BULL. AUSTRAL. MATH. SOC. 94A60, 11B37
VOL. 68 (2003) [21–38]

# A CUBIC ANALOGUE OF THE RSA CRYPTOSYSTEM

MOHAMAD RUSHDAN MD SAID AND JOHN LOXTON

In this paper, we investigate a public key cryptosystem which is derived from a third order linear recurrence relation and is analogous to the RSA and LUC cryptosystems. The explicit formulation involves a generalisation of the rule for composition of powers and of the calculus of the Euler totient function which underlie the algebra of the RSA cryptosystem. The security of all these systems appears to be comparable and to depend on the intractability of factorisation but the systems do not seem to be mathematically equivalent.

## 1. PUBLIC KEY CRYPTOSYSTEMS BASED ON RECURRENCES

Public key cryptography was invented by Diffie and Hellman in 1976 in their paper *New directions in cryptography* [**5**] and, since then, many articles have been published dealing with this concept. Some have proposed crytosystems that are practical to implement, although not all of these have proved resistant to attack. The best known survivor is the RSA (Rivest, Shamir and Adleman) cryptosystem ([**10**]). The strength of this system arises from the intractability of the problem of factorising certain large integers. No other general attack on the RSA cryptosystem is known. However, because of the rapid increases in factorising power and attacks based on the special structure of RSA, it is still of interest to look for variations of the original idea. That is the theme of our paper.

A. THE RSA CRYPTOSYSTEM. In the RSA system, each user places in a public file an encryption key $(e, N)$ where $e$ and $N$ are positive integers and $N$ is the product of two large primes $p$ and $q$ which are not revealed. The decoding key $d$ is determined by $ed \equiv 1 \bmod \phi(N)$ and is kept secret by the owner of the public key $(e, N)$. (Here, $\phi(N) = (p-1)(q-1)$ is the Euler totient function.) To encrypt a message, the sender raises the message $P$ to the $e$-th power modulo $N$. Thus, the encryption function is

$$E(P) = P^e \equiv C \bmod N,$$

where $C$ is the ciphertext which is sent to the owner of the public key $(e, N)$. To decrypt, the receiver raises $C$ to the $d$-th power, that is the decryption function is

$$D(C) = C^d \equiv (P^e)^d \equiv P \bmod N.$$

(The last congruence follows from Euler's theorem, as long as $P$ and $N$ are relatively prime.)

Received 26th August, 2003

https://doi.org/10.1017/S0004972700037382 Published online by Cambridge University Press

B. THE LUC CRYPTOSYSTEM. The LUC cryptosystem [11] is a similar scheme based on the Lucas sequence. The encryption function is defined by

$$E(P) = V_e(P, 1) \equiv C \bmod N,$$

where $N = pq$ as before and $V_e(P, 1)$ is the $e$-th term of the Lucas sequence derived from the second order recurrence relation $V_{n+2} = PV_{n+1} - V_n \bmod N$, with the initial values $V_0 = 2$ and $V_1 = P$. (See [8].) As in the RSA system, $(e, N)$ is the public key and the decoding key $d$ is chosen so that $de \equiv 1 \bmod S(N)$, where

$$S(N) = \operatorname{lcm}\left[p - \left(\frac{D}{p}\right), q - \left(\frac{D}{q}\right)\right]$$

and $(D/p)$ and $(D/q)$ are the Legendre quadratic residue symbols with $D = P^2 - 4$. The holder of the secret key is able to determine both Legendre symbols from the ciphertext $V_e$ without knowing $P$ and $D$. Indeed, if $U_n$ is defined by the same recurrence relation as $V_n$ but with initial values $U_0 = 0$ and $U_1 = 1$, then $DU_e^2 = V_e^2 - 4$ which implies that $(D/p) = \left((V_e^2 - 4)/p\right)$. To decrypt the ciphertext $C$, we invoke the following two crucial relationships for the Lucas sequence:

$$V_d(V_e(P, 1), 1) = V_{ed}(P, 1)$$

and

$$V_{kS(N)+1}(P, 1) \equiv P \bmod N.$$

The decryption function is therefore

$$D(C) = V_d(C, 1) = V_d(V_e(P, 1), 1) = V_{ed}(P, 1) = V_{kS(N)+1}(P, 1) \equiv P \bmod N$$

and this recovers the original message $P$. (In the second last step, $ed = kS(N) + 1$ for some integer $k$ by the definition of $d$.)

The characteristic equation of the Lucas sequence introduced above is the quadratic $x^2 - Px + 1 = 0$ with discriminant $D$. For the case of interest here, the coefficient $P$ is an integer, the discriminant is non-zero and the quadratic has distinct roots, say $\alpha$ and $\beta$. The Lucas sequences $U_n$ and $V_n$ associated with the quadratic are given by $U_n(P, 1) = (\alpha^n - \beta^n)/(\alpha - \beta)$ and $V_n(P, 1) = \alpha^n + \beta^n$ respectively. These formulae provide one way to derive the various identities mentioned above.

C. THE CUBIC CRYPTOSYSTEM. The main purpose of this paper is to investigate versions of these cryptosystems based on higher order recurrence sequences and, in particular, on cubic recurrences.

https://doi.org/10.1017/S0004972700037382 Published online by Cambridge University Press

We define the recurrence sequences in question in section 2, describe the necessary algebra for the investigation in section 3 and set up the cryptosystem in section 4. We shall see in section 5 that the higher order systems are not significantly more complex computationally. For example, decryption will take at worst twice as long as for an RSA system with similar block size. All these systems rely for their security on the computational intractability of factorisation and all have similar weaknesses to a chosen message attack as shown in section 6. The additional parameters in the higher order systems may allow choices which increase the cryptographic randomness of the underlying operations and so strengthen the cryptosystem. We plan to return to this question in a subsequent paper.

## 2. Cubic analogue of the Lucas sequence

By analogy with the Lucas sequence, we consider the cubic equation

$$x^3 - Px^2 + Qx - R = 0 \tag{1}$$

with integer coefficents $P, Q, R$ and roots $\alpha, \beta, \gamma$ and we define the following sequences of numbers:

$$\begin{aligned} V_n(P,Q,R) &= \alpha^n + \beta^n + \gamma^n \\ U_n(P,Q,R) &= \alpha^n + \omega\beta^n + \omega^2\gamma^n \\ W_n(P,Q,R) &= \alpha^n + \omega^2\beta^n + \omega\gamma^n \end{aligned} \tag{2}$$

where $\omega = \left(-1+\sqrt{-3}\right)/2$ is a cube root of unity. The sequences $V_n, U_n$ and $W_n$ all satisfy the linear recurrence

$$X_{n+3} = PX_{n+2} - QX_{n+1} + RX_n$$

with characteristic equation (1). All the $V_n$ are integers, because the first three terms $V_0, V_1$ and $V_2$ are integers, namely $V_0(P,Q,R) = 3, V_1(P,Q,R) = \alpha+\beta+\gamma = P$, and

$$\begin{aligned} V_2(P,Q,R) = \alpha^2+\beta^2+\gamma^2 &= (\alpha+\beta+\gamma)^2 - 2(\alpha\beta+\alpha\gamma+\beta\gamma) \\ &= V_1^2(P,Q,R) - 2Q = P^2 - 2Q. \end{aligned}$$

