A New Attack on RSA and Demytko's Elliptic Curve Cryptosystem

Abderrahmane Nitaj and Emmanuel Fouotsa

Abstract. Let $N = pq$ be an RSA modulus and e be a public exponent. Numerous attacks on RSA exploit the arithmetical properties of the key equation $ed - k(p-1)(q-1) = 1$. In this paper, we study the more general equation $eu - (p-s)(q-r)v = w$. We show that when the unknown integers u, v, w, r and s are suitably small and $p - s$ or $q - r$ is factorable using the Elliptic Curve Method for factorization ECM, then one can break the RSA system. As an application, we propose an attack on Demytko's elliptic curve cryptosystem. Our method is based on Coppersmith's technique for solving multivariate polynomial modular equations.

Mathematics Subject Classification (2010). 94A60, 11Y05.

Keywords. RSA, Cryptanalysis, Coppersmith's method, Elliptic Curve Method, Demytko's scheme.

1. Introduction

In 1976, Diffie and Hellman [6] invented the concept of the public-key cryptosystem. Since then, various schemes have been proposed as public-key cryptosystems.

In 1978, Rivest, Shamir, and Adleman [22] proposed RSA, the most widely used public-key cryptosystem. The public parameters in RSA are the modulus $N = pq$ and the public exponent e satisfying $\gcd(e, (p-1)(q-1)) = 1$ where p, q are large prime numbers of the same bit-size. The decryption exponent is the integer d such that $ed \equiv 1 \pmod{(p-1)(q-1)}$.

In 1985, Koblitz [13] and Miller [20] independently suggested the use of elliptic curves in cryptography, mainly for the Diffie-Hellman [6] key exchange protocol and the El Gamal cryptosystem [7]. Let $p > 3$ be a prime number and a, b be two integers such that $\gcd(4a^3+27b^2, p) = 1$. The elliptic curve $E_p(a,b)$ over the field $\mathbb{F}_p$ is the set of points $P = (x,y)$ such that $y^2 \equiv x^3 + ax + b \pmod{p}$ together with the point at infinity. The number of points in $E_p(a,b)$ is $\#E_p(a,b) = p + 1 - t_p$ where t_p is an integer satisfying the Hasse bound $|t_p| \leq 2\sqrt{p}$. Elliptic curves can be extended over the ring $\mathbb{Z}/n\mathbb{Z}$ where n is a composite integer. Such elliptic curves can serve to find small prime factors of n as in the Elliptic Curve Method (ECM) for factorization [15].

In 1994, Demytko [5] developed a cryptosystem using an elliptic curve $E_N(a,b)$ over the ring $\mathbb{Z}/N\mathbb{Z}$ where $N = pq$ is an RSA modulus. In the Demytko system, the public parameters are N, a, b together with a public exponent e satisfying $\gcd\left(e, \left(p^2 - t_p^2\right)\left(q^2 - t_q^2\right)\right) = 1$. The decryption exponent is an integer d satisfying $ed \equiv 1 \pmod{\text{lcm}(p+1 \pm t_p, q+1 \pm t_q)}$ where $t_p = p + 1 - \#E_p(a,b)$ and $t_q = q + 1 - \#E_q(a,b)$.

This paper was written while Emmanuel Fouotsa was spending a year in Caen financed by the French SIMPATIC (SIM and PAiring Theory for Information and Communications security), ANR-12-INSE-0014.

The RSA cryptosystem is deployed in many commercial systems for providing privacy and authenticity. If RSA is deployed in a device with small computing power, it is desirable to use a small public exponent e or a small private exponent d. Unfortunately, in 1990, Wiener [25] showed that RSA is insecure if $d < \frac{1}{3}N^{\frac{1}{4}}$. In 1999, Boneh and Durfee [3] improved this bound up to $d < N^{0.292}$. Their method is based on Coppersmith's method [4] for solving modular polynomial equations and uses the RSA key equation $ed - k(p-1)(q-1) = 1$. Afterwards, many attacks on RSA or variants of RSA have been presented using Coppersmith's method or other techniques (see [11], [19], [2]).

In this paper, using a variant RSA equation, we present a new attack on RSA by combining Coppersmith's method and the Elliptic Curve Method for factorization ECM. Let B be a positive integer. An integer n is said to be B-smooth if all prime factors are less than B. We say that B is an efficiency bound for ECM if every prime factor less than B of an integer n can be found by ECM.

Suppose that the public exponent $e = N^\beta$ satisfies a variant equation of the form $eu - (p-s)(q-r)v = w$ with suitably small unknown integers $0 < u < N^\delta$, $0 < v$, $|w| < N^\gamma$, $|r| < N^\alpha$ and $|s| < N^\alpha$ with $\alpha < \frac{1}{4}$. We show that the RSA modulus $N = pq$ can be factored under two conditions. The first condition is that $p - s$ is B-smooth for some efficiency bound B of ECM and the second condition is that δ satisfies the following inequality

$$\delta < \frac{7}{6} + \frac{1}{3}\alpha - \gamma - \frac{1}{3}\sqrt{(2\alpha+1)(2\alpha+6\beta-6\gamma+1)} - \varepsilon,$$

where ε is a small positive constant. Our method is based on combining Coppersmith's method and ECM. We use Coppersmith's method to find the small solutions $(u, v, w, (p-s)(q-r))$ of the equation $eu - (p-s)(q-r)v = w$ and ECM to factor $(p-s)(q-r)$ and to extract the value of $p - s$ from the B-smooth part of $(p-s)(q-r)$. Finally reusing Coppersmith's method, we can find p from the value of $p - s$.

We apply the new method to present a new attack on Demytko's scheme. In this scheme, the public exponent e and the private exponent d satisfy one of the four modular equations $ed \equiv 1 \pmod{\text{lcm}(p+1\pm t_p, q+1\pm t_q)}$. This gives rise to an equation of the form $eu - (p+1\pm t_p)(q+1\pm t_q)v = w$. Let $e = N^\beta$. Suppose that $|u| < N^\delta$, $0 < v$, $|w| < N^\gamma$, $|t_p| < N^\alpha$ and $|t_q| < N^\alpha$ with $\alpha < \frac{1}{4}$ and that $p + 1 \pm t_p$ or $q + 1 \pm t_q$ is B-smooth. Then applying the new method as for RSA, one can factor the RSA modulus $N = pq$.

