J Appl Math Comput manuscript No.
(will be inserted by the editor)

A New Generalization of the KMOV Cryptosystem

Maher Boudabra · Abderrahmane Nitaj

Received: date / Accepted: date

Abstract The KMOV scheme is a public key cryptosystem based on an RSA modulus $n = pq$ where p and q are large prime numbers with $p \equiv q \equiv 2 \pmod 3$. It uses the points of an elliptic curve with equation $y^2 \equiv x^3 + b \pmod n$. In this paper, we propose a generalization of the KMOV cryptosystem with a prime power modulus of the form $n = p^r q^s$ and study its resistance to the known attacks.

Keywords KMOV cryptosystem, Elliptic curves, Prime power modulus

Mathematics Subject Classification (2000) 94A60

1 Introduction

In 1978, Rivest, Shamir and Adleman [23] proposed RSA, the first and widely used cryptosystem. The RSA scheme is composed by an RSA modulus of the form $n = pq$ and a pair of keys (e, d) where e is the public exponent and d is the private exponent, related by the congruence $ed \equiv 1 \pmod{(p-1)(q-1)}$. The security of RSA is based on the difficulty factoring large integers $n = pq$, especially when p and q are large prime numbers of the same bit-size.

Since its invention, RSA has been intensively studied for vulnerability and for efficiency (see [1,7]). In order to gain a faster decryption, Takagi [27] proposed a variant of RSA with a modulus $n = p^r q$. For similar reasons, Lim et al. [17] presented a variant of RSA and Takagi schemes with a modulus $n = p^r q^s$. Such variants are used in cryptography for various applications such as electronic cash [6] and the design of Okamoto-Uchiyama scheme [22]. The exponents in the modulus $n = p^r q^s$ should be carefully chosen to resist the factorization methods such as the Number Field Sieve and the Elliptic Curve Method. Table 1 presents the optimal number of primes in the modulus $n = p^r q^s$ according to the study in [4].

Maher Boudabra
Université de Monastir, Tunisia
E-mail: maher_boudabra@protonmail.com

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

Modulus size in bits	Form of the modulus
2048	pq, p^2q
3072	pq, p^2q
3584	pq, p^2q
4096	pq, p^2q, p^3q
8192	pq, p^2q, p^3q, p^3q^2

Table 1 Optimal number of prime factors for a specific modulus size [4].

In 1985, Miller [20] and Koblitz [11] independently proposed to use elliptic curves for cryptography (ECC). The security of the ECC systems is based on the discrete logarithm problem. Nowadays, ECC is gaining interests and various applications in cryptography are based on ECC schemes such as the elliptic curve digital signature algorithm (ECDSA) and the elliptic curve Diffie-Hellman (ECDH) protocol for key exchange. We refer to [24] for more details.

In 1992, Koyama, Maurer, Okamoto and Vanstone [13] proposed a scheme, called KMOV, based on the elliptic curve with equation $y^2 \equiv x^3 + b \pmod{n}$ over the ring $\mathbb{Z}/n\mathbb{Z}$ where $n = pq$ is an RSA modulus with $p \equiv q \equiv 2 \pmod 3$. KMOV was extended in various ways, especially to singular cubic curves by Koyama [12] with the equation $y^2 + axy = x^3 \pmod{n}$ and by Kuwakado, Koyama and Tsuruoka [14] with the singular cubic curve with equation $y^2 = x^3 + bx^2 \pmod{n}$. Demytko [5] proposed a similar scheme where only one coordinate of a point on an elliptic curve is used. The security of the former systems is based on the difficulty of factoring large composite numbers, especially RSA moduli $n = pq$ where p and q are large prime numbers of the same bit-size.

In this paper, we propose a generalization of the KMOV cryptosystem by considering a prime power RSA modulus $n = p^r q^s$ and the elliptic curve with equation $y^2 \equiv x^3 + b \pmod{n}$ over the ring $\mathbb{Z}/n\mathbb{Z}$ where b is an integer such that $\gcd(b, pq) = 1$. When $p \equiv q \equiv 2 \pmod 3$, we show that the number of points on the curve is $p^{r-1}q^{s-1}(p+1)(q+1)$. Then, we use this to build a generalized KMOV cryptosystem with key generation, encryption and decryption schemes. We give a detailed study of the security of the new generalization of the KMOV cryptosystem.

The paper is organized as follows. In Section 2, we first give an introduction to elliptic curves over the finite field $\mathbb{F}_p$ where $p \geq 5$ is a prime number, then we present some results on the elliptic curves over a ring $\mathbb{Z}/n\mathbb{Z}$ with $n = pq$ and finally we present the KMOV cryptosystem. In Section 3, we study the number of solutions of the modular multivariate polynomial equation $f(x_1, \ldots, x_k) \equiv 0 \pmod{n}$ for $n = p^r$ and $n = p^r q^s$. In Section 4, we give our generalization of the KMOV system with a modulus of the form $n = p^r q^s$. We study the security of the new system in Section 5. Finally, we conclude the paper in Section 6.

2 Preliminaries

In this section, we present some facts on elliptic curves defined over a finite field $\mathbb{F}_p$ as well as over a ring $\mathbb{Z}/n\mathbb{Z}$ where $n = pq$ is an RSA modulus, and present the KMOV cryptosystem.

2.1 Elliptic curves over a finite field

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

$$y^2 \equiv x^3 + ax + b \pmod{p}. \tag{1}$$

together with an extra point $\mathcal{O}$, called the point at infinity (see [26,24,9] for more details). A very important task in the theory of elliptic curves is counting the number of points. For a curve $E_p(a,b)$, the number of points is usually denoted $\#E_p(a,b)$ and can be computed as

$$\#E_p(a,b) = p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p} \right),$$

where $\left(\frac{\div}{p}\right)$ is the Legendre symbol which is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p}, \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

When $E_p(a,b)$ is defined over $\mathbb{F}_p$ for a prime number p, $\#E_p(a,b)$ can be approximated by $p+1$ according to Hasse Theorem (see [26,24]).

