ABSTRACT

Title of Dissertation: Analysis and Extension of Non-Commutative NTRU

Kathryn Rendall Truman, Doctor of Philosophy, 2007

Dissertation directed by: Professor Lawrence Washington
Department of Mathematics

We discuss the ring based public-key cryptosystem known as non-commutative NTRU. The original system is defined over the group ring $R = \mathbb{Z}[D_N]$ (where D_N is the dihedral group of order $2N$) and uses a commutative subring $R_0 = \{\alpha \in R | Y\alpha = \alpha Y\}$ where Y is an element of order two for D_N. This system was broken by Coppersmith in [1]. To do this he uses properties of the subset $R_1 = \{\alpha \in R \mid Y\alpha = -\alpha Y\}$. He is able to create a 'fake' private key using R_1 and R_0. This 'fake' private key then allows him to create a map $\theta : R \to R$ that is used to break the system.

The present discussion first analyzes the original system and the attack on the system. We also determine what groups the original system can be defined over, and therefore when Coppersmith's attack will work. Second we extend this system to other group rings. The groups have two generators that do not commute, but the generators will have prime orders larger than two. We still

work with the ring $\mathbb{Z}[G]$ and the subring of elements that commute with Y, the generator with smaller order. We then extend the attack on the system. This is where the key difference arises. We develop the representation theory of these more general groups so that we can break the system. Also to break the system we need to look at subsets of $\mathbb{Z}[G]$ where conjugation by Y (of order k) multiplies the elements by a k^{th} root of unity. We denote these subsets by $R_1, R_2, \ldots, R_{k-1}$. One of the main results is to show that these R_j are principal R_0 modules. This allows us to define a similar θ. Since a primitive k^{th} root of unity does not always exist modulo q it is necessary to work in an extension ring to break the system in some cases. But when θ is created it maps into the original group ring, which allows us to break the system. Finally we give a few examples.

Analysis and Extension of Non-Commutative NTRU

by

Kathryn Rendall Truman

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2007

Advisory Committee:

Professor Lawrence Washington, Chairman/Advisor
Professor Jeffrey Adams
Professor Thomas Haines
Professor Harry Tamvakis
Professor William Gasarch, Dean's representative

DEDICATION

I would like to dedicate this to my husband Christopher Brian Rendall Truman and my daughter Isabelle Violet Truman. They are a constant source of love and support. My life would not be complete without them.

ACKNOWLEDGEMENTS

First I would like to thank my advisor Professor Larry Washington for his help and patience through this long process. He has been great a inspiration, prodded me along just when necessary, and distracted me with good conversation when that was necessary also.

I would also like to thank my family for their constant love and support. My parents, Doug and Susan Rendall, have been encouraging and supportive of my goals throughout my life and I could not have succeeded without their guidance. My sister, Dee Anna, my brother, Joe, and all of my in-laws have helped in immeasurable ways by providing babysitting, house cleaning, house repair, and conversation when I have needed each most. My husband Chris has seen me through this with a great deal of love and patience. My daughter Izzy brings me great joy and having her has helped give me the drive to finish. I know that I could not have finished this task without everything my family has done for me.

TABLE OF CONTENTS

Chapter 1

Non-commutative NTRU

1.1 Introduction

Public-key cryptography was introduced around forty years ago. It allows the users to communicate over non-secure channels without any prior communication. They do this by publishing one public key for encryption and using another private key for decryption. RSA[14] is probably the most famous public-key cryptosystem, but there are many others: ElGamal [3, 4], McEliece [11, 12], and commutative NTRU [8]. These are all commutative systems. There are also non-commutative systems such as a braid group system [10] and non-commutative NTRU [6, 1]. Our purpose is to further investigate non-commutative NTRU. We will analyze Coppersmith's attack [1] on the original system. We will also show that its original implementation can be extended and broken.

For a public-key cryptosystem, assume that Alice wants to send a message to Bob. Bob first publishes a public key and has another private key. Alice uses this public key to encrypt a message and send it to Bob. Bob then uses his private key to decrypt the message. Note that not only Alice can use Bob's public key, but also anyone who wants to send Bob a message can use his public key to do

so. In general, Bob creates his public key from his private key and it is hard for someone to find the private key from the public key.

Non-commutative NTRU is a ring based public-key cryptosystem. The original system is defined over the group ring $R = \mathbb{Z}[D_N]$ (where D_N is the dihedral group of order $2N$) and uses a commutative subring $R_0 = \{\alpha \in R \mid Y\alpha = \alpha Y\}$ where Y is an element of order two for D_N. This system was broken by Coppersmith in [1]. To do this he uses properties of the subset $R_1 = \{\alpha \in R \mid Y\alpha = -\alpha Y\}$. He is able to create a 'fake' private key using R_1 and R_0. This 'fake' private key then allows him to create a map $\theta : R \to R$ that is used to break the system.

In Sections 1.2 and 1.3 we analyze the original system and the attack on the system. Next in subsection 1.3.1 we determine what groups the original system can be defined over, and when Coppersmith's attack will work. Then in Section 2.1 we extend this system to other group rings. The groups still have two generators that do not commute, but the generators have prime orders larger than two. We still work with the ring $\mathbb{Z}[G]$ and the subring of elements that commute with Y, the generator with smaller order. We extend the attack to this generalization of the system in Section 2.3. This is where the key difference arises. Coppersmith's attack only works for $\mathbb{Z}[D_N]$ and closely related group rings. In Section 2.2 we develop the representation theory of these more general groups that is necessary to break the system. Also to break the system we need to look at subsets $R_1, R_2, \ldots, R_{k-1}$ of $\mathbb{Z}[G]$, where $R_i = \{\alpha \in R \mid Y\alpha = z_k^i \alpha Y\}$ and z_k is a primitive k^{th} root of unity. One of the main results is Theorem 2.3.10 which shows that these R_i are principal R_0 modules. Finally in Sections 2.4, 2.5, and 2.6 we define a θ to break the system. In Section 2.7 we give a few examples.

1.2 Description of Non-commutative NTRU

Non-commutative NTRU is a public-key cryptosystem. It was originally described in a manuscript by Hoffstein and Silverman [6], but the present description comes from a paper by Coppersmith[1]. The system uses the group ring $R = \mathbb{Z}[D_N]$, where D_N is the dihedral group of order $2N$. Later we will define the system using other rings, so we will call this $R_{\mathbb{Z}}$ to reduce confusion, but throughout this section it is not necessary. We can also think of this as a 'polynomial' ring with non-commutative variables $R = \mathbb{Z}[X, Y]/(X^N - 1, Y^2 - 1, YX - X^{N-1}Y)$. (This is somewhat an abuse of notation since it is normally reserved for commutative polynomial rings.) Multiplication in R will be denoted by $f * g$ or fg. Also, we need a commutative subring, R_0, consisting of all elements in R that commute with Y. In other words,

$$\begin{aligned} R_0 &= \{\alpha \in R \mid \alpha Y = Y\alpha\} \\ &= \{a_0 + \sum_{i=1}^{(N-1)/2} a_i(X^i + X^{N-i}) + b_0 Y + \sum_{i=1}^{(N-1)/2} b_i(X^i + X^{N-i})Y \mid a_i, b_i \in \mathbb{Z}\}. \end{aligned}$$

The system also involves integer parameters p, q, r, s, and t with p, r, and t small (on the order of 3 or 5) and q and s large (N is usually chosen to be somewhat large, but smaller than q.) The parameters are large to mask part of the message, or small so that when we encrypt and decrypt the message 'wrapping' modulo q does not occur. We need the assumption that p and q are prime and are relatively prime to $2N$ (otherwise the system will break down). For example Coppersmith gives the following choices of parameters in [1]:

$$N = 263, \quad p = 3, \quad q = 125003, \quad r = 5, \quad s = 90000, \quad t = 3$$

To set up the system we look at R and R_0 with restricted coefficients. We

denote these subsets as

$$R\{n\} = \{\alpha \in R \mid \text{the coefficients of } \alpha \text{ are in } \left(-\frac{n}{2}, \frac{n}{2}\right]\}.$$

The subsets we will choose our elements from are defined to be:

$$S_f = R_0\{q\}$$

$$S_m = R\{q\}$$

$$S_\phi = R_0\{r\}$$

$$S_\psi = R_0\{s\}$$

$$S_\omega = R\{t\}$$

Assume Alice wants to send a message to Bob. To start Bob must choose his private and public keys. First he chooses a random $f \in S_f$ and $\omega \in S_\omega$. Next he computes $F \in R_0$ such that $f * F \equiv 1 \pmod{q}$. (Please see Section 2.6 for when such an F exists.) Bob's public key is then $h = pF * \omega * f \pmod{q}$ and the private keys are f, F, and ω. Suppose Alice wants to send the message $m \in S_m$. To encrypt m she first randomly chooses $\phi, \phi' \in S_\phi$ and $\psi \in S_\psi$ and computes $\Psi \in R_0\{p\}$ such that $\Psi \equiv \psi \pmod{p}$. She then computes the pair (e, E) with

$$e \equiv \phi * h * \phi' + \psi \pmod{q}$$

$$E \equiv \Psi * h + m \pmod{q}$$

and sends the pair to Bob.

To decrypt the message Bob computes

$$a \equiv f * e * F \equiv p\phi * \omega * \phi' + \psi \pmod{q}$$

and then reduces this modulo p to recover $\Psi \equiv \psi \pmod{p}$. Now Bob can subtract $\Psi * h \pmod{q}$ from E to obtain m.

Example 1.2.1. *Let $N = 7, q = 101, p = r = t = 3$, and $s = 50$. Bob makes the following choices:*

$$\begin{aligned} f &= -3 + 5(X + X^6) + 2(X^2 + X^5) - (X^3 + X^4) \\ &\quad + 2Y - 3(X + X^6)Y - 5(X^2 + X^5)Y + (X^3 + X^4)Y \\ \omega &= -1 + X^2 - X^3 + X^4 + X^6 - Y + X^2Y - X^3Y + X^4Y + X^5Y \end{aligned}$$

and computes the following:

$$\begin{aligned} F &= f^{-1} \\ &= -39 + 30(X + X^6) - 37(X^2 + X^5) + 12(X^3 + X^4) \\ &\quad + 3Y - 32(X + X^6)Y - 9(X^2 + X^5)Y + 37(X^3 + X^4)Y \\ h &= F\omega f \\ &= -3 - 34X + 30X^2 + 17X^3 - 17X^4 - 27X^5 + 37X^6 \\ &\quad - 3Y + 25XY - 21X^2Y - 34X^3Y + 34X^4Y + 27X^5Y - 25X^6Y \end{aligned}$$

Bob now makes h public and keeps f, F, and ω private.

To send Bob a message Alice makes the following choices:

$$\begin{aligned} \phi &= (X + X^6) - (X^2 + X^5) + (X^3 + X^4) + Y - (X^3 + X^4)Y \\ \phi' &= 1 + (X^2 + X^5) - (X^3 + X^4) + (X + X^6)Y + (X^3 + X^4)Y \\ \psi &= -3(X + X^6) + 2(X^2 + X^5) + 2(X^3 + X^4) \\ &\quad + 4Y + 3(X + X^6)Y - 3(X^2 + X^5)Y + 4(X^3 + X^4)Y \end{aligned}$$

She reduces ψ modulo p to get $\Psi = -(X^2 + X^5) - (X^3 + X^4) + Y + (X^3 + X^4)Y$

and then computes the following:

$$\begin{aligned} e &= \phi h \phi' + \psi \\ &= 15 - 10X + 34X^2 + 26X^3 - 7X^4 - 9X^5 - 32X^6 \\ &\quad - 2Y + 43XY - 30X^2Y + 46X^3Y - 14X^4Y - 6X^5Y - 10X^6Y \\ E &= \Psi h + m \\ &= -4 - 20X - 13X^2 - 34X^3 + 26X^4 + 19X^5 + 22X^6 \\ &\quad - 11Y + 22XY + 7X^2Y + 24X^3Y - 25X^4Y + 2X^5Y - 24X^6Y \end{aligned}$$

using her message

$$m = 2 + 5X - 4X^2 + X^3 - 2X^5 - 3X^6 - 2Y + XY - 3X^3Y + 5X^4Y - 3X^6Y.$$

She now sends the pair (e, E) *to Bob.*

Bob uses his private keys to compute:

$$\begin{aligned} a &= feF \\ &= 15 - 12X + 8X^2 + 20X^3 - 1X^4 + 17X^5 - 30X^6 \\ &\quad - 2Y + 12XY - 12X^2Y + 22X^3Y + 10X^4Y - 24X^5Y + 21X^6Y \end{aligned}$$

which he then reduces modulo p *to get* $a_p = -X^2 - X^3 - X^4 - X^5 + Y + X^3Y + X^4Y$.

Next Bob computes:

$$E - ha_p = 2 + 5X - 4X^2 + X^3 - 2X^5 + 3X^6 - 2Y + XY - 3X^3Y + 5X^4Y - 3X^6Y$$

which is the message that Alice sent.

1.3 Coppersmith's Attack

In [1], Coppersmith described a method of attacking this cryptosystem. Coppersmith's attack allows a third party to decrypt a message without any knowledge of the private key. For the attack it is necessary to consider the subset R_1 of R defined by:

$$\begin{aligned} R_1 &= \{\alpha \in R \mid \alpha Y = -Y\alpha\} \\ &= \left\{ \sum_{i=1}^{(N-1)/2} a_i(X^i - X^{N-i}) + \sum_{i=1}^{(N-1)/2} b_i(X^i - X^{N-i})Y \;\middle|\; a_i, b_i \in \mathbb{Z} \right\}. \end{aligned}$$

Recall that to decrypt the message Bob used f and F to create a linear map that took the ciphertext $e \pmod q$ to the quantity $a \pmod q$. But it is not actually necessary to know f and F to create a suitable linear map. It is enough to create a linear map

$$\theta : R \pmod q \to R \pmod q$$

with the following properties:

- θ is the identity on $R_0 \pmod q$
- θ maps $R_1 \pmod q$ to itself
- θ is left and right R_0 linear
- $\theta(h)$ is a multiple of p and $\omega' = \theta(h)/p$ has small coefficients modulo q.

Such a θ gives us Ψ since

$$\begin{aligned} \theta(e) &\equiv \theta(\phi * h * \phi' + \psi) \pmod q \\ &\equiv \phi * \theta(h) * \phi' + \psi \pmod q \text{ since } \theta \text{ is } R_0 \text{ linear} \\ &\equiv \phi * p\omega' * \phi' + \psi \pmod q \end{aligned}$$

which reduces to Ψ modulo p since ω' is small (so that no wrapping occurs).