The rest of this paper is organized as follows. In Section 2, we review Coppersmith's method, the theory of elliptic curves, Demytko's elliptic curve cryptosystem and the Elliptic Curve Method ECM for factorization. In Section 3, we present the new attack on RSA, and in Section 4, we present the new attack on Demytko's scheme. We conclude in Section 5.

2. Preliminaries

The following classical result is useful for the proof of our new attack (see [21]).

Lemma 2.1. *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Then*

$$\frac{\sqrt{2}}{2}\sqrt{N} < q < \sqrt{N} < p < \sqrt{2}\sqrt{N}.$$

2.1. Coppersmith's method

In 1996, Coppersmith [4] describes a technique to find small modular roots of univariate polynomials and small integer roots of bivariate polynomials. This method has been extended to more variables and has many surprising results in cryptanalysis. A typical example is the following result [18].

Theorem 2.2 (Coppersmith). *Let $N = pq$ be an RSA modulus with $q < p < 2q$. Let $\widetilde{S}$ be an approximation of an unknown multiple pr of p with $r \neq q$ and $|pr - \widetilde{S}| < N^{\frac{1}{4}}$. Then one can factor N in polynomial time.*

Let $h(x, y, z) \in \mathbb{Z}[x, y, z]$ be a polynomial with ω monomials of the form

$$h(x, y, z) = \sum_{i,j,k} a_{i,j,k} x^i y^j z^k.$$

The Euclidean norm of $h(x, y, z)$ is defined as

$$\|h(x, y, z)\| = \sqrt{\sum_{i,j,k} a_{i,j,k}^2}.$$

Under some conditions, a modular polynomial equation can be solved over the integers as presented in the following result [12].

Theorem 2.3 (Howgrave-Graham). *Let e be a positive integer and $h(x, y, z) \in \mathbb{Z}[x, y, z]$ be a polynomial with at most ω monomials. Suppose that*

$$h(x_0, y_0, z_0) \equiv 0 \pmod{e^m} \quad \textit{and} \quad \|h(xX, yY, zZ)\| < \frac{e^m}{\sqrt{\omega}},$$

where $|x_0| < X$, $|y_0| < Y$, $|z_0| < Z$. Then $h(x_0, y_0, z_0) = 0$ holds over the integers.

To find polynomials with small coefficients that can be used in Howgrave-Graham's Theorem 2.3, Coppersmith's method uses a lattice and a lattice reduction algorithm such as the LLL algorithm [16]. This reduction algorithm can be applied to find a basis of lattice vectors with relatively small norms (see [18]).

Theorem 2.4 (LLL). *Let $\mathcal{L}$ be a lattice spanned by a basis $(u_1, \ldots, u_\omega)$, then the LLL algorithm produces a new basis $(b_1, \ldots, b_\omega)$ satisfying*

$$\|b_1\| \leq \ldots \leq \|b_i\| \leq 2^{\frac{\omega(\omega-1)}{4(\omega+1-i)}} \det(\mathcal{L})^{\frac{1}{\omega+1-i}}, \quad i = 1, \ldots, \omega - 1.$$

Under the condition of Howgrave-Graham's Theorem, some modular polynomial equations derived from the reduced basis can be transformed to polynomial equations over the integers. For multivariate modular equations, solving the system of these polynomials is heuristic and depends on some extra assumptions such as the following one.

Assumption 1. Let $h_1, h_2, h_3 \in \mathbb{Z}[x, y, z]$ be the polynomials that are found by Coppersmith's method. Then the ideal generated by the polynomial equations $h_1(x, y, z) = 0$, $h_2(x, y, z) = 0$, $h_3(x, y, z) = 0$ has dimension zero.

Under this assumption, a system of polynomials sharing the root can be solved by using Gröbner basis computation or resultant techniques (see [1] for more details).

2.2. Elliptic curves

Let $N = pq$ be an RSA modulus and let a and b be two integers such that $\gcd(4a^3 + 27b^2, N) = 1$. An elliptic curve $E_N(a, b)$ is the set of points (x, y) such that

$$y^2 \equiv x^3 + ax + b \pmod{N},$$

together with the point at infinity $\mathcal{O}$. It is well known that chord-and-tangent method in the case of elliptic curves $E_p(a, b)$ defined over the finite filed $\mathbb{F}_p$ still hold for $E_n(a, b)$ unless the inversion of a non-zero number Q does not exist modulo N. This case would lead to find a factor of N by computing $\gcd(Q, N)$. When the prime factors p, q in $N = pq$ are large, then with overwhelming probability the inversion of a non-zero number will exist modulo N.

Let p be a prime number. Under modulo p, the cardinality of $E_p(a, b)$ is denoted $\#E_p(a, b)$ and satisfies the following result (see [24], p. 131).

Theorem 2.5 (Hasse). *The order of an elliptic curve $E_p(a, b)$ over $\mathbb{F}_p$ is given by*

$$\#E_p(a, b) = p + 1 - t_p, \quad \textit{where} \quad |t_p| \leq 2\sqrt{p}.$$

When the prime number p and the elliptic curve $E_p(a,b)$ are given, one can find the value of t_p using computational methods such the Schoof-Elkies-Atkin algorithm (SEA) (see [23]). Conversely, let p be a prime number and t an integer with $|t| < 2\sqrt{p}$. Let $H(d)$ denote the Kronecker class number (see Section 1.6 of [15]). Deuring's theory of CM-elliptic curves implies that there are $H(t^2-4p)$ elliptic curves on $\mathbb{Z}/p\mathbb{Z}$ having $p+1-t$ points. Note that when $|t| < \sqrt{p}$, $H(t^2-4p)$ satisfies the following inequalities (see Proposition 1.9 of [15])

$$c_1 \frac{\sqrt{p}}{\log p} < H(t^2-4p) < c_2 \sqrt{p} (\log p)(\log\log p)^2,$$

where c_1 and c_2 are effectively computable positive constants. This shows that the number of elliptic curves with known cardinality is non negligible.

