A Generalize Estimating the $\phi(n)$ of Upper/Lower Bound to RSA Public Key Cryptosystem*

Jie Fang[1], Chenglian Liu[2]
(Corresponding author: Chenglian Liu)
School of Electronics and Information Engineering, Fuqing Branch of Fujian Normal University[1]
Department of Conputer Science and Technology, Neusoft Institute of Guangdon[2]
Nanhai Software and Technology Park, Foshan 528225, Guangdong, China
(Email: chenglian.liu@gmail.com)
(Received Sept. 18, 2016; revised and accepted Jan. 15, 2017)

Abstract

The RSA-768 (270 decimal digits) was factored by Kleinjung *et al.* on December 12, 2009, while the RSA-704 (212 decimal digits) was factored by Bai *et al.* on July 2, 2012. The RSA-200 (663 bits) was factored by Bahr *et al.* on May 9, 2005, while he RSA-210 (696 bits) was factored by Propper on September 26, 2013. In this paper the author will discuss an estimation method to approach the lower/upper bound of $\phi(n)$ to the RSA parameters. Our contribution may help researchers lock the (n) and the challenge RSA shortly.

Keywords: Euler's Totient Function; Factoring; RSA Cryptosystem

1 Introduction

Challenge RSA [19] is a good work to study. Recently, most scientists and researchers [2, 7, 12] using the general number field sieve (GNFS) algorithm to factor RSA modulus n. In a practical environment, it looks like if you want to break the RSA, the best choice is to choose GNFS if you have already factored the modulus n [5]. In theory, Wiener [24] first proposed a cryptanalysis of short secret exponents where the $d < N^{0.5}$ in 1990. Boneh [3] presented 'Twenty years of attacks on RSA cryptosystem' in 1999, where he classified and described a variety of attacks. Followed by Boneh and Durfee [4], they suggested the private key d should be greater than $N^{0.292}$ for the security problem. Even though, some people like to focus on secret key d or factor composite number n. Their purposes are clear. We believe that there must be a general way to estimate the value of RSA-210 without finding the factors of prime numbers p and q to challenge RSA. According to the latest news, the RSA-210 was factored by Propper [18], and RSA-220 was factored by Bai *et al.* [1]. In this article, the author will introduce a new methodology where we approach the lower bound and the upper bound of $\phi(n)$. For this general concept, it may match any bit length composite number n.

*The preliminary version of this paper appeared in Cryptology ePrint Archive: Report 2012/666 [14].

2 Review of RSA Conception

The signer prepares the prerequisite of a RSA signature: Two distinct large prime p and q, $n = pq$, Let e be a public key so that $\gcd(e, \phi(n)) = 1$, where $\phi(n) = (p-1)(q-1)$, then calculate the private key d such that $ed \equiv 1 \pmod{\phi(n)}$. The signer publishes (e, n) and keeps (p, q, d) secretly. The notation as same in [19].

2.1 RSA Encryption and Decryption

In RSA public-key encryption, Alice encrypts a plaintext M for Bob using Bob's public key (n, e) by computing the ciphertext

$$C \equiv M^e \pmod{n}, \tag{1}$$

where n, the modulus, is the product of two or more large primes, and e, the public exponent, is an (odd) integer $e \geq 3$ that is relatively prime to $\phi(n)$, the order of the multiplicative group $\mathbb{Z}_n^*$ [13].

2.2 RSA Digital Signature

$$s \equiv M^d \pmod{n}, \tag{2}$$

where (n, d) is the signer's RSA private key [6, 10]. The signature is verified by recovering the message M with the signer's RSA public key (n, e):

$$M \equiv s^e \pmod{n}. \tag{3}$$

3 Our Methodology

In this section, we would calculate the upper bound and the lower bound of $\phi(n)$ in RSA scheme. The detail de-

scribed as below.

Notation:

ℓ: Express lower bound.

u: Express upper bound.

ε: A decimal expansion number (e.g $99/100 = 0.99\cdots$).

