# A new attack on the KMOV cryptosystem

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

**Abstract**

In this paper, we analyze the security of the KMOV public key cryptosystem. KMOV is based on elliptic curves over the ring $\mathbb{Z}_n$ where $n = pq$ is the product of two large unknown primes of equal bit-size. We consider KMOV with a public key $(n, e)$ where the exponent $e$ satisfies an equation $ex - (p+1)(q+1)y = z$, with unknown parameters $x$, $y$, $z$. Using Diophantine approximations and lattice reduction techniques, we show that KMOV is insecure when $x$, $y$, $z$ are suitably small.

Keywords: KMOV, RSA, Cryptanalysis, Coppersmith's Method, Continued Fraction

## 1 Introduction

In the past decades, the advent of the Internet has exponentially increased the amount of data exchanged among the most diverse people, institutions and organizations, all over the world. Sensitive data exchanged between a user and a Web site needs to be encrypted to prevent it from being disclosed to or modified by unauthorized parties. Therefore, the development of secure communication has become a critical task and the most obvious way of achieving this goal is to use a cryptographic scheme to encrypt the data. Basically, there are two types of cryptography: symmetric-key cryptography and public-key cryptography. The concept of the public-key cryptography was proposed by Diffie and Hellman [4] and Merkle [8] in the mid 1970's. The first public-key cryptosystem, called RSA, was proposed in 1977 by Rivest, Shamir, and Adleman [10]. It is the most widely deployed public key cryptosystem and is used for securing web traffic in the Secure Sockets Layer (SSL) protocol and in the Transport Layer Security (TLS) protocol. In 1991, Koyama, Maurer, Okamoto and Vanstone [7] introduced a new public key cryptosystem called KMOV. The KMOV cryptosystem is based on elliptic curves over the ring $\mathbb{Z}_n$ where $n = pq$ is an RSA modulus, that is, the product of two large unknown primes of equal bit-size. The KMOV public key is denoted by $(n, e)$ where the public exponent $e$ is an integer satisfying $\gcd(e, (p+1)(q+1)) = 1$. The private exponent $d$ is an integer satisfying $ed \equiv 1 \pmod{(p+1)(q+1)}$. The security of RSA and KMOV is mainly based on the difficulty of factoring the RSA modulus $n$. To speed up the encryption or decryption one may try to use small public or secret decryption exponent. Many important papers studied RSA and KMOV to explore the weaknesses in using small exponents (see [2] and [6]). In 1990, Wiener [12] showed that it is possible to break RSA if the private exponent $d$ satisfies $d < \frac{1}{3}n^{0.25}$. In 1995, Pinch [9] extended the Wiener attack to KMOV. In 2004, Blömer and May described an attack on RSA starting with the equation $ex + y = k(p-1)(q-1)$. Using the continued fraction algorithm and lattice reduction techniques, they showed that RSA is insecure if $0 < x < \frac{1}{3}n^{0.25}$ and $|y| = \mathcal{O}\left(n^{-0.75}ex\right)$.

In this paper, we consider KMOV with a public exponent $e$ satisfying the equation

$$ex - (p+1)(q+1)y = z,$$

where $x$ and $y$ are co-prime positive integers. Observe that this equation has infinitely many solutions but we will focus on small solutions. We use Diophantine approximations to find $x$, $y$ among the convergents of the continued fraction expansion of $\frac{e}{n}$ when $x$, $y$ and $z$ satisfy

$$xy < \frac{\sqrt{2}\sqrt{n}}{12} \quad \text{and} \quad |z| < \frac{(p-q)n^{\frac{1}{4}}y}{3(p+q)}.$$

After finding $x$ and $y$, one can get an approximation $\tilde{p}$ of $p$ satisfying $|p - \tilde{p}| < n^{\frac{1}{4}}$ which leads to the factorization of $n$ by using Coppersmith's method for finding small roots of modular polynomial equations [3].

The rest of this paper is organized as follows. In the next section, we review some necessary definitions and notation on elliptic curves and recall the KMOV cryptosystem. In section 3, we present our new attack on KMOV. We conclude in Section 4.

