Elliptic-curve factorization and witnesses

Jacek Pomykała[0000−0002−6480−5751] and
Olgierd Żołnierczyk[0000−0002−5196−3494]

Faculty of Cybernetics, Military University of Technology, Warsaw, Poland
{jacek.pomykala,olgierd.zolnierczyk}@wat.edu.pl

Abstract. We define the EC (Elliptic Curve)-based factorization witnesses and prove related results within both conditional and unconditional approaches. We present experimental computations that support the conjecture of behavior of related admissible elliptic curves in relation to the deterministic complexity of suitable factoring algorithms based on the parameters of the witnesses. This paper features three main results devoted to the factorization of RSA numbers $N = pq$, where $q > p$. The first result of computational complexity of elliptic curve factorization is improved by the factor D^{σ}, comparing to previously known result $O\left(D^{(2+o(1))}\right)$, where D is smoothness bound, assuming additional knowledge of the admissible elliptic curve. The second result demonstrates the feasibility of achieving factorization in deterministic, polynomial time, based on knowledge obtained at a specific step in the elliptic curve method (ECM), a feat previously considered impossible. The third result establishes deterministic time for conditional factorization using the elliptic version of Fermat method. It has the magnitude order $(\log N)^{O(1)}\left(1+\left(\frac{|a_p|+|a_q|}{D}\right)^2\right)$, provided $\frac{q}{p} \ll 1$. Here a_p, a_q are the Frobenius traces of the corresponding curves $(E(\mathbb{F}p), E(\mathbb{F}_q))$, and D indicates the approximation of the quotient p/q by the quotient a_p/a_q, assuming that the order of the group of points over a pseudo elliptic curve $E(\mathbb{Z}_N)$ is known.

Keywords: EC factorization · B-smooth numbers · Factor bases

1 Introduction

The Fermat-Euclide (compositness) witness $a \in \mathbb{Z}_N^*$ in relation to deterministic Pollard's $p-1$ algorithm was introduced and investigated by Źrałek in [17]. It satisfies the condition

$$\nu_l(\mathrm{ord}_p a) \neq \nu_l(\mathrm{ord}_q a),$$

for some prime $l \mid \mathrm{ord}_N a$. The more detailed definition and treatment for the sake of oracle factoring methods was developed in [14] and [7] with the aid of Dirichlet's characters reinforced by the large and shifted sieve, respectively.

The first challenge in general is to focus here on small values $a \leq A = A(N)$, reducing the problem to small values of Dirichlet character's nonresidues or more generally small generating sets of $\mathbb{Z}_N^*$, as applied in the investigation of the least witness for N in [1].

The second one concerns small values of $l \leq B = B(N)$, related to well known Pollard's $p-1$ (see [13]) and Williams $p+1$ (see [16]) method of factoring. Both A and $B-$aspects are important in the deterministic approach to factoring integers. The particular interest concerns the semiprime numbers $N = pq\,(p < q)$ where p and q are large unknown primes applied in RSA cryptosystem [15].

In this paper we investigate factoring of integers with the aid of elliptic curves as proposed in [12], called unconditional and one based on the knowledge of the order of elliptic curve E over $\mathbb{Z}_N$ called conditional (cf. [6]). Both approaches are related to each other because in the deterministic approach of searching the related pairs (E, Q), where $E = E(\mathbb{Z}_N)$, $Q \in E(\mathbb{Z}_N)$ and $B = B(N)$ is suitably chosen parameter. In particular the classical Fermat factoring method has its "elliptic" version which can be adopted to "quantum annealing" method applied in [18]. Such approach is not the aim of the present work and is postponed to be investigated in another paper. Here we define the related notions of decomposition witnesses and prove the results concerning the factoring of N in time depending on the set of parameters X of the witnesses.

The notion of elliptic decomposition (factorization) witnesses (called in short witnesses) that we discuss below is new and relates to elliptic curve $E(\mathbb{Q})$ of Weierstrass equation with integer coefficients of the form $E := E_{\bar{b}} : y^2 = x^3 + b_1 x + b_2$, where $\bar{b} = (b_1, b_2) \in \mathbb{Z}^2$. In what follows we assume that N is coprime to 6, similarly as in section 2.1 [12] we define

$$\Delta_{\bar{b}} := 6(4b_1^3 + 27b_2^2) \tag{1}$$

and in order to have the elliptic curves $E(\mathbb{F}_p)$ and $E(\mathbb{F}_q)$ we assume that $\gcd(\Delta_{\bar{b}}, N) = 1$. Here and in the sequel we will use the abbreviation (Ell, N) for the unconditional approach and (Ell, E_N) for the conditional approach.

In the second approach we apply the elliptic curves and Fermat's factorization method, reducing decomposition $N = pq$ to the knowledge about E_N and the approximation of $\frac{p}{q}$ by $\frac{E_p}{E_q}$ or $\frac{p+1-E_p}{q+1-E_q} := \frac{a_p(E)}{a_q(E}$, respectively.

The deterministic time needed to decompose $N = pq$ depends on the witness $(u, v) = (b_1, b_2) \in \mathbb{Z}_N^2$ and a set of parameters $X = X_{u,v}$ of type $\{D\}, \{D, s, \alpha\}$ or $\{B, K\}$, where $1/D$ stands for the precision of approximation of p/q by the related quotient of Frobenius traces, $d \neq s \mid d^2\,, d \mid \gcd(E_p, E_q)$, α defines the precision of approximation of d/s by $1 + \frac{1}{D}$, while K measures the distance of E_r from the relevant $B-$factor of E_r.

In turn, the first approach is based on the largest $B-$smooth factor of E_r denoted by $s_B(E_r)$, and the lower bound for the reduced point $Q_{r'} \in E(\mathbb{F}_{r'})$, where $\{r, r'\} = \{p, q\}$. The related parameter $\beta \in [0, 1]$ indicates the lower bound for the related exponent of $B-$smooth factor of E_r, where $E = E_{\bar{b}}$ is the elliptic curve over $\mathbb{Z}_N$. On the other hand $\gamma \in [0, 1]$ points out the lower bound for $\mathrm{ord}Q_{r'}$ and occurs as an element of the set X of witness parameters, which is important in the investigation of the special case of witnesses called the nonseparating witnesses. On the other hand the separating witnesses are applied with the additional parameter $\sigma \in [1, 2]$ of E_r, which allows to improve the deterministic

time of decomposition $N = pq$ on the factor D^σ, compared to the conventional approach, when E is admissible curve.

The most characteristic example concerns the case $(\beta, \gamma) = (1, 1)$ and was applied in the seminal paper [12]. In the recent paper [4] the analysis concerned the more general case $(1, \gamma)$. Here we focus on the case when $\beta \in [0, 1], \gamma \in [0, 1]$ are arbitrary and prove the deterministic time of factoring N (depending on admissibility parameters B, β of E_r and set of parameters $X = X_{u,v}$ of the witness $(u, v) \in \mathbb{Z}_N^2$).

More accurately we analyze $(B, \beta, D, \Delta)-$admissible numbers E_r which are $(B, \beta)-$ smooth, $D-$smooth (where $D \geq B$) and such that the largest squarefree factor of $E_r/s_B(E_r)$ is $\leq \Delta$.