Note that the function $\theta'(\alpha) = f * \alpha * F$ is such a θ and is used by Bob to decrypt the message. We construct a θ without knowing f, F, and ω. To do this we create a suitable ω' as follows: We know that $\omega \in R\{t\}$ so we can write

$$\omega = \sum_{i=1}^{(N-1)/2} (a_i X^i + b_i X^i Y), \text{where } a_i, b_i \in \left(-\frac{t}{2}, \frac{t-1}{2}\right].$$

Also we know that

$$\begin{aligned} h + YhY &\equiv pF * \omega * f + Y(pF * \omega * f)Y \\ &\equiv pF(\omega + Y\omega Y)f \\ &\equiv p(\omega + Y\omega Y) \pmod{q}, \end{aligned}$$

since $\omega + Y\omega Y \in R_0$, so that f and F commute with it. Now we have

$$h + YhY \equiv c_0 + d_0 Y + \sum_{i=1}^{(N-1)/2} \left(c_i(X^i + X^{N-i}) + d_i(X^i + X^{N-i})Y\right) \pmod{q}$$

where $c_i, d_i \in \{-p(t-1), -p(t-2), \ldots, 0, p, 2p, \ldots, p(t-1)\}$ since if we use the labels for the coefficients of ω given above then we have $c_i = p(a_i + a_{N-i})$ and $d_i = p(b_i + b_{N-i})$.

To attack the system we must choose an $\omega' \in S_\omega$ that is 'small enough'. We choose such an ω' to satisfy the following:

$$\omega' = \sum_{i=0}^{(N-1)} (a'_i X^i + b'_i X^i Y)$$

where

$$\begin{aligned} \text{if } c_i = 2kp \quad & \text{then } a'_i = a'_{N-i} = k \\ \text{if } c_i = (2k+1)p \quad & \text{then } a'_i = k+1 \text{ and } a'_{N-i} = k \\ \text{if } d_i = 2kp \quad & \text{then } b'_i = b'_{N-i} = k \\ \text{if } d_i = (2k+1)p \quad & \text{then } b'_i = k \text{ and } b'_{N-i} = k+1 \end{aligned}$$

It is now clear that ω' satisfies

$$h + YhY \equiv p(\omega' + Y\omega'Y) \pmod{q}$$

and that it has small coefficients (on the order of ω's coefficients).

Now we can define $\theta(h) = p\omega'$ and define θ to have the other properties described above to break the system. To get θ we use linear algebra techniques and as long as h is invertible modulo q we can solve for θ. So we need to understand when h will be invertible. We will do this in Section 2.6.

We will continue with the previous example.

Example 1.3.1. *Let* $N = 7, q = 101, p = r = t = 3, s = 50$, *and*

$$\begin{aligned}
h = &-3 - 34X + 30X^2 + 17X^3 - 17X^4 - 27X^5 + 37X^6 \\
&- 3Y + 25XY - 21X^2Y - 34X^3Y + 34X^4Y + 27X^5Y - 25X^6Y \\
e = &\ 15 - 10X + 34X^2 + 26X^3 - 7X^4 - 9X^5 - 32X^6 \\
&- 2Y + 43XY - 30X^2Y + 46X^3Y - 14X^4Y - 6X^5Y - 10X^6Y \\
E = &-4 - 20X - 13X^2 - 34X^3 + 26X^4 + 19X^5 + 22X^6 \\
&- 11Y + 22XY + 7X^2Y + 24X^3Y - 25X^4Y + 2X^5Y - 24X^6Y
\end{aligned}$$

We compute

$$\begin{aligned}
h + YhY &= p(\omega + Y\omega Y) \\
&= -6 + 3(X + X^6) + 3(X^2 + X^5) - 6Y + 6(X^2 + X^5)Y \\
&= 3(-2 + (X + X^6) + (X^2 + X^5) - 2Y + 2(X^2 + X^5)Y)
\end{aligned}$$

So $\omega' = -1 + X + X^2 - Y + X^2Y + X^5Y$ *Now it is necessary to break both* h *and*

$p\omega'$ into their R_0 and R_1 parts. So we get the following:

$$\begin{aligned}
h_0 &= -3 - 49(X + X^6) - 49(X^2 + X^5) \\
&\quad - 3Y + 3(X^2 + X^5)Y \\
h_1 &= 15(X - X^6) - 22(X^2 - X^5) + 17(X^3 - X^4) \\
&\quad + 25(X - X^6)Y - 24(X^2 - X^5)Y - 34(X^3 - X^4)Y \\
\omega_0' &= h_0 \\
\omega_1' &= -49(X - X^6) - 49(X^2 - X^5)
\end{aligned}$$

Where $\omega_0' + \omega_1' = p\omega'$ Next we note that $(X - X^6)$ will generate R_1 as an R_0 module, since

$$\begin{aligned}
(X - X^6)(X + X^6) &= X^2 - X^5 \\
(X - X^6)(X^2 + X^5) &= -X + X^6 + X^3 - X^4 \quad \textit{and} \\
(X - X^6)(X^3 + X^4) &= -X^2 + X^5 - X^3 + X^4
\end{aligned}$$

so

$$\begin{aligned}
X - X^6 &= (X - X^6) * 1 \\
X^2 - X^5 &= (X - X^6) * (X + X^6) \quad \textit{and} \\
X^3 - X^4 &= (X - X^6) * (1 + (X^2 + X^5)).
\end{aligned}$$

Now we can rewrite h_1 and w_1 as the following:

$$\begin{aligned}
h_1 &= (X - X^6)(15 - 22(X + X^6) + 17(X^2 + X^5 + 1)) \\
&\quad + (X - X^6)(25 - 24(X + X^6) - 34(X^2 + X^5 + 1))Y \\
w_1 &= (X - X^6)(-49 - 49(X + X^6))
\end{aligned}$$

This reduces our work to solving

$$\theta(X - X^6)\Big((15 - 22(X + X^6) + 17(X^2 + X^5 + 1)$$
$$+ (25 - 24(X + X^6) - 34(X^2 + X^5 + 1))Y\Big)$$
$$= (X - X^6)(-49 - 49(X + X^6))$$

but $\theta(X - X^6)$ *is an element of* R_1 *so it must have the form*

$$(X - X^6) * (a + a_0(X + X^6) + a_1(X^2 + X^5) + a_2(X^3 + X^4))$$
$$+(X - X^6) * (b + b_0(X + X^6) + b_1(X^2 + X^5) + b_2(X^3 + X^4)) * Y.$$

Let

$$r_0 = a + a_0(X + X^6) + a_1(X^2 + X^5) + a_2(X^3 + X^4) +$$
$$(b + b_0(X + X^6) + b_1(X^2 + X^5) + b_2(X^3 + X^4))Y,$$

then we need only solve

$$(X - X^6)r_0\Big((15 - 22(X + X^6) + 17(X^2 + X^5 + 1)$$
$$+ (25 - 24(X + X^6) - 34(X^2 + X^5 + 1))Y\Big)$$
$$= (X - X^6)(-49 - 49(X + X^6))$$

for r_0*. Using Maple (version 9.5) and Magma (version 2-11.14) we find that*

$$r_0 = 10 + 3(X + X^6) + 7(X^2 + X^5) + 41(X^3 + X^4)$$
$$- 5Y - 6(X + X^6)Y - 36(X^3 + X^4)Y$$

Now we can define the following:

$$\theta(X - X^6) = (X - X^6)r_0,$$
$$\theta(X^2 - X^5) = (X - X^6)(X + X^6)r_0, \text{ and}$$
$$\theta(X^3 - X^4) = (X - X^6)(X^2 + X^5 + 1)r_0.$$

To break the system we need to find $\theta(e)$. To do this we break e into its R_0 and R_1 parts and get

$$\begin{aligned} e_0 &= 15 - 21(X + X^6) - 38(X^2 + X^5) - 41(X^3 + X^4) \\ &\quad - 2Y - 34(X + X^6)Y - 18(X^2 + X^5)Y + 16(X^3 + X^4)Y \\ e_1 &= 11(X - X^6) - 29(X^2 - X^5) - 34(X^3 - X^4) \\ &\quad - 24(X - X^6)Y - 12(X^2 - X^5)Y + 30(X^3 - X^4)Y. \end{aligned}$$

So $\theta(e)$ reduces to

$$\begin{aligned} \theta(e) &= e_0 + \theta(e_1) \\ &= 15 - 21X + 14X^2 + 14X^3 + 5X^4 + 11X^5 - 21X^6 \\ &\quad + (-2 + 9X + 27X^2 + 10X^3 + 22X^4 - 9X^5 + 24X^6)Y \end{aligned}$$

Reducing this modulo $p = 3$ we get $-(X^2 + X^5) - (X^3 + X^4) + (1 + (X^3 + X^4))Y$ which should be ψ modulo p. Using this and h we compute

$$\begin{aligned} &E - h * (-(X^2 + X^5) - (X^3 + X^4) + (1 + (X^3 + X^4))Y) \\ &\equiv 2 + 5X - 4X^2 + X^3 - 2X^5 - 3X^6 - 2Y + XY \\ &\quad - 3X^3Y + 5X^4Y - 3X^6Y \pmod{q}, \end{aligned}$$

which is the message m.

1.3.1 Why this works only for D_N

To attack this system we need to be able to create θ. Using θ to break the system relies on the fact that ω is small (which is necessary for the system to work). It also requires us to understand the structure of R_0 and R_1 and the fact that $p(\omega + Y\omega Y) = h + YhY$ to create ω'. We use two main facts:

- Y has order two,
- and $R_0 = \{\alpha \in R | Y\alpha = \alpha Y\}$ is commutative

Our goal is to show that given these necessary assumptions we can conclude that the group is something close to D_N.

We will use representation theory to study when the set $\{\alpha \in F[G] \mid Y\alpha = \alpha Y\}$ is commutative for $Y \in G$. This allows us to determine under what conditions we can set up the system given above. It is required that R_0 is commutative to decrypt the message (i.e. when Bob computes $a \equiv f * e * F \pmod{q}$.)

Lemma 1.3.2. *Let G be a finite group, and $R_F = F[G]$ for a ring F. Let $Y \in G$ and $R_{0,F} = \{\alpha \in R_F \mid Y\alpha = \alpha Y\}$. Then $\beta = \sum_{g \in G} a_g g \in R_{0,F}$ if and only if $\beta = \sum a_g \left(\sum_{h \in Y\text{-orbit}} h \right)$ where the outer sum is over representatives of the orbits under conjugation by Y (Y-orbits) (i.e. elements of a particular Y-orbit all have the same coefficient.)*

Proof. If $\beta = \sum_{g \in G} a_g g \in R_{0,F}$ then $\sum_{g \in G} a_g Y g Y^{-1} = \sum_{g \in G} a_g g$. So $a_{YgY^{-1}} = a_g$ for all $g \in G$. Therefore $\beta = \sum a_g \left(\sum_{h \in Y\text{-orbit}} h \right)$. Clearly if β has the form given it commutes with Y so it is in $R_{0,F}$. □

Proposition 1.3.3. *Let G be a finite group, and $R_{\mathbb{Z}} = \mathbb{Z}[G]$. Let $Y \in G$ and $R_{0,\mathbb{Z}} = \{\alpha \in R_{\mathbb{Z}} \mid Y\alpha = \alpha Y\}$, then $R_{0,\mathbb{Z}}$ is commutative if and only if $R_{0,\mathbb{C}}$ is commutative.*

Proof. This is clear from the previous lemma since it is only necessary for the sums $\sum_{h \in Y\text{-orbit}} h$ to commute with each other, which is independent of the coefficients in characteristic zero. □

This makes it possible to work over $\mathbb{C}$ and then deduce the results over $\mathbb{Z}$ when necessary. This is useful since we already understand the representation theory of G over $\mathbb{C}$.

For a general group G it is possible for $R_{0,F}$ to be non-commutative as the following shows:

Lemma 1.3.4. *Let F be a finite field or an algebraically closed field and $R_F = F[G]$ for a finite group G such that $char(F) \nmid |G|$. Let Y be an element of G. Let ρ be an irreducible representation of G over F. If $\rho(Y)$ has a repeated eigenvalue then $R_{0,F} = \{\alpha \in R_F \mid Y\alpha = \alpha Y\}$ is not commutative.*

Proof. Let ρ be an irreducible representation of G over F such that $\rho(Y)$ has a repeated eigenvalue for some $Y \in G$. By Wedderburn's theorem [13, p 142] we know that $F[G] \simeq \bigoplus M_{n_i}(D_i)$ where D_i is a division ring over F. But if F is algebraically closed then $D_i = F$, and if F is finite then D_i is also a finite field by another theorem of Wedderburn [13, p 143]. So $F[G]$ is a direct sum of matrix rings over fields. With out loss of generality let ρ be the projection of $F[G]$ onto M_{n_1}. Then $\rho(Y)$ can be put into rational canonical form. Now since $\rho(Y)$ is diagonalizable there are no repeated factors in the minimal polynomial and since $\rho(Y)$ has a repeated eigenvalue it has a repeated block. So $\rho(Y)$ has the following form:

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \vdots & \vdots \\ \vdots & \cdots & \ddots & 0 \\ 0 & \cdots & 0 & A_\beta \end{pmatrix}$$

where the A_j's come from the irreducible factors of the characteristic polynomial of $\rho(Y)$. We may assume that $A_1 = A_2$ since $\rho(Y)$ has a repeated eigenvalue.

Then the following matrices both commute with $\rho(Y)$ (as given above) and not with each other.

$$N_1 = \begin{pmatrix} 0 & I & \cdots & 0 \\ 0 & 0 & \vdots & \vdots \\ \vdots & \cdots & \ddots & 0 \\ 0 & \cdots & 0 & 0 \end{pmatrix} \qquad N_2 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ I & 0 & \vdots & \vdots \\ \vdots & \cdots & \ddots & 0 \\ 0 & \cdots & 0 & 0 \end{pmatrix}$$

Therefore $N_1 \oplus 0$ and $N_2 \oplus 0 \in M_{n_1} \oplus \left(\bigoplus_{j>1} M_{n_j}\right)$ correspond to elements in $R_{0,F}$ that do not commute with each other. So $R_{0,F}$ is non-commutative. □

We can, however, determine when $R_{0,\mathbb{C}}$ (and therefore $R_{0,\mathbb{Z}}$) is commutative.

