Further Results on Implicit Factoring in Polynomial Time

Santanu Sarkar and Subhamoy Maitra

Indian Statistical Institute, 203 B T Road, Kolkata 700 108, India
{santanu_r, subho}@isical.ac.in

Abstract. In a very recent work, May and Ritzenhofen presented some interesting problems related to factoring large integers with some implicit hints and one of the problems is as follows. Consider $N_1 = p_1q_1$ and $N_2 = p_2q_2$, where p_1, p_2, q_1, q_2 are large primes. The primes p_1, p_2 are of same bit-size with the constraint that certain amount of Least Significant Bits (LSBs) of p_1, p_2 are same. Further the primes q_1, q_2 are of same bit-size without any constraint. May and Ritzenhofen proposed a strategy to factorize both N_1, N_2 in poly$(\log N)$ time (N is an integer with same bit-size as N_1, N_2) with the implicit information that p_1, p_2 share certain amount of LSBs. We look at the same problem with a different lattice-based strategy and our method works when implicit information is available related to either Most Significant Bits (MSBs) or LSBs. Given $q_1, q_2 \approx N^\alpha$, we show that one can factor N_1, N_2 simultaneously in poly$(\log N)$ time (under some assumption related to Gröbner Basis) when p_1, p_2 share $(1 - \alpha - \beta) \log_2 N$ many LSBs or MSBs, where $-4\alpha^2 - 2\alpha\beta - \frac{1}{4}\beta^2 + 4\alpha + \frac{5}{3}\beta - 1 < 0$ provided $1 - \frac{3}{2}\beta - 2\alpha \geq 0$. The MSB case has not been studied earlier, which we consider in this paper and find encouraging results. The work of May and Ritzenhofen studied the LSB case, where we always find better results in experiments; our theoretical formula also provide improved results in certain range.

Keywords: Implicit Information, Prime Factorization.

1 Introduction

Very recently, in [9], a new direction towards factorization with implicit information has been introduced. Consider two integers N_1, N_2 such that $N_1 = p_1q_1$ and $N_2 = p_2q_2$ where p_1, q_1, p_2, q_2 are primes and p_1, p_2 share t least significant bits (LSBs). It has been shown in [9] that when q_1, q_2 are primes of bit-size α, then N_1, N_2 can be factored simultaneously if $t \geq 2(\alpha+1)$. This bound on t has further been improved when $N_1 = p_1q_1, N_2 = p_2q_2, \ldots, N_k = p_kq_k$ and all the p_i's share t many LSBs. The motivation of this problem comes from oracle based complexity of factorization problems. Prior to the work of [9], the main assumption in this direction was that an oracle explicitly outputs certain amount of bits of one prime. The idea of [9] deviates from that idea in the direction that none of the bits of the prime will be known, but some implicit information can be available regarding the prime. That is, an oracle, on input to N_1, outputs a different N_2 as described above. A nice motivation towards the importance of this problem is presented in the introduction of [9].

Factoring of large integers is one of the most challenging problems in Mathematics and Computer Science. The quadratic Sieve [11], the elliptic curve method [5] and number field sieve [6] are among the significant works on classical computing model. Till date, there is no known polynomial time factorization algorithm on this model, though in a seminal work Shor [13] has presented a polynomial time algorithm for factorization on quantum computing

platforms. Towards the partial results for efficient factorization in classical domain (factoring with explicit information from an oracle according to [9]), Rivest and Shamir [12] showed that N (where $N = pq$) can be factored efficiently when $\frac{3}{5}\log_2 p$ many MSBs of p are known. Later, Coppersmith [2] improved this bound, where $\frac{1}{2}\log_2 p$ many MSBs of p need to be known for efficient factorization.

In this paper we assume the equality of either the MSBs or the LSBs, i.e., we consider that p_1, p_2 share either t many MSBs or t many LSBs. Our approach in solving the problem is different from that of [9].

