2007－AL－110 (4)
2007／1／23

Shortest vector問題を用いたRSA暗号への攻撃における格子の構成方法

青野 良範†

Boneh 及び Durfee[1] らは格子に対する LLL アルゴリズム[4] を用いた小さな秘密鍵を持つ RSA 暗号に対する攻撃手法を提案した．彼らの攻撃は，パラメータ $d < N^{0.292}, e \approx N$ 及び $p \approx q$ を持つ RSA 暗号系に対して，公開鍵 (e, N) の組から $\log N$ の多項式時間で d 及び N の素因数分解を求める事が可能である．本研究においては，彼らが RSA 暗号を解くために導入した格子の生成方法ににについて考察を行った．結論として，彼らと同様の方法で生成した下三角行列で表される格子の中では彼らの構成方法が最適なもののうちの 1 つであることを示した．

Lattice construction method to attack RSA cryptosystem by shortest vector problem

YOSHINORI AONO†

Boneh and Durfee[1] proposed an efficient algorithm detecting the small secret key of the RSA cryprosystem based on LLL algorithm[4] for obtaining an approximate solution of the shortest vector problem. It is reported that the algorithm is successful when $d < N^{0.292}, e \approx N$ and $p \approx q$, where $N = pq$ is the base of the RSA system. In this paper, we discuss a way to construct a matrix representation of a lattice for the shortest vector problem used in the method of Boneh and Durfee. We showed the one used by them is the best for the case when a lattice is made from bivariate polynomial and it is represented by a triangle matrix.

1. RSA 暗号と Boneh 及び Durfee らの攻撃

1.1 RSA 暗号の概要

RSA 暗号とは，以下の系をもつ公開鍵暗号である．まず，受信者は大きな素数 p, q を生成し，$N = pq$ を計算．次に公開鍵として自然数 e を生成する．このとき，e は $\phi(N)$ と互いに素であるとする．☆次に，秘密鍵 d として $ed \equiv 1 \pmod{\phi(N)}$ を満たす自然数を計算する．このとき，e と d の生成の順番を入れ替える，つまり先に d を決定してから e を計算する事も可能である．その後，受信者は自らの公開鍵として (e, N) の組を送信者に送る．

情報の送信者は，メッセージを表現する自然数 m に対して，暗号文 $c = m^e \pmod{N}$ を計算し，受信者に送る．このとき，m は N と互いに素でかつ N より小さいとする．

受信者は，送られてきた暗号文 c に対して $c^d \pmod{N}$ を計算する．すると，公開鍵と秘密鍵の関係から次のようにして元のメッセージ m が復元できる．

$$c^d \equiv m^{ed} \equiv m^{ed \bmod \phi(N)} \equiv m \pmod{N}$$

1.2 剰余方程式への変換

以下では，RSA のパラメータ p, q, e, d をひとつ固定して議論をする．また，$p + q < 3N^{0.5}$ 及び $e > 0.5N \gg 2$ を仮定し，δ を $d = N^{\delta}$ を満たす実数，$A = N + 1$ とする．以降の節では，(e, N) の組が与えられたときに，秘密鍵 d を得ること，及び N の素因数分解を得る事を目標とする．

RSA 暗号の各パラメータには，以下の関係がある．

$$ed \equiv 1 \pmod{\phi(N)} \tag{1}$$

式 (1) より，ある $k \in \mathbb{Z}$ を用いて，

$$ed + k\phi(N) = 1$$

と書ける．e と N の関係に関する仮定から，$|k|$ の大きさは d と同じくらいになる．$\phi(N) = N + 1 - (p + q)$ であるので，全体を mod e で考え，未知数である $k, -(p + q)$ をそれぞれ x, y で置き換えると，次の剰余方程式が得られる．

$$x(A + y) - 1 \equiv 0 \pmod{e} \tag{2}$$

以降，この方程式の左辺を $f_{\mathrm{BD}}(x, y)$ または $g(x, y)$ と書き，この方程式を BD 方程式と呼ぶ．

† 東京工業大学 情報理工学研究科 数理・計算科学専攻
Tokyo Institute of Technology, Dept. Math. and Comput. Sci. (aono5@is.titech.ac.jp)

☆ $\phi(N)$ は N のオイラー関数

RSA 暗号の鍵は，BD 方程式の $|x| < N^{\delta}, |y| < 3N^{0.5}$ をみたすあるひとつの解に対応しているが，BD 方程式は他にも無関係な解をたくさん持っている．

いま，方程式 (2) の解 (x_0, y_0) をひとつ求めたときに，それが RSA 暗号の秘密鍵を求めるのに役立つかどうかを考える．e, d に関する仮定から，役に立つ x, y の大きさは大まかにそれぞれ $N^{\delta}, N^{0.5}$ 程度であるので $|x| < N^{\delta}, |y| < 3N^{0.5}$ の範囲で (2) の解を探索すれば良いことになる．しかし，$\delta < 0.5$ と適当な e, A を取ってきたときに，このような条件をみたす (x, y) が存在する確率がきわめて低いのは，次のことからわかる．

