arXiv:2304.03957v2 [cs.CR] 9 May 2023

一种基于连分数与双曲线的 RSA 密码系统攻击

GILDA RECH BANSIMBA、REGIS F. BABINDAMANA 和 BASILE GUY R. BOSSOTO

摘要。
本文在 Babindamana 等人关于双曲线的研究基础上，给出了新的算术和代数结果，并在这些新结果中描述了一种利用连分数攻击 RSA 型模数的方法。与 Wiener攻击相比，该方法独立于私钥大小 d 和公钥指数 e，且不受其限制。攻击成功时，其复杂度受限于 $\mathcal{O}(b\log\alpha_{j4}\log(\alpha_{i3}+\alpha_{j3}))$，其中 $b=10^y$、$\alpha_{i3}+\alpha_{j3}$ 是 n 的一个非平凡因子，且 α_{j4} 满足 $(n+1)/(n-1)=\alpha_{i4}/\alpha_{j4}$。该攻击的主要目标是利用 $\frac{\alpha_{i4}}{\alpha_{j4}}+\delta$的一个渐近分数，找到满足$\langle X_{\alpha_3}, P_3\rangle=0$ 的点 $X_\alpha=(-\alpha_3, \alpha_3+1)\in\mathbb{Z}_\star^2$，其中 $P_3\in\mathcal{B}_n(x, y)|_{x\geq 4^n}$。最后，我们给出了一些实验示例。我们认为，这些结果为利用连分数进行 RSA 密码分析开辟了一个新方向，且独立于参数 e 和 d。

引言

在 [1], Babindamana 等人给出了关于双曲线的算术结果，并将其应用于使用费马因式分解法求格点。具体而言，他们利用双曲线参数化的结果 $\mathcal{B}_n(x, y)|_{\mathbb{Z}}$ 证明，对于费马因数分解方程，若 $(N-6)\equiv 0 \mod 4$，则费马方法失效。否则，按格点数量计算，当 N 为奇素数、$N=N_a\times N_b$ 满足 N_a 且 N_b 为奇素数、$N=N_a^\alpha$ 满足 N_a 为素数、$N=\prod_{i=1}^n p_i$ 满足 p_i 为互异素数，以及 $N=\prod_{i=1}^n N_i^{\alpha_i}$ 满足 N_i 为奇素数时，格点数分别为 4、8、$2(\alpha+1)$、$(1-\delta_{2p_i})2^{n+1}$ 和 $2\prod_{i=1}^n(\alpha_i+1)$。

本文针对 [1], 中考虑的双曲线参数化给出新的算术结果。特别地，我们证明：给定 $p, a, \alpha_i, \alpha_j\in\mathbb{Z}_{>0}$，且 $\gcd(p+1,\ p-1)\neq 1$，若 $\gcd(\alpha_i,\ \alpha_j)=1$ 且 $\frac{p+1}{p-1}=\frac{\alpha_i}{\alpha_j}$，则 $\alpha_i+\alpha_j=p$ 并且

$$\alpha_i^a-\alpha_j^a=\begin{cases}1 & if\ a=1\\ p & if\ a=2\\ p\delta & if\ 2\mid a\end{cases}$$

此外，在其他结果中，我们证明：给定 RSA 模数 n，对于所有$P_i\in\mathcal{B}_n(x,\ y)|_{x\geq 4^n}$，都存在 $\alpha_i\in\mathbb{Z}_{\geq 0}$，使得

$P_i=\left(4n\frac{(\alpha_i+1)^2}{2\alpha_i+1},\ 4n(\alpha_i+1)\cdot\frac{\alpha_i}{2\alpha_i+1}\right)$，其中 $\alpha_0=0$、$\alpha_4=n-1$、α_i是整数序列，且 $\{P_2,\ P_3,\ P_4\}$ 是 $\mathcal{B}_n(x,y)|_{x\geq 4^n}$的代数子集。最后，我们提出一种利用连分数攻击这些结果的方法，其目标是找到 X_α 使得

2020年 数学主题分类。主要分类号：11Y05、11Y40、11T71。关键词和短语。双曲线、RSA 攻击、连分数、密码分析。

满足 $\langle X_{\alpha_3},\ P_3\rangle = 0$。攻击成功时，其复杂度为$\mathcal{O}\left(b\log\ \alpha_{j4}\log\left(\alpha_{i3}+\alpha_{j3}\right)\right)$，其中 $b = 10^y$ 是 n 的一个非平凡因子，且 α_{j4} 满足 $(n+1)/(n-1)\ = \alpha_{i4}/\alpha_{j4}$。

1. New algebraic results on $\mathcal{B}_N(x,y)_{|_{x\geq 4N}}$

在 [2], 作者 [2], 中给出了关于双曲线的一些算术结果，而在[1], Babindamana 等人给出了关于双曲线 $\mathcal{B}_n(x,\ y)_{|\mathbb{Z}}$ 的其他算术和代数结果，以及它们在费马因式分解法格点中的应用。

回顾一下，$\mathcal{B}_n(x,\ y)_{|_{\mathbb{Z}}} = \{(x,\ y)\ \in \mathbb{Z}\times\mathbb{Z}\ /\ y^2 = x^2-4nx\}$ 和 $\mathcal{B}_n(x,\ y)_{|_{x\geq 4n}} = \{(x,\ y)\ \in \mathbb{Z}_{\geq 4n}\times\mathbb{Z}_{\geq 0}\ /\ y^2 = x^2-4nx\}$。
在本节中，我们给出关于 $\mathcal{B}_N(x,\ y)_{|_{x\geq 4N}}$的新代数结果。

定理 1.1。
设 $p, a, \alpha_i, \alpha_j \in \mathbb{Z}_{>0}$，且 $\gcd(p+1, p-1)\ \neq 1$。若 $\gcd(\alpha_i, \alpha_j)\ = 1$且 $\dfrac{p+1}{p-1} = \dfrac{\alpha_i}{\alpha_j}$，则 $\alpha_i+\alpha_j = p$ 且

$$\alpha_i^a - \alpha_j^a = \begin{cases} 1 & if\ a = 1 \\ p & if\ a = 2 \\ p\delta & if\ 2\mid a \end{cases}$$

