A PROBABILISTIC VARIANT OF THE LUC PUBLIC KEY CRYPTOSYSTEM

AASHIR MEHROTRA

Abstract. The paper focuses on a cryptosystem devised by Guilhem Castagnos, which involves quadratic field quotients modulo a RSA number, which are numbers with two prime factors used in RSA encryption, and are often called semiprimes. The cryptosystem is probablistic, and adapts the LUC encryption system (which makes use of Lucas sequences) to quadratic fields modulo a semiprime.

1. Introduction

The paper will begin by introducing some basic terminology and tools from quadratic number theory, such as the norm and trace of elements. Specifically, we will be studying the ring of integers of the quadratic number field $\mathbb{Q}(\sqrt{\Delta})$ modulo a number a coprime to Δ We heavily consider the multiplicative group of norm 1, denoted by $(\mathcal{O}_\Delta/a\mathcal{O}_\Delta)^*$, and find the size of its order.

Next, we describe the Lucas sequences $U(P,Q)$ and $V(P,Q)$ giving an efficient algorithm that computes $V(P,1)$ similar to square and multiply used in ordinary exponentiation. The paper will subsequently show two cryptosystems: the LUC cryptosystem and the Catalano, Gennaro et al. cryptosystem. The first system uses the Lucas sequences $V(P,1)$ for encryption and decryption, along with quadratic number fields for its proof of correctness. The second system is a probablistic variant of RSA that maps a message in $\mathbb{Z}/n\mathbb{Z}$ to a ciphertext in $[\mathbb{Z}/(n^2)]^\times$. The cryptosystem given by Castagnos combines both these cryptosystems. Specifically, let $n = pq \equiv 1 \pmod 2$. Suppose e is an integer prime to $(p^2-1)(q^2-1)$, and we have the following:

$$\begin{aligned} \Lambda'_n &= \{x \in \mathbb{Z}, 0 \le x < n, \gcd(x,n) = \gcd(x^2-4,n) = 1\} \\ \Omega_n &= \{x \in \mathbb{Z}, 0 \le x < n^2, \gcd(x,n) = \gcd(x^2-4,n) = 1\} \\ \mathcal{E}'_e &: \mathbb{Z}/n\mathbb{Z} \times \Lambda'_n \to \Omega_n \mid (m,r) \to (1+mn)V_e(r) \pmod{n^2} \end{aligned} \tag{1.1}$$

where $V_e(r) = V_e(r,1)$ is a Lucas sequence. The paper's claim is that this map forms a bijection and makes a for a well-defined cryptosystem. To conclude, the paper provides an encryption and decryption algorithm for the Castagnos cryptosystem.

2. Quadratic Number Fields

For a non-square $\Delta \in \mathbb{Z}$, we define $\mathbb{Q}\left[\sqrt{\Delta}\right]$ as the field extension of $\mathbb{Q}$ adjoined by the square root of Δ. The set of algebraic integers (algebraic numbers that are the roots of monic polynomials with integer coefficients) in $\mathbb{Q}\left[\sqrt{\Delta}\right]$ can be written in the form

$$a + b\sqrt{\Delta},$$

Date: August 15, 2024.

where $a, b \in \mathbb{Z}$ if $\Delta \equiv 2, 3 \pmod 4$. If $\Delta \equiv 1 \pmod 4$, then either $a, b \in \mathbb{Z}$, or else $a + \frac{1}{2}, b + \frac{1}{2} \in \mathbb{Z}$. We denote the ring of integers as $\mathcal{O}_\Delta$. If we denote $\delta = \sqrt{\Delta}$, and $\eta = \frac{1}{2}(1 + \delta)$, then it's clear to see that the ring $\mathcal{O}_\Delta$ is isomorphic to either $\mathbb{Z}[\delta]$ or $\mathbb{Z}[\eta]$. For an integer a coprime to Δ, the quotient ring $\mathcal{O}_\Delta / a\mathcal{O}_\Delta$ is a free module of rank 2 over $\mathbb{Z}/a\mathbb{Z}$ (with basis elements equal to 1 and δ or 1 and η depending on Δ modulo 4). If $\alpha = a + b\delta \in \mathcal{O}_\Delta$, we define norm and trace functions by:

$$\mathrm{N}(\alpha) = a^2 - \Delta b^2$$

$$\mathrm{Tr}(\alpha) = 2a.$$

It's easy to show that the norm function is multiplicative and the trace function is additive. Also, the group of units can be described as elements with norm not equal to 0.
We denote the group of units with norm 1 in this ring by $(\mathcal{O}_\Delta / a\mathcal{O}_\Delta)^*$. Then we have the following proposition:

