Improved Cryptanalysis of the KMOV Elliptic Curve Cryptosystem

Abderrahmane Nitaj[1], Willy Susilo[2], and Joseph Tonien[2]

[1] LMNO, Université de Caen Normandie, France
abderrahmane.nitaj@unicaen.fr
[2] Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Australia
{willy.susilo,joseph.tonien}@uow.edu.au

Abstract. This paper presents two new improved attacks on the KMOV cryptosystem. KMOV is an encryption algorithm based on elliptic curves over the ring $\mathbb{Z}_N$ where $N = pq$ is a product of two large primes of equal bit size. The first attack uses the properties of the convergents of the continued fraction expansion of a specific value derived from the KMOV public key. The second attack is based on Coppersmith's method for finding small solutions of a multivariate polynomial modular equation. Both attacks improve the existing attacks on the KMOV cryptosystem.

1 Introduction

The RSA cryptosystem [21], invented in 1978 by Rivest, Shamir and Adleman, is the most widely used cryptosystem. The main parameters in RSA are two integers, the RSA modulus $N = pq$ where p and q are large prime numbers, and the public exponent e, which is an integer satisfying $\gcd(e, (p-1)(q-1)) = 1$. The private exponent is the integer d satisfying $ed \equiv 1 \pmod{(p-1)(q-1)}$. In many implementations, the private exponent d is required to be small to ease decryption and signature. Unfortunately, this scenario is dangerous and can be used to break the system [3,6]. In 1990, Wiener [25,24] presented an attack to break the RSA system if the private exponent d satisfies $d < \frac{1}{\sqrt[4]{18}} N^{\frac{1}{4}}$. Since then, Wiener's bound has been extended in many situations, mainly by Boneh and Durfee [2] to $d < N^{0.292}$.

In 1985, Miller [17] and Koblitz [13] independently proposed to use elliptic curves in cryptography. Since then, many cryptosystems have been proposed based on elliptic curves. In the direction of RSA, Koyama, Maurer, Okamoto and Vanstone [14] proposed a cryptosystem, called KMOV, based on the elliptic curve $E_N(0, b)$ where $N = pq$ is an RSA modulus and $E_N(0, b)$ is the set of solutions of the modular equation $y^2 \equiv x^3 + b \pmod N$, together with the point at infinity, denoted $\mathcal{O}$. When the prime factors p and q are such that $p \equiv q \equiv 2 \pmod 3$, then any point $P \in E_N(0, b)$ satisfies $(p+1)(q+1)P = \mathcal{O}$. In KMOV, the public key is a pair (N, e) where $N = pq$ with two prime integers satisfying $p \equiv q \equiv 2 \pmod 3$ and e is an integer satisfying $\gcd(e, (p+1)(q+1)) = 1$. The decryption exponent is the integer d such that $ed \equiv 1 \pmod{(p+1)(q+1)}$.

Notice that the modular equation $ed \equiv 1 \pmod{(p+1)(q+1)}$ is equivalent to the integer key equation $ed-k(p+1)(q+1)=1$. In 1995, Pinch [20] used the key equation and extended Wiener's attack to KMOV. He showed that one can factor the modulus $N=pq$ if $d<\frac{1}{3}N^{\frac{1}{4}}$. In [11], Ibrahimpasic extended the attack of Pinch by a few bits using an exhaustive search. Both attacks use the convergents of the continued fraction expansion of $\frac{e}{N}$. In [18], Nitaj considered the generalized equation $eu-(p+1)(q+1)v=w$ and showed that one can factor the modulus $N=pq$ if the parameters u, v, w satisfy some specific conditions, especially if $uv<\frac{\sqrt{2}\sqrt{N}}{12}$. The method combines the continued fraction algorithm [4,7] and Coppersmith's method [8] for solving univariate modular equations.

In this paper, we extend the former attacks on KMOV. In the first attack we consider the KMOV key equation $ed-k(p+1)(q+1)=1$ and instead of using the convergents of $\frac{e}{N}$, we use the convergents of $\frac{e}{N+1+\left(1+\frac{3\sqrt{2}}{4}\right)N^{\frac{1}{2}}}$. As a consequence, we show that one can factor the modulus $N=pq$ if the private exponent d is such that $d<2\sqrt{2}\frac{N^{\frac{3}{4}}}{\sqrt{e}}$. This bound improves the former bound $d<\frac{1}{3}N^{\frac{1}{4}}$, especially when the public exponent e is significantly smaller then N.

In the second attack we consider the generalized key equation $eu-(p+1)(q+1)v=w$ and transform it to the modular polynomial equation $v(p+q+1)+Nv+w\equiv 0 \pmod{e}$. We consider the polynomial $f(x,y,z)=xy+Nx+z$ and apply Coppersmith's method to find the small solutions of the modular polynomial equation $f(x,y,z)\equiv 0 \pmod{e}$. When $e=N^{\beta}$, $u<N^{\delta}$ and $|w|<N^{\gamma}$, if

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

where ε is a small constant, then Coppersmith's method enables us to find $p+q+1$, which combined with $N=pq$ gives p and q. We note that in the standard situation of a KMOV instance with $e\approx N$ and $eu-(p+1)(q+1)v=1$, our new bound is $\delta<0.284$ which is much larger than the existing bounds.