Let p be a prime number and $E_p(a,b)$ be an elliptic curve with equation $y^2 \equiv x^3 + ax + b \pmod p$ and cardinality $\#E_p(a,b) = p+1-t_p$. The twist of $E_p(a,b)$ is the elliptic curve $E'_p(a,b)$ defined by the equation $cy^2 \equiv x^3+ax+b \pmod p$ where c is a fixed quadratic non-residue modulo p. Then the cardinality of $E'_p(a,b)$ is $\#E'_p(a,b) = p+1+t_p$.

2.3. Demytko's elliptic curve cryptosystem

In 1994, Demytko [5] proposed a new cryptosystem defined over the field $\mathbb{Z}/N\mathbb{Z}$ where $N=pq$ is an RSA modulus such that $p \equiv q \equiv 2 \pmod 3$. Demytko's scheme uses fixed integers a and b and a fixed modulus N. Demytko's scheme uses only the x-coordinate of a point $P=(x,y) \in E_N(a,b)$ to compute a multiple $eP \in E_N(a,b)$ (see Lemma 2 in [14]). Demytko's scheme can be summarized as follows.

1. **Key Generation:**
   - Choose two distinct prime numbers p and q of similar bit-length.
   - Compute $N=pq$.
   - Select two integers $a, b < p$ such that $\gcd\left(n, 4a^3+27b^2\right) = 1$.
   - Choose e such that $\gcd\left(e, \left(p^2-t_p^2\right)\left(q^2-t_q^2\right)\right) = 1$.
   - Keep p, q secret and publish N, e, a, b.
2. **Encryption:**
   - Transform the message m as the x-coordinate of a point $P=(m_x, m_y)$ on the elliptic curve $E_N(a,b)$.
   - Compute the ciphertext point $C = eP = (c_x, c_y) = e(m_x, m_y)$ on the elliptic curve $y^2 = x^3+ax+b \pmod N$.
3. **Decryption:**
   - Compute $u = c_x^3 + ac_x + b \pmod N$.
   - Compute the Legendre symbols $u_p = \left(\frac{u}{p}\right)$ and $u_q = \left(\frac{u}{q}\right)$.
   - If $(u_p, u_q) = (1,1)$, then compute $d \equiv e^{-1} \pmod{\text{lcm}(p+1-t_p, q+1-t_q)}$.
   - If $(u_p, u_q) = (1,-1)$, then compute $d \equiv e^{-1} \pmod{\text{lcm}(p+1-t_p, q+1+t_q)}$.
   - If $(u_p, u_q) = (-1,1)$, then compute $d \equiv e^{-1} \pmod{\text{lcm}(p+1+t_p, q+1-t_q)}$.
   - If $(u_p, u_q) = (-1,-1)$, then compute $d \equiv e^{-1} \pmod{\text{lcm}(p+1+t_p, q+1+t_q)}$.
   - Compute m as the x-coordinate of $dC = deP = P = (m_x, m_y)$ on the elliptic curve $y^2 = x^3+ax+b \pmod N$.

A variant of Demytko's scheme is to consider $d \equiv e^{-1} \pmod{(p+1\pm t_p, q+1\pm t_q)}$ instead of modulo $\text{lcm}(p+1\pm t_p, q+1\pm t_q)$. Then e and d satisfy an equation of the form

$$ed - k(p-s)(q-r) = 1, \quad s = \mp t_p - 1, \quad r = \mp t_q - 1.$$

This equation matches the RSA variant key equation that will be studied in this paper.

2.4. The Elliptic Curve Method

An integer m is said to be B-*smooth* if all the prime factors of m are less than or equal to B. Smooth numbers are used in cryptography by many factoring and discrete logarithm algorithms (see [15] and[17]). The counting function of B-smooth numbers in an interval $[1, x]$ is defined as

$$\psi(x, B) = \#\{m : 1 \leq m \leq x, m \text{ is } B\text{-smooth}\}.$$

In the particular case $x = B^u$, Hildebrand [10] gave the asymptotic formula $\psi(x, B) = x\rho(u)$ where $\rho(u)$ is the Dikman rho-function defined as the solution of the differential equation $u\rho'(u) = -\rho(u-1)$ for $u \geq 1$ with the initial condition $\rho(u) = 1$ for $0 \leq u \leq 1$. For $1 \leq u \leq 2$, the Dikman function satisfies $\rho(u) = 1 - \log u$ so that $\psi(x, B) = x(1 - \log u)$. The Elliptic Curve method (ECM) is a probabilistic method for integer factorization and was discovered by H.W. Lenstra [15] in 1987. It is a fast partially factoring algorithm, especially for finding small prime factors p, in a heuristic running time $\mathcal{O}\left(\exp\left(c(\log p)^{1/2}\right)\left(\log\log p\right)^{1/2}\right)\right)$, for some constant $c > 0$. The ECM algorithm is based on the property of the Chinese Remainder Theorem, that is, for any elliptic curve $E(a, b)$, if $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$, then

$$E(\mathbb{Z}/n\mathbb{Z}) = E(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times E(\mathbb{Z}/p_2^{e_2}\mathbb{Z}) \times \cdots \times E(\mathbb{Z}/p_k^{e_k}\mathbb{Z}).$$

Suppose that the order of $E(\mathbb{Z}/p_1^{e_1}\mathbb{Z})$ is B-smooth and let m be a multiple of $|E(\mathbb{Z}/p_1^{e_1}\mathbb{Z})|$, typically $m = \text{lcm}(2, \ldots, B)$. Then, for every $P \in E(\mathbb{Z}/n\mathbb{Z})$, we have $mP = (0 : 1 : 0) \pmod{p_1}$. Consequently, computing mP where $P \in E(\mathbb{Z}/n\mathbb{Z})$, using the addition formulas on $E(\mathbb{Z}/n\mathbb{Z})$, we must get $mP = (x : y : z) = (0 : 1 : 0) \pmod{p_1}$. This implies that $z \equiv 0 \pmod{p_1}$ and that $\gcd(z, n) = p_1^r$ for some positive integer r which will reveal p_1.

