Cryptanalysis of RSA with a Small Parameter*

Xianmeng Meng[1] and Xuexin Zheng[2]

[1] School of Mathematics
Shandong University of Finance and Economics
Jinan, 250014, P.R. China
mxmeng@gmail.com

[2] Key Lab of Cryptologic Technology and Information Security
Ministry of Education, Shandong University
Jinan, 250100, P.R. China
zhxuexin@mail.sdu.edu.cn

Abstract. This paper investigates the security of RSA system with short exponents. Let $N = pq$ be an RSA modulus with balanced primes p and q. Denote the public exponent by e and the private exponent by d. Then e and d satisfy $ed - 1 = k\phi(N)$, which is usually called the RSA equation. When e and d are both short, and parameter k is the smallest unknown variable in RSA equation, we prove that there exist two new square root attacks. One attack applies the baby-step giant-step method, the other applies the Pollard's ρ method. We show that if K is a known upper bound of k, then k can be recovered in time $\tilde{O}(\sqrt{K})$ and memory $\tilde{O}(\sqrt{K})$ by using the baby-step giant-step method, and in time $\tilde{O}(\sqrt{K})$ and negligible memory by applying Pollard ρ method. As an application of our new attacks, we present the cryptanalysis on an RSA-type scheme proposed by Sun et al.

Keywords: RSA, square root attack, cryptanalysis.

1 Introduction

RSA scheme is the most famous and widely used public-key cryptosystem so far. It was proposed by Rivest, Shamir and Adleman [11] in 1978. Let $N = pq$ be RSA modulus. Usually, primes p and q are balanced with $q < p < 2q$. The public exponent e and private exponent d are chosen to be inverses of each other modulo $\varphi(N) = (p-1)(q-1)$, where $\varphi(N) = (p-1)(q-1)$ is Euler's totient function. The public key is then (N, e) and the secret key is (p, q, d). The security of RSA is based on the hardness of factorization.

To defend the factoring attack, usually RSA modulus N is chosen to be larger, e.g. $l_N = 1024$. Though it is hard to factor N, there are some other attacks as summarized in [8]. Among all the attacks, small private exponent attack is well-known. Using continued fractions, Wiener [22] described an attack, which applies

* This research is partially supported by the National Natural Science Foundation of China (Grant No. 61133013 and No. 60931160442) and the Technology Foundation of Ministry of Education of China (Grant No. 210123).

W. Susilo, Y. Mu, and J. Seberry (Eds.): ACISP 2012, LNCS 7372, pp. 115–123, 2012.

when the private exponent is smaller than $N^{0.25}$. Later, Boneh and Durfee [3,4] improved the result by applying Coppersmith's method [5] and showed that if the private exponent is less than $N^{0.292}$, then the RSA scheme can be broken in polynomial time. Weger [21] present extended attacks of Wiener [22] and Boneh-Durfee [3,4] on condition of small RSA prime difference. In [2], Blömer and May showed a generalized Wiener attack by applying the continued fraction method and Coppersmith's method.

All the above attacks show that choosing small exponents may cause the RSA scheme insecure. However, RSA is computationally complex, because of its requirement of exponentiation operations modulo a large integer N. The RSA encryption and decryption time is nearly proportional to the number of bits in the exponent. To lower the RSA decryption time, people attempt to design some RSA variants with short private exponent which can defend the private exponent attacks listed above. In [14,15], three RSA variants are given to get a secure private exponent shorter than the lower bound of Wiener [22] and Boneh-Durfee [3,4]. Unfortunately, the first and the third variants are broken by Durfee and Nyugen [7] and the second one is proved to be insecure if parameters are chosen careless.

In [16,17], Sun et al. improved the second variant of [14,15] and proposed two RSA schemes. One scheme has two balanced public and private exponents that can balance the encryption costs and decryption costs, and the other scheme can shift the work from decryptor to encryptor through changing the values of the public exponent and private exponent. By applying balanced primes, and these two schemes can defend the attacks of [7,2], etc. However, Sarkar and Maitra [12] presented a partial key exposure attack on RSA schemes of Sun et al. [16,17].

The former works [7,2,12] are all based on Coppersmith's method [5]. Here we investigate square root attacks against RSA. In RSA scheme, the public exponent e and private exponent d satisfy the following equation

$$ed - 1 = k\phi(N), \tag{1}$$

which is usually called the RSA equation. One can see that if e and d are short exponents, such as $l_e = 624$, $l_d = 512$ and usually $l_N = 1024$, then $l_k = 112$. In this case, k is the smallest parameters in (1). This observation leads us to recover k first, then p and q. Now we investigate two square root attacks to recover k. One attack applies the baby-step giant-step method, the other applies the Pollard's method. For these two methods, one can see [6,9] and for improved methods see [1,18,19,20]. We show that if K is a known upper bound of k such that $1 \leq k < K$, there exist two probabilistic algorithms to recover k and then p and q in time $\tilde{O}(\sqrt{K})$. Here and in the sequel, $\tilde{O}()$ is the usual notation hiding polynomial arithmetic terms. As an application of the new attacks, we analyze the security of RSA schemes of Sun et al. [16,17] and find that parameter k should be chosen larger than the values suggested in [16,17].

Notation. We denote the bit-length of an integer u by l_u. Denote by $\lfloor r \rfloor$ the integral part of a real number r. Let $v \equiv u \bmod e$ denote that v is congruent to u modulo e. Let $v = u \bmod e$ denote that v equals the least non-negative remainder of u modulo e.