The rest of this paper is organized as follows. In Section 2, we give some preliminaries on Coppersmith's method, continued fractions, elliptic curves and recall the KMOV cryptosystem. In Section 3, we present our first attack on KMOV based on continued fractions. In Section 4, we present our second attack on KMOV which is based on Coppersmith's method. We conclude the paper in Section 5.

2 Preliminaries

In this section, we give some preliminaries on Coppersmith's methods for solving modular polynomial equations, continued fractions and elliptic elliptic curves. For completeness, we recall the KMOV cryptosystem.

2.1 Coppersmith's method

One of the difficult problems in algebra is to solve modular polynomial equations of the form

$$f(x_1,\dots,x_n) \equiv 0 \pmod{e},$$

where $f(x_1,\dots,x_n) \in \mathbb{Z}[x_1,\dots,x_n]$ is multivariate polynomial. In 1996, Coppersmith [8] introduced a rigorous method for finding the small solutions of the univariate polynomial equation $f(x) \equiv 0 \pmod{e}$ and the small roots of the bivariate polynomial equation $f(x,y) = 0$. Coppersmith's method is based on lattice reduction and is useful in cryptography, especially for attacking the RSA cryptosystem (see [16,5,1,19]). Since then, numerous variants of Coppersmith's method have been presented for multivariate polynomial equations assuming certain hypothesis. The following result of Howgrave-Graham [10] is useful for solving the polynomial equations.

Theorem 1 (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. Let m be a positive integer. Suppose that*

$$h\left(x_0,y_0,z_0\right) \equiv 0 \pmod{e^m} \quad \textit{and}$$
$$\|h(xX,yY,zZ)\| = \sqrt{\sum_{i,j,k} a_{i,j,k} x^i y^j z^k} < \frac{e^m}{\sqrt{\omega}},$$

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

For a multivariate polynomial modular equation $f(x,y,z) \equiv 0 \pmod{e}$, the idea in Coppersmith's method is to build certain modular polynomials equations $h(x,y,z) \equiv 0 \pmod{e^m}$ sharing the modular solution (x_0,y_0,z_0). These polynomials are generally built by applying Jochemz-May [12] method and applying lattice reduction techniques such as the LLL algorithm [15]. The LLL algorithm acts on lattices and the following result is useful (see [15,16,12]).

Theorem 2 (LLL). *Let $\mathcal{L}$ be a lattice spanned by a basis $(u_1,\dots,u_\omega)$, then the LLL algorithm produces a new basis $(b_1,\dots,b_\omega)$ satisfying*

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

To find the root (x_0,y_0,z_0), we use a system with three polynomial equations $h_i(x,y,z) = 0$, $i = 1,2,3$. By using Gröbner basis computation or resultant techniques, the system can be solved under the following widely believed assumption.

Assumption 1 *The polynomials $h_1,h_2,h_3 \in \mathbb{Z}[x,y,z]$ that are derived from the reduced basis of the lattice in Coppersmith's method are algebraically independent.*

2.2 Continued fractions

Let $\xi \neq 0$ be real number. The continued fraction expansion of ξ is an expression of the form

$$\xi = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}},$$

where a_0 is an integer and for $i \geq 1$, a_i is a positive integer. The integers a_i, $i \geq 0$ are the partial quotients of the continued fraction expansion. The process to compute the integers a_i for $i \geq 0$ is the continued fraction algorithm. The starting term is $x_0 = \xi$ and for $i \geq 0$,

$$a_i = \lfloor x_i \rfloor, \; x_{i+1} = \frac{1}{x_i - a_i}.$$

When the continued fraction expansion is used with the first $k+1$ partial quotients, the fraction is a convergent. The following method is very useful for computing the convergents of ξ.

Theorem 3. *The k^{th} convergent can be determined as $[a_0, \ldots, a_k] = \frac{p_k}{q_k}$, where the sequences $\{p_n\}$ and $\{q_n\}$ are specified as follows*[3]*:*

$$\begin{aligned} p_{-2} &= 0, \quad p_{-1} = 1, \quad p_n = a_n p_{n-1} + p_{n-2}, \quad \forall n \geq 0, \\ q_{-2} &= 1, \quad q_{-1} = 0, \quad q_n = a_n q_{n-1} + q_{n-2}, \quad \forall n \geq 0. \end{aligned}$$

There are many properties related to the theory of continued fractions. One of the most important results is Legendre's Theorem (see Theorem 184 of [9]).

Theorem 4. *Let $\xi \neq 0$ be a real number and a, b be two positive integers such that $\frac{a}{b} \notin \mathbb{N}$ and $(a, b) = 1$. If*

$$0 < \left| \xi - \frac{a}{b} \right| < \frac{1}{2b^2}$$

then $\frac{a}{b}$ is a convergent of the continued fraction of ξ.

Note that computing a convergent $\frac{a}{b}$ of ξ with the continued fraction algorithm is done in polynomial time in $\log(b)$.

2.3 Elliptic curves

Let $p \geq 5$ be a prime number and a and b two integers satisfying $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$. An elliptic curve $E_p(a, b)$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the set of solutions $(x, y) \in \mathbb{F}_p^2$ satisfying the equation

$$E_p(a, b) : \quad y^2 \equiv x^3 + ax + b \pmod{p}, \tag{1}$$

[3] The convergents start with $\frac{p_0}{q_0}$, but it is a convention to extend the sequence index to -1 and -2 to allow the recursive formula to hold for $n = 0$ and $n = 1$

together with a point $\mathcal{O}$, called the point at infinity. If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are two points, then one have the following properties.