3. The Attack on RSA

In this section, we present an attack on RSA when the public key (N, e) satisfies an equation $eu - (p-s)(q-r)v = w$ with suitably small parameters u, v, w, r, s under the condition that one of the factors $(p-s)$ or $(q-r)$ is B-smooth for some ECM-efficiency bound B.

3.1. The attack

Theorem 3.1. *Let $N = pq$ be an RSA modulus and $e = N^\beta$ be a public exponent. Suppose that e satisfies the equation $eu - (p-s)(q-r)v = w$ with $|r|, |s| < N^\alpha < N^{\frac{1}{4}}$, $0 < u < N^\delta$, $0 < v$ and $|w| < N^\gamma$. If*

$$\delta < \frac{7}{6} + \frac{1}{3}\alpha - \gamma - \frac{1}{3}\sqrt{(2\alpha+1)(2\alpha+6\beta-6\gamma+1)} - \varepsilon,$$

where ε is a small positive constant, then, under assumption (1), one can find $(p-s)(q-r)$ in polynomial time.

Proof. Suppose that $N = pq$ is an RSA modulus and e is a public exponent satisfying $eu - (p-s)(q-r)v = w$. Since $(p-s)(q-r) = N - pr - qs + rs$, then $-v(N - pr - qs + rs) - w \equiv 0 \pmod{e}$, which can be rewritten as $v(pr+qs-rs) - Nv - w \equiv 0 \pmod{e}$. Consider the polynomial $f(x, y, z) = xy - Nx + z$, Then $(x, y, z) = (v, pr + qs - rs, -w)$ is a solution of the modular polynomial equation $f(x, y, z) \equiv 0 \pmod{e}$. The small solutions of this modular equation can be found by applying Coppersmith's method [4]. Let m and t be two positive integers. Consider the polynomials

$$\begin{aligned} G_{k,i_1,i_2,i_3}(x, y, z) &= x^{i_1-k}z^{i_3}f(x, y, z)^k e^{m-k}, \\ &\quad \text{for} \quad k = 0, \ldots m,\ i_1 = k, \ldots, m,\ i_2 = k,\ i_3 = m - i_1, \\ H_{k,i_1,i_2,i_3}(x, y, z) &= y^{i_2-k}z^{i_3}f(x, y, z)^k e^{m-k}, \\ &\quad \text{for} \quad k = 0, \ldots m,\ i_1 = k,\ i_2 = k+1, \ldots, i_1 + t,\ i_3 = m - i_1. \end{aligned}$$

Let $\mathcal{L}$ denote the lattice spanned by the coefficient vectors of the polynomials $G_{k,i_1,i_2,i_3}(Xx, Yy, Zz)$ and $H_{k,i_1,i_2,i_3}(Xx, Yy, Zz)$. We can get a left triangular matrix if the ordering of the rows follows the ordering of the k's and the ordering of the the monomials of a polynomial follows the natural ordering following the i_1's, then the i_2's, then the i_3's. Hence, using the triangular form of the matrix, the determinant of $\mathcal{L}$ is in the form $\det(\mathcal{L}) = e^{n_e} X^{n_X} Y^{n_Y} Z^{n_Z}$. For $m = 2$ and $t = 1$, the coefficient matrix for $\mathcal{L}$ is presented in Table 1. The non-zero elements are marked with an '$\circledast$'.

	z^3	xz^2	x^2z	x^3	xyz^2	x^2yz	x^3y	x^2y^2z	x^3y^2	x^3y^3	xy^2z^2	x^2y^3z	x^2yz	x^3y^4
G_{k,i_1,i_2,i_3}														
$G_{0,0,0,3}$	Z^3e^3	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,1,0,2}$	0	XZ^2e^3	0	0	0	0	0	0	0	0	0	0	0	0
$G_{0,2,0,1}$	0	0	X^2Ze^3	0	0	0	0	0	0	0	0	0	0	0
$G_{0,3,0,0}$	0	0	0	X^3	0	0	0	0	0	0	0	0	0	0
$G_{1,1,1,2}$	⊛	0	0	0	XYZ^2e^2	0	0	0	0	0	0	0	0	0
$G_{1,2,1,1}$	0	⊛	⊛	0	0	X^2YZe^2	0	0	0	0	0	0	0	0
$G_{1,3,1,0}$	0	0	⊛	⊛	0	0	X^3Ye^2	0	0	0	0	0	0	0
$G_{2,2,2,1}$	⊛	⊛	⊛	0	⊛	⊛	0	X^2Y^2Ze	0	0	0	0	0	0
$G_{2,3,2,0}$	0	⊛	⊛	⊛	0	⊛	⊛	0	X^3Y^2e	X^3Y^3	0	0	0	0
$G_{3,3,3,0}$	⊛	0	⊛	⊛	⊛	⊛	⊛	⊛	⊛	0	0	0	0	0
H_{k,i_1,i_2,i_3}														
$H_{0,0,1,3}$	0	0	0	0	⊛	0	0	0	0	⊛	$XY^2Z^2e^2$	0	0	0
$H_{1,1,2,2}$	0	0	0	0	⊛	⊛	0	⊛	0	0	⊛	X^2Y^3Ze	0	0
$H_{2,2,3,1}$	0	0	0	⊛	0	0	⊛	⊛	0	0	0	0	X^2YZe	0
$H_{3,3,4,0}$	0	0	0	0	⊛	0	0	⊛	⊛	0	0	0	0	X^3Y^4

TABLE 1. The coefficient matrix for the case $m = 2, t = 1$.

