Computer Security Symposium 2016
11 - 13 October 2016

CRT-RSAを攻撃する格子の新たな構成法

高安敦[1,a)]　盧堯[1]　彭力強[2]

概要：May (Crypto'02) によってその脆弱性が初めて指摘され，CRT 秘密鍵の小さな RSA 暗号への攻撃として Bleichenbacher-May(PKC'06) と Jochemsz-May(Crypto'07) の攻撃が知られている．これらの結果の価値は提案攻撃の提案のみにとどまらず，その構成法が後に別の文脈の攻撃においても利用されている点があげられる．本稿で我々は，CRT-RSA の鍵生成の方程式が持つ代数的性質をより有効に活用することにより，Bleichenbacher-May の攻撃と Jochemsz-May の攻撃を改良する．我々が提案する構成法は，今後別の文脈においても利用される有用なものであると考えている．

キーワード：暗号，CRT-RSA，LLL アルゴリズム，Coppersmith の手法

A New Lattice Construction Technique for Attacking CRT-RSA

Atsushi Takayasu[1,a)]　Yao Lu[1]　Liqiang Peng[2]

Abstract: May (Crypto'02) revealed the vulnerability of small CRT exponent RSA. Thus far, the attacks proposed by Bleichenbacher-May(PKC'06) and Jochemsz-May(Crypto'07) are the state-of-the-art. Contributions of these papers are not only the proposed attacks but also the lattice construction strategies which have been used in several subsequent works. In this paper, we propose a novel lattice construction technique which makes use of the algebraic structure of the CRT-RSA key generation. Our technique improves Bleichenbacher-May's attack and Jochemsz-May's attack. We believe that our technique will be used for attacking CRT-RSA in other attack scenarios.

Keywords: Cryptography, CRT-RSA, LLL algorithm, Coppersmith's method

1. 序論

1.1 背景

RSA 暗号の公開鍵 N はビット長の異なる二つの素数 p と q の積であり，暗号化指数 e と復号指数 d は $ed = 1 \pmod{(p-1)(q-1)}$ を満たす．公開鍵 N の素因数分解が困難であることは RSA 暗号が安全であるために必要である．復号指数 d を小さくすると，復号コスト・署名生成コストを削減することができ，より効率的になる．しかし，d が小さすぎると RSA 法 N は多項式時間で素因数分解されてしまうことが Wiener によって示された [34]．その後，Boneh と Durfee [4] によって $d < N^{0.292}$ のときに多項式時間で RSA 法 N を素因数分解する改良攻撃が提案された．この攻撃は LLL 格子簡約アルゴリズム [16] を用いる Coppersmith の法付き方程式を解く手法 [6] に基づいており，厳密な証明はないものの，様々な論文 [1], [14] でこの攻撃の最適性が言及されている．

Boneh-Durfee の攻撃を回避しつつ RSA 暗号の復号・署名生成を高速に行うために，中国人の剰余定理を利用した CRT-RSA が用いられる．CRT-RSA では復号指数 d の代わりに CRT 復号指数 d_p と d_q を用い，これらは $ed_p = 1 \pmod{p-1}$ と $ed_q = 1 \pmod{q-1}$ を満たす．復号指数 d が小さいときの攻撃があるように，CRT 復号指数 d_p, d_q が小さいときの攻撃が存在するかは RSA 暗号の安全性解析において理論的に興味深い問題である．この問題に対して，May (Crypto'02) は Coppersmith の法付き方程式を解

[1] 東京大学
The University of Tokyo
[2] 中国科学院
Chinese Academy of Science
[a)] a-takayasu@it.k.u-tokyo.ac.jp

く手法 [6] を用いて初めて CRT 復号指数が小さいときの多項式時間攻撃を提案した [19]．May の攻撃は d_q のみが小さいことを利用しており，d_p の大きさに制限はない．ただし，この攻撃は p が q よりビット長が異なるほど十分小さいときにしか適用できず，条件 $p < N^{0.384}$ が必要である．Bleichenbacher と May (PKC'06) は，May の攻撃に用いる格子に $N = pq$ なる関係を利用することで改良攻撃を提案した [3]．だが，Bleichenbacher-May の攻撃ですら $p < N^{0.468}$ のときにしか適用できない．その後，この攻撃状況における改良攻撃は報告されておらず，適用条件を $p < N^{0.5}$ まで改良するような攻撃の構成はこれらの論文で指摘され，10 年間解決されていない重要な未解決問題である．

d_q のみが小さいことを仮定する上記の攻撃は素数 p と q のビット長が異なる，実用的には利用されない状況でしか適用できない．そのため，d_p と d_q がいずれも小さいときの攻撃を Bleichenbacher と May は提案した [3]．この攻撃は Coppersmith の整数方程式を解く手法 [5] を用いているため，前述の攻撃とは構成が完全に異なる．この攻撃は p と q のビット長が等しくても適用可能だが，$e < N$ のときにしか適用できない．Jochemsz と May (Crypto'07) は，格子の構成を変更することで，e のビット長が N と等しくても $d_p, d_q < N^{0.073}$ のときに多項式時間で N を素因数分解する改良攻撃を提案した [13]．e が N に対して十分小さい場合を除いて [8], [25]，この攻撃の改良はこれまで報告されていない．

このように，Coppersmith の手法 [5], [6] を用いて CRT-RSA を攻撃する文脈では，Bleichenbacher-May の攻撃 [3] と Jochemsz-May の攻撃 [13] は既存の最高の結果であり，特に前者の攻撃は Shinohara ら [24] と Peng ら [22] によって RSA の変形方式に対する拡張攻撃も提案されている．また，これらの論文の価値は提案攻撃にとどまらず，そこで用いる格子の構成法は CRT-RSA を攻撃する他の文脈 [10], [17], [23], [30], [32] でも利用されているという点で技術的にも大いに意義がある結果である．

1.2 技術的困難

Bleichenbacher-May と Jochemsz-May の CRT 復号指数が小さい RSA の攻撃の改良は, 技術的に非常に困難であることが予想される．Bleichenbacher-May の攻撃と Jochemsz-May の攻撃は，いずれも Jochemsz と May (Asiacrypt '06) によって定式化された Coppersmith の手法における格子の構成に関する枠組み [12] に沿っている．さらに，前者の攻撃は，Durfee と Nguyen (Asiacrypt '00) が導入した格子の構成において $N = pq$ なる関係を利用し適用範囲を拡大する手法 [7] をも用いていおり，この文脈で適用しうる全ての既存技術を活用したものになっている．よって，Coppersmith の手法における格子の構成に関して，既存手法とは一線を画す完全に新たな枠組みが考案されない限りこれらの改良は困難であることが予想される．