Theorem 1 *Let $E_p(a,b)$ be an elliptic curve over $\mathbb{F}_p$. Then number of points on $E_p(a,b)$ is $\#E_p(a,b) = p + 1 - t$ with*

$$t \leq 2\sqrt{p}.$$

In [25], Schoof presented an algorithm to compute the number of points on an elliptic curve with a running time of $\mathcal{O}\left(\log(p)^8\right)$ but this algorithm is not efficient for large primes. The following result gives a more precise value for $\#E_p(a,b)$ when $ab = 0$ (see [9,24]).

Theorem 2 *Let $E_p(a,b)$ be an elliptic curve over $\mathbb{F}_p$ with the equation the $y^2 \equiv x^3 + ax + b \pmod{p}$. The number of points on $E_p(a,b)$ is*

$$\#E_p(a,b) = \begin{cases} p+1 & \text{if } a = 0, b \neq 0, p \equiv 2 \pmod{3}, \\ p+1 & \text{if } a \neq 0, b = 0, p \equiv 3 \pmod{4}. \end{cases}$$

It is well known that the chord-and-tangent rule [26,24] performs the addition of two points on the elliptic curve $E_p(a,b)$ and represents $E_p(a,b)$ as an Abelian group. Indeed, the addition of two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on an elliptic curve $E_p(a,b)$ is defined as follows.

- If $P_1 = \mathcal{O}$, then $P_1 + P_2 = P_2 + P_1 = P_2$.
- If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = P_2 + P_1 = \mathcal{O}$.

– Otherwise $P_1 + P_2 = P_2 + P_1 = P_3 = (x_3, y_3)$ where

$$\begin{cases} x_3 \equiv \lambda^2 - x_1 - x_2 \pmod{p} \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod{p}, \end{cases}$$

with

$$\lambda \equiv \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \pmod{p} & \text{if } x_1 \not\equiv x_2 \pmod{p}, \\ \frac{3x_1^2 + a}{2y_1} \pmod{p} & \text{if } x_1 \equiv x_2 \pmod{p}. \end{cases}$$

The multiplication by an integer k of a point P on the curve is defined as

$$kP = P + P + \ldots + P.$$

If P is a point of the elliptic curve $E_p(a, b)$, then we have $(\#E)P = \mathcal{O}$ and for any integer k $(1 + k\#E)P = P$. For the specific situations $p \equiv 2 \pmod 3$ and $p \equiv 3 \pmod 4$, we have the following result.

Lemma 1 *Let $E_p(a, b)$ be an elliptic curve over $\mathbb{F}_p$ with the equation $y^2 \equiv x^3 + ax + b \bmod p$. Then for any integer k*

$$(1 + k(p + 1))P = \begin{cases} P & \text{if } a = 0, b \neq 0, p \equiv 2 \pmod 3, \\ P & \text{if } a \neq 0, b = 0, p \equiv 3 \pmod 4. \end{cases}$$

2.2 Elliptic curves over a ring $\mathbb{Z}/n\mathbb{Z}$

In this section, we give an overview on the theory of elliptic curves over the ring $\mathbb{Z}/n\mathbb{Z}$ where $n = pq$ is the product of two prime numbers $p \geq 5$ and $q \geq 5$. Let $a, b \in \mathbb{Z}/n\mathbb{Z}$ such that $\gcd\left(4a^3 + 27b^2, n\right) = 1$. As for finite fields, an elliptic curve $E_n(a, b)$ is the set of points $P = (x, y)$ satisfying the equation

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

together with a point $\mathcal{O}$ called the point at infinity. We can define an addition on $E_n(a, b)$ using the same rules as in the addition operation on $E_p(a, b)$. However, the addition of two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ is not always defined as in the following situations

– if $x_1 \not\equiv x_2 \pmod n$ and $\gcd(x_2 - x_1, n) \neq 1$,
– if $x_1 \equiv x_2 \pmod n$ and $\gcd(2y_1, n) \neq 1$.

This problem can be reduced by the Chinese Remainder Theorem. The point $\mathcal{O}$ is represented by the pair $(\mathcal{O}_p, \mathcal{O}_q)$ of points at infinity of $E_p(a, b)$ and $E_q(a, b)$ and every point $P = (x, y) \neq \mathcal{O}$ on $E_n(a, b)$ can be uniquely represented by a couple $(P_p, P_q) \in E_p(a, b) \times E_q(a, b)$ with $P_p = (x \pmod p, y \pmod p)$ and $P_q = (x \pmod q, y \pmod q)$. Conversely, the points of the form $(\mathcal{O}, P_q)$ and $(P_p, \mathcal{O})$ can not be represented by this method. When the primes p and q in $n = pq$ are large, it is unlikely that the addition of two points on $E_n(a, b)$ is of the form $(\mathcal{O}, P_q)$ or $(P_p, \mathcal{O})$. In the two cases, this will find the factorization of n since $\gcd(x_2 - x_1, n)$ is p or q or similarly $\gcd(2y_1, n)$ is p or q with inconsiderable probability.

Since every point $P = (x, y)$ on $E_n(a, b)$ can be uniquely represented by a couple $(P_p, P_q) \in E_p(a, b) \times E_q(a, b)$, then using Theorem 2, we get the following result.

