The hidden number problem with non-prime modulus

Theodoulos Garefalakis
Department of Mathematics
University of Crete, 71409 Heraklion, Crete, Greece
theo@math.uoc.gr

May 3, 2007

Abstract

We consider a generalization of the Hidden Number Problem for general moduli N, and prove that it can be solved with high probability if roughly $2(\log N)^{1/2}$ aproximations of quality at least $(\log N)^{1/2}$ are given, and the multipliers are chosen uniformly at random from $\mathbb{Z}/N\mathbb{Z}$. We prove a similar result in the case that the multipliers are chosen uniformly at random from $(\mathbb{Z}/N\mathbb{Z})^{\times}$ and N is the product of two distinct primes. The last result holds in the more general case when N is squarefree and a technical condition related to the prime factors of N holds. The condition is related to the distribution of the solutions of a linear equation modulo N. The Hidden Number Problem modulo the product of two primes, with multipliers chosen from $(\mathbb{Z}/N\mathbb{Z})^{\times}$, is related to the bit security of the most significant bits of the RSA and Rabin functions. Our solution of the Hidden Number Problem implies that computing roughly $(\log(N))^{1/2}$ bits of the RSA and Rabin functions is equivalent to computing the entire values.

Keywords Hidden number problem, exponential sums, lattice basis reduction.

Classification 11Y16, 11B50, 11T23

1 Introduction

Let p be a prime, $\alpha \in \mathbb{Z}/p\mathbb{Z}$, and $\mu > 0$. For any integer t we denote by $\lfloor t \rfloor_p$ the remainder of the division of t by p. The Hidden Number Problem ($\mathcal{HNP}$) can be defined as follows: Given d elements t_i, $i = 1, \ldots, d$ chosen uniformly at random from a subgroup V of $(\mathbb{Z}/p\mathbb{Z})^{\times}$ and d integers s_i, $i = 1, \ldots, d$ such that

$$|\lfloor \alpha t_i \rfloor_p - s_i| \leq p2^{-\mu}, \quad i = 1, \ldots d$$

compute α.

The problem was introduced by Boneh and Venkatesan [1] in connection with the bit security of the Diffie-Hellman key, and solved it for $\mu \sim \sqrt{\log p}$ and $V = (\mathbb{Z}/p\mathbb{Z})^\times$. For specific applications one wishes to solve $\mathcal{HNP}$ for μ and the order of V as small as possible. In all subsequent works, the best value of μ is $\sim \sqrt{\log p}$.

Considering proper subgroups of $(\mathbb{Z}/p\mathbb{Z})^\times$ of as small order as possible is mathematically challenging and relevant to the bit security problem. González Vasco and Shparlinski [12] solved the problem for subgroups of order $p^{1/3+\epsilon}$ and proved that the method works for groups of order p^ϵ for almost all primes p. Finally, Shparlinski and Winterhof [10] showed that the mathod works for subgroups of order as small as $\log p/(\log\log p)^{1-\epsilon}$ for every prime p. Several variants of $\mathcal{HNP}$ have been considered, see for instance [8, 11, 3, 5, 9], with applications to the security of a variety of cryptosystems such as XTR and LUC.

In this work, we consider the Hidden Number Problem for general modulus N. Using lattice basis reduction techniques, we extend the results of [1] to non-prime moduli. Our results are stated in terms of the parameters d, the number of given approximations, and δ, the quality of the approximations. In our notation, we are given integers v_i, $i = 1, \ldots, d$ and integers s_i $i = 1, \ldots, d$ such that

$$|\alpha v_i - u_i N - s_i| \leq N^{1-\delta}, \quad i = 1, \ldots, d$$

for some integers u_i, $i = 1, \ldots, d$. We call the s_i aproximations of quality $\delta$of $\alpha v_i - u_i N$. The values $\alpha v_i - u_i N$ need not be the residues of αv_i modulo N, although this generalization is not deep. We consider two different situations regarding the distribution of the multipliers v_i. If they are chosen uniformly at random from $\mathbb{Z}/N\mathbb{Z}$, we solve the problem for any N and roughly $\delta \geq \frac{1}{d} + \frac{d}{4n}$. When they are chosen from $(\mathbb{Z}/N\mathbb{Z})^\times$ we solve the problem for N squarefree subject to a technical condition needed to ensure that the solutions of a linear equation modulo N are uniformly distributed. In this case, the algorithm works for roughly the same value of δ as before. Our results lead to a straightforward reduction of the problem of

computing the values of the RSA and Rabin functions to that of computing the $\sim \sqrt{\log n}$ most significant bits, where n is the RSA modulus. We note that result on the bit security of the RSA and Rabin functions is not the best known. Indeed, the best known results in this direction are given in [2], where the security every single bit is proved. Our intention is to show that the Hidden Number Problem which initially was considered in connection to the security of the Diffie-Hellman mapping has immediate implications to the security of two other well-known cryptographic functions.

