5-2009

New Directions in Multivariate Public Key Cryptography

Raymond Heindl
Clemson University, rheindl@gmail.com

New Directions in Multivariate Public Key Cryptography

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Mathematical Sciences

---

by
Raymond A. Heindl
May 2009

Accepted by:
Dr. Shuhong Gao, Committee Chair
Dr. Hiren Maharaj
Dr. Gretchen Matthews
Dr. Hui Xue

Abstract

Most public key cryptosystems used in practice are based on integer factorization or discrete logarithms (in finite fields or elliptic curves). However, these systems suffer from two potential drawbacks. First, they must use large keys to maintain security, resulting in decreased efficiency. Second, if large enough quantum computers can be built, Shor's algorithm will render them completely insecure.

Multivariate public key cryptosystems (MPKC) are one possible alternative. MPKC makes use of the fact that solving multivariate polynomial systems over a finite field is an NP-complete problem, for which it is not known whether there is a polynomial algorithm on quantum computers.

The main goal of this work is to show how to use new mathematical structures, specifically polynomial identities from algebraic geometry, to construct new multivariate public key cryptosystems. We begin with a basic overview of MPKC and present several significant cryptosystems that have been proposed. We also examine in detail some of the most powerful attacks against MPKCs. We propose a new framework for constructing multivariate public key cryptosystems and consider several strategies for constructing polynomial identities that can be utilized by the framework. In particular, we have discovered several new families of polynomial identities. Finally, we propose our new cryptosystem and give parameters for which it is secure against known attacks on MPKCs.

Dedication

To Adrienne,

who encourages and inspires me in all facets of life,

and above all, loves me.

Acknowledgments

I would like to express sincere gratitude to the following people, who have made my experience most excellent.

Shuhong Gao, without whom this work would not exist, for his instruction, eagerness to explore new ideas, patience, and friendship. I have truly benefited greatly from working alongside and standing on the shoulders of such a giant.

My committee: Gretchen Matthews, Hiren Maharaj, and Hui Xue, for their excellent instruction in the classroom, encouragement in research, and kind advice.

My officemates through the years: Ethan Smith, Jang-Woo Park, Mingfu Zhu, Christine Kraft, and Melissa Gardenghi, for countless hours of good conversation.

Jintai Ding, for his helpful encouragement and insight, and for his excellent book that introduced me to the exciting field of Multivariate Public Key Cryptography.

My family: my parents Paul and Carol, and my siblings Rob, Chris, Fiona, and Becca, for their constant love and support; and my wife Adrienne, for showing me love, patience, kindness, and faithfulness.

Finally, I give praise to my God and Savior Jesus Christ.

"Great are the works of the LORD, studied by all who delight in them." Psalm 111:2

Table of Contents

List of Tables

List of Figures

Chapter 1

Multivariate Public Key Cryptography

Since digital communication has become ubiquitous in our daily lives, the need for security is greater than ever. Cryptography, the science of secure communication in the presence of adversaries [Riv90], has provided the necessary security to enable safe electronic financial transactions, military communication, corporate privacy, data storage, and a host of other applications.

Classically, encryption and decryption were performed using the same secret key. However, these symmetric key cryptosystems have the inherent weakness that users must somehow securely exchange keys before sending and receiving messages. Diffie and Hellman [DH76] revolutionized the field by proposing the idea of public key cryptosystems, which eliminate the necessity of sharing secret keys. Shortly afterward, Rivest, Shamir, and Adleman proposed the now popular RSA system [RSA78].

Most public key cryptosystems used in practice are based on integer factorization or discrete logarithms (in finite fields or elliptic curves). However, these systems suffer from two potential drawbacks. First, advances in the field of number theory have caused a decrease in computational efficiency, since parameter sizes must be increased to meet security demands. Second, if large enough quantum computers can be built, Shor's algorithm [Sho97] will

render the current systems completely insecure. Therefore, it is important to search for alternative systems that facilitate both efficient and secure communication.

Multivariate public key cryptosystems (MPKC) are one possible alternative to the current public key schemes. In recent years, MPKC has become an active area of scientific research and has seen many significant advances. In 2003, the Sflash signature system was a final selection of the NESSIE (New European Schemes for Signatures, Integrity, and Encryption) project [NES03]. The first book about MPKC, written by Ding, Gower, and Schmidt, was published in 2006 [DGS06a]. While many papers on MPKC are accepted each year at annual international conferences such as the Public Key Cryptography conference and the Cryptographers' Track at the RSA conference, there is also a biyearly international workshop, PQCrypto, that is devoted solely to post-quantum cryptography and has a particularly strong focus on MPKC.