適当な整数 y_1 を選んだときに $A + y_1$ と e の最大公約数が 1 であれば，$x_1 = (A + y_1)^{-1} \pmod{e}$ を計算する事により方程式 (2) のひとつの解 (x_1, y_1) が得られる．このときの x_1 を各 y_1 に対して定まる $1 \leq x_1 < e$ の範囲の乱数であると仮定する．すると，y_1 を $|y_1| < 3N^{0.5}$ の範囲で動かしたときに，対応する x_1 が $|x_1| < N^{\delta}$ の範囲に入っている回数の期待値は大まかに $N^{\delta-0.5}$ である．$\delta < 0.5$ を仮定すると，この期待値は 1 よりも小さい．よって，適当に選んできた (RSA 暗号を基としていない)e 及び A に対しては $|x_0| < N^{\delta}, |y_0| < 3N^{0.5}$ をみたす解 (x_0, y_0) が存在しない可能性が高いことがわかる．

逆に，たとえ RSA 暗号を基にした e 及び A であっても，$\delta > 0.5$ であるような場合，つまり秘密鍵がある程度大きな場合には，方程式 (2) の解 (x_0, y_0) で，$|x_0| < N^{\delta}, |y_0| < 3N^{0.5}$ を満たすものが，大まかに $N^{\delta-0.5} \gg 1$ 個存在してしまう．つまり，方程式 (2) のそのような解を 1 つみつけたとしても，その解から RSA 暗号の秘密鍵を求められる可能性が極めて低くなる．

以上の議論により，e 及び A が RSA 暗号の系を基にしたものであり，なおかつ $\delta < 0.5$ であることを仮定すれば，方程式 (2) の解 (x_0, y_0) で，$|x_0| < N^{\delta}, |y_0| < 3N^{0.5}$ を満たすものを得たときに，次の式によって RSA 暗号の秘密鍵 d が得られる確率が高いと予想できる．☆

$$d = \frac{1 - x_0(A + y_0)}{e} \tag{3}$$

以上をまとめると，次の仮説が成り立つ．

仮説 $e \approx N, d < N^{0.5}$ 及び $p + q < 3N^{0.5}$ を満たす RSA 暗号の e と N から作られた BD 方程式には $|x_0| < N^{0.5}, |y_0| < N^{0.5}$ を満たす解がただ 1 組存在する．もし，その解を求める事ができれば，式 (3) を用いて秘密鍵 d を求める事ができる．

以降の節では，この仮説が成り立つものとして，議論を進める．

☆ 我々が計算機実験をした限りにおいては，後に示される δ の範囲内であれば 100% の確率で正しい

1.3 格子について

ここでは，格子の定義と簡単な性質を述べる．

定義 1.1. m 次元空間内の互いに独立な $n(\leq m)$ 本のベクトル $\mathbf{b}_1, \cdots, \mathbf{b}_n$ に対して，格子 $L = L(\mathbf{b}_1, \cdots, \mathbf{b}_n)$ を次のように定義する．

$$L = \left\{ \sum_{i=1}^{n} a_i \mathbf{b}_i \,\middle|\, a_1, \cdots, a_n \in \mathbb{Z} \right\}$$

格子を次のような行列で表現することができる．

$$\begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ b_{21} & b_{22} & \cdots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nm} \end{bmatrix}$$

この表現によって表される格子は，$1 \leq i \leq n$ に対する n 本のベクトル $\mathbf{b}_i = (b_{i1}, b_{i2}, \cdots, b_{im})$ の整数係数の一次結合によって生成される格子を意味している．

定義 1.2. 最短ベクトル問題 *(Shortest Vector Problem)*

ある格子 L が与えられたときに，$L \setminus \mathbf{0}$ の中で長さが最小のベクトルを求める問題を最短ベクトル問題という．

この問題は，一般には NP 困難であることが知られているが，Lenstra[4] らによって LLL アルゴリズムと呼ばれる次の補題のベクトルを発見するアルゴリズムが存在する．

補題 1.1. *(Lenstra-Lenstra-Lovasz)* L を次数 n の整数成分をもつ正方行列で表現される格子，$det(L)$ をその行列の行列式とすると，次の条件を満たすベクトル $\mathbf{b}$ が n の多項式時間☆☆で発見できる．