Lemma 1.3.5. *Let $R_{\mathbb{C}} = \mathbb{C}[G]$ where G is a finite non-commutative group and let $Y \in G$. If $\sigma(Y)$ has distinct eigenvalues for all irreducible representations σ of G over $\mathbb{C}$ then $R_{0,\mathbb{C}} = \{\alpha \in R_{\mathbb{C}} \mid Y\alpha = \alpha Y\}$ is commutative.*

Proof. If σ is an irreducible representation of G then, since Y has finite order, there is a basis for which $\sigma(Y)$ is diagonal and $\sigma(Y)$ has distinct eigenvalues. This implies that all matrices that commute with $\rho(Y)$ are also diagonal in the same basis. So $\sigma(R_{0,\mathbb{C}})$ consists of diagonal matrices in this basis, and those commute with each other. If this is true for all representations of G then it is true for the regular representation, which is faithful. Therefore $R_{0,\mathbb{C}}$ is commutative. □

Lemma 1.3.6. *Let H be a subgroup of G. Then each irreducible representation W of H maps injectively into some irreducible representation V of G.*

Proof. We know that the irreducible representations of H are contained in the irreducible representations of G since irreducible representations are contained in the complex group ring and $\mathbb{C}[H] \subset \mathbb{C}[G]$. This gives that each irreducible

representation of H maps into each irreducible representation of G by either the zero map or an injective map. Since not all of these maps can be zero for a particular irreducible representation W of H, there exists an irreducible representation V of G that W maps into injectively. □

Theorem 1.3.7. *Let G be a non-abelian group of order $2N$ where N is odd. Let $Y \in G$ have order 2 and suppose $R_{0,\mathbb{Z}} = \{\alpha \in R_{\mathbb{Z}} \mid Y\alpha = \alpha Y\}$ is a commutative subring of $R_{\mathbb{Z}} = \mathbb{Z}[G]$. Then $G = (B \rtimes \langle Y \rangle) \oplus A$, where A and B are abelian and Y acts on A as the identity and on B by inversion.*

Proof. Since Y is order two we know the only eigenvalues of $\sigma(Y)$ are 1 and -1 for all representations σ of G over $\mathbb{C}$. Therefore $dim(\sigma(R_{\mathbb{C}})) \leq 2$ for all representations σ of G since $R_{0,\mathbb{C}}$ is commutative which implies the irreducible representations cannot have repeated eigenvalues (by Lemma 1.3.4). Since G has order $2N$ where N is odd there exists $H \lhd G$ of index 2 with $|H| = N$ [2, p 124]. By Lemma 1.3.6 we know the irreducible representations of H are contained in the irreducible representations of G and therefore H has only one dimensional representations (the dimension of a representation must divide the order of the group [15, p 52]) and therefore is abelian. Since H is abelian we get that $G = H \rtimes \langle Y \rangle$. Now Y splits H into $H_- \oplus H_+$ where Y acts by inversion on the elements of H_- and trivially on the elements of H_+. We can see this by noting that $1 = \frac{1-Y}{2} + \frac{1+Y}{2}$ (2 is invertible since N is odd). So each element can be written as $\alpha = \frac{1-Y}{2}\,\alpha + \frac{1+Y}{2}\,\alpha$ and Y acts on $\frac{1-Y}{2}\,\alpha$ by inversion and trivially on $\frac{1+Y}{2}\,\alpha$. So $G = H_+ \times (H_- \rtimes \langle Y \rangle)$ and both H_- and H_+ are abelian since H is abelian. □

Theorem 1.3.8. *Consider the group $H_- \rtimes \langle Y \rangle$ where H_- has odd order k and is abelian, and where Y (order two) acts on the elements of H_- by inversion. Then*

$H_- \rtimes \langle Y \rangle = D_k$ (the dihedral group of order $2k$) if and only if $H_- \rtimes \langle Y \rangle$ can be generated by two elements.

Proof. Clearly D_k can be generated by two elements, so we want to show if $H_- \rtimes \langle Y \rangle$ can be generated by two elements that it is D_k. Since $H_- \rtimes \langle Y \rangle$ is the union of elements of H_- and elements of order two there are three cases to consider. Note that elements of order two have the form YA for $A \in H_-$.

Case 1: Both generators are in H_-. This causes a contradiction since they never generate $Y \notin H_-$.

Case 2: One generator $A \in H_-$ and the other generator B has order 2. Now since B has order two then $B = YC$ for some $C \in H_-$. So $BAB^{-1} = YCAC^{-1}Y = YAY = A^{-1}$ since C and A are in H_- and therefore commute with each other and Y acts by inversion on all elements of H_-. So this is D_k for k equal to the order of A.

Case 3: Both generators have order 2. Then they have the form YC and YD where $C, D \in H_-$. So consider $A = YCYD = C^{-1}D \in H_-$ and $B = YC$. Clearly A, B still generate the same group and give us Case 2.

So in all cases we conclude that $H_- \rtimes \langle Y \rangle$ is D_k for some odd k (since H has odd order). □

Putting together Theorem 1.3.7 and Theorem 1.3.8 we get the following:

Corollary 1.3.9. *Assume that G is a non-abelian group of order $2N$ where N is odd. Also assume that there exists an element Y of order two in G such that $G = H_+ \times (H_- \rtimes \langle Y \rangle)$ where $H = H_- \oplus H_+$ has order N, both H_- and H_+ are abelian, and Y acts by inversion on H_-. Then $H_- \rtimes \langle Y \rangle = D_k$ (the dihedral group of order $2k$) if and only if $H_- \rtimes \langle Y \rangle$ can be generated by two elements.*

We have now described all situations in which the group is generated by X and Y with Y order two so that $R_0 = \{\alpha \in R \mid Y\alpha = \alpha Y\}$ can be defined and is a commutative subring. So now we can set up the cryptosystem identically to the original system (except that we carry around A in the coefficients, which does not affect the system's implementation). We are also able to define $R_1 = \{\alpha \in R \mid Y\alpha = -\alpha Y\}$ which allows us to use Coppersmith's attack to break this slight generalization of the original system. In the next chapter we will extend the system and attack to a much larger set of group rings.

1.4 Commutative NTRU

The commutative system is also a public key cryptosystem and is based on a polynomial ring, $R = \mathbb{Z}[x]/(x^N - 1)$, where N is an odd prime and $(N-1)/2$ also an odd prime. NTRU was first presented by J. Hoffstein, J. Piper and J. H. Silverman in 1996 [8]. Since then there has been a variety of research published on the system and two different signature schemes (the first of which, NSS [5, 9], is insecure) have been developed. The second signature scheme (NTRUSign [7]) and the cryptosystem itself were discovered to be based on a $2N \times 2N$ lattice that can be used to obtain a submodule of $R \oplus R$. NTRU is currently owned by NTRU Cryptosystems, Inc. based in Burlington, MA. Their website, www.ntru.com, includes many articles and notes on the system, as well as challenges to break implementations of the system. They also describe their current beliefs on how secure this system is and compare it to other cryptosystems, such as RSA. In general all polynomials have coefficients of $1, 0, -1$ (it is necessary for them to be fairly small or the system won't work) but with varying numbers of non-zero coefficients. Example values of a current system are: $N = 503$, $q = 256$, $p = 3$.

We again assume Alice wants to send a message to Bob. Bob chooses a private key $f \in R$ that is invertible modulo both p and q (which are relatively prime positive integers) and another polynomial $g \in R$. Bob computes f_q^{-1} and f_p^{-1}, the inverses of f modulo q and p respectively. Next he computes $h \equiv f_q^{-1} g \pmod{q}$. This h is Bob's public key (so far everything but f and g are public). Assume now that Alice wants to send a message, $m \in R$ with coefficients small modulo p, to Bob. Alice then chooses a random $\phi \in R$ and computes $e \equiv p\phi * h + m \pmod{q}$. She sends e, the encrypted message, to Bob. After Bob receives e he computes

$$\begin{aligned} a \equiv & f * e \\ \equiv & f * (p\phi * h + m) \\ \equiv & f * (p\phi * (f_q^{-1} g) + m \\ \equiv & p\phi * g + f * m \pmod{q} \end{aligned}$$

He next regards a as a polynomial with integer coefficients and reduces it modulo p to get $f * m$. Then he computes

$$f_p^{-1} * (a \pmod{p}) \equiv m \pmod{p}$$

to get m. This reduces to m since f and m have small coefficients.

So, as we can see, non-commutative NTRU is similar to commutative NTRU. They both work with a group ring and work modulo q and p. They both rely heavily on 'smallness' of the coefficients. But it is also clear that non-commutative NTRU does not reduce to NTRU if we use the group ring of a commutative group. In commutative NTRU all of the polynomials have small coefficients, but in non-commutative NTRU f, F, ψ and m have 'large' coefficients. In particular it is interesting that the message must be small in commutative NTRU, but not in

non-commutative NTRU. It is also not necessary to have f_p^{-1} in non-commutative NTRU. The public keys are slightly different - in commutative NTRU we only have one multiplication, but in non-commutative NTRU there are two.

Chapter 2

Extensions of Non-commutative NTRU

2.1 Introduction and Extension to Other Group Rings

We now consider not only $\mathbb{Z}[D_N]$ but $R_{\mathbb{Z}} = \mathbb{Z}[G]$ where G is a finite group with two generators, X and Y, that do not commute with each other. Let the order of X be N and the order of Y be k, with N and k distinct primes, so that the order of G is $N \cdot k$. Unless it is otherwise stated we will assume that G is the group defined by the presentation

$$G = \langle X, Y \mid YXY^{-1} = X^u, X^N = 1, Y^k = 1 \rangle$$

where u has order k modulo N. Note that $\langle X \rangle \triangleleft G$ by definition and that $N - 1$ must be a multiple of k (since Y needs to act non-trivially on X). We also need the assumption that q is prime (larger than Nk, since otherwise the system will break down, as will the attack) and that p, r, s, and t are relatively prime to Nk. We will denote $R_{\mathbb{Z}}$ modulo q as R_q and $R_{0,\mathbb{Z}}$ modulo q as $R_{0,q}$. The cryptosystem is set up in exactly the same way as in Section 1.2 and $R_{0,\mathbb{Z}}$ is still the commutative subring of $R_{\mathbb{Z}}$ consisting of the elements that commute with Y.

We define the same subsets of $R_{0,\mathbb{Z}}$ and $R_{\mathbb{Z}}$,

$$S_f = R_{0,\mathbb{Z}}\{q\}$$

$$S_m = R_{\mathbb{Z}}\{q\}$$

$$S_\phi = R_{0,\mathbb{Z}}\{r\}$$

$$S_\psi = R_{0,\mathbb{Z}}\{s\}$$

$$S_\omega = R_{\mathbb{Z}}\{t\}.$$

Bob chooses $f \in S_f$, $\omega \in S_\omega$ and computes $F \in S_f$ such that $f * F \equiv 1 \pmod{q}$. Bob's public key is then $h = pF * \omega * f \pmod{q}$ and the private keys are f and F. Alice encrypts her message $m \in S_m$ by randomly choosing $\phi, \phi' \in S_\phi$ and $\psi \in S_\psi$. Then she computes $\Psi \in R_{0,\mathbb{Z}}\{p\}$ such that $\Psi \equiv \psi \pmod{p}$ and the pair (e, E) with

$$e \equiv \phi * h * \phi' + \psi \pmod{q}$$

$$E \equiv \Psi * h + m \pmod{q}.$$

She sends the pair (E, e) to Bob. To decrypt the message Bob computes

$$a \equiv f * e * F \equiv p\phi * \omega * \phi' + \psi \pmod{q}$$

and then reduces this modulo p to recover $\Psi \equiv \psi \pmod{p}$. Now Bob can subtract $\Psi * h \pmod{q}$ from E to obtain m.

We will give an example to help clarify the above description, but first it will be helpful to have a better understanding of what $R_{0,\mathbb{Z}}$ (or $R_{0,q}$) looks like.

Let v be a multiplicative generator of $(Z/NZ)^*$ and $m = \frac{N-1}{k} - 1$. Recall that u is an element of order k modulo N such that $YX = X^u Y$,

Definition 2.1.1. *Define* $W_i = X^{v^i} + X^{v^i u} + X^{v^i u^2} + \cdots + X^{v^i u^{k-1}} \in F[G]$ *for* $0 \leq i \leq m$, *for any ring* F.

Note that each W_i is the sum of a "Y-orbit". It is fixed under conjugation by Y and therefore the W_i are elements of $R_{0,F} = \{\alpha \in R_F \mid Y\alpha = \alpha Y\}$.

Lemma 2.1.2. *The elements of the subring* $R_{0,F} = \{\alpha \in R_F \mid Y\alpha = \alpha Y\}$ *have the following form:*

$$\alpha = P(Y) + W_0P_0(Y) + W_1P_1(Y) + \cdots + W_mP_m(Y)$$

where $P, P_0, P_1, \ldots, P_m$ *are polynomials in* Y *with coefficients in* F.

Proof. This is simply a restatement of Lemma 1.3.2. □

There is an example of this in Section 2.7.

2.2 Preliminary Representation Theory

In subsection 1.3.1 we stated that $F[G]$, where F is a field with $char(F) \nmid |G|$, is isomorphic to a direct sum of matrix rings over division rings [13, p 142]. We may use representation theory to directly see what these rings are in the $\mathbb{C}[G]$ case. Let $\zeta \in \mathbb{C}$ be a primitive N^{th} root of unity and $z_k \in \mathbb{C}$ be a primitive k^{th} root of unity. Recall that $m = \frac{N-1}{k} - 1$, v is a multiplicative generator of $(\mathbb{Z}/N\mathbb{Z})^*$, and that u is defined such that $YX = X^uY$. All representations in this section are over $\mathbb{C}$ unless otherwise stated.

Lemma 2.2.1. *Define the map* $\tau : G \to \mathbb{C}^*$ *by* $\tau(X) = 1$, $\tau(Y) = z_k$, *and* τ *is multiplicative. Then* $1, \tau, \tau^2, \tau^3, \ldots, \tau^{k-1}$ *are one-dimensional irreducible representations of* G.

