An Attack on RSA Using LSBs of Multiples of the Prime Factors

Abderrahmane Nitaj
Laboratoire de Mathématiques Nicolas Oresme
Université de Caen, Basse Normandie, France
abderrahmane.nitaj@unicaen.fr

Abstract. Let \( N = pq \) be an RSA modulus with a public exponent \( e \) and a private exponent \( d \). Wiener’s famous attack on RSA with \( d < N^{0.25} \) and its extension by Boneh and Durfee to \( d < N^{0.292} \) show that using a small \( d \) makes RSA completely insecure. However, for larger \( d \), it is known that RSA can be broken in polynomial time under special conditions. For example, various partial key exposure attacks on RSA and some attacks using additional information encoded in the public exponent \( e \) are efficient to factor the RSA modulus. These attacks were later improved and extended in various ways. In this paper, we present a new attack on RSA with a public exponent \( e \) satisfying an equation \( ed - k(N + 1 - ap - bq) = 1 \) where \( \frac{a}{b} \) is an unknown approximation of \( \frac{q}{p} \). We show that RSA is insecure when certain amount of the Least Significant Bits (LSBs) of \( ap \) and \( bq \) are known. Further, we show that the existence of good approximations \( \frac{a}{b} \) of \( \frac{q}{p} \) with small \( a \) and \( b \) substantially reduces the requirement of LSBs of \( ap \) and \( bq \).

Keywords: RSA, Cryptanalysis, Factorization, Lattice, LLL algorithm, Coppersmith’s method.

1 Introduction

The RSA cryptosystem was invented by Rivest, Shamir and Adleman [16] in 1977 and is today’s most important public-key cryptosystem. The standard notations in RSA are as follows:

- \( p \) and \( q \) are two large primes of the same bit size.
- \( N = pq \) is the RSA modulus and \( \phi(N) = (p - 1)(q - 1) \) is Euler’s totient function.
- \( e \) and \( d \) are respectively the public and the private exponents and satisfy \( ed - k\phi(N) = 1 \) for some positive integer \( k \).

There have been a large number of attacks on RSA. Some attacks, called small private key attacks can break RSA in polynomial time when the private key is small. For example, Wiener [17] showed that if the private key satisfies \( d < \frac{1}{3} N^{\frac{1}{4}} \), then \( N \) can be factored and Boneh and Durfee [4] showed that RSA is insecure if
Some attacks, called partial key exposure attacks exploit the knowledge of a portion of the private exponent or of one of the prime factors. Partial key exposure attacks are mainly motivated by using side-channel attacks, such as fault attacks, power analysis and timing attacks ([10], [11]). Using a side-channel, an attacker can expose a part of one of the modulus prime factors $p$ or $q$ or of the private key $d$. In 1998, Boneh, Durfee and Frankel [5] presented several partial key exposure attacks on RSA with a public key $e < N^{1/2}$ where the attacker requires knowledge of most significant bits (MSBs) or least significant bits (LSBs) of the private exponent $d$. In [2], Ernest et al. [7] proposed several partial key exposure attacks that work for $e > N^{1/2}$. Notice that Wiener’s attack [17] and the attack of Boneh and Durfee [4] can be seen as partial key exposure attacks because the most significant bits of the private exponent are known and are equal to zero. Sometimes, it is possible to factor the RSA modulus even if the private key is large and no bits are exposed. Such attacks exploit the knowledge of special conditions verified by the modulus prime factors or by the exponents. In 2004, Blömer and May [3] showed that RSA can be broken if the public exponent $e$ satisfies an equation $ex = y + k\phi(N)$ with $x < \frac{1}{3}N^{\frac{1}{4}}$ and $|y| < N^{-\frac{1}{4}}e$. At Africacrypt 2009, Nitaj [15] presented an attack when the exponent $e$ satisfies an equation $eX - (N - (ap + bq))Y = Z$ with the constraints that $\frac{a}{b}$ is an unknown convergent of the continued fraction expansion of $\frac{a}{b}$, $1 \leq Y \leq X < \frac{1}{2}N^{\frac{1}{4}}$, $\gcd(X, Y) = 1$, and $Z$ depends on the size of $|ap - bq|$. Nitaj’s attack combines techniques from the theory of continued fractions, Coppersmith’s method [6] for finding small roots of bivariate polynomial equations and the Elliptic Curve Method [12] for integer factorization.

In this paper we revisit Nitaj’s attack by studying the generalized RSA equation $ed - k(N + 1 - ap - bq) = 1$ with different constraints using Coppersmith’s method [6] only. We consider the situation when an amount of LSBs of $ap$ and $bq$ are exposed where $\frac{a}{b}$ is an unknown approximation of $\frac{a}{b}$, that is when $a = \left[\frac{bq}{p}\right]$. More precisely, assume that $ap = 2^{m_0}p_1 + p_0$ and $bq = 2^{m_0}q_1 + q_0$ where $m_0$, $p_0$ and $q_0$ are known to the attacker. We show that one can factor the RSA modulus if the public key $e$ satisfies an equation $ed_1 - k_1(N + 1 - ap - bq) = 1$ where $e = N^\gamma$, $d_1 < N^\delta$, $2^{m_0} = N^\beta$ and $a < b < N^\alpha$ satisfy

$$\delta \leq \begin{cases} \delta_1 & \text{if } \gamma \geq \frac{1}{2}(1 + 2\alpha - 2\beta), \\ \delta_2 & \text{if } \gamma < \frac{1}{2}(1 + 2\alpha - 2\beta). \end{cases}$$

with

$$\delta_1 = \frac{7}{6} + \frac{1}{3}(\alpha - \beta) - \frac{1}{3}\sqrt{4(\alpha - \beta)^2 + 4(3\gamma + 1)(\alpha - \beta) + 6\gamma + 1},$$

$$\delta_2 = \frac{1}{4}(3 - 2(\alpha - \beta) - 2\gamma).$$