- $P_1 + \mathcal{O} = \mathcal{O} + P_1 = P_1$.
- The opposite of P_1 is $-P_1 = (x_1, -y_1)$.
- If $P_2 = -P_1$, then $P_1 + P_2 = \mathcal{O}$.
- If $P_2 \neq -P_1$, then $P_1 + P_2 = P_3 = (x_3, y_3)$ where

$$x_3 \equiv \lambda^2 - x_1 - x_2 \pmod p, \quad y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod p,$$

with

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2, \\ \\ \dfrac{3x_1^2 + a}{2y_1} & \text{if } x_1 = x_2. \end{cases}$$

With the former addition law, the set $E_p(a, b)$ is a group of finite order $\#E_p(a, b)$ where $\#E_p(a, b)$ is the number of solutions $(x, y) \in \mathbb{F}_p^2$ of the equation (1) together with the point at infinity. According to a famous Theorem of Hasse (see [23], Chapter 5), we have $\#E_p(a, b) = p + 1 - t_p$, with $|t_p| < 2\sqrt{p}$, which is close to $p + 1$, up to a small value t_p.

For specific values of p, $\#E_p(a, b)$ can be explicitly computed as for $p \equiv 2 \pmod 3$ (see [22]).

Theorem 5. *Let $E_p(0, b)$ be an elliptic curve over $\mathbb{F}_p$ with equation $y^2 \equiv x^3 + b \pmod p$. If $p \equiv 2 \pmod 3$, then number of points on $E_p(0, b)$ is $\#E_p(0, b) = p + 1$.*

Since $\#E_p(a, b)$ is the order of the group $E_p(0, b)$ for the addition law, then $\#E_p(a, b) \cdot P = \mathcal{O}$ for any point $P \in E_p(a, b)$. When $p \equiv 2 \pmod 3$, then for any point $P \in$, we have $(p + 1)P = \mathcal{O}$. When N is a composite square free integer and a and b are integers satisfying $4a^3 + 27b^2 \not\equiv 0 \pmod p$, one can define an elliptic curve $E_N(a, b)$ over the ring $\mathbb{Z}/N\mathbb{Z}$ by the equation

$$E_N(a, b) : \quad y^2 \equiv x^3 + ax + b \pmod N, \tag{2}$$

together with a point O at infinity. An addition law can be defined over $E_N(a, b)$ by using the same rules as the addition law on $E_p(a, b)$ by replacing modulo p by modulo N. When the division by $x_2 - x_1$ is not possible, this means that $\gcd(x_2 - x_1, n) \neq 1$. Since $0 < |x_2 - x_1| < n$, then $\gcd(x_2 - x_1, n) = p$ or $\gcd(x_2 - x_1, n) = q$. If $N = pq$ is an RSA modulus, this is equivalent to factoring N. Since the integer factorization problem is very hard, especially for RSA moduli, then the scenario that the addition does not exist is unlikely to happen. By the Chinese remainder theorem, every point $P = (x, y) \in E_N(a, b)$ is uniquely represented by a pair of points $(P_p, P_q) \in E_p(a, b) \times E_q(a, b)$ with the convention that O is represented by the pair of points at infinity $(\mathcal{O}_p, \mathcal{O}_q) \in E_p(a, b) \times E_q(a, b)$. It follows that for $p \equiv q \equiv 2 \pmod 3$ and for any point $P \in E_N(0, b)$, we have

$$(p + 1)(q + 1)P = (p + 1)(q + 1)(P_p, P_q) = (\mathcal{O}_p, \mathcal{O}_q) = \mathcal{O}.$$

2.4 The KMOV Cryptosystem

In 1991, Koyama, Maurer, Okamoto and Vanstone proposed a cryptosystem, called KMOV, based on the elliptic curve $E_N(0,b)$ where $N = pq$ is an RSA modulus. The scheme works as follows.

- **KMOV Key Generation algorithm.**
  1. Choose two distinct prime numbers p and q of similar bit-length with $p \equiv q \equiv 2 \pmod 3$.
  2. Compute $N = pq$.
  3. Choose e such that $\gcd(e,(p+1)(q+1)) = 1$.
  4. Compute $d = e^{-1} \pmod{(p+1)(q+1)}$.
  5. Keep p, q, d secret, publish N, e.
- **KMOV Encryption algorithm.**
  1. For a message $m = (m_x, m_y) \in \mathbb{Z}_N^2$, compute $b = m_y^2 - m_x^3 \pmod N$.
  2. Compute the point $(c_x, c_y) = e(m_x, m_y)$ on the elliptic curve with equation $y^2 \equiv x^3 + b \pmod N$. The ciphertext is $c = (c_x, c_y)$.
- **KMOV Decryption algorithm.**
  1. For a ciphertext $c = (c_x, c_y) \in \mathbb{Z}_N^2$, compute $b = c_y^2 - c_x^3 \pmod N$.
  2. Compute the point $(m_x, m_y) = d(c_x, c_y)$ on the elliptic curve $y^2 \equiv x^3 + b \pmod N$. The plaintext is $m = (m_x, m_y)$.