1.1 Foundation: Structure, Security, and Efficiency

Let k be a finite field of characteristic p with q elements. The public key of an MPKC is a polynomial map, $\bar{F} : k^n \to k^m$, given by

$$\bar{F}(x_1, \ldots, x_n) = \begin{pmatrix} \bar{f}_1(x_1, \ldots, x_n) \\ \vdots \\ \bar{f}_m(x_1, \ldots, x_n) \end{pmatrix}^T$$

where $\bar{f}_i \in k[x_1, \ldots, x_n]$ are quadratic. The security of MPKC is based on the assumption that solving a system of quadratic multivariate polynomials over a finite field is, in general, an NP-complete problem.

Encryption is quite simple: given plaintext $(x_1, \ldots, x_n) \in k^n$, the ciphertext is

$$(y_1, \ldots, y_m) = \bar{F}(x_1, \ldots, x_n).$$

Then to decrypt, given ciphertext $(y_1, \ldots, y_m) \in k^m$, find $(x_1, \ldots, x_n) \in k^n$ such that

$$\bar{F}(x_1, \ldots, x_n) = (y_1, \ldots, y_m).$$

Usually $\bar{F}$ is injective in cryptographic applications, so we simply say that decryption is computing $\bar{F}^{-1}(y_1, \ldots, y_m)$.

Digital signature is also possible with MPKC: given document $(y_1, \ldots, y_m) \in k^m$, the signature is

$$(x_1, \ldots, x_n) = \bar{F}^{-1}(y_1, \ldots, y_m).$$

Then to verify the signature is valid, check that

$$\bar{F}(x_1, \ldots, x_n) = (y_1, \ldots, y_m).$$

(Note that in both cases, we have assumed $\bar{F}$ is invertible, although this is not necessarily required, especially with digital signature. We must, however, have the ability to compute preimages.)

Security. As with all public key cryptosystems, the necessity that $\bar{F}$ be a trapdoor one-way function is now apparent; if $\bar{F}^{-1}$ can be computed not only by the intended recipient (or document signer), but also by an adversary, the system is worthless. Therefore, while $\bar{F}$ must have the appearance (to an adversary) of a random system of multivariate polynomials, it must in fact have a trapdoor that allows legitimate users to decrypt (or sign) messages. To implement a trapdoor, we construct $\bar{F}$ by composing three maps:

$$\bar{F} = L_1 \circ F \circ L_2, \tag{1.1}$$

where $L_1 : k^m \to k^m$ and $L_2 : k^n \to k^n$ are two random invertible affine transformations, and the central map $F : k^n \to k^m$ is a nonlinear multivariate polynomial map which has the property that we can easily find preimages. Thus the security of an MPKC rests on the

known difficulty of

- solving quadratic multivariate systems over finite fields (the left side of (1.1)), and
- factoring multivariate maps (the right side of (1.1)).

In the first case, it is known that solving a random multivariate quadratic system over a finite field is NP-complete [GJ79, PG97]. For the second, also called the Isomorphism of Polynomials (IP) problem, Patarin et al. showed that this was at least as difficult as the Graph Isomorphism problem (an NP problem) [Pat96, PGC98]. Also, as the authors of [DS06] have pointed out, factoring multivariate maps is a hard problem because of its connection with the Jacobian conjecture from algebraic geometry.

The private key of an MPKC consists of L_1 and L_2, and sometimes F. Creating an F for which it is easy to find preimages requires adding structure, and though many ideas have been suggested, in most cases, the added structure has led to the discovery of some weakness.

Efficiency. Any practical cryptosystem must of course be efficient. As mentioned above, encryption is accomplished by evaluating the public key polynomials over a finite field; this is a very fast and efficient process. Regarding decryption, we insist F be designed such that finding preimages is efficient. Another important concern is size of the public key; even though the central map may have relatively few terms, the affine transformations L_1 and L_2 make the public key polynomials dense. Since the number of terms of a polynomial of total degree d in n variables is at most $\binom{n+d}{d}$ and hence grows large as d is increased, in practice, we only consider quadratic MPKCs.

This chapter gives a brief overview of central maps that have been proposed (following the descriptions presented in [DGS06a]), touching on the strengths and weaknesses (if known) of each. The second part of the chapter focuses on a new framework for constructing central maps.

1.2 Overview of Existing Schemes

It is difficult to succinctly classify the different types of central maps that have been proposed for use in multivariate cryptosystems. Wolf and Preneel [WP05a] were perhaps the first to attempt to classify MPKCs. They divided systems into single field systems (using multivariate polynomials over a ground field k) and mixed field systems (using univariate polynomials over an extension of k). Within the single field category are several Triangular systems and the Oil-Vinegar system [Pat97], along with its variants; within the mixed field category are the Matsumoto-Imai [IM85, MI88] and Hidden Field Equations (HFE) [Pat96] cryptosystems, along with their variants.

