

# On the Number of Sparse RSA Exponents

WILLIAM D. BANKS

Department of Mathematics, University of Missouri  
Columbia, MO 65211, USA  
`bbanks@math.missouri.edu`

and

IGOR E. SHPARLINSKI

Department of Computing, Macquarie University  
Sydney, NSW 2109, Australia  
`igor@ics.mq.edu.au`

## Abstract

An RSA modulus is a product  $M = pl$  of two primes  $p$  and  $l$ . We show that for almost all RSA moduli  $M$ , the number of sparse exponents  $e$  (which allow for fast RSA encryption) with the property that  $\gcd(e, \varphi(M)) = 1$  (hence RSA decryption can also be performed) is very close to the expected value.

**Key Words:** RSA, modular exponentiation, sum of digits

## 1 Introduction

Let  $M$  be an integer, and let  $\varphi(M)$  denote the Euler function.

We recall that given an integer  $e$  with  $\gcd(e, \varphi(M)) = 1$ , one round of the *RSA encryption* of a message  $x \in [0, M - 1]$  consists of the modular exponentiation  $x^e \equiv y \pmod{M}$ , which produces an encrypted message  $y \in [0, M - 1]$ . Because  $\gcd(e, \varphi(M)) = 1$ , if the factorization of  $M$  is known (hence the value of  $\varphi(M)$  can be computed), one can find an integer  $d$  with

$$ed \equiv 1 \pmod{\varphi(M)}. \tag{1}$$

The *decryption* then consists of the modular exponentiation

$$y^d \equiv x^{ed} \equiv x \pmod{M}.$$

In this paper, we estimate the number of *sparse* exponents  $e$ , which support fast modular exponentiation  $x^e \pmod{M}$  and therefore speed-up RSA encryption, that also satisfy the condition  $\gcd(e, \varphi(M)) = 1$ .

It is often recommended to select the encryption (or decryption) exponent in the RSA algorithm as a sparse integer (with say at most  $k$  non-zero binary digits); see Section 14.6.1 of [12]. If  $e$  is an  $n$ -bit integer with only  $k$  non-zero binary digits, then the computation of  $x^e \pmod{M}$  by repeated squaring requires  $n + k$  modular multiplications, while for an arbitrary  $n$ -bit integer it is about  $2n$  operations in the worst case and about  $1.5n$  operations “on average”. However, since we also require the condition  $\gcd(e, \varphi(M)) = 1$  for decryption, it is not clear how many such exponents are available. We remark that despite the existence of faster exponentiation methods, repeated squaring still remains one of the most commonly used in practice. In any

case, studying the properties of sparse integers is a very natural number theoretic question.

To be more precise, let us denote by  $\mathcal{N}_{n,k}(M)$  the set of  $e \in [1, 2^n - 1]$  with exactly  $k$  non-zero binary digits and such that  $\gcd(e, \varphi(M)) = 1$ . We will show that the cardinality  $N_{n,k}(M)$  of  $\mathcal{N}_{n,k}(M)$  is close to its expected value

$$N_{n,k}(M) \sim 2 \binom{n-1}{k-1} \frac{\varphi(\varphi(M))}{\varphi(M)}$$

when  $M$  runs through the set of RSA moduli  $M = pl$ , where  $p$  and  $l$  are two prime numbers. We remark that for an even  $m$  there are  $\varphi(m)$  integers  $x \in [0, m/2 - 1]$  for which  $\gcd(2x + 1, m) = 1$ , thus the density of such  $x \in [0, m/2 - 1]$  is equal to  $2\varphi(m)/m$ .

Throughout the paper,  $\mathcal{P}$  denotes the set of primes;  $\log z$  and  $\ln z$  denote the binary and natural logarithms of  $z > 0$ , respectively.

**Acknowledgement.** We thank Marcos Kiwi for his interest, his careful reading of the manuscript, and his helpful advice. We also thank Sergei Konyagin for interesting and helpful discussions.

Work supported in part, for W. B. by NSF grant DMS-0070628 and for I. S. by ARC grant A69700294.