The paper is organized as follows: In section 2, we prove two technical lemmas regarding the distribution of the solutions of linear congruences modulo N, that are needed in the proof of the main theorems. In Section 3, we prove that the natural generalization of the algorithm of [1, 12] works in this setting with high probability. In the next two sections we give the connection to the well known version of $\mathcal{HNP}$ and to the bit security of the RSA and Rabin functions. We conclude with some comments for further work.

2 Distribution modulo N

We state the following simple lemma that will be used in the proof of Lemma 5. Let λ, r and ℓ be integers. We denote by $N_\lambda(r, \ell)$ the number of integers $x \in [0, N-1]$ such that $\lambda x \equiv y \pmod N$ with $y \in [r+1, r+\ell]$.

Lemma 1. *Suppose that* $\gcd(\lambda, N) = g < N$. *The number* $N_\lambda(r, \ell)$ *of solutions* $x \in \mathbb{Z}/N\mathbb{Z}$ *to the congruence*

$$\lambda x \equiv y \pmod N, \quad \textit{with} \quad r+1 \le y \le r+\ell$$

satisfy

$$\max_{0 \le r, \ell \le N-1} |N_\lambda(r, h) - \ell| \le g.$$

The following technical lemma is needed in the proof of Lemma 3.

Lemma 2. *Let s be a squarefree integer. Then*

$$\sum_{a\in(\mathbb{Z}/s\mathbb{Z})^\times} \exp\left(2\pi ia/s\right) = (-1)^{\omega(s)},$$

where $\omega(s)$ is the number of distinct prime divisors of s.

Proof. We proceed by induction on the number of prime divisors of s. If s is prime, then

$$\sum_{a\in(\mathbb{Z}/s\mathbb{Z})^\times} \exp\left(2\pi ia/s\right) = -1$$

and the base case holds. Suppose the statement is true for any squarefree integer with k prime factors. Consider any integer s with $k+1$ prime factors and write it as $p\cdot t$. From the squarefreeness we have $(t,p)=1$ and the Chinese Remainder Theorem yields

$$\begin{aligned}\sum_{a\in(\mathbb{Z}/pt\mathbb{Z})^\times} \exp\left(2\pi ia/pt\right) &= \sum_{b\in(\mathbb{Z}/p\mathbb{Z})^\times}\sum_{c\in(\mathbb{Z}/t\mathbb{Z})^\times} \exp\left(2\pi i(bs+cp)/pt\right)\\ &= \sum_{b\in(\mathbb{Z}/p\mathbb{Z})^\times} \exp\left(2\pi ib/p\right) \sum_{c\in(\mathbb{Z}/t\mathbb{Z})^\times} \exp\left(2\pi ic/t\right)\\ &= (-1)\cdot(-1)^{\omega(t)} = (-1)^{\omega(s)},\end{aligned}$$

where the last equation holds since $\omega(t)=k+1$ and $\omega(s)=k$. □

We denote by $M_\lambda(r,\ell)$ the number of solutions of the equation $\lambda x \equiv y \pmod N$, with $x\in[0,N-1]$ with $(x,N)=1$, and $y\in[r+1,r+\ell]$.

Lemma 3. *Let N be a positive squarefree integer, $\lambda\in\mathbb{Z}$ and let $\gcd(\lambda,N)=g<N$. The number $M_\lambda(r,\ell)$ of solutions $x\in(\mathbb{Z}/N\mathbb{Z})^\times$ to the congruence*

$$\lambda x \equiv y \pmod N, \quad \text{with} \quad r+1\le y\le r+\ell$$

satisfies

$$\max_{0\le r,\ell\le N-1}\left|M_\lambda(r,\ell)-\frac{\phi(N)\ell}{N}\right| \le \phi(g)\log N\prod_{p\mid N/g}\left(2-\frac{1}{p}\right),$$

where the product is extended over all prime divisors of N/g.

Proof. We write $N = gm$ and $\lambda = g\mu$, $(\mu, N) = 1$.

$$\begin{aligned} M_\lambda(r,\ell) &= \frac{1}{N} \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \sum_{y=r+1}^{r+\ell} \sum_{c=0}^{N-1} \exp\left(2\pi i c(\lambda x - y)/N\right) \\ &= \frac{\ell\phi(N)}{N} + \frac{1}{N} \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \sum_{y=r+1}^{r+\ell} \sum_{c=1}^{N-1} \exp\left(2\pi i c(\lambda x - y)/N\right), \end{aligned}$$

therefore

$$\begin{aligned} M_\lambda(r,\ell) - \frac{\ell\phi(N)}{N} &= \frac{1}{N} \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \sum_{y=r+1}^{r+\ell} \sum_{c=1}^{N-1} \exp\left(2\pi i c(\lambda x - y)/N\right) \\ &= \frac{1}{N} \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \sum_{y=r+1}^{r+\ell} \sum_{h \mid m} \sum_{\substack{1 \le c < N \\ (c,m)=h}} \exp\left(2\pi i c(\lambda x - y)/N\right). \end{aligned}$$