(i) $\mathbf{b}$ は $\mathbf{0}$ でない格子上の点

(ii) $|\mathbf{b}| \leq 2^{(n-1)/4} |det(L)|^{1/n}$

1.4 Howgrave-Graham の補題

この節では，剰余方程式の解と一般の整数方程式の解との間に成り立つ関係を調べるために，Howgrave-Graham の補題[3] を述べる．

最初に，XY-norm の定義をする．

定義 1.3. 2 変数多項式 $f(x, y) = \sum a_{ij} x^i y^j$ と自然数 X, Y に対して，f の XY-*norm* $||f(x, y)||_{XY}$ を次のように定める．

$$||f(x, y)||_{XY} = \sqrt{\sum a_{ij}^2 X^{2i} Y^{2j}}$$

補題 1.2. *(Howgrave-Graham)* $f(x, y)$ を項数 w の 2 変数多項式，X, Y, M を自然数とし，次が成り立っていると仮定する．

$$||f(x, y)||_{XY} \leq \frac{M}{\sqrt{w}}$$

☆☆ 正確には，n と $\log B$ の多項式となる．ここで，B は行列に現れる整数の絶対値の中で最大のもの

このとき $|x| < X, |y| < Y$ をみたす整数 x, y に対して，次の関係が成り立つ．

$$f(x,y) = 0 \Leftrightarrow f(x,y) \equiv 0 \pmod{M} \qquad (4)$$

1.5 BD 方程式の解の求め方

この節では，Boneh と Durfee の論文[1] に従って RSA 暗号の公開鍵 (e, N) から秘密鍵 d を $\log N$ の多項式時間で求める方法を述べる．

最初に，記号 $[\![\cdot]\!]$ の導入をする．

定義 1.4. 自然数 M に対して，$[\![M]\!]$ を $[\log_2 M]+1$ ビットの自然数全体の集合とする．また，$X \in_R [\![M]\!]$ としたときには，自然数 X を $[\![M]\!]$ の中からランダムにひとつ取ってくるものとする．

他の記号は前節までのものを使い，$\delta < 0.25$, $X \in_R [\![N^\delta]\!]$ 及び $Y \in_R [\![N^{0.5}]\!]$ は予め定められているものとする．まず，適当な自然数 m を決め，$0 \le j \le i \le m$ を満たす整数の組 (i,j) の全てに対して，次の多項式を定義する．

$$g_{i,j}(x,y) = e^{m-j} x^{i-j} g^j(x,y)$$

このとき，次の事実が成り立つ．

事実 1.1. 各 (i,j) に対して，$g(x,y) \equiv 0 \ (mod\ e) \Rightarrow g_{i,j}(x,y) \equiv 0 \ (mod\ e^m)$ が成り立つ．

また，この事実から $g_{i,j}$ の整数係数の一次結合に対しても同様の性質が成り立つ．次に，定義された全ての多項式 $g_{i,j}$ に対して次の対応関係からベクトル $\mathbf{b}_{i,j}$ を作る．

定義 1.5. 多項式 $g(x,y)$ とベクトル $\mathbf{b}$ の対応関係

$$\begin{aligned} g &= a_{0,0}x^0y^0 + a_{1,0}x^1y^0 + \cdots + a_{m,m}x^my^m \\ &\quad \updownarrow \\ \mathbf{b} &= (a_{0,0}X^0Y^0,\ a_{1,0}X^1Y^0, \cdots,\ a_{m,m}X^mY^m) \end{aligned}$$

このときの係数の並べ方を解説する．まず，$0 \le j \le i \le m$ を満たす整数の組 (i,j) の全てに対して，i の小さい順に並べ，同じ i に対しては j の小さい順に並べる．☆つまり，(i,j) は $(0,0),(1,0),(1,1),(2,0),(2,1),\cdots$ の順になる．この列 $\{(i,j)\}$ に対して，$g(x,y)$ の項 $a_{i,j}x^iy^j$ を $a_{i,j}X^iY^j$ に置き換えたものを左側から並べていく．

この対応により作られたベクトル $\mathbf{b}_{i,j}$ は $(m+1)(m+2)/2$ 次元ベクトルとなる．また各 (i,j) に対して，$g_{i,j}$ の $a_{i,j}x^iy^j$ の項に対応する $\mathbf{b}_{i,j}$ 中の成分は $e^{m-j}X^iY^j$ となり，それよりも右側の成分は全て 0 となる．

さらに，作り方から次の事実がわかる．

事実 1.2. $||g_{i,j}(x,y)||_{XY} = |\mathbf{b}_{i,j}|$

以上の規則によって生成されたベクトル $\mathbf{b}_{i,j}$ を上の対応と同様に (i,j) の辞書順に並べて，次の行列を作る．

$$L_2 = \begin{bmatrix} \mathbf{b}_{0,0} \\ \mathbf{b}_{1,0} \\ \mathbf{b}_{1,1} \\ \vdots \\ \mathbf{b}_{m,m} \end{bmatrix} \qquad (5)$$

事実 1.3. L_2 は $(m+1)(m+2)/2$ 次の下三角行列で，$\det(L_2) = e^A X^B Y^C$ となる．但し，$A = B = m(m+1)(m+2)/3, C = A/2$.