3.1 Approaching $\phi(n)$

If n is composite, hence

$$\phi(n) \leq n - \sqrt{n}. \tag{4}$$

Sierpinski [22] mentioned it in 1964. It is known that if Equation (4) is a good upper bound for $\phi(n)$. Is there a good lower bound for $\phi(n)$? This question is also be discussed by a newsgroup dialog between Ray Steiner and Bob Silverman in 1999 [23]. For $n > 30$, the $\phi(n) > n^{2/3}$, Kemdall and Osborn proved it [11]. For $n \geq 3$, the $\phi(n) > \frac{\log 2}{2}\frac{n}{\log n}$ given by Hatalova and Salat [9].

3.1.1 Estimate Upper Bound

Is Equation (4) a good upper bound? In the following, we would estimate a new value that is smaller than previous and optimize.

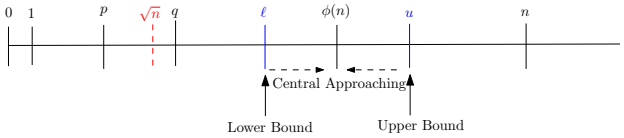

Figure 1: The lower/upper bound of $\phi(n)$ in RSA scheme

Theorem 1. *Assume p and q are large prime numbers, where $n = pq$, then $\phi(n) = 4k$, $k \in \mathbb{Z}$ where $1 \leq k \leq \lfloor \frac{n-2\lceil\sqrt{n}\rceil+1}{4} \rfloor$.*

Proof. As is known, the two variants p and q are large prime numbers. Also both p and $q > 2$, since $2 \nmid p,\ 2 \nmid q$, therefore $2 \mid p-1,\ 2 \mid q-1.\ 4 \mid (p-1)(q-1),\ 4 \mid \phi(n)$. $\phi(n) = 4k,\ k \in \mathbb{Z}^+$. We will discuss how to calculate the range of value k.

$$\begin{aligned} \phi(n) &= (p-1)(q-1) \\ &= pq - (p+q) + 1 \\ &= n - (p+q) + 1. \end{aligned} \tag{5}$$

And

$$\begin{aligned} p+q \geqslant 2\sqrt{n}, p+q \in \mathbb{Z}^+, 2 \mid p+q. \\ p+q \geqslant 2\lceil\sqrt{n}\rceil. \\ \phi(n) \leq n+1-2\lceil\sqrt{n}\rceil. \\ \phi(n) = 4k,\ k \in \mathbb{Z}^+. \\ \phi(n) \leq 4 \cdot \lfloor \frac{n+1-2\lceil\sqrt{n}\rceil}{4} \rfloor. \end{aligned} \tag{6}$$

Here, we know the maximum value (limit superior) for $k \leq \lfloor \frac{n-2\lceil\sqrt{n}\rceil+1}{4} \rfloor$ which we call the boundary value.

Consequently, according to the above reference, we obtain an upper bound u of $\phi(n)$ where $\phi(n) \leq 4\lfloor \frac{n-2\lceil\sqrt{n}\rceil+1}{4} \rfloor$. □

3.1.2 Estimate Lower Bound

Loomis *et al.* [15] found Shapiro's [20] lower bound $\phi(n) > n^{(\log 2)}/(\log 3)$ as a (naive) lower bound for E_n, where they can determine when all members of a given E_n have been found. Powell [17] noted that Konyagin's and Shparlinksi's lower bound $N_1(n,p) > (p-1)/2 - p^{3/2}/n$ where $n > 1$ is a positive integer and that p is an odd prime number with $p \equiv 1 \pmod{n}$; it is a good bound if p is a small compared to n, and establishes that

$$N_1(n,p) \geq (\sqrt{\phi(n)}(\prod_{\substack{q\ prime \\ q \mid n}} q^{1/(q-1)})/n)p^{1-1/\phi(n)}.$$

Powell also discussed an improvement the upper and lower bounds in [17]. What is the optimal lower bound? This is explained as follows.