Proof. This is trivial since the powers of τ are lifts of the irreducible representations of $G/\langle X \rangle$. □

Lemma 2.2.2. *The representations* $\{\rho_0, \rho_1, \rho_2, \ldots, \rho_m\}$ *defined by the following:*

$$\rho_i(X) = \begin{pmatrix} \zeta^{v^i} & & & & & \\ & \zeta^{v^i u} & & & & \\ & & \zeta^{v^i u^2} & & & \\ & & & \ddots & & \\ & & & & \zeta^{v^i u^{k-1}} \end{pmatrix}$$

and

$$\rho_i(Y) = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}.$$

are irreducible representations of G *over* $\mathbb{C}$ *of dimension greater than one.*

Proof. We need to show that each ρ_i preserves the group action. We know

$$\rho_i(YX) = \rho_i(Y)\rho_i(X) = \begin{pmatrix} 0 & \zeta^{v^i u} & 0 & 0 & \cdots & 0 \\ 0 & 0 & \zeta^{v^i u^2} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \zeta^{v^i u^{k-2}} & 0 \\ 0 & 0 & \cdots & 0 & 0 & \zeta^{v^i u^{k-1}} \\ \zeta^{v^i} & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}$$

So, now we need to show that this is equal to $\rho_i(X^uY)$, but this is clear since

$$\rho_i(X^u) = \begin{pmatrix} \zeta^{v^i u} & & & & \\ & \zeta^{v^i u^2} & & & \\ & & \zeta^{v^i u^3} & & \\ & & & \ddots & \\ & & & & \zeta^{v^i u^k} \end{pmatrix}$$

and multiplication by $\rho_i(Y)$ on the right clearly gives the previous matrix, since $u^k = 1$. Next we want to show that the only fixed subspaces of ρ_i are $\mathbb{C}^k$ and $\{0\}$. First consider the fact that $\rho_i(X)$ is diagonal with distinct entries, so only diagonal matrices commute with it. Now, $\rho_i(Y)$ is an order k permutation, so the only diagonal matrices that it commutes with are scalar. Therefore the only matrices that commute with all $\rho(g)$ are scalar. Suppose that $W \subset \mathbb{C}^k$ is fixed by ρ and that W' is a G-stable complement of W. Let P be the projection map from $\mathbb{C}^k = W \oplus W'$ onto W. Then P commutes with ρ since for any $g \in G$, $w \in W$ and $w' \in W'$ we know

$$\begin{aligned} P\rho(g)(w + w') &= P(\rho(g)w + \rho(g)w') \\ &= P(\rho(g)w) \\ &= \rho(g)w \\ &= \rho(g)P(w + w') \end{aligned}$$

Therefore P is scalar, so W is either $\mathbb{C}^k$ or $\{0\}$.

□

Theorem 2.2.3. *The following is a complete list of the irreducible representations of G:* $\{1, \tau, \tau^2, \tau^3, \ldots, \tau^{k-1}, \rho_0, \rho_1, \rho_2, \ldots, \rho_m\}$

Proof. All of the listed representations are distinct since $\rho_i(X)$ and $\rho_j(X)$ have distinct eigenvalues for distinct i and j and $\tau^i(Y)$ and $\tau^j(Y)$ have distinct eigenvalues for distinct i and j. There are k one-dimensional representations and $m+1$ representations of dimension k, so the sum of the squares of the dimensions of the representations is

$$k \cdot 1^2 + (m+1) \cdot k^2 = k + (\frac{N-1}{k})k^2 = k + Nk - k = Nk$$

which is the order of G. Therefore there are no other irreducible representations.

□

So we have the representations of G and therefore we know that $\mathbb{C}[G] \simeq \mathbb{C}^k \oplus M_k(\mathbb{C})^{(m+1)}$. Now we can define the following representation of G over $\mathbb{C}$.

Definition 2.2.4. *Let $\bar{\rho} : G \to M_{(m+1)k}(\mathbb{C})$ be the representation defined by:*

$$\bar{\rho}(X) = \begin{pmatrix} \rho_0(X) & & & \\ & \rho_1(X) & & \\ & & \ddots & \\ & & & \rho_m(X) \end{pmatrix}$$

and

$$\bar{\rho}(Y) = \begin{pmatrix} \rho_0(Y) & & & \\ & \rho_1(Y) & & \\ & & \ddots & \\ & & & \rho_m(Y) \end{pmatrix}$$

Next, we perform a change of basis on $\bar{\rho}$ to get the following representation ρ from G (over $\mathbb{Z}_q$) into the matrix ring $M = M_{(m+1)k}(\mathbb{Z}_q)$. Also, we give a

conjecture of the form of $\rho(Y)$ that would give ρ as mapping into $\mathbb{Z}$ rather than $\mathbb{Z}_q$.

Theorem 2.2.5. *Consider the matrix*

$$T = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1+\zeta^{-1} & 1+\zeta^{-u} & \dots & 1+\zeta^{-v^m u^{k-1}} \\ 1+\zeta^{-1}+\zeta^{-2} & 1+\zeta^{-u}+\zeta^{-2u} & \dots & 1+\zeta^{-}+\zeta^{-2\cdot v^m u^{k-1}} \\ \vdots & \vdots & \ddots & \vdots \\ 1+\dots+\zeta^{-(N-2)} & 1+\dots+\zeta^{-2\cdot(N-2)} & \dots & 1+\dots+\zeta^{-(N-2)\cdot v^m u^{k-1}} \end{pmatrix}$$

$\in M_{mk}(\mathbb{C})$ *(the order of the columns follows the order of* $\rho_0, \rho_1, \dots, \rho_m$*).* T *is a change of basis matrix that gives*

$$T\bar{\rho}(X)T^{-1} = \rho(X) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -1 \\ 1 & 0 & 0 & \cdots & 0 & -1 \\ 0 & 1 & 0 & \cdots & 0 & -1 \\ 0 & 0 & 1 & \cdots & 0 & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -1 \end{pmatrix}.$$

Define ρ *by* $\rho(\alpha) = T\bar{\rho}(\alpha)T^{-1}$ *for all* $\alpha \in G$*. Then* $\rho : G \to M_{(m+1)k}(\mathbb{Q})$ *is a representation. Also the only denominators that appear in* $\rho(g)$ *for any* $g \in G$ *are powers of* N*.*

Proof. T's columns are the eigenvectors of X and therefore it is the change of basis matrix that takes the diagonal form of X to its rational canonical form. T

can be transformed by row operations into the following:

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \zeta^{-1} & \zeta^{-u} & \dots & \zeta^{-v^m u^{k-1}} \\ \zeta^{-2} & \zeta^{-2u} & \dots & \zeta^{-2\cdot v^m u^{k-1}} \\ \zeta^{-3} & \zeta^{-3u} & \dots & \zeta^{-3\cdot v^m u^{k-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta^{-(N-2)} & \zeta^{-(N-2)\cdot u} & \dots & \zeta^{-(N-2)\cdot v^m u^{k-1}} \end{pmatrix}$$

which is a Vandermonde matrix and therefore its determinant is a product of $(\zeta^a - \zeta^b)$ for various a and b. Now each $(\zeta^a - \zeta^b)$ divides N, so the only denominators that can arise from the change of basis divide a power of N. Therefore the entries of $N^\ell T^{-1}$ are algebraic integers for some ℓ, so $N^\ell \rho(Y) = T\bar{\rho}(Y)N^\ell T^{-1}$ also has entries that are algebraic integers. We need to show that the entries are rational. To do this we show that $\rho(Y)$ is fixed by the Galois group of $\mathbb{Q}[\zeta]$. Let $\sigma \in Gal(\mathbb{Q}[\zeta]/\mathbb{Q})$. Then there exists $Q_\sigma \in M_{(m+1)k}(\mathbb{C})$ such that $\sigma(T) = TQ_\sigma$ and Q_σ is a permutation matrix that permutes the columns of $\bar{\rho}$. So

$$\begin{aligned} \sigma(\rho(Y)) &= \sigma(T\bar{\rho}(Y)T^{-1}) \\ &= \sigma(T)\sigma(\bar{\rho}(Y))\sigma(T^{-1}) \\ &= TQ_\sigma\sigma(\bar{\rho}(Y))Q_\sigma^{-1}T^{-1}. \end{aligned}$$

Now $\bar{\rho}(Y)$ is rational and therefore is fixed by all elements of $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$. Note $\bar{\rho}(Y) = Q_{\sigma_u}$ and since $Gal(Q_\zeta/Q)$ is abelian, Q_σ and Q_{σ_u} commute. Therefore we get

$$TQ_\sigma\sigma(\bar{\rho}(Y))Q_\sigma^{-1}T^{-1} = T\bar{\rho}(Y)T^{-1} = \rho(Y).$$

So we know that $\rho(Y)$ has rational entries, with the only possible denominators integer powers of N. □

Corollary 2.2.6. *The representation ρ given above can be reduced modulo q to a representation from G to $M_{(m+1)k}(\mathbb{Z}_q)$*

Proof. We have shown that the only denominators that arise are primes lying over N, therefore we can simply reduce each entry modulo q to get a representation into $M_{(m+1)k}(\mathbb{Z}_q)$. □

Through computing many examples we believe that $\rho(Y)$ actually lies in $M_{(m+1)k}(\mathbb{Z})$. It seems to have a nice pattern of zeros, ones, and negative ones. The following matrices are examples of $\rho(Y)$ that support the conjecture below:

This is for $N = 19$, $k = 3$, and $u = 7$:

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & -1 & 1 & 0 & 0 & 0 \\
1 & 0 & -1 & 1 & 0 & -1 & 1 & 0 & 0 & 0 & -1 & 1 & 0 & -1 & 1 & 0 & 0 & 0 \\
1 & 0 & -1 & 1 & 0 & -1 & 1 & 0 & 0 & 0 & -1 & 1 & 0 & -1 & 1 & 0 & -1 & 1 \\
1 & 0 & -1 & 1 & 0 & -1 & 1 & 0 & -1 & 1 & -1 & 1 & 0 & -1 & 1 & 0 & -1 & 1 \\
0 & 1 & -1 & 1 & 0 & -1 & 1 & 0 & -1 & 1 & -1 & 1 & 0 & -1 & 1 & 0 & -1 & 1 \\
0 & 1 & -1 & 1 & 0 & -1 & 1 & 0 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & 0 & -1 & 1 \\
0 & 1 & -1 & 0 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & 0 & -1 & 1 \\
0 & 1 & -1 & 0 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 & 1 \\
0 & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 & 1 \\
0 & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 & 0 \\
0 & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 & 0 & 0 & 0 & 1 & -1 & 0 & 1 & -1 & 0 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & 1 & -1 & 0 & 0 & 0 & 1 & -1 & 0 & 1 & -1 & 0 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

This is for $N = 19$, $k = 3$, and $u = 11$:

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\
1 & -1 & 1 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\
1 & -1 & 1 & 0 & 0 & 0 & -1 & 1 & -1 & 1 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\
1 & -1 & 1 & 0 & 0 & 0 & -1 & 1 & -1 & 1 & 0 & 0 & 0 & -1 & 1 & -1 & 1 & 0 \\
1 & -1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & 1 & 0 & 0 & 0 & -1 & 1 & -1 & 1 & 0 \\
1 & -1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & 1 & 0 \\
1 & -1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & 1 & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & 1 & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & -1 \\
0 & 0 & 1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & -1 \\
0 & 0 & 1 & -1 & 1 & -1 & 0 & 0 & 0 & 1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & -1 \\
0 & 0 & 1 & -1 & 1 & -1 & 0 & 0 & 0 & 1 & -1 & 1 & -1 & 0 & 0 & 0 & 1 & -1 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 1 & -1 & 1 & -1 & 0 & 0 & 0 & 1 & -1 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 1 & -1 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

This is for $N = 11$, $k = 5$, and $u = 4$:

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & -1 & 1 & 0 & -1 & 1 & 0 & 0 & 0 \\
1 & 0 & -1 & 1 & 0 & -1 & 1 & 0 & -1 & 1 \\
0 & 1 & -1 & 1 & 0 & -1 & 1 & 0 & -1 & 1 \\
0 & 1 & -1 & 0 & 1 & -1 & 1 & 0 & -1 & 1 \\
0 & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 & 1 \\
0 & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 & 0 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & 1 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0
\end{pmatrix}.$$

This is for $N = 11$, $k = 5$, and $u = 5$:

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & -1 & 1 \\
1 & 0 & 0 & 0 & -1 & 1 & -1 & 1 & -1 & 1 \\
1 & 0 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
0 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
0 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 0 \\
0 & 1 & -1 & 1 & -1 & 1 & -1 & 0 & 0 & 0 \\
0 & 1 & -1 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

Conjecture 2.2.7. *Let $N - 1 = u \cdot a + b$ and define $e_{A..B}$ to be the column with ones in positions A through B and zeros elsewhere, and $-e_{A..B}$ to be the column with negative ones in positions A through B and zeros elsewhere. Now define the following matrix:*

$$B_1 = \begin{pmatrix} e_{1..u} & e_{u+1..2u} & \cdots & e_{(a-1)\cdot u+1..a\cdot u} & -e_{2..a\cdot u} \end{pmatrix}$$

and let B_2 be B_1 shifted down by one with the new top row all zeros, B_3 be B_2 shifted down by one with the new top row all zeros, etc. So each B_ℓ has $a + 1$ columns. Let $N - 1 = (a + 1) \cdot c + d$, then $\rho(Y)$ has the following form:

$$\begin{pmatrix} B_1 & B_2 & \cdots & B_c & B_{c+1} \end{pmatrix}$$

with B_{c+1} truncated at the dth column.

2.3 Extension of Coppersmith's Attack

For the attack we need to do more work than in the D_N case, but just like in the D_N case we only need knowledge of the system setup (i.e. N, R, R_0, q, p, r, s, t) and the public information (i.e. h) to break the system. Let S be the ring of integers for a number field such that S contains ζ (a primitive N^{th} root of unity) and z_k, a primitive k^{th} root of unity. Let $\mathcal{Q}$ be a prime ideal in S such that $\mathcal{Q} \cap \mathbb{Z} = q\mathbb{Z}$. We need to move to an extension of $\mathbb{Z}$ since we do not always know that a primitive k^{th} root of unity modulo q exists. Let $R_S = S[G]$. Let $R_{0,S}$ be the elements that commute with Y, $R_{\mathcal{Q}} = R_S \pmod{\mathcal{Q}}$, and $R_{0,\mathcal{Q}} = R_{0,S} \pmod{\mathcal{Q}}$.

To start we consider the following subsets of $R_{\mathcal{Q}}$:

$$\begin{aligned} R_1 &= \{\alpha \in R_{\mathcal{Q}} \mid Y\alpha = z_k \alpha Y\} \\ R_2 &= \{\alpha \in R_{\mathcal{Q}} \mid Y\alpha = z_k^2 \alpha Y\} \\ \vdots &= \quad \vdots \\ R_{k-1} &= \{\alpha \in R_{\mathcal{Q}} \mid Y\alpha = z_k^{k-1} \alpha Y\}. \end{aligned}$$

Note that since we only define these R_j's modulo $\mathcal{Q}$ we won't worry about adding the subscript $\mathcal{Q}$. One of the key results of this section is Theorem 2.3.10. It proves that each of these R_i are principal $R_{0,\mathcal{Q}}$ modules. The following lemma shows that each R_j has a structure similar to $R_{0,\mathcal{Q}}$.