We like to point out that the event of getting two primes with a many LSBs equal is approximately as frequent as getting two primes with a many MSBs equal. This can be noted as follows. Let i be an a bit integer. Consider two sets A and B where

$$A = \{p : p \text{ is a prime of } a+b \text{ bits and } a \text{ many MSBs of } p \text{ is } i\},$$

$$B = \{p : p \text{ is a prime of } a+b \text{ bits and } a \text{ many LSBs of } p \text{ is } i\}.$$

We first calculate cardinality of A. Let $X = 2^b i$. Then from prime number theorem [1, Page 65] $|A| \approx \frac{X+2^b-1}{\log(X+2^b-1)} - \frac{X}{\log X} \approx \frac{2^b}{\log X}$ (assume $b < a$) $\approx \frac{2^b}{\log 2^{a+b}}$, which is $O(2^b)$. Also, we have $B = \{p : p \text{ is a prime of } a+b \text{ bits and } p \equiv i (\mathrm{mod} 2^a)\}$. From Dirichlet's theorem related to prime numbers [1, Page 154], we have $|B| \approx (\frac{2^{a+b}-1}{\log(2^{a+b}-1)} - \frac{2^{a+b-1}-1}{\log(2^{a+b-1}-1)})\frac{1}{\phi(2^a)} \approx \frac{2^{a+b-1}}{\log 2^{a+b}}\frac{1}{2^{a-1}}$, which is again $O(2^b)$. Thus, $|A|$ and $|B|$ are of the same order.

In the next section we present our ideas. The technique is based on lattice reduction. For detailed notion on the technique we use, the readers are referred to [10, 4].

2 Implicit Factoring of Two Large Integers

Here we present the exact conditions on p_1, q_1, p_2, q_2 under which N_1, N_2 can be factored efficiently. For this we first need the following discussion.

Suppose we have a set of polynomials $\{f_1, f_2, \ldots, f_l\}$ on three variables having same root $(x_{1,0}, x_{2,0}, \ldots, x_{n,0})$. Then a Gröbner Basis $\{g_1, g_2, \ldots, g_t\}$ is a set of polynomials that preserve the set of common roots of $\{f_1, f_2, \ldots, f_l\}$. In this case, $g_1, g_2, \ldots, g_t$ can be computed with respect to some ordering such that the roots can be collected eliminating the variables. Though this is true in practice, theoretically this may not always happen. For this to be always true, one needs the following assumption. This kind of assumption has already been used in [4, Section 6].

Assumption 1. Let J be the ideal generated by $\{f_1, f_2, \ldots, f_l\}$. We consider that the variety $V(J)$ of the ideal J is zero-dimensional.

Throughout this paper, we will consider p_1, p_2 are primes of same bit size and q_1, q_2 are primes of same bit size. Thus $N_1 = p_1 q_1$ and $N_2 = p_2 q_2$ are also of same bit size. We use N to represent an integer of same bit size as of N_1, N_2.

2.1 The MSB Case

The study when p_1, p_2 share some MSBs has not been considered in [9], which we present in this section. The following theorem states our main technical result.

Theorem 1. *Let $N_1 = p_1q_1$ and $N_2 = p_2q_2$, where p_1, q_1, p_2, q_2 are primes. Let $Q_1, Q_2 \approx N^\alpha$, and $|P_1 - P_2| < N^\beta$. Under Assumption 1, one can factor N_1, N_2 in polynomial time if $-4\alpha^2 - 2\alpha\beta - \frac{1}{4}\beta^2 + 4\alpha + \frac{5}{3}\beta - 1 < 0$ provided $1 - \frac{3}{2}\beta - 2\alpha \geq 0$.*

Proof. Here p_1, p_2 share certain amount of MSBs and we write $p_1 = p + P_1$ and $p_2 = p + P_2$, where the LSBs of p are zero. Thus, $N_1 = (p + P_1)q_1$ and $N_2 = (p + P_2)q_2$. Eliminating p, we get $q_2q_1(P_2 - P_1) + N_1q_2 - N_2q_1 = 0$. Thus we need to solve $f'(x, y, z) = xyz + N_1x - N_2y = 0$ whose roots corresponding to x, y, z are $q_2, q_1, p_2 - p_1$. Since there is no constant term in f', we define a new polynomial $f(x, y, z) = f'(x-1, y, z) = xyz - yz + N_1x - N_1 - N_2y$. The root (x_0, y_0, z_0) of f is $(q_2 + 1, q_1, p_2 - p_1)$. The idea of modifying the polynomial with a constant term was introduced in [3, Appendix A] and later used in [4] which we follow here.

