Bull. Korean Math. Soc. **51** (2014), No. 5, pp. 1347–1356
http://dx.doi.org/10.4134/BKMS.2014.51.5.1347

A NEW ATTACK ON THE KMOV CRYPTOSYSTEM

Abderrahmane Nitaj

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.

1. Introduction

In 1991, Koyama, Maurer, Okamoto and Vanstone [7] introduced a new public key cryptosystem based on elliptic curves, 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. Introduced in 1978 by Rivest, Shamir and Adleman, RSA [9] is one of the most popular cryptosystems in research as well as in commercial domain (see [2], [5]). The RSA public key is denoted by (n, e) where $n = pq$ is an RSA modulus and e is an integer satisfying $\gcd(e, (p-1)(q-1)) = 1$. The corresponding private exponent d is an integer satisfying $ed \equiv 1 \pmod{(p-1)(q-1)}$. Then, there exists some integer k such that

$$ed - k(p-1)(q-1) = 1. \tag{1}$$

Similarly, the KMOV public key is denoted by (n, e) where $n = pq$ and e is an integer satisfying $\gcd(e, (p+1)(q+1)) = 1$. The corresponding private exponent d is an integer satisfying $ed \equiv 1 \pmod{(p+1)(q+1)}$ which can be reformulated as an equation

$$ed - k(p+1)(q+1) = 1. \tag{2}$$

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

Received June 26, 2012; Revised January 15, 2014.
2010 *Mathematics Subject Classification.* 11T71, 94A60, 14G50.
Key words and phrases. cryptanalysis, factorization, Coppersmith's method, continued fraction.

studied RSA and KMOV to explore the weaknesses in using small exponents. In 1990, Wiener [11] showed that using equation (1) and the continued fraction algorithm, it is possible to break RSA if the private key d satisfies $d < \frac{1}{3}n^{0.25}$. In 2004, Blömer and May [1] described an attack on RSA starting with the equation

$$ex - k(p-1)(q-1) = y.$$

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 more general equation

$$ex - (p+1)(q+1)y = z, \tag{3}$$

where x and y are co-prime positive integers. Observe that this equation has infinitely many solutions but we will focus on small solutions. In 1995, Pinch [8] extended the Wiener attack to KMOV using similar techniques applied with equation (2), that is when $z = 1$. Similarly, Ibrahimpašić [6], studied the security of KMOV with short secret exponents.

We mainly focus on the equation (3) which is a generalization of the equation (2). 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

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

After finding x and y, one can get an approximation $\tilde{p}$ of p satisfying $|p-\tilde{p}| < n^{\frac{1}{4}}$ where

$$\tilde{p} = \frac{1}{2}\left(\frac{ex}{y} - n - 1\right) + \frac{1}{2}\sqrt{\left|\left(\frac{ex}{y} - n - 1\right)^2 - 4n\right|}.$$

Finally, this approximation leads to the factorization of n by using Coppersmith's Theorem [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. In Section 4, we propose a numerical example. We conclude in Section 5.

2. Preliminaries

In this section, we give a brief description of the KMOV cryptosystem and elliptic curves (see [10] for more details on elliptic curves).

2.1. Elliptic curves over $\mathbb{F}_p$

An elliptic curve over a field $\mathbb{K}$ is an algebraic curve with no singular points, given by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{K},$$

together with a single element denoted $\mathcal{O}$ and called the point at infinity. The elliptic curve E over $\mathbb{K}$ is denoted $E/\mathbb{K}$ and the set of solutions $(x, y) \in \mathbb{K}^2$ together with $\mathcal{O}$ is denoted $E(\mathbb{K})$. Given two points $P, Q \in E(\mathbb{K})$ we define a third point $P + Q$ so that $E(\mathbb{K})$ forms an abelian group with this addition operation.