Proposition 2.1. *If $\phi_\Delta(a)$ is the order of the group of units with norm 1 modulo a, $\gcd(a, \Delta) = 1$, and $a = \prod_{p|a} p^{a_p}$, then*

$$\phi_\Delta(a) = \prod_{p|a} p^{a_p - 1} \left(p - \left(\frac{\Delta}{p} \right) \right)$$

where $\left(\frac{\Delta}{p} \right)$ is the Legendre symbol.

This is equivalent to showing that the above expression for $\phi_\Delta(a)$ equals the number of solutions to the equation

$$x^2 - \Delta y^2 \equiv 1 \pmod a. \tag{2.1}$$

Proof of Proposition 2.1. We first prove the theorem for prime numbers, then prime powers. The theorem will then follow through the Chinese Remainder Theorem. Suppose first that Δ is a quadratic residue modulo p, with $\delta^2 = \Delta$. Then we have

$$x^2 - \Delta y^2 = (x + \delta y)(x - \delta y) = 1.$$

This means that there exists some $l \in \mathbb{F}_p^\times$ such that

$$x + \delta y = l \text{ and } x - \delta y = l^{-1}.$$

Then $x = \frac{l + l^{-1}}{2}$ and $y = \frac{l - l^{-1}}{2\delta}$. The map $l \to (x, y)$ given above is injective, and thus there are $p - 1$ solutions to Equation 2.1.

Now we assume Δ is a quadratic non-residue modulo p. Similar to deriving rational points in a circle, we choose a base solution to Equation 2.1, say $(x, y) = (0, 1)$. Then every other solution can be parametrized of the form $y = mx + 1$, where $m \in \mathbb{F}_p$ is arbitrarily chosen. Actually $m \neq 0$ gives a tangent line, and the point $(0, -1)$ cannot be attained through this parameterization. So we assume for know $m, x \neq 0$ for now.
We have

$$\begin{aligned} & x^2 - \Delta(mx + 1)^2 = 1 \\ \implies & (1 - \Delta m^2)x^2 = -2\Delta m x \\ \implies & x = \frac{-2\Delta m}{1 - \Delta m^2}. \end{aligned}$$

Note that we can divide by $1 - \Delta m^2$ as Δ is a non-square. This gives $p - 1$ solutions for (x, y) ranging m through $\mathbb{F}_p$ except for $m = 0$. In total, we have $p + 1$ solutions.

Now, we prove that for $r \geq 2, \phi_\Delta(p^r) = p\phi_\Delta(p^{r-1})$, which will complete the proof of the proposition through induction. Let $x = cp^{r-1}+d$ and $y = up^{r-1}+v$ be a solution to Equation 2.1 modulo p^r., where $0 \leq c, u < p$, and $0 \leq d, v < p^{r-1}$. We have

$$x^2 - \Delta y^2 \equiv (cp^{r-1} + d)^2 - \Delta(up^{r-1} + v)^2 \equiv d^2 - \Delta v^2 + 2p^{r-1}(cd - \Delta uv) \equiv 1 \pmod{p^r},$$

implying that $d^2 - \Delta v^2 \equiv 1 \pmod{p^{r-1}}$ and that $cd - \Delta uv \equiv 0 \pmod{p}$. For a fixed (d, v), there are exactly p distinct (c, u) pairs that satisfy the second congruence. Thus, the relation claimed above holds. ■

3. Lucas Sequences

For this paper, we would need to know the two **Lucas sequences** $U_k(P, Q)$ **and** $V_k(P, Q)$ where $P, Q \in \mathbb{Z}$ defined as

$$U_{k+2} = PU_{k+1} - QU_k;\ U_0 = 0,\ U_1 = 1$$
$$V_{k+2} = PV_{k+1} - QV_k;\ V_0 = 2,\ V_1 = P.$$

if $P^2 - 4Q^2$ is a square modulo n, then both sequences U_k and V_k can be expressed as

$$\equiv c_1\alpha_1^k + c_2\alpha_2^k \pmod{n} \tag{3.1}$$

where $c_1, c_2, \alpha_1, \alpha_2 \in \mathbb{Z}$. If $P^2 - 4Q$ is a non-square, then it's difficult to compute the Lucas sequence modulo p using Equation 3.1.