The quadratic and cubic versions of these Lucas sequences can be extended to Kummer fields of any prime order $q$ as shown by Williams [14]. Here, if $\alpha_0, \alpha_1, \ldots, \alpha_{q-1}$ are a complete set of conjugates (and hence distinct) in a Kummer field $\mathbf{Q}(\Delta^{1/q})$ and $\omega = e^{2\pi i/q}$, then the sequences

$$U_{k,n} = \sum_{j=0}^{q-1} \alpha_j^n \omega^{kj} \qquad (0 \leqslant k \leqslant q-1)$$

https://doi.org/10.1017/S0004972700037382 Published online by Cambridge University Press

form an integer basis for the set of related recurrences of order $q$ whose characteristic polynomial has $\alpha_0, \alpha_1, \dots, \alpha_{q-1}$ as its roots. These extended Lucas sequences satisfy similar identities to the familiar properties for the quadratic case. In particular, they exhibit divisibility properties which can be exploited in primality tests and in certain cryptosystems. We shall see in later sections how this works in the cubic case.

## 3. Cycles and totients

As with RSA and LUC, the cryptosystem will be derived from the terms of a recurrence sequence taken modulo $N$. A recurrence sequence modulo $N$ is periodic and an obvious necessary condition for a secure system is that the period is large. In this section, we investigate the computation of the period of a recurrence sequence modulo $N$. By the Chinese remainder theorem, the general result can be pieced together from the case of a prime power modulus and we build up to this by first studying the case of a prime modulus $p$.

A. Cyclic structure for a prime modulus. Let $f(x) = x^3 - Px^2 + Qx - R$ be the characteristic polynomial of the cubic recurrence sequence $V_n = PV_{n-1} - QV_{n-2} + RV_{n-3}$ as defined previously.

The factorisation of $f(x)$ modulo $p$ is unique and, following Ward [**12**], can be classified into five different cases or *types*:

I. type $t[3]$—$f(x)$ is irreducible,

II. type $t[2,1]$—$f(x)$ factors as an irreducible quadratic times a linear factor, and

III. type $t[1]$—$f(x)$ factors into three linear factors.

In this last case, we have three possibilities namely:

III.1. type $t[1,1,1]$—three distinct roots,

III.2. type $t[1^2,1]$—a double root and a single root, and

III.3. type $t[1^3]$—a triple root.

Let $\mathbf{F}_p$ denote the finite field of order $p$. In general, if $f(x) = \prod_{i=1}^{k} f_i(x)^{e_i} \bmod p$, where the $f_i(x)$ are distinct and irreducible of degree $d_i$ over $\mathbf{F}_p$, we say that $f$ is of *type* $t[d_1^{e_1}, \dots, d_k^{e_k}]$. For convenience, we take $d_1 \geqslant d_2 \geqslant \dots \geqslant d_k$.

The following proposition contains a characterisation of the period of a general recurrence sequence. We then restate it as Proposition 1A in the simplified form in which it is applied later in the paper to cubic recurrences and sketch the proof of the special case.

Proposition 1. *Suppose the polynomial $f(x)$ in $\mathbf{F}_p[x]$ has degree $d$ and factorisation $f(x) = \prod_{i=1}^{k} f_i(x)^{e_i}$ over $\mathbf{F}_p[x]$, where the $f_i(x)$ are distinct and irreducible of*

https://doi.org/10.1017/S0004972700037382 Published online by Cambridge University Press

*degree $d_i$ and $f(0) \not\equiv 0 \bmod p$. Let $\alpha_{ij}$ $(1 \leqslant j \leqslant d_i)$ be the roots of $f_i(x)$ in its splitting field over $\mathbf{F}_p$. The general solution $(X_n)$ of the recurrence relation with characteristic polynomial $f(x)$ has the shape*

$$X_n = \sum_{i=1}^{k} \sum_{j=1}^{d_i} p_{ij}(n)\alpha_{ij}^n,$$

*where $p_{ij}(x)$ is a polynomial of degree at most $\varepsilon_i - 1$.*

*Suppose $\alpha_{ij}$ has order $e_i$ in $\mathbf{F}_p^\times$, that is $e_i$ is the least positive integer such that $\alpha_{ij}^{e_i} \equiv 1 \bmod p$. Then $e_i \mid p^{d_i} - 1$ and, in case $f_i(0) = (-1)^{d_i}$, $e_i \mid 1 + p + \cdots + p^{d_i - 1}$.*

*The period of $X_n$ modulo $p$ is the least common multiple of the periods of the terms $p_{ij}(n)\alpha_{ij}^n$ and the periods of these terms have the respective shapes $p^{r_{ij}}e_i$ for some integers $r_{ij}$.*

COMMENTS. The form of the general solution of a recurrence relation over a field is well known.

Let $K$ be a finite field extension of $\mathbf{F}_p$. If $f(x)$ is an irreducible polynomial in $\mathbf{F}_p[x]$, then we have the following result from Galois theory (see, for example, [4, p. 287]): If $f(x)$ in $\mathbf{F}_p[x]$ is irreducible of degree $d$, $K$ is a finite field extension of $\mathbf{F}_p$, and $\alpha$ in $K$ is a root of $f(x)$, then in $K[x]$, $f(x) = (x - \alpha)(x - \alpha^p)$ $(x - \alpha^{p^2}) \ldots (x - \alpha^{p^{d-1}})$.

Consider a typical factor $f_i$ in the Proposition. The splitting field has degree $d_i$ over $\mathbf{F}_p$ and the set of conjugates $\alpha_{ij}$ has the shape $\alpha, \alpha^p, \alpha^{p^2}, \ldots \alpha^{p^{d_i - 1}}$, so each $\alpha_{ij}$ has the same order $e_i$ and $e_i \mid p^{d_i} - 1$. Since $(-1)^{d_i} f_i(0) = \alpha^{1 + p + p^2 + \cdots}$, we see that $e_i \mid 1 + p + p^2 + \cdots + p^{d_i - 1}$ if $f_i(0) = (-1)^{d_i}$.

PROPOSITION 1A. *The periods of the recurrence sequences $U_n, V_n, W_n$ modulo $p$ defined in* (2) *divide* (a) $p^3 - 1$ *in Case I,* (b) $p^2 - 1$ *in Case II and* (c) $p - 1$ *in Case III.*

PROOF: In Case III, the orders of the roots $a, b$ and $c$ of the characteristic cubic equation (1) divide $p - 1$ by Fermat's Little Theorem. This implies that the period of each of $U_n, V_n, W_n$ divides $p - 1$. The result here is simple because the particular recurrences $U_n, V_n, W_n$ only admit constant coefficients in the general solution $X_n$ considered in Proposition 1.