Bleichenbacher-May の攻撃と Jochemsz-May の攻撃の提案後，Herrmann と May (Asiacrypt '09) によって unravelled linearization [9] と呼ばれる新たな証明技法が提案された．この画期的な証明技法は，提案以降多くの論文 [2], [10], [14], [15], [26], [28], [29], [31], [33] で活用され，Coppersmith の手法を用いる RSA 暗号の安全性解析の研究を大きく進展させた．だが, CRT 復号指数が小さい RSA の攻撃を改良するという点では，この証明技法は不十分であった．Herrmann と May (PKC '10) は，unravelled linearization を用いて Jochemsz-May の攻撃を解析した [10] が，扱う格子の次元を小さくすることには成功したが，適用範囲を拡大するには至らなかった．

1.3 貢献

本稿で我々は，Bleichenbacher-May の攻撃 [3] と Jochemsz-May の攻撃 [13] の改良攻撃を提案する．前者の攻撃設定において我々は，May [19] や Bleichenbacher-May [3] によって重要な未解決問題とされていた，条件 $p < N^{0.5}$ の下で N を多項式時間で素因数分解する攻撃を構成する．我々の攻撃は，全てのパラメータにおいて Bleichenbacher-May の攻撃よりも適用範囲が広く，かつ，効率的である．より正確に言えば，我々は Bleichenbacher-May の攻撃の適用条件は必ずより小さな次元の格子を用いて達成可能であることを示し，また，さらに次元の大きな格子を用いれば適用範囲を拡大できることを示す．ページ数の都合で本稿では省略するが，我々はこの事実を実験的にも確認している．さらに，Jochemsz-May の攻撃設定において我々は，e のビット長が N と等しくても $d_p, d_q < N^{0.091}$ のときに多項式時間で N を素因数分解する改良攻撃を提案し，この条件は N の指数が Jochemsz-May のものより約 25%も改善された値となっている．我々の攻撃は，e が小さいときにも常に Jochemsz-May の攻撃を改良している．本稿の貢献は，Bleichenbacher-May [3] や Jochemsz-May [13] と同様，改良攻撃の提案のみならず，ここで用いられる技術は CRT-RSA の攻撃に関する他の文脈において適用可能であると考えている．事実，提案攻撃を拡張することで，RSA の変形方式に対する Shinohara らの攻撃 [24] と Peng らの攻撃 [22] を改良している．

1.4 技術的概要

詳細は第 3 章以降に譲るが, ここで簡単に Bleichenbacher-May の攻撃に対する我々の改良攻撃を構成に関する技術的概要について述べる．秘密鍵 d_q が小さいという条件を利用するために，その鍵生成に注目すると，ある整数 k_q を用いて $ed_q = 1 + k_q(q-1)$ と書くことができ，$N = pq$ なる関係を用いると，両辺に p を掛けることで

$ed_q p = p + k_q(N-p) = N + (k_q - 1)(N-p)$ なる方程式に変形できる．よって，May [19] は法付き方程式

$$f_p(x_p, y_p) = N + x_p(N + y_p) = 0 \pmod{e}$$

を解くことで $(x_p, y_p) = (k_q - 1, p)$ を計算し，N の素因数分解を行った．ここで Coppersmith の手法 [6] を用いてこの方程式を解くために May が構成した格子は，後に Jochemsz と May によって定式化される，この研究分野における最も標準的な構成法 [12] に基づいている．この攻撃を改良するために，Bleichenbacher と May [3] は，May と同じ方程式 $f_p(x_p, y_p) = 0$ を解いたが，方程式に陽には現れない新たな変数 $y_q = q$ を導入した．攻撃者はこの解を正確にはわからないが，$y_p y_q = N$ なる方程式を満たすことはわかっている．これは Durfee と Nguyen によって紹介された技法であり，これによって同じ方程式をより良い条件で解くことができる．

我々が注目したのは，秘密鍵 d_q の鍵生成方程式 $ed_q = 1 + k_q(q-1)$ である．素朴にこの方程式を定式化すると，

$$f_q(x_q, y_q) = 1 + x_q(N + y_q) = 0 \pmod{e}$$

なる法付き方程式が得られ，その解は $(x_q, y_q) = (k_q, q)$ である．p が q より小さいという点で，May や Bleichenbacher-May が $f_q(x_q, y_q) = 0$ ではなく $f_p(x_p, y_p) = 0$ を解いたのは妥当な方針である．しかし，これらの攻撃では $f_q(x_q, y_q) = 0$ の情報が完全に失われており，p が q より小さいという設定に大きく依存した構成となっており，$p < N^{0.5}$ という条件を達成できないのは自然である．そのため，我々は $f_p(x_p, y_p) = 0$ と $f_q(x_q, y_q) = 0$ という二つの方程式を相補的に用いて攻撃を構成する．これらはいずれも秘密鍵 d_q の鍵生成方程式から得られるという点で本質的には同じものだが，二つの異なる表現を同時に用いるというのが既存手法とは異なる点である．我々は p に依存するパラメータによっていずれの方程式を使うかの割合を適応的に変化させ，p が漸近的に 1 に近づくほど小さいときには $f_p(x_p, y_p) = 0$ のみを用い，p が漸近的に $N^{0.5}$ に近づくほど大きいときには二つの方程式を同じ割合で用いる．前述の通り，Bleichenbacher-May の攻撃と Jochemsz-May の攻撃は完全に異なる構成に基づいていたが，本稿で我々が提案する格子の構成技法は，同様にして Jochemsz-May の攻撃をも改良するほど強力なものである．

2. 準備

この章で，Coppersmith の法付き方程式を解く手法 [6] を簡単にまとめる．ただし，より理解しやすいため，Howgrave-Graham [11] の再定式化を説明する．ただし，ページ数の都合のため説明は最小限にとどめる．

一般に，r 変数法付き方程式 $h(x_1, \ldots, x_r) = 0 \pmod{W}$ の全ての解を求めることは不可能である．ただし，Coppersmith の手法では，取りうる解の絶対値が十分小さいときには多項式時間でその小さな解を計算することができる．方針としては解くべき法付き方程式と同じ解を整数上で持つ多項式を r 個見つければ良いが，以下の補題からそのためには整数 m に対して法 W^m で同じ解を持つ係数の小さな多項式を見つければ良いことがわかる．

補題 1 (Howgrave-Graham の補題 [11]) 多項式 $\tilde{h}(x_1, \ldots, x_r) \in \mathbb{Z}[x_1, \ldots, x_r]$ は，最大 n 個の単項を持ち，$m, W, X_1, \ldots, X_r$ を正の整数とする．以下の条件:

1 $\tilde{h}(\tilde{x}_1, \ldots, \tilde{x}_r) = 0 \pmod{W^m}$, $|\tilde{x}_1| < X_1, \ldots, |\tilde{x}_r| < X_r$,

