \mathbf{Z}_N$ をランダムに選ぶので $e \approx N$ と仮定すると $\alpha = 1$ で, さらに d_q を最小の値にとって $\delta = 0$ とおくと, 解読可能な条件 β の上限値が $\beta < 3/8$ で与えられる.

3.2 B-M method

B-M method も May's method と同じ多項式 (3) と e を法とする解 $(x_0, y_0) = (k+1, p)$ を対象としている. 従って解の上限値なども May's method のときと同じである.

ここで B-M method の特徴について説明する. 格子 L の体積 $|\det B|$ が小さいほどより大きな α, β, δ に対して解を求めることができるため, 可能な限り格子の体積が小さくなるように shift-polynomial が設定される必要がある. 特に本稿で扱う基底行列 B は正方行列なので, その対角成分が小さいことが望ましい. 新たな変数 z を p に割り当てることで正方行列の対角成分が小さくなるように May's method を改良したものが B-M method である.

Shift-polynomial の設定方法は以下のとおりであり, パラメータ τ, σ は後で最適化されるものとする.

$$\begin{aligned} g_{i,j}(x,y,z) &= e^{m-i}x^j z^{\sigma m} f(x,y)^i \qquad (10) \\ &\quad (0 \le i \le m, 0 \le j \le m-i), \\ h_{i,j}(x,y,z) &= e^{m-i}y^j z^{\sigma m} f(x,y)^i \qquad (11) \\ &\quad (0 \le i \le m, 1 \le j \le \tau m). \end{aligned}$$

つまり May's method での shift-polynomial (4) と (5) に $z^{\sigma m}$ をかけている. これは各 shift-polynomial に現れる yz を N に置き換えた後に不要な N を消すことで $\det L$ を小さくすることが狙いである. 具体的には, 最高次数の係数に現れる N の次数を ℓ としたときに, 多項式全体を N^ℓ で割っても解に影響を与えることなく対角成分を N^ℓ 小さくできる. こうすることで $\det L$ の値が小さくなり, より大きな α, β, δ に対して解を求めることができるようになる.

最終的に [1] で

$$\begin{aligned} \delta &< \frac{1}{3}((1-\beta)(\beta+3) \qquad (12) \\ &\quad -\sqrt{\beta^4 - 5\beta^3 + (4-12\alpha)\beta^2 + 12\alpha\beta}). \end{aligned}$$

が与えられている.

4 Takagi's RSA 暗号の解析

この節では May's method と B-M method を Takagi's RSA に拡張した場合に, その解読に必要な e, p, d_q の大きさの条件, すなわち α, β, δ の条件を示す.

4.1 準備

$N = p^r q$ で $p < N^\beta$, $d_q < N^\delta$ とする．May's method で紹介した $f(x,y)$ と同様の方法で，e を法として $(x_0, y_0) = (k+1, p^r)$ を解に持つ多項式

$$f(x,y) = x(N-y) - N \tag{13}$$

を得る．

4.2 May's method による解析

まず，May's method での解析結果について述べる．$p < N^\beta$ で，(13) の解 y_0 は p^r より，y_0 の上限値 Y は $N^{\beta r}$ となる．第 3.1 節 で述べた手順を進めることで

$$\delta < 1 - \frac{2}{3}\left(\sqrt{r^2\beta^2 + 3r\alpha\beta} + r\beta\right). \tag{14}$$

を得ることができる．通常の RSA 暗号に対応する条件 $r = 1$ のときに (14) が第 3.1 節の結果 (9) と一致することから，(14) が自然に拡張されたものであることがわかる．ここで，第 3.1 節と同様に Takagi's RSA 暗号を本手法で解読できるための p の大きさ N^β について考える．従って，同様に $\alpha = 1, \delta = 0$ として

$$\beta < \frac{3}{8r} \tag{15}$$

であることがわかる．次に $p \approx q$ のときに解読できるための e の大きさ N^α について考える．このとき $\beta = 1/(r+1)$ に注意して，同様に $\delta = 0$ として (14) より，

$$\alpha < \frac{3-r}{4r} \tag{16}$$

が得られる．

4.3 B-M method による解析

次に B-M method での解析結果について述べる．Shift polynomial $g_{i,j}(x,y,z), h_{i,j}(x,y,z)$ は (10) (11) で与えられ，それらの最高次の項はそれぞれ

$$e^{m-i}x^{i+j}y^j z^{\sigma m} = \begin{cases} e^{m-i}x^{i+j}z^{\sigma m - i} \\ (0 \le i \le \sigma m - 1, 0 \le j \le m-i), \\ e^{m-i}x^{i+j}y^{i-\sigma m} \\ (\sigma m \le i \le m, 0 \le j \le m-i), \end{cases}$$

$$e^{m-i}x^j y^{i+j} z^{\sigma m}(0 \le i \le m, 1 \le j \le \tau m) = \begin{cases} e^{m-i}x^j z^{i+j-\sigma m} & (i+j > \sigma m), \\ e^{m-i}x^j y^{\sigma m - i - j} & (i+j \le \sigma m) \end{cases}$$

となる．従って，

$$\begin{aligned}
&\deg_e(\log_N L)) = \frac{m^3}{6}(2 + 3\tau + o(1)), \\
&\deg_X(\log_N L)) = \frac{m^3}{6}(2 + 3\tau + o(1)), \\
&\deg_Y(\log_N L)) \\
&= \frac{m^3}{6}(3\tau^2 + (3-6\sigma)\tau + 3\sigma^2 - 3\sigma + 1 + o(1)), \\
&\deg_Z(\log_N L)) = \frac{m^3}{6}(3\sigma^2 + o(1))
\end{aligned}$$