We write $c = dh$, $m = sh$ with $(d, s) = 1$ and rearranging we get

$$\begin{aligned} &\sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \sum_{y=r+1}^{r+\ell} \sum_{h \mid m} \sum_{\substack{1 \le c < N \\ (c,m)=h}} \exp\left(2\pi i c(\lambda x - y)/N\right) \\ &= \sum_{h \mid m} \sum_{\substack{1 \le d < gs \\ (d,s)=1}} \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \exp\left(2\pi i d\mu x/s\right) \sum_{y=r+1}^{r+\ell} \exp\left(-2\pi i dy/gs\right). \end{aligned}$$

Since $N = gh \cdot s$ and $(gh, s) = 1$, using the Chinese Remainder Theorem we have

$$\begin{aligned} \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \exp\left(2\pi i d\mu x/s\right) &= \sum_{a \in (\mathbb{Z}/s\mathbb{Z})^\times} \sum_{b \in (\mathbb{Z}/gh\mathbb{Z})^\times} \exp\left(2\pi i d\mu(agh + bs)/s\right) \\ &= \sum_{a \in (\mathbb{Z}/s\mathbb{Z})^\times} \exp\left(2\pi i d\mu agh/s\right) \sum_{b \in (\mathbb{Z}/gh\mathbb{Z})^\times} \exp\left(2\pi i d\mu b\right) \\ &= \phi(N/s) \sum_{a \in (\mathbb{Z}/s\mathbb{Z})^\times} \exp\left(2\pi i d\mu agh/s\right) \\ &= \phi(N/s) \sum_{a \in (\mathbb{Z}/s\mathbb{Z})^\times} \exp\left(2\pi i a/s\right), \end{aligned}$$

since $(d\mu gh, s) = 1$. Lemma 2 now shows that

$$\left| \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \exp\left(2\pi i d\mu x/s\right) \right| = \phi(N/s).$$

The elementary estimate

$$\sum_{\substack{1\le d<gs\\(d,s)=1}}\left|\sum_{y=r+1}^{r+\ell}\exp\left(-2\pi idy/gs\right)\right|\le gs\log(gs),$$

yields the bound

$$\begin{aligned}\frac{1}{N}\left|\sum_{x\in(\mathbb{Z}/N\mathbb{Z})^\times}\sum_{y=r+1}^{r+\ell}\sum_{c=1}^{N-1}\exp\left(2\pi ic(\lambda x-y)/N\right)\right| &\le \frac{1}{N}\sum_{h|m}\phi(gh)\frac{N}{h}\log\left(\frac{N}{h}\right)\\ &\le \phi(g)\log N\sum_{h|m}\phi(h)/h\\ &= \phi(g)\log N\prod_{p|N/g}\left(2-\frac{1}{p}\right).\end{aligned}$$

which concludes the proof.

□

3 Lattices

Let $\{\mathbf{b}_1,\ldots,\mathbf{b}_t\}$ be a set of linearly independent vectors of $\mathbb{R}^t$. Then the set of vectors

$$\mathcal{L}=\left\{\mathbf{v}=\sum_{i=1}^{t}m_i\mathbf{b}_i : m_1,\ldots,m_t\in\mathbb{Z}\right\}$$

is called a t-dimensional lattice of full rank. The set $\{\mathbf{b}_1,\ldots,\mathbf{b}_t\}$ is called a basis of $\mathcal{L}$. It is well known that the basis is not unique. We will need the following result that is based on the lattice basis reduction of Lenstra, Lenstra, and Lovász [4]. We note that a somewhat stronger version of the result we state here holds, as has been shown in [6, 7].

Lemma 4. *There exists a polynomial time algorithm which, given a t-dimensional lattice $\mathcal{L}$ and a vector $\mathbf{s}=(s_1,\ldots,s_t)$ computes a lattice vector $\mathbf{x}=(x_1,\ldots,x_t)$ that satisfies,*

$$\|\mathbf{x}-\mathbf{s}\|\le 2^{\frac{t-1}{4}}\min\{\|\mathbf{v}-\mathbf{s}\|:\mathbf{v}\in\mathcal{L}\}.$$

Our problem is very similar to the Hidden number problem of [1] – only the modulus is not prime. So we use the same technique as in [1, 12]. Let $v_1, \ldots, v_d$ be integers in the interval $[0, N-1]$. We denote by $\mathcal{L}_N(v_1, \ldots, v_d)$ the $d+1$ dimensional lattice generated by the rows of the following $(d+1) \times (d+1)$ matrix

$$\begin{pmatrix} N & 0 & 0 & \ldots & 0 & 0 \\ 0 & N & 0 & \ldots & 0 & 0 \\ & \vdots & & & & \vdots \\ 0 & 0 & 0 & \ldots & N & 0 \\ v_1 & v_2 & v_3 & \ldots & v_d & 1/N \end{pmatrix}$$