To find the values of the exponents, define $S(x)$ to be

$$S(x) = \sum_{k=0}^{m} \sum_{i_1=k}^{m} \sum_{i_2=k}^{k} \sum_{i_3=m-i_1}^{m-i_1} x + \sum_{k=0}^{m} \sum_{i_1=k}^{k} \sum_{i_2=k+1}^{i_1+t} \sum_{i_3=m-i_1}^{m-i_1} x.$$

Using the construction of the polynomials G and H, we get

$$\begin{aligned} n_e &= S(m-k) = \frac{1}{6}m(m+1)(2m+3t+4), \\ n_X &= S(i_1) = \frac{1}{6}m(m+1)(2m+3t+4), \\ n_Y &= S(i_2) = \frac{1}{6}(m+1)\left(m^2+3mt+3t^2+2m+3t\right), \\ n_Z &= S(i_3) = \frac{1}{6}m(m+1)(m+3t+2), \\ \omega &= S(1) = \frac{1}{2}(m+1)(m+2t+2). \end{aligned} \tag{1}$$

Let $t = \tau m$ for some positive τ to be optimized later. The dominant terms of the exponents in (1) are

$$\begin{aligned} n_e &\approx \frac{1}{6}(3\tau+2)m^3 + o(m^3), \\ n_X &\approx \frac{1}{6}(3\tau+2)m^3 + o(m^3), \\ n_Y &\approx \frac{1}{6}\left(3\tau^2+3\tau+1\right)m^3 + o(m^3), \\ n_Z &\approx \frac{1}{6}(3\tau+1)m^3 + o(m^3), \\ w &\approx \frac{1}{6}(6\tau+3)m^2 + o(m^2). \end{aligned} \tag{2}$$

Applying the LLL algorithm 2.4 to the lattice $\mathcal{L}$, we get a reduced basis where the three first vectors h_i, $i = 1, 2, 3$ satisfy

$$\|h_1\| \le \|h_2\| \le \|h_3\| \le 2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(\mathcal{L})^{\frac{1}{\omega-2}}.$$

To apply Howgrave-Graham's Theorem 2.3 to h_1, h_2 and h_3, we set

$$2^{\frac{\omega(\omega-1)}{4(\omega-2)}} \det(\mathcal{L})^{\frac{1}{\omega-2}} < \frac{e^m}{\sqrt{\omega}}.$$

This can be transformed to

$$\det(\mathcal{L}) < 2^{-\frac{\omega(\omega-1)}{4}} \frac{1}{(\sqrt{\omega})^{\omega-2}} e^{m(\omega-2)},$$

or equivalently

$$e^{n_e} X^{n_X} Y^{n_Y} Z^{n_Z} < 2^{-\frac{\omega(\omega-1)}{4}} \frac{1}{(\sqrt{\omega})^{\omega-2}} e^{m(\omega-2)}. \tag{3}$$

Suppose that $e = N^\beta$, $0 < u < N^\delta$, $|w| < N^\gamma$ and $\max(|r|, |s|) < N^\alpha < N^{\frac{1}{4}}$. Since $q < p < \sqrt{2}\sqrt{N}$ by Lemma 2.1, then

$$p|r + q|s + |rs| < 3\max(p|r|, q|s|, |rs|) < 3\max\left(\sqrt{2}\sqrt{N} \cdot N^\alpha, N^{2\alpha}\right) = 3\sqrt{2}N^{\frac{1}{2}+\alpha}.$$

This gives

$$(p-r)(q-s) = N - pr - qs + rs > N - (p|r + q|s + |rs|) > N - 3\sqrt{2}N^{\frac{1}{2}+\alpha} > \frac{1}{2}N.$$

Using $0 < v$ and $|w| < eu < N^{\beta+\delta}$, we get

$$0 < v = \frac{eu - w}{(p-s)(q-r)} < \frac{eu + |w|}{(p-s)(q-r)} < \frac{2eu}{\frac{1}{2}N} < 4N^{\beta+\delta-1}, \tag{4}$$

Let $X = 4N^{\beta+\delta-1}$, $Y = 3\sqrt{2}N^{\frac{1}{2}+\alpha}$ and $Z = N^{\gamma}$. Then the target solution (x, y, z) satisfies $|x| < X$, $|y| < Y$ and $|z| < Z$. Using the approximations of n_e, n_X, n_Y, n_Z and ω given in (2), the inequality (3) can be transformed into

$$(3\tau+2)\beta + (3\tau+2)(\beta+\delta-1) + \left(3\tau^2+3\tau+1\right)\left(\frac{1}{2}+\alpha\right) + (3\tau+1)\gamma < (6\tau+3)\beta - \varepsilon_1,$$

where ε_1 collects all constant terms in e, X, Y and Z. It is a small positive constant that depends only on N. The optimal value for τ is

$$\tau_0 = \frac{1 - 2\delta - 2\alpha - 2\gamma}{2(1+2\alpha)},$$

and, plugging this value in the former inequality, we obtain

$$4\alpha^2 + 16\alpha\beta + 8\alpha\delta - 8\alpha\gamma - 12\delta^2 - 24\delta\gamma - 12\gamma^2 - 4\alpha + 8\beta + 28\delta + 20\gamma - 15 < -\varepsilon_2,$$

where ε_2 is another small positive constant. The former equation is valid for

$$\delta < \frac{7}{6} + \frac{1}{3}\alpha - \gamma - \frac{1}{3}\sqrt{(2\alpha+1)(2\alpha+6\beta-6\gamma+1)} - \varepsilon,$$

where ε is a small positive constant. Under this condition, the LLL algorithm applied to the lattice $\mathcal{L}$ outputs three vectors v_i, $i = 1, 2, 3$. These vectors represent the coefficients of three polynomials $h_i(Xx, Yy, Zz)$, $i = 1, 2, 3$ sharing the root $(x, y, z) = (v, pr + qs + rs, -w)$. Then, applying Gröbner basis computations, we get the expected solution, from which we deduce $(p-s)(q-r) = N - (pr + qs + rs)$. Since all the former steps can be done in polynomial time, then the method is a polynomial time algorithm. This terminates the proof. □

Remark. If $r = s = w = 1$, then the equation $eu - (p-s)(q-r)v = w$ is the classical RSA key equation $ed - (p-1)(q-1)k = 1$ with $d < N^{\delta}$. Using $\alpha = 0$, $\beta = 1$ and $\gamma = 0$, the bound of Theorem 3.1 gives $\delta < \frac{7}{6} - \frac{\sqrt{7}}{3}$. This retrieves the classical bound on the private exponent d (see [3]).

