How to choose secret parameters for RSA-type cryptosystems over elliptic curves

MARC JOYE joye@ee.tku.edu.tw
Laboratory of Cryptography and Information Security,
Dept of Electrical Engineering, Tamkang University,
Tamsui, Taipei Hsien 25137, TAIWAN, R.O.C.

JEAN-JACQUES QUISQUATER jjq@dice.ucl.ac.be
UCL Crypto Group & Laboratoire de Microélectronique,
Dép. d'Électricité, Université de Louvain,
Place du Levant 3, B-1348 Louvain-la-Neuve, BELGIUM

TSUYOSHI TAKAGI ttakagi@slab.ntt.co.jp
NTT Software Laboratories,
3-9-11, Midori-cho Musashino-shi, Tokyo 180-8585, JAPAN

Abstract. Recently, and contrary to the common belief, Rivest and Silverman argued that the use of *strong primes* is unnecessary in the RSA cryptosystem. This paper analyzes how valid this assertion is for RSA-type cryptosystems over elliptic curves. The analysis is more difficult because the underlying groups are not always cyclic. Previous papers suggested the use of strong primes in order to prevent factoring attacks and cycling attacks. In this paper, we only focus on cycling attacks because for both RSA and its elliptic curve-based analogues, the length of the RSA-modulus n is typically the same. Therefore, a factoring attack will succeed with equal probability against all RSA-type cryptosystems. We also prove that cycling attacks reduce to find fixed points, and derive a factorization algorithm which (most probably) completely breaks RSA-type systems over elliptic curves if a fixed point is found.

Keywords: RSA-type cryptosystems, Cycling attacks, Elliptic curves, Strong primes.

1. Introduction

The theory of elliptic curves has been extensively studied for the last 90 years. In 1985, Koblitz and Miller independently suggested their use in cryptography [9, 19]. After this breakthrough, elliptic curve-based analogues of RSA cryptosystem were proposed [10, 4].

RSA-type systems belong to the family of public-key cryptosystems. A public-key cryptosystem is a pair of public encryption function f_K and a secret decryption function f_K^{-1} indexed by a key K and representing a permutation on a finite set $\mathcal{M}$ of messages. The particularity of such systems is that given the encryption function f_K, it is computationally infeasible to recover f_K^{-1}. Moreover, it might be suitable that the encryption function does not let the message unchanged, i.e. given a message $m \in \mathcal{M}$, we want that $f_K(m) \neq m$. This is known as the *message-concealing problem* [3]. Simmons and Norris [29] exploited this feature for possibly recovering a plaintext from the only public information. Their attack, the so-

Technical Report No. TI-35/97
Technische Universität Darmstadt
November 1997

called *cycling attack*, relies on the cycle detection of the ciphertext. This was later generalized by Williams and Schmid [31] (see also [7, 1]).

There are basically two ways to compromise the security of cryptosystems. The first one is to find protocol failures [20] and the other one is to directly attack the underpinning crypto-algorithm. The cycling attack and its generalizations fall into the second category. So, it is important to carefully analyze the significance of this attack. For RSA, Rivest and Silverman [25] (see also [16]) concluded that the chance that a cycling attack will succeed is negligible, whatever the form of the public modulus n. For elliptic curve-based systems, the analysis is more difficult because the underlying group is not always cyclic. We will actually give some results valid for groups of any rank, but we will mainly dwell on the security of KMOV and Demytko's system.

The paper is organized as follows. In Section 2, we review KMOV and Demytko's system. We extend the message-concealing problem to elliptic curves in Section 3. Then, we show how this enables to mount a cycling attack on KMOV and Demytko's system in Section 4. We explain how the secret factors can be recovered thanks to the cycling attack in Section 5. Finally, in Section 6, we give some concluding remarks in order to help the programmer to implement *"secure"* RSA-type cryptosystems.

2. Elliptic curves

Let $n = pq$ be the product of two large primes p and q, and let two integers a, b such that $\gcd(4a^3 + 27b^2, n) = 1$. An *elliptic curve* $E_n(a, b)$ over the ring $\mathbb{Z}_n$ is the set of points $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n$ satisfying the Weierstraß equation

$$E_n(a, b) : y^2 = x^3 + ax + b, \tag{1}$$

together with a single element $\mathcal{O}_n$ called the *point at infinity*.

Let $E_p(a, b)$ be an elliptic curve defined over the prime field $\mathbb{F}_p$. It is well known that the *chord-and-tangent rule* [17, § 2.2] makes $E_p(a, b)$ into an Abelian group. Algebraically, we have:

(i) $\mathcal{O}_p$ is the identity element, i.e. $\forall \mathbf{P} \in E_p(a, b)$, $\mathbf{P} + \mathcal{O}_p = \mathbf{P}$.

(ii) The inverse of $\mathbf{P} = (x_1, y_1)$ is $-\mathbf{P} = (x_1, -y_1)$.

(iii) Let $\mathbf{P} = (x_1, y_1)$ and $\mathbf{Q} = (x_2, y_2) \in E_p(a, b)$ with $\mathbf{P} \neq -\mathbf{Q}$.
Then $\mathbf{P} + \mathbf{Q} = (x_3, y_3)$ where

$$x_3 = \lambda^2 - x_1 - x_2 \quad \text{and} \quad y_3 = \lambda(x_1 - x_3) - y_1, \tag{2}$$

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

The points of $E_n(a,b)$ unfortunately do not form an Abelian group. But writing $\widetilde{E}_n(a,b)$ for the group given by the direct product $\widetilde{E}_n(a,b) = E_p(a,b) \times E_q(a,b)$ and since $E_n(a,b) \subset \widetilde{E}_n(a,b)$, we can "add" points of $E_n(a,b)$ by the chord-and-tangent rule. For large p and q, the resulting point will be a point of $E_n(a,b)$ with high probability [10].

It is useful to introduce some notations. Let $\mathbf{P} = (p_1, p_2) \in E_n(a,b)$. Whenever it is defined, $[k]\mathbf{P}$ will denote $\mathbf{P} + \mathbf{P} + \cdots + \mathbf{P}$ (k times) on $E_n(a,b)$. The x-coordinate of $\mathbf{P}$ will be denoted by $\mathrm{x}(\mathbf{P})$. Moreover, since p_2 (the y-coordinate of $\mathbf{P}$) is not required to compute the x-coordinate of $[k]\mathbf{P}$, we will write $[k]_x\, p_1$ for $\mathrm{x}([k]\mathbf{P})$.

We can now define an analogue of RSA. The public encryption key e is chosen relatively prime to

$$N_n = \mathrm{lcm}(\#E_p(a,b), \#E_q(a,b)), \tag{3}$$

and the secret decryption key d is chosen according to $ed \equiv 1 \pmod{N_n}$. To encrypt a point $\mathbf{P} \in E_n(a,b)$, one computes the ciphertext $\mathbf{Q} = [e]\mathbf{P}$. Then, the authorized receiver recovers $\mathbf{P}$ by computing $\mathbf{P} = [d]\mathbf{Q}$ with his secret key d.

The only problem is to imbed messages as points on a given elliptic curve without the knowledge of the secret factors p and q. A first solution was proposed by Koyama, Maurer, Okamoto and Vanstone [10]. Another one was later proposed by Demytko [4].

2.1. KMOV

KMOV cryptosystem uses a family of supersingular elliptic curves of the form

$$E_n(0,b) : y^2 = x^3 + b. \tag{4}$$

The main property of this system is that if p and q are both congruent to 2 mod 3, then $N_n = \mathrm{lcm}(p+1, q+1)$ whatever the value of parameter b. Therefore, to encrypt a message $\mathbf{M} = (m_1, m_2)$, b is chosen according to

$$b = m_2^2 - m_1^3 \bmod n, \tag{5}$$

and the ciphertext is given by $\mathbf{C} = [e]\mathbf{M}$ over the curve $E_n(0,b)$. The plaintext is then recovered by $\mathbf{M} = [d]\mathbf{C}$.

Another possibility is to work with elliptic curves of the form $E_n(a,0)$ with p and q both congruent to 3 mod 4. The first system based on $E_n(0,b)$ with $p, q \equiv 2 \pmod 3$ will be referred as *Type 1 scheme*, and the second one based on $E_n(a,0)$ with $p, q \equiv 3 \pmod 4$ as *Type 2 scheme*. Later, both systems were extended by Kuwakado and Koyama to form-free primes [12].

2.2. Demytko's system

Demytko's system uses fixed parameters a and b. It has the particularity to only make use of the x-coordinate of points of elliptic curves. It relies on the fact that

if a number x is not the x-coordinate of a point on an elliptic curve $E_p(a,b)$, then it will be the x-coordinate of a point of the *twisted curve* $\overline{E_p(a,b)}$ defined as the set of points (x,y) satisfying

$$\overline{E_p(a,b)} : y^2 = x^3 + ax + b \tag{6}$$

where $y = u\sqrt{v}$ and v is a fixed quadratic non-residue modulo p, together with the point at infinity. So, N_n is given by

$$N_n = \mathrm{lcm}(E_p(a,b), \overline{E_p(a,b)}, E_q(a,b), \overline{E_q(a,b)}). \tag{7}$$

A message m is encrypted as $c = [e]_x\, m$. Then, m is recovered from the ciphertext c by $m = [d]_x\, c$.