Let X, Y, Z be the upper bounds of q_2+1, q_1, p_2-p_1 respectively. As given in the statement of this theorem, $X = N^\alpha, Y = N^\alpha, Z = N^\beta$. Following the "Extended Strategy" of [4, Page 274],

$$S = \bigcup_{0 \leq j \leq t} \{x^i y^j z^{k+j} : x^i y^j z^k \text{ is a monomial of } f^m\},$$

$$M = \{ \text{ monomials of } x^i y^j z^k f : x^i y^j z^k \in S\}.$$

We exploit t many extra shifts of z where t is a non-negative integer. Our aim is to find two more polynomials f_0, f_1 that share the root $(q_2 + 1, q_1, p_2 - p_1)$ over the integers.

From [4], we know that these polynomials can be found by lattice reduction if

$$X^{s_1} Y^{s_2} Z^{s_3} < W^s, \tag{1}$$

where $s_j = \sum_{x^{i_1}y^{i_2}z^{i_3} \in M \setminus S} i_j$ for $j = 1, \ldots, 3$, and $W = ||f(xX, yY, zZ)||_\infty \geq N_1X$.

One can check $s_1 = \frac{m^3}{2} + \frac{5}{2}m^2 + 4m + 2 + 2t + \frac{3}{2}m^2t + \frac{7}{2}mt$, $s_2 = \frac{5}{6}m^3 + 4m^2 + \frac{37}{6}m + 3 + 2t + \frac{3}{2}m^2t + \frac{7}{2}mt$, $s_3 = \frac{1}{2}m^3 + \frac{5}{2}m^2 + 4m + 2 + \frac{3}{2}t^2 + \frac{7}{2}t + \frac{3}{2}m^2t + mt^2 + \frac{9}{2}mt$, and $s = \frac{1}{3}m^3 + \frac{3}{2}m^2 + \frac{13}{6}m + 1 + t + m^2t + 2mt$.

Neglecting lower order terms, form (1), we get the condition as

$$X^{\frac{m^3}{2} + \frac{3}{2}m^2t} Y^{\frac{5}{6}m^3 + \frac{3}{2}m^2t} Z^{\frac{m^3}{2} + \frac{3}{2}m^2t + mt^2} < W^{\frac{m^3}{3} + m^2t}.$$

Let $t = \tau m$. Then we get the required condition is

$$\tau^2\beta + (2\alpha + \frac{3}{2}\beta - 1)\tau + (\alpha + \frac{\beta}{2} - \frac{1}{3}) < 0. \tag{2}$$

Now optimal value of τ to minimize the left hand side of (2) is $\frac{1 - \frac{3}{2}\beta - 2\alpha}{2\beta}$. Putting this optimal value, the required condition will be $-64\alpha^2 - 32\alpha\beta - 4\beta^2 + 64\alpha + \frac{80}{3}\beta - 16 < 0$. That is, when this condition holds, according to [4], we get two polynomials f_0, f_1 such that $f_0(x_0, y_0, z_0) = f_1(x_0, y_0, z_0) = 0$. Under Assumption 1, we can extract x_0, y_0, z_0 following the method of [8, Section 6]. □

Remark 1. In the proof of Theorem 1, we have applied extra shift over z. In fact, we have tried with extra shifts on x, y too. However, we have noted that the best theoretical as well as experimental results are achieved using extra shifts on z.

It is clear from Theorem 1, that fixing the bit-size of N, if the size of q_1, q_2 (i.e., α) increases, then the equality of the MSBs of p_1, p_2 should increase (i.e., β should decrease) for efficient factorization of N_1, N_2.

The theoretical as well as experimental results are presented in Table 1. The experimental results in each row are based on average of five runs where N_1, N_2 are 1000-bit integers. We have written the programs in SAGE 3.1.1 over Linux Ubuntu 8.04 on a computer with Dual CORE Intel(R) Pentium(R) D CPU 1.83 GHz, 2 GB RAM and 2 MB Cache. The experiments in Table 1 are performed with lattice dimension 46 (parameters $m = 2, t = 1$) and each lattice reduction takes around 30 seconds.