Theorem 3.2. *Let $N = pq$ be an RSA modulus and $e = N^{\beta}$ be a public exponent. Suppose that e satisfies the equation $eu - (p-s)(q-r)v = w$ with $|r|, |s| < N^{\alpha} < N^{\frac{1}{4}}$, $0 < u < N^{\delta}$, $0 < v$ and $|w| < N^{\gamma}$. Let B be an ECM-efficiency bound for the Elliptic Curve Method. If $(p-s)$ or $(q-r)$ is B-smooth and*

$$\delta < \frac{7}{6} + \frac{1}{3}\alpha - \gamma - \frac{1}{3}\sqrt{(2\alpha+1)(2\alpha+6\beta-6\gamma+1)} - \varepsilon,$$

then, under assumption (1), one can find p and q in polynomial time.

Proof. Suppose that, in the equation $eu - (p-s)(q-r)v = w$, the parameters satisfy $|r|, |s| < N^{\alpha} < N^{\frac{1}{4}}$, $e = N^{\beta}$, $0 < u < N^{\delta}$, $< v$, $|w| < N^{\gamma}$ and that the exponent parameters satisfy $\delta < \frac{7}{6} + \frac{1}{3}\alpha - \gamma - \frac{1}{3}\sqrt{(2\alpha+1)(2\alpha+6\beta-6\gamma+1)} - \varepsilon$. Then, by applying Theorem 3.1, we can find the exact value of $(p-s)(q-r)$. Next, suppose that $(p-s)$ is B-smooth where B is a bound for the efficiency of the Elliptic Curve Method (ECM). Hence, ECM will reveal a partial factorization of $(p-s)(q-r)$ as

$$(p-s)(q-r) = M \cdot \prod_{i=1}^{\omega((p-s)(q-r))} p_i^{e_i},$$

were $\omega((p-s)(q-r)$ is the number of distinct prime factors of $(p-s)(q-r)$ less than B and M is such that $M = 1$ or all prime factors of M are greater than B. The average order of the number

of prime factors of an integer n is $\omega(n) \approx \frac{\log n}{\log\log n}$ (see [9], pp. 355). Since $|r|, |s| < N^\alpha$ and $\sqrt{N} < p < \sqrt{2N}$, then

$$\left(\sqrt{N} - N^\alpha\right)^2 < (p-s)(q-r) < \left(\sqrt{2N} + N^\alpha\right)^2. \tag{5}$$

Hence, the average number of the prime factors of $(p-s)(q-r)$ satisfies

$$\omega((p-s)(q-r) \approx \frac{\log((p-s)(q-r))}{\log\log((p-s)(q-r))} \approx \frac{\log N}{\log\log N}.$$

On the other hand, according to the factorization

$$(p-s) = \prod_{i=1}^{\omega((p-s))} p_i^{e_i},$$

the number of distinct divisors of $p-s$ is exactly $\prod_{i=1}^{\omega(p-s)}(e_i+1)$. However, the average number of divisors of an integer n is $\log n$ (see Theorem 319 of [9]). Hence, the average number of divisors of $p-s$ is approximately $\log(p-s) \approx \frac{1}{2}\log N$. Let d be a divisor of $(p-s)(q-r)$ such that $d = p-s$. Then

$$d = \prod_{i=1}^{\omega(p-s)} p_i^{x_i}, \quad 0 \le x_i \le e_i.$$

Using (5), we get

$$\log\left(\sqrt{N} - N^\alpha\right) < \sum_{i=1}^{\omega(p-s)} x_i \log p_i < \log\left(\sqrt{2N} + N^\alpha\right).$$

The former inequalities can be solved by applying linear programming algorithms such as PSLQ [8] and LLL [16], and using a solution $(x_1, \ldots, x_{\omega(p-s)})$, we compute $d = \prod_{i=1}^{\omega(p-s)} p_i^{x_i}$ which is then a candidate for $p-s$. Since $|s| < N^\alpha < N^{\frac{1}{4}}$, then d is an approximation of the prime factor p of N with an error term less than $N^{\frac{1}{4}}$. Hence, using Theorem 2.2, this leads to the exact value of p if d is the good candidate. Repeating this process sequentially for the factors d of $(p-s)(q-r)$ in the range $\sqrt{N} - N^\alpha < d < \sqrt{2N} + N^\alpha$, we will find p and then get $q = \frac{N}{p}$. This achieves the factorization of the RSA modulus. □

3.2. A numerical example for RSA

We experimented our method with various sizes. In all cases, the assumption (1) was true and the method was successful to find the factorization of the RSA modulus.

As a numerical example, consider the following RSA 265 bit-size modulus N with the public exponent e,

$$\begin{aligned} N =& 43115265506687226436196728756959707266402158394261294759458139430520129183826747, \\ e =& 44291096833783216353731643543595440193954966593379368311328977066819711783511 39. \end{aligned}$$

Suppose that $N = pq$ with unknown factorization and e satisfies an equation $eu - (p-s)(q-r)v = w$ with the suitably small unknown parameters u, v, w, r and s. Then applying the method of Theorem 3.1 to solve the equation $eu - (p-s)(q-r)v = w$, with the bounds

$$u < N^\delta = N^{0.15},\ |w| < N^\gamma = N^{0.15},\ |r|, |s| < N^\alpha = N^{0.15},\ e = N^\beta = N^{0.987},$$

we get

$$\begin{aligned} v =& 8330878683394 \\ w =& 2516643, \\ ps + qr - rs =& 4562410349945334671522563904482968894145365714 7, \end{aligned}$$