Lemma 2 *Let $n = pq$ be the product of two large prime numbers p and q. Let $E_n(a, b)$ be an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$ with equation $y^2 \equiv x^3 + ax + b \pmod{p}$. Then for any integer k,*

$$(1 + k(p+1)(q+1))P = \begin{cases} P & \text{if } a = 0, b \neq 0, p \equiv q \equiv 2 \pmod 3, \\ P & \text{if } a \neq 0, b = 0, p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Proof Let $n = pq$ be the product of two distinct primes such that $p \equiv q \equiv 2 \pmod 3$ or $p \equiv q \equiv 3 \pmod 4$. If $P = \mathcal{O} = (\mathcal{O}_p, \mathcal{O}_q)$, then

$$(1 + k(p+1)(q+1))\mathcal{O} = \mathcal{O}$$

Now, suppose that $P \neq \mathcal{O}$ with $P = (x, y)$. Then, by the Chinese remainder theorem, P can be represented as a pair of points (P_p, P_q) with $P_p = (x \pmod p, y \pmod p)$ and $P_q = (x \pmod q, y \pmod q)$. If k is an integer, then

$$\begin{aligned} (1 + k(p+1)(q+1))P &= ((1 + k(p+1)(q+1))P_p, (1 + k(p+1)(q+1))P_q) \\ &= (P_p + k(q+1)(p+1)P_p, P_q + k(p+1)(q+1)P_q) \\ &= (P_p, P_q) \\ &= P, \end{aligned}$$

where we used $(p+1)P_p = \mathcal{O}_p$ and $(q+1)P_q = \mathcal{O}_q$ according to Theorem 2. □

2.3 The KMOV Cryptosystem

In 1991, Koyama, Maurer, Okamoto and Vanstone [13] proposed three cryptosystems based on elliptic curves over the ring $\mathbb{Z}/n\mathbb{Z}$ where $n = pq$ is an RSA modulus. In this section, we describe their Type 1 scheme. This scheme is based on a modulus of the form $n = pq$ with $p \equiv q \equiv 2 \pmod 3$ and on an elliptic curve with equation $y^2 \equiv x^3 + b \pmod n$ with $b \not\equiv 0 \pmod p$ and $b \not\equiv 0 \pmod q$.

- **Key generation.**
  1. Choose two large primes p and q with the same bit length, such that $p \equiv q \equiv 2 \pmod 3$.
  2. Compute the RSA modulus $n = pq$.
  3. Choose an integer e such that $\gcd(e, (p+1)(q+1)) = 1$. The pair (n, e) represents the public key.
  4. Compute $d \equiv e^{-1} \pmod{(p+1)(q+1)}$. The pair (n, d) represents the private key.
- **Encryption.**
  1. Represent the message as $M = (x_M, y_M) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
  2. Compute $b \equiv y_M^2 - x_M^3 \pmod n$. The elliptic curve $E_n(0, b)$ is defined by the equation $y^2 \equiv x^3 + b \pmod n$.
  3. Compute $(x_C, y_C) = e(x_M, y_M)$ on $E_n(0, b)$. The point (x_C, y_C) is the encrypted message.
- **Decryption.**
  1. Compute $b \equiv y_C^2 - x_C^3 \pmod n$. The elliptic curve $E_n(0, b)$ is defined by the equation $y^2 \equiv x^3 + b \pmod n$.

2. Compute $M = (x_M, y_M) = d(x_C, y_C)$ on $E_n(0, b)$. The point (x_M, y_M) is the original message.

The correctness of the KMOV scheme is obvious since $d \equiv e^{-1} \pmod{(p+1)(q+1)}$, then $ed - k(p+1)(q+1) = 1$ for some integer k. Also, we have

$$b \equiv y_M^2 - x_M^3 \equiv y_C^2 - x_C^3 \pmod{n}.$$

Then, by Lemma 2,

$$d(x_C, y_C) = deM = (1 + k(p+1)(q+1))M = M.$$

In [8] and [21], two attacks on KMOV have been presented, especially when d is sufficiently small. As a consequence, the private key d in the KMOV should be carefully chosen.

3 Multivariate Polynomial Equations

In this section, we study the number of solutions of a multivariate polynomial equation modulo a prime power of the form p^r. We start with the following lemma.

Lemma 3 *Let $f(t_1, \ldots, t_k) \in \mathbb{Z}[t_1, \ldots, t_k]$ be a polynomial with integer coefficients. For any integers p and $r \geq 2$, we have*

$$\begin{aligned} &f\left(t_1 + p^{r-1}h_1, \ldots, t_k + p^{r-1}h_k\right) \\ &\quad = f(t_1, \ldots, t_k) + p^{r-1} \sum_{i=1}^{k} \frac{\partial f}{\partial t_i}(t_1, \ldots, t_k)\, h_i \pmod{p^r}. \end{aligned}$$

Proof Since every polynomial is a finite sum of monomials, it is sufficient to prove the lemma for $f(t_1, \ldots, t_k) = t_1^{m_1} \ldots t_k^{m_k}$. We have

$$f\left(t_1 + p^{r-1}h_1, \ldots, t_k + p^{r-1}h_k\right) = \left(t_1 + p^{r-1}h_1\right)^{m_1} \ldots \left(t_k + p^{r-1}h_k\right)^{m_k}.$$

Observe that for $i = 1, \ldots, k$, by a binomial expansion, we get

$$\left(t_i + p^{r-1}h_i\right)^{m_i} \equiv t_i^{m_i} + m_i t_i^{m_i - 1} p^{r-1} h_i \pmod{p^r}.$$

Then

$$\begin{aligned} &f\left(t_1 + p^{r-1}h_1, \ldots, t_k + p^{r-1}h_k\right) \\ &\quad \equiv \left(t_1 + p^{r-1}h_1\right)^{m_1} \ldots \left(t_k + p^{r-1}h_k\right)^{m_k} \\ &\quad \equiv t_1^{m_1} \ldots t_k^{m_k} + p^{r-1} \left(\sum_{i=1}^{k} m_i t_1^{m_1} \ldots t_i^{m_i - 1} \ldots t_k^{m_k} h_i \right) \pmod{p^r} \\ &\quad \equiv f(t_1, \ldots, t_k) + p^{r-1} \sum_{i=1}^{k} \frac{\partial f}{\partial t_i}(t_1, \ldots, t_k)\, h_i \pmod{p^r}. \end{aligned}$$

This proves the lemma. □

Let p be an integer and $r \geq 1$. For a multivariate polynomial $f(t_1, \ldots, t_k)$, we consider the curve defined by the equation $f(t_1, \ldots, t_k) \equiv 0 \pmod{p^r}$. Every integer solution $(t_1, \ldots, t_k)$ will be considered as a point on the curve. In the following definition, we introduce the notion of a singular point.