Lemma 5. *Let $\delta > 0$ and $N, d \in \mathbb{N}$, $n = \log N$, $d \geq 2$, and $\delta \geq 1/d + (3 + 2/d)/n$. Let Q be a fixed integer in $[1, N-1]$. Choose integers $v_1, \ldots, v_d$ uniformly at random in the interval $[0, N-1]$. Suppose that the vector $\mathbf{s} = (s_1, \ldots, s_d, 0) \in \mathbb{R}^{d+1}$ satisfies*

$$\left(\sum_{i=1}^{d} (Qv_i - Nu_i - s_i)^2 \right)^{1/2} \leq N^{1-\delta},$$

for some integers $u_1, \ldots, u_d$. Then with probability at least $1 - 2^{-\delta} - 2^{3d-(d\delta-1)n}$, any vector $(x_1, \ldots, x_d, x_{d+1}) \in \mathcal{L}_N(v_1, \ldots, v_d)$ satisfying

$$\left(\sum_{i=1}^{d} (x_i - s_i)^2 \right)^{1/2} \leq N^{1-\delta} \tag{1}$$

is of the form

$$\mathbf{v}_P = (Pv_1 - m_1 N, \ldots, Pv_d - m_d N, P/N),$$

with $P \equiv Q \pmod{N}$, and $Pv_i - m_i N = Qv_i - u_i N$, $i = 1, \ldots, d$.

Proof. As in [1], we define the modular distance modulo N of two integers A and B as

$$\mathrm{dist}_N(A, B) = \min_{b \in \mathbb{Z}} |A - B + bN| = \min\{\lfloor A - B \rfloor_N, N - \lfloor A - B \rfloor_N\},$$

where $\lfloor A - B \rfloor_N$ denotes the remainder of $A - B$ upon division with N.

Any point in the lattice $\mathcal{L}_N(v_1, \ldots, v_d)$ is of the form

$$\mathbf{v}_P = (Pv_1 - m_1 N, \ldots, Pv_d - m_d N, P/N) \quad \text{with} \quad P, m_1, \ldots, m_d \in \mathbb{Z}.$$

Let $\gcd(P-Q,N)=g$. We denote by $\mathcal{C}$ the condition given by Eq.(1). We want to estimate the probability

$$\begin{aligned}
& \Pr\left(\forall P\in\mathbb{Z}\ \ \mathcal{C}\Rightarrow P\equiv Q \pmod N\right)\\
= \ & 1-\Pr\left(\exists P\in\mathbb{Z}\ \ \mathcal{C}\wedge \gcd(P-Q,N)<N\right)\\
= \ & 1-\Pr\left(\exists P\in\mathbb{Z}\ \ \mathcal{C}\wedge (2N^{1-\delta}<\gcd(P-Q,N)<N)\right)\\
& -\Pr\left(\exists P\in\mathbb{Z}\ \ \mathcal{C}\wedge (1\le \gcd(P-Q,N)\le 2N^{1-\delta})\right).
\end{aligned}$$

We proceed by estimating the two probabilities.

Suppose that $2N^{1-\delta}<g<N$. Then for every $1\le j\le d$ there is some $b_j\in\mathbb{Z}$ such that

$$\mathrm{dist}_N(Pv_j,Qv_j)=|(P-Q)v_j-b_jN|.$$

Suppose that $(P-Q)v_j-b_jN=0$ for every $1\le j\le d$. Writing $v_j(P-Q)/g=b_jN/g$ we see that N/g divides v_j for all j. This happens with probability at most 2^{-d}. Thus, with probability at least $1-2^{-d}$ there exists at least one index j_0 such that

$$|(P-Q)v_{j_0}-b_{j_0}N|=\left|\frac{P-Q}{g}v_{j_0}-b_{j_0}\frac{N}{g}\right|g\ge g,$$

which implies that

$$\mathrm{dist}_N(Pv_{j_0},Qv_{j_0})\ge g.$$

Then we have

$$\begin{aligned}
\left(\sum_{i=1}^{d}(Pv_i-m_iN-s_i)^2\right)^{1/2} \ & \ge \ |Pv_{j_0}-m_{j_0}N-s_{j_0}|\\
& \ge \ |Pv_{j_0}-Qv_{j_0}-(m_{j_0}-u_{j_0})N|-|Qv_{j_0}-u_{j_0}N-s_{j_0}|\\
& \ge \ \mathrm{dist}_N(Pv_{j_0},Qv_{j_0})-|Qv_{j_0}-u_{j_0}N-s_{j_0}|\\
& \ge \ g-N^{1-\delta}\\
& > \ N^{1-\delta},
\end{aligned}$$

which contradicts our assumption on $\mathbf{v}_P$. We note that the probability is over the random choice of the v_i and has nothing to do with P. We conclude that

$$\Pr\left(\exists P\in\mathbb{Z}\ \ \mathcal{C}\wedge (2N^{1-\delta}<g<N)\right)\le 2^{-d}$$