## 2 Counting Sparse Encryption Exponents

For an integer  $n$ , we denote by  $\mathcal{R}_n$  the set of  $n$ -bit integers that are products of two primes, that is,

$$\mathcal{R}_n = \left\{ M = pl : 2^{n-1} \leq M < 2^n, \quad p, l \in \mathcal{P} \right\}.$$

Let us consider the sum

$$W_k(n) = \frac{1}{|\mathcal{R}_n|} \sum_{M \in \mathcal{R}_n} \left| N_{n,k}(M) - 2 \binom{n-1}{k-1} \frac{\varphi(\varphi(M))}{\varphi(M)} \right|.$$

**Theorem.** *For any  $k$  and  $n$  with  $k \leq (n+1)/2$ , the bound*

$$W_k(n) = O \left( kn^3 \binom{n-1}{k-1} \exp(-ck^{3/2}n^{-1}) \right)$$

holds for some absolute constant  $c > 0$ .

*Proof.* Let us denote by  $\mu(m)$  the Möbius function. Recall that  $\mu(1) = 1$ ,  $\mu(m) = 0$  if  $m$  is not square-free, and  $\mu(m) = (-1)^{\nu(m)}$  otherwise, where  $\nu(m)$  is the number of prime divisors of  $m \geq 2$ . From the inclusion-exclusion principle (see also Theorem 2.1 of Chapter 2 of [13]), we see that

$$N_{n,k}(M) = \sum_{m|\varphi(M)} \mu(m)T_{n,k}(m),$$

where  $T_{n,k}(m)$  is the number of  $e \in [1, 2^n - 1]$  with exactly  $k$  non-zero binary digits and such that  $e \equiv 0 \pmod{m}$ . If  $m$  is odd, it is easily seen that  $T_{n,k}(2m) = T_{n-1,k}(m)$  and  $\mu(2m) = -\mu(m)$ ; consequently

$$N_{n,k}(M) = \sum_{\substack{m|\varphi(M) \\ m \text{ odd}}} \mu(m)(T_{n,k}(m) - T_{n-1,k}(m)) = \sum_{\substack{m|\varphi(M) \\ m \text{ odd}}} \mu(m)T_{n,k}^*(m), \quad (2)$$

where  $T_{n,k}^*(m)$  is the number of  $e \in [2^{n-1}, 2^n - 1]$  with exactly  $k$  non-zero binary digits and such that  $e \equiv 0 \pmod{m}$ .

By Theorem 2 of [10], there exist absolute constants  $c_1, c_2 > 0$  such that

$$T_{n,k}(m) = \frac{1}{m} \binom{n}{k} (1 + O(\exp(-c_1 k / \log m)))$$

uniformly for  $m \leq K$ , where  $K = \exp(c_2 k^{1/2})$ . For any such  $m$ , we have

$$T_{n,k}^*(m) = \frac{1}{m} \binom{n-1}{k-1} (1 + O(\exp(-c_1 k / \log m))). \quad (3)$$

To estimate  $T_{n,k}^*(m)$  for larger values of  $m$ , we remark that if  $m$  lies in the range  $2^s \leq m \leq 2^{s+1} - 1$  and if  $m|e$ , then those bits of  $e$  in the rightmost  $s$  positions are uniquely determined by the bits in the leftmost  $n-s$  positions. Since the first bit of  $e$  is 1, we have

$$T_{n,k}^*(m) \leq \sum_{j=0}^{k-1} \binom{n-1-s}{j}.$$

For any integer  $s \geq 0$ , we have the bound

$$T_{n,k}^*(m) \leq 2^{n-1-s} < 2^n/m. \quad (4)$$

If  $2k \leq n - s + 1$ , we have a better estimate

$$T_{n,k}^*(m) \leq k \binom{n-1-s}{k-1}.$$

Because  $1 - z \leq \exp(-z)$  for any  $z \geq 0$ , we obtain

$$\frac{n-1-s-j}{n-1-j} \leq \exp(-s/(n-1-s-j)) \leq \exp(-s/(n-1))$$

for  $j = 0, \dots, k-2$ . Therefore,

$$\binom{n-1-s}{k-1} \leq \binom{n-1}{k-1} \exp(-s(k-1)/(n-1)).$$

Using this inequality and defining

$$\vartheta = \frac{k-1}{(n-1) \ln 2},$$

we obtain

$$T_{n,k}^*(m) \leq k \binom{n-1}{k-1} 2^{-s\vartheta} \leq k \binom{n-1}{k-1} 2^{\vartheta} m^{-\vartheta} \leq 2k \binom{n-1}{k-1} m^{-\vartheta}. \quad (5)$$

Note that  $\vartheta < 1$  since  $2(k-1) \leq (n-1)$ .