Definition 1 Let $f(t_1, \ldots, t_k) \in \mathbb{Z}[t_1, \ldots, t_k]$ be a polynomial and p^r be a prime power integer. A point $(t_1, \ldots, t_k)$ on the curve $f(t_1, \ldots, t_k) \equiv 0 \pmod{p^r}$ is called a singular point if for all $i = 1, \ldots, k$, we have

$$\frac{\partial f}{\partial t_i}(t_1, \ldots, t_k) \equiv 0 \pmod{p}.$$

A non singular point is called a regular point.

In the following definition, we define the number of singular and regular points on a curve.

Definition 2 Let $f(t_1, \ldots, t_k) \in \mathbb{Z}[t_1, \ldots, t_k]$ be a polynomial and p^r be a prime power integer. The number of points on the curve $f(t_1, \ldots, t_k) \equiv 0 \pmod{p^r}$ is denoted c_{p^r} with

$$c_{p^r} = \#\left\{(t_1, \ldots, t_k) \in (\mathbb{Z}/p^r\mathbb{Z})^k \mid f(t_1, \ldots, t_k) \equiv 0 \pmod{p^r}\right\}$$

and the number of singular points is denoted s_{p^r} with

$$s_{p^r} = \#\{(t_1, \ldots, t_k) \in (\mathbb{Z}/p^r\mathbb{Z})^k \mid f(t_1, \ldots, t_k) \equiv 0 \pmod{p^r}, \\ \frac{\partial f}{\partial t_i}(t_1, \ldots, t_k) \equiv 0 \pmod{p},\ i = 1, \ldots, k\}.$$

A non-singular point is called a regular point. The number of regular points modulo p^r is $R_{p^r} = c_{p^r} - s_{p^r}$.

The following result gives an inductive relationship between R_{p^r} and $R_{p^{r-1}}$.

Theorem 3 *Let R_{p^r} be the number of regular points on the curve $f(t_1, \ldots, t_k) \equiv 0 \pmod{p^r}$ and $R_{p^{r-1}}$ be the number of regular points on the curve $f(t_1, \ldots, t_k) \equiv 0 \pmod{p^{r-1}}$. Then*

$$R_{p^r} = p^{k-1} R_{p^{r-1}}.$$

Proof Suppose that $f(w_1, \ldots, w_k) \equiv 0 \pmod{p^r}$. Then $f(w_1, \ldots, w_k) \equiv 0 \pmod{p^{r-1}}$. Hence, any solution $(w_1, \ldots, w_k)$ of the modular equation

$$f(w_1, \ldots, w_k) \equiv 0 \pmod{p^r}$$

is of the form

$$(w_1, \ldots, w_k) = (t_1, \ldots, t_k) + p^{r-1}(h_1, \ldots, h_k) \pmod{p^r}, \tag{3}$$

where $(t_1, \ldots, t_k)$ is a modular root of $f(t_1, \ldots, t_k) \equiv 0 \pmod{p^{r-1}}$ and $(h_1, \ldots, h_k) \in (\mathbb{Z}/p\mathbb{Z})^k$. Also note that, since for $i = 1, \ldots, k$, we have

$$\frac{\partial f}{\partial w_i}(w_1, \ldots, w_k) \equiv \frac{\partial f}{\partial t_i}(t_1, \ldots, t_k) \pmod{p},$$

then $(w_1, \ldots, w_k)$ is regular if and only if $(t_1, \ldots, t_k)$ is regular. Using (3) in Lemma 3, we get

$$f(w_1, \ldots, w_k) \equiv f(t_1, \ldots, t_k) + p^{r-1} \sum_{i=1}^{k} \frac{\partial f}{\partial w_i}(w_1, \ldots, w_k) h_i \pmod{p^r}.$$

Since $f(t_1, \ldots, t_k) \equiv 0 \pmod{p^{r-1}}$, then $f(t_1, \ldots, t_k) = up^{r-1}$ for some integer $u \in \mathbb{Z}/p\mathbb{Z}$. This implies that if $f(w_1, \ldots, w_k) \equiv 0 \pmod{p^r}$, then

$$u + \sum_{i=1}^{k} \frac{\partial f}{\partial w_i}(w_1, \ldots, w_k) h_i \equiv 0 \pmod{p}. \tag{4}$$

If $(w_1, \ldots, w_k)$ is a regular point, then $\dfrac{\partial f}{\partial w_i}(w_1, \ldots, w_k) \neq 0$ for some $i \in 1, \ldots, k$. Hence (4) is an affine equation over the field $\mathbb{Z}/p\mathbb{Z}$, which has p^{k-1} solutions $(h_1, \ldots, h_k)$. Consequently, using (3), we see that any regular point $(w_1, \ldots, w_k)$ on the curve modulo p^r is determined by a regular point $(t_1, \ldots, t_k)$ modulo p^{r-1} and p^{k-1} points $(h_1, \ldots, h_k)$ modulo p. This leads to

$$R_{p^r} = p^{k-1} R_{p^{r-1}}.$$

This terminates the proof. □

As a consequence of Theorem 3, we have the following result.

Corollary 1 *Let R_{p^r} be the number of regular points on the curve $f(t_1, \ldots, t_k) \equiv 0 \pmod{p^r}$. Then*

$$R_{p^r} = p^{(k-1)(r-1)} R_p.$$

An important consequence concerns curves without any singular points.