2 $||\tilde{h}(x_1 X_1, \ldots, x_r X_r)|| < W^m/\sqrt{n}$,

が成り立つならば，$\tilde{h}(\tilde{x}_1, \ldots, \tilde{x}_r) = 0$ が整数上で成り立つ．

同じ解を持つ係数の小さな多項式を見つけるために，格子と LLL アルゴリズムを用いる．線形独立な n 本の $\mathbb{Z}^n$ 行ベクトル $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ で張られる格子 $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ を $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) = \{\sum_{j=1}^{n} c_j \boldsymbol{b}_j : c_j \in \mathbb{Z}\}$ と定義する．格子基底は，基底ベクトルを各行に並べた行列 $\boldsymbol{B} \in \mathbb{Z}^{n \times n}$ を用いても表し，そのとき格子を $L(\boldsymbol{B})$ と書く．同じ格子に対して基底の選び方は無限に存在するが，いずれの基底においてもその体積 $\det(\boldsymbol{B})$ は不変である．LLL アルゴリズムは [16]，多項式時間でノルムの小さな基底ベクトルを計算可能で，そのノルムの大きさが May [20] によって証明されている．

命題 1 (LLL アルゴリズム [16], [20]) 線形独立な $\mathbb{Z}^n$ 上のベクトル $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ が与えられたとき，*LLL* アルゴリズムは格子 $L(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ の基底 $\tilde{\boldsymbol{b}}_1, \ldots, \tilde{\boldsymbol{b}}_n$ を n と入力長の多項式時間で計算し，全ての $1 \le j \le n$ において

$$||\tilde{\boldsymbol{b}}_j|| \le 2^{n(n-1)/4(n-j+1)} \det(L(\boldsymbol{B}))^{1/(n-j+1)}$$

が成り立つ．

法付き方程式 $h(x_1, \ldots, x_r) = 0 \pmod{W}$ を解くためには，法 W^m のもとで同じ解を持つ n 個の多項式 $h_j(x_1, \ldots, x_r)$ を構成し，$h_j(x_1 X_1, \ldots, x_r X_r)$ の係数からなる基底行列 $\boldsymbol{B}$ によって張られる格子 $L(\boldsymbol{B})$ の短いベクトルを LLL アルゴリズムによって計算し，そのベクトルの成分を係数とする r 個の多項式 $\tilde{h}_j(x_1, \ldots, x_r)$ が Howgrave-Graham の補題を満たすほどノルムが小さければ，これらの多項式のグレブナー基底を計算するなどしてその解を計算することができる．ただし，この手法は LLL アルゴリズムの出力ベクトルから構成される多項式がそれぞれ代数的に独立である保証がないためヒューリスティックである．本稿ではこれらの多項式が代数的に独立であることを仮定して議論する．一般に実装上は代数的に従属な多項式が得

られることは稀であり，なおページ数の都合で詳細なデータは省略するが，我々は構成したアルゴリズムの妥当性を計算機実験によって確認している．

3. Bleichenbacher-May 攻撃の改良

第 1.4 章で述べたように，秘密鍵 d_q の鍵生成方程式 $ed_q = 1 + k_q(q-1)$ から得られる二つの方程式

$$f_p(x_p, y_p) = N + x_p(N + y_p) = 0 \pmod e$$
$$f_q(x_q, y_q) = 1 + x_q(N + y_q) = 0 \pmod e$$

の解 $(x_p, x_q, y_p, y_q) = (k_q - 1, k_q, p, q)$ を求めたい．ただし，$e = N^\alpha, d_q = N^\delta$ とし，$0 < \beta \leq 1/2$ に関して $p = N^\beta$ とする．それぞれの解の大きさは，$X_p := N^{\alpha+\beta+\delta-1}, X_q := N^{\alpha+\beta+\delta-1}, Y_p := N^\beta, Y_q := N^{1-\beta}$ の定数倍で抑えられる．簡単のため，$X := X_p = X_q$ なる記法をも用いる．

3.1 基底行列の概要

我々の格子の構成技法は一見複雑であるため，読者の理解を容易にするため，この章で簡単な例を使ってその概要を既存研究のものと比較する．

3.1.1 May の行列

May [19] の構成する行列は，Jochemsz-May の構成技法 [12] に従う基本的なものである．方程式 $f_p(x_p, y_p) = 0$ を解くために，May は以下の行列を構成した．

$$\begin{pmatrix}
e & & & & & & \\
0 & eX_p & & & & & \\
N & NX_p & -X_pY_p & & & & \\
0 & 0 & 0 & eY_p & & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & & \\
0 & 0 & 0 & 0 & 0 & eY_p^2 & \\
0 & 0 & 0 & 0 & NX_pY_p^2 & NY_p^2 & -X_pY_p^3
\end{pmatrix}$$

この行列は，7 つの多項式 e,ex_p,$f_p(x_p, y_p)$,ey_p,$y_pf_p(x_p, y_p)$, ey_p^2,$y_p^2f_p(x_p, y_p)$ の係数からなり，いずれも e を法として元の方程式と同じ解 $(x_p, y_p) = (k_q - 1, p)$ を持つ．

3.1.2 Bleichenbacher-May の行列

Bleichenbacher-May [19] は，同じ方程式 $f_p(x_p, y_p) = 0$ を解くために，Durfee-Nguyen [7] と同様新たな変数 $y_q = q$ を導入し，$y_py_q = N$ なる関係を利用して以下の行列を構成した．

$$\begin{pmatrix}
e & & & & & & \\
0 & eX_p & & & & & \\
N & NX_p & -X_pY_p & & & & \\
0 & 0 & 0 & eY_p & & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & & \\
0 & 0 & 0 & 0 & 0 & eY_q & \\
0 & -X_p & 0 & 0 & 0 & Y_q & X_pY_q
\end{pmatrix}$$

ここで用いられている多項式は，May の行列から ey_p^2 と $y_p^2f_p(x_p, y_p)$ を削除し，代わりに ey_q と $N^{-1} \cdot y_qf_p(x_p, y_p)$ を加えたものである．これらの新たな多項式は，いずれも e を法として元の方程式と同じ解 $(x_p, y_p, y_q) = (k_q - 1, p, q)$ を持つ．対応する対角成分の大きさは，May の行列では eY_p^2 と $X_pY_p^3$ だったものが eY_q と X_pY_q となっている．よって，Bleichenbacher-May の行列は，May の行列から e と X_p の寄与を変えないまま，Y_q が新たに出てきはするが X_p の冪を削減している．この操作により，y_p と y_q の割合を適切に調整すれば，Bleichenbacher-May の攻撃はパラメータ α と β の全ての値に対して May の攻撃を改良することができる．