Suppose now that $1 \leq g \leq 2N^{1-\delta}$. We wish to estimate the probability that

$$\max_{1 \leq i \leq d} \text{dist}_N(Pv_i, Qv_i) > 2N^{1-\delta} \tag{2}$$

holds for any P with $\gcd(P - Q, N) \leq 2N^{1-\delta}$. From Lemma 1 we see that for any fixed i, and fixed P,

$$\text{dist}_N(Pv_i, Qv_i) \leq 2N^{1-\delta} \tag{3}$$

holds for at most

$$4N^{1-\delta} + g \leq 6N^{1-\delta}$$

values of v_i, which implies

$$\Pr(\text{dist}_N(Pv_i, Qv_i) \leq 2N^{1-\delta}) \leq 6N^{-\delta}.$$

Then

$$\Pr(\forall i, \text{dist}_N(Pv_i, Qv_i) \leq 2N^{1-\delta}) \leq (6N^{-\delta})^d.$$

There are at most N possible values for P, so the probability that Eq. (3) holds for at least one value of P is

$$\Pr(\exists P \ \ \forall i, \text{dist}_N(Pv_i, Qv_i) \leq 2N^{1-\delta}) \leq N(6N^{-\delta})^d.$$

If Eq.(2) holds, then

$$\begin{aligned}
\left(\sum_{i=1}^{d}(Pv_i - m_iN - s_i)^2\right)^{1/2} &\geq \max_{1 \leq i \leq d}|Pv_i - m_iN - s_i| \\
&\geq \max_{1 \leq i \leq d}\min_{b \in \mathbb{Z}}(|(P-Q)v_i - bN| - |Qv_i + u_iN - s_i|) \\
&\geq \max_{1 \leq i \leq d}(\text{dist}_N(Pv_i, Qv_i) - |Qv_i + u_iN - s_i|) \\
&> N^{1-\delta},
\end{aligned}$$

which again contradicts the assumption on the vector $\mathbf{v}_P$. Therefore condition $\mathcal{C}$ can hold in this case only if Eq.(3) holds for some P and all $1 \leq i \leq d$, which happens with probability at most $N(6N^{-\delta})^d$, that is

$$\Pr\left(\exists P \in \mathbb{Z} \ \ \mathcal{C} \wedge (\gcd(P - Q, N) \leq 2N^{1-\delta})\right) \leq 2^{3d-(d\delta-1)\log N},$$

and the statement about the probability follows. Finally, to see that $Pv_i - m_iN = Qv_i - u_iN,\ i = 1, \ldots, d$, it suffices to note that if $Pv_j - m_jN \neq Qv_j - u_jN$ for some $1 \leq j \leq d$, then the vector $\mathbf{v}_P - \mathbf{s}$ would have norm at least $N - N^{1-\delta} > N^{1-\delta}$, which contradicts the assumption on $\mathbf{v}_P$. □

A similar result holds if the numbers $v_1, \ldots, v_d$ are chosen uniformly at random from $(\mathbb{Z}/N\mathbb{Z})^\times$.

Lemma 6. *Let $\delta > 0$ and $N, d \in \mathbb{N}$, $N = pq$, $q < p < N^{1-2\delta}$ primes, $n = \log N$, $d \geq 2$, and $\delta \geq 1/d + 3/n$. Let Q be a fixed integer in $[1, N-1]$. Choose integers $v_1, \ldots, v_d$ uniformly at random in $(\mathbb{Z}/N\mathbb{Z})^\times$. Let $\mathbf{s} = (s_1, \ldots, s_d, 0) \in \mathbb{R}^{d+1}$ and suppose that there exist integers $u_1, \ldots, u_d$ such that*

$$\left(\sum_{i=1}^{d} (Qv_i - Nu_i - s_i)^2 \right)^{1/2} \leq N^{1-\delta}.$$

Then with probability at least $1 - 2^{3d-(d\delta-1)n}$, any vector $(x_1, \ldots, x_d, x_{d+1}) \in \mathcal{L}_N(v_1, \ldots, v_d)$ satisfying

$$\left(\sum_{i=1}^{d} (x_i - s_i)^2 \right)^{1/2} \leq N^{1-\delta} \tag{4}$$

is of the form

$$\mathbf{v}_P = (Pv_1 - m_1N, \ldots, Pv_d - m_dN, P/N),$$

with $P \equiv Q \pmod{N}$, and $Pv_i - m_iN = Qv_i - u_iN,\ i = 1, \ldots, d$.