Corollary 2 *If a curve $f(t_1, \ldots, t_k) \equiv 0 \pmod{p^r}$ has no singular point, then the number of points on the curve is*

$$c_{p^r} = p^{(k-1)(r-1)} c_p.$$

Remark 1 For a univariate polynomial equation with non singular point, we have $k = 1$ and $c_{p^r} = c_p$, which retrieves Hensel's Lemma.

Let p^r be a prime power and b be an integer with $\gcd(p, b) = 1$. The following result allows to compute the number of solutions of the equation $y^2 \equiv x^3 + b \pmod{p^r}$ in terms of the number of solution of the equation $y^2 \equiv x^3 + b \pmod{p}$.

Corollary 3 *Let p^r be a prime power and b be an integer with $\gcd(p, b) = 1$. Then*

$$\begin{aligned} &\#\left\{(x, y) \in (\mathbb{Z}/p^r\mathbb{Z})^2 \mid y^2 \equiv x^3 + b \pmod{p^r}\right\} \\ &= p^{r-1} \#\left\{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid y^2 \equiv x^3 + b \pmod{p}\right\}. \end{aligned}$$

Proof If $y^2 \equiv x^3 + b \pmod{p^r}$, then $f(x, y) \equiv 0 \pmod{p^r}$ where $f(x, y) = y^2 - x^3 - b$. Since there is no singular point on the curve $f(x, y) \equiv 0 \pmod{p^r}$, then by Corollary 1, we get $c_{p^r} = p^{r-1} c_p$ and proves the corollary. □

In the special case $p \equiv 2 \pmod 3$, we have the following explicit result.

Corollary 4 *Let p^r be a prime power with $p \equiv 2 \pmod 3$ and b be an integer such that $\gcd(p, b) = 1$. Then*

$$\# \left\{ (x, y) \in (\mathbb{Z}/p^r\mathbb{Z})^2 \mid y^2 \equiv x^3 + b \pmod{p^r} \right\} = p^r.$$

Proof This follows Theorem 2 and Corollary 3. □

Also, when $p \equiv 2 \pmod 3$, we have an explicit result about the number of solutions of the projective curve with equation $y^2 z \equiv x^3 + bz^3 \pmod p$.

Corollary 5 *Let p be a prime number with $p \equiv 2 \pmod 3$ and b be an integer with $\gcd(p, b) = 1$. Then*

$$\# \left\{ (x, y, z) \in (\mathbb{Z}/p\mathbb{Z})^3 \mid y^2 z \equiv x^3 + bz^3 \pmod{p} \right\} = p^2.$$

Proof Suppose that $p \equiv 2 \pmod 3$ and b is an integer with $\gcd(p, b) = 1$. If $z \not\equiv 0 \pmod p$, then the equation $y^2 z \equiv x^3 + bz^3 \pmod p$ can be reduced to $y^2 \equiv x^3 + b \pmod p$. By Theorem 2, the number of points of this elliptic curve is $p+1$. Removing the point $\mathcal{O}$, we find that the number of solutions of the equation $y^2 \equiv x^3 + b \pmod p$ is p. If $z = 0$, then $x = 0$ and y is any integer with $0 \leq y \leq p-1$. Hence, the number of solutions of the equation $y^2 z \equiv x^3 + bz^3 \pmod p$ is $(p-1)p + p = p^2$. □

The former result can be extended to the equation $y^2 z \equiv x^3 + bz^3 \pmod{p^r}$. In the following, we put $(x : y : z)$ to represent the projective point with $\gcd(p, xyz) = 1$ which satisfies the following property

$$(x : y : z) = \{(\lambda x, \lambda y, \lambda z) \in (\mathbb{Z}/p^r\mathbb{Z})^3, \mid \lambda \in \mathbb{Z}/p^r\mathbb{Z}, , \ \gcd(p, \lambda) = 1\}.$$

We denote by $\mathbb{P}_{p^r}$ the set of such projective points.

Theorem 4 *Let p be a prime number with $p \equiv 2 \pmod 3$ and b be an integer with $\gcd(p, b) = 1$. Then the number of non singular points on the curve $y^2 z \equiv x^3 + bz^3 \pmod{p^r}$ is*

$$\# \left\{ (x : y : z) \in \mathbb{P}_{p^r} \mid y^2 z \equiv x^3 + bz^3 \pmod{p^r} \right\} = p^{r-1}(p+1).$$

Proof Suppose that $p \equiv 2 \pmod 3$ and b is an integer with $\gcd(p, b) = 1$. Since the only singular point of the curve with equation $y^2 z \equiv x^3 + bz^3 \pmod{p^r}$ is $(0, 0, 0)$ which is not represented in $\mathbb{P}_{p^r}$, then by combining Corollary 1 and Corollary 5, the number of regular points is

$$c_{p^r} - 1 = p^{2(r-1)}(c_p - 1) = p^{2(r-1)}(p^2 - 1).$$

Also, since each tuple $(x : y : z)$ represents $\phi(p^r) = p^{r-1}(p-1)$ tuples $(u, v, w) \in (\mathbb{Z}/p\mathbb{Z})^3$, then the number of regular solutions $(x : y : z)$ of the equation $y^2 z \equiv x^3 + bz^3 \pmod{p^r}$ is

$$\frac{p^{2(r-1)}(p^2 - 1)}{p^{r-1}(p-1)} = p^{r-1}(p+1).$$

This terminates the proof. □

We can use the former result to find the number of points on the elliptic curve defined by the equation $y^2 \equiv x^3 + b \pmod{p^r q^s}$ by splitting the curve in two pieces. The next result concerns the polynomial equation $f(t_1, \ldots, t_k) \equiv 0 \pmod{p^r q^s}$ where p and q are integers with $\gcd(p, q) = 1$.