To explain the results of Table 1, let us concentrate on the first row. As $\alpha = 0.23$, we have q_1, q_2 are of bit size $0.23 \times 1000 = 230$. Thus, p_1, p_2 are of bit size $1000 - 230 = 770$. Now, the numerical value from Theorem 1 tells that $770 - 0.255 \times 1000 = 515$ many MSBs of p_1, p_2 need to be equal to have efficient factorization of N_1, N_2 simultaneously. However, the average of the experimental results are more encouraging which shows that only $770 - 0.336 \times 1000 = 434$ many MSBs of p_1, p_2 need to be equal to have efficient factorization of N_1, N_2 simultaneously.

α	Numerical upper bound of β following Theorem 1	Results achieved for β from experiments
0.23	0.255	0.336
0.24	0.239	0.313
0.25	0.225	0.296
0.26	0.210	0.269
0.27	0.196	0.250

Table 1. Theoretical and experimental values of α, β for which N_1, N_2 can be factored efficiently.

Remark 2. From Table 1 it is clear that we get much better results in experiments than the theoretical bound. This is because, for the parameters we consider here, the shortest vectors belong to some sub-lattice. However, the theoretical calculation in Theorem 1 cannot capture that and further, identifying such optimal sub-lattice seems to be difficult as pointed out in [4, Section 7.1].

We also present evidences to show that higher lattice dimension provides better experimental results. In Examples 1, 2, we find that when $\alpha = 0.25$, the values of β that can be achieved are as high as 0.308, 0.311 respectively for lattice parameters $m = 3, t = 2$. These results are better than the average $\beta = 0.296$ as presented in Table 1 for $m = 2, t = 1$.

Example 1. For a demonstration of the experiment, consider 750-bit primes p_1 and p_2
396778011092655898569559925922550870735308234813817371391424958007814853787 2

659986732427543412353227686360435307307811045754814960959318503826990494991538951443158292762268189891045388828922478530615979139037853178431738420087 and
396778011092655898569559925922550870735308234813817371391424958007814853787265998673242754341235322768636043530730781104575481496095976726398499046698751141487176339721078617296105516700049994688783715717616627568674346533214 7.
Note that p_1, p_2 share 442 many MSBs. Further, q_1, q_2 are 250-bit primes
1791405259026492103131865184203435870047916914753003354202248185126637129539 and
1359854273468970113914581544928445498889538930116761650886947228775354080297
respectively. We use lattice of dimension 105 (parameters $m = 3, t = 2$) and the lattice reduction takes 6457.84 seconds. □

Example 2. As another experimental result, consider 750-bit primes p_1 and p_2
3103293851234545621612884177271352199071965229969307590769556901553501696121486894504150753778107049899894702257572943969973109842059427848262110574521661287756193724060104016731225285634163002534645448007119837656454227440177 and
3103293851234545621612884177271352199071965229969307590769556901553501696121486894504150753778107049899894702257572943969973109842063500611566034390188986791515114690594523923567275780555267831035031294553991617471138271288077.
Note that p_1, p_2 share 439 many MSBs. Further, q_1, q_2 are 250-bit primes
1761986055485501596400884508719659270275271677762068580864458138443043985389 and
1793915333056311315115475413216227307458109801843263226409813428452265284467
respectively. We use lattice of dimension 105 (parameters $m = 3, t = 2$) and the lattice reduction takes 7150.09 seconds. □

In Theorem 1, we have considered that given the conditions, we can find f_0, f_1 by lattice reduction. However, in practice, one may get more polynomials. In our experiments, we used four polynomials f_0, f_1, f_2, f_3 that come after lattice reduction. Let J be the ideal generated by $\{f, f_0, f_1, f_2, f_3\}$ and let the corresponding Gröbner Basis be G. We studied the first three elements of G and found that one of them is of the form $xy - \frac{q_2}{q_1}y^2 - y$. Note that $x_0 = q_2 + 1, y_0 = q_1$ is the root of this polynomial.

Thus the result of Theorem 1 and the experimental evidences show that under certain conditions polynomial time factoring is possible with implicit hints.

2.2 The LSB Case

Let us first explain the ideas presented in [9]. Let $N_1 = p_1q_1$ and $N_2 = p_2q_2$. In [9, Section 3], it has been explained that if $q_1, q_2 \approx N^\alpha$, then for efficient factorization of N_1, N_2, the primes p_1, p_2 need to share at least $2\alpha \log_2 N$ many LSBs.

Our strategy is different from the strategy of [9] and we apply the similar technique as explained in Section 2.1.