If $\Delta = \Delta(\beta, \sigma) = \min\left(D^{2-\sigma}, (r + 1 - \sqrt{r})^{1-\beta}\right)$, where $\sigma \in [0, 1]$ then we call such number $(B, \beta, D, \sigma)-$admissible. Clearly the bigger β is, the less space there is for the contribution of primes $q \in (B, D]$ (counting with multiplicity), while the number of prime divisors $q > B$ is (essentially) restricted by the parameter σ. On the other hand the bigger value of σ is, the better estimate of the deterministic time of factoring N, depending on the set X and parameters B, β satisfying the inequality $D^{2-\sigma} \leq (r + 1 - \sqrt{r})^{1-\beta}$. The witness parameters X play the significant role in deterministic factorization of N provided E_r is the admissible number.

We have made some numerical support to the extension of conjecture assumed in [12] for $B = L(\alpha_1, r)$, $D = L(\alpha_2, r)$, where $L(\alpha, r) := \exp\left(\alpha\sqrt{\log r \log\log r}\right)$ and suitable values of parameters β and σ below.

Summarizing, in this work we consider the witnesses $(u, v) \in \mathbb{Z}_N^2$ called $(\mathcal{A}, X)-$elliptic witness for N, where X is the set of parameters applied in the algorithm $\mathcal{A}$ if

- The algorithm has N, (u, v) and X as input and decomposition $N = pq$ depending on E_r or $a_r(E)$ for $r \in \{p, q\}$, as output
- The factorization $N = pq$ may be conditional meaning that $E_N = E_p E_q$ is known
- The complexity $t_{\mathcal{A}}$ of $\mathcal{A}$ depends on X and admissibility parameters of E_r or $a_r(E)$ for $r \in \{p, q\}$
- We consider two types of witnesses, namely $(u, v) = \bar{b}$ or $(u, v) = (x, y) := Q$, where $Q \in E_{\bar{b}}(\mathbb{Z}_N)$.

2 Separating and nonseparating witnesses in (Ell, N) factorization

2.1 Notation and basic facts concerning the arithmetic in $E(\mathbb{Z}_N)$

In this section we recall basic facts on elliptic curves over $\mathbb{Z}_N$, where $N = \prod_{i=1}^s p_i$ is coprime to 6 (see [11, 12]). The projective plane $\mathbb{P}^2(\mathbb{Z}_N)$ is defined to be the set of equivalence classes of primitive triples in $\mathbb{Z}_N^3$ (i.e., triples (x_1, x_2, x_3) with $\gcd(x_1, x_2, x_3, N) = 1$) with respect to the equivalence $(x_1, x_2, x_3) \sim (y_1, y_2, y_3)$ if $(x_1, x_2, x_3) = u(y_1, y_2, y_3)$ for a unit $u \in \mathbb{Z}_N^*$. An elliptic curve over $\mathbb{Z}_N$ is given

by the short Weierstrass equation $E : y^2z = x^3 + axz^2 + bz^3$, where $a, b \in \mathbb{Z}_N$ and the discriminant $-16(4a^3 + 27b^2) \in \mathbb{Z}_N^*$. The point $O = (0 : 1 : 0)$ called the zero point belongs to $E(\mathbb{Z}_N)$. Let $V(E(\mathbb{Z}_N)) = \{(x, y) \in E(\mathbb{Z}_N)\} \cup \{O\}$ be the set of finite points in $E(\mathbb{Z}_N)$ with the zero point O. For each point $(x : y : z) \in E(\mathbb{Z}_N) \setminus V(E(\mathbb{Z}_N))$ the $\gcd(z, N)$ is a nontrivial divisor of n.

Let $E(\mathbb{F}_{p_i})$ be the group of $\mathbb{F}_{p_i}$-rational points on the reduction $E \mod p_i$ for primes $p_i \mid N$. For the set $E(\mathbb{Z}_N)$ of points in $\mathbb{P}^2(\mathbb{Z}_N)$ satisfying the equation of E there exists by the CRT the bijection

$$\varphi : E(\mathbb{Z}_N) \to \prod_{i=1}^{s} E(\mathbb{F}_{p_i}) \tag{2}$$

induced by the reductions mod p_i The points $(x : y : z) \in E(\mathbb{Z}_N)$ with $z \in \mathbb{Z}_N^*$ can be written $(x/z : y/z : 1)$ and are called finite points. The set $E(\mathbb{Z}_N)$ is a group with the addition for which φ is a group isomorphism, which in general can be defined using the so-called complete set of addition laws on E (see [11]).

To add two finite points $P, Q \in E(\mathbb{Z}_N)$ we can also use the same formulas as for elliptic curves over fields in the following case: for $\varphi(P) = (P_1, \ldots, P_s)$ and $\varphi(Q) = (Q_1, \ldots, Q_s) \in \prod_i E(\mathbb{F}_{p_i})$ either $Q_i \neq \pm P_i$ for each i or $Q_i = P_i$ and $Q_i \neq -P_i$ for each i. Then

$$\begin{cases} x_{P+Q} = \lambda^2 - x_P - x_Q \\ y_{P+Q} = \lambda(x_P - x_{P+Q}) - y_P, \end{cases} \tag{3}$$

where

$$\lambda = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} & \text{if } Q_i \neq \pm P_i \text{ for each } i \\ \frac{3x_P^2 + a}{2y_P} & \text{if } Q_i = P_i \text{ and } Q_i \neq -P_i \text{ for each } i. \end{cases}$$

Let $P, Q \in E(\mathbb{Z}_N)$ and if $R = P + Q$ is finite then the formulas (3) give the coordinates of the resulted point R. Otherwise either we find the nontrivial divisor of N or prove that all local orders $\mathrm{ord}R_i$ are equal each other for $i = 1, 2, ..., s$ (see e.g. [12], [5] for details).

In what follows we assume that $N = pq$ has two distinct prime divisors (both > 3) and $B = B(N)$ is fixed. We apply the above formulas to compute the point $mQ \in E(E_N)$. The computation of finite point mQ takes $O(\log m)$ adding operations in $E(\mathbb{Z}_N)$. For $B-$smooth number $m = m_B$ represented as $m = p_k^{e_k} \ldots 3^{e_3} 2^{e_2}$, where $e_i = e_i(m)$ is the highest exponent in which p_i does not exceed $\min(p, q) + 2\sqrt{\min(p, q)} + 1$ the computation of $m_B Q$ takes

$$\ll \log N \sum_{i \leq k} \log(p_i) = O\left(B \log N\right) \tag{4}$$

adding operations in $E(\mathbb{Z}_N)$.

2.2 Admissible numbers and witnesses definitions

Here and in the sequel we will use the symbol $o(1)$ as p and q tend to infinity. We let

Definition 1. *The number $m \in \mathbb{N}$ is called $B-$ smooth if all prime factors of m are $\leq B$. Moreover it is called $(B,\beta)-$smooth if the largest $B-$smooth divisor of m denoted by $s_B(m)$ is $\geq m^{\beta}$. If additionally m is $D-$smooth then we call it $(B,\beta,D)-$smooth number.*

Let m^* stand for the largest squarefree divisor of m and κ be a real,positive number. Conventionally we denote by $\omega(m)$ the number of distinct prime divisors of m. Let $I_r^{\pm} := r+1\pm\sqrt{r}$. By $P^+(m)$ we denote the largest prime divisor of m.