Theorem 5 *Let $c_{p^r q^s}$ be the number of points on the curve $f(t_1, \ldots, t_k) \equiv 0 \pmod{p^r q^s}$ where $\gcd(p, q) = 1$. Then*

$$c_{p^r q^s} = c_{p^r} \times c_{q^s}.$$

Proof Since $\gcd(p, q) = 1$, then by the Chinese Remainder Theorem, there is a one to one correspondence from the set of solutions of the equation $f(t_1, \ldots, t_k) \equiv 0 \pmod{p^r q^s}$ to the set of the solutions of the system

$$f(t_1, \ldots, t_k) \equiv 0 \pmod{p^r}, \quad f(t_1, \ldots, t_k) \equiv 0 \pmod{q^s}.$$

Hence $c_{p^r q^s} = c_{p^r} \times c_{q^s}$. □

As a corollary of Theorem 5 and Corollary 4, we have the following result.

Corollary 6 *Let p^r and q^s be two prime powers such that $\gcd(p, q) = 1$, with $p \equiv q \equiv 2 \pmod 3$. Then the number of points on the elliptic curve with equation $y^2 \equiv x^3 + b \pmod{p^r q^s}$ is*

$$\begin{aligned} &\#\left\{\left\{(x, y) \in (\mathbb{Z}/p^r q^s \mathbb{Z})^2 \mid y^2 \equiv x^3 + b \pmod{p^r q^s}\right\} \cup \mathcal{O}\right\} \\ &\quad = p^r q^s + 1. \end{aligned}$$

Proof This is immediate since, by Corollary 4, we have

$$\#\left\{(x, y) \in (\mathbb{Z}/p^r \mathbb{Z})^2 \mid y^2 \equiv x^3 + b \pmod{p^r}\right\} = p^r$$

and

$$\#\left\{(x, y) \in (\mathbb{Z}/q^s \mathbb{Z})^2 \mid y^2 \equiv x^3 + b \pmod{q^s}\right\} = q^s$$

Then, by the Chinese Remainder Theorem, we get

$$\#\left\{(x, y) \in (\mathbb{Z}/p^r q^s \mathbb{Z})^2 \mid y^2 \equiv x^3 + b \pmod{p^r q^s}\right\} = p^r q^s.$$

Adding the point at infinity $\mathcal{O}$, we get the result. □

Remark 2 Notice that $\left\{\left\{(x, y) \in (\mathbb{Z}/p^r q^s \mathbb{Z})^2 \mid y^2 \equiv x^3 + b \pmod{p^r q^s}\right\} \cup \mathcal{O}\right\}$ is the set of points that we use for encryption in practice.

4 The Proposed Generalization of the KMOV Cryptosystem

In this section, we propose a generalization of the KMOV cryptosystem to elliptic curves with equation $y^2 \equiv x^3 + b \pmod{p^r q^s}$ where $\gcd(b, pq) = 1$. We will need the following lemma which is a consequence of Theorem 4 combined with the Chinese Remainder Theorem.

Lemma 4 *Let $n = p^r q^s$ be a prime power RSA modulus. Then, for any point P on the elliptic curve with equation $y^2 \equiv x^3 + b \pmod{p^r q^s}$ and any integer k, we have*

$$\left(1 + kp^{r-1}q^{s-1}(p+1)(q+1)\right) P = \mathcal{O}.$$

Recall that the previous lemma reveals why we have used the projective points rather that the affine ones, since :

1. The projective coordinates give the cardinality $p^{r-1}(p+1)$ of the curve modulo p^r, which satisfies $p^{r-1}(p+1)P = \mathcal{O}$, while the affine coordinates fail to do that because the number of points of the elliptic curve with equation $y^2 \equiv x^3 + b \pmod{p^r}$ is p^r and we have $p^r < p^{r-1}(p+1)$.
2. There is no need to add the point at infinity in the cardinality, since it is counted in $\mathbb{P}_{p^r}$ from the beginning.

Next, we describe the generalization of the KMOV cryptosystem by presenting the key generation, the encryption and the decryption.

4.1 Key generation

1. Choose two large primes p and q such that $p \equiv q \equiv 2 \pmod 3$.
2. Choose two integers r and s from the Table 1 and compute $n = p^r q^s$.
3. Choose an integer e such that $\gcd\left(e, p^{r-1}(p+1)q^{s-1}(q+1)\right) = 1$. The pair (n, e) represents the public key.
4. Compute the private exponent $d \equiv e^{-1} \pmod{p^{r-1}(p+1)q^{s-1}(q+1)}$.

4.2 Encryption

1. Represent the message as a point $M = (x_M, y_M) \in (\mathbb{Z}/n\mathbb{Z})^2$.
2. Compute $b \equiv y_M^2 - x_M^3 \pmod n$.
3. Compute $C = eM = (x_C, y_C)$ on the elliptic curve $y^2 = x^3 + b \pmod n$.
4. Send the encrypted message C.

4.3 Decryption

1. Compute $b \equiv y_C^2 - x_C^3 \pmod n$.
2. Compute the message $M = dC$ on the elliptic curve $y^2 = x^3 + b \pmod n$.

The decryption is exact since $de \equiv 1 \pmod{p^{r-1}(p+1)q^{s-1}(q+1)}$ and there exists an integer k such that $de = 1 + kp^{r-1}(p+1)q^{s-1}(q+1)$. Hence, using Lemma 4, we get

$$dC = deM = \left(1 + kp^{r-1}(p+1)q^{s-1}(q+1)\right) M = M.$$

5 Security of the New Cryptosystem

In this section, we discuss the security of the proposed scheme.

5.1 Factoring the modulus

In our scheme, the modulus is of the form $n = p^r q^s$ where p and q are two prime numbers with $p \equiv q \equiv 2 \pmod 3$. When p and q are large and the exponents r and s are chosen according to Table 1, the problem is believed hard (see [4,3]) as for the RSA situation where the modulus is $n = pq$. The factoring methods such as the Elliptic Curve Method [15] and the Number Field Sieve [16] are ineffective for large primes p and q.