Proof. The proof is similar to that of Lemma 5, and in fact a bit simpler due to the special form of N. We outline the main points. As before, we want to estimate the probability

$$\begin{aligned} & \Pr\left(\forall P \in \mathbb{Z}\ \ \mathcal{C} \Rightarrow P \equiv Q \pmod{N}\right) \\ = \ & 1 - \Pr\left(\exists P \in \mathbb{Z}\ \ \mathcal{C} \wedge (2N^{1-\delta} < \gcd(P-Q, N) < N)\right) \\ & - \Pr\left(\exists P \in \mathbb{Z}\ \ \mathcal{C} \wedge (1 \leq \gcd(P-Q, N) \leq 2N^{1-\delta})\right). \end{aligned}$$

We denote $(P-Q,N)=g$. The case $2N^{1-\delta}<g<N$ leads to a contradiction here, since for any $b\in\mathbb{Z}$ and any $1\le j\le d$ we have

$$\begin{aligned}\left(\sum_{i=1}^{d}(Pv_i-m_iN-s_i)^2\right)^{1/2} &\ge |Pv_j-m_jN-s_j|\\ &\ge |Pv_j-Qv_j-(m_j-u_j)N|-|Qv_j-u_jN-s_j|\\ &\ge g-N^{1-\delta}\\ &> N^{1-\delta},\end{aligned}$$

because

$$|Pv_j-Qv_j-(m_j-u_j)N|=g\left|\frac{P-Q}{g}v_j-(m_j-u_j)\frac{N}{g}\right|>2N^{1-\delta},$$

and $|\frac{P-Q}{g}v_j-(m_j-u_j)\frac{N}{g}|\ge 1$ since $(v_j,N)=1$.

In the case $1\le g\le 2N^{1-\delta}$, we see from Lemma 6 that

$$\operatorname{dist}_N(Pv_i,Qv_i)\le 2N^{1-\delta}$$

holds for at most

$$\frac{\phi(N)4N^{1-\delta}}{N}+O(p\log N)=4\phi(N)N^{-\delta}+O(p\log N)$$

elements $v_i\in(\mathbb{Z}/N\mathbb{Z})^\times$, so this happens with probability at most

$$4N^{-\delta}+O\left(\frac{p\log N}{\phi(N)}\right)=4N^{-\delta}+O\left(\frac{N^{1-2\delta}\log N}{N}\right)=4N^{-\delta}+O(N^{-2\delta}\log N).$$

For N sufficiently large, we see that

$$\Pr(\operatorname{dist}_N(Pv_i,Qv_i)\le 2N^{1-\delta})\le 5N^{-\delta}.$$

The proof is now virtually identical to that of Lemma 5. □

Theorem 7. *Let $d,N,Q\in\mathbb{N}$, with $1\le Q<N$ and $n=\log N$. There exist a probabilistic polynomial time algorithm $\mathcal{A}$ such that given integers $v_1,\dots,v_d$ chosen*

uniformly at random from $[1, N-1]$*, and integers* $s_1, \ldots, s_d \in [0, N-1]$ *such that there exist integers* $u_1, \ldots, u_d \in [1, Q-1]$ *that satisfy*

$$|Qv_i - Nu_i - s_i| < N^{1-\delta} \quad i = 1, \ldots, d$$

with

$$\delta \geq \frac{1}{d} + \frac{3 + 2/d}{n} + \frac{d}{4n} + \frac{\log(d+1)}{2n},$$

computes Q *with probability at least* $1 - 2^{-d} - 2^{3d-(d\eta-1)n}$*, where* $\eta = \delta - \frac{d}{4n} - \frac{\log(d+1)}{2n}$.

Proof. The argument is essentially the same as in [1, 12]. We consider the lattice $\mathcal{L}_N(v_1, \ldots, v_d)$, and observe that there exist integers $u_1, \ldots, u_d$ such that the vector $\mathbf{v}_Q = (Qv_1 - u_1 N, \ldots, Qv_d - u_d N, Q/N) \in \mathcal{L}_N(v_1, \ldots, v_d)$ is very close to the vector $\mathbf{s} = (s_1, \ldots, s_d)$. Specifically,

$$\left(\sum_{i=1}^{d} (Qv_i - u_i N - s_i)^2 \right)^{1/2} \leq \sqrt{d} N^{1-\delta}.$$

Lemma 4 asserts that we can compute in polynomial time a vector $\mathbf{x}$ in $\mathcal{L}_N(v_1, \ldots, v_d)$ such that

$$\begin{aligned} \left(\sum_{i=1}^{d} (x_i - s_i)^2 \right)^{1/2} \leq \|\mathbf{x} - \mathbf{s}\| &\leq 2^{\frac{d}{4}} \min \{ \|\mathbf{v} - \mathbf{s}\| \colon \mathbf{v} \in \mathcal{L}_N(v_1, \ldots, v_d) \} \\ &\leq 2^{\frac{d}{4}} \|\mathbf{v}_Q - \mathbf{s}\| \\ &\leq 2^{\frac{d}{4}} \sqrt{d+1} N^{1-\delta} \\ &= N^{1-\eta}, \end{aligned}$$

with

$$\eta = \delta - \frac{d}{4 \log N} - \frac{\log(d+1)}{2 \log N}.$$

If the condition

$$\eta \geq \frac{1}{d} + \frac{3 + 2/d}{n} \iff \delta \geq \frac{1}{d} + \frac{3 + 2/d}{n} + \frac{d}{4n} + \frac{\log(d+1)}{2n}$$

is satisfied, then Lemma 5 applies, and we see that with probability at least $1 - 2^{-d} - 2^{3d-(d\eta-1)n}$, the vector $\mathbf{x}$ is of the form $(Pv_1 - m_1 N, \ldots, Pv_d - m_d N, P/N)$ with