- The point $\mathcal{O}$ serves as the identity element.
- The opposite of $P = (x_1, y_1)$, is $-P = (x_1, -y_1 - a_1x_1 - a_3)$.
- If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ with $Q \neq -P$, then $P + Q = (x_3, y_3)$ where

$$\begin{cases} x_3 &= \lambda^2 - x_1 - x_2 - a_2 + a_1\lambda, \\ y_3 &= -y_1 - (x_3 - x_1)\lambda - a_1x_3 - a_3, \end{cases}$$

where

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if} \quad x_1 \neq x_2, \\ \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1^2 + a_1x_1 + a_3} & \text{if} \quad x_1 = x_2, \end{cases}$$

If $\mathbb{K}$ is of characteristic different from 2 or 3, the equation of the elliptic curve E can be transformed into the reduced Weierstrass form

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{K},$$

where $4a^3 + 27b^2 \neq 0$. When $\mathbb{K} = \mathbb{F}_p$ for some prime $p > 3$, such a curve will be denoted $E_p(a, b)$.

Theorem 2.1 (Hasse)**.** *The order of the group $E_p(a, b)(\mathbb{F}_p)$ is given by*

$$\#E_p(a, b) = p + 1 - a_p,$$

where $|a_p| \leq 2\sqrt{p}$.

For the special case $a = 0$, the order $\#E_p(0, b)$ can easily be determined.

Lemma 2.2. *Let $p > 3$ be a prime satisfying $p \equiv 2 \pmod 3$ and $0 < b < p$. Then*

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

2.2. Elliptic curves over $\mathbb{Z}_n$

We now consider elliptic curves over the ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ where $n = pq$ is the product of two large distinct primes p and q. An elliptic curve $E_n(a, b)$ over $\mathbb{Z}_n$ is the set of points $(x, y) \in \mathbb{Z}_n^2$ satisfying

$$y^2 = x^3 + ax + b \pmod n$$

together with the point at infinity $\mathcal{O}$. The addition law can be extended for points in a curve $E_n(a, b)$ over $\mathbb{Z}_n$. Note that the addition law is not always well-defined when using analytical expressions since there are elements in $\mathbb{Z}_n$

which are not invertible. It follows that $E_n(a,b)(\mathbb{Z}_n)$ is not a group. By the Chinese Remainder Theorem, the mapping

$$E_n(a,b) \to E_p(a,b) \times E_q(a,b)$$

defined by the natural projections is a bijection. Thus, a point (x,y) of the elliptic curve $E_n(a,b)$ is associated to the point

$$((x \pmod p),\ y \pmod p)), (x \pmod q),\ y \pmod q)) \in E_p(a,b) \times E_q(a,b).$$

The points $(\mathcal{O}, P)$ and $(P, \mathcal{O})$ can not be represented like this. Finding such a point is, however, very unlikely and would lead to the factorization of n. The Chinese Remainder Theorem leads to the following lemma.

Lemma 2.3. *Let $n = pq$ be an RSA modulus 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*

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

2.3. KMOV Scheme

In 1991, Koyama, Maurer, Okamoto and Vanstone [7] proposed the so called KMOV cryptosystem using elliptic curves defined over the elliptic curve $E_n(a,b)$ where $n = pq$ is an RSA modulus. The authors propose using the elliptic curve $E_n(0,b)$ with equation $y^2 = x^3 + b$ modulo $n = pq$ where p and q are both congruent to 2 mod 3. In this case, the order $\#E_p(0,b)$ is $p+1$ and the order $\#E_q(0,b)$ is $q+1$.

- **Key Generation**
  INPUT: The bit-length k of the RSA modulus.
  OUTPUT: The public key (n,e) and the private key (n,d).

  (1) Find two primes, p and q, of length $k/2$ bits satisfying $p \equiv q \equiv 2 \pmod 3$.
  (2) Compute the RSA modulus $n = pq$.
  (3) Choose a public key e co-prime to $(p+1)(q+1)$.
  (4) Compute the inverse d of e mod $((p+1)(q+1))$.
  (5) Return the public key (n,e) and the private key (n,d).