Now we consider two separate cases. First, suppose that  $K < 2^{n-2k+1}$ , and put  $L = 2^{n-2k+1}$ . We use the bound (3) for  $m \leq K$ , the bound (5) for  $K < m \leq L$ , and the bound (4) for  $m > L$ . Therefore, from (2) we derive

$$\begin{aligned} N_{n,k}(M) &= \binom{n-1}{k-1} \sum_{\substack{m|\varphi(M) \\ m \leq K \\ m \text{ odd}}} \frac{\mu(m)}{m} + O\left(\binom{n-1}{k-1} \sum_{\substack{m|\varphi(M) \\ m \leq K \\ m \text{ odd}}} \exp(-c_1 k / \log m)\right) \\ &\quad + k \binom{n-1}{k-1} \sum_{\substack{m|\varphi(M) \\ K < m \leq L \\ m \text{ odd}}} m^{-\vartheta} + 2^n \sum_{\substack{m|\varphi(M) \\ m > L \\ m \text{ odd}}} m^{-1}. \end{aligned}$$

Since  $\vartheta < 1$ , one can extend the first summation to include all odd divisors of  $\varphi(M)$  with the same error term. Because  $\varphi(M)$  is even we have

$$\sum_{\substack{m|\varphi(M) \\ m \text{ even}}} \frac{\mu(m)}{m} = \sum_{\substack{m|\varphi(M) \\ m \text{ odd}}} \frac{\mu(2m)}{2m} = -\frac{1}{2} \sum_{\substack{m|\varphi(M) \\ m \text{ odd}}} \frac{\mu(m)}{m}.$$

Therefore

$$\frac{1}{2} \sum_{\substack{m|\varphi(M) \\ m \text{ odd}}} \frac{\mu(m)}{m} = \sum_{\substack{m|\varphi(M) \\ m \text{ odd}}} \frac{\mu(m)}{m} + \sum_{\substack{m|\varphi(M) \\ m \text{ even}}} \frac{\mu(m)}{m} = \sum_{m|\varphi(M)} \frac{\mu(m)}{m}.$$

Using the well known identity

$$\sum_{m|\varphi(M)} \frac{\mu(m)}{m} = \frac{\varphi(\varphi(M))}{\varphi(M)},$$

which follows from the inclusion-exclusion principle (see also Theorem 2.1 of Chapter 2 of [13]), we obtain

$$\sum_{\substack{m|\varphi(M) \\ m \text{ odd}}} \frac{\mu(m)}{m} = 2 \frac{\varphi(\varphi(M))}{\varphi(M)}.$$

Hence,

$$\begin{aligned} N_{n,k}(M) &= 2 \binom{n-1}{k-1} \frac{\varphi(\varphi(M))}{\varphi(M)} \\ &= O \left( \sum_{\substack{m|\varphi(M) \\ m \leq K \\ m \text{ odd}}} \binom{n-1}{k-1} \exp(-c_1 k / \log m) \right. \\ &\quad \left. + k \binom{n-1}{k-1} \sum_{\substack{m|\varphi(M) \\ K < m \leq L \\ m \text{ odd}}} m^{-\vartheta} + 2^n \sum_{\substack{m|\varphi(M) \\ m > L \\ m \text{ odd}}} m^{-1} \right) \\ &= O \left( \tau(\varphi(M)) \left( \binom{n-1}{k-1} \exp(-c_1 k / \log K) + k \binom{n-1}{k-1} K^{-\vartheta} + 2^n / L \right) \right) \\ &= O \left( \tau(\varphi(M)) \left( \binom{n-1}{k-1} \exp(-c_1 k / \log K) + k \binom{n-1}{k-1} K^{-\vartheta} + 2^{2k} \right) \right), \end{aligned}$$

where  $\tau(r)$  denotes the number of integer divisors of  $r \geq 2$ .