Definition 2.3.1. *Define* $W_{i,j} = X^{v^i} + z_k^{-j} X^{v^i u} + z_k^{-2j} X^{v^i u^2} + \cdots + z_k^{-(k-1)j} X^{v^i u^{k-1}}$ *for* $0 \le j \le k-1$ *and for* $0 \le i \le m$. *(For* $j = 0$ *we get the* W_i *as defined for* $R_{0,\mathcal{Q}}$*.)*

Lemma 2.3.2. *The elements of the subset* R_j *as defined above have the following form for* $1 \le j \le k-1$*:*

$$P(Y) + W_{0,j}P_0(Y) + W_{1,j}P_1(Y) + \cdots + W_{m,j}P_m(Y)$$

Proof. Follows just as in the proof of Lemma 1.3.2. □

Note that only $R_{0,\mathcal{Q}}$ is actually a subring. The other R_j are closed under addition but not multiplication and in fact are $R_{0,\mathcal{Q}}$ modules.

Lemma 2.3.3. *Let $\alpha \in R_i$ and $\beta \in R_j$ for some $i, j \in \{1, 2, \ldots, k-1\}$. Then $\alpha\beta \in R_{i+j}$.*

Proof. Conjugation of $\alpha\beta$ by Y gives the following:

$$\begin{aligned} Y(\alpha\beta)Y^{-1} &= (Y\alpha Y^{-1})(Y\beta Y^{-1}) \\ &= z_k^i \alpha z_k^j \beta \\ &= z_k^{i+j}\alpha\beta. \end{aligned}$$

Therefore $\alpha\beta \in R_{i+j}$. □

Definition 2.3.4. *Define σ as the action of conjugation by Y on $R_{\mathcal{Q}}$. Define $\pi_j \in End(R_{\mathcal{Q}})$ by $\pi_j = (I + z_k^{-j}\sigma + z_k^{-2j}\sigma^2 + \cdots + z_k^{-(k-1)j}\sigma^{k-1})$ for $0 \leq j \leq k-1$, where I represents the identity action on $R_{\mathcal{Q}}$.*

Lemma 2.3.5. *We have the following:*

$$\begin{aligned} R_j &= \{\alpha \in R_{\mathcal{Q}} \mid \sigma(\alpha) = z_k^j \alpha\} \\ &= \{\alpha \in R_{\mathcal{Q}} \mid \alpha = \sum_{\ell=0}^{k-1} \left[\sum_{i=0}^{m} a_{i,\ell}\pi_j(X^{v^i})\right] Y^\ell\} \end{aligned}$$

for $0 \leq j \leq k-1$ (where $R_0 = R_{0,\mathcal{Q}}$).

Proof. Given the definition of the π_j, Lemma 2.1.2, and Lemma 2.3.2, the result is clear. □

Theorem 2.3.6. *The group ring $R_{\mathcal{Q}}$ breaks into the sum $R_{0,\mathcal{Q}} + R_1 + \cdots R_{k-1}$ and each element of R can be written uniquely as a sum of this form.*

Proof. Let $\pi = \pi_0 + \pi_1 + \cdots + \pi_{k-1}$. Then $\pi \equiv k \cdot I \pmod{\mathcal{Q}}$ since $1 + z_k + z_k^2 + \cdots + z_k^{k-1} \equiv 0 \pmod{\mathcal{Q}}$. Now by Lemma 1.3.2 we know that $\pi_0(\alpha) \in R_{0,\mathcal{Q}}$ and similarly for any $\alpha \in R_{\mathcal{Q}}$, $\pi_j(\alpha) \in R_j$ for all j. Then $k\alpha \equiv \pi(\alpha) \equiv \pi_0(\alpha) + \pi_1(\alpha) + \cdots + \pi_{k-1}(\alpha) \pmod{\mathcal{Q}}$, which gives us $k\alpha$ as an element of the sum. Then dividing by k modulo $\mathcal{Q}$ gives the desired result. Suppose that $r \in R$ can be written as $r_0 + r_1 + \cdots + r_{k-1}$ and as $r'_0 + r'_1 + \cdots + r'_{k-1}$. Then the difference of these two sums is zero. Therefore $\sum_{j=0}^{k-1} z_k^{aj} Y^j (r_0 + r_1 + \cdots + r_{k-1} - r'_0 - r'_1 - \cdots - r'_{k-1}) Y^{-j} = 0$. But this sum is equal to $k(r_a - r'_a)$, so $r_a - r'_a = 0$. This is true for any choice of a and therefore each element of R can uniquely be written as a sum in $R_{0,\mathcal{Q}} + R_1 + \cdots R_{k-1}$. □

Lemma 2.3.7. *Let $\mathbb{F}$ be a field. Let $M \in M_\ell(\mathbb{F})$ be a matrix, let $f(t) \in \mathbb{F}(t)$, and suppose the number of elements of $\mathbb{F}$ is greater than ℓ. If every $\mathbb{F}$-linear combination of $f(M), f(M^2), \ldots, f(M^{k-1})$ is not invertible in $\mathbb{F}$, then they have a common non-zero null space element of $\mathbb{F}^{k-1}$.*

Proof. For all choices of $a_1, a_2, \ldots, a_{k-1} \in \mathbb{F}$:

$$det\left(a_1 f(M) + a_2 f(M^2) + \cdots + a_{k-1} f(M^{k-1})\right) = g(a_1, a_2, \ldots, a_{k-1}) = 0.$$

Note g is a polynomial of degree less than or equal to ℓ in every variable and it is the zero function on $\mathbb{F}^{k-1}$. We want to show that g is the zero polynomial. Suppose that a_1 through a_{k-2} are chosen, then g reduces to a polynomial in a_{k-1} that is the zero function on $\mathbb{F}$ with degree less than ℓ. Therefore it is the zero polynomial on $\mathbb{F}$. This implies that the coefficients are zero polynomials in $a_1, a_2, \ldots, a_{k-2}$. Now by induction on k we get that $g(t_1, t_2, \ldots, t_{k-1})$ is the zero

polynomial in $\mathbb{F}[t_1, t_2, \ldots, t_{k-1}]$. Now we know there exists a matrix A over $\bar{\mathbb{F}}$ such that

$$AMA^{-1} = \begin{pmatrix} \lambda_1 & * & * & \cdots & * \\ 0 & \lambda_2 & * & \cdots & * \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \lambda_{\ell-1} & * \\ 0 & 0 & \cdots & 0 & \lambda_\ell \end{pmatrix}.$$

is the Jordan form of M, Therefore

$$A\left(\sum_{i=1}^{k-1} t_i f(M^i)\right)A^{-1} = \begin{pmatrix} \sum_{i=1}^{k-1} t_i f(\lambda_1^i) & * & * & \cdots & * \\ 0 & \sum_{i=1}^{k-1} t_i f(\lambda_2^i) & * & \cdots & * \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \sum_{i=1}^{k-1} t_i f(\lambda_{\ell-1}^i) & * \\ 0 & 0 & \cdots & 0 & \sum_{i=1}^{k-1} t_i f(\lambda_\ell^i) \end{pmatrix}$$

This gives us that $g(t_1, t_2, \ldots, t_{k-1}) = 0 = \prod_{j=1}^{\ell}\left(\sum_{i=1}^{k-1} t_i f(\lambda_j^i)\right)$, so $\sum_{i=1}^{k-1} t_i f(\lambda_{j_0}^i) = 0$ for some j_0 which corresponds to a true eigenvector of M. Therefore $f(\lambda_{j_0}^i) = 0$ for all i. Let e_{j_0} be the j_0^{th} basis vector in $\bar{\mathbb{F}}^\ell$, then $Af(M^i)A^{-1}e_{j_0} = 0$ for all i and so $f(M^i)A^{-1}e_{j_0} = 0$ for all i since A is invertible. Hence $A^{-1}e_{j_0} \in \widetilde{\mathbb{F}}^{k-1}$ is a common null space vector for $\{f(M), f(M^2), \ldots f(M^{k-1})\}$, where $\widetilde{\mathbb{F}}$ is an extension of $\mathbb{F}$ of dimension r for some $r \in \mathbb{Z}$. Let $\widetilde{\mathbb{F}} = \mathbb{F}\beta_1 + \mathbb{F}\beta_2 + \cdots + \mathbb{F}\beta_r$, then $A^{-1}e_{j_0} = v_1\beta_1 + v_2\beta_2 + \cdots + v_r\beta_r$ for some $v_i \in \mathbb{F}^m$. This gives us that $f(M^i)v_1\beta_1 + f(M^i)v_2\beta_2 + \cdots + f(M^i)v_r\beta_r = 0$ for all i, which implies that $f(M^i)v_1 = 0$ for all i since the β_i are linearly independent. Therefore v_1 is a common null space element in $\mathbb{F}^\ell$.

□

Lemma 2.3.8. *For any invertible matrix M, the inverse of M is a polynomial in M.*

Proof. Let $P(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ be the minimal polynomial of M. Then $P(M) = 0$ and $a_0 \neq 0$ since zero is not an eigenvalue. So $M(\frac{-a_n}{a_0}M^{n-1} + \frac{-a_{n-1}}{a_0}M^{n-2} + \cdots + \frac{-a_1}{a_0}) = I$ and therefore $\frac{-a_n}{a_0}M^{n-1} + \frac{-a_{n-1}}{a_0}M^{n-2} + \cdots + \frac{-a_1}{a_0}$ is the inverse of M. □

Definition 2.3.9. *Define the polynomial*

$$f_j(t) = t + z_k^{-j}t^u + z_k^{-2j}t^{u^2} + \cdots + z_k^{-(k-1)j}t^{u^{k-1}}$$

for $1 \leq j \leq k-1$.

Note that $f_j(X^\ell) \in R_j$ for all $\ell \geq 0$ and for $1 \leq j \leq k-1$.

The following is the key result that allows us to extend Coppersmith's attack to these group rings.

Theorem 2.3.10. *For $1 \leq j \leq k-1$, the subset R_j of $R_{\mathcal{Q}}$ is equal to $\Gamma_j R_{0,\mathcal{Q}}$ and $R_{0,\mathcal{Q}}\Gamma_j$ for some $\Gamma_j \in R_j$.*

Proof. Fix j. Suppose for all $a_i \in S$ the sum $\sum_{i=1}^{k-1} a_i f_j(\rho(X)^i)$ is not invertible modulo $\mathcal{Q}$. Then we know $f_j(\rho(X)), f_j(\rho(X^2)), \ldots, f_j(\rho(X^{k-1}))$ have a common null space element modulo $\mathcal{Q}$ and the proof of Lemma 2.3.7 gives us that $f_j(\zeta^{ai}) \equiv 0$ in $S/\mathcal{Q}$ for some a and for all $1 \leq i \leq k-1$. We also know that $f_j(1)$ is zero in $S/\mathcal{Q}$ since its coefficients sum to zero modulo $\mathcal{Q}$. Therefore

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ \zeta & \zeta^u & \zeta^{u^2} & \ldots & \zeta^{u^{k-1}} \\ \zeta^2 & \zeta^{2u} & \zeta^{2u^2} & \ldots & \zeta^{2u^{k-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \zeta^{k-1} & \zeta^{(k-1)u} & \zeta^{(k-1)u^2} & \ldots & \zeta^{(k-1)u^{k-1}} \end{pmatrix} \begin{pmatrix} 1 \\ z_k^{-j} \\ z_k^{-2j} \\ \vdots \\ z_k^{-(k-1)j} \end{pmatrix} = 0$$

in $S/\mathcal{Q}$. But it is a Vandermonde matrix, so its determinant is a product of $(\zeta^a - \zeta^b)$ for various a and b and these divide N. Therefore the matrix is invertible modulo $\mathcal{Q}$. This is a contradiction since it has a non-empty null space. Therefore there exists $\Gamma'_j = \sum_{i=1}^{k-1} a_i f_j(\rho(X^i))$ that is invertible modulo $\mathcal{Q}$. We can then pull this back to R_S to get $\Gamma_j = \sum_{i=1}^{k-1} a_i f_j(X^i)$ and since $f_j(X^i) \in R_j$ for all i, $\Gamma_j \in R_j$. Since Γ'_j is an invertible matrix its inverse, r', is a polynomial in Γ'_j (by Lemma 2.3.8). Hence r' is in the image of ρ. So there exists an $r \in R$ with $\rho(r) = r'$. Now since $I = \Gamma'_j r' = \rho(\Gamma_j r)$ (where I is the identity matrix) we get that $\Gamma_j r - 1$ is in the kernel of ρ. The kernel of ρ is contained in $R_{0,\mathcal{Q}}$, so $\Gamma_j r - 1 \in R_{0,\mathcal{Q}}$. But $1 \in R_{0,\mathcal{Q}}$, so $\Gamma_j r \in R_{0,\mathcal{Q}}$. Now we need to show that r can be chosen to be in R_{-j}, so that $r\beta \in R_{0,\mathcal{Q}}$ for all $\beta \in R_j$. Let $r = r_0 + r_1 + \cdots + r_{k-1}$ where $r_i \in R_i$. Then

$$\begin{aligned}
\Gamma_j r &= Y \Gamma_j r Y^{-1} \\
&= z_k^{-j} \Gamma_j Y (r_0 + r_1 + \cdots + r_{k-1}) Y^{-1} \\
&= z_k^{-j} \Gamma_j (r_0 + z_k^{-1} r_1 + \cdots + z_k^{-(k-1)} r_{k-1}).
\end{aligned}$$

Now $\Gamma_j r_i \in R_{j+i}$ for $0 \leq i \leq k-1$, so from the expansion of the left hand side we get $\Gamma_j r_i = z_k^{-j-i} \Gamma_j r_i$ for all i. Therefore $\Gamma_j r_i = 0$ for $i \neq -j$. So $\Gamma_j r = \Gamma_j r_{-j}$ and $\rho(\Gamma_j)\rho(r) = \rho(\Gamma_j)\rho(r_{-j})$. Now since $\rho(\Gamma_j) = \Gamma'_j$ is invertible, $\rho(r) = \rho(r_{-j})$. Therefore without loss of generality we may assume that $r \in R_{-j}$. Let $\beta \in R_j$ then $r\beta \in R_{0,\mathcal{Q}}$ and $\Gamma_j r\beta \in R_j$. Now $\rho(\beta - \Gamma_j r\beta) = 0$ so $\beta - \Gamma_j r\beta \in R_{0,\mathcal{Q}}$. But both summands are elements of R_j and therefore they must be equal. Since $\beta \in R_j$ we get $\beta = \Gamma_j \alpha$ where $\alpha = r\beta \in R_{0,\mathcal{Q}}$ which gives $R_j = \Gamma_j R_{0,\mathcal{Q}}$. Now it is clear from the proof that we could have also written $R_j = R_{0,\mathcal{Q}} \Gamma_j$ with the same Γ_j since Γ'_j and r' commute with each other (see proof of Lemma 2.3.8). $\square$

Next we want to show that it is not necessary to use this technique to find all of the Γ_j (unless z_k exists modulo q). Let $\mathbb{F} = S/\mathcal{Q}$. Then $\mathbb{F}$ is a finite extension of $\mathbb{F}_q$. Let the number of $Gal(\mathbb{F}/\mathbb{F}_q)$ orbits of z_k be δ. Let $z_k^{j_1}, z_k^{j_2}, \ldots z_k^{j_\delta}$ be representatives of these orbits. Then we need to find $\Gamma_{j_1}, \Gamma_{j_2}, \ldots, \Gamma_{j_\delta}$ using Theorem 2.3.10, but we can obtain the rest of the Γ_j by applying elements of $Gal(\mathbb{F}/\mathbb{F}_q)$ to these Γ_j. This allows us to write each element α of R in the following way:

$$\alpha = \alpha_0 + \sum_{i=1}^{\delta} \sum_{\sigma \in Gal(\mathbb{Q}[z_k]/Q)} \sigma(\Gamma_{j_i})\sigma(\alpha_{0,j_i}).$$

2.4 Breaking the System when z_k exists

Now we would like to break the system. This requires the creation of θ. Recall that θ needs the following properties:

- θ is the identity on $R_0 \pmod q$
- θ maps $R_j \pmod q$ to itself for all j
- θ is left and right R_0 linear
- $\theta(h)$ is a multiple of p and $\omega' = \theta(h)/p$ has small coefficients modulo q.