Theorem 2. *Let $N_1 = p_1q_1$ and $N_2 = p_2q_2$, where p_1, q_1, p_2, q_2 are primes. Let $q_1, q_2 \approx N^\alpha$. Consider that $\gamma \log_2 N$ many LSBs of p_1, p_2 are same, i.e., $p_1 \equiv p_2 \bmod N^\gamma$. Let $\beta = 1-\alpha-\gamma$. Under Assumption 1, one can factor N_1, N_2 in polynomial time if $-4\alpha^2 - 2\alpha\beta - \frac{1}{4}\beta^2 + 4\alpha + \frac{5}{3}\beta - 1 < 0$ provided $1 - \frac{3}{2}\beta - 2\alpha \geq 0$.*

Proof. We can write $p_1 = p + N^\gamma P_1$ and $p_2 = p + N^\gamma P_2$. Thus, $p_1 - p_2 = N^\gamma(P_1 - P_2)$. Since, $p_1 = \frac{N_1}{q_1}$ and $p_2 = \frac{N_2}{q_2}$, we get $N^\gamma(P_1 - P_2)q_1q_2 + N_2q_1 - N_1q_2 = 0$. Thus we need to solve $f'_{LSB}(x, y, z) = N^\gamma xyz + N_2y - N_1x = 0$ whose roots corresponding to x, y, z are $q_2, q_1, P_2 - P_1$. Since there is no constant term in f'_{LSB}, we define a new polynomial $f_{LSB}(x, y, z) = f'_{LSB}(x - 1, y, z) = N^\gamma xyz - N^\gamma yz + N_2y - N_1x + N_1$. The root (x_0, y_0, z_0) of f_{LSB} is $(q_2 + 1, q_1, P_2 - P_1)$.

One may note the form of f_{LSB} is similar to that of f in the proof of Theorem 1. From this point, the proof of this theorem follow in a similar manner that of the proof of Theorem 1. One should note that the bound of W as in the proof of Theorem 1 and in this proof are same as the terms $N^\gamma XYZ$ and N_1X are of the same order. Thus the final result is same as the result achieved in Theorem 1. □

The numerical values related to the theoretical result of [9] and Theorem 2 as well as experimental results are presented in Table 2. The experimental results in each row are based on one run where N_1, N_2 are 1000-bit integers. The experiments in Table 2 are performed with lattice dimension 46 (parameters $m = 2, t = 1$) and each lattice reduction takes around 30 seconds. Similar to the observation in Section 2.1, we note from Table 2 that better results are obtained in experiments than the theoretical bound. We believe the reason is same as explained in Remark 2 in Section 2.1.

α	Numerical upper bound of β following [9]	Numerical upper bound of β following Theorem 2	Results achieved for β from experiments
0.23	0.31	0.255	0.336
0.24	0.28	0.239	0.314
0.25	0.25	0.225	0.296
0.26	0.22	0.210	0.268
0.27	0.19	0.196	0.251

Table 2. Theoretical and experimental values of α, β for which N_1, N_2 can be factored efficiently.

In our notation, the number of MSBs in each of p_1, p_2 that are unshared is $\beta \log_2 N$. Thus $\beta = (1-\alpha) - 2\alpha = 1 - 3\alpha$, where $\alpha \log_2 N$ is the bit size of q_1, q_2. Table 2 identifies that while our theoretical result is either worse or better than that of [9] based on the values of α, the experimental results that we obtain are always better than [9]. In the introduction of [9], it has been pointed out that for 250-bit q_1, q_2 and 750-bit p_1, p_2, the primes p_1, p_2 need to share 502 many LSBs. We have implemented the strategy of [9] and observed similar results.

On the other hand, our experimental results are better as evident from Table 2, when $\alpha = 0.25$. In fact, we experimented with a higher lattice dimension as explained in Examples 3, 4 and our strategy requires only 442 and 439 many LSBs respectively to be shared in p_1, p_2. These results are much better than [9], where 502 many LSBs have been shared.