Definition 2. *The number $m \in \mathbb{N}$ is called $(r,B,\beta,D,\sigma)-$admissible if it is $(B,\beta,D)-$smooth and the following conditions hold*

$$\beta \leq 1 - \frac{(2-\sigma)\log D}{\log I_r^-}, \tag{5}$$

$$\left(\frac{m}{s_B(m)}\right)^* \leq D^{2-\sigma}. \tag{6}$$

Directly from 6 it follows that

$$\omega\left(\frac{m}{s_B(m)}\right) \leq \kappa := (2-\sigma)\frac{\log D}{\log B}, \tag{7}$$

In what follows we assume that $\kappa \geq 2$, which implies that $B^2 \leq D^{2-\sigma}$. We call the related $(r,B,\beta,D,\sigma)-$admissible numbers shortly $(\beta,\sigma)-$admissible, if the remaining parameters are clear from the context.

Let $N(N=pq)$ be fixed and $E = E_{\bar{b}}$ be an elliptic curve over $\mathbb{Z}_N$. Then E is called $(B,\beta,D,\sigma)-$admissible if E_r is $(r,B,\beta,D,\sigma)-$admissible for some $r \in \{p,q\}$.

The value σ indicates an improvement in the exponent of the standard complexity bound $D^{2+o(1)}$, when searching the factors p and q of N provided E_r is $(r,B,\beta,D,\sigma)-$admissible number.

We prove the results concerning the factorization of N in deterministic time $t = t_{\mathcal{A}}$ depending on the set of parameters X of the witness. In unconditional case we distinct 2 types of witnesses (depending on X) corresponding to $D-$smooth number E_r:

- Separating witnesses $Q = (x,y) \in \mathbb{Z}_N^2$ such that $\mathrm{ord}Q_r \neq \mathrm{ord}Q_{r'}$, where $\{r,r'\} = \{p,q\}$.
- Nonseparating witnesses $Q = (x,y) \in \mathbb{Z}_N^2$ such that $\mathrm{ord}Q_r = \mathrm{ord}Q_{r'}$, where $\{r,r'\} = \{p,q\}$.

Let N and $E = E_{\bar{b}}$ over $\mathbb{Z}_N$ be given. Below we consider the pairs (E, Q), where $Q \in E(\mathbb{Z}_N)$, such that E is admissible curve and Q is suitable witness for N. The separating witnesses below are applied only for the value $\gamma = 1$ (hence the related restriction can be suppressed), but in order to keep the consistency of presentation we will maintain the following general definition.

In what follows we let $\vartheta > 1$.

Definition 3. *Let $N = pq$, $\vartheta > 1$, $p < q < \vartheta p$, $0 \leq \gamma \leq 1$, E be $(B, \beta, D, \sigma)-$admissible and $\{r, r'\} = \{p, q\}$. The pair $Q = (x, y)$ is called $(E, \gamma)-$strong separating witness for N if $Q \in E(\mathbb{Z}_N)$ and we have*

$$P^+(\mathrm{ord}Q_{r'}) \text{ does not divide } E_r \tag{8}$$

$$\mathrm{ord}Q_{r'} \geq 4\vartheta^{1/3} \min(r, r')/N^{\gamma/2}. \tag{9}$$

The first condition above was applied in [12], for the factorization of N in expected subexponential time, while the second in [4] in the context of oracle factoring (deterministic approach).

Definition 4. *Let $N = pq\, p < q$, $0 \leq \gamma \leq 1$, E be $(B, \beta, D, \sigma)-$admissible, and $\{r, r'\} = \{p, q\}$. The pair $Q = (x, y)$ is called $(E, \gamma)-$weak separating witness for N if $Q = (x, y) \in E(\mathbb{Z}_N)$ and we have*

$$\mathrm{ord}Q_{r'} \neq \mathrm{ord}Q_r \tag{10}$$

$$\mathrm{ord}Q_{r'} \geq 4\vartheta^{1/3} \min(r, r')/N^{\gamma/2}. \tag{11}$$

Given the admissible curve E and the suitable separating witness we discover the factorization $N = pq$ in deterministic time $O\left((B^2 + D^{2-\sigma})^{1+o(1)}\right)$, thus improving $t_{\mathcal{A}}$(for $(\beta, \sigma)-$admissible values of E_r) on the power D^{σ}.

In the following definition we restrict ourselves to the range $\gamma \in [0, 1/4)$ in view of the application to Theorem 2).

Definition 5. *Let $N = pq$, $p < q < \vartheta p$, $0 \leq \gamma < 1/4$ and E be $(B, \beta, D, \sigma)-$admissible and $\{r, r'\} = \{p, q\}$. The pair $Q = (x, y) \in E(\mathbb{Z}_N)$ is called $(E, \gamma)-$nonseparating witness for N if*

$$\mathrm{ord}Q_r = \mathrm{ord}Q_{r'} \geq 4\vartheta^{1/3} \min(r, r')/N^{\frac{\gamma}{2}} \tag{12}$$

and either

$$1 \leq \min(a_r(E), a_{r'}(E)) \leq \min(r, r')^{1/2-\gamma} \tag{13}$$

or

$$\gamma \leq 2(2 - \sigma)\frac{\log D}{\log N}. \tag{14}$$

In section 4 we state the main results regarding factorization $N = pq$ with the aid of nonseparating witness in deterministic time $O(D^{2-\sigma+o(1)})$.

3 Decomposition witnesses in (Ell, E_N) factorization

The classical Fermat's factoring method allows to efficiently factor the positive integer N provided $N = n_1 n_2$, where the absolute value of $n_1 - n_2$ is of order of magnitude $N^{1/4}$, since then we are able to find the related divisor close to $\sqrt{ab} = \sqrt{N}$. In the context of factoring N, the linear forms of type $ap + bq$ with integral coefficients a, b were considered in [9], and in [10] the factorization of N in deterministic time $O(N^{1/3+o(1)})$ was proved.

In this work we consider the special linear forms of type $F^{\pm} := F^{\pm}(a, b) = ap \pm bq$, where the coefficients a, b are related to the given elliptic curves $E(\mathbb{F}_q)$ and $E(\mathbb{F}_p)$ respectively. Namely we analyse the cases when a, b are either the Frobenius traces $a_q(E)$ and $a_p(E)$ or the values of E_q and E_p respectively. We search for the good approximation for F^+ by the geometric mean $\sqrt{abpq} = \sqrt{NE_N}$ in terms of $|F^-|$ also in the case when p and q are not of the similar order of magnitude. This leads to the definition of the relevant witnesses parameters $X \in \{D, (D, s, \alpha), (B, K)\}$, provided E_N is known.

In [6] the authors applied the Coppersmith factoring method [2] to prove that $N = pq$ can be factored in random polynomial time provided the factorization of E_N is known. The authors also proved that factoring can be derandomized provided the number of prime divisors of E_N is not too large. Here we follow another (conditional) approach which can be expressed in terms of the witnesses and their parameters X. Certainly they are also connected to non-separating witnesses since $\mathrm{ord}Q_r = \mathrm{ord}Q_{r'} \geq 4\vartheta^{1/3} \min(r, r')/N^{\gamma/2}$ implies that $d = \gcd(E_r, E_{r'}) \geq \gcd(\mathrm{ord}Q_r, \mathrm{ord}Q_{r'}) \geq 4\vartheta^{1/3} \min(r, r')/N^{\gamma/2}$ and moreover E_r has large $B-$smooth factor. But here we focus rather on the precision of approximating p/q by the related quotients of $a_q(E_q)$ and $a_p(E_p)$ respectively.