The complexity of the encryption and decryption algorithms are based on the size of the encryption key e and the size of decryption key d, respectively. In a cryptosystem with a limited resource such as a credit card, it is desirable to have a smaller value of d or e. Unfortunately, when d is too small, Pinch [20] showed that one can factor the RSA modulus $N = pq$ if $d < \frac{1}{3}N^{\frac{1}{4}}$. Using a generalized attack, Nitaj [18] showed that one can factor N when $d \equiv \frac{y}{x} \pmod{(p+1)(q+1)}$ is much larger under some extra conditions on x and y.

3 A New Improved Attack Based on Continued Fractions

In this section, we give an improved attack on KMOV based totally on the continued fraction algorithm.

3.1 The new attack based on continued fractions

The attacks presented in [20] and [11] take advantage on using the convergents of the continued fraction expansion of $\frac{e}{N}$. Instead of using the convergents of $\frac{e}{N}$, we will use the convergents of $\frac{e}{\phi_0}$ where ϕ_0 is given by $\phi_0 = N + 1 + \left(1 + \frac{3\sqrt{2}}{4}\right)N^{\frac{1}{2}}$. To this end, we will need the following result.

Lemma 1. *For any $N > 10^6$, we have*

$$\frac{\left(\frac{3}{\sqrt{2}} - 2\right)N^{\frac{1}{2}} + 2}{(N + 2N^{\frac{1}{2}})^2} < \frac{1}{8N^{\frac{3}{2}}}.$$

Proof. Suppose that

$$\frac{\left(\frac{3}{\sqrt{2}}-2\right)N^{\frac{1}{2}}+2}{\left(N+2N^{\frac{1}{2}}\right)^2}<\frac{1}{8N^{\frac{3}{2}}}.$$

Then, clearing the denominators, we get

$$8N^{\frac{1}{2}}\left(\left(\frac{3}{\sqrt{2}}-2\right)N^{\frac{1}{2}}+2\right)<\left(N^{\frac{1}{2}}+2\right)^2,$$

which is equivalent to

$$\left(12\sqrt{2}-16\right)N+16N^{\frac{1}{2}}<N+4N^{\frac{1}{2}}+4.$$

This is true if

$$\left(12\sqrt{2}-16\right)N+16N^{\frac{1}{2}}<N+4N^{\frac{1}{2}},$$

or equivalently $12<\left(17-12\sqrt{2}\right)N^{\frac{1}{2}}$. This is valid if

$$N>10^6>\left(\frac{12}{17-12\sqrt{2}}\right)^2.$$

This terminates the proof. □

The following lemma is useful for approximating the sizes of the prime factors of an RSA modulus $N=pq$ when p and q are of the same bit-size.

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

$$2N^{\frac{1}{2}}<p+q<\frac{3\sqrt{2}}{2}N^{\frac{1}{2}}.$$

Proof. Assume that $q<p<2q$. Then $1<\sqrt{\frac{p}{q}}<\sqrt{2}$, so, since the function $f(x)=x+\frac{1}{x}$ is increasing on $[1,+\infty)$, we get

$$2<\sqrt{\frac{p}{q}}+\sqrt{\frac{q}{p}}<\sqrt{2}+\frac{1}{\sqrt{2}}=\frac{3\sqrt{2}}{2}.$$

If we multiply by $N^{\frac{1}{2}}$, we get

$$2N^{\frac{1}{2}}<p+q<\frac{3\sqrt{2}}{2}N^{\frac{1}{2}}.$$

This terminates the proof. □

Now, we present our first improved attack on KMOV based on the continued fraction algorithm. The following result shows that the secret information p,q,d in a KMOV cryptosystem can be recovered from public information (e,N).

Theorem 6. *Let (N,e) be a public key in a KMOV cryptosystem with $N = pq > 10^6$, $q < p < 2q$ and $\gcd(e,(p+1)(q+1))$. If $ed \equiv 1 \pmod{(p+1)(q+1)}$ and $d < 2\sqrt{2}\frac{N^{\frac{3}{4}}}{\sqrt{e}}$, then one can factor N in polynomial time in $\log(N)$.*

Proof. Suppose that $N = pq$ with $q < p < 2q$. Then, by Lemma 2, we get

$$N + 1 + 2N^{\frac{1}{2}} < (p+1)(q+1) < N + 1 + \frac{3\sqrt{2}}{2}N^{\frac{1}{2}}.$$

We set $\phi_1 = N+1+2N^{\frac{1}{2}}$ and $\phi_2 = N+1+\frac{3\sqrt{2}}{2}N^{\frac{1}{2}}$. Then $(p+1)(q+1) \in]\phi_1, \phi_2[$. Let

$$\phi_0 = N + 1 + \left(1 + \frac{3\sqrt{2}}{4}\right)N^{\frac{1}{2}},$$

be the midpoint of the interval $[\phi_1, \phi_2]$. Since $(p+1)(q+1) \in (\phi_1, \phi_2)$, then

$$|(p+1)(q+1) - \phi_0| \leq \frac{1}{2}(\phi_2 - \phi_1). \tag{3}$$

If $ed \equiv 1 \pmod{(p+1)(q+1)}$, then $ed - k(p+1)(q+1) = 1$, and

$$\begin{aligned}\left|\frac{e}{\phi_0} - \frac{k}{d}\right| &= \left|\left(\frac{e}{\phi_0} - \frac{e}{(p+1)(q+1)}\right) + \left(\frac{e}{(p+1)(q+1)} - \frac{k}{d}\right)\right| \\ &= \left|\frac{e((p+1)(q+1)-\phi_0)}{\phi_0(p+1)(q+1)} + \frac{1}{d(p+1)(q+1)}\right| \\ &= \left|\frac{e((p+1)(q+1)-\phi_0)}{\phi_0(p+1)(q+1)} + \frac{e}{(p+1)(q+1)(k(p+1)(q+1)+1)}\right|.\end{aligned}$$