3.1.3 提案手法

我々の新たな構成技法に基づく行列の概要を述べる．第 1.4 章で述べた通り，提案手法の核となるアイディアは，方程式 $f_p(x_p, y_p) = 0$ のみならず $f_q(x_q, y_q) = 0$ をも利用するところである．提案手法による行列は以下のようになる．

$$\begin{pmatrix}
e & & & & & & \\
0 & eX_p & & & & & \\
N & NX_p & -X_pY_p & & & & \\
0 & 0 & 0 & eY_p & & & \\
0 & 0 & NX_pY_p & NY_p & -X_pY_p^2 & & \\
0 & -X_p & 0 & 0 & 0 & X_qY_q &
\end{pmatrix}$$

ここで用いられている多項式は，Bleichenbacher-May の行列から ey_q と $N^{-1} \cdot y_qf_p(x_p, y_p)$ を削除し，代わりに $f_q(x_q, y_q)$ を加えたものである．ただし，$x_p + 1 = x_q$ なる関係を用いている．この新たな多項式は，e を法として元の方程式と同じ解 $(x_p, x_q, y_p, y_q) = (k_q - 1, k_q, p, q)$ を持つ．対応する対角成分の大きさは，Bleichenbacher-May の eY_q と X_pY_q を X_qY_q に置き換えたものになっている．つまり，X_pY_q と X_qY_q はほとんど同じ大きさだが，eY_q を削除することに成功している．削除された対角成分は法の値 e よりも大きく，行列を下三角のままでこのような多項式を削除することは攻撃の改良に繋がることがこれまでの研究でわかっている [21], [27]．この結果は，Bleichenbacher-May の構成した行列には不要な多項式が含まれており，適切にこのような多項式を削除すると，より小さな次元の行列を用いて Bleichenbacher-May の攻撃を実装可能であることを示しており，さらに，方程式 $f_p(x_p, y_p) = 0$ と $f_q(x_q, y_q) = 0$ の割合を適切に設定すれば，提案手法はパラメータ α と β の全ての値に対して Bleichenbacher-May の攻撃を改良することができる．

3.2 提案攻撃

この章で次の定理を証明する．

定理 1 $N = pq$ は *RSA* 法で，$0 < \beta \leq 1/2$ に対して $p = N^\beta, q = N^{1-\beta}$ を満たす．暗号化指数 $e = N^\alpha$ と *CRT* 復号指数 $d_q < N^\delta$ は $ed_q = 1 \pmod{(q-1)}$ を満たす．

LLL アルゴリズムの出力するベクトルによって構成される多項式が代数的に独立であることを仮定し，条件 $\alpha > \frac{\beta}{1-\beta}$ と

$$\delta < \frac{(1-\beta)(3+2\beta) - 2\sqrt{\beta(1-\beta)(\alpha\beta+3\alpha+\beta)}}{3+\beta}$$

を満たすとき，または，条件 $\beta(1-\beta) \leq \alpha \leq \frac{\beta}{1-\beta}$ と

$$\delta < 1 - \beta - \sqrt{\alpha\beta(1-\beta)}$$

を満たすとき，公開要素 N と e のみから *RSA* 法 N を多項式時間で素因数分解することができる．

3.2.1 $\alpha > \frac{\beta}{1-\beta}$ の攻撃

まず，$\alpha > \frac{\beta}{1-\beta}$ のときのアルゴリズムの構成を示す．任意の正の整数 m に対して，次の 3 つの多項式を用いて行列を構成する．

$$\begin{aligned} g_{[i,j]}(x_p, y_p) &:= x_p^j f_p^i(x_p, y_p) e^{m-i} \\ g'_{[i,j]}(x_p, y_p) &:= y_p^j f_p^i(x_p, y_p) e^{m-i} \\ g''_{[i,j]}(x_p, x_q, y_p, y_q) &:= f_p^{i-j}(x_p, y_p) f_q^j(x_q, y_q) e^{m-i} \end{aligned}$$

これらの多項式は，いずれも e^m を法として元の方程式と同じ解 $(x_p, x_q, y_p, y_q) = (k_q - 1, k_q, p, q)$ を持つ．$\tau_p \geq 0$ と $0 \leq \tau_q \leq 1$ を満たす二つのパラメータを用いて，行列に選ぶ多項式のインデックスを次のように定義する．

$$\begin{aligned} \mathcal{I} &:= \{i = 0, 1, \ldots, m; j = 0, 1, \ldots, m - i\} \\ \mathcal{I}' &:= \{i = 0, 1, \ldots, m; j = 1, 2, \ldots, \lceil \tau_p m \rceil\} \\ \mathcal{I}'' &:= \{i = 1, 2, \ldots, m; j = 1, 2, \ldots, \lceil \tau_q i \rceil\} \end{aligned}$$

行列 $\boldsymbol{B}$ を多項式 $g_{[i,j]}(x_pX_p, y_pY_p)$，$g'_{[i,j]}(x_pX_p, y_pY_p)$，$g''_{[i,j]}(x_pX_p, x_qX_q, y_pY_p, y_qY_q)$ の係数ベクトルによって構成する．ただし，それぞれの多項式のインデックス (i, j) は，$\mathcal{I}, \mathcal{I}', \mathcal{I}''$ なるものを選ぶ．行列 $\boldsymbol{B}$ において多項式を以下のように並べる．

- $g_{[i,j]} \prec g'_{[i,j]}, g'_{[i,j]}$
- $i < i'$ のとき $g_{[i,j]} \prec g_{[i',j']}, g'_{[i,j]} \prec g'_{[i',j']}$, $g''_{[i,j]} \prec g''_{[i',j']}$
- $j < j'$ のとき $g_{[i,j]} \prec g_{[i,j']}, g'_{[i,j]} \prec g'_{[i,j']}, g''_{[i,j]} \prec g''_{[i,j']}$

多項式の各単項において，y_py_q は全て N で置き換え，対角成分に N の冪乗が現れないよう適切に $N^{-1} \pmod{e^m}$ を掛ける．この操作は，Durfee-Nguyen [7] や Bleichenbacher-May [3] と同じである．このとき，詳細は省略するが，行列 $\boldsymbol{B}$ は以下の対角成分を持つ三角行列になる．

- $g_{[i,j]}(x_pX_p, y_pY_p)$ の対角成分は $X_p^{i+j} Y_p^i e^{m-i}$
- $g'_{[i,j]}(x_pX_p, y_pY_p)$ の対角成分は $X_p^i Y_p^{i+j} e^{m-i}$
- $g''_{[i,j]}(x_pY_p, x_qX_q, y_pY_p, y_qY_q)$ の対角成分は $X_q^i Y_q^j e^{m-i}$

厳密な証明は与えないが，行列 $\boldsymbol{B}$ を三角行列にするための核となるアイディアだけを述べる．まず，素因数を表す 2 つの変数 y_p と y_q があるが，これらは $y_py_q = N$ なる関係によって各単項に必ずどちらかしか存在しない．そして，秘密情報 k_q に対応する 2 つの変数 x_p と x_q があり，$x_p + 1 = x_q$ なる関係が成り立つ．この関係を用いて，y_p の指数部が非負である単項においては x_q を全て x_p に置き換え，逆に y_q の指数部が正である単項においては x_p を全て x_q に置き換える．各単項において x_px_q なる成分が登場しないのは，前述の対角成分から確認することができる．この操作によって，第 3.1.3 章で例として挙げた三角行列をさらに高次元に拡張することができる．この性質が本稿の改良攻撃の核となっている．