これと補題 1.1 により，次の条件をみたすベクトル $\mathbf{b_0}$ が発見できることがわかる．

(i) $\mathbf{b_0}$ は各 $\mathbf{b}_{i,j}$ の整数係数の一次結合

(ii) $|\mathbf{b_0}| \le 2^{m(m+3)/8} |det(L)|^{2/(m+1)(m+2)}$

このベクトル $\mathbf{b_0}$ から，定義 1.5 の対応によって多項式 g_0 を作る．この多項式は各 $g_{i,j}(x,y)$ の整数係数の一次結合になっているので，事実 1.1 と同様の性質 $g(x,y) \equiv 0 \pmod{e} \Rightarrow g_0(x,y) \equiv 0 \pmod{e^m}$ が満たされる．さらに，$\delta < 0.25$ と仮定したので

$$\begin{aligned} ||g_0(x,y)||_{XY} &= |\mathbf{b_0}| \\ &\le 2^{m(m+3)/8} |det(L)|^{2/(m+1)(m+2)} \\ &= 2^{m(m+3)/8} e^{2m/3} X^{2m/3} Y^{m/3} \\ &\approx e^{(\frac{5}{6}+\frac{2}{3}\delta)m} < e^m \end{aligned}$$

が成り立つため，補題 1.2 の仮定が満たされる．(補題における $\sqrt{w}$ の部分は，小さいため無視される．) このときの，$g(x,y), g_{i,j}(x,y), g_0(x,y)$ の関係をまとめると次のようになる．

事実 1.4. $|x| < X, |y| < Y$ をみたす x, y に対して，

(a) $g(x,y) \equiv 0 \pmod{e}$

(b) $g_{i,j}(x,y) \equiv 0 \pmod{e^m}$
for $^\forall i,j$ s.t. $0 \le j \le i \le m$

(c) $g_0(x,y) \equiv 0 \pmod{e^m}$

(d) $g_0(x,y) = 0$

とすれば (a)⇒(b)⇒(c)⇔(d) となる．

この事実により，$g_0(x,y) = 0$ の整数解を $|x| < N^\delta, |y| < N^{0.5}$ の範囲で全て求めれば，その中に少なくとも 1 つは BD 方程式の解が存在する事がわかる．しかし，2 変数多項式の整数根を 1 つの方程式から求めることは難しいので，最初に選んだ X, Y とは別の $X \in_R [\![N^\delta]\!], Y \in_R [\![N^{0.5}]\!]$ をもう 1 組選び (これを X_1, Y_1 とする)，最終的に得られる多項式 (X,Y から得た g_0 に対応する) を $g_1(x,y)$ とする．すると，$g_1(x,y)$ も事実 1.4 で述べたような $g_0(x,y)$ と同様の性質を持っているので，その整数解の中に BD 方程式の解を含んでいる．ここで，g_0 と g_1 は共通因数を持たないと仮定する．☆☆

以上により，連立方程式 $g_0(x,y) = g_1(x,y) = 0$ の整数解は BD 方程式の $|x_0| < X, |y_0 < Y|$ を満たす整数解 (x_0, y_0) を含んでいるので，これを解いて解の候補を全て出力した後実際に BD 方程式に代入する事に

☆ 簡単に言うと，(i,j) の辞書順である．

☆☆ この仮定は，計算機実験では常に正しい

より，BD 方程式の解が求まる．最後に，その BD 方程式の解を用いて式 (3) から RSA の秘密鍵が求まる．

連立方程式を解くためには，まず g_0, g_1 の終結式 $h(x)$ を計算[2] し，$h(x)=0$ を Newton 法等の方法で解くことによって可能であり，計算時間は g_0, g_1 の次数及び係数の大きさの対数の多項式で抑えられる．

2. 下三角行列の構成

この節では，RSA 暗号を解くための格子の中で，下三角行列で表現されるものの一般的な構成方法を示す．また，Boneh と Durfee らの構成方法がある条件の下で最良であることを示す．以下，ある RSA 暗号の系及びそこから導かれる BD 方程式 $f_{\mathrm{BD}}(x,y) \equiv 0 \pmod e$ を固定する．以下の議論では，$d < N^{\delta}$ であると仮定し，$X \in_{\mathrm{R}} [\![N^{\delta}]\!]$ 及び $Y \in_{\mathrm{R}} [\![N^{\delta}]\!]$ は固定されているものとする．また，XY-norm はこの X, Y に対して定義するものとする．

2.1 多項式図形

定義 2.1. $C(f), C(f_1, f_2, \cdots, f_i)$
整数係数の 2 変数の多項式 $f(x,y)$ に対して，f の多項式図形を $C(f) = \{(i,j) | f(x,y)$ の $x^i y^j$ の係数が 0 でない $\} \subset \mathbb{Z}^2$ と定義する．また，複数の整数係数 2 変数多項式 $f_1, f_2, \cdots, f_i$ に対して $C(f_1, f_2, \cdots, f_i) = C(f_1) \cup C(f_2) \cup \cdots \cup C(f_i)$ とする．

例 2.1. $C(g(x,y)) = \{(0,0),(1,0),(1,1)\}, C(g^2(x,y)) = \{(0,0),(1,0),(1,1),(2,0),(2,1),(2,2)\}$ であり，それらを視覚的に表すと，以下のようになる．