Since $\phi_0(p+1)(q+1) > \phi_1^2$ and $(p+1)(q+1)(k(p+1)(q+1)+1) > \phi_1^2$, then

$$\begin{aligned}\left|\frac{e}{\phi_0} - \frac{k}{d}\right| &< e\frac{\frac{1}{2}(\phi_2 - \phi_1)}{\phi_1^2} + e\frac{1}{\phi_1^2} \\ &= e\frac{\phi_2 - \phi_1 + 2}{2\phi_1^2}.\end{aligned}$$

Then, combining (3) and $\phi_1 = N + 1 + 2\sqrt{N} \geq N + 2\sqrt{N}$, we get

$$\left|\frac{e}{\phi_0} - \frac{k}{d}\right| < e\frac{\left(\frac{3\sqrt{2}}{2} - 2\right)\sqrt{N} + 2}{2\left(N + 2\sqrt{N}\right)^2}.$$

Using Lemma 1, for $N > 10^6$, we get

$$\left|\frac{e}{\phi_0} - \frac{k}{d}\right| < \frac{e}{16N^{\frac{3}{2}}}.$$

Now, suppose that $\frac{e}{16N^{\frac{3}{2}}} < \frac{1}{2d^2}$, that is $d < \frac{2\sqrt{2}N^{\frac{3}{4}}}{\sqrt{e}}$, then

$$\left|\frac{e}{\phi_0} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

It follows by Theorem 4 that $\frac{k}{d}$ is a convergent of $\frac{e}{\phi_0}$ from which we deduce k and d. Using the equation $ed - k(p+1)(q+1) = 1$, we get $p + q = \frac{ed-1}{k} - N - 1$ and combining with $N = pq$, we easily find p and q. This gives to the factorization of $N = pq$. Notice that, since the continued fraction algorithm works in polynomial time, then finding p and q is done in polynomial time. □

3.2 Comparison with former attacks

In [20], Pinch extended Wiener's attack [25] on RSA to KMOV and showed that one can factor the modulus $N = pq$ if the private exponent d satisfies $d < \frac{1}{3}N^{\frac{1}{4}}$. In [11], Ibrahimpasic slightly extended the attack of Pinch by an extra exhaustive research. In both attacks, the bounds do not depend on the size of e. In our new attack, the bound is $d < 2\sqrt{2}\frac{N^{\frac{3}{4}}}{\sqrt{e}}$ and depends on e. In the typical situation where $e \approx N$, our bound becomes $d < 2\sqrt{2}N^{\frac{1}{4}} \approx 2.828N^{\frac{1}{4}}$ while the bound in [20] is $d < \frac{1}{3}N^{\frac{1}{4}} \approx 0.333N^{\frac{1}{4}}$. Observe that our new bound $d < 2\sqrt{2}\frac{N^{\frac{3}{4}}}{\sqrt{e}}$ is more significative for moderately small e.

Let us consider a numerical example. Consider the 1024 bit modulus N

$$\begin{aligned} N =& 128072253291560984675731339942623874155571330351805615681477940\\ &737860111553200263411409851831323456088583497355190072283898949\\ &746366445389418926799490964902211240447125449181697155706714427\\ &483626444781096408044876129844375261551528718257946239064984462\\ &4268738622294534859499980507160388244109820054662465276 21, \end{aligned}$$

and the 999 bit public exponent.

$$\begin{aligned} e =& 296526935093015710407136686034981189608183689687233930438373260\\ &994003008667647176609955506859286957594312864516062333691708865\\ &839614673732252521930067346220763331390433471403382719324360755\\ &735108333314843772805919919463508848644534123617058298952149225\\ &537288122181124813399940600506973710718085464 4647. \end{aligned}$$

Then, applying the continued fraction algorithm to $\frac{e}{\phi_0}$ and computing the convergents, the 130th convergent is $\frac{k}{d}$ where

$$\begin{aligned} k =& 439246113481593542214907254431461323475931905724710548163257922\\ &73119943084,\\ d =& 189713759006418854581978701838234268226797542876185500122247305\\ &6385648715923809927. \end{aligned}$$

Using this convergent, we get $p+q=\frac{ed-1}{k}$. Then combining with $pq=N$, we get

$$\begin{aligned}p =&122295652435077729919345520517086986879675097236430221980450907\\&006278884550539602496027848592931847870084590996181730049111792\\&444063000820719718514051784 17,\\q =&104723471964426405086080002568566304601367956338101575543737215\\&792893331651240463496547152238295322902114471979717345643807495\\&2583266784170210291778297461 3.\end{aligned}$$

We notice that $\frac{k}{d}$ is not among the convergents of $\frac{e}{N}$ which implies that the methods of Pinch and Ibrahimpasic will not succeed.