この攻撃の適用条件を導出する．行列 $\boldsymbol{B}$ の次元を n とし，その行列式を $\det(\boldsymbol{B}) = X^{s_X} Y_p^{s_{Y_p}} Y_q^{s_{Y_q}} e^{s_e}$ とすると，これらは以下のように計算できる．

$$\begin{aligned} n &= \sum_{(i,j)\in\mathcal{I}} 1 + \sum_{(i,j)\in\mathcal{I}'} 1 + \sum_{(i,j)\in\mathcal{I}''} 1 \\ &= \frac{1 + 2\tau_p + \tau_q}{2} m^2 + o(m^2) \\ s_X &= \sum_{(i,j)\in\mathcal{I}} (i+j) + \sum_{(i,j)\in\mathcal{I}'} i + \sum_{(i,j)\in\mathcal{I}''} i \\ &= \frac{2 + 3\tau_p + 2\tau_q}{6} m^3 + o(m^3) \\ s_{Y_p} &= \sum_{(i,j)\in\mathcal{I}} i + \sum_{(i,j)\in\mathcal{I}'} (i+j) \\ &= \frac{1 + 3\tau_p + 3\tau_p^2}{6} m^3 + o(m^3) \\ s_{Y_q} &= \sum_{(i,j)\in\mathcal{I}''} j = \frac{\tau_q^2}{6} m^3 + o(m^3) \\ s_e &= \sum_{(i,j)\in\mathcal{I}} (m-i) + \sum_{(i,j)\in\mathcal{I}'} (m-i) + \sum_{(i,j)\in\mathcal{I}''} (m-i) \\ &= \frac{2 + 3\tau_p + \tau_q}{6} m^3 + o(m^3) \end{aligned}$$

LLL の出力ベクトルが Howgrave-Graham の補題を満たす条件は $X^{s_X} Y_p^{s_{Y_p}} Y_q^{s_{Y_q}} e^{s_e} < e^{nm}$ と書くことができる．m に関する低次の項を無視し，適用範囲を最大化するように $\tau_p = \frac{1-2\beta-\delta}{2\beta}, \tau_q = \frac{1-\beta-\delta}{1-\beta}$ とパラメータを設定すると，条件

$$\delta < \frac{(1-\beta)(3+2\beta) - 2\sqrt{\beta(1-\beta)(\alpha\beta+3\alpha+\beta)}}{3+\beta}$$

が得られる．ただし，制約 $0 \leq \tau_q \leq 1$ は常に成り立つが，制約 $\tau_p \geq 0$ を満たすために，$\alpha > \frac{\beta}{1-\beta}$ が成り立たなければならない．

3.2.2 $\beta(1-\beta) \leq \alpha \leq \frac{\beta}{1-\beta}$ の攻撃

次に，$\beta(1-\beta) \leq \alpha \leq \frac{\beta}{1-\beta}$ のときのアルゴリズムの構成を示す．技術的には前章の構成より複雑にはなるが，核となるアイディアは同じである．さらに，第 4 章と第 5 章で他の攻撃状況に適用する際には，本章の構成を利用する．

任意の正の整数 m と $0 < \lambda \leq 1$ なるパラメータに対して，次の 2 つの多項式を用いて行列を構成する．

$$
\begin{aligned}
&g_{[i,j],\lambda}(x_p, x_q, y_p, y_q)\\
&:= x_p^j f_p^{\lceil \lambda i \rceil}(x_p, y_p) f_q^{\lfloor (1-\lambda) i \rfloor}(x_q, y_q) e^{m-i}\\
&g'_{[i,j],\lambda}(x_p, x_q, y_p, y_q)\\
&:= y_q^j f_p^{\lceil \lambda i \rceil}(x_p, y_p) f_q^{\lfloor (1-\lambda) i \rfloor}(x_q, y_q) e^{m-i}
\end{aligned}
$$

これらの多項式は，いずれも e^m を法として元の方程式と同じ解 $(x_p, x_q, y_p, y_q) = (k_q - 1, k_q, p, q)$ を持つ．ここで，任意の非負整数 i に対して $\lceil \lambda i \rceil + \lfloor (1-\lambda) i \rfloor = i$ となる．$1 - \lambda < \tau \leq 1$ なるパラメータを用いて，行列に選ぶ多項式のインデックスを次のように定義する．

$$
\begin{aligned}
\mathcal{I} &:= \{i = 0, 1, \ldots, m; j = 0, 1, \ldots, m - i\}\\
\mathcal{I}' &:= \{i = 1, 2, \ldots, m; j = 1, 2, \ldots, \lceil \tau i \rceil - \lfloor (1-\lambda) i \rfloor\}
\end{aligned}
$$

行列 $\boldsymbol{B}$ を多項式 $g_{[i,j],\lambda}(x_p X_p, x_q X_q, y_p Y_p, y_q Y_q)$ と $g'_{[i,j],\lambda}(x_p X_p, x_q X_q, y_p Y_p, y_q Y_q)$ の係数ベクトルによって構成する．ただし，それぞれの多項式のインデックス (i, j) は，$\mathcal{I}, \mathcal{I}'$ なるものを選ぶ．行列 $\boldsymbol{B}$ において多項式を以下のように並べる．

- $g_{[i,j],\lambda} \prec g'_{[i,j],\lambda}$
- $i < i'$ のとき $g_{[i,j],\lambda} \prec g_{[i',j'],\lambda}$, $g'_{[i,j],\lambda} \prec g'_{[i',j'],\lambda}$
- $j < j'$ のとき $g_{[i,j],\lambda} \prec g_{[i,j'],\lambda}$, $g'_{[i,j],\lambda} \prec g'_{[i,j'],\lambda}$

前章と同様に，多項式の各単項において，$y_p y_q$ は全て N で置き換え，対角成分に N の冪乗が現れないよう適切に $N^{-1} \pmod{e^m}$ を掛ける．さらに，$x_p + 1 = x_q$ なる関係を用いて，y_p の指数部が非負である単項においては x_q を全て x_p に置き換え，逆に y_q の指数部が正である単項においては x_p を全て x_q に置き換える．このとき，詳細は省略するが，行列 $\boldsymbol{B}$ は以下の対角成分を持つ三角行列になる．