For Case I, we invoke the result from Galois theory cited in the comment above. If $\alpha$ is one root of the cubic equation (1), then the other roots are $\beta \equiv \alpha^p$, $\gamma \equiv \alpha^{p^2}$ and $R \equiv \alpha^{1+p+p^2}$ modulo $p$. Therefore we have $\alpha^{p^3} \equiv \alpha$, $\beta^{p^3} \equiv \beta$, $\gamma^{p^3} \equiv \gamma$ modulo $p$ and so the period modulo $p$ of any of the simple recurrence sequences in (2) divides $p^3 - 1$ and even divides $1 + p + p^2$ if $R = (-1)^3 f(0) = 1$.

https://doi.org/10.1017/S0004972700037382 Published online by Cambridge University Press

In Case II, the cubic polynomial in (1) can be written as $f(x) = (x^2 + Ax + B)(x - c)$ where $x^2 + Ax + B$ is an irreducible quadratic and its two roots are given by $\alpha = \left(-A + \sqrt{A^2 - 4B}\right)/2$ and $\beta = \left(-A - \sqrt{A^2 - 4B}\right)/2$. Instead of calling on the Proposition, we give a simple explicit calculation:

$$\alpha^p = \left(\frac{1}{2}\left(-A + \sqrt{A^2 - 4B}\right)\right)^p \equiv \frac{1}{2}\left(-A + \left(\frac{A^2 - 4B}{p}\right)\sqrt{A^2 - 4B}\right) \bmod p,$$

and similarly for $\beta^p$, where $\left((A^2 - 4B)/p\right)$ is the Legendre Symbol. Since $x^2 + Ax + B$ is irreducible modulo $p$, $\left((A^2 - 4B)/p\right) = \pm 1$. Therefore, $\alpha^p \equiv \alpha, \beta^p \equiv \beta \bmod p$ when $A^2 - 4B$ is a quadratic residue and $\alpha^p \equiv \beta \bmod p, \beta^p \equiv \alpha \bmod p$ when $A^2 - 4B$ is a non-residue, and in either case, $\alpha^{p^2} \equiv \alpha, \beta^{p^2} \equiv \beta \bmod p$. Of course, $c^{p^2} \equiv c^p \equiv c$ modulo $p$. Thus, the period of the recurrence sequence divides $p^2 - 1$.

For cases I, II and III.1, these results apply to any solution of the recurrence and not just to the simple solutions $U_n, V_n, W_n$. In case III.2 and III.3, we must allow for the possibility of repeated roots so that the general solution has the form

$$X_n = (rn + s)a^n + tb^n \quad \text{or} \quad X_n = \left(rn^2 + sn + t\right)a^n$$

and the period divides $p^\delta(p - 1)$ for some integer $\delta$. □

B. Cyclic structure for a prime power modulus. The passage to a prime power modulus is elementary. The following proposition gives a general result which we then restate as Proposition 2A in the simplified form in which it is applied later for cubic recurrences. Again we only sketch the argument in the special case.

Proposition 2. *Suppose $\alpha$ is a root of an irreducible polynomial $f$ in $\mathbf{F}_p[x]$, $f$ has degree $d$ and $f(0) \not\equiv 0 \bmod p$. Let $e$ denote the order of $\alpha$ modulo $p^m$. Then $e \mid p^{m-1}(p^d - 1)$ and, in case $f(0) = (-1)^d$, $e \mid p^{m-1}(1 + p + \cdots + p^{d-1})$.*

Comment. The period of the recurrence sequence modulo $p^m$ is therefore determined in the same way as in Proposition 1, except that $e_i$ is now the order of $\alpha_{ij}$ modulo $p^m$.

Proposition 2A. *The periods of the recurrence sequences $U_n, V_n, W_n$ modulo $p^m$ divide* (a) $p^{m-1}(p^3 - 1)$ *in Case I,* (b) $p^{m-1}(p^2 - 1)$ *in Case II, and* (c) $p^{m-1}(p - 1)$ *in Case III.*

Proof: Consider Case I. If $\alpha$ is one root of the cubic equation (1), then the other roots satisfy $\beta \equiv \alpha^p$ and $\gamma \equiv \alpha^{p^2}$ and we have $R \equiv \alpha^{1+p+p^2} \bmod p$. Raising the last congruence to the power of $p^{m-1}$ gives

$$\begin{aligned}\left(\alpha^{p^2+p+1}\right)^{p^{m-1}} &= (R \bmod p)^{p^{m-1}} = (R + p\theta)^{p^{m-1}} \quad \text{for some integral } \theta \\ &= R^{p^{m-1}} + \binom{p^{m-1}}{1} R^{p^{m-1}-1}(p\theta) + \binom{p^{m-1}}{2} R^{p^{m-1}-2}(p\theta)^2 + \cdots + (p\theta)^{p^{m-1}}\end{aligned}$$

where all the terms apart from $R^{p^{m-1}}$ are divisible by $p^m$. Therefore,

$$\alpha^{p^{m-1}(p^2+p+1)} \equiv (\alpha\beta\gamma)^{p^{m-1}} \equiv R^{p^{m-1}} \bmod p^m$$

and, by Euler's Theorem,

$$\alpha^{p^{m-1}(p^3-1)} \equiv R^{p^{m-1}(p-1)} \equiv 1 \bmod p^m.$$

The other roots of the polynomial satisfy the same congruence. The other two types can be dealt with in the same way. □

C. Generalisation of the Euler totient function. The Lehmer totient function, $S(N)$, is the generalisation of the Euler totient function for the Lucas functions. (See [7].) In the case of third order linear recurrence sequences, an analogue of this function can be constructed following a similar procedure. In order to extend this theory, the value of the constant coefficient $R$ of the cubic (1) is restricted to 1.

Consider the cubic $f(x) = x^3 - Px^2 + Qx - 1$ with roots $\alpha, \beta$ and $\gamma$ and the corresponding linear recurrence sequence $V_n = \alpha^n + \beta^n + \gamma^n$ as defined previously. Suppose that $N$ is a positive integer, written in its canonical form,

$$N = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where the $p_i$ are distinct primes and the $a_i$ are positive integers.