For efficiency purposes, the original scheme (see [4]) was presented with message-dependent decryption keys. The length of the decryption key is divided by a factor of 2, on average. However, in the sequel, we will use the message-independent description because this simplifies the analysis, and because we are not concerned with efficiency issues.

3. Concealing-message problem

In [3], Blakley and Borosh showed that there are always at least 9 messages that are unconcealable (i.e. the ciphertext of a message is exactly the same as the cleartext) for any RSA cryptosystem. Though this problem is well-known for RSA, nothing appears in the literature about its elliptic curve-based analogues. Since unconcealed messages must be avoided, effective criteria are needed for evaluating the concealing power of these latter systems.

Before analyzing the number of unconcealed messages for elliptic curve-based systems, we will first give some general group-theoretic results.

LEMMA 1 *Let G be an Abelian (multiplicatively written) finite group of order $\#G$. Consider the map $\pi_k : G \to G, x \mapsto x^k$. Then π_k permutes the elements of G if and only if* $\gcd(k, \#G) = 1$. ■

THEOREM 1 *Let G be an Abelian (multiplicatively written) finite group of rank r whose generators are $g_1, g_2, \ldots, g_r$. If $\pi_k : G \to G, x \mapsto x^k$ permutes the elements of G, then π_k has exactly*

$$\mathrm{Fix}(G,k) = \prod_{i=1}^{r} \gcd(k-1, \#\langle g_i \rangle) \tag{8}$$

fixed points.

Proof: Write $G = \{g_1^{x_1} g_2^{x_2} \cdots g_r^{x_r} \mid 0 \le x_i < \#\langle g_i \rangle, i = 1, \ldots, r\}$. So,

$$\begin{aligned} \pi_k(x) = x &\iff g_1^{(k-1)x_1} g_2^{(k-1)x_2} \cdots g_r^{(k-1)x_r} = 1 \\ &\iff (k-1)\, x_i \equiv 0 \pmod{\#\langle g_i \rangle} \quad \text{for } i = 1, 2, \ldots, r. \end{aligned}$$

Each equation has $\gcd(k-1, \#\langle g_i \rangle)$ solutions. There are thus $\prod_{i=1}^{r} \gcd(k-1, \#\langle g_i \rangle)$ fixed points by the permutation map π_k. ■

Let p and q be distinct primes and let $n = pq$. By unconcealed message on RSA, we mean a message $m \in \mathbb{Z}_n$ so that $m^e \equiv m \pmod{n}$ for a fixed integer e satisfying $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.[1] This latter condition ensures that the exponentiation by e is a permutation map, or equivalently that RSA encryption is a permutation of $\mathbb{Z}_n$.

COROLLARY 1 *Let $n = pq$ be the RSA-modulus and let e be the RSA-encryption key. Then, the number of unconcealed messages for RSA is given by*

$$\mathrm{Fix}(\mathbb{Z}_n, e) = (\gcd(e-1, p-1) + 1)\,(\gcd(e-1, q-1) + 1). \tag{9}$$

Proof: Since $\mathbb{Z}_p = \mathbb{F}_p^* \cup \{0\}$ and since 0 is always solution to $x^e \equiv x \pmod{p}$, Theorem 1 tells that there are $(\gcd(e-1, p-1) + 1)$ fixed points in $\mathbb{Z}_p$. Moreover, since $\mathbb{Z}_n = \mathbb{Z}_p \times \mathbb{Z}_q$ by Chinese remaindering, the proof is complete. ■

Note that since p, q and e are odd integers, there are at least 9 unconcealed messages for the original RSA system. If we exclude to encrypt 0 and ± 1 (that are always unconcealable messages), there are at least 6 unconcealed messages.

An elliptic curve $E_p(a, b)$ over the prime field $\mathbb{F}_p$ is an Abelian group of rank 1 or 2 and of type (n_1, n_2) [17, Theorem 2.12]. Therefore, we can write $E_p(a, b) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ with $n_2 \mid n_1$ and $n_2 \mid p - 1$. If we call *x-fixed point* a point $\mathbf{P} \in E_p(a, b)$ such that, when given an integer k, $\mathrm{x}([k]\mathbf{P}) = \mathrm{x}(\mathbf{P})$, then Theorem 1 becomes:

THEOREM 2 *Let $E_p(a, b)$ be an elliptic curve over the prime field $\mathbb{F}_p$. If*

$$\pi_k : E_p(a, b) \to E_p(a, b), \mathbf{P} \mapsto [k]\mathbf{P}$$

permutes $E_p(a, b) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, then π_k has exactly

$$\mathrm{Fix}(E_p(a, b), k) = \gcd(k-1, n_1)\ \gcd(k-1, n_2) \tag{10}$$

fixed points. Furthermore, π_k has exactly

$$\begin{aligned} \mathrm{Fix}_x(E_p(a, b), k) = {} & \gcd(k-1, n_1)\ \gcd(k-1, n_2) + \\ & \gcd(k+1, n_1)\ \gcd(k+1, n_2) - \nu_2 - 1 \end{aligned} \tag{11}$$

x-fixed points, where ν_2 is the number of points of order 2.

Proof: The first part follows immediately from Theorem 1.

Let $\mathbf{P} \in E_p(a, b)$. $\mathbf{P}$ is a x-fixed point if and only if $[k]\mathbf{P} = \mathbf{P}$ or $[k]\mathbf{P} = -\mathbf{P}$. If we let $E_p(a, b) = \{\mathbf{P} = [u]\mathbf{R} + [v]\mathbf{S} \mid 0 \le u < n_1 \text{ and } 0 \le v < n_2\}$, we have

$$\begin{aligned} \mathrm{x}(\pi_k(\mathbf{P})) = \mathrm{x}(\mathbf{P}) &\iff [(k \mp 1)u]\mathbf{R} + [(k \mp 1)v]\mathbf{S} = \mathcal{O}_p \\ &\iff \begin{cases} (k \mp 1)u \equiv 0 \pmod{n_1} \\ (k \mp 1)v \equiv 0 \pmod{n_2} \end{cases}. \end{aligned}$$

Since $\mathcal{O}_p$ and points of order 2 are counted twice, we obtain Eq. (11). Indeed, $[k-1]\mathbf{P} = [k+1]\mathbf{P}$ if and only if $[2]\mathbf{P} = \mathcal{O}_p$. ■

KMOV Type 1 scheme is based on elliptic curves of the form $E_p(a,b)$ with $a = 0$ and $p \equiv 2 \pmod 3$. The underlying group is isomorphic to the cyclic group $\mathbb{Z}_{p+1}$. Type 2 scheme uses curves of the form $E_p(a,b)$ where $b = 0$ and $p \equiv 3 \pmod 4$. In that case, the underlying group is also isomorphic to $\mathbb{Z}_{p+1}$ if a is a quadratic residue modulo p; and it is isomorphic to $\mathbb{Z}_{\frac{p+1}{2}} \oplus \mathbb{Z}_2$ otherwise. From Eq. (10), for an odd $k \geq 3$, we see that, for a *given* KMOV elliptic curve $E_p(a,b)$, there are at least 2 fixed points if $E_p(a,b)$ is cyclic and at least 4 fixed points otherwise. These points correspond to the point at infinity together with the points of order 2. Noting that the encryption key e is always odd for KMOV, and since the point at infinity is not used to represent messages, there are at least 1, 3 or 9 unconcealed messages on a given KMOV elliptic curve $E_n(a,b)$. Consequently, the probability that a random message is unconcealed can be at least $1/n$. This has to be compared with $6/n$ for the original RSA.

Demytko's encryption works in a group of the form $G_p^{(i)} \times G_q^{(j)}$ $(1 \leq i,j \leq 2)$, where $G_p^{(1)} = E_p(a,b)$, $G_p^{(2)} = \overline{E_p(a,b)}$, $G_q^{(1)} = E_q(a,b)$ and $G_q^{(2)} = \overline{E_q(a,b)}$. Writing $G_p^{(i)} \cong \mathbb{Z}_{n_{1,p}^{(i)}} \oplus \mathbb{Z}_{n_{2,p}^{(i)}}$, we define

$$\text{x-Fix}(G_p^{(i)}, e) = \frac{\gcd(e-1, n_{1,p}^{(i)})\,\gcd(e-1, n_{2,p}^{(i)}) + \gcd(e+1, n_{1,p}^{(i)})\,\gcd(e+1, n_{2,p}^{(i)})}{2}, \tag{12}$$

and similarly for $G_q^{(j)}$. Demytko's system only makes use of the x-coordinate. So, since the point at infinity is never used for encryption, Theorem 2 indicates that there are $\sum_{1 \leq i,j \leq 2} (\text{x-Fix}(G_p^{(i)}, e) - 1)(\text{x-Fix}(G_q^{(j)}, e) - 1)$ unconcealed messages.[2] This number may be equal to 0, and we cannot give general information on the minimal number of unconcealed messages in Demytko's system.