Theorem 2. *For all $n \geq 3$ we have $\phi(n) \geq \frac{n}{e^\gamma \log\log n} + \emptyset(\frac{n}{(\log\log n)^2})$, where γ is the Euler-Mascherone Constant, and the above holds with equality infinitely often.*

Remark: *note in particular that since $\log\log n \to \infty$ as n grows large, we see that the result $\frac{n}{m} < \phi(n)$ can not hold for any fixed integer m.*

Proof. Consider R, set of all n such that $m < n$ implies $\frac{\phi(n)}{n} < \frac{\phi(m)}{m}$. This set is then all of the 'record breaking' n. If $n \in R$ has k prime factors, let n^* be the product of the first k prime factors. If $n \neq n^*$ and $\frac{\phi(n)^*}{n^*} \leq \frac{\phi(n)}{n}$, which is impossible. Hence, R consist entirely of n of the form $n = \prod_{p \leq y} p$ for some y. Now for $n \in R$, we can choose y so that $\log n = \sum_{p \leq y} \log p = \theta(y)$. Then using one of Mertens estimates we see that $\frac{\phi(n)}{n} = \prod_{p \leq y}(1 - \frac{1}{p}) = \frac{e^{-\gamma}}{\log y} + O(\frac{1}{(\log y)^2})$. Since $\log\log n = \log(\theta(y)) = \log y + \emptyset(1)$ by Mertens estimates again, we have for $n \in R$, $\phi(n) = \frac{ne^{-r}}{\log\log n} + O(\frac{1}{(\log\log n)^2}$. □

Is there a simple computation method? We observed the modulus n with $\phi(n)$, there are some characteristics. Aa an example for RSA-200, the modulus n and the $\phi(n)$ are 200 decimal digits. We compared n and $\phi(n)$ with each other and found that the first **110** digits are the same. The example is shown in Table 1. A discussion on RSA modulus number with half of the bit prescribed, is introduced in some literatures in [8, 16, 21].

In RSA-704, the n and $\phi(n)$ had same digits 106, it amounts same length with p or q. We computed the upper bound value according to Theorem 1. This upper bound had the same 108 digits with its $\phi(n)$. When we analyzed the RSA-768, the n had 115 digits. The same 115 digits was found with $\phi(n)$; the $\phi(n)$ had the same 120 digits with its upper bound u. See Table 2.

We observed the relationship of $\phi(n)$ and its boundary value k. When $\phi(n)$ is divided by k, we found that the

Table 1: The same digits of $\phi(n)$ and modulus n parameters in RSA

RSA-200	Same digits length
n	279978339112213278708294676387226016210704467869554285375600099293261284001076093456710529553608560618223519109513657886371059544820065767750985805576135790987349501441788631789462951872378692218239 83
$\phi(n)$	279978339112213278708294676387226016210704467869554285375600099293261284001076093456710529553608560503640200220702626340174151348034825203659253229957685947151011399122897366813709597472806079535501 68

Table 2: Comparison of some types in RSA parameters. Unit: decimal digits

type \ length	n	$\phi(n)$	$p,\ q$	$n\&\phi(n)$	$\phi(n)\&u$
RSA-200	200	200	100	110	101
RSA-210	210	210	105	?	?
RSA-704	212	212	106	106	108
RSA-220	220	220	109	?	?
RSA-768	232	232	116	115	120

quotient approaches and that, these lower bounders are very close to multiples of number 4. As an example, we say $3.\overline{999}$, and have 106 9's after the decimal point for case of RSA-200 type. The lower bound approximation figure diagram is shown in Figure 2 and in Table 3.

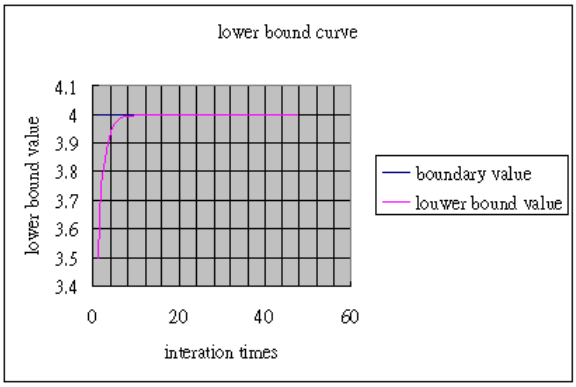

Figure 2: The lower bound approximation curve status.