If the cubic $f(x)$ is of type $t[3]$ modulo $p_i$ and $\alpha$ is one of its roots in its splitting field over $\mathbf{F}_{p_i}$, then for any positive integer $k$, $\alpha^{kp_i^{a_i-1}(p_i^2+p_i+1)} \equiv R^{kp_i^{a_i-1}} \equiv 1$ modulo $p_i^{a_i}$, using the calculation in the proof of Proposition 2A and the assumption that $R = 1$. The other two conjugates give the same result. Therefore,

$$V_{kp_i^{a_i-1}(p_i^2+p_i+1)+1} \equiv \alpha^{kp_i^{a_i-1}(p_i^2+p_i+1)+1} + \cdots \equiv \alpha + \beta + \gamma \equiv P \bmod p_i^{a_i}.$$

Similarly, for a cubic of type $t[2,1]$ modulo $p_i$, $\alpha^{kp_i^{a_i-1}(p_i^2-1)+1} \equiv \alpha \bmod p_i^{a_i}$ which leads to

$$V_{kp_i^{a_i-1}(p_i^2-1)+1} \equiv P \bmod p_i^{a_i}.$$

Finally, for a cubic of type $t[1]$ modulo $p_i$, the congruence $\alpha^{kp_i^{a_i-1}(p_i-1)+1} \equiv \alpha \bmod p_i^{a_i}$ yields

$$V_{kp_i^{a_i-1}(p_i-1)+1} \equiv P \bmod p_i^{a_i}.$$

We define the totient

$$\Phi(N) = p_1^{a_1-1}\overline{p_1}\,p_2^{a_2-1}\overline{p_2} \cdots p_r^{a_r-1}\overline{p_r},$$

https://doi.org/10.1017/S0004972700037382 Published online by Cambridge University Press

where

$$\overline{p_i} = \begin{cases} p_i^2 + p_i + 1 & \text{if } f(x) \text{ is of type } t[3] \text{ modulo } p_i \\ p_i^2 - 1 & \text{if } f(x) \text{ is of type } t[2,1] \text{ modulo } p_i \\ p_i - 1 & \text{if } f(x) \text{ is of type } t[1] \text{ modulo } p_i. \end{cases}$$

Since $V_{kp_i^{a_i-1}\overline{p_i}+1} \equiv P \bmod p_i^{a_i}$ for each $i = 1, 2, \ldots, r$ and any integer $k$, we have $V_{k\Phi(N)+1} \equiv P \bmod p_i^{a_i}$ which implies that $V_{k\Phi(N)+1} \equiv P \bmod N$. We have therefore proved the following Proposition.

PROPOSITION 3. *Let $N = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ where the $p_i$ are distinct primes and $a_i$ are positive integers and let $f(x) = x^3 - Px^2 + Qx - 1$ be the characteristic polynomial of the recurrence sequence $V_n = V_n(P, Q, 1)$. Then $V_{k\Phi(N)+l} \equiv V_l \bmod N$ and, in particular,*

$$V_{k\Phi(N)+1}(P, Q, 1) \equiv P \bmod N,$$

*where $\Phi(N)$ is the totient function defined above.*

D. COMPOSITION OF RECURRENCES. We state here some properties of the sequence $(V)_n$ which are straightforward consequences of the definition. The identity (3) which is the rule for the composition of powers for the third order function is of particular importance in what follows.

Let $\alpha, \beta$ and $\gamma$ be the roots of the equation $x^3 - Px^2 + Qx - R = 0$ and let $V_n(P, Q, R) = \alpha^n + \beta^n + \gamma^n$. By exploiting the relations between the roots $\alpha, \beta, \gamma$ and the coefficients $P, Q, R$, we find

$$V_{-k}(P, Q, R) = \alpha^{-k} + \beta^{-k} + \gamma^{-k} = V_k(QR^{-1}, PR^{-1}, R^{-1})$$

because the cubic corresponding to the last recurrence, namely $x^3 - QR^{-1}x^2 + PR^{-1}x - R^{-1}$ has roots $\alpha^{-1}, \beta^{-1}$ and $\gamma^{-1}$. Similarly,

$$V_k(Q, PR, R^2) = (\alpha\beta)^k + (\beta\gamma)^k + (\gamma\alpha)^k.$$

Using this identity, we see that the cubic with roots $\alpha^k, \beta^k$ and $\gamma^k$ is $x^3 - V_k(P, Q, R)x^2 + V_k(Q, PR, R^2)x - R^k$ so

$$(3) \qquad V_{nk}(P, Q, R) = \alpha^{nk} + \beta^{nk} + \gamma^{nk} = V_n\big(V_k(P, Q, R), V_k(Q, PR, R^2), R^k\big).$$

Finally, by direct calculation and the evaluation of $V_k(Q, PR, R^2)$ above,

$$V_k(P, Q, R)^2 = V_{2k}(P, Q, R) + 2V_k(Q, PR, R^2)$$

E. INVERSION OF RECURRENCES. We can now formulate an inverse operation. Consider the sequence $V_n(P, Q, 1)$ and suppose $ed \equiv 1 \bmod \Phi(N)$, that is $ed = k\Phi(N) + 1$ for some integer $k$. Then, by (3) and Proposition 3,

$$(4) \qquad V_d\big(V_e(P, Q, 1), V_e(Q, P, 1), 1\big) = V_{ed}(P, Q, 1) = V_{k\Phi(N)+1}(P, Q, 1) \equiv P \bmod N,$$

and, for the same reason,

$$V_d\big(V_e(Q,P,1),V_e(P,Q,1),1\big)\equiv Q \bmod N.$$

There is an obvious difference between Euler's function $\phi(n)$ and its extension $\Phi(n)$. The function $\phi(n)$ depends only on the prime factors of $n$, whereas the function $\Phi(n)$ also depends on the type of the characteristic polynomial $f(x)$. If we replace each $\overline{p_i}$ respectively in the definition of $\Phi(N)$ by $\operatorname{lcm}\big(p_i-1,p_i^2-1,p_i^2+p_i+1\big)$ we get a new uniform 'totient' function, $R(N)$ say, which works in each case and enables us to do away with determining the type of the polynomial. The drawback is that the new function is generally larger and, in the interests of computational efficiency, it is desirable to avoid moduli which are larger than necessary.

For the quadratic $f(x)=x^2-Px+1$, the additional information needed to compute $S(N)$ is the set of Legendre symbols $(D/p)$, where $D=P^2-4$ is the discriminant of the quadratic and $p$ runs through the prime factors of $N$. In discussing LUC, we observed that the inversion relation involves the quantity $V_d(V_e(P,1),1)$ which comes from the recurrence associated with the quadratic $g(x)=x^2-V_e(P,1)x+1$ with discriminant $V_e(P,1)^2-4$. However, $\big((P^2-4)/p\big)=\big((V_e^2-4)/p\big)$, so the type of the decoding polynomial $g(x)$ is the same as the type of $f(x)$ and it can be found directly from the cipher $V_e(P,1)$ without decoding.

We wish to investigate the extension of this phenomenon to cubic equations. That is, given $P$ and $Q$ and the arguments $C_1=V_e(P,Q,1)$ and $C_2=V_e(Q,P,1)$ in (4), we want to determine whether the type of the polynomial $g(x)=x^3-C_1x^2+C_2x-1$ is in any way related to the type of the polynomial $f(x)=x^3-Px^2+Qx-1$.