The somewhat more accurate Definition 7 below, refers to finding a "good" approximation of $(s/d)^2$ by $1 + 1/D$, which allows the time of decomposition $N = pq$ to be expressed in terms of two stages of appropriate approximations in Theorem 3. Finally the last definition below refers to the direct application of Coppersmith result (see Lemma 3).

Definition 6. *Let N and $M = M(N) \leq N^{1/2}$ be given. Let $D = D(N)$ and $q \in [Mp, 2Mp]$, where $pq = N$ and assume that the condition (1) holds true. The pair $\bar{b} \in \mathbb{Z}_N^2$ is called $D-$ factoring witness if*

$$\left| \frac{p}{q} - \frac{a_p(E_{\bar{b}})}{a_q(E_{\bar{b}})} \right| \leq \frac{1}{D} \tag{15}$$

for some $r \in \{p, q\}$ (if $a_p(E) = a_q(E) = 0$ then we set $0/0 := 0$).

Definition 7. *Let N, E_N and $d \mid \gcd(E_p, E_q) > 1$ be given. The pair $\bar{b} \in \mathbb{Z}_N^2$ is called $(D, s, \alpha)-$ factoring witness if the condition (1) holds true and $s \neq d$, $s \mid d^2$ satisfies the condition*

$$\left(\frac{d}{s}\right)^2 = 1 + \frac{1}{D} + \left(\frac{\alpha\theta}{D^2}\right), \tag{16}$$

for some $|\theta| \leq 1$.

Definition 8. *Let* N *be given,* $M = 1$ *and* $B = B(N), K = K(N)$. *The pair* $\bar{b} \in \mathbb{Z}_N^2$ *is called* $(B, K)-$ *factoring witness if the condition (1) holds true and* $s_B(E_r) > r/K$ *for some* $r \in \{p, q\}$, *where* $s_B(m)$ *denotes the largest* $B-$*smooth factor of* m.

4 Main results for (Ell, N) factorization

Below we state the results for separating ($\gamma = 1$) and nonseparating ($\gamma \in [0, 1/4)$) witnesses separately.

4.1 Separating witnesses

We proceed the main result (Theorem 1 below) by some definitions and auxiliary results. The separation witnesses for admissible elliptic curve E give the benefits in saving the factor D^σ in computational cost in comparison to the standard approach. The following lemma follows directly from Proposition 2.5 of [4].

Lemma 1. *Let* $Q \in E_{\bar{b}}(\mathbb{Z}_N)$ *be a finite point on the elliptic curve* $E_{\bar{b}}$ *over* $\mathbb{Z}_N$, *where* $\gcd(\Delta_{\bar{b}}, N) = 1$. *Assume that the reduction point* $Q_r \in E(\mathbb{F}_r)$ *has a* $B-$*smooth order* $\mathrm{ord}Q_r$ *for some* $r \in \{p, q\}$. *Then either one can discover the factorization* $N = pq$ *or compute* $\mathrm{ord}Q_r$ *and conclude that* $s_B(\mathrm{ord}Q_r) = \mathrm{ord}Q_r = \mathrm{ord}Q_{r'}$ *in deterministic time* $O(B^{2+o(1)})$.

Let $m^* = \prod_i q_i$, where $q_1 > q_2 > ..... > q_k$ are distinct prime numbers. We say that the sequence $(q_1, ..., q_k)$ belongs to the tuple $\bar{l} = (l_1, ..., l_k)$ if $q_i \in [2^{l_i}, 2^{l_i+1})$ for $i = 1, 2, ..., k$.

Definition 9. *The tuple* $\bar{l} = (l_1, l_2, ..., l_k)$ *is called* $\Delta-$*admissible if* $l_1 \geq l_2 \geq ... \geq l_k$ *and*

$$\sum_{i \leq k} l_i \leq \log \Delta / \log 2. \tag{17}$$

Definition 10. *Let* $\kappa = \kappa(\sigma, B, D) = (2 - \sigma)\frac{\log D}{\log B}$. *The number* m *is called* $(B, D, \sigma)-$*admissible if* $\omega\left(\frac{m}{s_B(m)}\right) \leq \kappa$.

The following lemma allows to reduce counting the sequences $(q_1, ..., q_k)$ with the coordinates depending only on the values of l_i, $i = 1, ..., k$, $(k \leq \lfloor \kappa \rfloor)$ of $\Delta-$admissible tuples $\bar{l}$.

Lemma 2. *The number of sequences* $(q_1, ..., q_k)$ *belonging to a fixed* $\Delta-$*admissible tuple* $\bar{l}$ *is* $\leq \Delta$. *Moreover the number of* $\Delta-$ *admissible tuples* $\bar{l} = (l_1, ..., l_k)$, *to which some sequence* $(q_1, ..., q_k)$ *may belong is equal to* $O\left((\log \Delta)^k\right)$, *where the constant implied by the symbol* O *does not depend on* Δ.

Proof. Each $q_1 q_1 \cdots q_k \le \Delta$ belongs to exactly one $\Delta-$admissible tuple $\bar{l}$. Since $q_i \in [2^{l_i}, 2^{l_i+1})$ the number of relevant sequences $(q_1, ..., q_k)$ belonging to a fixed tuple $\bar{l}$ is $\le 2^{l_1} \cdots 2^{l_k} \le \Delta$, by 17. Moreover the number of $\Delta-$admissible tuples $\bar{l}$ is bounded by the product of choices for l_i, where $0 \le l_i \le \log q_i / \log 2$, for $i = 1, 2, ..., k$, that is by $\le \prod_{i \le k} (\log q_i / \log 2 + 1) \le (\log \Delta / \log 2 + 1)^k = O\left((\log \Delta)^k\right)$, where the constant implied by the symbol O does not depend on Δ. This completes the proof of the Lemma 2.

We are now in a position to state and prove the first main result of this section.

Theorem 1. *Let $N\,(N = pq, p < q)$ be given, $\{r, r'\} = \{p, q\}$ and E be $(r, B, \beta, D, \sigma)-$ admissible curve, where $\omega(E_r/s_B(E_r)) \le (2-\sigma)\frac{\log D}{\log B}$.*

Let $\gamma = 1$ and the point $Q = (x, y) \in E(\mathbb{Z}_N)$ is $(E, \gamma)-$strong or $(E, \gamma)-$weak separating witness for N. Then one can find p and q in deterministic time $O\left((B^2 + D^{2-\sigma})^{1+o(1)}\right)$.

Proof. Let E be elliptic curve over $\mathbb{Z}_N$ which is $(B, \beta, D, \sigma)-$admissible. Assume that $\gamma = 1$ and the point $Q = (x, y) \in E(\mathbb{Z}_N)$ is $(E, \gamma)-$strong or $(E, \gamma)-$weak separating witness for N. We claim that one can find p and q in deterministic time $O\left((B^2 + D^{2-\sigma})^{1+o(1)}\right)$.