- $i = 0$ と $\lceil \lambda i \rceil - \lceil \lambda (i-1) \rceil = 1$ なる i に対して $g_{[i,j],\lambda}(x_p X_p, x_q X_q, y_p Y_p, y_q Y_q)$ の対角成分は $X_p^{i+j} Y_p^{\lceil \lambda i \rceil} e^{m-i}$
- $i \neq 0$ かつ $\lceil \lambda i \rceil - \lceil \lambda (i-1) \rceil = 0$ なる i に対して $g_{[i,j],\lambda}(x_p X_p, x_q X_q, y_p Y_p, y_q Y_q)$ の対角成分は $X_q^{i+j} Y_q^{\lfloor (1-\lambda) i \rfloor} e^{m-i}$
- $g'_{[i,j],\lambda}(x_p X_p, x_q X_q, y_p Y_p, y_q Y_q)$ の対角成分は $X_q^{i} Y_q^{\lfloor (1-\lambda) i \rfloor + j} e^{m-i}$

この攻撃の適用条件を導出する．行列 $\boldsymbol{B}$ の次元を n とし，その行列式を $\det(\boldsymbol{B}) = X^{s_X} Y_p^{s_{Y_p}} Y_q^{s_{Y_q}} e^{s_e}$ とすると，これらは以下のように計算できる．

$$
\begin{aligned}
n &= \sum_{(i,j)\in\mathcal{I}} 1 + \sum_{(i,j)\in\mathcal{I}'} 1 = \frac{\lambda+\tau}{2} m^2 + o(m^2)\\
s_X &= \sum_{(i,j)\in\mathcal{I}} (i+j) + \sum_{(i,j)\in\mathcal{I}'} i = \frac{\lambda+\tau}{3} m^3 + o(m^3)\\
s_{Y_p} &= \sum_{(i,j)\in\mathcal{I}} \lceil \lambda i \rceil = \frac{\lambda^2}{6} m^3 + o(m^3)\\
s_{Y_q} &= \sum_{(i,j)\in\mathcal{I}} \lfloor (1-\lambda) i \rfloor + \sum_{(i,j)\in\mathcal{I}'} (\lfloor (1-\lambda) i \rfloor + j)\\
&= \frac{\tau^2}{6} m^3 + o(m^3)\\
s_e &= \sum_{(i,j)\in\mathcal{I}} (m-i) + \sum_{(i,j)\in\mathcal{I}'} (m-i)\\
&= \frac{1+\lambda+\tau}{6} m^3 + o(m^3)
\end{aligned}
$$

LLL の出力ベクトルが Howgrave-Graham の補題を満たす条件は $X^{s_X} Y_p^{s_{Y_p}} Y_q^{s_{Y_q}} e^{s_e} < e^{nm}$ と書くことができる．m に関する低次の項を無視し，適用範囲を最大化するように $\lambda = \frac{1-\beta-\delta}{\beta}, \tau = \frac{1-\beta-\delta}{1-\beta}$ とパラメータを設定すると，条件

$$
\delta < 1 - \beta - \sqrt{\alpha\beta(1-\beta)}
$$

が得られる．ただし，制約 $0 < \lambda \leq 1$ と $1 - \lambda < \tau \leq 1$ を満たすために，$\beta(1-\beta) \leq \alpha \leq \frac{\beta}{1-\beta}$ が成り立たなければならない．

4. Jochemsz-May 攻撃の改良

この章で，Jochemsz-May 攻撃の改良について述べる．ただし，ページ数の都合で，概要のみにとどめる．

秘密鍵 d_q と d_p の鍵生成方程式は，整数 k_q と k_p を用いて $ed_q = 1 + k_q(q-1), ed_p = 1 + k_p(p-1)$ と書くことができる．これらの方程式より，以下の法付き方程式を解くことができれば，RSA 法 N を素因数分解することができる．

$$
\begin{aligned}
f_{q,1}(x_{q,1}, y_q) &= 1 + x_{q,1}(y_q - 1) = 0 \mod e\\
f_{p,2}(x_{p,2}, y_p) &= 1 + x_{p,2}(y_p - 1) = 0 \mod e
\end{aligned}
$$

これらの方程式の解は $(x_{q,1}, x_{p,2}, y_q, y_p) = (k_q, k_p, q, p)$ である．また，秘密鍵 d_q と d_p の鍵生成方程式にそれぞれ p と q を掛けることで，以下の式が得られる．

$$
\begin{aligned}
ed_q p &= p + k_q(N - p) = N + (k_q - 1)(N - p)\\
ed_p q &= q + k_p(N - q) = N + (k_p - 1)(N - q)
\end{aligned}
$$

これより，方程式 $f_{q,1}(x_{q,1}, y_q) = 0$ と $f_{p,2}(x_{p,2}, y_p) = 0$ の別の表現に対応する以下の方程式が得られる．

$$
\begin{aligned}
f_{p,1}(x_{p,1}, y_p) &= N + x_{p,1}(N - y_p) = 0 \mod e\\
f_{q,2}(x_{q,2}, y_q) &= N + x_{q,2}(N - y_q) = 0 \mod e
\end{aligned}
$$

これらの方程式の解は $(x_{p,1}, x_{q,2}, y_p, y_q) = (k_q - 1, k_p - 1, p, q)$ である．

議論を整理すると，以下の連立法付き方程式を解くことができれば，RSA 法 N を素因数分解することができる．

$$
\begin{aligned}
f_{p,1}(x_{p,1}, y_p) &= N + x_{p,1}(N - y_p) = 0 \mod e\\
f_{q,1}(x_{q,1}, y_q) &= 1 + x_{q,1}(y_q - 1) = 0 \mod e\\
f_{p,2}(x_{p,2}, y_p) &= 1 + x_{p,2}(y_p - 1) = 0 \mod e\\
f_{q,2}(x_{q,2}, y_q) &= N + x_{q,2}(N - y_q) = 0 \mod e
\end{aligned}
$$

これらの方程式の解は $(x_{p,1}, x_{q,1}, x_{p,2}, x_{q,2}, y_p, y_q) = (k_q - 1, k_q, k_p, k_p - 1, p, q)$ である．p と q のビット長が同じ RSA 法に対して $e = N^\alpha$, $d_p < N^\delta, d_q < N^\delta$ なる状況を考える．$x_{p,1}, x_{q,1}, x_{p,2}, x_{q,2}$ の解の絶対値の大きさは $X = N^{\alpha+\delta-1/2}$, y_p と y_q の解の絶対値の大きさは $Y = N^{1/2}$ の定数倍でそれぞれ抑えることができる．