**PROPOSITION 4.** *Let $p$ be a prime and consider the cubic polynomials $f(x)=x^3-Px^2+Qx-1$ and $g(x)=x^3-V_e(P,Q,1)x^2+V_e(Q,P,1)x-1$.*

(a) *If $\big(e,\Phi(p)\big)=1$, then $f$ and $g$ have the same type.*

(b) *If the discriminant of $g$ is non-zero modulo $p$, then $f$ and $g$ have the same type.*

(c) *In any case, $f$ and $g$ have the same type except possibly in the cases described in the table:*

| *Type of $f$* | *Roots of $f$* mod $p$ | *Type of $g$* | *Roots of $g$* mod $p$ |
|---|---|---|---|
| $3$ | $\alpha,\beta,\gamma$ | $1^3$ | $\alpha^e=\beta^e=\gamma^e$ |
| $2,1$ | $\alpha,\beta,c$ | $1^2,1$ | $\alpha^e=\beta^e,c^e$ |
| | | $1^3$ | $\alpha^e=\beta^e=c^e$ |
| $1,1,1$ | $a,b,c$ | $1^2,1$ | $a^e=b^e,c^e$ |
| | | $1^3$ | $a^e=b^e=c^e$ |
| $1^2,1$ | $a,c$ | $1^3$ | $a^e=c^e$ |

https://doi.org/10.1017/S0004972700037382 Published online by Cambridge University Press

COMMENT. We adopt the convention that $a, b, c$ denote elements of $\mathbf{F}_p$ and $\alpha, \beta, \gamma$ denote elements of the splitting field of $f$ over $\mathbf{F}_p$.

PROOF: Note that if $\alpha, \beta, \gamma$ denote the roots of $f$ then, by the remark preceding the identity (3), the roots of $g$ are $\alpha^e, \beta^e, \gamma^e$.

(a) If $\left(e, \Phi(p)\right) = 1$, then we can find $d$ with $ed \equiv 1 \bmod \Phi(p)$ and we have $\alpha^{ed} \equiv \alpha \bmod p$. Consequently, $\alpha^e \equiv \beta^e \bmod p$ if and only if $\alpha \equiv \beta \bmod p$.

If $\alpha$ and $\beta$ are any two distinct conjugate roots of $f$, then as in the proof of Proposition 1A and after interchanging $\alpha$ and $\beta$ if necessary, we have $\beta \equiv \alpha^p \bmod p$. Consequently, if $\alpha^e = a$, say, is in $\mathbf{F}_p$, then $\beta^e \equiv \alpha^{pe} = a^p \equiv a = \alpha^e \bmod p$, contrary to the assumption that $\alpha$ and $\beta$ are distinct.

It follows that $f$ and $g$ have the same number of distinct roots and the same number of roots in $\mathbf{F}_p$ and so have the same type.

(b) If the discriminant of $g$ is non-zero, then $g$ has distinct roots. Further, by the second remark in the proof of (a), if $\alpha$ and $\beta$ are distinct conjugate roots of $f$, then $\alpha^e$ and $\beta^e$ are distinct conjugate roots of $g$. So, again, $f$ and $g$ have the same type.

(c) The exceptional cases occur when the $e$-th powers of certain roots of $f$ coincide. Some combinations are impossible. For example, if $f$ has type $t[3]$ and conjugate roots $\alpha, \beta \equiv \alpha^p, \gamma \equiv \alpha^{p^2}$ and $\alpha^e = a$ is in $\mathbf{F}_p$, then $\alpha^e \equiv \beta^e \equiv \gamma^e \equiv a \bmod p$ so $g$ either has type $t[3]$ or type $t[1^3]$. □

F. AN ALGORITHM FOR COMPUTING THE TYPE. We sketch an algorithm in the form of a decision tree to compute the type of a cubic polynomial $f(x) = x^3 - Px^2 + Qx - R$ in $\mathbf{F}_p[x]$.

STEP 1. Compute the discriminant of $f$. Let $\alpha, \beta, \gamma$ denote the roots of $f$. The *discriminant* (see, for example, [**4**, p. 282]) is given by

$$D = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2 = -27R^2 + 18PQR - 4Q^3 + P^2Q^2 - 4P^3R$$

and $D \equiv 0 \bmod p$ if and only if $f$ has a repeated root, that is $f$ is of type $t[1^2, 1]$ or type $t[1^3]$.

IA. Type $t[1^3]$: $D \equiv 0 \bmod p$ and either $Q \equiv P^2/3, R \equiv P^3/27 \bmod p$ if $p \neq 3$ or $P \equiv Q \equiv 0 \bmod p$ if $p = 3$.

The specifications imply $f(x) \equiv (x - P/3)^3 \bmod p$ if $p \neq 3$ and $f(x) \equiv (x - R)^3 \bmod p$ if $p = 3$.

IB. Type $t[1^2, 1]$. $D \equiv 0 \bmod p$ and the conditions of IA are not satisfied.

STEP II. Let $D$ denote the discriminant of $f$ and let $r$ denote the number of irreducible factors of $f$ in $\mathbf{F}_p[x]$. Suppose $D \not\equiv 0 \bmod p$ so that the type is $t[1,1,1], t[2,1]$, or $t[3]$.

https://doi.org/10.1017/S0004972700037382 Published online by Cambridge University Press

The following theorem of Stickelberger can be used in deciding whether the function $f$ has an odd or even number of distinct irreducible factors. (See [**4**, p. 282].)

STICKELBERGER'S THEOREM. *Let $p$ be an odd prime, $f(x)$ a monic polynomial of degree $d$ with coefficients in $\mathbf{F}_p[x]$ without multiple factors* ($D \not\equiv 0 \bmod p$). *Let $r$ be the number of irreducible factors of $f(x)$ in $\mathbf{F}_p[x]$. Then $r \equiv d \bmod 2$ if and only if $(D/p) = 1$.*

IIA. Type $t[2,1]$. *$D \not\equiv 0 \bmod p$ and either $(D/p) = -1$ if $p > 2$ or $P \equiv Q \bmod 2$ if $p = 2$.*

By Stickelberger's Theorem, in the case $p > 2$, $r \not\equiv 1 \bmod 2$, so $r = 2$ and $f$ has type $t[2,1]$. The case $p = 2$ follows by enumerating all possibilities.

IIB. Type $t[1,1,1]$ *or* type $t[3]$. *$D \not\equiv 0 \bmod p$ and either $(D/p) = 1$ if $p > 2$ or $P \equiv Q \bmod 2$ if $p = 2$.*

STEP III. Let $D$ denote the discriminant of $f$ and suppose $(D/p) = 1$ so that the type is $t[1,1,1]$ or $t[3]$. In order to decide between the two possible types, we must decide whether or not $f$ factorises in $\mathbf{F}_p$.