As before we have

$$\begin{aligned} 2^{2k-2} &\leq (2k-2) \binom{2k-2}{k-1} \\ &\leq (2k-2) \binom{n-1}{k-1} \exp(-(n-2k+1)(k-1)/(n-1)) \\ &= (2k-2) \binom{n-1}{k-1} 2^{-\vartheta(n-2k+1)} \leq (2k-2) \binom{n-1}{k-1} K^{-\vartheta}. \end{aligned}$$

Therefore,

$$N_{n,k}(M) - 2 \binom{n-1}{k-1} \frac{\varphi(\varphi(M))}{\varphi(M)} = O \left( \tau(\varphi(M)) k \binom{n-1}{k-1} \exp(-c_3 k^{3/2} n^{-1}) \right)$$

where  $c_3 > 0$  is an absolute constant.

Next we turn to the case  $K \geq 2^{n-2k+1}$ . We use the bound (3) for  $m \leq K$ , and the bound (4) for  $m > K$ . Proceeding as before, we obtain in this case

$$\begin{aligned} N_{n,k}(M) - 2 \binom{n-1}{k-1} \frac{\varphi(\varphi(M))}{\varphi(M)} &= O \left( \sum_{\substack{m|\varphi(M) \\ m \leq K \\ m \text{ odd}}} \binom{n-1}{k-1} \exp(-c_1 k / \log m) + 2^n \sum_{\substack{m|\varphi(M) \\ m > K \\ m \text{ odd}}} m^{-1} \right) \\ &= O \left( \tau(\varphi(M)) \left( \binom{n-1}{k-1} \exp(-c_1 k / \log K) + 2^n K^{-1} \right) \right) \\ &= O \left( \tau(\varphi(M)) \exp(-c_4 k^{1/2}) \left( \binom{n-1}{k-1} + 2^n \right) \right). \end{aligned}$$

It follows from Lemma 8 of [11] that

$$\binom{n-1}{k-1} \geq (2n)^{-1/2} 2^{(n-1)H((k-1)/(n-1))},$$

where

$$H(\alpha) = -\alpha \log \alpha - (1-\alpha) \log(1-\alpha), \quad 0 < \alpha < 1.$$

Note that  $H(\alpha)$  is strictly increasing for  $0 < \alpha < 1/2$ , as is easily verified.

For  $0 < \delta < 1$

$$\begin{aligned} H\left(\frac{1-\delta}{2}\right) &= -\frac{1-\delta}{2} \log \frac{1-\delta}{2} - \frac{1+\delta}{2} \log \frac{1+\delta}{2} \\ &= -\frac{1-\delta}{2} (\log(1-\delta) - 1) - \frac{1+\delta}{2} (\log(1+\delta) - 1) \\ &= 1 + \frac{\delta}{2} \log(1-\delta) - \frac{\delta}{2} \log(1+\delta). \end{aligned}$$

Taking into account that  $\ln(1 \pm \delta) = O(\delta)$  we obtain

$$H\left(\frac{1-\delta}{2}\right) = 1 + O(\delta^2).$$

From the condition on  $K$  we derive the inequality

$$\frac{1}{2} \geq \frac{k-1}{n-1} \geq \frac{1}{2} - \frac{\log K}{2(n-1)} = \frac{1-\delta}{2},$$

where

$$\delta = \frac{\log K}{2(n-1)} = O(n^{-1/2}).$$

Therefore

$$H\left(\frac{k-1}{n-1}\right) \geq H\left(\frac{1-\delta}{2}\right) = 1 + O(n^{-1}).$$

Thus

$$\binom{n-1}{k-1} \geq 2^{n+O(\log n)}$$

and we obtain

$$2^n K^{-1} \leq \binom{n-1}{k-1} \exp(-c_4 k^{1/2})$$

for some absolute constant  $c_4 > 0$ .

Therefore for any  $k \leq (n+1)/2$  we have

$$N_{n,k}(M) - 2 \binom{n-1}{k-1} \frac{\varphi(\varphi(M))}{\varphi(M)} = O\left(\tau(\varphi(M)) k \binom{n-1}{k-1} \exp(-c_5 k^{3/2} n^{-1})\right)$$

for some absolute constant  $c_5 > 0$ .