证明 1.2。

- 考虑 $p\in\mathbb{Z}\setminus\{0,\ 1\}$，其中 $\gcd(p+1,p-1)\ \neq 1$，则有理分数$\dfrac{p+1}{p-1}$是可约的。现在假设 $\dfrac{p+1}{p-1} = \dfrac{\alpha_i}{\alpha_j}$是其既约表达式，其中 $\gcd(\alpha_i,\alpha_j)\ = 1$。重新整理该表达式中的各项，得到$p\alpha_j+\alpha_j = p\alpha_i-\alpha_i$，于是 $-p(\alpha_i-\alpha_j)\ = -(\alpha_i+\alpha_j)$，从而 $p = \dfrac{\alpha_i+\alpha_j}{\alpha_i-\alpha_j}$。现在，由假设可知，$p$ 是整数，因此 $(\alpha_i-\alpha_j)\mid(\alpha_i+\alpha_j)$，这只有在 $\alpha_i-\alpha_j$=1 时才成立，因为 $\gcd(p+1,p-1)\ \neq 1$。假设 $\alpha_i-\alpha_j\neq 1$, $p+1 = \dfrac{2\alpha_i}{\alpha_i-\alpha_j}$且 $p-1 = \dfrac{2\alpha_j}{\alpha_i-\alpha_j}$。在这种情况下，$\gcd(p+1,\ p-1)\ = \gcd(\dfrac{2\alpha_i}{\alpha_i-\alpha_j},\ \dfrac{2\alpha_j}{\alpha_i-\alpha_j})$。由于最大公约数仅在欧几里得整环中定义，因此这意味着 $(\alpha_i-\alpha_j)\ \mid 2\alpha_i$ 且 $(\alpha_i-\alpha_j)\ \mid 2\alpha_j$，这与假设矛盾，因为按假设，$\gcd(\alpha_i,\alpha_j)\ = 1$；由高斯引理可知，若 $(\alpha_i-\alpha_j)\ \mid 2\alpha_i$，则 $(\alpha_i-\alpha_j)\nmid 2\alpha_j$ ；反之，若 $(\alpha_i-\alpha_j)\ \mid 2\alpha_j$，则 $(\alpha_i-\alpha_j)\nmid 2\alpha_i$。因此，在这种情况下，$gcd$ 没有定义。所以，只有当 $\alpha_i-\alpha_j = 1$时，这才成立。
- 若 $a = 1$，由于 $p = \dfrac{\alpha_i+\alpha_j}{\alpha_i-\alpha_j}$，则 $\alpha_i-\alpha_j = 1$
- 如果 $a = 2$, $\alpha_i^2-\alpha_j^2 = (\alpha_i-\alpha_j)(\alpha_i+\alpha_j)\ = 1\times p = p$.
- 根据牛顿二项式定理 $(\alpha_i+\alpha_j)^{\ n} = \sum_{k=0}^{n}\binom{n}{k}\alpha_i^k\alpha_j^{n-k}$，假设 $2\mid a$，则存在 $\beta\in\mathbb{Z}$ 使得 $a = 2\beta$。在这种情况下

$$\alpha_i^a-\alpha_j^a = \alpha_i^{2\beta}-\alpha_j^{2\beta} = (\alpha_i^2)^\beta-(\alpha_j^2)^\beta$$

$$
\begin{aligned}
&= (\alpha_i^2 - \alpha_j^2)(\alpha_i^{2(\beta-1)} + \alpha_i^{2(\beta-2)}\alpha_j^2 + \cdots + \alpha_i^2\alpha_j^{2(\beta-2)} + \alpha_j^{2(\beta-1)}) \\
&= p(\alpha_i - \alpha_j)\left(\sum_{k=0}^{\beta-1} \alpha_i^{2(\beta-1-k)}\alpha_j^{2k}\right) \\
&= p\left(\sum_{k=0}^{\beta-1} \alpha_i^{2(\beta-1-k)}\alpha_j^{2k}\right)
\end{aligned}
$$

Setting $\delta = \left(\sum_{k=0}^{\beta-1} \alpha_i^{2(\beta-1-k)}\alpha_j^{2k}\right)$, we have $\alpha_i^a - \alpha_j^a = p\delta$

定理 1.3。
如果 δ是一个素数的完全平方数，那么 $Card\left(\mathcal{B}_\delta\left(x,\ y\right)_{|x\geq 4\delta}\right) = 3$。

证明 1.4。
δ是一个完全平方数，其素数因数为 t，且满足 $\delta = t^2$。在这种情况下， $Div(\delta) = \{1, t, \delta\}$, 换言之， δ 有 3 个因数。
根据 [1], 中使用单射同态的定理 2，我们得到平凡单射态射 $f_{1\longrightarrow\delta}$、平凡自同构 $f_{\delta\longrightarrow\delta}$ 以及态射 $f_{t\longrightarrow\delta}$。其中，$\mathcal{B}_1(x,y)_{|x\geq 4}\{(4,0)\}$， $\mathcal{B}_t(x,y)_{|x\geq 4t}\{(4,0),\ ((t+1)^2, t^2-1)\}$。 $\mathcal{B}_1(x,y)_{|x\geq 4} = \{(4,0)\}$， 且 $\mathcal{B}_t(x,y)_{|x\geq 4t} = \{(4t,0),\ ((t+1)^2, t^2-1)\}$ 定义如下：对所有 $i \in Div(\delta)$

$$
\begin{aligned}
f_{i\to\delta}:\ \mathcal{B}_i(x,y)_{|x\geq 4i} &\longrightarrow \mathcal{B}_\delta(x,y)_{|x\geq 4\delta} \\
(x,y) &\longmapsto \left(x\frac{\delta}{i}, y\frac{\delta}{i}\right)
\end{aligned}
$$

当 $f_{i\to\delta}((4,0)) = (4\delta, 0) \in \mathcal{B}_\delta(x,y)_{|x\geq 4\delta}$、 $f_{t\to\delta}((4,0)) = (4\delta, 0) \in \mathcal{B}_\delta(x,y)_{|x\geq 4\delta}$、$f_{t\to\delta}(((t+1)^2, t^2-1)) = (t(t+1)^2,\ t(t^2-1)) \in \mathcal{B}_\delta(x,y)_{|x\geq 4\delta}$ 以及 $((\delta+1)^2, \delta^2-1) \in \mathcal{B}_\delta(x,y)_{|x\geq 4\delta}$时。

因此 $\in \mathcal{B}_\delta(x,\ y)_{|x\geq 4\delta}$ 恰好有 3 个点。

定理 1.5。

(1) 设 n 为一个 RSA 模数， α_i 为一个整数序列， $\{P_0,\ P_2,\ P_3,\ P_4\}$ 为 $\mathcal{B}_n(x,y)_{|x\geq 4n}$的代数子集。存在 $X_{\alpha_i} = (-\alpha_i,\ \alpha_i + 1) \in \mathbb{Z}^2$，使得 $\langle X_{\alpha_i},\ P_i\rangle_{i=0,2\cdots 4} = 0$以及 $2\alpha_i + 1 \in \{1, p, q, n\}$成立。(2) 对于 P_2 和 P_3 ，若有 $\langle X_{\alpha_2},\ P_2\rangle = 0$ 和 $\langle X_{\alpha_3},\ P_3\rangle = 0$，则 $\begin{matrix} x_{P_1} \\ y_{P_1} \end{matrix} = \alpha_3 + \alpha_2 + 1\alpha_3 - \alpha_2$(3) p、q 分别由 n 和 $\varphi(n)$ 给出，即 $2\alpha_2 + 1$、 $2\alpha_3 + 1$ 分别为$2\alpha_4 + 1$ 和 $4\alpha_2\alpha_3$。

(4)

$$
\forall\ P_i \in \{P_0, P_1, P_2, P_3, P_4\},\quad P_i = \begin{cases} x_{P_i}\left(1,\ \dfrac{\alpha_3 - \alpha_2}{\alpha_3 + \alpha_2 + 1}\right) & if\ i = 1 \\ x_{P_i}\left(1,\ \dfrac{\alpha_i}{\alpha_i + 1}\right) & else \end{cases}
$$

(5)

$P_0 = (16\alpha_2\alpha_3 + 8\alpha_2 + 8\alpha_3 + 4,\ 0)$

$P_1 = \big(4\alpha_2^2 + 8\alpha_2\alpha_3 + 4\alpha_3^2 + 8\alpha_2 + 8\alpha_3 + 4,$
$P_2 = \big(8\,\alpha_2\alpha_3^2 + 16\,\alpha_2\alpha_3 + 4\,\alpha_3^2 + 8\,\alpha_2 + 8\,\alpha_3 + 4,$
$8\,\alpha_2\alpha_3^2 + 8\,\alpha_2\alpha_3 + 4\,\alpha_3^2 + 4\,\alpha_3\big)P_3 = \big(8\,\alpha_2^2\alpha_3 + 4\,\alpha_2^2 + 16\,\alpha_2\alpha_3 + 8\,\alpha_2 + 8\,\alpha_3 + 4,$
$8\,\alpha_2^2\alpha_3 + 4\,\alpha_2^2 + 8\,\alpha_2\alpha_3 + 4\,\alpha_2\big)P_4 = \big(4\,\alpha_4^2 + 8\,\alpha_4 + 4, \quad 4\,\alpha_4^2 + 4\,\alpha_4\big)$