For efficiency purposes, the public encryption key e is usually relatively small (for example, $e = 3$ or $e = 2^{16} + 1$ are common choices). In all systems, the number of unconcealed messages depends on expressions of the form $\big(\gcd(e \pm 1, \#G_p)\,\gcd(e \pm 1, \#G_q)\big)$. Therefore, the maximal number of unconcealed messages is mainly bounded by $(e \pm 1)^2$. So, if the encryption key is equal to $2^{16} + 1$, then the probability that a message is unconcealed is at most $\approx 10^{-144}$ for a 512-bit RSA-modulus and $\approx 10^{-299}$ for a 1024-bit RSA-modulus. Even if the number of unconcealed messages is small, we will see in the next section how this can be turned into an active attack.

4. Cycling attack

4.1. Previous results on RSA

Let $c = m^e \bmod n$ be the ciphertext corresponding to message m, where (e,n) is the public key. If we find an integer k that satisfies the equation

$$c^{e^k} \equiv c \pmod n, \tag{13}$$

then we can obviously recover the plaintext m by computing $m = c^{e^{k-1}} \bmod n$.

Note that we do not have to factor the public modulus n, so this might be a serious failure for the RSA cryptosystem. This attack, firstly proposed by Simmons and Norris [29], was later extended by Williams and Schmid [31] (see also [7]) in the following way. Let $\mathcal{P}(t)$ be a polynomial. They showed that if the ciphertext c has a period such that

$$c^{\mathcal{P}(g)} \equiv 1 \pmod{n} \tag{14}$$

for some integer g, then the plaintext m can be recovered.

4.2. Generalizing the cycling attack

We can generalize the results of the previous paragraph to any Abelian finite group G.

THEOREM 3 *Let G be an Abelian (multiplicatively written) finite group. Let a message $m \in G$ and let $c = m^e$ be the corresponding ciphertext, where* $\gcd(e, \#G) = 1$.[3] *If we find an integer P such that $c^P = 1$ in G, then the plaintext m can be recovered by computing*

$$m = c^Q, \tag{15}$$

where Q satisfies $eQ \equiv 1 \pmod{P'}$ and $P' = P/\gcd(e, P)$.

Proof: Let $t = \mathrm{ord}_G(m)$, i.e. t is the smallest integer such that $m^t = 1$ in G. By Lagrange's Theorem, $t \mid \#G$ and since $\gcd(e, \#G) = 1$, it follows that $\gcd(e, t) = 1$. So, $c^P = m^{eP} = 1$ implies that $t \mid eP$ and thus $t \mid P$. Therefore, $\exists \alpha \in \mathbb{Z}$ such that $P = \alpha t$ and we have $m^{P/\alpha} = 1$. Moreover, $\gcd(e, t) = 1$ yields $\gcd(e, P) = \gcd(e, \alpha t) = \gcd(e, \alpha) \mid \alpha$. Hence, letting $P' = P/\gcd(e, P)$, we obtain $m^{P'} = 1$. Since $eQ \equiv 1 \pmod{P'}$, we can write $eQ = \delta P' + 1$ for some integer δ, and $c^Q = m^{eQ} = m^{\delta P'} m = m$. ■

We call this theorem the *generalized cycling attack*. This theorem indicates that KMOV and Demytko's system are also susceptible to the cycling attack.

Detecting the integer P is equivalent to the problem of finding a polynomial $\mathcal{P}(t)$ and an integer $t = g$ with $P = \mathcal{P}(g)$. Moreover, the relation $c^{\mathcal{P}(g)} = 1$ is equivalent to

$$\mathcal{P}(g) \equiv 0 \pmod{\mathrm{ord}_G(c)}. \tag{16}$$

If $\#G = \prod_{i=1}^{r} p_i^{f_i}$ denotes the prime decomposition of group order $\#G$ and since $\mathrm{ord}_G(c)$ divides $\#G$, Eq. (16) can be reduced to

$$\mathcal{P}(g) \equiv 0 \pmod{p_i^{f_i}}, \tag{17}$$

for all primes p_i dividing $\mathrm{ord}_G(c)$.

Here, we must check that these relations hold by picking up a random polynomial $\mathcal{P}(t)$ and a random integer $t = g$. This means that the cycling attack depends on the distribution of such polynomial and of the order of ciphertext c.

Roughly speaking, if the order of G is smooth, we can expect that there are many elements $c \in G$ with small order. So, primes p_i in Eq. (17) will be small, and polynomial $\mathcal{P}$ will be more easily found. Consequently, it might be desirable to impose that $\#G$ contains at least one large prime in order to make harder the cycling attack. We will now analyze in more details this assumption for elliptic curve-based systems.

4.3. Application to elliptic curve systems

As previously mentioned, an elliptic curve $E_p(a, b,)$ over the prime field $\mathbb{F}_p$ is not necessarily cyclic, but isomorphic to $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ with $n_2 \mid n_1$ and $n_2 \mid p-1$. Therefore, for analyzing the cycling attack over elliptic curves, we have to estimate the number of points in $E_p(a, b)$ of a given order. If $n_2 = 1$ (i.e. $E_p(a, b)$ is a cyclic group), then the number of elements of order d is given by the Euler's totient function, namely $\phi(d)$. For the general case, we have:

PROPOSITION 1 *Let $E_p(a, b)$ be an elliptic curve over the prime field $\mathbb{F}_p$. If we write $E_p(a, b) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ with $n_2 \mid n_1$, then the number of elements of order d is equal to*

$$F(d) = \phi(d)\ \gcd(d, n_2) \prod_{p_i \in \Omega_{d,n_2}} \left(\frac{p_i + 1}{p_i}\right), \tag{18}$$

where Ω_{d,n_2} is the set of primes $p_i \mid n_2$ such that $\mathrm{var}_{p_i}(d) \leq \mathrm{var}_{p_i}(n_2)$, and $\mathrm{var}_{p_i}(n)$ is the power of p_i which appears in the prime decomposition of n.
Furthermore, given the prime factorization of $\gcd(\#E_p(a, b), p - 1)$, $F(d)$ can be computed in probabilistic polynomial time.

Note that if $\Omega_{d,n_2} = \emptyset$, then we take $\prod_{p_i \in \Omega_{d,n_2}} (\frac{p_i+1}{p_i}) = 1$.

Proof: The first part of the proposition is proved in Appendix A. The second part follows from Miller's probabilistic polynomial time algorithm for finding n_1 and n_2 (see [17, §5.4]). ■

We can now derive a lower bound on the number of elements whose order is divisible by a large prime factor of the order of $E_p(a, b)$.

PROPOSITION 2 *Let $E_p(a, b)$ be an elliptic curve over the prime field $\mathbb{F}_p$. Suppose that $\#E_p(a, b)$ is exactly divisible by a prime factor l_p. If $F_{\mathrm{div}}(l_p)$ denotes the number of elements of order divisible by l_p, then*

$$F_{\mathrm{div}}(l_p) = \phi(l_p)\, \frac{\#E_p(a, b)}{l_p}. \tag{19}$$

Proof: See Appendix B. ■

This proposition indicates that if we randomly pick up an element in $E_p(a,b)$, it has order divisible by l_p with probability $\phi(l_p)/l_p = 1 - 1/l_p$. When l_p is large, this probability is non-negligible (i.e. really "nearly 1").

RSA-type cryptosystems over elliptic curves are constructed on groups of the form $E_n(a,b)$, which can be considered as $E_p(a,b) \times E_q(a,b)$ by Chinese remaindering. In the sequel, we will suppose that $\#E_p(a,b)$ (resp. $\#E_q(a,b)$) contains a large prime factor l_p (resp. l_q). With high probability, a random point $\mathbf{P}_p \in E_p(a,b)$ (resp. $\mathbf{P}_q \in E_q(a,b)$) will have order divisible by l_p (resp. l_q). Therefore a random point $\mathbf{P}$ on $E_n(a,b)$ (represented by $\mathbf{P} = [\mathbf{P}_p, \mathbf{P}_q]$ by Chinese remaindering) will have order divisible by l_p and l_q with high probability.

As we discussed in Paragraph 4.2, the cycling attack is reduced to find a polynomial $\mathcal{P}$ and an integer g with $c^{\mathcal{P}(g)} = 1$ for some ciphertext c. For elliptic curves, this attack becomes *"Find a polynomial $\mathcal{P}$ and an integer g so that $[\mathcal{P}(g)]\mathbf{C} = \mathcal{O}_n$ for some ciphertext $\mathbf{C} \in E_n(a,b)$"*. Equivalently, this can be formulated by an expression of the form of Eq. (17). Since the order of ciphertext $\mathbf{C}$ is supposed to be divisible by l_p and l_q with high probability, we must have $\mathcal{P}(g) \equiv 0 \pmod{l_p}$ and $\mathcal{P}(g) \equiv 0 \pmod{l_q}$ to mount a successful cycling attack. Williams and Schmid [31] estimated that these relations are rarely fulfilled except when $\mathcal{P}(t) = t - 1$ and $t = e^k$ for some k. So, we have thus to take care whether or not

$$e^k \equiv 1 \pmod{l_p}, \tag{20}$$

and similarly for prime q. Letting $\mathrm{ord}_{l_p}(e)$ for the smallest integer satisfying Eq. (20), k must be a multiple of $\mathrm{ord}_{l_p}(e)$. Consequently, the cycling attack will be useless if $\mathrm{ord}_{l_p}(e)$ is large.