We will only be concerned with computing $V_k(P, 1)$ modulo n such that $P^2 - 4$ is a not a perfect sqaure. Using the characteristic equation, it is possible to check the following identity

$$V_{i+j} = V_iV_j - V_{i-j} \tag{3.2}$$

holds in $\mathbb{Z}$.

Lemma 3.1. *Let Δ be a non-square integer and a and odd integer with $\gcd(a, \Delta) = 1$. Let $\alpha = x + \Delta y$ be an element of $\mathcal{O}_\Delta$. For natural numbers n we have*

$$\alpha^n \equiv \frac{V_n(2x, \mathrm{N}(\alpha))}{2} + yU_n(2x, \mathrm{N}(\alpha))\sqrt{\Delta} \pmod{a\mathcal{O}_\Delta}.$$

As a corollary, we have

$$\mathrm{Tr}(\alpha^n) \equiv V_n(2x, \mathrm{N}(\alpha)) \pmod{a\mathcal{O}_\Delta}.$$

Proof. Let $P = 2x$ and $Q = x^2 - \Delta y^2$. Since Δ is a non-square, so must $P^2 - 4Q$. The result holds trivially for $n = 0$ and $n = 1$. By induction, the following expression holds:

$$\alpha^n = P\alpha^{n-1} - Q\alpha^n,$$

which proves the lemma by induction along with the defining recurrences of U_n and V_n. ■

We shall now present an algorithm that mimicks the square and multiply approach used to exponentiate quickly modulo n.

Algorithm 1. Let

$$k = \sum_{i=0}^{s-1} k_i 2^i$$

be the binary expansion of k Note that $k_i \in \{0,1\}$, and $k_{s-1} = 1$. We define K_i from $s-1 \geq i \geq 0$ so that

$$K_j = \sum_{i=j}^{s-1} k_i 2^{i-j}.$$

We have the following identities for K_{j-1} and $K_{j-1}+1$:

$$K_{j-1} = k_{j-1} + 2K_j = (K_j + k_{j-1}) + K_j$$
$$K_{j-1} + 1 = k_{j-1} + 2K_j + 1 = (K_j + k_{j-1}) + (K_j + 1)$$

Plugging these identites to Equation 3.2 gives

$$V_{K_{j-1}} = V_{K_j + k_{j-1}} V_{K_j} - V_{k_{j-1}}$$
$$V_{K_{j-1}+1} = V_{K_j + k_{j-1}} V_{K_j+1} - V_{k_{j-1}+1}.$$

The algorithm thus must find V_0, V_1, and V_2 as a pre-computation .Thus, we can inductively find $V_{K_{j-1}}$ and $V_{K_{j-1}+1}$ using V_{K_j} and V_{K_j+1}. Eventually, the algorithm terminates when it reaches $K_0 = k$.

4. The LUC and the Catalano, Gennaro et al. cryposystems

A natural number n is an **RSA integer** if it is the product of two primes p and q. These numbers are used as the modulus when encrypting and decrypting in the RSA cryptosystem. The LUC cryptosystem improves the speed of RSA, by working in the ring $\mathcal{O}./a\mathcal{O}.$ and computing the trace of α^e, for some element α. As seen in Lemma 3.1, this can be done using a Lucas sequence.