Example 3. In this experiment, consider 750-bit primes p_1 and p_2

523246440179017349688977681373199246300779679719795875248443960719154045523566080873243780899117355727443003322341020696579559344619892893099620681032 50

78810654140616439325724089448684722792481034854929045247229685114499401607 and
43117967184022373153326220379007738003558323245492616146998953161907332541040376948850231036794311185546576317750184830286997614825307318419096215142451357302696651881931971908384412624064535232790055330917280424424920209509193573026966518819319719083844126240645352327900553309172804244249202095091.
Note that p_1, p_2 share 442 many LSBs which will be clear if one writes p_1, p_2 in binary and checks the LSBs. Further, q_1, q_2 are 250-bit primes
1631651738790114027147107602960138604308539138427653628254827153426896347739 and
1776124692833044236475237348456766321872003926797460168161822934670015844393
respectively. We use lattice of dimension 105 (parameters $m = 3, t = 2$) and the lattice reduction takes 7160.63 seconds. □

Example 4. Here we consider 750-bit primes p_1 and p_2
589525413967922807714238741658649003961328319146624140130749426182460596690846904207227162754390752815664870747005792755657396108802785184052727673670100332217332947627771123511694759914704886336601966226161930457596168266829746904942344746869094705955909000801680277401455969654717495533379446523428615649346253501206754072656012248789459690026524713466850400698503016817420142894918107629408891591088684705545955400539206624614659487642347293364.
Note that p_1, p_2 share 439 many LSBs. Further, q_1, q_2 are 250-bit primes
916010977814643010666950783967979656772444969801926690589674791043059104197 and
158706175206503232628029032601471134104482708215075739571825411154499494575
respectively. We use lattice of dimension 105 (parameters $m = 3, t = 2$) and the lattice reduction takes 7273.52 seconds. □

We now discuss in more details how our strategy compares with that of [9]. It is indeed clear from Table 2, that our experimental results provide much better performance than the theoretical results presented in our paper as well as in [9]. Moreover, we now explain how the technique of [9] and our strategy compare in terms of theoretical results.

Let us first concentrate on the formula $\beta = 1 - 3\alpha$, that characterizes the bound on the primes for efficient factoring in [9]. When $\alpha = \frac{1}{3}$, then β becomes zero, implying that p_1, p_2 need to have all the bits shared. Thus, the upper bound on the smaller primes q_1, q_2 is $N^{\frac{1}{3}}$, where sharing of LSBs in p_1, p_2 helps in efficient factoring.

However, in our case, the bound on the primes is characterized by $-4\alpha^2 - 2\alpha\beta - \frac{1}{4}\beta^2 + 4\alpha + \frac{5}{3}\beta - 1 < 0$ provided $1 - \frac{3}{2}\beta - 2\alpha \geq 0$. We find that β becomes zero when $\alpha = \frac{1}{2}$. Thus in our case, the upper bound on smaller primes q_1, q_2 is $N^{\frac{1}{2}}$, where sharing of LSBs in p_1, p_2 helps in efficient factoring.

One may check that our method starts performing better (i.e., β in our case is greater than that of [9]) than [9] when $\alpha \geq 0.266$. Thus for $q_1, q_2 \geq N^{0.266}$, our method will require less number of LSBs of p_1, p_2 to be equal than that of [9]. This is also presented in Figure 1. The shaded region in the figure identifies our improvement in terms of theoretical analysis. However, we like to reiterate that our experimental results outperforms the theoretical results presented by us as well as in [9].

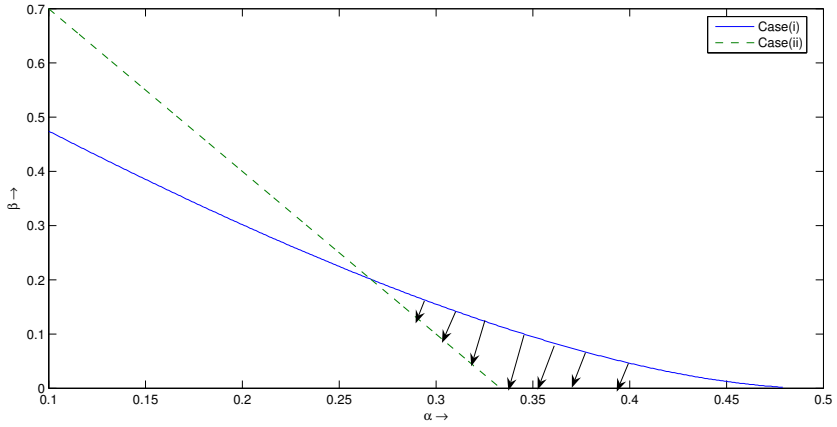

Fig. 1. Comparison of our theoretical results (case (i)) with that of [9] (case (ii)).