Assume that $\mathrm{ord}Q_r \ne \mathrm{ord}Q_{r'}$ and that $s_D/s_B = E_r/s_B(E_r) = \prod_{i \le k} q_i^{\nu_i}$. If $s_D/s_B = 1\,(k = 0)$ then E_r is $B-$smooth and the result follows from Lemma 1. Otherwise let $\Delta = D^{2-\sigma}$ and assume that for some $k \le \kappa$ the sequence$(q_1, ..., q_k)$ belongs to $\Delta-$admissible tuple $\bar{l} = (l_1, ..., l_k)$.

Let $q^\nu = q_1^\nu$ vary over all primes in the interval $[2^{l_1}, 2^{l_1+1})$ in exponent $0 \le \nu \le \log \Delta / \log q$. We compute the multiples $(q^\nu m_B)Q := q^\nu R_0 \in E(\mathbb{Z}_N)$, where $R_0 = m_B(Q)$ and m_B is the product of all primes $p \le B$ in maximal powers that are less than I_r^+.

If for some power q^ν the point $q^\nu R_0 \in E(\mathbb{Z}_N)$ is not finite then in view of Lemma 1 we will discover the decomposition $N = pq$ in $\ll D \log(q^\nu) \le D^{1+o(1)}$ adding operations in $E(\mathbb{Z}_N)$. Hence if $\omega(E_r/s_B(E_r)) \le 1$ we decompose N in deterministic time $\ll (B^2 + D)^{1+o(1)}$.

Otherwise we conclude that $\mathrm{ord}Q_r$ $(\mathrm{ord}Q_r \mid E_r)$ has at least two prime divisors $q_1 > q_2$, that is $\omega(E_r/s_B(E_r) \ge 2$. Now rising $q_2 \in [2^{l_2}, 2^{l_2+1})$ to maximal possible powers ν_2 we follow the computation of $q_2^{\nu_2} R_1$ similarly as above, where $R_1 = q_1^{\nu_1} m_B(Q)$ is a finite point in $E(\mathbb{Z}_N)$.

Since $\bar{l}$ is $\Delta-$admissible the number of possible choices for the pairs (q_1, q_2) with the related exponents (ν_1, ν_2) is in view of Lemma 2 bounded by $\Delta^{1+o(1)} = D^{2-\sigma+o(1)}$. We continue this procedure for all $k \le \kappa$ and by the assumption that $\mathrm{ord}Q_{r'} \ne \mathrm{ord}Q_r \mid E_r$ we infer that this procedure terminates after at most $\lfloor \kappa \rfloor$ steps, giving the deterministic total time $O\left((B^2 + D^{2-\sigma})^{1+o(1)}\right)$, as required.

4.2 Nonseparating witnesses

From now on we let $\vartheta > 1$ and $0 \le \gamma < 1/4$. In the proof of Theorem 2 we apply the the following

Lemma 3. *(Coppersmith) (see [2]) If we know N and the high order $(1/4)(\log_2 N)+O_\vartheta(1)$ bits of q, where $p<q<\vartheta p$, then in polynomial time in $\log N$ we can discover p and q.*

Corollary 1. *Assume that $p<q<\vartheta p$ and E_r is known. Then one can discover the decomposition $N=pq$ in deterministic polynomial time.*

Proof. Since $E_r \in [I_r^-, I_r^+]$ where $I_r^\pm = r+1\pm\sqrt{r}$ we deduce that E_r distincts from r at most on $\log_2 r + O(1) = \frac{1}{4}\log_2 N + O(1)$ least significant bits. Hence by Lemma 3 we get the conclusion.

The nonseparating witnesses allow to handle also the case when $0 \le \gamma < 1/4$. Moreover if $\gamma = O(\log\log N)/\log N)$ then the direct application of Coppersmith result gives the polynomial time factorization $N=pq$, provided we have $Q \in E(\mathbb{Z}_N)$ satisfying $\mathrm{ord}Q_r \ge \min(r,r')/N^{\gamma/2}$ for some $r \in \{p,q\}$ whenever E_r is $D-$smooth with $D=(\log N)^{O(1)}$.

Theorem 2. *Let N $(N=pq,\ p<q<\vartheta p)$ be given, $\gamma<1/4$, $\{r,r'\}=\{p,q\}$ and E be $(B,\beta,D,\sigma)-$ admissible curve $(E_r \in I_r, E_{r'} \in I_{r'})$.*

Assume that the point $Q=(x,y)\in E(\mathbb{Z}_N)$ is $(E,\gamma)-$nonseparating witness for N and satisfy the conditions (12) and (13). Then one can find p and q in deterministic polynomial time.

On the other hand if (12) and (14) hold true, then one can compute the decomposition of $N=pq$ in deterministic time $O(D^{2-\sigma+o(1)})$, provided

$$\gamma \le \min\left(2(2-\sigma)\frac{\log D}{\log N},\ \frac{1}{4}\right).$$

Moreover if E_r is $D-$smooth where $D=(\log N)^{O(1)}$ and we have the point $Q\in E(\mathbb{Z}_N)$ such that $\mathrm{ord}Q_r \ge c(\vartheta)\min(r,r')/N^{\gamma/2}$ for some $r\in\{p,q\}$ and $\gamma = O(\log\log N/\log N)$, then the decomposition $N=pq$ can be computed in polynomial time.

Proof. In order to prove the Theorem 2 we first show that if we are given $Q\in E(\mathbb{Z}_N)$ that is (E,γ) nonseparating witness, $(0\le\gamma<1/4)$ that is the conditions 12 and 13 hold true, then we can decompose $N=pq\,(p<q)$ in deterministic polynomial time. Next we show that if the conditions 12 and 14 hold true then we can decompose $N=pq$ in deterministic time $O(D^{2-\sigma+o(1)})$.

To prove the first assertion we apply the assumption that

$$1 \le \min(a_p(E), a_q(E)) \le 2p^{1/2-\gamma}$$

and the condition

$$m := \mathrm{ord}Q_p = \mathrm{ord}Q_q \ge c(\vartheta)\frac{\min(q,p)}{N^{\gamma/2}} = c(\vartheta)p/N^{\gamma/2},$$

where $c(\vartheta) > 4\vartheta^{5/4}$. Moreover by the assumption $\gamma<1/4$ we have that $m > N^{3/8} > N^{1/3}$ for sufficiently large $N\ge N_0 = N_0(\vartheta,\gamma)$. Therefore we can represent the number N in base m,

$$N = c_0 + c_1 m + c_2 m^2.$$

Since $E_p = p + 1 - a_p(E) = mr_p$ and $E_q = q + 1 - a_q(E) = mr_q$, letting $t_p = a_p(E) - 1$ and $t_q = a_q(E) - 1$ we have

$$N = pq = (mr_p + a_p(E) - 1)(mr_q + a_q(E) - 1) = (mr_p + t_p)(mr_q + t_q)$$

$$= r_p r_q m^2 + (r_p t_q + r_q t_p)m + t_p t_q$$

where $t_p, t_q \geq 0$. Thus the coefficients $r_p r_q$, $r_p + r_q$, and $t_p t_q$ are uniquely defined by c_i, $i = 0, 1, 2$ provided all they are in the interval $[0, m)$.