Since $(p-s)(q-r) = N - (pr + qs - rs)$, we get

$$\begin{aligned} (p-s)(q-r) =& 4311526550668722643619672875695966164229865894091457953 \\ & 38190945108311877301696 00. \end{aligned}$$

Then, using the Elliptic Curve Method with the bound $B = N^{\frac{1}{10}} \approx 91931238$, we get the factorization

$$\begin{aligned} (p-s)(q-r) = & 2^8 \cdot 3 \cdot 5^2 \cdot 13 \cdot 23 \cdot 53 \cdot 89 \cdot 181 \cdot 1663 \cdot 2833 \cdot 2969 \cdot 5197 \cdot 5233 \cdot \\ & 6481 \cdot 12007 \cdot 18439 \cdot 36973 \cdot 435876180528100336114933071348569. \end{aligned}$$

Using the factorization of $(p-s)(q-r)$, we can find the set of the factors d such that $\sqrt{N} - N^{\alpha} < d < \sqrt{2N} + N^{\alpha}$. Such divisors are candidate for $p - s$, that is $p - s = d$ for one of these factors. Then by applying Coppersmith's Theorem 2.2, we can find p using the correct candidate. For the divisor $d = 667222401466234017857972147432672818 5600$, we apply Coppersmith's Theorem 2.2 and find $p = 667222401466234017857972147432673415 2749$. Then $q = \frac{N}{p} = 646190316930915448383379701178588650 6503$.

4. Application to Demytko's Scheme

In this section, we show how to apply the technique of Theorem 3.1 and Theorem 3.2 to break the Demytko scheme in some situations and provide a numerical example.

4.1. The attack on Demytko's Scheme

In Demytko's scheme, the RSA modulus is $N = pq$ and the elliptic curve $E_N(a, b)$ is such that $\#E_p(a, b) = p+1-t_p$ and $\#E_q(a, b) = q+1-t_q$ where, according to Hasse Theorem, $|t_p| < 2\sqrt{p}$ and $|t_q| < 2\sqrt{q}$. Also, the public exponent e and the private exponent d satisfy one of the four equations

$$eu - (p + 1 \pm t_p)(q + 1 \pm t_q)v = w.$$

These equations can be transformed into one of the form $eu-(p-s)(q-r)v = w$ where $s = \mp t_p - 1$ and $t = \mp t_q - 1$, which can be studied using the technique of Theorem 3.1 and Theorem 3.2.

Corollary 4.1. *Let (N, e, a, b) the public parameters of a Demytko's instance where $N = pq$. Suppose that $e = N^{\beta}$ satisfies an equation of the form $eu - (p + 1 \pm t_p)(q + 1 \pm t_q)v = w$ with $| \pm t_p - 1|, | \pm t_q - 1| < N^{\alpha} < N^{\frac{1}{4}}$, $0 < u < N^{\delta}$, $< v$ and $|w| < N^{\gamma}$. Let B be an ECM-efficiency bound for the Elliptic Curve Method. If $p + 1 \pm t_p$ or $q + 1 \pm t_q$ is B-smooth and*

$$\delta < \frac{7}{6} + \frac{1}{3}\alpha - \gamma - \frac{1}{3}\sqrt{(2\alpha + 1)(2\alpha + 6\beta - 6\gamma + 1)} - \varepsilon,$$

then, under assumption (1), one can find p and q in polynomial time.

Proof. Since the equation $eu - (p + 1 \pm t_p)(q + 1 \pm t_q)v = w$ can be transformed into $eu - (p - s)(q - r)v = w$ with $s = \mp t_p - 1$ and $t = \mp t_q - 1$, then this equation can be solved under the conditions of Theorem 3.1 and Theorem 3.2 when $|t_p - 1| < N^{\alpha}$ and $|t_q - 1| < N^{\alpha}$. □

4.2. A numerical example for Demytko

Let us consider the Demytko public parameters (N, e, a, b) where N is an 510-bit RSA modulus

$$\begin{aligned}
N =&244564152049718837289391032953867582433145492152016390042656239363441852689757568224991629341622126967445954070062427486023623868460973836075181541009161 7,\\
e =&207753540686843587408555602893982678168821441852165899252123932416370824148707563812033872059010473801740084336709522813588017197501164099322578137710783,\\
a =&0,\\
b =&9,
\end{aligned}$$

with the elliptic curve $E_N(a, b)$ with equation $y^2 \equiv x^3 + 9 \pmod N$. We suppose that e satisfies the equation $eu - (p + 1 \pm t_p)(q + 1 \pm t_q)v = w$ with $t_p, t_q < N^\alpha = N^{0.1}$. Then applying the method of Theorem 3.1 to solve the equation $eu - (p - s)(q - r)v = w$ where $s = \mp t_p - 1$ and $r = \mp t_p - 1$, we get for $e = N^\beta \approx N$, $u < N^\delta = N^{0.1}$, $|w| < N^\gamma = N^{0.1}$

$$\begin{aligned}
v =&6889077569105,\\
w =&2916646,\\
pr + qs - rs =&784357999339618220094311636350013903165826707133763 3,\\
&244222164466922717093026565590439040792,
\end{aligned}$$

Then

$$\begin{aligned}
&N - (pr + qs - rs) = (p - s)(q - r)\\
&= 244564152049718837289391032953867582433145492152016\\
&\quad 390042656238579083853350139348130679992991608223801 6\\
&\quad 192469362991030638071771761892645334186224971050825.
\end{aligned}$$

Applying the Elliptic Curve Method for factorization with the bound $B = 2^{80} \approx N^{0.16}$, we get the factorization

$$\begin{aligned}
(p - s)(q - r) =&3^6 \cdot 5^2 \cdot 7^2 \cdot 13^3 \cdot 43^2 \cdot 103^2 \cdot 277 \cdot 674^2 \cdot 1021 \cdot 4177 \cdot 15061\\
&\cdot 21737^2 \cdot 27109^2 \cdot 52291^2 \cdot 84991 \cdot 90841 \cdot 132661 \cdot 347329^2\\
&\cdot 3834631 \cdot 29327821 \cdot 69689551 \cdot 30404961633073956301\\
&\cdot 30519653713567559160549 1.
\end{aligned}$$