As known as the modulus number n of RSA-210, we re-estimated its lower/upper bounds. We assume:

$$(3+\varepsilon)\lfloor\frac{n-2\lceil\sqrt{n}\rceil+1}{4}\rfloor \le \phi(n) \le 4\lfloor\frac{n-2\lceil\sqrt{n}\rceil+1}{4}\rfloor, \quad (7)$$

where $\varepsilon = 0.\overbrace{99999}^{106's\ 9}$. We therefore compute the upper bound u and lower bound ℓ; those results are shown in Figure 2.

According to Equation (7), the author estimates the upper bound of RSA-220. There are same 109 digits between RSA-220 modulus n and upper bound u. The result is shown in Figure 4.

Table 3: The relationship of $\phi(n)$ and its boundary value k.

Type	$\phi(n)/k$	Statement
RSA-200	$3.\overbrace{99999}^{99's\ 9}8$	there have 99's 9 after the decimal point
RSA-210	$3.\overbrace{99999}^{106's\ 9}2$	Estimating have 106's 9 after decimal point
RSA-704	$3.\overbrace{99999}^{107's\ 9}8$	there have 107's 9 after decimal point
RSA-220	$3.\overbrace{99999}^{109's\ 9}8$	there have 110's 9 after decimal point
RSA-768	$3.\overbrace{99999}^{117's\ 9}7$	there have 117's 9 after decimal point

4 Conclusion

In this paper, we use another method to estimate a lower/upper bound values of $\phi(n)$ in RSA-210 and upper bound of RSA-220's $\phi(n)$. We think our methodology is easy and intuitive. It may prove useful to researchers who would like to quickly reduce the searching ranges. More researchers focus on secret d or modulus n, such as well known attacks such as short exponent, side channel (or common modulus) and cyclic. Our method is different than previous methods. Finally, the author provides a general method to estimate the lower/upper bound of RSA's $\phi(n)$ public key cryptography.

Acknowledgement

The authors would like to thank the anonymous reviewers for their useful comments. This work is partially supported from Huizhou University project under the number HZUXL201513 and HZUXL201514. This work also partially supported by student innovation training program under the grant number CX2016024, CX2016088 and CX2016089. This work is partially supported from Fujian Provincial Department of Education, the education and scientific research projects for young and middle-

RSA-210	
u	24524664490027821197651766357308801846702678767833275974341445171506160083003858721695220839933207154910263637952541924188359187871980787492506171803735359303932360552651876303774098901774411576748296463270900 8
ℓ	24524664490027821197651766357308801846702678767833275974341445171506160083003858721695220839933207154910261798602705172101757973413153506663360872332013570325789540507021898760211318657098381023213529964583321 6

Figure 3: The lower/upper bound parameters of $\phi(n)$ in RSA-210.

RSA-220	
Modulus n	22601385262034057849416540486101975135080389157197767183211977681094456418179666766085931213065825772506315628866769704480700018111497118630021124879281994874820660701310665866460833279828035603792053919801399464969552615
Upper bond	22601385262034057849416540486101975135080389157197767183211977681094456418179666766085931213065825772506315627915951419800939395463128318782257067976157557055085147087364121932298229970715560080630126490020980805527016920
Lower bound	

Figure 4: The upper bound parameters of $\phi(n)$ in RSA-220.

aged teachers where the project number JAT170673. This research partially supported from foundation for high level recruited talents of university; the project number is NUIT2017-001.

References

[1] S. Bai, P. Gaudry, A. Kruppa, E. Thomé, and P. Zimmermann, "Factorisation of rsa-220 with cado-nfs," 2016. (https://en.wikipedia.org/wiki/RSA_numbers#cite_note-33)

[2] S. Bai, E. Thomé, and P. Zimmermann, "Factorisation of RSA-704 with cado-NFS," *IACR Cryptology ePrint Archive*, pp. 369, 2012.

[3] D. Boneh, "Twenty years of attacks on the RSA cryptosystem," *Notices of the AMS*, vol. 46, pp. 203–213, 1999.

[4] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than $N^{0.292}$," *IEEE Transactions on Information Theory*, vol. 46, pp. 1339–1349, July 2000.

[5] C. C. Chang, C. Y. Sun, and S. C. Chang, "A strong RSA-based and certificateless-based signature scheme," *International Journal of Network Security*, vol. 18, no. 2, pp. 201-208, 2016.