To complete the proof, recall that  $\tau(rs) \leq \tau(r)\tau(s)$  for integers  $r, s \geq 1$ .

Consequently

$$\sum_{M \in \mathcal{R}_n} \tau(\varphi(M)) \leq \sum_{M=pl \in \mathcal{R}_n} \tau(p-1)\tau(l-1) \leq \sum_{\substack{p \in \mathcal{P} \\ p < 2^n}} \tau(p-1) \sum_{\substack{l \in \mathcal{P} \\ 2^{n-1}/p \leq l < 2^n/p}} \tau(l-1).$$

From Theorem 7.1 of [13] we have

$$\sum_{\substack{l \leq L \\ l \in \mathcal{P}}} \tau(l-1) = O(L).$$

Hence,

$$\begin{aligned} \sum_{M \in \mathcal{R}_n} \tau(\varphi(M)) &= O\left(2^n \sum_{\substack{p < 2^n \\ p \in \mathcal{P}}} \frac{\tau(p-1)}{p}\right) \\ &= O\left(2^n \sum_{j=1}^n 2^{-j} \sum_{\substack{2^{j-1} \leq p < 2^j \\ p \in \mathcal{P}}} \tau(p-1)\right) = O(2^n n). \end{aligned}$$

Thus

$$\begin{aligned} \sum_{M \in \mathcal{R}_n} \left| N_{n,k}(M) - 2 \binom{n-1}{k-1} \frac{\varphi(\varphi(M))}{\varphi(M)} \right| \\ = O \left( kn2^n \binom{n-1}{k-1} \exp(-c_5 k^{3/2} n^{-1}) \right). \end{aligned}$$

From the prime number theorem, one easily derives that  $|\mathcal{R}_n| \geq c_6 2^n n^{-2}$  for some absolute constant  $c_6 > 0$ , and the result follows.  $\square$

In particular, we see that for any  $1/3 > \varepsilon > 0$  and  $k \sim n^{2/3+\varepsilon}$  the bound

$$N_{n,k}(M) = 2 \binom{n-1}{k-1} \frac{\varphi(\varphi(M))}{\varphi(M)} (1 + O(\exp(-n^\varepsilon)))$$

holds for almost all  $M \in \mathcal{R}_n$ .

### 3 Remarks

Let  $t, s$  be nonzero integers and  $n = st$ . We think of the binary representation of an  $n$  bit number as a sequence of  $t$  blocks of  $s$  bits each. Let  $\mathcal{N}_{n,k,t}(M)$  be the set of  $e \in [1, 2^n - 1]$  with exactly  $k$  non-zero bit blocks and such that  $\gcd(e, \varphi(M)) = 1$ . Let  $N_{n,k,t}(M)$  denote the cardinality of  $\mathcal{N}_{n,k,t}(M)$ . Is it true that

$$N_{n,k,t}(M) \sim 2^s (2^s - 1)^{k-1} \binom{t-1}{k-1} \frac{\varphi(\varphi(M))}{\varphi(M)}$$

when  $M$  runs through the set of RSA moduli  $M = pl$ , where  $p$  and  $l$  are two primes?

Note that the case  $s = 1$  reduces to what has already been shown. The motivation for the problem comes from the fact that in order to speed up exponentiation one sometimes uses the *window method* (see Algorithm 14.82 of [12]). Here, rather than “sparse” RSA exponents one is interested in using “block sparse” RSA exponents.

It is known [1, 2, 3, 14, 15] that if some information about the bits of the decryption exponent  $d$  is available then the corresponding encryption is vulnerable to various attacks. Thus it will be very important to show that the set of  $d$  defined by (1) for  $e \in \mathcal{N}_{n,k}(M)$  is uniformly distributed modulo  $\varphi(M)$ . Although we hope that the method of [6] combined with the Hua Loo Keng method of estimating of exponential sums can be applied to this

problem, so far there have been several obstacles that we have not been able to overcome.