5.2 Finding the order

For an elliptic curve curve with equation

$$y^2 \equiv x^3 + ax + b \pmod p,$$

where p is a large prime number, there is no known method to find the number of solutions of the underlying equation. This is valid when the equation is in the form

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

where n is the product of large unknown prime factors. This shows that finding the order $\psi(n) = p^{r-1}q^{s-1}(p+1)(q+1)$ in the new scheme is unfeasible.

Comparatively, in the original KMOV, the modulus is $n = pq$ and the order is $(p+1)(q+1)$ while in the standard RSA the modulus is similar and the order is $(p-1)(q-1)$. Finding one of these orders is known to be computationally equivalent to factoring the modulus $n = pq$. In our new scheme, the modulus is $n = p^r q^s$ and the order is $\psi(n) = p^{r-1}q^{s-1}(p+1)(q+1)$. Hence, finding the order $\psi(n)$ will lead to p and q. It follows that finding the order in the new scheme is also equivalent to factoring the modulus.

On the other hand, note that the order $\psi(n)$ represents the number of points on the elliptic curve with equation

$$y^2 z \equiv x^3 + bz^3 \pmod n,$$

where the factorization of n is unknown. It is known that by the Chinese Remainder Theorem, finding a solution modulo n can be done by finding a solution modulo p^r and modulo q^s. Since the factorization of n is unknown, this is infeasible.

5.3 Solving the elliptic curve discrete logarithm

In the new scheme, the public parameters are the modulus $n = p^r q^s$, the exponent e, the ciphertext $C = (x_C, y_C)$ which is computed as $C = eM = e(x_M, y_M)$ on the elliptic curve with equation

$$y^2 \equiv x^3 + b \pmod n, \quad b \equiv y_M^2 - x_M^3 \pmod n.$$

Solving the equation $C = eM$ for M is equivalent to solving the discrete logarithm problem since if P is a point on the elliptic curve such that $M = uP$, then $C = eM = euP$ and finding u is computationally infeasible since the elliptic curve discrete logarithm problem is hard (see [10]).

5.4 Solving the key equation

In the new scheme, the public exponent e and the private exponent d are related with the modular equation $ed \equiv 1 \pmod{p^{r-1}q^{s-1}(p+1)(q+1)}$, or equivalently by the equation

$$ed - kp^{r-1}q^{s-1}(p+1)(q+1) = 1.$$

This equation is related to the prime power RSA key equation

$$ed - kp^{r-1}q^{s-1}(p-1)(q-1) = 1,$$

which has been intensively studied. In [18], it is shown that if $r, s > 1$, and

$$d < n^{1-\frac{3r+s}{(r+s)^2}},$$

then one can find d and factor the modulus $n = p^r q^s$. In [19], for $s = 1$, the bound is

$$d < n^{\frac{r(r-1)}{(r+1)^2}}.$$

Observe that the key equation in our scheme is slightly different from the prime power RSA key equation, nevertheless, the techniques are similar and we conclude that when d is sufficiently large, then the equation is not vulnerable to the former attacks. For comparison, in the standard RSA and KMOV, the bound for vulnerability is $d < n^{0.292}$ (see [2,8]).

5.5 Impossible addition on the elliptic curve method

As the elliptic curve is defined over the ring $\mathbb{Z}/p^r q^s\mathbb{Z}$, then the addition is not always defined if one of the inversion modulo p^r or modulo q^s is not possible. This situation can be used to factor the modulus $n = p^r q^s$. On the other hand, this scenario is very unlikely to happen and the following result gives a precise probability.

Corollary 7 *The probability that the sum of two points on the elliptic curve with equation $y^2 \equiv x^3 + b \pmod{p^r q^s}$ is not defined is approximately*

$$\frac{p^{r-1}\,(p+1)\,q^{s-1}\,(q+1) - (p^r q^s + 1)}{p^{r-1}\,(p+1)\,q^{s-1}\,(q+1)} \approx \frac{p+q}{(p+1)(q+1)}.$$

Proof We first give an estimation of solutions $(x : y : z)$ of the equation

$$y^2 z \equiv x^3 + bz^3 \pmod{p^r q^s},$$

with $\gcd(pq, z) = 1$. Notice that

$$\begin{aligned}
&\left\{(x : y : z) \in \mathbb{P}_{p^r q^s},\, p \nmid z,\, q \nmid z \mid zy^2 \equiv x^3 + bz^3 \pmod{p^r q^s}\right\} \\
&\quad = \left\{(x : y : 1) \in \mathbb{P}_{p^r q^s}, \mid zy^2 \equiv x^3 + bz^3 \pmod{p^r q^s}\right\} \\
&\quad = \left\{(x, y) \in \mid y^2 \equiv x^3 + b \pmod{p^r q^s}\right\}
\end{aligned}$$

therefore

$$\#\left\{(x:y:z)\in(\mathbb{Z}/p^rq^s\mathbb{Z})^3 \mid \gcd(pq,z)=1, zy^2=x^3+bz^3\right\}\cup\mathcal{O}=p^rq^s+1$$

We know that the sum of two points on the curve $zy^2\equiv x^3+bz^3 \pmod{p^rq^s}$ is not defined if and only if the third coordinate of the sum is divisible by p or q but not divisible by p^rq^s. The probability of such situations is

$$\begin{aligned}\frac{p^{r-1}(p+1)q^{s-1}(q+1)-(p^rq^s+1)}{p^{r-1}(p+1)q^{s-1}(q+1)} &= \frac{p+q}{(p+1)(q+1)}+\frac{p^{r-1}q^{s-1}-1}{p^{r-1}(p+1)q^{s-1}(q+1)}\\ &\approx \frac{p+q}{(p+1)(q+1)}\end{aligned}$$

This shows that the probability that the sum of two points is not defined is very low since when p and q are large and of the same bit size, then $\frac{p+q}{(p+1)(q+1)}\approx\frac{1}{\sqrt{pq}}$. □

6 Conclusion.

We presented a generalization of the KMOV cryptosystem by using an elliptic curve defined on the ring $\mathbb{Z}/n\mathbb{Z}$ where $n=p^rq^s$ is a prime power modulus. We described the theory for computing the number of points on the elliptic curve $y^2\equiv x^3+b \pmod{n}$ and gave an explicit estimation when $p\equiv q\equiv 2 \pmod 3$. Finally, we studied the security of the new system and showed that it is mainly based on factoring the modulus.