If we can define such a θ then $\theta(e) \pmod q$ modulo p will allow us to find the message m that was sent. All that is left to be able to create θ is to define ω'. We do this by noting that

$$h + YhY^{-1} + Y^2hY^{-2} + \cdots Y^{-1}hY = p(\omega + Y\omega Y^{-1} + Y^2\omega Y^{-2} + \cdots Y^{-1}\omega Y) \in R_{0,q}$$

just as before. So we create our ω' by dividing the coefficients of this sum into k equal (or as close to equal as possible) parts to define ω' modulo q. This ω' will

have coefficients of the same size as ω, so that the coefficients are 'small enough' to break the system.

We solve $\theta(h) = p\omega'$ by using Theorem 2.3.6 and Theorem 2.3.10 to reduce it to solving equations in $R_{0,q}$. Let

$$\begin{aligned} h &= h_0 + h_1 + h_2 + \cdots + h_{k-1} \\ &= h_0 + \Gamma_1 h_{0,1} + \Gamma_2 h_{0,2} + \ldots \Gamma_{k-1} h_{0,k-1} \end{aligned}$$

and

$$\begin{aligned} p\omega' &= \omega'_0 + \omega'_1 + \omega'_2 + \cdots + \omega'_{k-1} \\ &= \omega'_0 + \Gamma_1 \omega'_{0,1} + \Gamma_2 \omega'_{0,2} + \ldots \Gamma_{k-1} \omega'_{0,k-1} \end{aligned}$$

(incorporating the p into the notation) where $h_j, \omega'_j \in R_j$ and $h_{0,j}, \omega'_{0,j} \in R_{0,q}$ for all j. Now since θ takes R_j into itself for $1 \leq j \leq k-1$, we must have $\theta(\Gamma_j) = \Gamma_j r_{0,j}$ for some $r_{0,j} \in R_{0,q}$. Therefore

$$\begin{aligned} \theta(h) &= \theta(h_0 + \Gamma_1 h_{0,1} + \Gamma_2 h_{0,2} + \ldots \Gamma_{k-1} h_{0,k-1}) \\ &= h_0 + \theta(\Gamma_1 h_{0,1}) + \theta(\Gamma_2 h_{0,2}) + \cdots + \theta(\Gamma_{k-1} h_{0,k-1}) \\ &= h_0 + \theta(\Gamma_1) h_{0,1} + \theta(\Gamma_2) h_{0,2} + \ldots \theta(\Gamma_{k-1}) h_{0,k-1} \\ &= h_0 + \Gamma_1 r_{0,1} h_{0,1} + \Gamma_2 r_{0,2} h_{0,2} + \ldots \Gamma_{k-1} r_{0,k-1} h_{0,k-1} \end{aligned}$$

This must equal

$$p\omega' = \omega'_0 + \Gamma_1 \omega'_{0,1} + \Gamma_2 \omega'_{0,2} + \ldots \Gamma_{k-1} \omega'_{0,k-1}$$

Since $R = \oplus R_j$ we now need only solve $r_{0,j} h_{0,j} = \omega'_{0,j}$ for $r_{0,j}$ for all j such that $1 \leq j \leq k-1$. To do this we can write down the system of equations or the matrix that represents this system for the coefficients of $r_{0,j}$ and solve using linear algebra techniques. Again we need to worry about when a solution exists. This is discussed in Section 2.6. There is an example in Section 2.7.

Theorem 2.4.1. *Define $\theta(\alpha) = \bar{r}_{0,j}\alpha$ for $\alpha \in R_j$ where $\bar{r}_{0,j}$ is such that $\bar{r}_{0,j}\Gamma_j = \Gamma_j r_{0,j}$ with $r_{0,j}$ defined above. Then θ is a ring homomorphism from R to R that is left and right R_0 linear.*

Proof. We know that each R_j is a principal left and right R_0 module, so there exists such an $\bar{r}_{0,j} \in R_0$. Let $\alpha \in R_j$ and $x, y \in R_0$ then

$$\begin{aligned}\theta(x\alpha y) &= \bar{r}_{0,j}x\alpha y \\ &= x\bar{r}_{0,j}\alpha y \quad \text{since } R_0 \text{ is commutative} \\ &= x\theta(\alpha)y\end{aligned}$$

Therefore θ is left and right R_0 linear. □

2.5 When z_k does not exist modulo q

Creating the system is exactly the same as when z_k does exist modulo q. The difference arrives when we try to break the system. If z_k does not exist then we need S and $\mathcal{Q}$ to be as described in Section 2.3 and then everything works as in the last section except that we must show that $\theta(e)$ is rational.

Theorem 2.5.1. *Let $\tau \in Gal(\mathbb{Q}[z_k]/\mathbb{Q})$, then $\tau(\theta(e)) = \theta(e)$.*

Proof. We know that

$$\begin{aligned}\theta(e) &= \theta(e_0 + \Gamma_1 e_{0,1} + \Gamma_2 e_{0,2} + \cdots + \Gamma_{k-1}e_{0,k-1}) \\ &= e_0 + \theta(\Gamma_1)e_{0,1} + \theta(\Gamma_2)e_{0,2} + \cdots + \theta(\Gamma_{k-1})e_{0,k-1} \\ &= e_0 + \Gamma_1 r_{0,1}e_{0,1} + \Gamma_2 r_{0,2}e_{0,2} + \cdots + \Gamma_{k-1}r_{0,k-1}e_{0,k-1}.\end{aligned}$$

Now by the discussion at the end of the previous section we also know that

$$\theta(e) = e_0 + \sum_{i=0}^{\delta} \sum_{\sigma \in Gal(\mathbb{Q}[z_k]/Q)} \sigma(\Gamma_{j_i})\sigma(r_{0,j_i})\sigma(e_{0,j_i}).$$

This sum is clearly invariant under the Galois group, so $\theta(e)$ is rational. □

So to solve in this situation it is necessary to work in an extension field, but the results will lie in the base field. Note that Theorem 2.4.1 still applies here, so that θ is both left and right R_0 linear.

There is an example in Section 2.7.

2.6 Invertibility of h

We know that finding θ reduces to solving $r_{0,j_i}h_{0,j_i} = \omega_{0,j_i}$ for r_{0,j_i} for $1 \leq i \leq \delta$. It suffices to invert h_{0,j_i}. Now $h_{0,j_i} \in R_{0,S}$ and if we assume it is a random element, then we can use the following argument to determine the probability that it is invertible.

We know that $R = \oplus M_{n_i}(\mathbb{F}_{q^{m_i}})$ by [13, p 142]. Now Y maps to a permutation matrix of order k in each of the matrix rings where $n_i \neq 1$ under the maps ρ_i. We know that Y is diagonalizable and has distinct eigenvalues. Suppose that $B\rho_i(Y)B^{-1}$ is diagonal. Then the only matrices that commute with $B\rho_i(Y)B^{-1}$ are also diagonal. Let D be such a matrix. Then $B^{-1}DB$ commutes with $\rho_i(Y)$, so R_0 maps into this set of matrices contained in $\oplus M_{n_i}(\mathbb{F}_{q^{m_i}})$. We know that D is an n_i by n_i matrix, so in the worst case it has the following probability of being invertible:

$$\left(1 - \frac{1}{q^{m_i}}\right)^{n_i}.$$

So the total chance of being invertible is at least

$$\prod_i \left(1 - \frac{1}{q^{m_i}}\right)^{n_i}$$

We know that there are k one-dimensional representations and $\frac{N-1}{k}$ representations of dimension k. Also, 1 will be a lower bound on the m_i's so we get the probability is greater than or equal to

$$\left(1 - \frac{1}{q}\right)^{1*k+k*\frac{N-1}{k}} = \left(1 - \frac{1}{q}\right)^{k+N-1}.$$

This is approximately

$$1 - \frac{k+N-1}{q}$$

which is close to 1 as long as q is large enough compared to N and k, and this is a required for the system to work. If we recall the numbers that Coppersmith gave as an example, $N = 263, k = 2, q = 125003$ we get the probability that $h_{0,1}$ is invertible is at least 97.88%.

2.7 Examples

Example 2.7.1. *Let* $N = 7$, $k = 3$, $q = 199$, $p = r = t = 3$, *and* $s = 50$. *So our group* $G = \langle X, Y \mid X^7 = 1, Y^3 = 1, YX = X^2Y \rangle$. *In this situation a primitive third root of unity does exist modulo* 199 *and is equal to* 92 *modulo* 199. *To simplify notation let:*

$$W_0 = X + X^2 + X^4$$

$$W_1 = X^3 + X^6 + X^5$$

The following is the system set-up, the encryption, and decryption.

Bob makes the following choices:

$$\begin{aligned}
f &= 66 + 91W_0 - 26Y + 64W_0Y - 2W_1Y + 37Y^2 + 18W_0Y^2 + 35W_1Y^2 \\
\omega &= 1 + X - X^2 + X^3 - X^4 + X^5 - X^6 \\
&\quad + Y - XY + X^2Y + X^4Y - X^5Y \\
&\quad - Y^2 + XY^2 + X^2Y^2 + X^3Y^2 + X^4Y^2 - X^5Y^2
\end{aligned}$$

and computes the following:

$$\begin{aligned}
F &= f^{-1} \\
&= -98 - 78W_0 + 5W_1 - 74Y - 70W_0Y + 56W_1Y \\
&\quad - 29Y^2 + 64W_0Y^2 - 65W_1Y^2 \\
h &= F\omega f \\
&= 3 - 96X - 65X^2 + 83X^3 - 41X^4 - X^5 - 79X^6 \\
&\quad + 3Y + 6XY - 16X^2Y - 80X^3Y + 13X^4Y + 12X^5Y + 65X^6Y \\
&\quad - 3Y^2 + 81XY^2 + 56X^2Y^2 + 71X^4Y^2 + 40X^5Y^2 - 40X^6Y^2
\end{aligned}$$

Bob now makes h public and keeps $f, F,$ and ω private.

To send Bob a message Alice makes the following choices:

$$\begin{aligned}
\phi &= -W_0 + Y + W_0Y + W_1Y - Y^2 - W_1Y^2 \\
\phi' &= 1 + W_0 + W_1 + W_0Y + Y^2 + W_1Y^2 \\
\psi &= -23 - 6W_0 - 7W_1 + 7Y - 3W_0Y - 17W_1Y - 3Y^2 + 13W_0Y^2 - 17W_1Y^2
\end{aligned}$$

She reduces ψ modulo p to get $\Psi = 1 - W_1 + Y + W_1Y + W_0Y^2 + W_1Y^2$ and then

computes the following:

$$\begin{aligned} e &= \phi h \phi' + \psi \\ &= -41 - 46X + 99X^2 - 44X^3 - 35X^4 + 41X^5 + 36X^6 \\ &\quad + 22Y + 75XY - 59X^2Y - X^3Y - 70X^4Y - 81X^5Y + 4X^6Y \\ &\quad - 25XY^2 - 36X^2Y^2 + 4X^3Y^2 - 90X^4Y^2 - X^5Y^2 - 81X^6Y^2 \\ E &= \Psi h + m \\ &= -36 + 58X - 38X^2 - 89X^3 + 26X^4 + 39X^5 - X^6 \\ &\quad - 10Y + 70XY + 5X^2Y + 22X^3Y - 48X^4Y - 13X^5Y + 39X^6Y \\ &\quad + 48Y^2 - 78XY^2 + 72X^2Y^2 - 43X^3Y^2 - 79X^4Y^2 + X^5Y^2 + 30X^6Y^2 \end{aligned}$$

using her message

$$\begin{aligned} m &= -48 + 22X^2 - 3X^3 + 6X^4 - 23X^5 - 31X^6 \\ &\quad - 19Y + 48XY - 36X^2Y + 27X^3Y - 89X^5Y + 92X^6Y \\ &\quad + 54Y^2 - 28XY^2 + 81X^2Y^2 - 81X^3Y^2 + 49X^4Y^2 + 60X^5Y^2 - 3X^6Y^2 \end{aligned}$$

She now sends the pair (e, E) *to Bob.*

Bob uses his private keys to compute:

$$\begin{aligned} a &= feF \\ &= -41 + 6X + 12X^2 + 23X^3 + 17X^5 - 7X^6 \\ &\quad + 22Y - 12XY - 24X^2Y - 44X^3Y - 18X^4Y - 14X^5Y - 20X^6Y \\ &\quad + 10XY^2 + 16X^2Y^2 - 20X^3Y^2 + 22X^4Y^2 - 44X^5Y^2 - 14X^6Y^2 \end{aligned}$$

which he then reduces modulo p *to get*

$$\begin{aligned} a_p &= 1 - X^3 - X^5 - X^6 + Y + X^3Y + X^5Y + X^6Y \\ &\quad + XY^2 + X^2Y^2 + X^3Y^2 + X^4Y^2 + X^5Y^2 + X^6Y^2. \end{aligned}$$

Next Bob computes:

$$\begin{aligned} E - ha_p = &-48 + 22X^2 - 3X^3 + 6X^4 - 23X^5 - 31X^6 \\ &- 19Y + 48XY - 36X^2Y + 27X^3Y - 89X^5Y + 92X^6Y \\ &+ 54Y^2 - 28XY^2 + 81X^2Y^2 - 81X^3Y^2 + 49X^4Y^2 + 60X^5Y^2 - 3X^6Y^2 \end{aligned}$$

which is the message that Alice sent.