- **KMOV Encryption**
  INPUT: The public key (n,e) and the plaintext message m.
  OUTPUT: The cyphertext (c_1, c_2).

  (1) Represent the message m as a couple $(m_1, m_2) \in \mathbb{Z}_n^2$.
  (2) Compute $b = m_2^2 - m_1^3 \pmod n$.
  (3) Compute the point $(c_1, c_2) = e(m_1, m_2)$ on the elliptic curve $y^2 = x^3 + b \pmod n$.
  (4) Return (c_1, c_2).

- **KMOV Decryption**
  INPUT: The private key (n, d) and the cyphertext (c_1, c_2).
  OUTPUT: The plaintext message (m_1, m_2).

  (1) Compute $b = c_2^2 - c_1^3 \pmod{n}$. Note that the receiver of a message never need to compute b, but he can compute it.
  (2) Compute the point $(m_1, m_2) = d(c_1, c_2)$ on the elliptic curve $y^2 = x^3 + b \pmod{n}$.
  (3) Return (m_1, m_2).

The decryption scheme is valid since, using Lemma 2.2 and Lemma 2.3, we have

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

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

3. The new attack on the KMOV cryptosystem

Let $n = pq$ be an RSA modulus as required by the KMOV Cryptosystem. Suppose that e is an integer satisfying $\gcd(e, (p+1)(q+1)) = 1$. Let x, y be co-prime positive integers. Define z by

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

In this section, we show that, under some conditions, it is possible find x, y, p, q which leads to the factorization of the RSA modulus and breaks the system. We shall need the following useful result.

Lemma 3.1. *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 $\sqrt{n} < p < \sqrt{2n}$. Notice that $p + q = p + \frac{n}{p}$ is optimal for $p = \sqrt{2n}$. Hence

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

This terminates the proof. □

We shall also need the following result (see [4], Theorem 184).

Theorem 3.2. *Let α 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 α.

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

$$|z|<n^{\frac{1}{4}}y, \quad xy<\frac{\sqrt{2}\sqrt{n}}{12}.$$

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

$$\frac{e}{n}-\frac{y}{x}=\frac{(p+q+1)y+z}{nx}. \tag{4}$$

Assume that $|z|<n^{\frac{1}{4}}y$. Then using Lemma 3.1, we get

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

Now, assume that $xy<\frac{\sqrt{2}\sqrt{n}}{12}$. Then (4) implies

$$\left|\frac{e}{n}-\frac{y}{x}\right|=\frac{|(p+q+1)y+z|}{nx}<\frac{3\sqrt{2}\sqrt{n}y}{nx}<\frac{1}{2x^2}.$$

Then, applying Theorem 3.2, $\frac{y}{x}$ is a convergent of the continued fraction expansion of $\frac{e}{n}$. This terminates the proof. □

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

Theorem 3.4 (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 $\log n$.*

Next we present the main result.

Theorem 3.5. *Let $n = pq$ be an RSA modulus with $q < p < 2q$. Suppose that e is an exponent satisfying an equation $ex-(p+1)(q+1)y = z$ with $\gcd(x, y) = 1$ and*

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

Then n can be factored in polynomial time.

Proof. Suppose e satisfies an equation $ex - (p+1)(q+1)y = z$. If $|z| < \frac{(p-q)n^{\frac{1}{4}}y}{3(p+q)}$ then $|z| < n^{\frac{1}{4}}y$. In addition if $\gcd(x, y) = 1$ and $xy < \frac{\sqrt{2}\sqrt{n}}{12}$, then, by Theorem 3.3, 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

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

Hence

$$|U - p - q| < n^{\frac{1}{4}}. \tag{5}$$

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

$$|p - q - V| \le \frac{|p+q-U|\,(p+q+U)}{p-q+V}. \tag{6}$$

Observe that (5) 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 (6), 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 (5), we deduce

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

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 3.4 will find p in polynomial time and the factorization of n follows. □

Let us summarize the factorization algorithm.