References

1. Boneh, D.: Twenty years of attacks on the RSA cryptosystem, Notices of the American Mathematical Society (AMS) **46**(2), 203–213 (1999)
2. 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 **1592**, Springer-Verlag, 1–11 (1999)
3. Boneh, D., Durfee, G., and Howgrave-Graham, N.: Factoring $N=p^rq$ for Large r. In M. Wiener, Ed., Crypto'99, Lecture Notes in Computer Science **1666**, Springer-Verlag, 326–337 (1999)
4. Compaq Computer Corporation: Cryptography Using Compaq MultiPrime Technology in a Parallel Processing Environment (2000)
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, 40–49 (1994)
6. Fujioka, A., Okamoto, T., Miyaguchi, S.: ESIGN: An Efficient Digital Signature Implementation for Smard Cards. Eurocrypt 1991, Lecture Notes in Computer Science **547**, Springer-Verlag, 446–457 (1991)
7. Hinek, M.J.: Cryptanalysis of RSA and its Variants, Chapman & Hall/CRC Cryptography and Network Security. CRC Press, Boca Raton, FL (2010)
8. Ibrahimpasic, B.: Cryptanalysis of KMOV cryptosystem with short secret exponent, Central European Conference on Information and Intelligent Systems, CECIIS (2008)
9. Ireland, K., Rosen M.: A Classical Introduction to Modern Number Theory, Springer-Verlag (1990)
10. Joux, A., Odlyzko A., Pierrot C.: The past, evolving present, and future of the discrete logarithm. In: Koç, C.K., (Ed.) Open Problems in Mathematics and Computational Science, Springer International Publishing, Berlin, 5–36 (2014).
11. Koblitz, N.: Elliptic curve cryptosystems. Mathematics of Computation, **48**, 203–209 (1987)

12. Koyama, K.: Fast RSA type scheme based on singular cubic curve $y^2+axy = x^3 \pmod n$. Proc. Eurocrypt'95, Lecture Notes in Computer Science, **921**, Springer-Verlag, 329–339 (1995)
13. Koyama, K., Maurer, U.M., Okamoto T., Vanstone S.A.: 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, 252–266 (1991)
14. Kuwakado H., Koyama K., Tsuruoka, Y.: A new RSA-type scheme based on singular cubic curves $y^2 \equiv x^3+bx^2 \pmod n$, IEICE Transactions on Fundamentals, E78-A, 27–33 (1995)
15. Lenstra, H.W.: Factoring integers with elliptic curves. Annals of Mathematics **126**, 649–673 (1987)
16. A. K. Lenstra, A.K., H. W. Lenstra, H.W. Jr.: The development of the number field sieve, Lecture Notes in Mathematics **1554**, Springer-Verlag (1993)
17. Lim S., Kim S., Yie I., Lee H.: A Generalized Takagi-Cryptosystem with a modulus of the form $p^r q^s$ in Advances in Cryptography - Proceedings of Indocrypt 1998, Lecture Notes in Computer Science **1977**, Springer-Verlag, 283–294 (2000)
18. Lu, Y., Peng, L., Sarkar, S.: Cryptanalysis of an RSA variant with Moduli $N = p^r q$. Pascale Charpin, Nicolas Sendrier, Jean-Pierre Tillich. The 9th International Workshop on Coding and Cryptography 2015 WCC2015, Apr 2015, Paris, France (2016)
19. Lu Y., Zhang R., Peng L., Lin D.: Solving Linear Equations Modulo Unknown Divisors: Revisited. In: Iwata T., Cheon J. (eds) Advances in Cryptology – ASIACRYPT 2015. Lecture Notes in Computer Science **9452**, Springer-Verlag (2015)
20. Miller, V.S.: Use of elliptic curves in cryptography. In H. C. Williams, editor, Advances in Cryptology - CRYPTO'85, Lecture Notes in Computer Science **218**, Springer-Verlag, 417–426 (1986)
21. Nitaj A.: A new attack on the KMOV cryptosystem, Bulletin of the Korean Mathematical Society **51** (5), 1347–1356 (2014)
22. Okamoto T., Uchiyama S.: A New public key cryptosystem as secure as factoring. Eurocrypt 1998, Lecture Notes in Computer Science **1403**, 308–318 (1998)
23. Rivest R., Shamir A. and Adleman L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, **21** (2), 120–126 (1978)
24. Schmitt, S., Zimmer, H.G.: Elliptic Curves. A Computational Approach. Walter de Gruyter, Berlin (2003)
25. Schoof, R.: Elliptic curves over finite fields and the computation of square roots mod p. Math. Comp. **44**, 483–494 (1985)
26. Silverman, J.H.: The Arithmetic of Elliptic Curves, Springer-Verlag, GTM **106**, 1986, Expanded 2nd Edition, (2009)
27. Takagi, T.: Fast RSA-Type Cryptosystem Modulo $p^k q$ in Advances in Cryptography - Proceedings of CRYPTO 1998, Lecture Notes in Computer Science **1462**, Springer-Verlag, 318–326 (1998)