NOTE 1 In his fast generation algorithm of secure keys, Maurer [15] suggested to verify that $e^{(l_p-1)/r_{i_p}} \not\equiv 1 \pmod{l_p}$ for $i = 1, \ldots, s$, where $l_p - 1 = \prod_{i=1}^{s} r_{i_p}^{\alpha_i}$ is the prime decomposition of $l_p - 1$. This criteria implies that $\mathrm{ord}_{l_p}(e)$ must be large and the cycling attack is not applicable. Another method is to impose that $l_p - 1$ contains a large prime factor r_p. The probability that $\mathrm{ord}_{l_p}(e)$ is divisible by r_p will be then $1 - 1/r_p$.

Proof: Let $l_p - 1 = r_p \prod_{i=1}^{t} p_i^{e_i}$ (with $\gcd(r_p, p_i) = 1$) be the prime decomposition of $l_p - 1$. The number of elements in $\mathbb{Z}_{l_p}^*$ whose order divisible by r_p is given by $\sum_{d \mid \frac{l_p-1}{r_p}} \phi(r_p d) = \phi(r_p) \sum_{d \mid \frac{l_p-1}{r_p}} \phi(d) = \phi(r_p) \frac{l_p-1}{r_p} = (1 - 1/r_p) \#\mathbb{Z}_{l_p}^*$. ■

This is known as the *strong primes criteria*.

Through this section, we have proven some conditions to preclude cycling attacks. Putting all together, we have:

THEOREM 4 *The cycling attack does not apply against KMOV if the secret prime p has the following properties: (i) $p+1$ has a large prime factor l_p, and (ii) $\mathrm{ord}_{l_p}(e)$ is large; and similarly for prime q.* ■

THEOREM 5 *The cycling attack does not apply against Demytko's system if the elliptic curves over $\mathbb{F}_p$ have the following properties: (i) $\#E_p(a,b)$ has a large prime factor l_p and $\#\overline{E_p(a,b)}$ has a large prime factor l'_p, and (ii)* $\mathrm{ord}_{l_p}(e)$ *and* $ord_{l'_p}(e)$ *are large; and similarly for prime q.* ■

5. Factoring the RSA-modulus

5.1. Relation between unconcealed message and cycling attack

For a given ciphertext $\mathbf{C} \in E_n(a,b)$, the cycling attack detects an integer k satisfying $[e^k]\mathbf{C} = \mathbf{C}$. This is equivalent to the message-concealing problem where the message is now a ciphertext instead of a cleartext. If $E_p(a,b) \cong \mathbb{Z}_{n_{1,p}} \oplus \mathbb{Z}_{n_{2,p}}$ with $n_{2,p} \mid n_{1,p}$ and if $E_q(a,b) \cong \mathbb{Z}_{n_{1,q}} \oplus \mathbb{Z}_{n_{2,q}}$ with $n_{2,q} \mid n_{1,q}$, from Theorem 2, we know that there are

$$\begin{aligned}\mathrm{Fix}(E_n(a,b), e^k) = \ & \gcd(e^k - 1, n_{1,p}) \gcd(e^k - 1, n_{2,p}) \cdot \\ & \gcd(e^k - 1, n_{1,q}) \gcd(e^k - 1, n_{2,q})\end{aligned} \tag{21}$$

unchanged ciphertexts $\mathbf{C}$ via encryption by e^k. Moreover, by Eq. (20), $[e^k]\mathbf{C} = \mathbf{C}$ yields $l_p \mid e^k - 1$ for some (large) prime l_p dividing $\#E_p(a,b) = n_{1,p}n_{2,p}$, and similarly for prime q. So the number of unchanged ciphertexts $\mathbf{C}$ is larger than $l_p l_q$.

Suppose that primes p and q were chosen so that both $\#E_p(a,b)$ and $\#E_q(a,b)$ contain a large prime factor l_p and l_q, respectively. Then, there may be many ciphertexts $\mathbf{C}$ such that $[e^k]\mathbf{C} = \mathbf{C}$, and the corresponding cleartexts can be recovered. This means that a cycling attack is really effective when applicable. To prevent this attack, the designer has also to verify that $\mathrm{ord}_{l_p}(e)$ (resp. $\mathrm{ord}_{l_q}(e)$) is large (see Theorems 4 and 5).

5.2. Factoring by means of fixed points

In Section 4, we explained how the cycling attack can recover a plaintext. Here, we will show that the knowledge of a unchanged ciphertext enables still more, i.e. to completely break the system by factoring the RSA-modulus $n = pq$.

This can be illustrated by the elliptic curve factoring method (ECM) [13] introduced by Lenstra. It can basically be described as follows. Suppose that n is the product of two primes p and q. Consider an elliptic curve $E_n(a,b)$ over the ring $\mathbb{Z}_n$. Assume that $\#E_p(a,b)$ or $\#E_q(a,b)$ is B-smooth. Then define $r = \mathrm{lcm}(1,2,\ldots,B)$ and choose a random $\mathbf{P} \in E_n(a,b)$—note that $[r]\mathbf{P} = \mathcal{O}_n \in E_n(a,b)$. Then compute $[r]\mathbf{P}$ in $E_n(a,b)$ (and not in $E_p(a,b) \times E_q(a,b)$ because p and q are unknown). As mentioned in Section 2, some points are not "realizable" because $E_n(a,b)$ is not a group. During the computation of $[r]\mathbf{P}$, at step i, three situations can occur: (i) $[r_i]\mathbf{P} = \mathcal{O}_p \pmod p$ and $[r_i]\mathbf{P} \neq \mathcal{O}_q \pmod q$, (ii) $[r_i]\mathbf{P} \neq \mathcal{O}_p \pmod p$ and $[r_i]\mathbf{P} = \mathcal{O}_q \pmod q$, or (iii) $[r_i]\mathbf{P} = \mathcal{O}_p \pmod p$ and $[r_i]\mathbf{P} = \mathcal{O}_q \pmod q$. In cases (i) and (ii), the denominator of λ in the chord-and-tangent formulas (see

Eq. (2)) will have a non-trivial factor with n. So n is factored. In case (iii), $[r]\mathbf{P}$ is correctly computed, we obtain $[r]\mathbf{P} = \mathcal{O}_n$. No factor of n is found and we then re-iterate the process with another point $\mathbf{P}$ or with other parameters a and b.

Let $\mathrm{ord}_p(\mathbf{P})$ and $\mathrm{ord}_q(\mathbf{P})$ be the order of point $\mathbf{P}$ in $E_p(a,b)$ and $E_q(a,b)$, respectively. Let π be a prime. We can write $\mathrm{ord}_p(\mathbf{P}) = \pi^{f_p} s_p$ with $f_p \geq 0$ and $\gcd(\pi, s_p) = 1$, and $\mathrm{ord}_q(\mathbf{P}) = \pi^{f_q} s_q$ with $f_q \geq 0$ and $\gcd(\pi, s_q) = 1$. Hence, if we know an integer r of the form $r = \mathrm{lcm}(\pi^{f_p} s_p, \pi^{f_q} s_q)\pi^f s$ with $\gcd(\pi, s) = 1$, we must have $[r]\mathbf{P} = \mathcal{O}_n$ in $E_n(a,b)$. If $f_p \neq f_q$, or without loss of generality $f_p < f_q$, then we define $r' = \frac{r}{\pi^{f+f_q-f_p}}$. So, we have $\mathrm{ord}_p(\mathbf{P}) \mid r'$ and $\mathrm{ord}_q(\mathbf{P}) \nmid r'$, or equivalently

$$[r']\mathbf{P} = \mathcal{O}_p \pmod{p} \quad \text{and} \quad [r']\mathbf{P} \neq \mathcal{O}_q \pmod{q} \tag{22}$$

and we find a non-trivial factor of n similarly as in ECM.

The message-concealing problem or the cycling attack is due to the presence of fixed points $\mathbf{P} \in E_n(a,b)$ such that $[r]\mathbf{P} = \mathbf{P}$. We have $r = e$ and $\mathbf{P} = \mathbf{M}$ for message-concealing problem, and $r = e^k$ and $\mathbf{P} = \mathbf{C}$ for the cycling attack. The knowledge of a fixed point $\mathbf{P}$ gives $[r-1]\mathbf{P} = \mathcal{O}_n$. We are then in the conditions of ECM and the RSA-modulus can be factored with some probability as follows.