Suppose first that $p > 3$. We can solve the cubic equation $f(x) = 0$ by Cardan's formula: if $y = x - P/3$, then

$$\begin{aligned} f(x) = y^3 + Ay + B \quad \text{where} \quad & A = Q - P^2/3, \\ & B = -R + PQ/3 - 2P^3/27 \quad \text{and} \\ & D = -27B^2 - 4A^3 \end{aligned}$$

and the roots are obtained from $y = u - v$ where $3uv = A$ and $u^3 - v^3 = -B$. Thus, $u$ and $v$ can be determined by taking the cube root of

$$u^3 = \frac{1}{2}\left(-B + \frac{\sqrt{D}}{3\sqrt{-3}}\right).$$

By hypothesis, $D \equiv \mu^2 \bmod p$, say, so $f(x)$ factorises in $\mathbf{F}_p$ if and only if $\left(-B + \mu/3\sqrt{-3}\right)/2$ is a cube modulo $p$. This question can be decided by computing a cubic residue symbol and the law of cubic reciprocity provides an efficient mechanism for doing so. Williams and Zarnke [**16**] give an explicit algorithm requiring O(log $p$) steps.

The cases with $p = 2$ and $p = 3$ can be handled by enumerating all the possibilities. This leads to the final step in the classification.

IIIA. Type $t[1,1,1]$. *$(D/p) = 1$ and either $\left(R - (PQ/3) + (2P^3/27) + (\sqrt{D}/3\sqrt{-3})\right)/2$ is a cube modulo $p$ if $p > 3$ or $R \equiv 0 \bmod 3$ if $p = 3$.* [In the latter case, $P \equiv 0$ and $Q \equiv -1 \bmod 3$.]

https://doi.org/10.1017/S0004972700037382 Published online by Cambridge University Press

IIIB. Type $t[3]$. Either

(a) $(D/p) = 1$ and $\left(R - (PQ/3) + (2P^3/27) + (\sqrt{D}/3\sqrt{-3})\right)/2$ is not a cube modulo $p$ if $p > 3$, or

(b) $D \equiv 1$ and $R \not\equiv 0 \bmod 3$ if $p = 3$, or

(c) $P \not\equiv Q \bmod 2$ if $p = 2$.

This yields a computationally feasible way of determining the type of the polynomial $f$ and therefore also the function $\Phi(N)$. Moreover, in the most important cases for the application (cases (a) and (b) in Proposition 4), $\Phi(N)$ has the same value whether it is derived from $f$ or $g$.

## 4. The cubic cryptosystem

In the previous section, we have obtained two results which will be used to develop a public-key cryptosystem. These are the higher order analogues of the two equations that were used in the LUC system:

1. the extension (3) of the rule for the composition of powers, and
2. the extension $\Phi(N)$ of the Euler totient function.

As in the RSA and LUC cryptosystems, the strength of the system that is to be constructed, depends on the difficulty of factoring large numbers. Thus, it is necessary to pick two large secret primes $p$ and $q$, the product $N$ of which is part of the public key. The encryption key is $(e, N)$ which is made public. Note that, $e$ must be chosen so that it is relatively prime to the function $\Phi(N) = \overline{pq}$ because it is necessary to solve the congruence $ed \equiv 1 \bmod \Phi(N)$ to find the decoding key $d$. In practice, since $\Phi(N)$ depends on the type of an auxiliary polynomial, we choose $e$ prime to $p-1, q-1$, $p+1, q+1, p^2+p+1$ and $q^2+q+1$ to cover all possible cases.

Another problem that needs to be addressed, which is not present in the LUC cryptosystem, is that an extra term of the recurrence is required to effect the encoding and decoding. In order to compute $V_{ed}(P, Q, 1)$ via the composition law (3), in addition to the term $V_e(P, Q, 1)$, we shall need to know $V_{-e}(P, Q, 1) = V_e(Q, P, 1)$. Since $V_e(Q, P, 1)$ is unknown to the receiver with only the knowledge of $V_e(P, Q, 1)$, both

$$C_1 = V_e(P, Q, 1) \quad \text{and} \quad C_2 = V_e(Q, P, 1)$$

must be incorporated in the encoded message derived from $P$ and $Q$.

A. The cubic cryptosystem defined. With these preliminary observations, we can now set up a public-key cryptosystem based on the cubic recurrence sequence $V_n$ derived from the cubic polynomial (1).

The encryption function is defined by

$$E(P, Q) = \left(V_e(P, Q, 1), V_e(Q, P, 1)\right) \equiv (C_1, C_2) \bmod N,$$

https://doi.org/10.1017/S0004972700037382 Published online by Cambridge University Press

where $N = pq$ as above, $V_e(P, Q, 1)$ is the $e$-th term of the cubic recurrence defined by $V_{n+3} = PV_{n+2} - QV_{n+1} + V_n \bmod N$ with initial values $V_0 = 3, V_1 = P$ and $V_2 = P^2 - 2Q$, and $(P, Q)$ constitutes the message. The public key is $(e, N)$.

The decryption key is $(d, N)$ where $d$ is the inverse of $e$ modulo $\Phi(N)$. To decipher the message, the receiver must know or be able to compute $\Phi(N)$ and then calculate

$$D(C_1, C_2) = \left(V_d(C_1, C_2, 1), V_d(C_2, C_1, 1)\right) \equiv (P, Q) \bmod N$$

which recovers the original message $(P, Q)$. To see this, observe that

$$V_d(C_1, C_2, 1) = V_d(V_e(P, Q, 1), V_e(Q, P, 1), 1) = V_{ed}(P, Q, 1) = V_{k\Phi(N)+1}(P, Q, 1) \equiv P$$

modulo $N$. A similar calculation gives the other half of the assertion.

In decoding, we are given $g(x) = x^3 - C_1x^2 + C_2x - 1$ but not $f(x) = x^3 - Px^2 + Qx - 1$ and so we have to deduce the type of $f$ in order to apply the algorithm correctly. In the present circumstances, $\left(e, \Phi(N)\right) = 1$, so this is resolved by Proposition 4(a). A similar question arises in the LUC cryptosystem where the decoder needs the value of the Legendre symbol $(D/p) = \left((P^2 - 4/p)\right)$ and must deduce this from the cipher $C = V_e(P, 1)$. This is resolved because $(D/p) = (C/p)$ as remarked in section 1.

B. An Example. To illustrate this rather terse description and the details required in the computations, we show how the system works in a particular case. (Of course, the primes here are much too small to give any security and must be chosen very much larger in any practical example.)

Let $p = 29$ and $q = 41$ be the two primes and thus, $N = 1189$. Assume that the plaintext messages are $P = 15$ and $Q = 24$. The function $f$ is given by

$$f(x) = x^3 - 15x^2 + 24x - 1.$$

If the encrypting key is $e = 13$, the sender then calculates $V_{13}(15, 24, 1) \bmod 1189$ and $V_{13}(24, 15, 1) \bmod 1189$ which are equal to $C_1 = 622$ and $C_2 = 319$ respectively. The receiver thus constructs the function

$$g(x) = x^3 - 622x^2 + 319x - 1.$$

In order to determine the decrypting key $d$, the owner of the public key (13,1189) has to determine the function $\Phi(N)$ and, to this end, must deduce the type of the function $f$ with respect to the primes $p$ and $q$.