(6) 如式（1）所定义的 $\alpha_{i|_{i=2,\cdots 4}}$s 满足以下方程组：

$$\begin{cases} 4\alpha_2\alpha_3 + 2(\quad\quad \alpha_2 + \alpha_3 \ + 1 = n)(a) \\ \quad\quad 4 \\ \\ \\ \\ \\ \end{cases}$$

$$16\alpha_2^3\alpha_3^3 + 32\alpha_2^3\alpha_3^2 + 32\alpha_2^2\alpha_3^3 + 20\alpha_2^3\alpha_3 + 68\alpha_2^2\alpha_3^2 + 20\alpha_2\alpha_3^3 - 2\alpha_2^2\alpha_3 n - 2\alpha_2\alpha_3^2 n +$$
$$46\alpha_2^2\alpha_3 + 46\alpha_2\alpha_3^2 + 4\alpha_3^3 - \alpha_2^2 n - 8\alpha_2\alpha_3 n - \alpha_3^2 n + 10\alpha_2^2 + 34\alpha_2\alpha_3 +$$
$$10\alpha_3^2 - 4\alpha_2 n - 4\alpha_3 n + n^2 + 8\alpha_2 + 8\alpha_3 - 2n + 2 \ = n\ n+1\ ^2 \quad\quad b \quad\quad\quad\quad)\,(\,)\,()\,($$

$$8\alpha_2^2\alpha_3^2 + 12\alpha_2^2\alpha_3 + 12\alpha_2\alpha_3^2 + 4\alpha_2^2 + 18\alpha_2\alpha_3 + 4\alpha_3^2 -$$
$$\alpha_2 n - \alpha_3 n + 6\alpha_2 + 6\alpha_3 - n + 2 \quad 2\alpha_2\alpha_3 + \alpha_2 + \alpha_3 \quad)(\,) = n(n^2-1)\,(c)$$ 或等价地，令 $P = \alpha_2\alpha_3$ and $S = \alpha_2 + \alpha_3$, $P$and S 满足以下方程组：

$$\begin{cases} 4P + 2S + 1 = n\,(a)\ (32S + 28)P^2 + (20P + 10 - n)S^2 + (34 - 2n) \\ \\ 16P^3 + 4S^3 + \\ \ 14 - 6n\ P + \\ \\ \\ \end{cases}$$

$$PS + (\,)\,(8 - 4n)S = {}^{n}(n+1)_4 \quad ^2 - n^2 + 2n - 2\,(b)\big[8P^2 + 4S^2 + 12PS + 10P + (6-n)S - n + 2\big]\,(2P + S) \ = {}^{n}$$
$(n^2-1)\,4\,(c)$

(7) 对所有 $i \in \{0,2,3,4\}$、$\dfrac{\alpha_{ai}}{\alpha_{bi}} \leq \dfrac{\alpha_{aj}}{\alpha_{bj}}\ \forall\ j > i$。(8) 更一般地，存在 $\alpha_i \in \mathbb{Z}_{\geq 0}$，使得 $P_i = \left(4n^{(\alpha_i+1\ ^2)},\ 4n(\alpha_i+1)\cdot {}^{\alpha_i}_{2\alpha_i+1}\right) \in \mathcal{B}_n(x,y)|_{x\geq 4n}$

(9) 考虑 RSA 模数 n 下的 $\mathcal{B}_n(x,y)|_{x\geq 4n}$，数列 α_n 的通项为 $\alpha_i = {}^{\tau_i - 1}_{2} \quad \forall\ \tau_i \in Div(n)$，其中 $\alpha_0 = 0$ 和 $\alpha_4 = {}^{n-1}_{2}$。

证明 1.6。

(1) 为了证明这一点，我们考虑 $X_{\alpha_i} = (-\alpha_i, \quad \alpha_i + 1) \in \mathbb{Z}^2$ 和 $P_i = (x_{P_i}, \quad y_{P_i})$，其中 $i \in \{0,2,3,4\}$。标量积 $\langle X_{\alpha_i},\ P_i\rangle_{i=0,\ 2\cdots 4} = 0$ 等价于 $-\alpha_i x_{P_i} + (\alpha_i+1)y_{P_i} = 0$，最终得到 $\alpha_i = {}^{y_{P_i}}_{x_{P_i} - y_{P_i}}$。这里不失一般性，对于所有 $P_i \in \{P_0,\ P_2,\ P_3,\ P_4\}$，根据 $\mathcal{B}_n(x,\ y)|_{x\geq 4n}$结构，$x_{P_i} \neq y_{P_i}$，因此 α_i 是定义良好的，并且

$$X_{\alpha_i} = \left(-\frac{y_{P_i}}{x_{P_i} - y_{P_i}},\ \frac{x_{P_i}}{x_{P_i} - y_{P_i}}\right). \text{ By the same,}$$
$$2\alpha_i + 1 = \frac{2y_{P_i}}{x_{P_i} - y_{P_i}} + 1$$
$$= \frac{x_{P_i} + y_{P_i}}{x_{P_i} - y_{P_i}} = \frac{(x_{P_i} + y_{P_i})^2}{x_{P_i}^2 - y_{P_i}^2} = \frac{x_{P_i}^2 + y_{P_i}^2 + 2x_{P_i}y_{P_i}}{x_{P_i}^2 - y_{P_i}^2}$$

$$= \frac{x_{P_i}^2 + x_{P_i}^2 + 2x_{P_i}y_{P_i} - 4nx_{P_i}}{x_{P_i}^2 - x_{P_i}^2 + 4nx_{P_i}} \text{ since } y_{P_i}^2 = x_{P_i}^2 - 4nx_{P_i}^2$$

$$= \frac{2x_{P_i}^2 + 2x_{P_i}y_{P_i} - 4nx_{P_i}}{4nx_{P_i}}$$

$$= \frac{x_{P_i}}{2n} + \frac{y_{P_i}}{2n} - 1, \text{ since for all } P_i \in \{P_0,\ P_2,\ P_3,\ P_4\},$$

$$P_i \in \left\{(4n,\ 0)\,,\ \left(p(q+1)^2,\ p(q^2-1)\right)\,,\ \left(q(p+1)^2,\ q(p^2-1)\right)\right\}$$

$$\cup \left\{\left((n+1)^2,\ n^2-1\right)\right\}$$

对于每个 P_i，我们有:

$$\frac{x_{P_i}}{2n} + \frac{y_{P_i}}{2n} - 1 = \frac{4n+0}{2n} - 1 = 2 - 1 = 1 \ \in \{1, p, q, n\} \text{ or}$$

$$\frac{x_{P_i}}{2n} + \frac{y_{P_i}}{2n} - 1 = \frac{p(q+1)^2 + p(q^2-1)}{2n} - 1 = \frac{nq + 2n + p + qn - p - 2n}{2n} = q$$

$$\in \{1, p, q, n\} \text{ or}$$

$$= \frac{q(p+1)^2 + q(p^2-1)}{2n} - 1 = \frac{np + 2n + q + pn - q - 2n}{2n} = p$$

$$\in \{1, p, q, n\} \text{ or}$$

$$= \frac{(n+1)^2 + n^2 - 1}{2n} - 1 = \frac{n^2 + 2n + 1 + n^2 - 1}{2n} = \frac{2n^2}{2n} = n$$

Hence $2\alpha_i + 1 \ \in \{1, p, q, n\}$ for all $i \in \{0, 2, 3, 4\}$.