だが，第 3 章で提案した技法を用いて上記連立方程式を解いても攻撃を改良することができず，攻撃の適用条件は定理 1 と同じになる．そのため，我々はさらなる代数的関係を用いることで Jochemsz-May の攻撃を改良する．再び秘密鍵 d_q と d_p の鍵生成方程式より，$k_q - 1 = k_q q \pmod e$ と $k_p - 1 = k_p p \pmod e$ を得る．これらの両辺同士を掛け合わせることで，以下の方程式を得る．

$$(k_q - 1)(k_p - 1) = k_q k_p N \pmod e.$$

よって，同じ未知数 k_q と k_p を解に持つ以下の新たな法付き方程式を得る．

$$\begin{aligned} &h(x_{p,1}, x_{q,1}, x_{p,2}, x_{q,2}) \\ &= (N-1)x_{p,1}x_{p,2} + x_{p,1} + Nx_{p,2} = 0 \pmod e \\ &= (N-1)x_{q,1}x_{q,2} + Nx_{q,1} + x_{q,2} = 0 \pmod e \end{aligned}$$

この方程式は，Galbraith ら [8] が e が小さいときの攻撃に用いた方程式である．この方程式はこれまでのものと同様，未知数 k_q と k_p に対応して，$x_{p,1}$ と $x_{p,2}$ なる変数を持つ，または，$x_{q,1}$ と $x_{q,2}$ なる変数を持つ 2 つの表現がある．この新たな方程式を前述の連立方程式と組み合わせ，第 3 章で提案した行列の構成技法を用いることで，我々は以下の結果を得る．

定理 2 *$N = pq$ は RSA 法で, 素数 p と q は同じビット長である．暗号化指数 $e = N^\alpha$ と CRT 復号指数 $d_p, d_q < N^\delta$ は，それぞれ $ed_q = 1 \pmod{(q-1)}$ と $ed_p = 1 \pmod{(p-1)}$ を満たす．LLL アルゴリズムの出力するベクトルによって構成される多項式が代数的に独立であることを仮定し，条件 $\alpha \geq \frac{3}{8}$ と*

$$\delta < \frac{1}{2} - \sqrt{\frac{\alpha}{6}}$$

を満たすとき，公開要素 N と e のみから RSA 法 N を多項式時間で素因数分解することができる．

暗号化指数 e が RSA 法 N と同じビット長で $\alpha = 1$ となるとき，求めうる CRT 復号指数 $d_p, d_q < N^\delta$ の大きさは $\delta < \frac{1}{2} - \sqrt{\frac{1}{6}} = 0.091751\cdots$ となる．

5. 変形方式への攻撃

第 3 章の d_q が小さい攻撃を RSA の変形方式に適用した結果をこの章でまとめる．前述の通り，我々の攻撃は全てのパラメータにおいて Bleichenbacher-May の攻撃を改良している．本章では $N = p^r q$ の RSA 法に対する攻撃と，同じ $N = pq$ に対して複数の鍵ペア $(e_1, d_{q,1}), \ldots, (e_r, d_{q,r})$ が与えられたときの攻撃を扱う．そしてこれらの変形方式に対する既存攻撃である Shinohara らの攻撃 [24] と Peng らの攻撃 [22] はいずれも Bleichenbacher-May の攻撃の拡張であるため，全てのパラメータに対して本章で我々が提案する攻撃は既存の攻撃を改良している．ページ数の都合で証明は省略するが，これらの結果を以下にまとめる．

定理 3 *$N = p^r q$ は RSA 法，$r \geq 1$ で素数 p と q は同じビット長である．暗号化指数 $e = N^\alpha$ と CRT 復号指数 $d_p < N^{\delta_p}, d_q < N^{\delta_q}$ は，それぞれ $ed_p = 1 \pmod{(p-1)}$ と $ed_q = 1 \pmod{(q-1)}$ を満たす．LLL アルゴリズムの出力するベクトルによって構成される多項式が代数的に独立であることを仮定し，条件 $\frac{r}{(r+1)^2} \leq \alpha \leq \frac{1}{r}$ と*

$$\min\{\delta_p, \delta_q\} < \frac{1 - \sqrt{r\alpha}}{r+1}$$

を満たすとき，公開要素 N と e のみから RSA 法 N を多項式時間で素因数分解することができる．

定理 4 *$N = pq$ は RSA 法で, 素数 p と q は同じビット長である．$\ell = 1, \ldots, r$ に対して，暗号化指数 $e_\ell = N^\alpha$ と CRT 復号指数 $d_{q,\ell} < N^\delta$ は，それぞれ $e_\ell d_{q,\ell} = 1 \pmod{(q-1)}$ を満たす．LLL アルゴリズムの出力するベクトルによって構成される多項式が代数的に独立であることを仮定し，条件*

$$\delta < \frac{1}{2} - \sqrt{\frac{\alpha}{3r+1}},$$

を満たすとき，公開要素 N と $e_1, \ldots, e_r$ のみから RSA 法 N を多項式時間で素因数分解することができる．

謝辞 本研究は JSPS 科研費 14J08237 の助成を受けたものです．

参考文献

[1] Aono, Y., Agrawal, M., Satoh, T. and Watanabe, O.: On the Optimality of Lattices for the Coppersmith Technique, *ACISP 2012* (Susilo, W., Mu, Y. and Seberry, J., eds.), LNCS, Vol. 7372, Springer, pp. 376–389 (2012).

[2] Bauer, A., Vergnaud, D. and Zapalowicz, J.: Inferring Sequences Produced by Nonlinear Pseudorandom Number Generators Using Coppersmith's Methods, *PKC 2012* (Fischlin, M., Buchmann, J. A. and Manulis, M., eds.), LNCS, Vol. 7293, Springer, pp. 609–626 (2012).

[3] Bleichenbacher, D. and May, A.: New Attacks on RSA with Small Secret CRT-Exponents, *PKC 2006* (Yung, M., Dodis, Y., Kiayias, A. and Malkin, T., eds.), Lecture Notes in Computer Science, Vol. 3958, Springer, pp. 1–13 (2006).

[4] Boneh, D. and Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$, *IEEE Trans. Information*

Theory, Vol. 46, No. 4, pp. 1339–1349 (2000).

[5] Coppersmith, D.: Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known, *EUROCRYPT '96* (Maurer, U. M., ed.), LNCS, Vol. 1070, Springer, pp. 178–189 (1996).

[6] Coppersmith, D.: Finding a Small Root of a Univariate Modular Equation, *EUROCRYPT '96* (Maurer, U. M., ed.), LNCS, Vol. 1070, Springer, pp. 155–165 (1996).

[7] Durfee, G. and Nguyen, P. Q.: Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99, *ASIACRYPT 2000* (Okamoto, T., ed.), Lecture Notes in Computer Science, Vol. 1976, Springer, pp. 14–29 (2000).

[8] Galbraith, S. D., Heneghan, C. and McKee, J. F.: Tunable Balancing of RSA, *ACISP 2005* (Boyd, C. and Nieto, J. M. G., eds.), Lecture Notes in Computer Science, Vol. 3574, Springer, pp. 280–292 (2005).

[9] Herrmann, M. and May, A.: Attacking Power Generators Using Unravelled Linearization: When Do We Output Too Much?, *ASIACRYPT 2009* (Matsui, M., ed.), Lecture Notes in Computer Science, Vol. 5912, Springer, pp. 487–504 (2009).