[Step 1] Let $i \leftarrow 0$. Choose a prime power factor π of $r-1$, i.e. $\pi^t \, mid (r-1)$

[Step 2i] Put $r' \leftarrow (r-1)/\pi^i$.

[Step 3] Compute $[r']\mathbf{P}$ in $E_n(a,b)$.
If an error occurs (i.e. Eq. (22) is satisfied[4]), then n is factored. Otherwise, if $i < t$ then $i \leftarrow i+1$ and go to Step 2i; if $i = t$ then go to Step 1.

The next theorem says more about the probability of factoring the RSA-modulus n using one iteration of this method.

THEOREM 6 *Consider KMOV or Demytko's system. Let* $E_p(a,b) \cong \mathbb{Z}_{\pi^{F_p} S_p} \oplus \mathbb{Z}_{\pi^{A_p} B_p}$ *with* $\pi^{A_p} B_p \mid \pi^{F_p} S_p$ *and* $E_q(a,b) \cong \mathbb{Z}_{\pi^{F_q} S_q} \oplus \mathbb{Z}_{\pi^{A_q} B_q}$ *with* $\pi^{A_q} B_q \mid \pi^{F_q} S_q$, *and* π *is prime. Let* γ_π *denotes the probability that* $F_p + F_q \geq 2\max(A_p, A_q)$. *If we know a fixed point* $\mathbf{P} \neq \mathcal{O}_n$ *such that* $[r-1]\mathbf{P} = \mathcal{O}_n$ *and if* $r-1$ *is divisible by* π, *then we can factor the RSA-modulus* $n = pq$ *with probability at least* $\gamma_\pi \frac{2(\pi^2-1)}{\pi^2(\pi^2+1)}$.

Proof: See in Appendix C. ■

Assume for example that $\gamma_\pi = 0.5$ and that we know a point $\mathbf{P}$ such that $[r-1]\mathbf{P} = \mathcal{O}_n$. If $2 \mid (r-1)$ (which is the most probable case), then our algorithm will find the secret factors of n with probability at least 15%. Otherwise, we re-iterate the algorithm with another prime factor π of $r-1$.

5.3. Remark on efficiency

Reconsider the cycling attack $[e^k]\mathbf{C} = \mathbf{C} \pmod{n}$. From Eq. (20), k must be a multiple of both $\mathrm{ord}_{l_p}(e)$ and $\mathrm{ord}_{l_q}(e)$ to apply the attack. However, what we ultimately need to factor the modulus n is to find an integer r' such that, for example,

$[r']\mathbf{C} = \mathcal{O}_p \pmod{p}$ and $[r']\mathbf{C} \neq \mathcal{O}_q \pmod{q}$ (see Eq. (22)); or equivalently, such that $[r'+1]\mathbf{C} = \mathbf{C} \pmod{p}$ and $[r'+1]\mathbf{C} \neq \mathbf{C} \pmod{q}$. This means that a cycling attack just modulo p (or modulo q) rather than modulo both primes simultaneously enables to factor n. Therefore, k needs to be just a multiple of $\mathrm{ord}_{l_p}(e)$ or of $\mathrm{ord}_{l_q}(e)$, not of both of them. This results in a higher probability of success.

6. Concluding remarks

In Section 4, we proved that if the conditions of Theorems 4 and 5 are fulfilled, then cycling attacks are useless for elliptic curve-based RSA systems. This is the elliptic version of the well-known strong primes criteria. For RSA, Rivest and Silverman [25] claimed that this criteria is not required. They said:

"Strong primes offer little protection beyond that offered by random primes."

We will now analyze more accurately how valid this assertion is, and if it remains valid for elliptic curve-based systems. The analogue of Theorems 4 and 5 for original RSA is:

THEOREM 7 *Let $n = pq$ be the RSA modulus and let e be the public encryption exponent. The cycling attack does not apply against RSA if the secret prime p has the following properties: (i) $p-1$ has a large prime factor l_p, and (ii) $l_p - 1$ has a large prime factor r_p (cf Note 1); and similarly for prime q.* ■

A prime p satisfying conditions (i) and (ii) of the previous theorem is said to be a *strong prime*. Some authors also recommend that (iii) $p+1$ has a large prime factor. Condition (iii) is required in order to protect against the $p+1$ factoring algorithm [30].

In their paper, Rivest and Silverman only consider the primes p and q. They did not take into account the second condition of Theorem 7.[5] Our analysis is based on a previous work of Knuth and Trabb-Pardo [11] (see also [22, pp. 161–163]), whom rigorously calculated the distribution of the largest, second largest, ... prime factors of random numbers. Also, they have tabulated:

Table 1. Proportion $\rho(\alpha)$ of (large) numbers N whose largest prime factor is $\leq N^{1/\alpha}$.

α	1.5	2.0	2.5	3.0	4.0	5.0	6.0	8.0
$\rho(\alpha)$	0.594535	0.306853	0.130320	0.048608	0.004911	0.000355	$2{\cdot}10^{-5}$	$3{\cdot}10^{-8}$

We can now more precisely quantify what "large" means in Theorem 7 in order to prevent cycling attacks. A cycling attack remains to find an integer k such that $c^{e^k} \equiv c \pmod{n}$ for some ciphertext c, where e is the public encryption key and $n = pq$ is the RSA-modulus. From k, the plaintext m corresponding to c is then given by $m = c^{e^{k-1}} \bmod n$. However, we noticed in §5.3 that it just suffices to mount a cycling attack modulo p (instead of modulo n) to factor the RSA-modulus. For RSA, the secret prime factors are recovered as follows. Suppose that there exists

an integer k such that $c^{e^k} \equiv c \pmod{p}$ and $c^{e^k} \not\equiv c \pmod{q}$, then $\gcd(c^{e^k} - c, n)$ will give p; and hence $q = n/p$. Knowing p and q, the secret key d is computed as $d = e^{-1} \bmod \mathrm{lcm}(p-1, q-1)$ and the plaintext m is then given by $m = c^d \bmod n$.

From Eqs (17) and (20), if l_p denotes the largest prime factor of $p-1$, k must be (with probability $1-1/l_p)^6$ a multiple of $\mathrm{ord}_{l_p}(e)$ to apply the cycling attack modulo p; we thus have $k \geq \mathrm{ord}_{l_p}(e)$ with probability at least $1 - 1/l_p$. From Knuth and Trabb-Pardo's results, we can derive how does a *typical* integer k look. We note that an average case analysis makes a sense since the distribution of the largest prime factor, the second largest prime factor, ... is monotone. The average size of l_p is $(p-1)^{0.624} \approx p^{0.624}$ [11]; and similarly, the average size of the largest prime factor r_p of $l_p - 1$ is $(l_p - 1)^{0.624} \approx p^{0.389}$. (Note that we suppose that $l_p - 1$ and $p-1$ behave like random numbers. This assumption was confirmed by experimental results using the LiDIA package [14]: over 1 000 000 random 100-bit primes l_p, 423 were such that $l_p - 1$ was a 20-bit smooth number, that is, a proportion of $0.000423 \approx 10^{-3.37}$. This has to be compared with $\rho(5.0) \approx 10^{-3.45}$.) The average size of the second largest prime factor r'_p of $l_p - 1$ is $(l_p - 1)^{0.210} \approx p^{0.131}$ [11]. Hence, since $r_p r'_p$ divides $\mathrm{ord}_{l_p}(e)$ with probability $(1 - 1/r_p)(1 - 1/r'_p) \approx 1 - 1/p^{0.131}$ (see Note 1), we have $k \geq r_p r'_p$ with probability at least $(1 - 1/l_p)(1 - 1/p^{0.131}) \approx 1 - 1/p^{0.131}$. For a 512-bit RSA modulus $n = pq$, this probability is already greater than $1 - 10^{-10}$; and is greater than $1 - 10^{-20}$ for a 1024-bit modulus. In summary, we have:

Table 2. Lower bound K on a typical value for k such that $c^{e^k} \equiv c \pmod{p}$ for a t-bit RSA modulus $n = pq$.

t	512 bits	768 bits	1024 bits
Lower bound K	10^{40}	10^{60}	10^{80}

Albeit very high, the estimation of the bound K (see Table 2) is quite pessimistic; in practice, k will be much larger than K and a cycling attack (modulo p) will have thus fewer chances to be effective. Indeed, if we take into account the third largest prime r''_p of l_p, we have $k \geq r_p r'_p r''_p$ with probability at least $\approx 1 - 1/r''_p$; for example, for a 1024-bit RSA modulus, we have $k \geq 10^{88}$ with probability at least $1 - 10^{-8}$. More importantly, we only take into account the largest prime factor l_p of $p-1$. Let l'_p be the second largest prime factor of $p-1$, its average size is $(p-1)^{0.210} \approx p^{0.210}$. The ciphertext c has its order divisible $l_p l'_p$ with probability at least $(1 - 1/l_p)(1 - 1/l'_p) \approx 1 - 1/p^{0.210}$. Therefore, from Eq. (17) (see also Eq. (20)), k is very likely (i.e., with probability $(1 - 1/l_p)(1 - 1/l'_p) \approx 1 - 1/p^{0.210}$) a multiple of $\mathrm{lcm}(\mathrm{ord}_{l_p}(e), \mathrm{ord}_{l'_p}(e))$. The largest prime factor s_p of $l'_p - 1$ has an average size of $(l'_p - 1)^{0.624} \approx p^{0.131}$. So, we have $k \geq r_p r'_p s_p$ with a probability of at least $(1 - 1/p^{0.210})(1 - 1/p^{0.131})^2 \approx 1 - 2/p^{0.131}$; for example, for a 1024-bit RSA modulus, we have $k \geq 10^{100}$ with probability at least $1 - 2 \cdot 10^{-40}$.