(2) 在此处，在与上述相同的条件下，考虑 $2\alpha_2 + 1 = p$ and $2\alpha_3 + 1 = q$。根据 $\mathcal{B}_n(x, y)|_{x \geq 4n}$ 结构,

$$\frac{x_{P_1}}{y_{P_1}} = \frac{(p+q)^2}{p^2 - q^2} = \frac{p+q}{p-q}$$

$$= \frac{2\alpha_2 + 1 + 2\alpha_3 + 1}{2\alpha_2 + 1 - 2\alpha_3 - 1}$$

$$= \frac{\alpha_2 + \alpha_3 + 1}{\alpha_2 - \alpha_3}.$$

(3) 这是由 (2) 对于 p and q，以及欧拉函数 $\varphi(n) = (p-1)(q-1) = \alpha_2\alpha_3$ 得出的。

(4) 若 $i = 1$，由 *(2)* 可得 $\dfrac{x_{P_1}}{y_{P_1}} = \dfrac{\alpha_2 + \alpha_3 + 1}{\alpha_2 - \alpha_3}$，因此 $y_{P_1} = \dfrac{\alpha_3 - \alpha_2}{\alpha_3 + \alpha_2 + 1}$，从而 $\left(x_{P_1},\ \dfrac{\alpha_3 - \alpha_2}{\alpha_3 + \alpha_2 + 1} x_{P_1}\right)$。若非如此，考虑由 *(1)* 得到的标量积关系，

$\langle X_{\alpha_i},\ P_i\rangle_{i=2\cdots4} = 0$，可得 $\dfrac{x_{P_i}}{y_{P_i}} = \dfrac{\alpha_i + 1}{\alpha_i}$，进而 $y_{P_1} = \dfrac{\alpha_i}{\alpha_i + 1}$。在此情况下，对所有 $i \in \{2, 3, 4\}$，$P_i = (x_{P_i},\ y_{P_i}) = \left(x_{P_i},\ \dfrac{\alpha_i}{\alpha_i + 1} x_{P_i}\right)$。这对 $i = 0$ 成立。因此

$$\forall\ P_i \in \{P_0, P_1, P_2, P_3, P_4\}\,,\quad P_i = \begin{cases} x_{P_i}\left(1,\ \dfrac{\alpha_3 - \alpha_2}{\alpha_3 + \alpha_2 + 1}\right) & if\ i = 1 \\ x_{P_i}\left(1,\ \dfrac{\alpha_i}{\alpha_i + 1}\right) & else \end{cases}$$

(5) 由 (1) 得到 $2\alpha_2+1=p$、 $2\alpha_3+1=q$ 和 $2\alpha_4+1=n$，将这些值代入 $\mathcal{B}_n(x,y)|_{x\geq 4n}=\{(4n,0)$ $((p+q)^2$，可得 $p^2-q^2)$、 $(p(q+1)^2$、 $p(q^2-1))$、 $(q(p+1)^2$、 $q(p^2-1)$ $)$、 $((n+1)^2$、 $n^2-1)\}$。对于 $P_0=(4n,0)$，得到 $P_0=(16\alpha_2\alpha_3+8\alpha_2+8\alpha_3+4,0)$。对于 P_1、 P_2、 P_3 和 P_4，展开后得到$P_1=\big(4\,\alpha_2^2+8\,\alpha_2\alpha_3+4\,\alpha_3^2+8\,\alpha_2+8\,\alpha_3+4$、$4\,\alpha_2^2-4\,\alpha_3^2+4\,\alpha_2-4\,\alpha_3\big)$; $P_2=\big(8\,\alpha_2\alpha_3^2+16\,\alpha_2\alpha_3+4\,\alpha_3^2+8\,\alpha_2+8\,\alpha_3+4$、$8\,\alpha_2\alpha_3^2+8\,\alpha_2\alpha_3+4\,\alpha_3^2+4\,\alpha_3\big)$; $P_3=\big(8\,\alpha_2^2\alpha_3+4\,\alpha_2^2+16\,\alpha_2\alpha_3+8\,\alpha_2+8\,\alpha_3+4$、$8\,\alpha_2^2\alpha_3+4\,\alpha_2^2+8\,\alpha_2\alpha_3+4\,\alpha_2\big)$和 $P_4=\big(4\,\alpha_4^2+8\,\alpha_4+4$、 $4\,\alpha_4^2+4\,\alpha_4\big)$

(6) 对于 (a)，由于 $n=(2\alpha_2+1)(2\alpha_3+1)=4\alpha_2\alpha_3+2(\alpha_2+\alpha_3)+1$。现在对于 (b) 和 (c)，我们从 [1], 知道 $P_2+P_3=P_4$。由于 $(x_{P_2+P_3},\ y_{P_2+P_3})=(x_{P_4},\ y_{P_4})$。我们令 $((b),\ (c))=(x_{P_2+P_3},\ y_{P_2+P_3})$。回顾 $\mathcal{B}_n(x,\ y)|_{\mathbb{Z}}$ 上点 P_2 和 P_3 的加法群律定义如下

$$\begin{cases} x_{P_2+P_3}=\dfrac{1}{2n}\left[(x_{P_2}-2n)(x_{P_3}-2n)+y_{P_2}y_{P_3}\right]+2n \\ y_{P_2+P_3}=\dfrac{1}{2n}\left[y_{P_2}(x_{P_3}-2n)+y_{P_3}(x_{P_2}-2n)\right] \end{cases}$$

然后，将系统中以 $\alpha_i^{'}$ 表示的 P_2 和 P_3 的表达式（来自 (3)）代入

$$\begin{cases} \dfrac{1}{2n}\left[(x_{P_2}-2n)(x_{P_3}-2n)+y_{P_2}y_{P_3}\right]+2n=x_{P_4}=(n+1)^2 \\ \dfrac{1}{2n}\left[y_{P_2}(x_{P_3}-2n)+y_{P_3}(x_{P_2}-2n)\right]=y_{P_4}=n^2-1 \end{cases}$$

最终得到

$$\begin{cases} 16\alpha_2^3\alpha_3^3+32\alpha_2^3\alpha_3^2+32\alpha_2^2\alpha_3^3+20\alpha_2^3\alpha_3+68\alpha_2^2\alpha_3^2+20\alpha_2\alpha_3^3-2\alpha_2^2\alpha_3 n-2\alpha_2\alpha_3^2 n+ \\ 46\alpha_2^2\alpha_3+46\alpha_2\alpha_3^2+4\alpha_3^3-\alpha_2^2 n-8\alpha_2\alpha_3 n-\alpha_3^2 n+10\alpha_2^2+34\alpha_2\alpha_3+ \\ 4(10\alpha_3^2-4\alpha_2 n-4\alpha_3 n+n^2+8\alpha_2+8\alpha_3-2n+2=n\ n+1\ ^2 \qquad b \qquad)\ (\ )\ ()\ (\\ \\ \\ \\ 4 \\ 8\alpha_2^2\alpha_3^2+12\alpha_2^2\alpha_3+12\alpha_2\alpha_3^2+4\alpha_2^2+18\alpha_2\alpha_3+4\alpha_3^2- \\ \alpha_2 n-\alpha_3 n+6\alpha_2+6\alpha_3-n+2\ \ 2\alpha_2\alpha_3+\alpha_2+\alpha_3 \quad)(\ )=n(n^2-1) \qquad (c) \end{cases} \tag{6.2}$$