Any divisor d of $(p - s)(q - r)$ is a candidate for $p - s$ or $q - r$. Using the divisor

$$\begin{aligned}
d =&3^3 \cdot 13^2 \cdot 277 \cdot 1021 \cdot 15061 \cdot 21737^2 \cdot 27109^2 \cdot 52291^2 \cdot 90841\\
&\cdot 30519653713567559160549 1,
\end{aligned}$$

as a candidate for $p - s$ in Coppersmith's Theorem 2.2, we get p and then $q = \frac{N}{p}$ as follows

$$\begin{aligned}
p =&685920425598306143251778583414905266471238279458502857 5\\
&98279318189925533951 71,\\
q =&356548869114654893865594787391255957316985729824840925 8\\
&028717586055707648202 7,
\end{aligned}$$

which completes the factorization of N.

5. Conclusion

In this paper, we consider an instance of RSA where the public exponent satisfies a generalized key equation with many unknown parameters. Under suitable conditions, we combine Coppersmith's method and the Elliptic Curve Method for factorization ECM, we solve the equation and find the prime factors of the RSA modulus. We apply the same technique to launch an attack on Demytko's Elliptic Curve Cryptosystem when the secret parameters are suitably small.

References

[1] Bauer, A. and Joux, A.: Toward a rigorous variation of Coppersmith's algorithm on three variables. In Proceedings of Eurocrypt'07, volume 4515 of Lecture Notes in Computer Science, Springer-Verlag, pp. 361–378 (2007)

[2] Blömer, J., May, A.: A generalized Wiener attack on RSA. In Public Key Cryptography - PKC 2004, volume 2947 of Lecture Notes in Computer Science, Springer-Verlag, pp. 1–13 (2004)

[3] Boneh, D., Durfee, G.: Cryptanalysis of RSA with private key d less than $N^{0.292}$, Advances in Cryptology-Eurocrypt'99, Lecture Notes in Computer Science Vol. 1592, Springer-Verlag, pp. 1–11 (1999)

[4] Coppersmith, D.: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology, 10(4), pp. 233–260 (1997)

[5] Demytko, N.: A new elliptic curve based analogue of RSA, in T. Helleseth (ed.), EUROCRYPT 1993, Lecture Notes in Computer Science 765, Springer-Verlag, pp. 40–49 (1994)

[6] Diffie, W., Hellman, M.E.: New directions in cryptography, IEEE Transactions on Information Theory, Vol. IT–22, 1976, pp. 644–654 (1976)

[7] El Gamal, T.: A public key cryptosystem and signature scheme based on discrete logarithms. IEEE Transactions on Information Theory IT-31, 496-473 (1985)

[8] Ferguson, H.R.P., Bailey, D.H.: A polynomial time, numerically stable integer relation algorithm. RNR Technical Report RNR-91-032, NASA Ames Research Center, Moffett Field, CA. December (1991)

[9] Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Oxford University Press, London (1975)

[10] Hildebrand, A.: On the number of positive integers $\leq x$ and free of prime factors $\leq y$, J. Number Theory, 22 (1986), pp. 289–307 (1986)

[11] Hinek, M.J.: Cryptanalysis of RSA and its variants. Chapman & Hall/CRC Cryptography and Network Security. CRC Press, Boca Raton, FL, (2010)

[12] Howgrave-Graham, N.: Finding small roots of univariate modular equations revisited, In Cryptography and Coding, LNCS 1355, pp. 131-142, Springer-Verlag (1997)

[13] Koblitz, N.: Elliptic curve cryptosystems. Mathematics of Computation, 48: pp. 203–209, (1987)

[14] Kurosawa, K., Okada, K., Tsujii, S.: Low exponent attack against elliptic curve RSA, Low exponent attack against elliptic curve RSA. Inform. Process. Lett. 53, no. 2, pp. 7783 (1995)

[15] Lenstra, H.: Factoring integers with elliptic curves, Annals of Mathematics, Vol. 126, pp. 649–673 (1987)

[16] Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients, Mathematische Annalen, Vol. 261, pp. 513–534, (1982)

[17] Lenstra, A.K., Lenstra, H.W. Jr. (eds.): The Development of the Number Field Sieve, Lecture Notes in Mathematics, vol. 1554, Berlin, Springer-Verlag, (1993)

[18] May, A.: New RSA Vulnerabilities using Lattics Reduction Methods, Ph.D. Dissertation. University of Paderborn, (2003)

[19] May A.: Using LLL-reduction for solving RSA and factorization problems: a survey. In: LLL+25 Conference in Honour of the 25th Birthday of the LLL Algorithm. Springer, Berlin, Heidelberg (2007)

[20] Miller, V.S.: Use of elliptic curves in cryptography. In H. C. Williams, editor, Advances in Cryptology - CRYPTO'85, Vol. 218 of Lecture Notes in Computer Science, Springer-Verlag, pp. 417–426 (1986)

[21] Nitaj, A.: Another generalization of Wiener's attack on RSA, in Vaudenay, S. (ed.) Africacrypt 2008. Lecture Notes in Computer Science, Springer-Verlag Vol. 5023, pp. 174–190 (2008)

[22] Rivest, R., Shamir, A., Adleman, L.: A Method for Obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21 (2), pp. 120–126 (1978)

[23] Schoof, R.: Counting points on elliptic curves over finite fields, Journal de Théorie des Nombres de Bordeaux, 7(1):219254, (1995)

[24] Silverman, J.H.: The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, Springer-Verlag, 106 (1986)

[25] Wiener, M.: Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory, Vol. 36, pp. 553–558 (1990)

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

Emmanuel Fouotsa
Laboratoire de Mathématiques Nicolas Oresme
Université de Caen Basse Normandie, France
and University of Bamenda, Cameroun
e-mail: emmanuel.fouotsa@unicaen.fr