Since all they are nonnegative it remains to check that they are $< m$. We have that $r_p r_q = (E_p E_q)/m^2 \leq N/m^2 < m$, since $m > N^{1/3}$ for sufficiently large $N = N(\vartheta)$ by the above. Moreover we have $r_p t_q + r_q t_p \leq 2\max(\sqrt{p}, \sqrt{q})(E_p + E_q)/m = 4\sqrt{q}(q/m) \leq 4q^{3/2}/m \leq 4\vartheta^{3/2}(N^{1/2})^{3/2}/m < m$, since $N^{3/4} < m^2/4\vartheta^{3/2}$ if $\gamma < 1/4$ and N is sufficiently large.

Finally we have $t_p t_q \leq 2(p^{(1/2)-\gamma})(2q^{1/2}) \leq 4N^{1/2}/p^{\gamma} \leq 4N^{1/2}/(q/\vartheta)^{\gamma}) \leq 4\vartheta^{1/4}N^{1/2-\gamma/2} < m$, since $m \geq 4\vartheta^{5/4}p/N^{\gamma/2}$

To complete the argument it remains to remark that $c_1 = r_p + r_q = c_0 u^{-1} + c_2 u$, where $u = \frac{t_p}{r_p} \in \mathbb{Q}$ is assumed to be in the reduced form. Now we have that $N = pq = (mr_p + t_p)(mr_q + t_q)$ and both factors are ≥ 2. Hence we discover p by computing $\gcd(N, mr_p + t_p)$. This implies the required factorization $N = pq$ in the case when the condition 13 holds.

On the other hand the condition 14 implies that E_r for any $r \mid N$, differ from $m = \mathrm{ord}Q_r$ at most on the factor $\ll N^{\gamma/2}$ which is $\leq D^{2-\sigma}$ by the assumption.

Therefore we are in a position to apply Lemma 3. Since for any $r \in \{p, q\}$, $E_r \in I_r$ differs from r on at most $\log_2 r^{1/2} \leq \log N^{1/4}$ least significant bits, the application of Lemma 3 to detect the factor $r \mid N$ in deterministic polylog(N) time, which implies that the total deterministic time in this case is $O(D^{2-\sigma+o(1)})$, as required. If $D = \log N)^{O(1)}$, the conclusion follows immediately from Corollary 1. This completes the proof of Theorem 2.

5 Separating witnesses for subexponential B and D

Here we investigate the distribution of random elliptic curves $E = E_{\bar{b}}$ that are $(B, \beta, D, \sigma)-$admissible, where $B = L(\alpha_1, r)$ and $D = L(\alpha_2, r)$, where $\alpha_1 < \alpha_0 < \alpha_2$ and $\alpha_0 = 1/\sqrt{2}$. By [12] the expected fraction of triples $(x, y, b_1) \in \mathbb{Z}_N^3$ such that $E_r \in I_r$ is $B-$ smooth number for some $r \in \{p, q\}$ is equal to $1/L_B$, where

$$L_B = L\left(\frac{1}{2\alpha_1} + o(1),\, r\right).$$

Then the expected time of finding the separating witness is $L(\alpha_1 + o(1), r)$ giving the optimal choice of α_1 satisfying the equality $\frac{1}{2\alpha_1} = \alpha_0 = 1/\sqrt{2}$. The expected time of factoring N is then equal to

$$L(2\alpha_0 + o(1), r) = \exp\left(\sqrt{(2 + o(1))\log r \log\log r}\right).$$

The analogous question for $(B,\beta,D,\sigma)-$admissible numbers E_r is more delicate, since we have to enter the additional parameters $\beta, D = L(\alpha_2, r)$ and σ satisfying the the following inequality

$$\omega(E_r/s_B(E_r)) \leq \kappa := (2-\sigma)\,\frac{\log D}{\log B}, \tag{18}$$

giving the deterministic time $\ll (B^2 + D^{2-\sigma})^{1+o(1)} \ll D^{2-\sigma+o(1)}$.

If $\omega(E_r/s_B(E_r)) \leq 1$ then the decomposition $N = pq$ is by Lemma 2 discovered in deterministic time $O\left((B^2+D)^{1+o(1)}\right)$. The contribution of all $(B,\beta,D,\sigma)-$admissible numbers $E_r \in I_r$ comes from the numbers of type $s_B(E_r)\prod_{i\leq\lfloor\kappa\rfloor} q_i^{\nu_i}$, where $\prod_{i\leq\lfloor\kappa\rfloor} q_i^{\nu_i} \leq D^{2-\sigma}$ and $\lfloor\kappa\rfloor$ denotes the integer part of κ.

Bearing in mind [8] (Theorem 5.2) we state the analogous conjecture as in [12] called $\beta-$conjecture for $(B,\beta,D,\sigma)-$admissible numbers. Namely consider the admissible triples $T = (x, y, b_1) \in \mathbb{Z}_N^3$ such that $E_r \in I_r$.

Namely let

$$f_\beta(B,D,\sigma) = \frac{\#\{T \in \mathbb{Z}_N^3 : E_r \in I_r : E_r \text{ is } (r,B,\beta,D,\sigma) - \text{ admissible}\}}{\#\{T \in \mathbb{Z}_N^3 : E_r \in I_r\}} \tag{19}$$

$\beta-$Conjecture:

Let $0 < \beta < 1$. Let $B = L(\alpha_1, r) \leq L(\alpha_0, r) \leq D = L(\alpha_2, r)$. Selecting randomly the triples $(x, y, b_1) \in \mathbb{Z}_N^3$ with $E_r \in I_r$ we conjecture that

$$f_\beta(B,D,\sigma) = 1/L\left(\frac{1-\theta(1-\beta)}{2\alpha_1} + o(1),\, r\right), \tag{20}$$

where $\theta = \theta(\alpha_1, \alpha_2, \sigma) > 0$.

5.1 Computational support

β-Conjecture. Assume that $\alpha_1 = \alpha_0 - \delta$ and $\alpha_2 = \alpha_0 + \delta$. Let us illustrate the β-Conjecture through computational support by examining $f_\beta(B,D,\sigma)$ - the density levels of (B,β,D,σ)-admissible numbers. Experiments returning the value of f_β are conducted as procedures $\texttt{Exp}(\lambda, c, \delta, \beta, \sigma)$, where λ denotes the bit length of the numbers p, q, and c determines the accuracy of the search, that is,

$$\#\{\mathbb{Z}_N^3 \xrightarrow{\$} (x, y, b_1)\} \geq L(c, r).$$

The `Exp` procedure returns $f_\beta(B,D,\sigma)$ - the ratio of the counts of orders from these two categories, according to the formula (19).

The ranges of the remaining parameters define relationships from the definition 2 of admissible number. More precisely, these ranges are determined from the inequality (5): and from the inequality (7):

$$\omega\left(\frac{E_r}{s_B(E_r)}\right) \leq (2-\sigma)\frac{\log D}{\log B} = (2-\sigma)\frac{\alpha_2}{\alpha_1},$$

because inequality (6) can be replaced by the last one. The value of $\omega\left(\frac{E_r}{s_B(E_r)}\right)$ we fixed at 3, to control ranges of dependent parameters. Let the selection of parameters, fully consistent with these dependencies, be as follows:

$$\lambda = 30, c = 1.1, \sigma = 0.45, \delta = 0.35,$$
$$\beta \in \{0.24, 0.27, 0.30, 0.33, 0.36, 0.39, 0.42, 0.45, 0.48\} = \bar{\beta}.$$

This entails repeating the experiment $\texttt{Exp}(30, 1.1, 0.35, \beta_i, 0.45)$ for all $\beta_i \in \bar{\beta}$.