令 $P=\alpha_2\alpha_3$、 $S=\alpha_2+\alpha_3$，并代入上述关系式（a）和方程组（6.2），得到:

$$\begin{cases} 4P+2S+1=n \qquad (a) \\ \\ 16P^3+4S^3+(32S+28)P^2+(20P+10-n)S^2+(34-2n)PS+ \\ (14-6n)P+(8-4n)S=\dfrac{n(n+1)^2}{4}-n^2+2n-2 \qquad (b) \\ \\ \left[8P^2+4S^2+12PS+10P+(6-n)S-n+2\right](2P+S)=\dfrac{n(n^2-1)}{4} \qquad (c) \end{cases}$$

(7) 这里先回顾一下，$(\alpha_{ai},\ \alpha_{bi})=(\alpha_{ai},\ \alpha_{ai}+1)$ 且 $(\alpha_{aj},\ \alpha_{bj})=(\alpha_{aj},\ \alpha_{aj}+1)$。若 $j>i$，则 $\alpha_j>\alpha_i$ 考虑 (1)。现在 $\alpha_i<\alpha_j$ 则 $\alpha_i+\alpha_i\alpha_j<\alpha_j+\alpha_i\alpha_j$ 因为 $\alpha_i>0$，$\alpha_j>0$。我们有 $\alpha_i(\alpha_j+1)<\alpha_j(\alpha_i+1)$。最后 $\dfrac{\alpha_i}{\alpha_i+1}<\dfrac{\alpha_j}{\alpha_j+1}$。因此 $\dfrac{\alpha_{ai}}{\alpha_{bi}}<\dfrac{\alpha_{aj}}{\alpha_{bj}}$。

(8) Consider $P_i = \left(4n\dfrac{(\alpha_i+1)^2}{2\alpha_i+1},\ 4n(\alpha_i+1)\cdot\dfrac{\alpha_i}{2\alpha_i+1}\right) \in \mathcal{B}_n(x,y)_{|_{x\geq 4n}}$, since from (1), $2\alpha_i+1\ \in\{1,p,q,n\}$ then $\alpha_i \in \left\{0, \dfrac{p-1}{2}, \dfrac{q-1}{2}, \dfrac{n-1}{2}\right\}$ then:

If $\alpha_i = 0$, $P_i = \left(4n\dfrac{1}{1},\ 4n\cdot(1)\cdot 0\right) = (4n,\ 0) \in \mathcal{B}_n(x,y)_{|_{x\geq 4n}}$.

If $\alpha_i = \dfrac{p-1}{2}$, $P_i = \left(4n\cdot\dfrac{\left(\frac{p+1}{2}\right)^2}{p},\ 4n\cdot\dfrac{p+1}{2}\cdot\dfrac{\frac{p-1}{2}}{p}\right)$

$$= \left(4n\cdot\frac{(p+1)^2}{4p},\ 4n\cdot\frac{p+1}{2}\cdot\frac{p-1}{2p}\right)$$

$$= \left(q(p+1)^2,\ q(p^2-1)\right) \in \mathcal{B}_n(x,y)_{|_{x\geq 4n}}.$$

If $\alpha_i = \dfrac{q-1}{2}$, $P_i = \left(4n\cdot\dfrac{\left(\frac{q+1}{2}\right)^2}{q},\ 4n\cdot\dfrac{q+1}{2}\cdot\dfrac{\frac{q-1}{2}}{q}\right)$

$$= \left(4n\cdot\frac{(q+1)^2}{4q},\ 4n\cdot\frac{q+1}{2}\cdot\frac{q-1}{2q}\right)$$

$$= \left(p(q+1)^2,\ p(q^2-1)\right) \in \mathcal{B}_n(x,y)_{|_{x\geq 4n}}$$

If $\alpha_i = \frac{n-1}{2}$, $P_i = \left(4n\cdot\dfrac{\left(\frac{n+1}{2}\right)^2}{n},\ 4n\cdot\dfrac{n+1}{2}\cdot\dfrac{\frac{n-1}{2}}{n}\right)$

$$= \left(4n\cdot\frac{(n+1)^2}{4n},\ 4n\cdot\frac{n+1}{2}\cdot\frac{n-1}{2n}\right)$$

$$= \left((n+1)^2,\ n^2-1\right) \in \mathcal{B}_n(x,y)_{|_{x\geq 4n}}.$$

(9) 这是由 1 得出的直接观察。由于 $2\alpha_i+1 \in \{1,p,q,n\}$, then either $\alpha_i = 0$, $\alpha_i = \dfrac{p-1}{2}$ or $\alpha_i = \dfrac{q-1}{2}$ or $\alpha_i = \dfrac{n-1}{2}$.

猜想1.7。
对于所有 $i\in\{1,2,3,4\}$, $P_i \in \{P_1,P_2,\ P_3,\ P_4\}$, $\mathcal{B}_n(x,y)$ 的代数子集$_{|_{x\geq 4n}}$。若存在 $(\alpha_{ii},\alpha_{ji})\ \in \mathbb{Z}^2_{\geq 0}$，使得 $\begin{matrix} x_{P_i} \\ y_{P_i} \end{matrix} = \begin{matrix} \alpha_{ii} \\ \alpha_{ji} \end{matrix}$ 且最大公约数$(\alpha_{ii},\ \alpha_{ji})\ = 1$，则 $\alpha_{i1}+\alpha_{j1} = \alpha_{i3}+\alpha_{j3}$且 $\alpha_{ii}+\alpha_{ji} \in \{p,q,n\}$。

例1.8。
这里我们考察下表中的 11 个不同的 n，它们的 $\mathcal{B}_n(x,\ y)_{|_{x\geq 4n}}$结构及其对应的 $\begin{matrix} \alpha_{ii} \\ \alpha_{ji} \end{matrix}$:

—

TABLE 1. Table of $\mathcal{B}_n(x,y)|_{x\geq 4n}$ and $\dfrac{\alpha_{ii}}{\alpha_{ji}}$ for 11 different n values

n	$\mathcal{B}_n(x,y)\|_{x\geq 4n}$	$\frac{\alpha_{i1}}{\alpha_{j1}}$	$\frac{\alpha_{i2}}{\alpha_{j2}}$	$\frac{\alpha_{i3}}{\alpha_{j3}}$	$\frac{\alpha_{i4}}{\alpha_{j4}}$
15	$\{(60,0),(64,16),(80,40),(108,72),(256,224)\}$	$\frac{4}{1}$	$\frac{2}{1}$	$\frac{3}{2}$	$\frac{8}{5}$
35	$\{(140,0),(144,24),(252,168),(320,240),(1296,1224)\}$	$\frac{6}{2}$	$\frac{3}{2}$	$\frac{4}{3}$	$\frac{13}{8}$
77	$\{(308,0),(324,72),(704,528),(1008,840),(6084,5928)\}$	$\frac{9}{2}$	$\frac{4}{3}$	$\frac{6}{5}$	$\frac{17}{13}$
143	$\{(572,0),(576,48),(1872,1560),(2156,1848),(20736,20448)\}$	$\frac{12}{2}$	$\frac{5}{3}$	$\frac{7}{6}$	$\frac{39}{38}$
391	$\{(1564,0),(1600,240),(7452,6624),(9792,8976),(153664,152880)\}$	$\frac{20}{3}$	$\frac{6}{3}$	$\frac{12}{11}$	$\frac{77}{196}$
713	$\{(2852,0),(2916,432),(17856,16368),(23552,22080),(509796,508368)\}$	$\frac{27}{4}$	$\frac{12}{11}$	$\frac{16}{15}$	$\frac{195}{356}$
14893	$(59572,0),(111556,76152),(819396,789048),(4214772,4184880),$ $(221831236,221801448)$	$\frac{167}{114}$	$\frac{27}{26}$	$\frac{141}{140}$	$\frac{7447}{7446}$
44923	$(179692,0),(190096,44472),(7592256,7501872),(12174300,12084120),$ $(201816776,201807592 8)$	$\frac{218}{51}$	$\frac{84}{83}$	$\frac{135}{134}$	$\frac{22462}{22461}$
58307	$(233228,0),(242064,46248),(11720000,11602800),$ $(17200764,17083752),(3399822864,3399706248)$	$\frac{246}{47}$	$\frac{100}{99}$	$\frac{147}{146}$	$\frac{29154}{29153}$
439007603	$(1756030412,0),(2065157136,798996408),(6116692964112,6115814885880),$ $(13835324622476,1383444657940 8),(19272767636982081 6,19272767549180560 8)$ $(48400115563041438556,0),(49139988961662726400,60297073429211040),$ $(37206579369977836429336472656,37206579345777778639945602360),$ $(47614527370423585388056617100,47614527346223527600386064680),$ $(14641069915723537932$ $215814598214092960 0,14641069915723537932$ $979580882006202103 20)$	$\frac{22722}{8791}$	$\frac{6966}{6965}$	$\frac{15757}{15756}$	$\frac{219503802}{219503801}$
12100028890		$\frac{3504996040}{430079469}$	$\frac{15374582 86}{15374582 85}$	$\frac{19675377 55}{19675377 54}$	$\frac{60500144453801798 20}$
760359639					$\frac{60500144453801798 19}$