# 2 Preliminaries

In this section, we give a brief description of the KMOV cryptosystem and elliptic curves (see [11] for more details on elliptic curves).

## 2.1 Elliptic Curves

Let $p \geq 3$ be a prime. An elliptic curve over the finite field $\mathbb{F}_p$ is an algebraic curve with no singular points, given by the Weierstrass equation

$$E_p(a,b): \quad y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_p, \quad 4a^3 + 27b^2 \neq 0,$$

together with a single element denoted $\mathcal{O}$, called the point at infinity. Given two points $P, Q \in E_p(a,b)$, we define a third point $P+Q$ so that $E_p(a,b)$ forms an abelian group with this addition operation. For the special case $a = 0$, the order $\#E_p(0,b)$ can easily be determined.

**Lemma 1.** *Let $p > 3$ be a prime satisfying $p \equiv 2 \pmod 3$ and $0 < b < p$. Then*

$$\#E_p(0,b) = p + 1.$$

Let $n = pq$ be an RSA modulus. Let $(a,b) \in \mathbb{Z}_n^2$ such that $\gcd\left(4a^3 + 27b^2, n\right) = 1$. An elliptic curve $E_n(a,b)$ over $\mathbb{Z}_n$ is the set of points $(x,y) \in \mathbb{Z}_n^2$ satisfying

$$E_n(a,b): \quad y^2 = x^3 + ax + b \pmod n,$$

together with the point at infinity. The addition law can be extended for points in $E_n(a,b)$ and the Chinese Remainder Theorem leads to the following lemma.

**Lemma 2.** *Let $n = pq$ be the product of two primes and $E_n(a,b)$ an elliptic curve over $\mathbb{Z}_n$ with $\gcd\left(4a^3 + 27b^2, n\right) = 1$. Then for any $P \in E_n(a,b)$ and any integer $k$, we have*

$$(1 + k\#E_p(a,b)\#E_q(a,b))P = P.$$

## 2.2 KMOV Scheme

The KMOV cryptosystem [7] is based on elliptic curves $E_n(a,b)$ over $\mathbb{Z}_n$ where $n = pq$ is an RSA modulus. The scheme works as follows.

- **Key Generation**
  1. Find two primes, $p$ and $q$ with $p \equiv q \equiv 2 \pmod 3$ and compute $n = pq$.
  2. Choose an exponent $e$ co-prime to $(p+1)(q+1)$ and compute $d \equiv e^{-1} \pmod{(p+1)(q+1)}$.
  3. Return the public key $(n, e)$ and the private key $(n, d)$.

- **KMOV Encryption**
  1. Represent the message $m$ as a couple $(m_1, m_2) \in \mathbb{Z}_n^2$.
  2. Compute $b = m_2^2 - m_1^3 \pmod n$ and the point $(c_1, c_2) = e \times (m_1, m_2)$ on $E_n(0,b)$.
  3. Return $(c_1, c_2)$.

- **KMOV Decryption**
  1. Compute $b = c_2^2 - c_1^3 \pmod n$ and the point $(m_1, m_2) = d \times (c_1, c_2)$ on $E_n(0,b)$.
  2. Return $(m_1, m_2)$.

The correctness of the decryption is based on Lemma 1 and Lemma 2. Indeed

$$\begin{aligned} d \times (c_1, c_2) &= de \times (m_1, m_2) \\ &= (1 + k(p+1)(q+1)) \times (m_1, m_2) \\ &= (1 + k\#E_p(0,b)\#E_q(0,b)) \times (m_1, m_2) \\ &= (m_1, m_2), \end{aligned}$$

where $k$ is the integer satisfying $ed = 1 + k(p+1)(q+1)$.

# 3 The New attack on the KMOV Cryptosystem

Let $(n, e)$ be a KMOV public key with $n = pq$. Let $x$, $y$ be co-prime positive integers. Define $z$ by

$$z = ex - (p+1)(q+1)y.$$

In this section, we show that, under some conditions, it is possible find $x$, $y$, $p$, $q$ using only the public key $(n, e)$ which leads to the factorization of $n$ and breaks the system. We shall need the following useful result.