Specifically, we have the following (here $V_e(x)$ denoted $V_e(x,1)$):

Definition 4.1. Let $n = pq$ be an RSA integer, and let Λ_n be the set

$$\Lambda_n = \{x \in \mathbb{Z}, 0 \leq x < n, \gcd(x^2 - 4, n) = 1\}$$

and let e be an integer coprime to $(p^2-1)(q^2-1)$. Define the function $\mathbf{LUC}_e : \Lambda_n \to \Lambda_n$ as

$$x \to V_e(x) \pmod{n}$$

Claim 4.2. *The function defined above is well-defined and is a permutation of Λ_n.*

Proof. Suppose $x \in \Lambda_n$, and let Δ be a non-square integer such that $\Delta \equiv x^2 - 4 \pmod{n}$. Then $\gcd(\Delta, n) = 1$. Define $\alpha \in \mathcal{O}_\Delta$ such that $\alpha \equiv \frac{x+\sqrt{\Delta}}{2} \pmod{n\mathcal{O}_\Delta}$. Thus, α is a norm 1 element modulo n, and has trace x. Thus, we have $\mathrm{LUC}_e(x) \equiv V_e(x) \equiv \mathrm{Tr}(\alpha^e) \pmod{n}$. As $\mathrm{N}(\alpha^e) \equiv 1 \pmod{n\mathcal{O}_\Delta}$, and by Lemma 3.1

$$\alpha^e \equiv \frac{V_e(x) + U_e(x)\sqrt{\Delta}}{2} \pmod{n}.$$

It follows that

$$4 \equiv 4\mathrm{N}(\alpha^e) \equiv \mathrm{N}(2\alpha^e) = (V_e(x))^2 - (U_e(x))^2\Delta \pmod{n}$$
$$\implies (V_e(x))^2 - 4 \equiv (U_e(x))^2\Delta \pmod{n}$$

Thus, $V_e(x) \in \Lambda_n$ if and only if $U_e(x)$ is coprime to n.
Since the order of $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^*$ equals

$$\phi_\Delta(n) = \left(p - \left(\frac{\Delta}{p}\right)\right)\left(q - \left(\frac{\Delta}{q}\right)\right),$$

we have that the number e is coprime to $\phi_\Delta(n)$, making the homomorphism $\alpha \to \alpha^e$ an automorphism in the group $(\mathcal{O}_\Delta/n\mathcal{O}_\Delta)^*$. The inverse is a map $\alpha \to \alpha^d$ where $de \equiv 1 \pmod{\phi_\Delta(n)}$ (in fact, e is the public key of the LUC cryptosystem, and d is the private key). By Lemma 3.1, we have the following:

$$\begin{aligned}\frac{x+\Delta}{2} &\equiv \alpha \equiv (\alpha^e)^d \pmod{n\mathcal{O}_\Delta} \\ &\equiv \frac{V_d(V_e(x)) + U_e(x)U_d(V_e(x))\sqrt{\Delta}}{2} \pmod{n\mathcal{O}_\Delta}\end{aligned}$$

Thus, $V_d(V_e x)) \equiv 1 \pmod{n}$, and $U_e(x)U_d(V_e(x)) \equiv 1 \pmod{n}$. The second congruence implies that $U_e(x)$ is coprime to n, and thus $V_e(x) \in \Lambda_n$. Since e and d play symmetric roles, we can conclude by the first congruence that the LUC function is a permutation of Λ_n. ■

Corollary 4.3. *With the same notation as above, LUC_e is well-defined in and a permutation of the set*

$$\Lambda'_n = \{x \in \Lambda_n : \gcd(x, n) = 1\}.$$

Proof. It suffices to show that LUC_e is a self map of $\{x \in \mathbb{N} : \gcd(x, n) \neq 1\}$. Thus we must prove that $V_e(0) \equiv 0 \pmod{\pi}$ for every prime factor π of n. Since e, coprime to $(p^2-1)(q^2-1)$, must be odd, we have

$$V_e(0) \equiv \mathrm{Tr}((\sqrt{\Delta}/2)^e) \equiv 0 \pmod{\pi},$$

proving that the set of all numbers not coprime to n are mapped to themselves. ■

The decryption algorithm for the LUC cryptosystem boils down to finding $e^{-1} \pmod{\phi_\Delta(n)}$ and computing $V_d(c) \pmod{n}$, where c is the ciphertext.