Consequently, k is expected to be very large, and a cycling attack will thus have very little chance to be successful.

Hasse's Theorem [27, Theorem 1.1] indicates that $\#E_p(a,b) \in [p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$, and we can thus consider that $\#E_p(a,b) = O(p)$ and p have the same

bit-size. Therefore, from Theorems 4 and 5, the previous discussion still applies to elliptic curve-based cryptosystems and the conclusion of Rivest and Silverman remains valid, i.e. the use of strong primes offers (quasi) no additional security against cycling attacks.

However, as remarked by Pinch [21], a user might intentionally choose a "weak" RSA-modulus. Suppose that a user chooses his public RSA-modulus $n = pq$ so that a cycling attack is possible. In that case, this user can repudiate a document by asserting that an intruder has discovered *by chance* (the probability of a cycling attack is negligible) the weakness. If the use of strong primes is imposed in standards [8], such arguments cannot be used for contesting documents in court.

In conclusion, from a mathematical point of view, strong primes are not needed, but they may be useful for other purposes (e.g., legal issues). On the other hand, since the generation of strong primes is only just a little bit more time consuming, there is no reason to not use them.

Acknowledgments

We are grateful to Jean-Marc Couveignes for providing useful comments on a previous version of this work. We also thank Markus Maurer for teaching us how to use LiDIA.

Notes

1. $\phi(n)$ is the Euler's totient function and denotes the number of positive integers not greater than and relatively prime to n.
2. Note that this expression slightly differs from Eq. (11). This is because Eq. (11) counts the number of x-fixed points; here we have to count the number of x-coordinates that are unchanged by Demytko's encryption.
3. This condition is equivalent to $\pi_e(x) = x^e$ in G is a permutation map (see Lemma 1).
4. Or if $[r']\mathbf{P} \neq \mathcal{O}_p \pmod{p}$ and $[r']\mathbf{P} = \mathcal{O}_q \pmod{q}$ is satisfied.
5. See [25] on p. 17: "Suppose r does *not* divide $\mathrm{ord}(e) \bmod \lambda(N)$". Note also the typo, N should be replaced by $\lambda(N)$.
6. This is the probability that l_p divides $\mathrm{ord}_{\mathbb{Z}_p^*}(c)$ (see Note 1).

References

1. S. Berkovits. Factoring via superencryption. *Cryptologia*, 6(3):229–237, 1982.
2. B. Blakley and G.R. Blakley. Security of number theoretic cryptosystems against random attack, I, II, III. *Cryptologia*, 2(4):305–312, 1978, 3(1):29–42, 1979, 3(2):105–118, 1979.
3. G.R. Blakey and I. Borosh. Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages. *Comp & Maths. with Appls.*, 5:169–178, 1979.
4. N. Demytko. A new elliptic curve based analogue of RSA. In T. Helleseth, editor, *Advances in Cryptology – EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 40–49. Springer-Verlag, 1994.
5. J. Gordon. Strong RSA keys. *Electronics Letters*, 20(12):514–516, 1984.
6. J.A. Gordon. Strong primes are easy to find. In T. Beth, N. Coth, and I. Ingermarsson, editors, *Advances in Cryptology – EUROCRYPT84*, volume 209 of *Lecture Notes in Computer Science*, pages 216–223. Springer-Verlag, 1985.

7. T. Herlestam. Critical remarks on some public-key cryptosystems. *BIT*, 17:493–496, 1978.
8. International Organization for Standardization. The RSA public-key cryptosystem. Annex C of *ISO/IEC 9594-8*, Geneva (Switzerland), 1989.
9. N. Koblitz. Elliptic curve cryptosystems. *Math. of Comp.*, 48(177):203–209, 1987.
10. 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 J. Feigenbaum, editor, *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 252–266. Springer-Verlag, 1992.
11. D.E. Knuth and L. Trabb-Pardo. Analysis of a simple factorization algorithm. *Theoretical Computer Sc.*, 3:321–348, 1976.
12. H. Kuwakado and K. Koyama. Efficient cryptosystems over elliptic curves based on a product of form-free primes. *IEICE Trans. Fundamentals*, E77-A(8):1309–1318, 1994.
13. H.W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Mathematics*, 126:649–673,1987.
14. The LiDIA Group. LiDIA – A library for computational number theory. Available at URL `http://www.informatik.tu-darmadt.de/TI/LiDIA`, Technische Universität Darmstadt, Germany.
15. U.M. Maurer. Fast generation of secure RSA-moduli with almost maximal diversity. In J.-J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology – EUROCRYPT '89*, volume 434 of *Lecture Notes in Computer Science*, pages 636–647. Springer-Verlag, 1990.
16. U.M. Maurer. Fast generation of prime numbers and secure public-key cryptographic parameters. *Journal of Cryptology*, 8(3):123–155, 1995. An earlier version appeared in [15].
17. A.J. Menezes. *Elliptic curve public key cryptosystems.* Kluwer Academic Publishers, 1993.
18. A.J. Menezes, P.C. van Oorschot and S.A. Vanstone. *Handbook of applied cryptography*, CRC Press, 1997.
19. V. Miller. Use of elliptic curves in cryptography. In H. C. Williams, editor, *Advances in Cryptology – CRYPTO '85*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer-Verlag, 1986.
20. J.H. Moore. Protocol failures in cryptosystems. In G. Simmons, editor, *Contemporary Cryptology*, pages 541–558. IEEE Press, 1992.
21. R.G.E. Pinch. On using Carmichael numbers for public-key encryption systems. In M. Darnell, editor, *Cryptography and Coding*, volume 1355 of *Lecture Notes in Computer Science*, pages 265–269, Springer-Verlag, 1997.
22. H. Riesel. *Prime Numbers and Computer Methods for Factorization.* Birkhäuser, 2nd ed., 1994.
23. R.L. Rivest. Remarks on a proposed cryptanalytic attack on the M.I.T. public-key cryptosystem. *Cryptologia*, 2(1):62–65, 1978.
24. R.L. Rivest. Critical remarks on "Critical remarks on some public-key cryptosystems" by T. Herlestam. *BIT*, 19:274–275, 1979.
25. R.L. Rivest and R.D. Silverman. Are 'strong' primes needed for RSA. In *The 1997 RSA Laboratories Seminar Series*, Seminars Proceedings, 1997.
26. R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.
27. J.H. Silverman. *The Arithmetic of Elliptic Curves.* GTM 106, Springer-Verlag, 1986.
28. R.D. Silverman. Fast generation of random, strong RSA primes. *CryptoBytes*, 3(1):9–13, 1997.
29. G.J. Simmons and M.J. Norris. Preliminary comment on the M.I.T. public-key cryptosystem. *Cryptologia*, 1:406–414, 1977.
30. H.C. Williams. A $p+1$ method of factoring. *Math. of Comp.*, 39(159):225–234, July 1982.
31. H.C. Williams and B. Schmid. Some remarks concerning the M.I.T. public-key cryptosystem. *BIT*, 19:525–538, 1979.

Appendix A

Proof of Proposition 1

LEMMA 2 *Let $G_p = \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, where p is a prime and α, β are integers with $\alpha \geq \beta$. If $F(p^f)$ denotes the number of elements with order p^f in G_p, then*

$$F(p^f) = \phi(p^f)\ \gcd(p^f, p^\beta)\,\Delta, \tag{A.1}$$

where $\Delta = (p+1)/p$ if $f \leq \beta$ and $\Delta = 1$ otherwise.

Proof: Since $G_p = \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, we will represent the elements in G_p as (a, b) with $a \in \mathbb{Z}_{p^\alpha}$ and $b \in \mathbb{Z}_{p^\beta}$. Moreover, in the sequel, a_i (resp. b_i) will denote an element of order p^i in $\mathbb{Z}_{p^\alpha}$ (resp. $\mathbb{Z}_{p^\beta}$).

(i) Suppose $f > \beta$. Then elements of order p^f are of the form (a_f, b) for any $b \in \mathbb{Z}_{p^\beta}$. Since there are $\phi(p^f)$ elements of order p^f in $\mathbb{Z}_{p^\alpha}$ and since there are p^β elements in $\mathbb{Z}_{p^\beta}$, we have $F(p^f) = \phi(p_f)\, p^\beta$ and Eq. (A.1) is satisfied.