$P \equiv Q \pmod N$. So the denominator Q can be recovered from the last coordinate of the computed vector. □

The same argument, using Lemma 6 yields the following theorem.

Theorem 8. *Let $d, N, Q \in \mathbb{N}$, with $N = pq$, $q < p < N^{1-2\delta}$ primes, $1 \leq Q < N$ and $n = \log N$. There exist a probabilistic polynomial time algorithm $\mathcal{A}$ such that given integers $v_1, \ldots, v_d$ chosen uniformly at random from $(\mathbb{Z}/N\mathbb{Z})^\times$, and integers $s_1, \ldots, s_d \in [0, N-1]$ such that there exist integers $u_1, \ldots, u_d \in [1, Q-1]$ that satisfy*

$$|Qv_i - Nu_i - s_i| < N^{1-\delta} \quad i = 1, \ldots, d$$

with

$$\delta \geq \frac{1}{d} + \frac{3}{n} + \frac{d}{4n} + \frac{\log(d+1)}{2n},$$

computes Q with probability at least $1 - 2^{3d-(d\eta-1)n}$, where $\eta = \delta - \frac{d}{4n} - \frac{\log(d+1)}{2n}$.

4 Connection to the hidden number problem

The hidden number problem with approximation parameter μ ($\mathcal{HNP}$) can be described as follows. Fix a prime p and denote with $\lfloor \alpha \rfloor_p$ the remainder of of the division of α with p. We call an approximation of an integer $0 \leq v < p$ any integer u that satisfies $|v - u| \leq p/2^\mu$. Fix an (unknown) integer $0 \leq \alpha < p$. Given approximations $u_1, \ldots, u_d$ to d integers $\lfloor \alpha t_1 \rfloor_p, \ldots, \lfloor \alpha t_d \rfloor_p$, with $t_i, i = 1 \ldots, d$ known, we wish to compute α. We want to do this for as small a value of μ as possible. The problem was first defined and studied in [1] for the case when the t_i are uniformly distributed in $(\mathbb{Z}/p\mathbb{Z})^\times$, and was extended in [12] to the case when the t_i are uniformly distributed to subgroups of $(\mathbb{Z}/p\mathbb{Z})^\times$ of appropriately large size.

From the definition of the approximations, and writing $at_i = v_i p + \lfloor \alpha t_i \rfloor_p$ we have

$$|\alpha t_i - v_i p - u_i| \leq \frac{p}{2^\mu} = p^{1-\delta} \quad \text{for} \quad i = 1, \ldots, d, \tag{5}$$

for $\delta = \mu / \log p$. This can be seen to be a special case of the problem considered in Theorem 7.

5 Bit security of RSA

We consider the RSA cryptosystem with modulus $n = pq$, encryption exponent a and decryption exponent b, where $ab \equiv 1 \pmod{n}$. Let

$$\begin{array}{ccc} f : (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ c \mod n & \mapsto & c^b \mod n \end{array}$$

be the RSA decryption function. We make the assumption that the classes of $(\mathbb{Z}/n\mathbb{Z})^\times$ are represented by the standard reduced residue system, that is, by the set of integers $\{0 \leq k < n \mid (k, n) = 1\}$. We denote the remainder of an integer t upon division with n with $\lfloor t \rfloor_n$.

The main result of this section is that the problem of computing the first roughly $(\log n)^{1/2}$ bits of the values of f is equivalent to the problem of computing all the bits. For any $\mu > 0$, we define a μ-approximation of t, $\mathrm{APPR}_\mu(t)$, to be any integer s such that

$$|\lfloor t \rfloor_n - s| \leq n2^{-\mu}.$$

Let $\mathcal{O}_{n,\mu}$ be an oracle which, given an integer t outputs $\mathrm{APPR}_\mu(t^b)$.