4 A New Improved Attack Based on Coppersmith's Method

In this section, we present a new attack on KMOV based on Coppersmith's method.

4.1 The new attack

Theorem 7. *Let (N,e) be a public key for the KMOV cryptosystem where $N=pq$ is an RSA modulus and $e=N^{\beta}$. Suppose that e satisfies the equation $eu-(p+1)(q+1)v=w$ with $u<N^{\delta}$ and $|w|<N^{\gamma}$. If*

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

for a small positive constant ε, then one can factor N in polynomial time.

Proof. Suppose that $N=pq$ is an RSA modulus and e is a public exponent satisfying $eu-(p+1)(q+1)v=w$. Since $(p+1)(q+1)=N+p+q+1$, then $v(N+p+q+1)+w\equiv 0 \pmod{e}$, which can be rewritten as $v(p+q+1)+Nv+w\equiv 0 \pmod{e}$. Consider the polynomial $f(x,y,z)=xy+Nx+z$, Then $(x,y,z)=(v,p+q+1,w)$ is a solution of the modular polynomial equation $f(x,y,z)\equiv 0 \pmod{e}$. To find the solution $(v,p+q+1,w)$, we apply Coppersmith's method [8]. Let m and t be two positive integers to be optimized later. We use $f(x,y,z)$ to build the sets of polynomials

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

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 $H_{k,i_1,i_2,i_3}(Xx,Yy,Zz)$. By choosing the increasing ordering following the i_1's, then the i_2's, and the i_3's, one find a left triangular matrix. For $m = 2$ and $t = 1$, the coefficient matrix for $\mathcal{L}$ is presented in Table 1 where the monomials are

$$\{z^3, xz^2, x^2z, x^3, xyz^2, x^2yz, x^3y, x^2y^2z, x^3y^2, x^3y^3, xy^2z^2, x^2y^3z, x^2yz, x^3y^4\}.$$

The non-zero elements are marked with an '$\circledast$' and do not influence the value of the determinant.

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

	xy^2z^2	x^2y^3z	x^2yz	x^3y^4
G_{k,i_1,i_2,i_3}				
$G_{0,0,0,3}$	0	0	0	0
$G_{0,1,0,2}$	0	0	0	0
$G_{0,2,0,1}$	0	0	0	0
$G_{0,3,0,0}$	0	0	0	0
$G_{1,1,1,2}$	0	0	0	0
$G_{1,2,1,1}$	0	0	0	0
$G_{1,3,1,0}$	0	0	0	0
$G_{2,2,2,1}$	0	0	0	0
$G_{2,3,2,0}$	0	0	0	0
$G_{3,3,3,0}$	0	0	0	0
H_{k,i_1,i_2,i_3}				
$H_{0,0,1,3}$	$XY^2Z^2e^2$	0	0	0
$H_{1,1,2,2}$	$\circledast$	X^2Y^3Ze	0	0
$H_{2,2,3,1}$	0	0	X^2YZe	0
$H_{3,3,4,0}$	0	0	0	X^3Y^4

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

The determinant of the triangular matrix is then the determinant of the lattice $\mathcal{L}$ and can be easily computed as

$$\det(\mathcal{L}) = e^{n_e} X^{n_X} Y^{n_Y} Z^{n_Z}. \tag{4}$$

To find the values of the exponents n_e, n_X, n_Y, n_Z, define the sum $S(a)$ by

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

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

$$\begin{aligned} n_e &= S(m-k) = \frac{1}{6}m(m+1)(2m+3t+4), \\ n_X &= S(i_1) = \frac{1}{6}m(m+1)(2m+3t+4), \\ n_Y &= S(i_2) = \frac{1}{6}(m+1)\left(m^2+3mt+3t^2+2m+3t\right), \\ n_Z &= S(i_3) = \frac{1}{6}m(m+1)(m+3t+2). \end{aligned} \tag{5}$$

The dimension of the lattice is the number of rows in the matrix. It can be estimated as

$$\omega = S(1) = \frac{1}{2}(m+1)(m+2t+2). \tag{6}$$

If we set $t = \tau m$ for some positive τ, then the dominant terms of the exponents in (5) and 6 are

$$\begin{aligned} n_e &\approx \frac{1}{6}(3\tau+2)m^3 + o(m^3), \\ n_X &\approx \frac{1}{6}(3\tau+2)m^3 + o(m^3), \\ n_Y &\approx \frac{1}{6}\left(3\tau^2+3\tau+1\right)m^3 + o(m^3), \\ n_Z &\approx \frac{1}{6}(3\tau+1)m^3 + o(m^3), \\ w &\approx \frac{1}{6}(6\tau+3)m^2 + o(m^2). \end{aligned} \tag{7}$$

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

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

To apply Howgrave-Graham's Theorem 1 to h_1, h_2 and h_3, we set

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

from which we deduce

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

Using (4), we get

$$e^{n_e} X^{n_X} Y^{n_Y} Z^{n_Z} < 2^{-\frac{\omega(\omega-1)}{4}} \frac{1}{\left(\sqrt{\omega}\right)^{\omega-2}} e^{m(\omega-2)}. \tag{8}$$