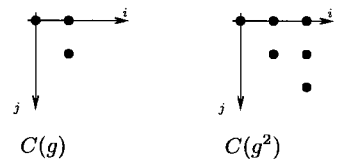

図 1　多項式図形の例

一般に，自然数 n に対して $C(g^n)$ は $(0,0),(n,0),(n,n)$ を頂点とした三角形の内部及び境界上の整数点の全てとなる．

2.2 下三角行列の構成方法

この節では，上で定義した多項式図形を用いて，RSA 暗号を解くための格子の中で，下三角行列で表現されるものを多項式の列から構成する方法を述べ，(i)Boneh と Durfee による構成を視覚的に表す．(ii) 彼らの構成方法がある条件の下で最良である事を示す．以上の目的を達成するために，次の条件をみたす 2 変数多項式の列 $h_1, h_2, \cdots, h_u$ を考える．

条件 2.1. 整数係数 2 変数多項式の列 $h_1, h_2, \cdots, h_u$ に対する条件

(i) $\phi \subsetneq C(h_1) \subsetneq C(h_1, h_2) \subsetneq \cdots \subsetneq C(h_1, h_2, \cdots, h_u)$

(ii) $|C(h_1)| = 1$ かつ，$\forall l \geq 2$ に対して，$|C(h_1, h_2, \cdots, h_l) \backslash C(h_1, h_2, \cdots, h_{l-1})| = 1$

(iii) $\forall l \geq 1$ に対して，$d_l = C(h_1, h_2, \cdots, h_l) \backslash C(h_1, h_2, \cdots, h_{l-1}) = (i_l, j_l)$ とおいたときに $h_l(x,y)$ の $x^{i_l} y^{i_l}$ の係数と e との最大公約数は 1

条件 (ii) より，$\forall l \geq 1$ に対して，$|C(h_1, h_2, \cdots, h_l)| = l$ となる．

以上の条件 (i) から (iii) を満たす多項式列 $h_1, \cdots, h_u$ に対して，以下のものを定義する．

定義 2.2. $r(f), \pi(h_l, d_l), P(\{h_l\})$
2 変数多項式 f に対して，$r(f) = \max\{i | f = g^i k, k \in \mathbb{Z}[x,y]\}$ とする．これは，f を整数の範囲で因数分解したときにその因数に含まれている $g(x,y)$ の次数である．d_l と $r(\cdot)$ を使って，多項式 h_l のスコア $\pi(h_l, d_l)$ を $\delta i_l + 0.5 j_l - r(h_l)$，多項式列 $h_1, \cdots, h_u$ に対するスコアを $P(\{h_l\}) = \sum_{l=1}^{u} \pi(h_l, d_l)$ と定義する．

定義 2.3. $m, \hat{h}_l$
$m = max_i r(h_i)$ とする．さらに，$c_l = (h_l(x,y)$ の $x^{i_l} y^{i_l}$ の係数$)$ として，$\hat{h}_l(x,y)$ を $(c_l^{-1} \bmod e^{r(h_l)}) \cdot e^{m-r(h_l)} \cdot h_l(x,y)$ の係数を mod e^m したものとする．

事実 1.1 のときと同様に，$\hat{h}_l$ に対して次の補題が成り立つ．

補題 2.1. $g(x,y) \equiv 0 \ (mod\ e) \Rightarrow \hat{h}_l(x,y) \equiv 0 \ (mod\ e^m)$

(証明) 定義より，$g(x,y) \equiv 0 \pmod e \Rightarrow e^{r(h_l)} | h_l(x,y)$ が成り立つので，両辺に $e^{m-r(h_l)}$ をかければ $e^m | h_l(x,y) \cdot e^{m-r(h_l)}$．これに自然数をかけて mod e^m したものが $\hat{h}_l$ であるので，$e^m | \hat{h}_l$ □

以上の準備の下に，多項式列 $\hat{h}_1, \hat{h}_2, \cdots, \hat{h}_u$ から下三角行列で表現される格子を構成する．

定義 2.4. 多項式 $\hat{h}_l$ とベクトル $\mathbf{b}_l$ の対応
多項式 $\hat{h}_l$ と u 次のベクトル $\mathbf{b}_l$ の間に以下の対応をつける．

$$\begin{array}{rcl} h_l & = & a_{i_1 j_1} x^{i_1} y^{j_1} + a_{i_2 j_2} x^{i_2} y^{j_2} + \cdots + a_{i_u j_u} x^{i_u} y^{j_u} \\ & & \updownarrow \\ \mathbf{b}_l & = & (a_{i_1 j_1} X^{i_1} Y^{j_1},\ a_{i_2 j_2} X^{i_2} Y^{j_2}, \cdots,\ a_{i_u j_u} X^{i_u} Y^{j_u}) \end{array}$$

事実 2.1. 上の対応において，$|\mathbf{b}_l| = ||\hat{h}_l(x,y)||_{XY}$

定義 2.5. 行列 L
多項式 $\hat{h}_1, \cdots, \hat{h}_u$ からそれぞれ定義 2.4 の対応によってベクトル $\mathbf{b}_1, \cdots, \mathbf{b}_u$ を作り，以下のように並べる．

$$L = \begin{bmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_u \end{bmatrix}$$