The theoretical analysis of our results related to LSBs, presented in this section, will apply similarly for our analysis related to MSBs as explained in Section 2.1.

3 Conclusion

In this paper we have studied poly($\log N$) time factorization strategy when two integers N_1, N_2 (of same size) are given where $N_1 = p_1q_1$ and $N_2 = p_2q_2$ and p_1, p_2 share certain amount of LSBs or MSBs. The results either extend or improve the problem presented in [9]. Our technique does not immediately extend the following generalized problems studied in [9].

1. Our strategy is hard to extend with more than two integers, i.e., when one considers that $N_1, N_2, \ldots, N_k$ are available such that $N_1 = p_1q_1, N_2 = p_2q_2, \ldots, N_k = p_kq_k$ and all the p_i's share t many MSBs. This is because, the idea presented in Theorem 1 exploits the fact that $p_2 - p_1$ is small. It is not clear how to extend the idea when $p_j - p_i$ is small in general. Similar bottleneck exists when we consider sharing of LSBs too.
2. Our idea does not work when one considers that p_i, q_i are of same bit-size. The bound presented in Theorem 1 does not accommodate this case. Even if we consider that some information regarding q_i's are available, that also does not help much. This is because, under such information the structure of the polynomial f' in Theorem 1 changes and more number of monomials arrive, that prevents to achieve a good bound.

Still, we like to point out that the problem of factorization with two integers N_1, N_2 in this domain is harder than the case of factorization with more than two integers $N_1, N_2, \ldots, N_k$. For the case of two integers, we present results that could not be achieved earlier.

The strategy presented in [9] used lattice dimension 2 only for the case with two integers N_1, N_2 and it is also not immediate whether similar technique can be extended with higher lattice dimensions. However, our strategy allows to exploit larger lattice dimensions and thus during experiments we get better results as lattice dimension increases.

References

1. T. Apostol. An Introduction to Analytic Number Theory. Narosa Publishing House, 1979.
2. D. Coppersmith. Finding a Small Root of a Bivariate Integer Equations. Eurocrypt 1996, LNCS 1070, pp. 178–189, 1996.
3. J. -S. Coron. Finding Small Roots of Bivariate Integer Equations Revisited. Eurocrypt 2004, LNCS 3027, pp. 492–505, 2004.
4. E. Jochemsz and A. May. A Strategy for Finding Roots of Multivariate Polynomials with new Applications in Attacking RSA Variants. Asiacrypt 2006, LNCS 4284, pp. 267–282, 2006.
5. H. W. Jr. Lenstra. Factoring Integers with Elliptic Curves. AA. Math 126, pp. 649–673, 1987.
6. A. K. Lenstra and H. W. Jr. Lenstra. The Development of the Number Field Sieve. Springer-Verlag, 1993.
7. A. K. Lenstra, H. W. Lenstra and L. Lovász. Factoring Polynomials with Rational Coefficients. Mathematische Annalen, 261:513–534, 1982.
8. E. Jochemsz and A. May. A Polynomial Time Attack on RSA with Private CRT-Exponents Smaller Than $N^{0.073}$. Crypto 2007, LNCS 4622, pp. 395–411, 2007.
9. A. May and M. Ritzenhofen. Implicit Factoring: On Polynomial Time Factoring Given Only an Implicit Hint. PKC 2009. Available at http://www.cits.rub.de/personen/may.html [last accessed 5 March, 2009].
10. A. May. Using LLL-Reduction for Solving RSA and Factorization Problems: A Survey. LLL+25 Conference in honour of the 25th birthday of the LLL algorithm, 2007. Available at http://www.informatik.tu-darmstadt.de/KP/alex.html [last accessed 23 December, 2008].
11. C. Pomerance. The Quadratic Sieve Factoring Algorithm. Eurocrypt 1984, LNCS 209, pp. 169–182, 1985.
12. R. Rivest and A. Shamir. Efficient Factoring Based on Partial Information. Eurocrypt 1985, LNCS 219, pp. 31–34, 1986.
13. P. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Science Press, pp. 124–134, 1994.