For the prime $p = 29$, the discriminant of $g$ is $D \equiv 27 \bmod 29$ which is non-zero and this implies that $f$ is of the same type as $g$, namely $t[1, 1, 1]$, since the function

https://doi.org/10.1017/S0004972700037382 Published online by Cambridge University Press

$g(x) = x^3 - 622x^2 + 319x - 1 \equiv x^3 - 13x^2 - 1 \equiv (x-4)(x-12)(x-26) \bmod 29$. (In fact, $f(x) \equiv (x+7)(x-10)(x-12) \bmod 29$.)

In the case of the prime $p = 41$, the discriminant of $g$ is $D \equiv 6 \bmod 41$ which is also non-zero and this implies again that $f$ is of the same type as $g$, namely $t[2,1]$, since the function $g(x) = x^3 - 622x^2 + 319x - 1 \equiv x^3 - 7x^2 + 32x - 1 \equiv (x-40)\big(x^2 + 33x + 40\big) \bmod 41$. (Here, $f(x) \equiv (x+1)\big(x^2 - 16x + 1\big) \bmod 41$.)

Therefore,

$$\Phi(29 \cdot 41) = (29-1)\big(41^2 - 1\big) = 47040$$

and $d$ can be calculated to be 7237 by solving the congruence $de \equiv 1 \bmod 47040$. The cipher can now be readily decoded by computing

$$D(C_1, C_2) = \big(V_{7237}(622, 319, 1), V_{7237}(319, 622, 1)\big) \bmod 1189 \equiv (15, 24) \bmod 1189$$

which recovers the original message.

## 5. Efficiency of computation

As in the LUC cryptosystem, the first obvious test of the efficiency of the extended system is the ability to compute the $e$-th term of the third order linear recurrence sequence, that is $V_e(P,Q,1)$ and $V_e(Q,P,1) = V_{-e}(P,Q,1)$, in a reasonable amount of time, close to the efficiency of calculating the $e$-th power of an integer. Smith and Lennon [**11**] claim that LUC is as efficient as RSA. Indeed, computation of Lucas functions can be done efficiently by using the 'Doubling Rule'

$$V_{2n} = V_n^2 - 2, \; V_{2n+1} = V_n V_{n+1} - P \quad \big(V_n = V_n(P,1)\big),$$

which is used in the same way as repeated squaring in the computation of powers of integers by the so-called 'Russian peasant' method of multiplication. (See Knuth [**6**, pp. 398–401].) This algorithm produces the value of $V_n \bmod N$ in at most $\lceil \log_2 n \rceil$ steps, each of which involves a multiplication of two integers less than $N$, an addition of a bounded integer and a reduction modulo $N$. An explicit algorithm of this type is given by Williams in [**15**].

In the case of the cubic system, the doubling rule is given in section 3D:

$$V_{2n}(P,Q,1) = V_n^2(P,Q,1) - 2V_{-n}(P,Q,1), \; V_{-2n}(P,Q,1) = V_{-n}^2(P,Q,1) - 2V_n(P,Q,1).$$

This formula provides for the simultaneous calculation of $V_n(P,Q,1)$ and $V_n(Q,P,1) = V_{-n}(P,Q,1)$. Adams and Shanks [**1**] give an algorithm which takes only $O(\log n)$ operations to compute $V_n$ and $V_{-n}$ together. Define the *signature* of $n \bmod N$ as

$$V_{-n-1}, V_{-n}, V_{-n+1}, V_{n-1}, V_n, V_{n+1} \bmod N.$$

https://doi.org/10.1017/S0004972700037382 Published online by Cambridge University Press

The idea is to compute the signature of $n \bmod N$ assuming we already have the signatures of all $m \bmod N$ with $m < n$. The doubling rule is used to compute

$$V_{-2m-2}, V_{-2m}, V_{-2m+2}, V_{2m-2}, V_{2m}, V_{2m+2} \bmod N.$$

The gaps in the above list can be filled by taking the equations:

$$\begin{aligned} V_{-2m-1} &= V_{-2m+2} - PV_{-2m+1} + QV_{-2m} \\ V_{-2m+1} &= PV_{-2m} - QV_{-2m-1} + V_{-2m-2} \end{aligned}$$

and

$$\begin{aligned} V_{2m-1} &= V_{2m+2} - PV_{2m+1} + QV_{2m} \\ V_{2m+1} &= PV_{2m} - QV_{2m-1} + V_{2m-2} \end{aligned}$$

and solving each of the two pairs simultaneously to obtain five successive values centred around $V_{-2m}$ and $V_{2m}$ and thus giving the signature of $2m$ and $2m+1$ modulo $N$.

Suppose the integer $n$ is written in binary and read from left to right one bit at a time. The first (that is, most significant) bit is 1. If the first $k$ bits produce some number $m$, then the first $k+1$ produce $2m$ or $2m+1$ according as the $(k+1)$-st bit equals 0 or 1. In $\lceil \log_2 n \rceil$ steps, we have the six values above, corresponding to the signature of $n$. The main computation time in each step is the time used in computing $V_m^2$ for the doubling rule but it can be economised by using Toom-Cook arithmetic. (See [**6**, pp. 260-266].)

Selecting the appropriate keys and finding suitable primes do not appear to be any more difficult than in the case of the RSA or the LUC cryptosystems. Although a maximal period is not guaranteed, iterating $P^e$ or $V_e(P,Q,1)$ almost surely gives a large orbit. Otherwise, the Pollard method factorises $N$ easily and leads to a successful attack on the cryptosystem. (See, for example, Riesel [**9**, pp. 172–183 and 235].) A specific result of this type is that if $e < N$ and $d < n^{1/4}$, then $d$ can be easily determined and thus $N$ can be factorised (Wiener [**13**]). The only extra work needed is to determine the type of the function $f$ and thus find the appropriate $\Phi(N)$. This has been discussed in Section 4F where it was shown that the calculations can be handled efficiently.

The decryption key $d$ may have up to twice as many digits as in an RSA system of similar block size because it is obtained by solving a congruence modolo $\Phi(N) \sim p^2q^2$. In this worst case, decryption may take about twice as long as in the similar RSA system with the algorithms described above.

https://doi.org/10.1017/S0004972700037382 Published online by Cambridge University Press

## 6. Security against a chosen message attack

As one of the applications of their new ideas, Diffie and Hellman [**5**] proposed a scheme which uses a public key system to sign messages. For the RSA cryptosystem, and in its simplest form, a user A whose public key is $(e, N)$ and secret decoding key is $d$ signs a message $M$ with the signature $C \equiv M^d \bmod N$. The signature can be checked using the public key by computing $C^e \equiv M \bmod N$. This RSA signature scheme is susceptible to a chosen message attack. Suppose B wants to make A sign or decode the message $M$ without A's consent. B chooses a random integer $k$ and asks A to sign $M' = Mk^e \bmod N$. This yields $C' \equiv M^d k^{ed} \equiv M^d k \bmod N$. Consequently, B can compute the signature of $M$ by means of $C \equiv M^d \equiv C' k^{-1} \bmod N$.