(ii) Suppose $f = \beta$. Then elements of order p^f are either of the form (a_f, b) for any $b \in \mathbb{Z}_{p^\beta}$ or (a_i, b_f) for $i = 0, \ldots, f-1$. So, we obtain

$$F(p^f) = \phi(p^f)p^\beta + \sum_{i=0}^{f-1} \phi(p^i)\,\phi(p^f) = \phi(p^f)\,(p^\beta + p^{f-1}) = \phi(p^f)\,p^\beta\Delta.$$

(iii) Suppose that $f < \beta$. Then elements of order p^f are of the form (a_f, b_f) or (a_f, b_i) for $0 \leq i \leq f-1$ or (a_i, b_f) for $0 \leq i \leq f-1$. Therefore,

$$\begin{aligned} F(p^f) &= \phi(p^f)\,\phi(p^f) + \sum_{i=0}^{f-1} \phi(p^f)\,\phi(p^i) + \sum_{i=0}^{f-1} \phi(p^i)\,\phi(p^f) \\ &= \phi(p^f)^2 + 2\,\phi(p^f)p^{f-1} \\ &= \phi(p^f)\big(\phi(p^f) + 2p^{f-1}\big) = \phi(p^f)\,p^{f-1}(p+1) = \phi(p^f)\,p^f\Delta, \end{aligned}$$

which concludes the proof. ■

PROPOSITION 1 *Let $E_p(a, b)$ be an elliptic curve over the prime field $\mathbb{F}_p$. If we write $E_p(a, b) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ with $n_2 \mid n_1$, then the number of elements of order d is equal to*

$$F(d) = \phi(d)\ \gcd(d, n_2) \prod_{p_i \in \Omega_{d,n_2}} \Big(\frac{p_i + 1}{p_i}\Big), \tag{A.2}$$

where Ω_{d,n_2} is the set of primes $p_i \mid n_2$ such that $\mathrm{var}_{p_i}(d) \leq \mathrm{var}_{p_i}(n_2)$, and $\mathrm{var}_{p_i}(n)$ is the power of p_i which appears in the prime decomposition n.

Note that if $\Omega_{d,n_2} = \emptyset$, then we take $\prod_{p_i \in \Omega_{d,n_2}} (\frac{p_i+1}{p_i}) = 1$.

Proof: Since $n_2 \mid n_1$, we can write $n_1 = \prod_{i=1}^{r} p_i^{\alpha_i}$ $(\alpha_i \geq 1)$ and $n_2 = \prod_{i=1}^{r} p_i^{\beta_i}$ $(\beta_i \geq 0)$. By Chinese remaindering, $E_p(a,b)$ is isomorphic to a product of p_i-primary groups of the form $\mathbb{Z}_{p_i^{\alpha_i}} \oplus \mathbb{Z}_{p_i^{\beta_i}}$. Consider the group $G_{p_i} = \mathbb{Z}_{p_i^{\alpha_i}} \oplus \mathbb{Z}_{p_i^{\beta_i}}$. By Lemma 2, the number of elements of order $p_i^{f_i}$ in G_{p_i} is equal to

$$\phi(p_i^{f_i})\ \gcd(p_i^{f_i}, p_i^{\beta_i})\,\Delta_i.$$

Consequently, if $d = \prod_{i=1}^{r} p_i^{f_i}$, there are

$$\begin{aligned} F(d) &= \prod_{i=1}^{r} \phi(p_i^{f_i})\ \gcd(p_i^{f_i}, p_i^{\beta_i})\Delta_i = \phi(d)\ \gcd(d, n_2) \prod_{i=1}^{r} \Delta_i \\ &= \phi(d)\ \gcd(d, n_2) \prod_{p_i \in \Omega_{d,n_2}} \Big(\frac{p_i+1}{p_i}\Big) \end{aligned}$$

elements of order d in $E_p(a,b)$. ■

Appendix B

Proof of Proposition 2

LEMMA 3 *For any $n_2 \mid n$, we have*

$$\sum_{d \mid n} \phi(d) \gcd(d, n_2) \prod_{p_i \in \Omega_{d,n_2}} \big(\tfrac{p_i+1}{p_i}\big) = n n_2. \tag{B.1}$$

Proof: Let the prime decompositions $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ $(\alpha_i \geq 1)$ and $n_2 = \prod_{i=1}^{r} p_i^{\beta_i}$ $(\beta_i \geq 0)$. Since $d \mid n$, we can write $d = \prod_{i=1}^{r} p_i^{j_i}$ with $0 \leq j_i \leq \alpha_i$. We define symbol $\delta_{j_i} = 1$ if $1 \leq j_i \leq \beta_i$, and $\delta_{j_i} = 0$ if $j_i = 0$ or $\beta_i < j_i \leq \alpha_i$. So, we can write

$$\prod_{p_i \in \Omega_{d,n_2}} \Big(\frac{p_i+1}{p_i}\Big) = \prod_{i=1}^{r} \Big(\frac{p_i+1}{p_i}\Big)^{\delta_{j_i}},$$

whence

$$\begin{aligned} \sum_{d \mid n} \phi(d) &\quad \gcd(d, n_2) \prod_{p_i \in \Omega_{d,n_2}} \big(\tfrac{p_i+1}{p_i}\big) \\ &= \sum_{j_1=0}^{\alpha_1} \sum_{j_2=0}^{\alpha_2} \cdots \sum_{j_r=0}^{\alpha_r} \phi\Big(\prod_{i=1}^{r} p_i^{j_i}\Big) \gcd\Big(\prod_{i=1}^{r} p_i^{j_i}, \prod_{i=1}^{r} p_i^{\beta_i}\Big) \prod_{i=1}^{r} \big(\tfrac{p_i+1}{p_i}\big)^{\delta_{j_i}} \\ &= \sum_{j_1=0}^{\alpha_1} \sum_{j_2=0}^{\alpha_2} \cdots \sum_{j_r=0}^{\alpha_r} \prod_{i=1}^{r} \phi(p_i^{j_i}) \gcd(p_i^{j_i}, p_i^{\beta_i}) \Big(\frac{p_i+1}{p_i}\Big)^{\delta_{j_i}} \\ &= \prod_{i=1}^{r} \sum_{j_i=0}^{\alpha_i} \phi(p_i^{j_i}) \gcd(p_i^{j_i}, p_i^{\beta_i}) \Big(\frac{p_i+1}{p_i}\Big)^{\delta_{j_i}}. \end{aligned}$$

Moreover, since

$$\begin{aligned}
&\sum_{j_i=0}^{\alpha_i} \phi(p_i^{j_i}) \gcd(p_i^{j_i}, p_i^{\beta_i}) \Big(\frac{p_i+1}{p_i}\Big)^{\delta_{j_i}} \\
&\quad = 1 + \sum_{j_i=1}^{\beta_i} \phi(p_i^{j_i}) p_i^{j_i} \, \frac{p_i+1}{p_i} + \sum_{j_i=\beta_i+1}^{\alpha_i} \phi(p_i^{j_i}) p_i^{\beta_i} \\
&\quad = 1 + (p_i-1)(p_i+1) \sum_{j_i=1}^{\beta_i} p_i^{2(j_i-1)} + p_i^{\beta_i} \left[\sum_{j_i=0}^{\alpha_i} \phi(p_i^{j_i}) - \sum_{j_i=0}^{\beta_i} \phi(p_i^{j_i}) \right] \\
&\quad = 1 + (p_i^{2\beta_i} - 1) + p_i^{\beta_i}(p_i^{\alpha_i} - p_i^{\beta_i}) = p_i^{\beta_i} p_i^{\alpha_i},
\end{aligned} \tag{B.2}$$

we obtain Eq. (B.1). ■

PROPOSITION 2 *Let $E_p(a,b)$ be an elliptic curve over the prime field $\mathbb{F}_p$. Suppose that $\#E_p(a,b)$ is exactly divisible by a prime factor l_p. If $F_{\rm div}(l_p)$ denotes the number of elements of order divisible by l_p, then*

$$F_{\rm div}(l_p) = \phi(l_p) \, \frac{\#E_p(a,b)}{l_p}. \tag{B.3}$$

Proof: We can write $E_p(a,b) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ with $n_2 \mid n_1$. Let $\#E_p(a,b) = l_p \prod_{i=1}^{r} p_i^{e_i}$ be the prime decomposition of $\#E_p(a,b)$. Since $n_2 \mid n_1$ and since $l_p \; mid \#E_p(a,b) = n_1 n_2$, it follows that $\gcd(l_p, n_2) = 1$. From Eq. (A.2) and since $\phi(mn) = \phi(m)\phi(n)$ for any coprime integers m, n, we obtain

$$\begin{aligned}
F_{\rm div}(l_p) \;&=\; \sum_{d \mid \frac{n_1}{l_p}} F(l_p d) = \sum_{d \mid \frac{n_1}{l_p}} \left[\phi(l_p d) \, \gcd(l_p d, n_2) \prod_{p_i \in \Omega_{l_p d, n_2}} \big(\tfrac{p_i+1}{p_i}\big) \right] \\
&=\; \phi(l_p) \sum_{d \mid \frac{n_1}{l_p}} \left[\phi(d) \, \gcd(d, n_2) \prod_{p_i \in \Omega_{l_p d, n_2}} \big(\tfrac{p_i+1}{p_i}\big) \right].
\end{aligned}$$