To illustrate the computational support for the $(\beta, \sigma)-$conjecture, in this case, we want to show that there exists a constant value $\theta(\alpha_1, \alpha_2, \sigma)$ for which the density function $f_\beta(B, D, \sigma)$ behaves in accordance with the predictions presented in equality (20), with accuracy to the error indicated there, asymptotically equal to $o(1)$.

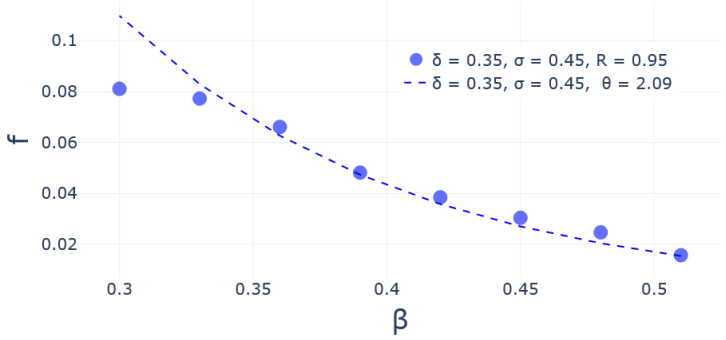

Fig. 1. The graph shows experimentally obtained densities $f_\beta(B, D, \sigma)$, with fixed $\sigma = 0.45, \delta = 0.35$ for the bit length p, q equal to 30 bits. For $\theta \approx 2.09$, the consistency coefficient R of the sample approximated by the function of θ was equal to 0.95 .

In the Fig 1, we observe that there is no dependency of the parameter θ on the parameter β, which is consistent with the $\beta-$conjecture. The key conclusion from the numerical example is that the behavior of the function $f_\beta(B, D, \sigma)$ is well approximated by the constant value θ, resulting from the fact that θ does not depend on other parameters than $\alpha_1, \alpha_2, \sigma$. This means that the form of the function, presented in equation (20), is consistent with the experimentally obtained results. Furthermore, the optimal value of $\theta \approx 2.09$, meaning that the examined densities of (B, β, D, σ)-admissible orders E_r exceed the B-smooth densities from these ranges.

We conclude that the experimental searches conducted align with the proposed hypothesis.

6 Main result for (Ell, E_N) factorization

We recall that $a_p = a_p(E), a_q = a_q(E)$ are the related Frobenius traces modulo p and q respectively. By by $\omega(m), (\Omega(m))$ we denote the number of distinct (all) prime divisors of m, respectively.

In what follows we use the convention that polylog(N) means the time bounded by some power (which can be explicitly given) of $\log N$, as N tends to infinity.

The proof of Theorem 3 below is based on two lemmas. The first, is commonly known starting point in the Fermat factoring method and will be applied in the proof of (i) of Theorem 3.

Lemma 4. *Let $X \leq Y$ be real positive numbers and XY be given. Then $X+Y$ can be approximated from below by $2\sqrt{XY}$ with precision $\geq \frac{(X-Y)^2}{4\sqrt{XY}}$.*

The second is directly applied in the proof of (ii) of Theorem 3.

Lemma 5. *Let $N = pq$, where $p < q < \vartheta p$, $1 < a_q := q + 1 - E_q$, $1 < d \mid \gcd(E_p, E_q)$. Assume that N, E_N and $d \neq s \mid d^2$ are known and for some $c = c(\vartheta) > 0$ the following condition holds*

$$\left| \frac{p}{q} - \frac{E_p}{E_q} \left(\frac{d}{s} \right)^2 \right| < \frac{c}{D^2} \tag{21}$$

Then p and q can be computed in deterministic time (polylog$N$)$(D^{-4}NM^2)$.

Proof. Let $E_p = dE'_p$, $E_q = dE'_q$, $d^2 = rs$ and set $X = pE'_q s$, $Y = qE'_p r$. Then $XY = N\frac{E_N}{d^2}sr = NE_N$. One can solve the system of equations

$$XY = NE_N$$
$$X + Y = A$$

in deterministic polylog(N) time. Then by the assumption $a_q > 1$ we deduce that $p \mid \gcd(X, NE_N)$ but the condition $q \mid X$ would imply that $q \mid E_q^2 = (q + 1 - a_q)^2$, which gives the contradiction. Hence $\gcd(X, NE_N) = p$ gives the required decomposition $N = pq$. Now we are in a position to apply Lemma 4 to evaluate the time of search for $X+Y$ in the interval $\left[2\sqrt{NE_N},\ 2\sqrt{NE_N} + \frac{(X-Y)^2}{4\sqrt{XY}}\right]$. Since

$$|X - Y| = |pE'_q s - qE'_p r| = \frac{s}{d}\left|pE_q - qE_p\left(\frac{r}{s}\right)\right| = \frac{r}{d}(qE_q)\left|\frac{p}{q} - \frac{E_p}{E_q}\left(\frac{d}{s}\right)^2\right|$$

we obtain by (21) that the total time satisfies the bound

$$t \ll polylogN \frac{(X-Y)^2}{4\sqrt{XY}} \ll polylogN \frac{(qE_q)^2}{\sqrt{NE_N}D^4}$$
$$\ll polylogN \frac{(\sqrt{NM})^4}{ND^4} \ll polylogN \frac{NM^2}{D^4},$$

which completes the proof of Lemma 5.

Now we are in a position to state and prove the main result of this section.

Theorem 3. *Let N and E_N be given, where $N = pq$, $q \in [Mp, 2Mp]$. Then we have*

(i) Assume that $D = D(N)$ and $\bar{b} \in \mathbb{Z}_N^2$ is $D-$factoring witness. Then we can factor N in deterministic time

$$t = t(N, M, D, a_p, a_q) = (polylogN)\left(M\left(1 + \left(\frac{|a_p| + |a_q|}{D}\right)^2\right)\right). \quad (22)$$

Unconditionally we have $t = (polylogN)M$, provided $D > (MN)^{1/4}$.

(ii) Let $N = pq$, $p < q < \vartheta p$, $d \mid \gcd(E_p, E_q)$ and $d \neq s \mid d^2$ be given. Assume that $\bar{b} \in \mathbb{Z}_N^2$ is $(D, s, \alpha)-$ factoring witness. Let $\beta = \beta(\alpha)$ be a positive constant such that

$$\frac{p}{q} - \frac{E_p}{E_q} = \frac{p}{q}\left(\frac{1}{D} + \frac{\beta\theta}{D^2}\right) \quad (23)$$

for some $|\theta| \leq 1$. Then we can detect p, q in deterministic time $O\left(polylogN\frac{NM^2}{D^4}\right)$, where the constant implied by the symbol O depends on α, β and ϑ. Hence $t = polylogN$, provided $D > N^{1/4}M^{1/2}$ (which is stronger than the bound for t in (i) if $M = M(N)$ and $D = D(N)$ are suitably large).