**Lemma 3.** *Let $n = pq$ be an RSA modulus with $q < p < 2q$. Then*

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

*Proof.* We have $(p+q)^2 = (p-q)^2 + 4n > 4n$. Then $p + q > 2\sqrt{n}$. On the other hand, since $q < p < 2q$, then $n < p^2 < 2n$ and $\sqrt{n} < p < \sqrt{2n}$. Let $f(p) = p + \frac{n}{p}$. The derivative satisfies $f'(p) = 1 - \frac{n}{p^2} > 0$. Hence $f(p) < f(\sqrt{2n})$ and

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

This terminates the proof. □

We shall also need the following result (see [5], Theorem 184).

**Theorem 1.** *Let $\alpha$ be a real number. If $x$ and $y$ are positive integers such that $\gcd(x, y) = 1$ and*

$$\left|\alpha - \frac{y}{x}\right| < \frac{1}{2x^2},$$

*then $\frac{y}{x}$ is one of the convergents of the continued fraction expansion of $\alpha$.*

Now, we can prove the following theorem which permits to find $x$ and $y$ using the convergents of the continued fraction expansion of $\frac{e}{n}$.

**Theorem 2.** *Let $n = pq$ be an RSA modulus with $q < p < 2p$. Suppose that a KMOV public exponent $e$ satisfies an equation $ex - (p+1)(q+1)y = z$ with $\gcd(x, y) = 1$ and*

$$xy < \frac{\sqrt{2}\sqrt{n}}{12} \quad \text{and} \quad |z| < \frac{(p-q)n^{\frac{1}{4}}y}{3(p+q)}.$$

*Then $\frac{y}{x}$ is one of the convergents of the continued fraction expansion of $\frac{e}{n}$.*

*Proof.* Transforming the equation $ex - (p+1)(q+1)y = z$, we get $ex - ny = (p+q+1)y + z$. Dividing by $nx$, we get

$$\frac{e}{n} - \frac{y}{x} = \frac{(p+q+1)y + z}{nx}. \tag{1}$$

If $|z| < \frac{(p-q)n^{\frac{1}{4}}y}{3(p+q)}$ then $|z| < n^{\frac{1}{4}}y$. Then using Lemma 3, we get

$$\begin{aligned} |(p+q+1)y + z| &\leq (p+q+1)y + |z| \\ &\leq (p+q+1)y + n^{\frac{1}{4}}y \\ &= (p+q+1+n^{\frac{1}{4}})y \\ &< 2(p+q)y \\ &\leq 3\sqrt{2}\sqrt{n}y. \end{aligned}$$

Plugging in (1), we get

$$\left|\frac{e}{n}-\frac{y}{x}\right|<\frac{3\sqrt{2}\sqrt{n}y}{nx}.$$

Now, assume that $xy<\frac{\sqrt{2}\sqrt{n}}{12}$. Then $\frac{3\sqrt{2}\sqrt{n}y}{nx}<\frac{1}{2x^2}$ which implies

$$\left|\frac{e}{n}-\frac{y}{x}\right|<\frac{1}{2x^2}.$$

Then, by Theorem 1, $\frac{y}{x}$ is a convergent of the continued fraction of $\frac{e}{N}$. This terminates the proof. □

Now assume that $x$ and $y$ are known in the equation $ex-(p+1)(q+1)y=z$. Next, we show how to find $p$ and $q$. Let us first refer to the following existing result (see [3]).

**Theorem 3** (Coppersmith)**.** *Let $n=pq$ be an RSA modulus with $q<p<2q$. Suppose we know an approximation $\tilde{p}$ of $p$ with $|p-\tilde{p}|<n^{\frac{1}{4}}$. Then $n$ can be factored in time polynomial in* $\log n$.

Let us present the main result.