補題 2.2. L は下三角行列かつ $det(L) = X^A Y^B e^C$. 但し, $A = \sum_{l=1}^{u} i_l$, $B = \sum_{l=1}^{u} j_l$, $C = um - \sum_{l=1}^{u} r(h_l)$.
(証明) 定義から $C(h_l) \subset \{(i_1, j_1), (i_2, j_2), \cdots, (i_l, j_l)\}$ となるので, 定義 2.4 によって作られるベクトル $\mathbf{b}_l$ の $l+1$ 項以降は全て 0 になる. また, 条件 (iii) より, $\mathbf{b}_l$ の第 l 項は 0 でないので, L は下三角行列となる. 次に, 作り方から L の (l,l)-成分は $X^{i_l} Y^{j_l} e^{m-r(h_l)}$ となるので,

$$\begin{aligned} det(L) &= \prod_{l=1}^{u} X^{i_l} Y^{j_l} e^{m-r(h_l)} \\ &= X^{\sum_{l=1}^{u} i_l} Y^{\sum_{l=1}^{u} j_l} e^{um - \sum_{l=1}^{u} r(h_l)} \end{aligned}$$

となる. □

ここで議論を簡単にするために, $X = N^{\delta}$, $Y = N^{0.5}$,$e = N$ と近似すると, $\det(L) = X^A Y^B e^C = N^{um+P(\{h_l\})}$ となる. いま, 全体のスコア $P(\{h_l\})$ が 0 よりも小さいと仮定すると, LLL アルゴリズムにより、その大きさが $2^{(u-1)/4} N^m$ よりも小さいベクトル $\mathbf{b}_0$ が見つかる. このベクトルから定義 2.4 の対応により, $|\mathbf{b}_0| = ||g_0(x,y)||_{XY}$ となるような多項式 $g_0(x,y)$ が作れる. $2^{(u-1)/4}$ の部分を無視すると, この多項式 g_0 は Howgrave-Graham の補題を満たす. まとめると, 次の定理が得られる.
定理 2.1. *RSA* 暗号の系が与えられ, $f_{\mathrm{BD}}(x,y) = x(y+A) - 1$ としたときに, ある $\delta < 0.5$ に対して, $P(\{h_l\}) < -\epsilon$ となるような多項式の列 $h_1, \cdots, h_u$ が存在するならば, $f_{\mathrm{BD}}(x,y) \equiv 0 \ (mod\ e)$ の解 (x_0, y_0) で, $|x_0| < N^{\delta}, |y_0| < N^{0.5}$ となるものを得るための格子を構成することができる.
ここで, ϵ は小さいため 0 だと思う事ができる. ☆

2.3 多項式列の最良な取り方

秘密鍵 $d < N^{\delta}$ を持つような RSA 暗号を $\log N$ の多項式時間で解くためには, 多項式列 $h_1, h_2, \cdots, h_u$ を作ったときに列のスコア $P(\{h_l\})$ が 0 より小さくなる必要があることを述べた. この節では, ある条件の下に Boneh と Durfee らの構成が最も大きな δ に対して $P(\{h_l\}) < 0$ を満たすものであることを示す.
定義 2.6. $S_{\{h_l\}}$
2 変数多項式の列 $h_1, h_2, \cdots, h_u$ に対して, $S_{\{h_l\}} = C(h_1, \cdots, h_u)$ とおく.

☆ 正確には, $\epsilon = -0.5 \log u - \frac{u-1}{4} \log 2 + (1 - logN)(\delta A + 0.5B)$ となる. ここで, log の底は e である (自然底数ではなく, 秘密鍵の e)

ここでは, ある $S \subset \mathbb{Z}^2$ をひとつ固定して, $S_{\{h_l\}} = S$ となるような多項式列 $h_1, \cdots, h_u (u = |S|)$ の中で最も良いもの, つまり最も大きい δ に対して $P(\{h_l\}) < 0$ を満たすものを構成する問題を考える. Boneh と Durfee らの論文では, S が $\Delta_n = \{(i,j) | 0 \le j \le i \le n\}$ 及び $S_{n,k} = \{0 \le i \le n, 0 \le j \le i + k\}$ の場合を考えて格子を構成しているが, この節ではその構成方法がそれぞれ $\Delta_n, S_{n,k}$ に対する最良な $\{h_l\}$ の 1 つであることを示す.
まず, 定義より $P(\{h_l\}) = \sum_{l=1}^{u} \pi(h_l, d_l) = \sum_{l=1}^{u} \delta i_l + 0.5 j_l - r(h_l)$ である. S を固定したときに, $\sum_{l=1}^{u} \delta i_l + 0.5 j_l$ は $\{h_l\}$ の取り方によらず一定であるので, 列のスコアの優劣を決めるのは $\sum -r(h_l)$ の部分のみであることを注意しておく. つまり, 列のスコア $P(\{h_l\})$ は S, δ 及び各 $r(h_l)$ によって決まる. S を固定しているという仮定であったので, このスコアを小さくする問題は, なるべく $\sum r(h_l)$ が大きくなるような順序で S 内の点を 1 つずつ取っていくという問題に変換することができる.
以上の仮定の下に, 本研究においては次の結果が得られた.
定理 2.2. 任意の $n \ge 2$ に対して, $S_{\{h_l\}} = \Delta_n = \{(i,j) | 0 \le j \le i \le n\}$ となるような $h_1, \cdots, h_u$ で条件 *2.1* を満たすどのような列に対しても, $\delta > 0.25$ に対して $P(\{h_l\}) < 0$ となることはできない.