Theorem 9. *Let $\mu = \lceil \sqrt{\log n} \rceil + \lceil \log \log n \rceil$ and (n, a) an RSA public key, where $n = pq$, $q < p < n^{1-3/\sqrt{\log n}}$ primes, and $a^{-1} \equiv b \pmod{n}$. There exists a probabilistic polynomial time algorithm, which given the public key (n, a) and a value $c \in (\mathbb{Z}/n\mathbb{Z})^\times$ makes $O(\sqrt{\log n})$ calls to the oracle $\mathcal{O}_{n,\mu}$ and computes the value $\lfloor c^b \rfloor_n$ correctly with probability at least $1 - 2^{-\sqrt{\log n}}$, for n sufficiently large.*

Proof. The goal of the algorithm is to compute $\lfloor c^b \rfloor_n$, which we denote by Q. The algorithm selects u_i uniformly at random from $(\mathbb{Z}/n\mathbb{Z})^\times$ and computes $\lfloor u_i^a c \rfloor_n$, for $i = 1, \ldots, d$. For each computed value, it queries the oracle to obtain approximations of

$$(u_i^a c)^b \equiv u_i c^b \equiv u_i Q \pmod{n}.$$

More precisely it obtains values $s_1, \ldots, s_d$ such that

$$|\lfloor u_i Q \rfloor_n - s_i| \leq n2^{-\mu} \leq n^{1-\delta}, \quad i = 1, \ldots, d,$$

where $\delta = \mu / \log n$. Then, choosing $d = 2\lceil \sqrt{\log n} \rceil$ we see that the conditions of Theorem 8 are satisfied, and therefore the value Q can be computed with probability at least $1 - 2^{-\sqrt{\log n}}$, for n sufficiently large. □

Clearly the same proof, with $a = 2$, gives a result about the computational difficulty of computing the $\sqrt{\log n}$ most significant bits of the Rabin function.

6 Conclusion

We presented a generalization of the Hidden Number Problem with a non-prime modulus. In the case that the multipliers are chosen from $[1, N-1]$ the problem can be solved with high probability for any N. In the case that the multipliers are chosen from $(\mathbb{Z}/N\mathbb{Z})^\times$ we presented a solution in the case that N is the product of two primes. A slight modification of Lemma 6 holds in the case of squarefree integers subject a condition that ensures that the error term of Lemma 3 is not too large. For instance, insisting that the number of prime divisors of N is bounded by $\log \log N$ is sufficient for Lemma 6 to hold for $\delta \geq 1/d + \log \log N / \log N$. It would interesting, to extend the result in the case that the multipliers are chosen from a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$. We conclude this work by showing how the solution of the Hidden Number Problem implies the security of the $\sim \sqrt{\log n}$ most significant bits of the RSA encryption, where n is the RSA modulus. A very important open problem is to prove Theorem 8 for as small δ as possible. Any significant improvement in that direction would have immediate implications to the security of the most significant bits of the RSA and Rabin functions.

References

[1] D. Boneh and R. Venkatesan. Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes. In *Advances in Cryptology – Crypto '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 129–142, Berlin, 1996. Springer-Verlag.

[2] Johan Håstad and Mats Näslund. The security of all RSA and discrete log bits. *J. ACM*, 51(2):187–230, 2004.

[3] N.A. Howgrave-Graham, P.Q. Nguyen, and I.E. Shparlinski. Hidden number problem with hidden multipliers, timed-release crypto and noisy exponentiation. *Math. Comp.*, 72(243):1473–1485, 2003.

[4] A.K. Lenstra, H.W. Lenstra, and L. Lovasz. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[5] W.-C.W. Li, M. Naslund, and I.E. Shparlinski. The hidden number problem with the trace and bit security of XTR and LUC. In *Advances in Cryptology – Crypto 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 433–448, Santa Barbara, 2002. Springer Verlag.

[6] D. Micciancio. *On the hardness of the shortest vector problem.* PhD thesis, MIT, 1998.

[7] P. Nguyen and J. Stern. Lattice reduction in cryptology: An update. In *4th International Algorithmic Number Theory Symposium – ANTS IV*, volume 1838 of *Lecture Notes in Computer Science*, pages 85–112. Springer Verlag, 2000.

[8] I.E. Shparlinski. On the generalised hidden number problem and bit security of XTR. In *Proc. 14th Symp. on Appl. Algebra, Algebraic Algorithms, and Error-Correcting Codes*, volume 2227 of *Lecture Notes in Computer Science*, pages 268–277, Melbourne, 2001. Springer Verlag.

[9] I.E. Shparlinski. Sparse polynomial approximation in finite fields. In *Proc. 33rd ACM Symposium on Theory of Computing*, pages 209–215, Crete, Greece, 2001.

[10] I.E. Shparlinski and A. Winterhof. A hidden number problem in small subgroups. *Math. Comp.*, 74(252):2073–2080, 2005.

[11] M.I. González Vasco, M. Naslund, and I.E. Shparlinski. The hidden number problem in extension fields and its applications. In *Proc. 5th Latin American Theoretical Informatics Conference*, volume 2286 of *Lecture Notes in Computer Science*, pages 105–117, Cancun, 2002. Springer Verlag.

[12] M.I. González Vasco and I.E. Shparlinski. On the security of Diffie-Hellman bits. In *Proc. Workshop on Cryptography and Computational Number Theory*, pages 257 – 268, Singapore, 1999. Birkhäuser, 2001.