**Theorem 4.** *Let $n=pq$ be an RSA modulus with $q<p<2q$. Suppose that a KMOV public exponent $e$ satisfies an equation $ex-(p+1)(q+1)y=z$ with* $\gcd(x,y)=1$ *and*

$$xy<\frac{\sqrt{2}\sqrt{n}}{12}\quad \textit{and}\quad |z|<\frac{(p-q)n^{\frac{1}{4}}y}{3(p+q)}.$$

*Then $n$ can be factored in polynomial time.*

*Proof.* Suppose $e$ satisfies an equation $ex-(p+1)(q+1)y=z$. If $\gcd(x,y)=1$, $xy<\frac{\sqrt{2}\sqrt{n}}{12}$ and $|z|<\frac{(p-q)n^{\frac{1}{4}}y}{3(p+q)}$, then, by Theorem 2, we find $x$ and $y$ among the convergents of $\frac{e}{n}$. Next, put

$$U=\frac{ex}{y}-n-1,\qquad V=\sqrt{|U^2-4n|}.$$

Starting with the equation $ex-(p+1)(q+1)y=z$, we get

$$|U-p-q|=\left|\frac{ex}{y}-n-1-p-q\right|=\frac{|z|}{y}<\frac{(p-q)n^{\frac{1}{4}}}{3(p+q)}<n^{\frac{1}{4}}. \tag{2}$$

Now, we have

$$\begin{aligned}\left|(p-q)^2-V^2\right| &= \left|(p-q)^2-\left|U^2-4n\right|\right|\\ &\le \left|(p-q)^2-U^2+4n\right|\\ &= \left|(p+q)^2-U^2\right|\\ &= |p+q-U|\,(p+q+U).\end{aligned}$$

Dividing by $p-q+V$, we get

$$|p-q-V|\le\frac{|p+q-U|\,(p+q+U)}{p-q+V}. \tag{3}$$

Observe that (2) implies

$$p+q+U<2(p+q)+n^{\frac{1}{4}}<3(p+q).$$

On the other hand, we have $p-q+V>p-q$. Plugging in (3), we get

$$|p-q-V|<\frac{3(p+q)(p-q)n^{\frac{1}{4}}}{3(p+q)(p-q)}=n^{\frac{1}{4}}.$$

Combining this with (2), we deduce

$$\left|p-\frac{U+V}{2}\right|=\left|\frac{p+q}{2}-\frac{U}{2}+\frac{p-q}{2}-\frac{V}{2}\right|\le\left|\frac{p+q}{2}-\frac{U}{2}\right|+\left|\frac{p-q}{2}-\frac{V}{2}\right|<n^{\frac{1}{4}}.$$

This implies that $\frac{U+V}{2}$ is an approximation of $p$ up to an error term of at most $n^{\frac{1}{4}}$. Then Coppersmith's Theorem 3 will find $p$ in polynomial time and the factorization of $n$ follows. □

# 4 Conclusion

In this paper, we describe a new attack on the KMOV cryptosystem with a public key $(n, e)$ where $n = pq$ is an RSA modulus and $e$ is a KMOV public exponent satisfying $\gcd(e, (p+1)(q+1)) = 1$. We prove that KMOV is insecure if there exist relatively small integers $x$, $y$ and $z$ satisfying an equation $ex - (p+1)(q+1)y = z$. The attack combines the continued fraction algorithm and Coppersmith's lattice reduction based method and can be seen as an extension of Pinch's attack on small KMOV secret decryption exponents.

# References


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

[2] D. Boneh: Twenty years of attacks on the RSA cryptosystem. Notices of the American Mathematical Society (AMS) 46(2), pp. 203–213 (1999).

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

[4] W. Diffie, E. Hellman: New directions in cryptography, IEEE Transactions on Information Theory, 22, 5, pp. 644–654 (1976).

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

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

[7] K. Koyama, U.M. Maurer, T. Okamoto, S.A. Vanstone: New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$, Advances in Cryptology - Crypto'91, Lecture Notes in Computer Science, Springer-Verlag, pp. 252–266 (1991).

[8] R.C. Merkle: Secure communications over insecure channels. Communications of the ACM, pp. 294–299, April 1978. Submitted 1975.

[9] R.G.E. Pinch: Extending the Wiener attack to RSA-type cryptosystems, Electronics Letters 31, pp. 1736–1738 (1995).

[10] R. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, Vol. 21 (2), pp. 120–126 (1978).

[11] J.H. Silverman: The Arithmetic of Elliptic Curves. Springer-Verlag, GTM 106, 1986. Expanded 2nd Edition, (2009).

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