To break the system we only know:

$$\begin{aligned} h = &\, 3 - 96X - 65X^2 + 83X^3 - 41X^4 - X^5 - 79X^6 \\ &+ 3Y + 6XY - 16X^2Y - 80X^3Y + 13X^4Y + 12X^5Y + 65X^6Y \\ &- 3Y^2 + 81XY^2 + 56X^2Y^2 + 71X^4Y^2 + 40X^5Y^2 - 40X^6Y^2 \\ e = &-41 - 46X + 99X^2 - 44X^3 - 35X^4 + 41X^5 + 36X^6 \\ &+ 22Y + 75XY - 59X^2Y - X^3Y - 70X^4Y - 81X^5Y + 4X^6Y \\ &- 25XY^2 - 36X^2Y^2 + 4X^3Y^2 - 90X^4Y^2 - X^5Y^2 - 81X^6Y^2 \\ E = &-36 + 58X - 38X^2 - 89X^3 + 26X^4 + 39X^5 - X^6 \\ &- 10Y + 70XY + 5X^2Y + 22X^3Y - 48X^4Y - 13X^5Y + 39X^6Y \\ &+ 48Y^2 - 78XY^2 + 72X^2Y^2 - 43X^3Y^2 - 79X^4Y^2 + X^5Y^2 + 30X^6Y^2 \end{aligned}$$

We compute

$$\begin{aligned} h + YhY^2 + Y^2hY &= p(\omega + Y\omega Y^2 + Y^2\omega Y) \\ &= 3(3 + W_0 - W_1 + 3Y + W_0Y - W_1Y - 3Y^2 + 3W_0Y^2) \end{aligned}$$

So $\omega' = 1 + X - X^3 + Y + XY - X^3Y - Y^2 + XY^2 + X^2Y^2 + X^4Y^2$.

Now it is necessary to break both h *and* $p\omega'$ *into their* R_0*,* R_1*, and* R_2 *parts. We*

define the following to simplify notation:

$$W_{10} = X - 93X^2 + 92X^4$$

$$W_{11} = X^3 - 93X^6 + 92X^5$$

$$W_{20} = X + 92X^2 - 93X^4$$

$$W_{21} = X^3 + 92X^6 - 93X^5$$

So we get the following:

$$h_0 = 3 - W_0 + W_1 + 3Y + W_0Y - W_1Y - 3Y^2 + 3W_0Y^2$$

$$h_1 = -91W_{10} + 24W_{11} + 37W_{10}Y + 69W_{11}Y + 74W_{10}Y^2 + 54W_{11}Y^2$$

$$h_2 = -4W_{20} + 58W_{21} - 32W_{20}Y + 51W_{21}Y + 4W_{20}Y^2 - 54W_{21}Y^2$$

$$\omega_0' = h_0$$

$$\omega_1' = -W_{10} + W_{11} + W_{10}Y - W_{11}Y$$

$$\omega_2' = -W_{20} + W_{21} + W_{20}Y - W_{21}Y$$

where $\omega_0' + \omega_1' + \omega_2' = p\omega'$. *Next we note that* W_{10} *generates* R_1 *as an* R_0 *module and* W_{20} *generates* R_2 *as an* R_0 *module, since*

$$W_{10} = W_{10} * 1$$

$$W_{11} = W_{10} * (92W_0 - W_1)$$

$$W_{20} = W_{20} * 1$$

$$W_{21} = W_{20} * (-93W_0 - W_1).$$

Now we can rewrite $h_1, h_2, w_1,$ and w_2 as the following:

$$\begin{aligned}
h_1 &= W_{10}(-91 + 24(92W_0 - W_1) + (37 + 69(92W_0 - W_1))Y \\
&\quad + (74 + 54(92W_0 - W_1))Y^2) \\
h_2 &= W_{20}(-4 + 58(-93W_0 - W_1) + (-32 + 51(-93W_0 - W_1))Y \\
&\quad + (4 - 54(-93W_0 - W_1))Y^2) \\
w_1 &= W_{10}(-1 + (92W_0 - W_1) + (1 - (92W_0 - W_1))Y) \\
w_2 &= W_{20}(-1 + (-93W_0 - W_1) + (1 - (-93W_0 - W_1))Y)
\end{aligned}$$

This reduces our work to solving

$$\begin{aligned}
&\theta(W_{10})\Big((-91 + 24(92W_0 - W_1) + (37 + 69(92W_0 - W_1))Y \\
&\qquad + (74 + 54(92W_0 - W_1))Y^2)\Big) \\
&= W_{10}(-1 + (92W_0 - W_1) + (1 - (92W_0 - W_1))Y)
\end{aligned}$$

and

$$\begin{aligned}
&\theta(W_{20})\Big((-4 + 58(-93W_0 - W_1) + (-32 + 51(-93W_0 - W_1))Y \\
&\qquad + (4 - 54(-93W_0 - W_1))Y^2)\Big) \\
&= W_{20}(-1 + (-93W_0 - W_1) + (1 - (-93W_0 - W_1))Y).
\end{aligned}$$

But $\theta(W_{10})$ is an element of R_1 and $\theta(W_{20})$ is an element of R_2 so they must have the following forms:

$$\begin{aligned}
\theta(W_{10}) &= W_{10}r_{0,1} \\
\theta(W_{20}) &= W_{20}r_{0,2}
\end{aligned}$$

where $r_{0,1}, r_{0,2} \in R_0$. *Let*

$$r_{0,1} = a + a_0W_0 + a_1W_1 + bY + b_0W_0Y + b_1W_1Y + cY^2 + c_0W_0Y^2 + c_1W_1Y^2$$

$$r_{0,2} = d + d_0W_0 + d_1W_1 + eY + e_0W_0Y + e_1W_1Y + fY^2 + f_0W_0Y^2 + f_1W_1Y^2$$

then we need only solve

$$\begin{aligned} &W_{10}r_{0,1}\Big((-91 + 24(92W_0 - W_1) + (37 + 69(92W_0 - W_1))Y \\ &\quad + (74 + 54(92W_0 - W_1))Y^2)\Big) \\ &= W_{10}(-1 + (92W_0 - W_1) + (1 - (92W_0 - W_1))Y) \end{aligned}$$

and

$$\begin{aligned} &W_{20}r_{0,2}\Big((-4 + 58(-93W_0 - W_1) + (-32 + 51(-93W_0 - W_1))Y \\ &\quad + (4 - 54(-93W_0 - W_1))Y^2)\Big) \\ &= W_{20}(-1 + (-93W_0 - W_1) + (1 - (-93W_0 - W_1))Y) \end{aligned}$$

for $r_{0,1}$ *and* $r_{0,2}$. *Using Maple and Magma we find that*

$$\begin{aligned} r_{0,1} &= 8 - 30X - 30X^2 - 62X^3 - 30X^4 - 62X^5 - 62X^6 \\ &\quad + (-68 + 40X + 40X^2 + 64X^3 + 40X^4 + 64X^5 + 64X^6)Y \\ &\quad + (60 - 10X - 10X^2 - 2X^3 - 10X^4 - 2X^5 - 2X^6)Y^2 \\ r_{0,2} &= 2 + 56X + 56X^2 + 31X^3 + 56X^4 + 31X^5 + 31X^6 \\ &\quad + (7 - 10X - 10X^2 + 2X^3 - 10X^4 + 2X^5 + 2X^6)Y \\ &\quad + (-9 - 46X - 46X^2 - 33X^3 - 46X^4 - 33X^5 - 33X^6)Y^2 \end{aligned}$$

Now we can define the following:

$$\theta(W_{10}) = W_{10}r_{0,1}$$

$$\theta(W_{20}) = W_{20}r_{0,2}$$

To break the system we need to find $\theta(e)$. To do this we break e into its R_0, R_1, and R_2 parts and we get the following:

$$\begin{aligned}
e_0 &= -41 + 6W_0 + 11W_1 + (22 - 18W_0 - 26W_1)Y \\
&\quad + (0 + 16W_0 - 26W_1)Y^2 \\
e_1 &= W_{10}(-7 - 49(92W_0 - W_1) + (54 - 20(92W_0 - W_1))Y \\
&\quad + (-47 + 69(92W_0 - W_1))Y^2) \\
e_2 &= W_{20}(-45 - 6(-93W_0 - W_1) + (39 + 45(-93W_0 - W_1))Y \\
&\quad + (6 - 39(-93W_0 - W_1))Y^2).
\end{aligned}$$

So $\theta(e)$ reduces to

$$\begin{aligned}
\theta(e) &= -41 + 3X + 14X^3 + 15X^4 + 8X^5 + 11X^6 \\
&\quad + (22 - 24X - 9X^2 - 26X^3 - 21X^4 - 23X^5 - 29X^6)Y \\
&\quad + (25X + 13X^2 - 29X^3 + 10X^4 - 26X^5 - 23X^6)Y^2
\end{aligned}$$

Reducing this modulo $p = 3$ we get $1 - X^3 - X^5 - X^6 + (1 + X^3 + X^5 + X^6)Y + (X + X^2 + X^3 + X^4 + X^5 + X^6)Y^2$ which should be ψ modulo p. Using this and h we compute

$$\begin{aligned}
&E - h(1 - X^3 - X^5 - X^6 + (1 + X^3 + X^5 + X^6)Y \\
&\quad + (X + X^2 + X^3 + X^4 + X^5 + X^6)Y^2) \\
&\quad \equiv -48 + 22X^2 - 3X^3 + 6X^4 - 23X^5 - 31X^6 \\
&\quad - 19Y + 48XY - 36X^2Y + 27X^3Y - 89X^5Y + 92X^6Y \\
&\quad + 54Y^2 - 28XY^2 + 81X^2Y^2 - 81X^3Y^2 + 49X^4Y^2 + 60X^5Y^2 - 3X^6Y^2
\end{aligned}$$

which is the message m.

Example 2.7.2. *Let* $N = 7,\ k = 3,\ q = 197,\ p = r = t = 3,$ *and* $s = 50$. *So our group* $G = \langle X, Y \mid X^7 = 1, Y^3 = 1, YX = X^2Y \rangle$. *In this situation a primitive third root of unity does not exist (modulo* 197*) so we must formally adjoin one to our coefficient ring. It will be denoted by* z. *To simplify notation let:*

$$W_0 = X + X^2 + X^4$$
$$W_1 = X^3 + X^6 + X^5$$

The following is the system set-up, the encryption, and decryption.
Bob makes the following choices:

$$f = 37 - 42W_0 - 79W_1 - 19Y + 35W_0Y + 40W_1Y + 26Y^2 + 74W_0Y^2 + 37W_1Y^2$$
$$\omega = 1 + X + X^3 - Y + XY + X^2Y + X^3Y - X^4Y + X^5Y + X^6Y$$
$$+ X^2Y^2 - X^3Y^2 - X^4Y^2 + X^5Y^2 - X^6Y^2$$

and computes the following:

$$F = f^{-1}$$
$$= 75 - 81X - 81X^2 - 49X^3 - 81X^4 - 49X^5 - 49X^6$$
$$- 8Y - 46XY - 46X^2Y + 15X^3Y - 46X^4Y + 15X^5Y + 15X^6Y$$
$$+ 77Y^2 - 32XY^2 - 32X^2Y^2 + 34X^3Y^2 - 32X^4Y^2 + 34X^5Y^2 + 34X^6Y^2$$
$$h = F\omega f$$
$$= 3 + 50X - 84X^2 - 71X^3 + 37X^4 + 10X^5 + 64X^6$$
$$+ -3Y + 39XY - 6X^2Y + 80X^3Y - 30X^4Y + 75X^5Y + 51X^6Y$$
$$+ 8XY^2 - 57X^2Y^2 + 7X^3Y^2 + 49X^4Y^2 - 57X^5Y^2 + 47X^6Y^2$$

Bob now makes h *public and keeps* $f, F,$ *and* ω *private.*

To send Bob a message Alice makes the following choices:

$$\phi = W_1 + Y - W_0Y + W_1Y + W_1Y^2$$

$$\phi' = -1 - W_0 - W_1 + Y + W_0Y + W_1Y - Y2 + W_0Y^2 + W_1Y^2$$

$$\psi = 12 + 8W_0 + 2W_1 - 6Y - 22W_0Y - 2W_1Y - 24Y2 + 22W_0Y^2 + 13W_1Y^2$$

She reduces ψ modulo p to get $\Psi = -W_0 - W_1 - W_0Y + W_1Y + W_0Y^2 + W_1Y^2$ and then computes the following:

$$\begin{aligned} e &= \phi h\phi' + \psi \\ &= 21 + 63X - 92X^2 - 33X^3 + 2X^4 - 54X^5 + 75X^6 \\ &\quad - 15Y - 64XY + 26X^2Y - 23X^3Y + 47X^4Y - 29X^5Y - 37X^6Y \\ &\quad + 30Y^2 + 72XY^2 + 76X^2Y^2 - 39X^3Y^2 + 20X^4Y^2 + 72X^5Y^2 - 71X^6Y^2 \end{aligned}$$

$$\begin{aligned} E &= \Psi h + m \\ &= 4 + 54X + 90X^2 - 53X^3 - 80X^4 - 18X^5 + 35X^6 \\ &\quad - 62Y + 43XY - 22X^2Y - 24X^3Y - 15X^4Y + 46X^5Y + 84X^6Y \\ &\quad - 68Y^2 + 57XY^2 - 9X^2Y^2 + 55X^3Y^2 - 43X^4Y^2 + 2X^5Y^2 - 38X^6Y^2 \end{aligned}$$

using her message

$$\begin{aligned} m &= -5 - 50X - 47X^2 - 54X^3 - 33X^4 - 28X^5 + 52X^6 \\ &\quad - 47Y + 77XY + 97X^2Y - 12X^3Y + 68X^4Y - 29X^5Y - 32X^6Y \\ &\quad - 71Y^2 + 56XY^2 - 58X^2Y^2 - 50X^3Y^2 - 44X^4Y^2 + 96X^5Y^2 - 45X^6Y^2 \end{aligned}$$

She now sends the pair (e, E) to Bob.