[6] L. Deng, H. Huang, and Y. Qu, "Identity based proxy signature from RSA without pairings," *International Journal of Network Security*, vol. 19, no. 2, pp. 229-235, 2017.

[7] J. Franke F. Bahr, M. Boehm and T. Kleinjung, "RSA-200 is factored," 2005. (http://www.rsa.com/rsalabs/node.asp?id=2879)

[8] S. W. Graham and I. E. Shparlinski, "On RSA moduli with almost half of the bits prescribed," *Discrete Applied Mathematics*, vol. 156, no. 16, pp. 3150–3154, 2008.

[9] H. Hatalova and T. Salat, "Remarks on two results in the elementary theory of numbers," *Acta. FacRer. Natur Univ Comenian. Math.*, no. 20, pp. 113–117, 1969.

[10] M. S. Hwang, K. F. Hwang, I. C. Lin, "Cryptanalysis of the batch verifying multiple RSA digital signatures", *Informatica*, vol. 11, no. 1, pp. 15-19, Jan. 2000.

[11] D. G. Kendall and H. B. Osborn, *Two Simple Lower Bounds for Euler's Function*, vol. 17, Texas Journal of Science, 1965.

[12] T. Kleinjung, K. Aoki, J. Franke, *et al.*, "Factorization of a 768-bit RSA modulus," in *Advances in Cryptology (CRYPTO'10)*, pp. 333–350, Springer, 2010.

[13] C. Liu, C. C. Chang, Z. P. Wu, S. L. Ye, "A study of relationship between RSA public key cryptosystem and Goldbach's conjecture properties," *International Journal of Network Security*, vol. 17, no. 4, pp. 445-453, 2015.

[14] C. Liu and Z. Ye, "Estimating the $\phi(n)$ of Upper/Lower Bound in Its RSA Cryptosystem,". Cryptology ePrint Archive, Report 2012/666, 2012. (http://eprint.iacr.org/2012/666)

[15] P. Loomis, M. Plytage, and J. Polhill, "Summing up the Euler ϕ function," *The College Mathematics Journal*, vol. 39, no. 1, pp. 34–42, 2008.

[16] X. Meng, "On RSA moduli with half of the bits prescribed," *Journal of Number Theory*, vol. 133, no. 1, pp. 105–109, 2013.

[17] C. Powell, "Bounds for multiplicative cosets over fields of prime order," *Mathematics of Computation*, vol. 66, pp. 807–822, Apr. 1997.

[18] R. Propper, "RSA-210 factored," 2013. (http://www.mersenneforum.org/showpost.php?p=354259)
[19] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, 1978.
[20] H. Shapiro, "An arithmetic function arising from the ϕ function," *The American Mathematical Monthly*, vol. 50, pp. 18–30, 1943.
[21] I. E. Shparlinski, "On RSA moduli with prescribed bit patterns," *Designs, Codes and Cryptography*, vol. 39, pp. 113–122, 2006.
[22] W. F. Sierpinski, *Elementary Theory of Numbers*, Warsawa: North-Holland PWN-Polish Scientific Publishers, 1964.
[23] B. Silverman, "Euler's phi functions," 2012. (http://www.math.niu.edu/~rusin/known-math/99/min_phi)
[24] M. J. Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Transations on Information Theory*, vol. 36, pp. 53–558, Sept. 1990.

Biography

Jie Fang received his associate B.S degree in computer science from Fuqing Branch of Fujian Normal University in 2002 and obtained B.S degree from Fujian Normal University in 2006, and the MSc degree of software engineering at University of Electronic Science and Technology of China in 2010. He is currently a lecturer with school of electronics and information engineering at Fuqing Branch of Fujian Normal University. His research includes Computer Security, E-Learning and Laboratory Management.

Chenglian Liu received his B.S degree in information management from National Union University in 1992 and the MSc degree in National Defense from National Defense University in 2004. He studied his doctorate course at Royal Holloway, University of London from 2006 to 2009 under the supervised by Chris Mitchell. His research interests are in Key Agreement and Password Authentication, Number Theory and Cryptanalysis so on.