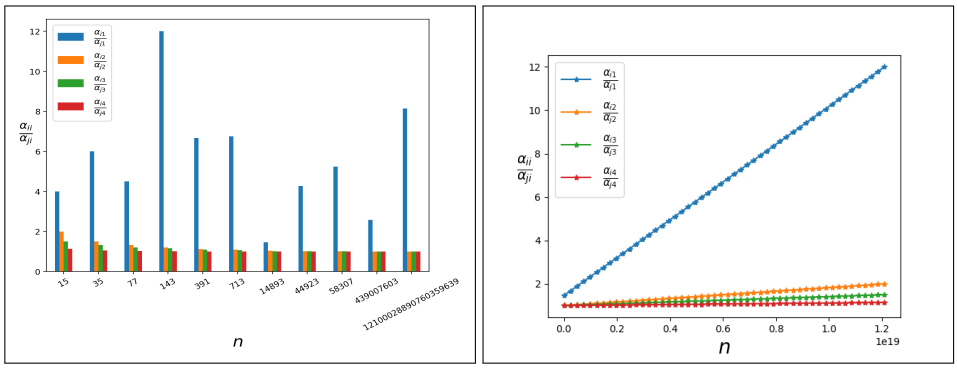

图 1. $\frac{\alpha_{ii}}{\alpha_{ji}}$ 来自一个 10 $\mathcal{B}_n(x,y)|_{x\geq 4n}$样本

从这些图中可以观察到，$\frac{\alpha_{ii}}{\alpha_{ji}}$ 在 $\mathcal{B}_n(x,y)|_{x\geq 4n}$上的最大值出现在 $i=1$处：点 P_1；其次是 $i=2$处的点P_2，再其次是 P_3，最后是点 P_4。数列 α_{ii} 是一个α_{ji}递减数列。

关于这个样本，还有一点值得注意：对于 $i\in\{2,3,4\}$，数列 $\frac{\alpha_i}{\alpha_j}$似乎随着$n$ 趋于无穷而收敛，并且随着 n 增大，$\alpha_{i2}\simeq\alpha_{i3}\simeq\alpha_{i4}$ 也如此。$\alpha_{j2}\quad\alpha_{j3}\quad\alpha_{j4}$

2. 攻击

本节介绍该攻击。这是一种通用攻击，仅依赖于模数 n，而不依赖于密码系统设定中公开参数 e 或私有指数 d 的大小。与 Wiener攻击相比，这是一种新方法。

在介绍之前，先回顾 RSA密码系统的一些预备知识，以及迄今为止与非通用攻击相关的研究工作。

2.1. RSA密码系统回顾。 我们分别用 $\mathcal{P}$、$\mathcal{C}$、$\mathcal{K}$、$\mathcal{E}_k$、$\mathcal{D}_k$ 表示明文空间、密文空间、密钥空间、加密算法和解密算法。

其中 $\mathcal{P}=\mathcal{C}=\mathbb{Z}/n\mathbb{Z}$，且
$\mathcal{K}=\{(p,q,n,e,d)\in\mathbb{Z}_+^5,\ p,q\text{个素数}\ /\ n=pq,\ ed\equiv 1\text{模}\ \varphi(n)\}$, p,q 是随机选取的，$1<e<\varphi(n)$ / 最大公约数$(e,\varphi(n))=1$，并且 d 满足 $ed\equiv 1$ 模 $\varphi(n)$。公开参数为(n,e)，秘密参数为(p,q,d)。以下是加密算法和解密算法。

$$\mathcal{E}_k:\mathcal{P}\longrightarrow\mathcal{C}\quad;\quad m\longmapsto\mathcal{E}_k(m)=m^e\mod n$$

$$\mathcal{D}_k:\mathcal{C}\longrightarrow\mathcal{P}\quad;\quad c\longmapsto\mathcal{D}_k(c)=c^d\mod n$$

$\forall\, m\in\mathcal{P}$，$\mathcal{E}_k(m)=m^e$ 模 $n=c$ 且 $\mathcal{D}_k(c)=c^d$ 模 $n=m$。当 $\mathcal{D}_k(\mathcal{E}_k)=\mathcal{E}_k(\mathcal{D}_k)=id$ 时。

2.2. 关于非通用攻击的相关工作。大多数非通用攻击基于连分数的发展 [5]以及 Coppersmith [8] 定理的应用。Wiener 在 [5], 的研究表明，对于界限 $d < \frac{1}{3}N^{0.25}$，可以在多项式时间内恢复私钥 d。沿着同一思路，De Weger 在 [6] 提出了另一个界限 $d < \frac{N^{\frac{3}{4}}}{|p-q|}$。随后，Nitaj 等人在 [7], 提出了改进后的界限 $d < \frac{\sqrt{6}\sqrt{2}}{6}N^{0.25}$。在 [4], ，Bunder 等人提出了一个新的改进界限，并证明当 $d < 2\sqrt{2}N^{\frac{1}{4}}$ 时可以恢复 d 。

最近，在 [3] Ariffin 等人提出了一种改进的新型短解密指数攻击，针对 $d < \sqrt{\frac{a^j+b^i}{2}}\left(\frac{N}{e}\right)^{\frac{1}{2}}N^{0.375}$。通过设定 $N_1 = N - \left\lceil\left(\frac{a^{\frac{j}{i}}+b^{\frac{j}{i}}}{2ab}\right)^{-\frac{j}{2i}} + \left(2ab\right)^{\frac{1}{2j}}\right)\sqrt{N}\rceil + 1$，他们证明可以在多项式时间内，根据 $\frac{e}{N_1}$ 的连分数的渐近分数恢复 d。所有这些攻击都受欧拉函数近似值以及私钥 d 的长度或公钥指数 e 的长度的限制，因此，当公开参数 e 选择得当时，这些攻击的效果有限，相应地， d 也会选择得当。

因此，我们提出一种基于连分数的通用攻击。该攻击独立于公钥和私钥 e 以及 d 。

该攻击通过 $\frac{\alpha_{i4}}{\alpha_{j4}} + \delta$的一个渐近分数，寻找满足 $\langle X_{\alpha_3}, P_3\rangle = 0$的 $X_\alpha = (-\alpha_3, \alpha_3 + 1)$。