Bob uses his private keys to compute:

$$\begin{aligned} a &= feF \\ &= 21 - 4X - 13X^2 - 10X^3 - 10X^4 - 19X^5 + 17X^6 \\ &\quad - 15Y + 14XY - 22X^2Y + 7X^3Y + 17X^4Y + 61X^5Y + 40X^6Y \\ &\quad + 30Y^2 + 76XY^2 + 40X^2Y^2 + 67X^3Y^2 + 52X^4Y^2 + 49X^5Y^2 + 43X^6Y^2 \end{aligned}$$

which he then reduces modulo p to get $a_p = -X - X^2 - X^3 - X^4 - X^5 - X^6 - XY - X^2Y + X^3Y - X^4Y + X^5Y + X^6Y + XY^2 + X^2Y^2 + X^3Y^2 + X^4Y^2 + X^5Y^2 + X^6Y^2$. *Next Bob computes:*

$$\begin{aligned} E - ha_p &= -5 - 50X - 47X^2 - 54X^3 - 33X^4 - 28X^5 + 52X^6 \\ &\quad - 47Y + 77XY + 97X^2Y - 12X^3Y + 68X^4Y - 29X^5Y - 32X^6Y \\ &\quad - 71Y^2 + 56XY^2 - 58X^2Y^2 - 50X^3Y^2 - 44X^4Y^2 + 96X^5Y^2 - 45X^6Y^2 \end{aligned}$$

which is the message that Alice sent.

To break the system we only know:

$$\begin{aligned} h &= 3 + 50X - 84X^2 - 71X^3 + 37X^4 + 10X^5 + 64X^6 \\ &\quad + -3Y + 39XY - 6X^2Y + 80X^3Y - 30X^4Y + 75X^5Y + 51X^6Y \\ &\quad + 8XY^2 - 57X^2Y^2 + 7X^3Y^2 + 49X^4Y^2 - 57X^5Y^2 + 47X^6Y^2 \\ e &= 21 + 63X - 92X^2 - 33X^3 + 2X^4 - 54X^5 + 75X^6 \\ &\quad - 15Y - 64XY + 26X^2Y - 23X^3Y + 47X^4Y - 29X^5Y - 37X^6Y \\ &\quad + 30Y^2 + 72XY^2 + 76X^2Y^2 - 39X^3Y^2 + 20X^4Y^2 + 72X^5Y^2 - 71X^6Y^2 \\ E &= 4 + 54X + 90X^2 - 53X^3 - 80X^4 - 18X^5 + 35X^6 \\ &\quad - 62Y + 43XY - 22X^2Y - 24X^3Y - 15X^4Y + 46X^5Y + 84X^6Y \\ &\quad - 68Y^2 + 57XY^2 - 9X^2Y^2 + 55X^3Y^2 - 43X^4Y^2 + 2X^5Y^2 - 38X^6Y^2 \end{aligned}$$

We compute

$$\begin{aligned} h + YhY^2 + Y^2hY &= p(\omega + Y\omega Y^2 + Y^2\omega Y) \\ &= 9 + 3X + 3X^2 + 3X^4 + 3X^3 + 3X^5 + 3X^6 \\ &- 9Y + 3XY + 3X^2Y + 3X^4Y + 9X^3Y + 9X^5Y + 9X^6Y \\ &- 3X^3Y^2 - 3X^5Y^2 - 3X^6Y^2 \end{aligned}$$

So $\omega' = 1 + X + X^3 - Y + XY + X^3Y + X^5Y + X^6Y - X^3Y^2$ *Now it is necessary to break both* h *and* $p\omega'$ *into their* $R_0, R_1,$ *and* R_2 *parts. We define the following to simplify notation:*

$$\begin{aligned} W_{10} &= X + z^2X^2 + zX^4 \\ W_{11} &= X^3 + z^2X^6 + zX^5 \\ W_{20} &= X + zX^2 + z^2X^4 \\ W_{21} &= X^3 + zX^6 + z^2X^5 \end{aligned}$$

So we get the following:

$$\begin{aligned} h_0 &= 3 + W_0 + W_1 - 3Y + W_0Y + 3W_1Y - W_1Y^2 \\ h_1 &= (91z + 70)W_{10} + (18z - 27)W_{11} + (8z + 23)W_{10}Y + (-8z - 64)W_{11}Y \\ &\quad + (96z + 52)W_{10}Y^2 + (-31z + 87)W_{11}Y^2 \\ h_2 &= (-91z - 21)W_{20} + (-18z - 45)W_{21} + (-8z + 15)W_{20}Y + (8z - 56)W_{21}Y \\ &\quad + (-96z - 44)W_{20}Y^2 + (31z - 79)W_{21}Y^2 \\ \omega_0' &= h_0 \\ \omega_1' &= W1_0 + W1_1 + W1_0Y - W1_1Y^2 \\ \omega_2' &= W2_0 + W2_1 + W2_0Y - W2_1Y^2 \end{aligned}$$

Where $\omega_0' + \omega_1' + \omega_2' = p\omega'$ *Next we note that* W_{10} *generates* R_1 *as an* R_0 *module and* W_{20} *generates* R_2 *as an* R_0 *module, since*

$$\begin{aligned} W_{10} &= W_{10} * 1 \\ W_{11} &= W_{10} * (zW_0 - W_1) \\ W_{20} &= W_{20} * 1 \\ W_{21} &= W_{20} * (z^2W_0 - W_1). \end{aligned}$$

Now we can rewrite $h_1, h_2, w_1,$ *and* w_2 *as the following:*

$$\begin{aligned} h_1 &= W_{10}(91z + 70 + (18z - 27)(zW_0 - W_1) \\ &\quad + (8z + 23 + (-8z - 64)(zW_0 - W_1))Y \\ &\quad + (96z + 52 + (-31z + 87)(zW_0 - W_1))Y^2) \\ h_2 &= W_{20}(-91z - 21 + (-18z - 45)(z^2W_0 - W_1) \\ &\quad + (-8z + 15 + (8z - 56)(z^2W_0 - W_1))Y \\ &\quad + (-96z - 44 + (31z - 79)(z^2W_0 - W_1))Y^2) \\ w_1 &= W_{10}(1 + zW_0 - W_1 + Y - (zW_0 - W_1)Y^2) \\ w_2 &= W_{20}(1 + z^2W_0 - W_1 + Y - (z^2W_0 - W_1)Y^2) \end{aligned}$$

This reduces our work to solving

$$\begin{aligned} &\theta(W_{10})\Big(91z + 70 + (18z - 27)(zW_0 - W_1) \\ &+ (8z + 23 + (-8z - 64)(zW_0 - W_1))Y \\ &+ (96z + 52 + (-31z + 87)(zW_0 - W_1))Y^2\Big) \\ &= W_{10}(1 + zW_0 - W_1 + Y - (zW_0 - W_1)Y^2) \end{aligned}$$

and

$$\begin{aligned}
&\theta(W_{20})\Big(-91z - 21 + (-18z - 45)(z^2W_0 - W_1) \\
&+ (-8z + 15 + (8z - 56)(z^2W_0 - W_1)) \\
&+ (-96z - 44 + (31z - 79)(z^2W_0 - W_1))Y^2\Big) \\
&= W_{20}(1 + z^2W_0 - W_1 + Y - (z^2W_0 - W_1)Y^2)
\end{aligned}$$

but $\theta(W_{10})$ *is an element of* R_1 *and* $\theta(W_{20})$ *is an element of* R_2 *so they must have the following forms:*

$$\begin{aligned}
\theta(W_{10}) &= W_{10}r_{0,1} \\
\theta(W_{20}) &= W_{20}r_{0,2}
\end{aligned}$$

where $r_{0,1}, r_{0,2} \in R_0$. *Let*

$$\begin{aligned}
r_{0,1} &= a + a_0W_0 + a_1W_1 + bY + b_0W_0Y + b_1W_1Y + cY^2 + c_0W_0Y^2 + c_1W_1Y^2 \\
r_{0,2} &= d + d_0W_0 + d_1W_1 + eY + e_0W_0Y + e_1W_1Y + fY^2 + f_0W_0Y^2 + f_1W_1Y^2
\end{aligned}$$

then we need only solve

$$\begin{aligned}
&W_{10}r_{0,1}\Big(91z + 70 + (18z - 27)(zW_0 - W_1) \\
&+ (8z + 23 + (-8z - 64)(zW_0 - W_1))Y \\
&+ (96z + 52 + (-31z + 87)(zW_0 - W_1))Y^2\Big) \\
&= W_{10}(1 + zW_0 - W_1 + Y - (zW_0 - W_1)Y^2)
\end{aligned}$$

and

$$\begin{aligned}
&W_{20}r_{0,2}\Big(-91z - 21 + (-18z - 45)(z^2W_0 - W_1) \\
&+ (-8z + 15 + (8z - 56)(z^2W_0 - W_1)) \\
&+ (-96z - 44 + (31z - 79)(z^2W_0 - W_1))Y^2\Big) \\
&= W_{20}(1 + z^2W_0 - W_1 + Y - (z^2W_0 - W_1)Y^2)
\end{aligned}$$

for $r_{0,1}$ *and* $r_{0,2}$*. Using Maple and Magma we find that*

$$\begin{aligned}
r_{0,1} &= 84 - 54z + (68z - 89)W_0 + (77 - 11z)W_1 \\
&+ (5z + 33 + (25 + 36z)W_0 + (31 - 17z)W_1)Y \\
&+ (-15 - 24z + (-45z + 15)W_0 + (-8z + 49)W_1)Y^2 \\
r_{0,2} &= -59 + 54z + (-68z + 40)W_0 + (88 + 11z)W_1 \\
&+ (-5z + 28 + (-11 - 36z)W_0 + (48 + 17z)W_1)Y \\
&+ (9 + 24z + (45z + 60)W_0 + (8z + 57)W_1)Y^2
\end{aligned}$$

Now we can define the following:

$$\begin{aligned}
\theta(W_{10}) &= W_{10}r_{0,1} \\
\theta(W_{20}) &= W_{20}r_{0,2}
\end{aligned}$$

To break the system we need to find $\theta(e)$*.*

To do this we break e into its R_0, R_1, and R_2 parts and we get the following:

$$e_0 = 21 - 9W_0 - 4W_1 + (-15 + 3W_0 + 36W_1)Y + (30 + 56W_0 + 53W_1)Y^2$$

$$\begin{aligned} e_1 = W_{10}(&-97z + 86 + (43z + 7)(zW_0 - W_1) \\ &+ (-7z - 37 + (63z + 2)(zW_0 - W_1))Y \\ &+ (-47z + 83 + (18z - 37)(zW_0 - W_1))Y^2) \end{aligned}$$

$$\begin{aligned} e_2 = W_{20}(&97z - 14 - (43z + 36)(z^2W_0 - W_1) \\ &+ (7z - 30 - (63z + 61)(z^2W_0 - W_1))Y \\ &+ (47z - 67 + (-18z - 55)(z^2W_0 - W_1))Y^2). \end{aligned}$$

So $\theta(e)$ reduces to

$$\begin{aligned} \theta(e) = 21 &- 7X - 16X^2 - X^3 - 4X^4 - 16X^5 + 5X^6 \\ &- 15Y - 4XY + 2X^2Y + 25X^3Y + 11X^4Y + 43X^5Y + 40X^6Y \\ &+ 30Y^2 + 61XY^2 + 46X^2Y^2 + 67X^3Y^2 + 61X^4Y^2 + 46X^5Y^2 + 46X^6Y^2 \end{aligned}$$

Reducing this modulo $p = 3$ we get $-X - X^2 - X^3 - X^4 - X^5 - X^6 + (-X - X^2 + X^3 - X^4 + X^5 + X^6)Y + (X + X^2 + X^3 + X^4 + X^5 + X^6)Y^2$ which should be ψ modulo p. Using this and h to compute m we get small

$$\begin{aligned} &E - h * \Big(- X - X^2 - X^3 - X^4 - X^5 - X^6 + \\ &(-X - X^2 + X^3 - X^4 + X^5 + X^6)Y + (X + X^2 + X^3 + X^4 + X^5 + X^6)Y^2 \Big) \\ \equiv &- 5 - 50X - 47X^2 - 54X^3 - 33X^4 - 28X^5 + 52X^6 \\ &- 47Y + 77XY + 97X^2Y - 12X^3Y + 68X^4Y - 29X^5Y - 32X^6Y \\ &- 71Y^2 + 56XY^2 - 58X^2Y^2 - 50X^3Y^2 - 44X^4Y^2 + 96X^5Y^2 - 45X^6Y^2 \end{aligned}$$

which is the message m.

BIBLIOGRAPHY

[1] D. Coppersmith. Attacking non-commutative NTRU. *IBM Research Report*, page 5, April 1997.

[2] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[3] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in cryptology (Santa Barbara, Calif., 1984)*, volume 196 of *Lecture Notes in Comput. Sci.*, pages 10–18. Springer, Berlin, 1985.

[4] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory*, 31(4):469–472, 1985.

[5] Craig Gentry, Jakob Jonsson, Jacques Stern, and Michael Szydlo. Cryptanalysis of the NTRU signature scheme (NSS) from Eurocrypt 2001. In *Advances in cryptology—ASIACRYPT 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 1–20. Springer, Berlin, 2001.

[6] J. Hoffstein and J. H. Silverman. A non-commutative version of the NTRU public key cryptosystem. February 1997. It was for a while available at http://www.tiac.net/users/ntru/NTRUFTP.html.

[7] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte. NTRUSign: digital signatures using the NTRU lattice. In *Topics in cryptology—CT-RSA 2003*, volume 2612 of *Lecture Notes in Comput. Sci.*, pages 122–140. Springer, Berlin, 2003.

[8] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: a ring-based public key cryptosystem. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 267–288. Springer, Berlin, 1998.

[9] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NSS: an NTRU lattice-based signature scheme. In *Advances in cryptology—EUROCRYPT 2001 (Innsbruck)*, volume 2045 of *Lecture Notes in Comput. Sci.*, pages 211–228. Springer, Berlin, 2001.

[10] Karl Mahlburg. An overview of braid group cryptography. http://citeseer.ist.psu.edu/mahlburg04overview.html.

[11] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DNS progress report no.42-44, Jet Propulsion Laboratory, Pasadena, California*, 1978.

[12] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.

[13] César Polcino Milies and Sudarshan K. Sehgal. *An introduction to group rings*, volume 1 of *Algebras and Applications*. Kluwer Academic Publishers, Dordrecht, 2002.

[14] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126, 1978.

[15] Jean-Pierre Serre. *Linear representations of finite groups*. Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[16] Wade Trappe and Lawrence Washington. *Introduction to Cryptography with Coding Theory*. Pearson Prentice Hall, Upper Saddle River, NJ, second edition, 2006.