Suppose that $e = N^{\beta}$, $u < N^{\delta}$ and $|w| < N^{\gamma}$. Then, using Lemma 2, we have $p + q + 1 \leq 2p < 2\sqrt{2}\sqrt{N}$. Since $p + q + 1$ is represented by y, we set $Y = \left\lfloor 2\sqrt{2}\sqrt{N} \right\rfloor$. On the other hand, since $(p + 1)(q + 1) > N$ and $|w| < eu$, we get

$$|v| = \frac{|eu - w|}{(p + 1)(q + 1)} < \frac{eu + |w|}{(p + 1)(q + 1)} < \frac{2eu}{N} < 2N^{\beta+\delta-1}. \tag{9}$$

Since v is represented by x, we set $X = \left\lfloor 2N^{\beta+\delta-1} \right\rfloor$. Also, since w is represented by Z, we set $Z = \lfloor N^{\gamma} \rfloor$. It follows that the solution $(x, y, z) = (v, p + q + 1, w)$ satisfies $|x| < X$, $|y| < Y$ and $|z| < Z$ and (8) is satisfied if

$$2^{n_X} \left(2\sqrt{2}\right)^{n_Y} N^{n_e\beta+n_X(\beta+\delta-1)+\frac{n_Y}{2}+n_Z\gamma} < 2^{-\frac{\omega(\omega-1)}{4}} \frac{1}{\left(\sqrt{\omega}\right)^{\omega-2}} N^{m(\omega-2)\beta}. \tag{10}$$

Using the approximations of n_e, n_X, n_Y, n_Z given in (7) and ω given 6, the inequality 8 leads to

$$\begin{aligned} &N^{\left((3\tau+2)\beta+(3\tau+2)(\beta+\delta-1)+\frac{3\tau^2+3\tau+1}{2}+(3\tau+1)\gamma\right)m^3} \\ &\quad < 2^{-n_X}\left(2\sqrt{2}\right)^{-n_Y} 2^{-\frac{\omega(\omega-1)}{4}} \frac{1}{\left(\sqrt{\omega}\right)^{\omega-2}} N^{-2\beta m} N^{(6\tau+3)\beta m^3}. \end{aligned} \tag{11}$$

To homogenize the exponentiation of N, we set

$$2^{-n_X}\left(2\sqrt{2}\right)^{-n_Y} 2^{-\frac{\omega(\omega-1)}{4}} \frac{1}{\left(\sqrt{\omega}\right)^{\omega-2}} N^{-2\beta m} = N^{-\mu m^3},$$

where μ is a small positive constant. Then, taking logarithms and dividing by $m^3 \log N$, we get

$$(3\tau + 2)\beta + (3\tau + 2)(\beta + \delta - 1) + \frac{3\tau^2 + 3\tau + 1}{2} + (3\tau + 1)\gamma - (6\tau + 3)\beta < -\mu.$$

The optimal value for the left hand side is $\tau_0 = \frac{1-2\delta-2\gamma}{2}$, which, plugged in the former inequality leads to

$$-12\delta^2 - 24\delta\gamma - 12\gamma^2 + 8\beta + 28\delta + 20\gamma - 15 < -8\mu,$$

and consequently

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

where ε is a small positive constant that depends on m and N. Within this condition, the reduced lattice has three polynomials $h_1(x, y, z)$, $h_2(x, y, z)$ and $h_2(x, y, z)$ sharing the root $(x_0, y_0, z_0) = (v, p+q+1, w)$. Then, applying Gröbner basis or resultant computations, we get the expected solution (x_0, y_0, z_0) from which we deduce $p + q = y - 1$. Together with the equation $pq = N$, this leads to finding p and q. This terminates the proof. □

4.2 Comparison with former attacks

In [18], Nitaj presented an algorithm for factoring the modulus $N = pq$ when the public exponent e satisfies an equation of the form $eu-(p+1)(q+1)v = w$, where the unknown parameters u, v and w are such that

$$|w| < \frac{(p-q)N^{\frac{1}{4}}v}{3(p+q)}, \quad uv < \frac{\sqrt{2}\sqrt{N}}{12}. \tag{12}$$

The idea in [18] is to compute the convergents of the continued fraction of $\frac{e}{N}$, and for each convergent $\frac{v}{u}$ with $uv < \frac{\sqrt{2}\sqrt{N}}{12}$, to compute U and V with

$$U = \frac{eu}{v} - N - 1, \qquad V = \sqrt{|U^2-4N|}.$$

Then $\tilde{p} = \frac{1}{2}(U+V)$ is a possible approximation of the prime factor p with error term of at most $2N^{\frac{1}{4}}$. If so, then by applying Coppersmith's method, one can find p, and then factor N.