となり，$Z \le N^{1-r\beta}$ に注意して，e, X, Y, Z と N の関係から

$$\begin{aligned}
&\log_N \det(L) \\
&= \frac{m^3}{6}\{\alpha(2+3\tau) + (\alpha + r\beta + \delta - 1)(2 + 3\tau) \\
&+ r\beta(3\tau^2 + (3-6\sigma)\tau + 3\sigma^2 - 3\sigma + 1) \\
&+ (1 - r\beta)3\sigma^3 + o(1)\}
\end{aligned} \tag{17}$$

を得る．ここで，簡単のため $\beta' = r\beta$ とする．(6), (8) と (17) から

$$\begin{aligned}
&F(\sigma) \\
&= 3\sigma^2 + (-6\beta'\tau - 3\beta')\sigma + \alpha + 6\beta'\tau + 3\beta' \\
&+ 3\delta\tau + 2\delta - 3\tau - 2 + 3\beta'\tau^2 \\
&= 3\left(\sigma + \frac{-2\beta'\tau - \beta'}{2}\right)^2 + (-3\beta'^2 + 3\beta')\tau^2 \\
&+ (-3\beta'^2 + 6\beta' + 3\delta - 3)\tau - \frac{3}{4}\beta'^2 + \alpha + 3\beta' \\
&+ 2\delta - 2
\end{aligned}$$

を得る．$\sigma_0 = \frac{2\beta'\tau+\beta'}{2}$ のとき最少となり

$$\begin{aligned}
&F_{\sigma_0}(\tau) := F(\sigma_0)\\
&= 3\beta'(1-\beta')\left(\tau - \frac{(\beta'-1)^2-\delta}{2\beta'(1-\beta')}\right)^2\\
&-\frac{3((\beta'-1)^2-\delta)^2}{4\beta'(1-\beta')} - \frac{3}{4}\beta'^2 + \alpha + 3\beta'\\
&+2\delta - 2 < 0
\end{aligned}$$

さらに $\tau_0 = \frac{(\beta'-1)^2-\delta}{2\beta'(1-\beta')}$ のとき最少より，

$$\begin{aligned}
&F_{\sigma_0,\tau_0}(\delta) := F_{\sigma_0}(\tau_0)\\
&= -\frac{3((\beta'-1)^2-\delta)^2}{4\beta'(1-\beta')} - \frac{3}{4}\beta'^2 + \alpha + 3\beta' + 2\delta\\
&= \frac{1}{4\beta'(1-\beta')}\{-3\left(\delta - \frac{-\beta'^2-2\beta'+3}{3}\right)^2\\
&+\frac{(-\beta'^2-2\beta'+3)^2}{3} - 3\beta'^3 + 2\beta'^2 + 4\beta' - 3\\
&+4\alpha\beta' - 4\beta'^2\alpha\} < 0
\end{aligned}$$

よって，$\beta'(1-\beta') > 0$ より

$$\begin{aligned}
&3\left(\delta - \frac{-\beta'^2-2\beta'+3}{3}\right)^2\\
&> \frac{\beta'}{3}(\beta'^3 - 5\beta'^2 + (4-12\alpha)\beta' + 12\alpha)(>0).
\end{aligned}$$

最終的に

$$\begin{aligned}
\delta &< \frac{1}{3}((1-\beta')(\beta'+3) \qquad (18)\\
&-\sqrt{\beta'^4 - 5\beta'^3 + (4-12\alpha)\beta'^2 + 12\alpha\beta'}).
\end{aligned}$$

を得る．これは，オリジナルの B-M method の結果における条件 $r = 1$ のときの (12) に一致し，(18) も自然に拡張されたものであることがわかる．ここで，Takagi's RSA 暗号に本手法が適応できるための p の大きさ N^β について考える．従って，同様に $\alpha = 1, \delta = 0$ として

$$\beta < \frac{-5+\sqrt{61}}{6r}. \qquad (19)$$

をえる．次に $p \approx q$ のときに本手法を適応するための e の大きさ N^α について考えると

$$\alpha < \frac{-r^2+5r+3}{4r(r+1)} \qquad (20)$$

が得られる．

5 まとめ

本稿では May の手法と Bleichenbacher-May の手法を用いて Takagi's RSA 暗号の解析を行った．その結果得られた α, β, γ の関係式 (14) と (18) がともに, 通常の RSA 暗号場合の結果を自然に拡張させたものであることを得た．さらにこれらの関係式から, Takagi's RSA 暗号を解読するための p の条件 (15) と (19), e の条件 (16) と (20) を示した．これらの結果は Takagi's RSA 暗号においても CRT-exponent が十分小さいときに May's method と B-M method を適用できることを意味している．

参考文献

[1] D. Bleichenbacher, A. May, "New Attacks on RSA with Small Secret CRT-Exponents," PKC 2006. LNCS 3958, pp. 1-13, 2006.

[2] N. Howgrave-Graham, "Finding small roots of univariate modular equations revisited," Proc. of Cryptography and Coding, LNCS 1355, pp. 131-142, 1997.

[3] K. Itoh, N. Kunihiro, K. Kurosawa, "Small Secret Key Attack on a Takagi's Variant of RSA," IEICE Trans. Fundamentals, Vol. E92-A, no.1, pp. 33-41, 2009.

[4] A. Lenstra, H. Lenstra, L. Lovasz, "Factoring polynomials with rational coefficients," Mathematische Annalen 261(4), pp. 515-534, 1982.

[5] A. May, "Cryptanalysis of Unbalanced RSA with Small CRT-Exponent," Advances in Cryptology - Crypto'02, LNCS 2442, pp. 242-256, 2002.

[6] T. Takagi, "Fast RSA-Type Cryptosystem Modulo $p^k q$," in Proc. of Crypto'98, LNCS 1462, pp.318-326, 1998.