It may appear from this description that the chosen message attack on RSA is a consequence of its multiplicative structure. One reason for interest in the the LUC cryptosystem was a suggestion [**11**] that it would manifest greater security because it apparently lacked a multiplicative or another simple functional structure. Bleichenbacher, Bosma and Lenstra [**2**] showed that LUC does have a multiplicative structure and that signatures for two chosen messages could be used to break the LUC cryptosystem. This paper left open the possibility that LUC might be harder to attack than RSA. However, Bleichenbacher, Joyce and Quisquater [**3**] recently showed how to use one chosen message to make a successful attack on LUC. The argument is easily adapted to our cubic cryptosystem. In this sense, the security of the cubic cryptosystem is comparable to that of both RSA and LUC.

**Proposition 5.** *The cubic cryptosystem is susceptible to a chosen message attack.*

Proof: Suppose A uses the public key $(e, N)$. Suppose B wants to make A sign or decode the message $M = (P, Q)$ without A's consent. Denote the secret decoding key corresponding to this message by $d$.

B chooses a random integer $k$ with $(k, e) = 1$ and $(k, \Phi(N) = 1)$ and finds integers $r$ and $s$ with $kr + es = 1$. B asks A to sign the message $M' = (P', Q') = \big(V_k(P, Q, 1), V_k(Q, P, 1)\big)$ and gets $C' = (C'_1, C'_2) = \big(V_d(P', Q', 1), V_d(Q', P', 1)\big)$. Note that, by Proposition 4, the type is the same for the messages $(P, Q)$ and $(P', Q')$ and, in particular, the same decoding key $d$ applies.

B can now compute the signature $C = (C_1, C_2) = \big(V_d(P, Q, 1), V_d(Q, P, 1)\big)$ of $M$ by means of the equations

$$C_1 \equiv \frac{1}{3}\big[V_r(C'_1, C'_2, 1)V_s(P, Q, 1) + U_r(C'_1, C'_2, 1)W_s(P, Q, 1) + W_r(C'_1, C'_2, 1)U_s(P, Q, 1)\big]$$

$$C_2 \equiv \frac{1}{3}\big[V_r(C'_2, C'_1, 1)V_s(Q, P, 1) + U_r(C'_2, C'_1, 1)W_s(Q, P, 1) + W_r(C'_2, C'_1, 1)U_s(Q, P, 1)\big]$$

To verify these equations, observe that from the definition (2), a direct calculation gives

$$V_{n+m} = \frac{1}{3}(V_n V_m + U_n W_m + W_n U_m).$$

The observation leading to the identity (3) also gives

$$U_{nk}(P,Q,1) = U_n\big(V_k(P,Q,1), V_k(Q,P,1),1\big)$$
$$W_{nk}(P,Q,1) = W_n\big(V_k(P,Q,1), V_k(Q,P,1),1\big).$$

Now it is easy to verify that $V_{dkr}(P,Q,1) \equiv V_r(C_1', C_2', 1) \bmod N$ with similar congruences for $U$ and $W$. Consequently,

$$\begin{aligned} V_d(P,Q,1) &= V_{d(kr+es)}(P,Q,1) \equiv V_{dkr+s}(P,Q,1) \\ &\equiv \frac{1}{3}(V_{dkr}V_s + U_{dkr}W_s + W_{dkr}U_s)(P,Q,1) \bmod N \\ . \end{aligned}$$

and this can be computed from $C_1'$ and $C_2'$ without knowing $d$.

## References

[1] W. Adams and D. Shanks, 'Strong primality tests that are not sufficient', *Math. Comp.* **39** (1982), 255–300.

[2] D. Bleichenbacher, W. Bosma and A.K. Lenstra, 'Some remarks on Lucas-based cryptosystems', in *Crypto '95*, (G. Goos, J. Hartmanis and J. van Leeuwen, Editors), Lecture Notes in Computer Science **963** (Springer-Verlag, New York, 1996), pp. 386–396.

[3] D. Bleichenbacher, M. Joyce and J. J. Quisquater, 'A new and optimal chosen-message attack on RSA-type cryptosystems', in *Information and Communications Security*, (Y. Han, T. Okamoto and S. Qing, Editors), Lecture Notes in Computer Science **1334** (Springer-Verlag, New York, 1997), pp. 302–313.

[4] L. Childs, *A concrete introduction to higher algebra* (Springer-Verlag, New York, 1979).

[5] W. Diffie and M. Hellman, 'New directions in cryptography', *IEEE Trans. Inform. Theory* **IT-22** (1976), 644–654.

[6] D.E. Knuth, *The art of computer programming*, Seminumerical Algorithms, Vol. 2 (Addison-Wesley, Reading, 1969).

[7] D.H. Lehmer, 'An extended theory of Lucas' functions', *Annals Math.* **31** (1930), 419–448.

[8] E.A. Lucas, 'Théorie des fonctions numériques simplement périodiques', *Amer. J. Math.* **1** (1878), 184–239, 289–322.

[9] H. Riesel, *Prime numbers and computer methods for factorisation*, Progress in Mathematics **57** (Birkhauser, Boston, 1985).

[10] R. Rivest, A. Shamir and L. Adleman, 'A method for obtaining digital signatures and public key cryptosystems', *Comm. ACM* **21** (1978), 120–126.

https://doi.org/10.1017/S0004972700037382 Published online by Cambridge University Press

[11] P.J. Smith and M.J.J. Lennon, 'LUC: A new public key system', in *Proceedings of the ninth IFIP International Symposium on Computer Security* (Elsevier Science Publications, Amsterdam, 1994), **pp.** 103–117.

[12] M. Ward, 'The characteristic number of a sequence of integers satisfying a linear recursion relation', *Trans. Amer. Math. Soc.* **35** (1933), 153–165.

[13] M.J. Wiener, 'Cryptanalysis of short RSA secret exponents', *IEEE Trans. Inform. Theory* **IT-36** (1990), 553–558.

[14] H.C. Williams, 'On a generalization of the Lucas Functions', *Acta Arith.* **20** (1972), 33–51.

[15] H.C. Williams, 'A $p+1$ method of factoring', *Math. Comp.* **39** (1982), 225–234.

[16] H.C. Williams and C.R. Zarnke, 'Some algorithms for solving a cubic congruence modulo $p$', *Utilitas Math.* **6** (1974), 285-306.

Mathematics Department
Universiti Putra Malaysia
43400 UPM Serdant
Malaysia
e-mail: mrushdan@fsas.upm.edu.my

Deputy Vice-Chancellor
Macquarie University
Sydney NSW 2109
Australia
e-mail: John.Loxton@mq.edu.au

https://doi.org/10.1017/S0004972700037382 Published online by Cambridge University Press