To compare our new results and the result of [18], suppose that $e = N^{\beta}$, $u < N^{\delta}$ and $|w| < N^{\gamma}$. Then, by (9), we get $|v| < 2N^{\beta+\delta-1}$. Hence, the inequalities (12) are fulfilled if

$$N^{\gamma} < \frac{2(p-q)N^{\frac{1}{4}}N^{\beta+\delta-1}}{3(p+q)}, \quad 2N^{\delta}N^{\beta+\delta-1} < \frac{\sqrt{2}\sqrt{N}}{12}.$$

Then, neglecting the constants and assuming that $p-q \approx p+q$, the former two inequalities are true if

$$\gamma < \frac{1}{4} + \beta + \delta - 1, \quad 2\delta + \beta - 1 < \frac{1}{2}.$$

This leads to $\delta < \frac{3}{4} - \frac{1}{2}\beta$, which is to be compared with the new bound

$$\delta < \frac{7}{6} - \gamma - \frac{1}{3}\sqrt{6\beta-6\gamma+1} - \varepsilon.$$

Define

$$\delta_0 = \frac{3}{4} - \frac{1}{2}\beta, \quad \delta_1 = \frac{7}{6} - \gamma - \frac{1}{3}\sqrt{6\beta-6\gamma+1}.$$

A typical situation is when $e \approx N$, that is $\beta = 1$, and $|w|$ is small, that is $\gamma = 0$. Then the bounds δ_0 and δ_1 are $\delta_0 = 0.25$, $\delta_1 \approx 0.284$. We see that the new method overcome the method of [18] in the most realistic situations of instances of KMOV.

5 Conclusion

We have presented two new attacks on the KMOV cryptosystem which is an RSA type cryptosystem based on elliptic curves. The first attack is based on the continued fraction algorithm and the second is based on Coppersmith's method. Both attacks work when the private key is suitably small and the new results improve the former attacks on the KMOV elliptic curve cryptosystem.

References

1. D. Boneh, Twenty years of attacks on the RSA cryptosystem, Notices of the American Mathematical Society 46(2), 203–213, 1999.
2. D. Boneh, G. Durfee, Cryptanalysis of RSA with private key d less than $N^{0.292}$, IEEE Transactions on Information Theory 46, 1339–1349, 2000.
3. M. Bunder, J. Tonien, A new improved attack on RSA, in Proceedings of the 5th International Cryptology and Information Security Conference, 2016, pp. 101–110.
4. M. Bunder, A. Nitaj, W. Susilo, J. Tonien, A new attack on three variants of the RSA cryptosystem, in: Proceedings of ACISP 2016, Lecture Notes in Computer Science 9723, 2016, pp. 258-268.
5. M. Bunder, A. Nitaj, W. Susilo, J. Tonien, A generalized attack on RSA type cryptosystems, Theoretical Computer Science 704, 74–81, 2017.
6. M. Bunder, J. Tonien, A new attack on the RSA cryptosystem based on continued fractions, Malaysian Journal of Mathematical Sciences 11(S3), 45–57, 2017.
7. M. Bunder, A. Nitaj, W. Susilo, J. Tonien, Cryptanalysis of RSA-type cryptosystems based on Lucas sequences, Gaussian integers and elliptic curves, Journal of Information Security and Applications 40, 193–198, 2018.
8. D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities, Journal of Cryptology 10(4), 233–260, 1997.
9. G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, London, 1965.
10. N. Howgrave-Graham, Finding small roots of univariate modular equations revisited, in: Proceedings of IMA International Conference on Cryptography and Coding 1997, Lecture Notes in Computer Science 1355, 1997, pp. 131–142.
11. B. Ibrahimpasic, Cryptanalysis of KMOV cryptosystem with short secret exponent, in: Proceedings of Central European Conference on Information and Intelligent Systems, 2008.
12. E. Jochemsz, A. May, A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants, in: Proceedings of ASIACRYPT 2006, Lecture Notes in Computer Science 4284, 2006, pp. 267–282.
13. N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation 48, 203–209, 1987.
14. K. Koyama, U. M. Maurer, T. Okamoto and S. A. Vanstone, New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$, in: Proceedings of CRYPTO 1991, Lecture Notes in Computer Science 576, 1991, pp. 252–266.
15. A.K. Lenstra, H.W. Lenstra, L. Lovász, Factoring polynomials with rational coefficients, Mathematische Annalen 261, 513–534, 1982.
16. A. May, New RSA Vulnerabilities using Lattics Reduction Methods, Ph.D. Dissertation. University of Paderborn, (2003) `http://www.cits.rub.de/imperia/md/content/may/paper/bp.ps`
17. V.S. Miller, Use of elliptic curves in cryptography, in: Proceedings of CRYPTO 1985, Lecture Notes in Computer Science 218, 1986, pp. 417–426.
18. A. Nitaj, A new attack on the KMOV cryptosystem, Bulletin of the Korean Mathematical Society 51 (5), 1347–1356, 2014.
19. A. Nitaj, Y. Pan, J. Tonien, A Generalized Attack on Some Variants of the RSA Cryptosystem, in: Proceedings of SAC 2018, Lecture Notes in Computer Science 11349, 2019, pp. 421–433.
20. R.G.E. Pinch, Extending the Wiener attack to RSA-type cryptosystems, Electronics Letters 31 (20), 1736–1738, 1995.

21. R. Rivest, A. Shamir, L. Adleman, A Method for Obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (2), 120–126, 1978.
22. S. Schmitt, H.G. Zimmer, Elliptic curves. A computational approach. Walter de Gruyter, Berlin, 2003.
23. J.H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics 106, Springer-Verlag, 1986.
24. W. Susilo, J. Tonien, G, Yang, The Wiener Attack on RSA Revisited: A Quest for the Exact Bound, in: Proceedings of ACISP 2019, Lecture Notes in Computer Science 11547, 2019, pp. 381–398.
25. M. Wiener, Cryptanalysis of short RSA secret exponents, IEEE Transactions on Information Theory 36, 553–558, 1990.