(iii) $N = pq$, $p < q < \vartheta p$. Assume that $d \mid \gcd(E_p, E_q)$ be such that $N^{1/2}/d < (\log N)^{O(1)}$. Then one can factor N in deterministic polynomial time (depending on ϑ).

Proof. CASE(i). Assume that for some $D \geq 1/2$, the pair $\bar{b} \in \mathbb{Z}_N^2$ is $D-$ factoring witness. We require that N can be factored in deterministic time

$$t = t(N, M, D, a_p, a_q) = polylog(N)M\left(1 + \left(\frac{|a_p| + |a_q|}{D}\right)^2\right) \quad (24)$$

For the proof we apply Lemma 4 with $X = pE_q$ and $Y = qE_p$ and $F^{\pm} := F^{\pm}(E_p, E_q) := pE_q \pm qE_p$. The deterministic time to find X and Y is by Lemma 21 bounded by $polylogN\frac{(X-Y)^2}{4\sqrt{XY}}$, the first factor coming from the cost of solving the related system of equations in X and Y. For the second factor we have by the definition of the definition of $D-$factoring witness the following bound (having in view that $q \ll \sqrt{NM}$).

$$(pE_q - qE_p)^2/4\sqrt{XY} \ll (|p-q|^2/\sqrt{NE_N} + |pa_q - qa_p|^2)/\sqrt{NE_N}$$

$$\ll \frac{NM}{N} + \left(\frac{1}{D}(q\max(|a_p|, |a_q|)\right)^2 \times \frac{1}{N} \ll M + (NM)\frac{|a_p|^2 + |a_q|^2}{D^2N},$$

as required. The unconditional polynomial bound for t follows from the Hasse bound $|a_q| \leq 2\sqrt{q} \ll (MN)^{1/4}$.

CASE (ii). Let $d \mid \gcd(E_p, E_q)$ and $s \mid d^2$, $s \neq d$ such that $\bar{b} \in \mathbb{Z}_N^2$ is $(D, s, \alpha)-$ factoring witness, be given and the condition (23) holds true.

Then we have

$$\frac{p}{q}-\frac{E_p}{E_q}\frac{s}{r}=\frac{E_p}{E_q}+\frac{p}{q}\left(\frac{1}{D}+\left(\frac{\beta\theta_2}{D^2}\right)\right)-\frac{E_p}{E_q}\frac{s}{r}=\frac{E_p}{E_q}+\frac{p}{q}\left(\frac{1}{D}+\left(\frac{\beta\theta_2}{D^2}\right)\right)-\frac{E_p}{E_q}\left(\frac{d}{r}\right)^2=$$

$$\frac{E_p}{E_q}+\frac{p}{q}\left(\frac{1}{D}+\left(\frac{\beta\theta_2}{D^2}\right)\right)-\frac{E_p}{E_q}\left(\frac{d}{r}\right)^2=\frac{p}{q}\left(\frac{1}{D}+\frac{\beta\theta_2}{D^2}\right)-\frac{E_p}{E_q}\left(\frac{1}{D}+\frac{\alpha\theta_1}{D^2}\right)$$

$$=\frac{1}{D}\left(\frac{p}{q}-\frac{E_p}{E_q}\right)+\left(\frac{c\theta}{D^2}\right)\leq\frac{2}{D^2}+\frac{\beta\theta_2}{D^2}+\frac{c\theta}{D^2}\leq\frac{c'}{D^2},$$

for some $c'=c'(\alpha,\beta)$. Now the result follows by Lemma 5 (with c=c').

CASE (iii) By the assumption $d \leq N/(\log N)^{O(1)}$. Hence for any $r \in \{p, q\}$ we have

$$N^{1/2}/(\log N)^{O(1)} < d \leq E_r \leq r + 1 - a_r(E) = r + O(\sqrt{N})$$

Writting $E_r = dk$, we check all possible $k \leq K = (\log N)^{O(1)}$ to find the suitable E_r and the result follows by applying Corollary 1.

References

1. Burthe Jr., R. J.: The average least witness is 2. Acta Arith. **80** (1997) 327-341.
2. Coppersmith, D.: Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known. In: EUROCRYPT 1996: Advances in Cryptology — EUROCRYPT '96 pp 178–189. LNCS 1070. Springer, Berlin (1996).
3. Dąbrowski, A., Pomykała, J., Shparlinski, I.: On oracle factoring of integers. Journal of Complexity, (76) Issue CJun 2023.
4. Dryło, R., Pomykała, J.: Smooth factors of integers and elliptic curve based factoring with an oracle. Banach Center Publications (126), Number Theoretic methods in Cryptology, M. Grześkowiak, J. Pieprzyk, J. Pomykała eds. p. 73-88.
5. Dryło, R., Pomykała, J.: Integer factoring problem and elliptic curves over the ring Z_n. Colloquium Mathematicum, **159** (2020), 259-284.
6. Dieulefait, L. V., Jimenez Urroz, J.: Factorization and Malleability of RSA Moduli, and Counting Points on Elliptic Curves Modulo N. Mathematics 2020, 8(12), 2126; [https://doi.org/10.3390/math8122126].
7. Hittmeir, M., Pomykała, J.: Deterministic Integer Factorization with Oracles for Euler's Totient Function. Fundamenta Informaticae, 172(1) 2020, 39-51.
8. Konyagin, S., Pomerance, C.: On primes recognizable in deterministic polynomial time. In: Graham, R. L. (ed.) The mathematics of Paul Erdös. Vol. I. Berlin: Springer. Algorithms Comb. 13, 176-198 (1997).
9. Lawrence, F. W.: Factorisation of numbers. Messenger of Math, 24:100–109, 1895.
10. Lehman, R. S.: Factoring Large Integers. Math. Comp., **28**(126): 637–646, 1974.
11. Lenstra, H. W.: Elliptic curves and number-theoretic algorithms. Proc. Intern. Congress of Math., Berkeley, 1986, Amer. Math. Soc., Providence, 99–120.
12. Lenstra, H. W.: Factoring integers with elliptic curves. Ann. of Math. **126** (1987), 649-673.

13. Pollard, J. M.: Theorems on factorization and primality testing. Mathematical Proceedings of the Cambridge Philosophical Society, 76 (3), (1974), 521-528.
14. Pomykała, J., Radziejewski, M.: Integer factoring and compositeness witnesses. J. Math. Cryptol. 2020; 14, 346-358.
15. Rivest, R., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM. 21 (2): 120–126 (1978).
16. Williams, H. C.: A p+1 method of factoring. Mathematics of Computation, 39 (159), (1982), 225-234.
17. Źrałek, B.: A deterministic version of Pollard's p–1 algorithm. Math. Comp., 2010;79(269):513–533.
18. Żołnierczyk, O., Wroński, M. (2023). Searching B-Smooth Numbers Using Quantum Annealing: Applications to Factorization and Discrete Logarithm Problem. In: Mikyška, J., de Mulatier, C., Paszynski, M., Krzhizhanovskaya, V.V., Dongarra, J.J., Sloot, P.M. (eds) Computational Science – ICCS 2023. ICCS 2023. Lecture Notes in Computer Science, vol 10477. Springer, Cham.