Another cryptosystem, introduced by Catalano, Gennaro et al. employs a probabalistic approach to RSA. Let $n = pq$, and let e be an integer coprime to $\phi(n) = (p-1)(q-1)$. The pair (n, e) is the public key of the cryptosystem. Next, we choose a random element r from the set

$$R_n = \{x \in \mathbb{Z}, 0 \leq x < n, \gcd(x, n) = 1\}.$$

The cipher function $\mathcal{E}_e : \mathbb{Z}/n\mathbb{Z} \times R_n \to (\mathbb{Z}/n^2\mathbb{Z})^\times$ is as follows

$$(m, r) \to (1 + mn)r^e \pmod{n^2},$$

where m is the plaintext and r is random.

This function can be shown to be bijective. We have that the ciphertext $c \equiv (1+mn)r^e \equiv r^e \pmod{n}$. Since exponentiation by an exponent e coprime to $\phi(n)$ gives rise to an automorphism in R_n, the random number r is uniquely determined by c. The uniqueness of m follows as a consequence of the uniqueness of r, by diving c by r^e modulo n^2.

To decrypt $c \in \mathbb{Z}/n^2\mathbb{Z}$, we first compute $d \equiv e^{-1} \pmod{\phi(n)}$. Next, we reduce c modulo n, and exponentiate this by d to retrieve the value of r. By computing $c/r^e \pmod{n^2}$, we can retrieve $1 + mn$, and thsu retrieve m.

5. Castagnos' Quadratic Number Field Cryptosystem

This cryptosystem aims to bridge the two cryposystems that have just been described. This system is able to have an extremely good computational efficiency due to exponentiating being hastened by Algorithm 1. The description of the cryposystem has been made in 1.1. We shall now prove that the cryposystem works:

Proposition 5.1. *The function $\mathcal{E}'_e$ is well-defined and bijective.*

Proof. Let (m, r) be an element of $\mathbb{Z}/n\mathbb{Z} \times \Lambda'_n$. To prove that $\mathcal{E}'_e(m, r)$ is well defined, we need to show that $c \equiv (1 + mn)V_e(r) \in \Omega_n$. Since $c \pmod n$ equals $\mathrm{LUC}_e(r)$, and $r \in \Lambda'_n$, it follows that $c \pmod n$ is in Λ'_n, which implies that $c \in \Omega_n$.

I claim that $|\Lambda'_n| = (p-3)(q-3)$. This is because, if we require that n is coprime with $x^2 - 4$ and x, this implies that p and q must not divide any of $(x-2), (x+2)$, and x. This restrict the congruences classes modulo p and modulo q to $p-3$ and $q-3$ respectively, and thus $(p-3)(q-3)$ congruences $\pmod n$ will satisfy the conditions for Λ'_n. Since Ω_n has the exact same definition, though extended till n^2, we have $|\Omega_n| = n(p-3)(q-3)$.

These results imply that the domain and co-domain of $\mathcal{E}'_e$ have the same cardinality, thus it sufficies to show that the cipher function is one to one. Suppose there exists distinct $(m_1, r_1), (m_2, r_2)$ such that $(1 + m_1 n)V_e(r_1) = (1 + m_2 n)V_e(r_2)$. Reducing modulo n gives us the LUC function on r_1 and r_2, which we know is bijective over Λ'_n. Thus $r_1 = r_2$, and $m_1 = m_2$ by a similar argument to the one we used for the Catalano, Gennaro et al. cryposystem. ∎

To conclude this paper, we present the encryption and decryption algorithm for the Castagnos cryptosystem. First, we prove a lemma:

Lemma 5.2. *Let $n = pq$. Suppose $c = \mathcal{E}'_e(m, r)$ be the cipher text of some message, and let $\Delta \equiv r^2 - 4 \pmod n$ be a non-square integer. For each prime factor π of n we have that*

$$\left(\frac{\Delta}{p}\right) = \left(\frac{c^2 - 4}{p}\right)$$

Proof. Let $\alpha \in \mathcal{O}_\Delta$ such that $\alpha = \frac{r+\Delta}{2} \pmod{n^2}$. We have $\mathrm{N}(\alpha) \equiv 1 \pmod{n^2}$, and thus by Lemma 3.1,

$$\begin{aligned} 4 \equiv 4\mathrm{N}(\alpha^e) &\equiv (V_e(r))^2 - (U_e(r))^2\Delta \pmod n \\ \implies \Delta &\equiv \frac{(V_e(r))^2 - 4}{(U_e(r))^2} \pmod n \end{aligned} \tag{5.1}$$