この定理の証明をするために, 条件 2.1 を満たす列 $h_1, \cdots, h_u$ で, $S_{\{h_l\}} = \Delta_n$ となるものにに対して, いくつかの補題を証明する.
補題 2.3. 任意の整数 $k \ge 0$ に対して, 多項式列 $h_1, \cdots, h_l$ の中で $r(h_l) \ge n - k$ となるものは高々 $(k+1)(k+2)/2$ 個しかない.
この補題を証明するために, 多項式列 $h_1, \cdots, h_u$ の中で $r(h_l) \ge n - k$ となるものを取り出して新たな列 $h'_1, h'_2, \cdots, h'_{u'}$ を作る. この列に対して多項式図形を考えると, 当然次の性質が成り立つ.

$$\begin{aligned} &\phi \subsetneq C(h'_1) \subsetneq C(h'_1, h'_2) \subsetneq \cdots \\ &\subsetneq C(h'_1, h'_2, \cdots, h'_{u'}) \subset \Delta_n \end{aligned} \tag{6}$$

また, 各 h'_i の選び方から, $t_i(x,y) = h'_i(x,y)/g^{n-k}(x,y)$ を作ったときに必ず整数係数の多項式になる. この $t_i(x,y)$ に対して, 多項式図形の列を考えると, 次のようになる.

$$\begin{aligned} &\phi \subsetneq C(t_1) \subset C(t_1, t_2) \subset \cdots \\ &\subset C(t_1, t_2, \cdots, t_{u'}) \subset \Delta_k \end{aligned} \tag{7}$$

この多項式図系列 (7) に対して, 次の性質が成り立つ.
補題 2.4. 任意の $s \ge 1$ に対して, 列 *(7)* の中で $|C(t_1, t_2, \cdots, t_l)| \le s$ となる $l \ge 1$ は s 個以下しか無い.
(証明) 背理法で行う. もし, ある s に対して, $|C(t_1, t_2, \cdots, t_l)| \le s$ となる l が $s+1$ 個存在したと

すると，多項式図形の定義より，t_{s+1} は $t_1, t_2, \cdots, t_s$ の線形結合として次のように書ける．

$$t_{s+1} = \beta_1 t_1 + \beta_2 t_2 + \cdots + \beta_s t_s$$

ここで，両辺に $g^{n-k}(x,y)$ をかけると，

$$h'_{s+1} = \beta_1 h'_1 + \beta_2 h'_2 + \cdots + \beta_s h'_s$$

となるので，$C(h'_{s+1}) \subset C(h'_1, \cdots, h'_s)$ となり，多項式図形の列 (6) に矛盾する．□

この補題を用いて，補題 2.3 の証明を行う．

(補題 2.3 の証明) 補題 2.4 より，任意の整数 $k \geq 0$ に対して式 (7) の長さは $|\Delta_k| = (k+1)(k+2)/2$ 以下となるので，$r(h_l) \geq n-k$ となる h_l はそれ以上多く取れない．□

以上の補題を用いて，任意の n に対して $S_{\{h_l\}} = \Delta_n$ のときの $\sum_{l=1}^{u} r(h_l)$ の上限を示す．

補題 2.5. 任意の n に対して $S_{\{h_l\}} = \Delta_n$ のとき，どのような $h_1, \cdots, h_u$ を取ったとしても $\sum_{i=1}^{u} r(h_l) \leq n(n+1)(n+2)/6$

(証明) 各 k に対して，補題 2.3 を満たすぎりぎりの取り方ができたと仮定して，そのような $h_1, \cdots, h_u$ に対して $r(h_l)$ の大きい順に並べると，

l	l_1	l_2	l_3	l_4	$\cdots$	l_u
$r(h_l)$	n	$n-1$	$n-1$	$n-2$	$\cdots$	0

(8)