若攻击成功，则可在 $\mathcal{O}(b\log\ \alpha_{j4}\log(\alpha_{i3}+\alpha_{j3}))$内恢复 RSA 私钥 d。为此，我们先考虑以下结果。

引理 2.1。
RSA 类型的模数，并考虑结构 $\mathcal{B}_n(x,\ y)|_{x\geq 4n}$，则 $3\alpha_{j3} < \alpha_{j4}$。

证明 2.2。
$\forall\ n = pq, pq < n+2$，那么 $q < \frac{pq}{3} < \frac{n+2}{3}$ 最后 $q < \frac{n+2}{3}$ 然后 $3q < n+2$，且 $3(q-1) < n-1$ 因此 $3\alpha_{j3} < \alpha_4$。

定理 2.3。
设 n 是一个 RSA 模数， $\mathcal{B}_n(x,\ y)|_{x\geq 4n}$ 是相应的双曲线结构。存在 $\delta \leq \frac{1+\alpha_{j4}-\alpha_{j3}}{\alpha_{j4}\alpha_{j3}}$，更精确地说 $0 < \frac{\alpha_{j4}-\alpha_{j3}}{\alpha_{j4}\alpha_{j3}} < \delta \leq \frac{1+\alpha_{j4}-\alpha_{j3}}{\alpha_{j4}\alpha_{j3}}$，使得 $\frac{\alpha_{i3}}{\alpha_{j4}}$ 是 $\frac{\alpha_{i4}}{\alpha_{j3}} + \delta$ 的渐近分数。

证明 2.4。
考虑

$$0 < \frac{\alpha_{j4}-\alpha_{j3}}{\alpha_{j4}\alpha_{j3}} < \delta \leq \frac{1+\alpha_{j4}-\alpha_{j3}}{\alpha_{j4}\alpha_{j3}}$$
$$\alpha_{j4}-\alpha_{j3} < \delta\alpha_{j4}\alpha_{j3} \leq 1+\alpha_{j4}-\alpha_{j3}$$
$$0 < \delta\alpha_{j4}\alpha_{j3} - (\alpha_{j4}-\alpha_{j3}) \leq 1$$

$$\begin{aligned}
&\text{From Lemma 2.1, } 3\alpha_{j3} < \alpha_{j4} \\
0 < 3\alpha_{j3}\left[\delta\alpha_{j4}\alpha_{j3} - (\alpha_{j4} - \alpha_{j3})\right] &\le 3\alpha_{j3} < \alpha_{j4} \\
0 < 2\alpha_{j3}\left[\delta\alpha_{j4}\alpha_{j3} - (\alpha_{j4} - \alpha_{j3})\right] &< \alpha_{j4} \\
0 < 2\alpha_{j3}\left[\alpha_{j4}\alpha_{j3} - \alpha_{j4}\alpha_{j3} + \delta\alpha_{j4}\alpha_{j3} - (\alpha_{j4} - \alpha_{j3})\right] &< \alpha_{j4} \\
0 < 2\alpha_{j3}\left[\alpha_{j3}(\alpha_{j4} + 1) + \delta\alpha_{j4}\alpha_{j3} - \alpha_{j4}(\alpha_{j3} + 1)\right] &< \alpha_{j4} \\
0 < 2\alpha_{j3}\left[\alpha_{j3}\alpha_{i4} + \delta\alpha_{j4}\alpha_{j3} - \alpha_{j4}\alpha_{i3}\right] &< \alpha_{j4} \\
0 < (\alpha_{j3}\alpha_{i4} + \delta\alpha_{j4}\alpha_{j3} - \alpha_{j4}\alpha_{i3}) &< \frac{\alpha_{j4}}{2\alpha_{j3}} = \frac{\alpha_{j4}\alpha_{j3}}{2\alpha_{j3}^2} \\
&\text{Dividing the whole expression by } \alpha_{j4}\alpha_{j3}\text{, we have:} \\
0 < \left|\frac{\alpha_{i4}}{\alpha_{j4}} + \delta - \frac{\alpha_{i3}}{\alpha_{j3}}\right| &< \frac{1}{2\alpha_{j3}^2}
\end{aligned}$$

现在应用勒让德定理 [9], $\frac{\alpha_{i3}}{\alpha_{j3}}$ 是 $\frac{\alpha_{i4}}{\alpha_{j4}} + \delta$的一个渐近分数。即存在 $k \le n$，使得 $[a_0, a_1, \ldots, a_k] = \frac{\alpha_{i3}}{\alpha_{j3}}$，且满足 $\frac{\alpha_{i4}}{\alpha_{j4}} + \delta = [a_0, a_1, \ldots, a_n]$。

注 2.5。
我们采用以下记号表示 x, $x = [a_0, a_1, \ldots, a_n] =$ 的连分数

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}.$$

x 的第 k 个渐近分数表示为 $[a_0, a_1, \ldots, a_k]$，其中 $k \le n$；我们将其记作 $\frac{p_k}{q_k} = [a_0, a_1, \ldots, a_k]$，数列（$p_k$）和（$q_k$）通过以下递归公式计算：

$$\begin{aligned}
p_{-2} = q_{-1} = 0, &\quad p_k = a_k p_{k-1} + p_{k-2} \quad \text{for all } k \ge 0, \\
p_{-1} = q_{-2} = 1, &\quad q_k = a_k q_{k-1} + q_{k-2} \quad \text{for all } k \ge 0.
\end{aligned}$$

讨论：
定理 2.3 给出了一个重要结果，使我们能够以不依赖“参数 e 和 d”的方式，使用连分数方法攻击任意 RSA 模数 n。相比之下，现有的相关攻击均受到限制，且依赖于参数 e 和 d。
根据我们的结果，找到满足 $\delta \le \frac{1 + \alpha_{j4} - \alpha_{j3}}{\alpha_{j4}\alpha_{j3}}$ 的 δ 是关键所在。我们通过近似求得 $\frac{1}{\alpha_{j3}}$ 的值来处理这个问题，因为重新排列各项后，我们得到 $\delta \le \frac{1 + \alpha_{j4} - \alpha_{j3}}{\alpha_{j4}\alpha_{j3}} = \frac{1 + \alpha_{j4}}{\alpha_{j4}\alpha_{j3}} - \frac{1}{\alpha_{j4}\alpha_{j3}} = \frac{1}{\alpha_{j4}} \cdot \frac{1}{\alpha_{j3}} - \frac{1}{\alpha_{j4}\alpha_{j3}} > 0$。
已知 $0 < \frac{1}{\alpha_{j3}} < 0.5$，通过归纳法和一个简单的经验观察（见表2）不难发现，$\frac{1}{\alpha_{j3}}$ 的小数部分恰好有（α_{j3}的位数）-1个零。

表2. α_{j3} 和 $\frac{1}{\alpha_{j3}}$的一些取值

α_{j3}	2	3	5	6	11	15	140	146	15756	1967537754	···
$\frac{1}{\alpha_{j3}}$	0.5	0.3	0.2	0.16	0.09	$0.\underbrace{0}_{1}6$	$0.\underbrace{00}_{2}714$	$0.\underbrace{00}_{2}68$	$0.\underbrace{0000}_{4}635$	$0.\underbrace{000000000}_{9}508$	···

另一个观察是，如果 α_{i4} 或 α_{j4} 有 x 位，那么 α_{i3} 有 $\frac{x}{2}$ 位。等价地，如果 α_{j4} 在十进制下有 k 个十进制位数，那么 α_{j3} 有 $\lfloor\frac{k}{2}\rfloor+1$ 位。最后，$\frac{1}{\alpha_{j3}}$ 的小数部分有 $\lfloor\frac{k}{2}\rfloor$ 个零，其中 k 是 α_{j4}的十进制位数。这些信息有助于我们近似求出 $\frac{1}{\alpha_{j3}}$。