It must be that $U_e(r)$ is invertible in the above congruence as $r \in \Lambda'_n$ implies that Δ is coprime to n, along with Claim 4.2 implying that $\gcd((V_e(r))^2 - 4, n) = 1$. Thus, Equation 5.1 alongside the fact that $c \equiv V_e(r) \pmod \pi$. implies that

$$\left(\frac{\Delta}{\pi}\right) = \left(\frac{(V_e(r))^2 - 4}{\pi}\right) = \left(\frac{c^2 - 4}{\pi}\right).$$

∎

Algorithm 2 (Encryption). Given a public key (n, e) and a plaintext $m \in \mathbb{Z}/n\mathbb{Z}$, the encryptor chooses a random r between 1 and n excluding 2 and $n-2$. Note that if n is hard to factor, then $r \in \Lambda'_n$ with probability close to 1. The cipher text is generated by

$$\mathcal{E}'_e(m, r) = (1 + mn)V_e(r).$$

The decryptor will be knowing the factorisation of $n = pq$, and would also be aware of these four private key exponents:

$$d := (d_{p,1}, d_{p,-1}, d_{q,1}, d_{q,-1}),$$

where $d_{\pi,i} = e^{-1} \pmod \pi$ for $i = \pm 1$ and for π being a prime divisor of n.

Algorithm 3 (Decryption). The decryptor is aware of p, q, and the four component vector private key d, along with the ciphertext c. For the pre-computation, the decryptor finds $\text{inv}_p \equiv p^{-1} \pmod{q}$ and $\text{inv}_q \equiv q^{-1} \pmod{p}$.

For each $\pi \in \{p, q\}$, we compute

$$i_\pi = \left(\frac{c^2 - 4}{\pi}\right)$$
$$r_\pi = V_{d_{\pi,i_\pi}}(c) \pmod{\pi}.$$

This will compute the value of r modulo p and q; its proof of correctness follows immediately from Lemma 5.2 and the fact that V_e and $V_{(d,i_\pi)}$ are inverses of one another modulo n.

We then compute

$$r = r_p + p(r_q - r_p)\text{inv}_p \pmod{n}$$

Now that we have the value of r, the following computations will easily allow use to retrieve the value of m easily:

For $\pi \in \{p, q\}$, compute

$$k_\pi = c(V_e(r))^{-1} \pmod{\pi^2}$$
$$l_\pi = \frac{k_\pi - 1}{\pi}$$
$$m_\pi = k_\pi \times \text{inv}_{n/\pi} \pmod{\pi},$$

where $\text{inv}_{n/\pi}$ is the inverse of the prime not chosen as π modulo π. Finally, we can combine m_p and m_q to recover the original plaintext m:

$$m = m_p + p(m_q - m_p)\text{inv}_p \pmod{n}$$

Note that from this algorithm, we can infer that we require e to be coprime to $(p^2-1)(q^2-1)$ as it is a common multiple of all possible values of $\phi_\Delta(n)$.

6. Acknowledgements

I would like to thank my instructor Simon Rubinstein-Salzedo, my and my mentor Carson Mitchell for their guidance and feedback on this paper, which was done for a cryptography class in Euler Circle.

References

[1] Guilhem Castagnos. An efficient probabilistic public-key cryptosystem over quadratic fields quotients. *Finite Fields and Their Applications*, 13(3):563–576, 2007.

[2] Henri Cohen. *A course in computational algebraic number theory*, volume 138. Springer Science & Business Media, 2013.

[3] Marc Joye and Jean-Jacques Quisquater. Efficient computation of full lucas sequences. *Electronics Letters*, 32(6):537–537, 1996.

[4] Simon Rubinstein-Salzedo. *Cryptography*, volume 260. Springer, 2018.

[5] Peter J Smith and Michael JJ Lennon. Luc: A new public key system. In *SEC*, pages 103–117. Citeseer, 1993.