$r(h_l) = n$ となる l が 1 個，$r(h_l) = n-1$ となる l が 2 個，$\cdots$，$r(h_l) = n-k$ となる l が $k+1$ 個，$\cdots$，$r(h_l) = 0$ となる l が $n+1$ 個現れる．いま，$\sum_{i=1}^{u} r(h_l) < \sum_{i=1}^{u} r(h'_l)$ となるような別の多項式列 $h'_1, \cdots h'_u$ が取れたと仮定して，同様に $r(h'_l)$ の大きい順に並べると，

l	l'_1	l'_2	l'_3	l'_4	$\cdots$	l'_u
$r(h'_l)$	n	$*$	$*$	$*$	$\cdots$	0

となるが，$\sum_{i=1}^{u} r(h_l) < \sum_{i=1}^{u} r(h'_l)$ より，どこかで $r(h_{l_i}) < r(h'_{l_i})$ となる部分ができてしまう．これは補題 2.3 に矛盾する．つまり，最適な $h_1, \cdots, h_u$ を取れたとしてもそのときの各 $r(h_l)$ は (8) のようなものであり，そのときの $\sum_{i=1}^{u} r(h_l) = 1 \cdot n + 2 \cdot (n-1) + 3 \cdot (n-2) + \cdots + (n+1) \cdot 0 = n(n+1)(n+2)/6$ で，これより大きな値は取れない．□

補題 2.6. 任意の n に対して $S = \Delta_n$ のときに $\sum_{i=1}^{u} r(h_l) = n(n+1)(n+2)/6$ となるような $h_1, \cdots, h_u$ が具体的に構成できる．

(証明) Boneh と Durfee らによる構成がその一例となっている．ある $t \geq 2$ をひとつ固定し，(i_l, j_l) を次の図で示される順序で取る．つまり，$(0,0), (1,0), (1,1), \cdots, (t,t)$ の順でそれぞれ $(i_1, j_1), \cdots, (i_u, j_u)$ に割り当てる．このとき，$h_l(x,y) = x^{i_l - j_l} \cdot g^{j_l}(x,y)$ と取れて $r(h_l) = j_l$ となる．この $\{h_l\}$ は条件 (i)-(iii) を満たしていて，なおかつ $r(h_l)$ は補題 2.5 に挙げたぎりぎりの取り方となる．□

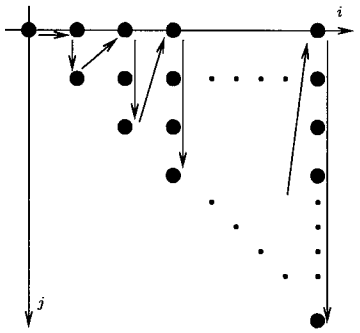

図 2 Boneh と Durfee らによる格子の構成を視覚的に表現した図

以上の補題を使って，定理 2.2 の証明を行う．

(定理 2.2 の証明)

任意の $n \geq 2$ と $S = \Delta_n$ 及び補題 2.6 の構成方法から具体的にスコア $P(\{h_l\})$ を計算すると，

$$P(\{h_l\}) = \frac{n(n+1)(n+2)}{3}\delta - \frac{n(n+1)(n+2)}{12}$$

となるので，$\delta < 0.25$ ならば定理 2.1 により構成される格子が RSA 暗号の秘密鍵を求めるためのものとなるが，逆に補題 2.5 により，$P(\{h_l\})$ はこれ以上小さくできないので，$\delta > 0.25$ に対して $P(\{h_l\}) < 0$ となるのは不可能である．□

また，これと同様にして，以下の定理が示される．

定理 2.3. 任意の $n \geq 2, k \geq 2$ に対して，$S = S_{n,k} = \{(i,j) | 0 \leq i \leq n, 0 \leq j \leq i+k\}$ と取ったときに，どのような $h_1, \cdots, h_u$ の選び方をしても，$\delta > \frac{7}{6} - \frac{\sqrt{7}}{3} \approx 0.2847$ に対して $P(\{h_l\}) < 0$ となることはできない．

3. 結論と今後の展開

本研究においては Boneh と Durfee の構成，つまり S が Δ_n の場合と $S_{n,k}$ において最適な多項式列の取り方の一例が彼らの構成方法であることを示した．

今後は任意の S と多項式列 $h_1, \cdots, h_u$ に対して彼らの構成方法が最適な δ の上界を与えることをいいたい．また，BD 方程式の代わりに 3 変数の方程式 $ez + x(A+y) - 1 = 0$ を用いても同様の結果が得られると予想される．

謝辞 本研究を進めるにあたり，重要な助言を頂いた渡辺治教授に感謝いたします．

参 考 文 献

1) D. Boneh and G. Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. *IEEE Transactions on Information Theory* vol.46 No.4 pp.1339-1349, 2001.

2) Alexander D. Healy Resultants, Resolvents and the Computation of Galois Groups available online at `http://www.alexhealy.net/papers/math250a.pdf`
3) N. Howgrave-Graham. Finding small roots of univariate modular equations revisited. in *proceedings Cryptography and Coding*, Lecture Notes in Computer Science, vol.1355, Springer-Verlag,pp.131-142,1997.
4) A.K.Lenstra, H.W.Lenstra, Jr.and L.Lovasz Factoring Polynomials with Rational Coefficients *Mathematische Annalen* 261 pp.515-534,1982.