因此，得到以下算法。

2.3. **攻击算法**。 此处给出该算法。其复杂度分析见命题 2.8

算法 1：攻击算法

输入： $n,\ P_4 \in \mathcal{B}_n(x,y)|_{x\geq 4n},\ e$: RSA 公钥指数

输出： p 和 q 的非平凡因子 n

1 **步骤 1**: 求取 n的因子

初始化界限 $b = 10^y,\ y \in \{2,3,4,5,6,7,8,9,...\}$。

初始化 n 的 $k = \sharp$ 十进制位数

初始化 $\frac{\alpha_{i4}}{\alpha_{j4}} = \frac{x_{P_4}}{y_{P_4}}$

当 $i \leq b$ **时**

$\delta \leftarrow \frac{1+\alpha_{j4}}{\alpha_{j4}} \cdot \frac{i}{10^{\lfloor\frac{k}{2}\rfloor+1+\sharp\text{的 i 的十进制位数}}} - \frac{1}{\alpha_{j4}}$

如果 $\delta > 0$ **那么**

计算渐近分数 $\frac{p_k}{q_k} = \frac{\alpha_{i3}}{\alpha_{j3}}$ of $\frac{\alpha_{i4}}{\alpha_{j4}} + \delta$

for $\frac{\alpha_{i3}}{\alpha_{j3}} \in$ 的渐近分数 $\frac{\alpha_{i4}}{\alpha_{j4}} + \delta$ **执行**

如果 最大公约数$(n,\ \alpha_{i3}+\alpha_{j3}) \neq 1,\ n$ **那么**

返回 $\alpha_{i3}+\alpha_{j3}$, 最大公约数$(n,\ \alpha_{i3}+\alpha_{j3})$

结束 if

结束 for

结束 if

结束 while

2 **步骤 2**: 从 e 获取 d： RSA 私钥

$\psi \leftarrow (\alpha_{i3}+\alpha_{j3}-1)$ (最大公约数$(\alpha_{i3}+\alpha_{j3})\ -1$)

使用扩展欧几里得算法求解 $ed + k\psi = 1$

返回 d

示例 2.6。

RSA 模数	位数	δ	$\frac{\alpha'_{i3}}{\alpha'_{j3}}$	最大公约数$(\alpha'_{i3}+\alpha'_{j3}\ \ n)$
14893	17	$\frac{7}{10^3}$	$\frac{141}{140}$	281
439007603	30	$\frac{969}{5\cdot 10^7}$	$\frac{122935301}{122932918}$	13931

注记 2.7。
此攻击可以按以下方式并行化：在 while 循环中，遍历 i 到 b 之间的不同取值时，将区间离散为不同的步长。例如，假设我们要将工作分配给 2 个中央处理器，则：在中央处理器 $_1$ 中，以步长 2 从 0 遍历到 b：0，2，4，$\cdots$，直到 b。在中央处理器 $_2$ 中，以步长 2 从 1 遍历到 b：1，3，5，$\cdots$，直到 $b-1$。

命题 2.8。

该算法 1 的复杂度为 $\mathcal{O}(b\log\ \alpha_{j4}\log(\alpha_{i3}+\alpha_{j3}))$。

证明 2.9。
步骤 1 中，初始化在常数时间内完成 $\mathcal{O}(1)$，$\frac{\alpha_{i4}}{\alpha_{j4}}+\delta$ 有$\mathcal{O}(\log\alpha_{j4})$ 个渐近分数，且计算 n 与 $\alpha_{i3}+\alpha_{j3}$的最大公约数的复杂度为 $\mathcal{O}(\alpha_{i3}+\alpha_{j3})$，因为 $\min(n,\ \alpha_{i3}+\alpha_{j3})=\alpha_{i3}+\alpha_{j3}$，因此总复杂度为 $\mathcal{O}(b\log\ \alpha_{j4}\log(\alpha_{i3}+\alpha_{j3}))$。

步骤 2 的复杂度为 $\mathcal{O}(\log e)$，因为 $1<e<\psi$ 意味着 $\min(e,\ \psi)=e$。现在，$\max(b\log\ \alpha_{j4}\log(\alpha_{i3}+\alpha_{j3}),\ \log\ e)=b\log\ \alpha_{j4}\log(\alpha_{i3}+\alpha_{j3})$，因此$\mathcal{O}$(步骤 $1+$步 2) $=\mathcal{O}(b\log\ \alpha_{j4}\log(\alpha_{i3}+\alpha_{j3}))$。

结论

我们基于 Babindamana 等人关于双曲线的研究 [1]，提出了新的算术和代数结果，并在这些新结果的基础上，描述了一种基于连分数攻击 RSA 型模数的方法。该方法不同于依赖参数 e 和 d的 Wiener攻击。攻击成功时，其复杂度为 $\mathcal{O}(b\log\ \alpha_{j4}\log(\alpha_{i3}+\alpha_{j3}))$。
与 Weiner 的攻击及其改进方法相比，这种攻击的特点是独立于私钥大小 d 和公钥指数 e，不受它们的限制。作为未来的工作，应对该方法进行深入研究，以找出 δ的最佳界限、可更快$\alpha_{j3}^{\alpha_{i3}}$ 检索的模数情形，并降低b，从而使整体复杂度达到多项式时间。

参考文献

[1] Regis F. Babindamana、Gilda R. Bansimba、Basile G. R. Bossoto（2022年）。“费马因式分解法上的格点”，《数学杂志》，第2022卷，文章编号6360264。[2] Gilda R. Bansimba、Regis F. Babindamana、Basile G. R. Bossoto（2021年）。双曲线上的一些算术性质，《JP代数、数论与应用杂志》，第50卷，第1期，第45–100页。[3] Abubakar, S. I.、Ariffin, M. R. K. 和 Asbullah, M. A.（2019年）。一种针对 *RSA* 模数 *N* 上短解密指数的改进界 $=pq$：基于 *Wiener*方法，《马来西亚数学科学杂志》 13 89 99 (S) 4月：– Bunder, M. 和 Tonien, J.（）[4] 2017。一种基于连分数的 *RSA*密码系统新攻击，《马来西亚数学科学杂志》第11(S)卷，8月：45–57（2017年）。[5] Wiener, M. J.（1990年）。短 *RSA*秘密指数的密码分析，《IEEE信息论汇刊》，36(3)：553–558。[6] De Weger, B.（2002年）。具有较小素数差的 *RSA* 密码分析。《工程、通信与计算中的应用代数》，13(1)：17–28。[7] Nitaj, A.（2013年）。*RSA*密码系统的丢番图与格密码分析。载于《人工智能、进化计算与元启发式》，第139–168页。施普林格。

[8] Don Coppersmith（1997年），多项式方程的小解与低指数 *RSA* 漏洞。《密码学杂志》，10(4)，233–260。[9] S. Lang（1966年），丢番图逼近导论，Addison-Wesley 出版公司。

数学与计算机科学系，马里安·恩古瓦比大学，科学与技术学院，邮政信箱：69，布拉柴维尔，刚果
现地址：数学与计算机科学系，马里安·恩古瓦比大学，科学与技术学院，邮政信箱：69，布拉柴维尔，刚果电子邮箱地址：bansimbagilda@gmail.com

数学与计算机科学系，马里安·恩古瓦比大学，科学与技术学院，邮政信箱：69，布拉柴维尔，刚果电子邮箱地址：regis.babindamana@umng.cg

数学系，马里安·恩古瓦比大学，科学与技术学院，邮政信箱：69，布拉柴维尔，刚果电子邮箱地址：basile.bossoto@umng.cg