[10] Herrmann, M. and May, A.: Maximizing Small Root Bounds by Linearization and Applications to Small Secret Exponent RSA, *PKC 2010* (Nguyen, P. Q. and Pointcheval, D., eds.), Lecture Notes in Computer Science, Vol. 6056, Springer, pp. 53–69 (2010).

[11] Howgrave-Graham, N.: Finding Small Roots of Univariate Modular Equations Revisited, *Cryptography and Coding, 6th IMA International Conference* (Darnell, M., ed.), LNCS, Vol. 1355, Springer, pp. 131–142 (1997).

[12] Jochemsz, E. and May, A.: A Strategy for Finding Roots of Multivariate Polynomials with New Applications in Attacking RSA Variants, *ASIACRYPT 2006* (Lai, X. and Chen, K., eds.), LNCS, Vol. 4284, Springer, pp. 267–282 (2006).

[13] Jochemsz, E. and May, A.: A Polynomial Time Attack on RSA with Private CRT-Exponents Smaller Than $N^{0.073}$, *CRYPTO 2007* (Menezes, A., ed.), LNCS, Vol. 4622, Springer, pp. 395–411 (2007).

[14] Kunihiro, N.: On Optimal Bounds of Small Inverse Problems and Approximate GCD Problems with Higher Degree, *ISC 2012* (Gollmann, D. and Freiling, F. C., eds.), Lecture Notes in Computer Science, Vol. 7483, Springer, pp. 55–69 (2012).

[15] Kunihiro, N., Shinohara, N. and Izu, T.: A Unified Framework for Small Secret Exponent Attack on RSA, *IEICE Transactions*, Vol. 97-A, No. 6, pp. 1285–1295 (2014).

[16] Lenstra, A., Lenstra, H. and Lovász, L.: Factoring polynomials with rational coefficients, *Math. Ann.*, Vol. 261, pp. 515–534 (1982).

[17] Lu, Y., Zhang, R. and Lin, D.: New Partial Key Exposure Attacks on CRT-RSA with Large Public Exponents, *ACNS 2014* (Boureanu, I., Owesarski, P. and Vaudenay, S., eds.), LNCS, Vol. 8479, Springer, pp. 151–162 (2014).

[18] Lu, Y., Zhang, R., Peng, L. and Lin, D.: Solving Linear Equations Modulo Unknown Divisors: Revisited, *ASIACRYPT 2015* (Iwata, T. and Cheon, J. H., eds.), Lecture Notes in Computer Science, Vol. 9452, Springer, pp. 189–213 (2015).

[19] May, A.: Cryptanalysis of Unbalanced RSA with Small CRT-Exponent, *CRYPTO 2002* (Yung, M., ed.), LNCS, Vol. 2442, Springer, pp. 242–256 (2002).

[20] May, A.: New RSA vulnerabilities using lattice reduction methods, PhD Thesis, University of Paderborn (2003).

[21] May, A.: Using LLL-Reduction for Solving RSA and Factorization Problems, *The LLL Algorithm - Survey and Applications* (Nguyen, P. Q. and Vallée, B., eds.), Information Security and Cryptography, Springer, pp. 315–348 (2010).

[22] Peng, L., Hu, L., Lu, Y., Sarkar, S., Xu, J. and Huang, Z.: Cryptanalysis of Variants of RSA with Multiple Small Secret Exponents, *INDOCRYPT 2015* (Biryukov, A. and Goyal, V., eds.), Lecture Notes in Computer Science, Vol. 9462, Springer, pp. 105–123 (2015).

[23] Sarkar, S. and Maitra, S.: Partial Key Exposure Attack on CRT-RSA, *ACNS 2009* (Abdalla, M., Pointcheval, D., Fouque, P. and Vergnaud, D., eds.), LNCS, Vol. 5536, pp. 473–484 (2009).

[24] Shinohara, N., Izu, T. and Kunihiro, N.: Small Secret CRT-Exponent Attacks on Takagi's RSA, *IEICE Transactions*, Vol. 94-A, No. 1, pp. 19–27 (2011).

[25] Sun, H. and Wu, M.: An Approach Towards Rebalanced RSA-CRT with Short Public Exponent, *IACR Cryptology ePrint Archive*, Vol. 2005, p. 53 (2005).

[26] Takayasu, A. and Kunihiro, N.: Cryptanalysis of RSA with Multiple Small Secret Exponents, *ACISP 2014* (Susilo, W. and Mu, Y., eds.), Lecture Notes in Computer Science, Vol. 8544, Springer, pp. 176–191 (2014).

[27] Takayasu, A. and Kunihiro, N.: Better Lattice Constructions for Solving Multivariate Linear Equations Modulo Unknown Divisors, *IEICE Transactions*, Vol. 97-A, No. 6, pp. 1259–1272 (2014).

[28] Takayasu, A. and Kunihiro, N.: General Bounds for Small Inverse Problems and Its Applications to Multi-Prime RSA, *ICISC 2014* (Lee, J. and Kim, J., eds.), LNCS, Vol. 8949, Springer, pp. 3–17 (2014).

[29] Takayasu, A. and Kunihiro, N.: Partial Key Exposure Attacks on RSA: Achieving the Boneh-Durfee Bound, *SAC 2014* (Joux, A. and Youssef, A. M., eds.), Lecture Notes in Computer Science, Vol. 8781, Springer, pp. 345–362 (2014).

[30] Takayasu, A. and Kunihiro, N.: Partial Key Exposure Attacks on CRT-RSA: Better Cryptanalysis to Full Size Encryption Exponents, *ACNS 2015* (Malkin, T., Kolesnikov, V., Lewko, A. B. and Polychronakis, M., eds.), LNCS, Vol. 9092, Springer, pp. 518–537 (2015).

[31] Takayasu, A. and Kunihiro, N.: How to Generalize RSA Cryptanalyses, *PKC 2016* (Cheng, C., Chung, K., Persiano, G. and Yang, B., eds.), LNCS, Vol. 9615, Springer, pp. 67–97 (2016).

[32] Takayasu, A. and Kunihiro, N.: Partial Key Exposure Attacks on CRT-RSA: General Improvement for the Exposed Least Significant Bits, *ISC 2016*, (Bishop, M. and Nascimento, A. C. A., eds.), LNCS, Springer, (2016).

[33] Takayasu, A. and Kunihiro, N.: Partial Key Exposure Attacks on RSA with Multiple Exponent Pairs, *ACISP 2016* (Liu, J. K. and Steinfeld, R., eds.), LNCS, Vol. 9723, Springer, pp. 243–257 (2016).

[34] Wiener, M. J.: Cryptanalysis of short RSA secret exponents, *IEEE Trans. Information Theory*, Vol. 36, No. 3, pp. 553–558 (1990).