Noting that $\Omega_{l_p d, n_2} = \Omega_{d, n_2}$, we finally obtain $F_{\rm div}(l_p) = \phi(l_p) \, \frac{n_1}{l_p} \, n_2$ by Eq. (B.1), which concludes the proof. ■

Appendix C
Proof of Theorem 6

THEOREM 6 *Consider KMOV or Demytko's system. Let $E_p(a,b) \cong \mathbb{Z}_{\pi^{F_p} S_p} \oplus \mathbb{Z}_{\pi^{A_p} B_p}$ with $\pi^{A_p} B_p \mid \pi^{F_p} S_p$ and $E_q(a,b) \cong \mathbb{Z}_{\pi^{F_q} S_q} \oplus \mathbb{Z}_{\pi^{A_q} B_q}$ with $\pi^{A_q} B_q \mid \pi^{F_q} S_q$. Let γ_π denotes the probability that $F_p + F_q \geq 2\max(A_p, A_q)$. If we know a fixed*

point $\mathbf{P} \neq \mathcal{O}_n$ *such that* $[r-1]\mathbf{P} = \mathcal{O}_n$ *and if* $r-1$ *is divisible by* π*, then we can factor the RSA-modulus* $n = pq$ *with probability at least* $\gamma_\pi \frac{2(\pi^2-1)}{\pi^2(\pi^2+1)}$.

Proof: Let π be a prime factor of $\#E_n(a,b)$. We can write $\mathrm{ord}_p(\mathbf{P}) = \pi^{f_p} s_p$ with $\gcd(\pi, s_p) = 1$ and $\mathrm{ord}_q(\mathbf{P}) = \pi^{f_q} s_q$ with $\gcd(\pi, s_q) = 1$. The probability that n will be factored is given by the proportion of points $\mathbf{P}$ for which $f_p \neq f_q$.

Using the same technique as in the proof of Proposition 2, we can show that the number of points $\mathbf{P} \in E_p(a,b)$ such that π^{f_p}
$mid\, \mathrm{ord}_p(\mathbf{P})$ is given by $B_p S_p F^{(p)}(\pi^{f_p})$, where $F^{(p)}(\pi^{f_p})$ denotes the number of points $\mathbf{P}$ such that $\mathrm{ord}_p(\mathbf{P}) = \pi^f$. Similarly, there are $B_q S_q F^{(q)}(\pi^{f_q})$ points $\mathbf{P} \in E_q(a,b)$ such that π^{f_q}
$mid\, \mathrm{ord}_q(\mathbf{P})$. For each point $\mathbf{P} \in E_n(a,b)$ (modulo p) with π^{f_p}
$mid\, \mathrm{ord}_p(\mathbf{P})$, there are

$$\sum_{\substack{f_q=0 \\ f_q \neq f_p}}^{F_q} B_q S_q F^{(q)}(\pi^{f_q})$$

points $\mathbf{P} \in E_n(a,b)$ (modulo q) such that $\pi^{f_q} \mid \mathrm{ord}_q(\mathbf{P})$ and $f_q \neq f_p$. The number N of points $\mathbf{P} \in E_n(a,b)$ with $f_p \neq f_q$ is thus equal to

$$\begin{aligned} N &= B_p S_p B_q S_q \sum_{f_p=0}^{F_p} F^{(p)}(\pi^{f_p}) \sum_{\substack{f_q=0 \\ f_q \neq f_p}}^{F_q} F^{(q)}(\pi^{f_q}) \\ &= B_p S_p B_q S_q \sum_{f_p=0}^{F_p} F^{(p)}(\pi^{f_p}) \left[\pi^{F_q+A_q} - F^{(q)}(\pi^{f_p})\right], \end{aligned}$$

from Eqs (A.1) and (B.2)

$$= B_p S_p B_q S_q \left\{ \pi^{F_p+A_p}\, \pi^{F_q+A_q} - \sum_{f_p=0}^{F_p} F^{(p)}(\pi^{f_p}) F^{(q)}(\pi^{f_p}) \right\}.$$

Letting $A_{\max} = \max(A_p, A_q)$ and $A_{\min} = \min(A_p, A_q)$, and defining $\delta_{f_p}^{(p)} = 1$ if $f_p \leq A_p$ and $\delta_{f_p}^{(p)} = 0$ otherwise, $\delta_{f_p}^{(q)} = 1$ if $f_p \leq A_q$ and $\delta_{f_p}^{(q)} = 0$ otherwise, we obtain from Eq. (A.1)

$$\begin{aligned} &\sum_{f_p=0}^{F_p} F^{(p)}(\pi^{f_p}) F^{(q)}(\pi^{f_p}) \\ &\qquad = \sum_{f_p=0}^{F_p} \phi(\pi^{f_p})^2 \gcd(\pi^{f_p}, \pi^{A_p}) \left(\frac{\pi+1}{\pi}\right)^{\delta_{f_p}^{(p)}} \gcd(\pi^{f_p}, \pi^{A_q}) \left(\frac{\pi+1}{\pi}\right)^{\delta_{f_p}^{(q)}} \end{aligned}$$

$$= 1 + \sum_{f_p=1}^{A_{\min}} \phi(\pi^{f_p})^2\, \pi^{2f_p} \left(\frac{\pi+1}{\pi}\right)^2 + \sum_{f_p=A_{\min}+1}^{A_{\max}} \phi(\pi^{f_p})^2\, \pi^{A_{\min}+f_p} \left(\frac{\pi+1}{\pi}\right) + \sum_{f_p=A_{\max}+1}^{F_p} \phi(\pi^{f_p})^2\, \pi^{A_p+A_q}$$

$$= 1 + (\pi^2-1)^2 \sum_{f_p=1}^{A_{\min}} \pi^{4(f_p-1)} + (\pi-1)^2(\pi+1)\,\pi^{A_{\min}} \sum_{f_p=A_{\min}+1}^{A_{\max}} \pi^{3(f_p-1)} + (\pi-1)^2\,\pi^{A_p+A_q} \sum_{f_p=A_{\max}+1}^{F_p} \pi^{2(f_p-1)}$$

$$= 1 + \tfrac{(\pi^2-1)(\pi^{4A_{\min}}-1)}{\pi^2+1} + \tfrac{(\pi^2-1)\,\pi^{A_{\min}}\,(\pi^{3A_{\max}}-\pi^{3A_{\min}})}{\pi^2+\pi+1} + \tfrac{(\pi-1)\pi^{A_p+A_q}\,(\pi^{2F_p}-\pi^{2A_{\max}})}{\pi+1}$$

$$= \tfrac{2}{\pi^2+1} + \tfrac{\pi^{4A_{\min}}(\pi^2-1)\pi}{(\pi^2+1)(\pi^2+\pi+1)} + \tfrac{\pi^{A_p+A_q+2A_{\max}(\pi-1)\pi}}{(\pi^2+\pi+1)(\pi+1)} + \tfrac{(\pi-1)\pi^{A_p+A_q+2F_p}}{\pi+1},$$

noting that $A_{\min} + 3A_{\max} = A_p + A_q + 2A_{\max}$. Let γ_π be the probability that $F_p + F_q \geq 2A_{\max}$. Since $F_p, F_q \geq 1$, $F_p \geq A_p$ and $F_q \geq A_q$, the proportion τ of points $\mathbf{P}$ for which $f_p \neq f_q$ is

$$\begin{aligned}
\tau &= \frac{N}{B_p S_p B_q S_q \pi^{F_p+A_p+F_q+A_q}} = 1 - \frac{\sum_{f_p=0}^{F_p} F^{(p)}(\pi^{f_p}) F^{(q)}(\pi^{f_p})}{\pi^{F_p+A_p+F_q+A_q}} \\
&= 1 - \frac{\frac{2}{\pi^2+1} + \frac{\pi^{4A_{\min}}(\pi^2-1)\pi}{(\pi^2+1)(\pi^2+\pi+1)} + \frac{\pi^{A_p+A_q+2A_{\max}(\pi-1)\pi}}{(\pi^2+\pi+1)(\pi+1)} + \frac{(\pi-1)\pi^{A_p+A_q+2F_p}}{\pi+1}}{\pi^{F_p+A_p+F_q+A_q}} \\
&\geq \gamma_\pi \left[1 - \tfrac{2}{(\pi^2+1)\pi^2} - \tfrac{(\pi^2-1)\pi}{(\pi^2+1)(\pi^2+\pi+1)} - \tfrac{(\pi-1)\pi}{(\pi^2+\pi+1)(\pi+1)} - \tfrac{\pi-1}{\pi+1}\right] \\
&= \gamma_\pi \left[1 - \frac{\pi^4-\pi^2+2}{\pi^2(\pi^2+1)}\right] = \gamma_\pi\, \frac{2(\pi^2-1)}{\pi^2(\pi^2+1)}.
\end{aligned}$$

■