Algorithm 1 The factorization algorithm

Require: a public key (N, e) satisfying $N = pq$, $q < p < 2q$ and $ex - (p+1)(q+1)y = z$ for some parameters x, y, z.
Ensure: the prime factors p and q.
1: Compute the continued fraction expansion of $\frac{e}{n}$.
2: For every convergent $\frac{y}{x}$ of $\frac{e}{n}$ with $x < \sqrt{n}$:
3: Compute $U = \frac{ex}{y} - n - 1$ and $V = \sqrt{|U^2 - 4n|}$.
4: Apply Coppersmith's algorithm with $\frac{U+V}{2}$ as an approximation of p.
5: If Coppersmiths algorithm outputs the factorization of n, then stop.

4. A numerical example

As an example to illustrate our attack, let us take for n and e the numbers

$$n = 173428286141894798156748251,$$
$$e = 723753947009734907342239.$$

Suppose that n and e satisfy an equation of the form $ex - (p+1)(q+1)y = z$ with $\gcd(x, y) = 1$ and

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

Following Theorem 3.3, $\frac{x}{y}$ is among the convergents of $\frac{e}{n}$. The first convergents of the continued fraction expansion of $\frac{e}{n}$ are

$$[0, \frac{1}{239}, \frac{1}{240}, \frac{2}{479}, \frac{3}{719}, \frac{5}{1198}, \frac{8}{1917}, \frac{69}{16534}, \frac{146}{34985}, \frac{215}{51519}, \frac{361}{86504},$$
$$\frac{5269}{1262575}, \frac{16168}{3874229}, \frac{21437}{5136804}, \frac{80479}{19284641}, \frac{262874}{62990727}, \ldots].$$

Applying the factorization algorithm with the convergent $\frac{x}{y} = \frac{80479}{19284641}$, we get

$$U = \frac{ex}{y} - n - 1 \approx 27457254767091,$$
$$V = \sqrt{|U^2 - 4n|} \approx 7758072877807.$$

Applying Coppersmith's Theorem with $\frac{U+V}{2} = 17607663822449$ as an approximation for p, we get

$$p = 17607663822197, \qquad q = 9849590944783,$$

which leads to the factorization of n. Using p and q, we can compute the secret exponent d satisfying $ed \equiv 1 \pmod{(p+1)(q+1)}$, namely

$$d \equiv e^{-1} \equiv 701543110849178108139495 67 \pmod{(p+1)(q+1)},$$

Observe that $d \approx n^{0.985}$. This explains why the attacks on KMOV with small secret exponents do not work in this example.

5. Conclusion

We have presented a new attack on the KMOV cryptosystem with a public key (n, e) where $n = pq$ is an RSA modulus and e a public exponent satisfying $\gcd(e, (p+1)(q+1)) = 1$ as required by KMOV. We prove that KMOV is insecure if there exist integers x, y and z with

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

and 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 and 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 Amer. Math. Soc. **46** (1999), no. 2, 203–213.

[3] D. Coppersmith, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, J. Cryptology **10** (1997), no. 4, 233–260.

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, London, 1975.

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

[6] B. Ibrahimpašić, *Cryptanalysis of KMOV cryptosystem with short secret exponent*, Central European Conference on Information and Intelligent Systems, CECIIS, 2008.

[7] K. Koyama, U. M. Maurer, T. Okamoto, and S. A. Vanstone, *New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$*, Advances in Cryptology - Crypto'91, Lecture Notes in Computer Science, Vol. 576, 252–266, Springer-Verlag, 1991.

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

[9] R. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM **21** (1978), no. 2, 120–126.

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, GTM 106, 1986; Expanded 2nd Edition, 2009.

[11] M. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Trans. Inform. Theory **36** (1990), no. 3, 553–558.

Laboratoire de Mathématiques Nicolas Oresme
Université de Caen
France
E-mail address: abderrahmane.nitaj@unicaen.fr