On the other hand, there does exist a slightly different set of encryption exponents that also admit fast modular exponentiation (because they are small) and for which the corresponding set of decryption exponents can be shown to be uniformly distributed. The result is based on a recent estimate of a double exponential sum from [7, 8, 9]; see also [5]. To be more specific, it follows from Theorem 2 of [7] that for any  $\varepsilon > 0$ , there exists a constant  $c(\varepsilon) > 0$  that for

$$X = \lfloor \exp(c(\varepsilon)(\log M)^{2/3+\varepsilon}) \rfloor$$

the inverses modulo  $\varphi(M)$  of the elements

$$\mathcal{E} = \{e = pl : p, l \in \mathcal{P}, X \leq p < l \leq 2X, \gcd(pl, \varphi(M)) = 1\}$$

are uniformly distributed modulo  $\varphi(M)$ . For any  $e \in \mathcal{E}$ , the exponentiation  $x^e \equiv (x^p)^l \pmod{M}$  requires only  $O((\log M)^{2/3+\varepsilon})$  modular multiplications, which is much smaller than what is required for a general exponent. On the other hand, since the corresponding decryption exponents are uniformly distributed, it is very unlikely that they will possess any special properties that make them vulnerable to attacks similar to those described in [1, 2, 3, 14, 15].

Finally, it is easy to derive from Theorem 3.1 of [4] that for all integer  $M \in [2^{n-1}, 2^n - 1]$ , except maybe  $o(2^n)$  of them the bound

$$\tau(\varphi(M)) \leq 2^{(0.5+o(1)) \ln^2 \ln M}$$

holds. Using this bound one can show that  $N_{n,k}(M)$  is close to its expected value for almost all integer  $M \in [2^{n-1}, 2^n - 1]$  (rather than just for almost all  $M \in \mathcal{R}_n$ ).

## References

- [1] D. Boneh, ‘Twenty years of attacks on the RSA cryptosystem’, *Notices Amer. Math. Soc.*, **46** (1999), 203–213.
- [2] D. Boneh and G. Durfee, ‘Cryptanalysis of RSA with private key  $d$  less than  $N^{0.292}$ ’, *Proc. EuroCrypt’99*, Springer-Verlag, Berlin, 1999, 1–11.

- [3] D. Boneh, G. Durfee and Y. Frankel, ‘An attack on RSA given a small fraction of the private key bits’, *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1514** (1998), 25–34.
- [4] P. Erdős and C. Pomerance, ‘On the normal number of prime factors of  $\varphi(n)$ ’, *Rocky Mountain J. Math.*, **15** (1985), 343–352.
- [5] J. Friedlander and H. Iwaniec, ‘The Brun–Titchmarsh theorem’, *Analytic Number Theory*, Lond. Math. Soc. Lecture Note Series **247**, 1997, 363–372.
- [6] J. B. Friedlander and I. E. Shparlinski, ‘On the distribution of Diffie–Hellman triples with sparse exponents’, *Preprint*, 1999, 1-21.
- [7] A. A. Karatsuba, ‘Fractional parts of functions of a special form’, *Izv. Ross. Akad. Nauk Ser. Mat. (Transl. as Russian Acad. Sci. Izv. Math.)*, **55**(4) (1995), 61–80 (in Russian)
- [8] A. A. Karatsuba, ‘Analogues of Kloosterman sums’, *Izv. Ross. Akad. Nauk Ser. Mat. (Transl. as Russian Acad. Sci. Izv. Math.)*, **55**(5) (1995), 93–102 (in Russian)
- [9] A. A. Karatsuba, ‘Kloosterman double sums’, *Matem. Zametki (Transl. as Math. Notes)*, **66** (1999), 682–687 (in Russian)
- [10] Ch. Mauduit and A. Sárközy, ‘On the arithmetic structure of the integers whose sum of digits is fixed’ *Acta Arith.*, **81** (1997), 145–173.
- [11] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.
- [12] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1996.
- [13] K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin, 1957.
- [14] E. R. Verheul and H. C. A. van Tilborg, ‘Cryptanalysis of ‘less short’ RSA secret exponents’, *Appl. Algebra in Engin., Commun. and Comp.*, **8** (1997), 425–435.
- [15] M. J. Wiener, ‘Cryptanalysis of short RSA secret exponents’, *IEEE Trans. Inform. Theory*, **36** (1990), 553–558.