Unfortunately, this classification does not work so well for systems that have been proposed since 2005. There have been at least four significant new central maps proposed since then which don't fit into the existing categories (often using ideas from both): Rainbow [DS05], MFE [WYHL06], ℓ-Invertible Cycles (ℓ-IC) [DWY07], and the system we propose in Chapter 4 of this work.

1.2.1 Univariate-Multivariate Correspondence

As mentioned above, mixed field systems employ univariate polynomials over extensions of k. However, it may not be entirely obvious that this is an acceptable strategy, since a central map must be a quadratic system of multivariate polynomials. The key observation is that there is a correspondence between univariate polynomials over an extension field and a system of multivariate polynomials over the ground field.

From univariate to multivariate. Let K be a degree n extension of k, and fix a basis $\{\alpha_1, \ldots, \alpha_n\}$ of K over k. We identify K with k^n via the natural isomorphism $\pi : K \to k^n$ given by

$$\pi(a_1\alpha_1 + \cdots + a_n\alpha_n) = (a_1, \ldots, a_n),$$

where $a_i \in k, 1 \leq i \leq n$. We can then view a polynomial $f \in K[X]$ component-wise over k by substituting $X = x_1\alpha_1 + \cdots + x_n\alpha_n$, and then $f = f_1\alpha_1 + \cdots + f_n\alpha_n$ with $f_i \in k[x_1, \ldots, x_n]$. So π is extended to the polynomial rings via

$$f \in K[X] \mapsto (f_1, \ldots, f_n) \in k[x_1, \ldots, x_n]^n.$$

Thus, the process of converting from univariate polynomials in $K[X]$ to multivariate systems in $k[x_1, \ldots, x_n]^n$ is fairly straightforward.

Quotient rings. Before continuing, we must emphasize a critical point regarding the rings we are working with. Since plaintext components are actually field values, we can view $(x_1, \ldots, x_n) \in k^n$ (similarly $X \in K$), and hence require that they satisfy the equations

$$x_i^q - x_i = 0, \quad 1 \leq i \leq n, \quad \text{(similarly, } X^{q^n} - X = 0).$$

Therefore, we do not work in the polynomial ring $k[x_1, \ldots, x_n]$, but rather the ring of *functions* from k^n to k, i.e.

$$k[x_1, \ldots, x_n]/(x_1^q - x_1, \ldots, x_n^q - x_n),$$

or similarly the ring of functions from K to K, i.e.

$$K[X]/(X^{q^n} - X).$$

Notice that when we write $k[x_1, \ldots, x_n]$ or $K[X]$, we will always be talking about the ring of functions, unless otherwise noted.

Degree considerations. Since we are interested in multivariate polynomials of degree two, it is necessary to determine the degree of $\pi(f)$ for $f \in K[X]$. Consider a monomial X^e

and write the base-q expansion of e, i.e. $e = a_0 + a_1 q + \cdots + a_{n-1} q^{n-1}$, $0 \leq a_i < q$. Then

$$\begin{aligned} X^e &= (\pi^{-1}(x_1, \ldots, x_n))^e \\ &= (x_1\alpha_1 + \cdots + x_n\alpha_n)^{\sum_{i=0}^{n-1} a_i q^i} \\ &= \prod_{i=0}^{n-1} (x_1\alpha_1 + \cdots + x_n\alpha_n)^{a_i q^i} \\ &= \prod_{i=0}^{n-1} (x_1\alpha_1^{q^i} + \cdots + x_n\alpha_n^{q^i})^{a_i}. \end{aligned}$$

We see that each component of $\pi(X^e)$ will have total degree $\sum_{i=0}^{n-1} a_i$ as a polynomial in $k[x_1, \ldots, x_n]$, and we define this to be *q-Hamming weight* of X^e. We can then define the q-Hamming weight of $f \in K[X]$ as the largest of the q-Hamming weights among the terms of f. Therefore, we can conlcude that polynomials in $K[X]$ with a q-Hamming weight of two correspond to quadratic systems in $k[x_1, \ldots, x_n]^n$.

From multivarite to univariate. For the sake of completeness, we now examine the conversion from multivariate systems in $k[x_1, \ldots, x_n]^n$ to univariate polynomials in $K[X]$, following [KS99] but giving a more explicit construction using a Vandermonde matrix instead of interpolation as suggested by the authors. We begin by considering functions $F_i : k^n \to k^n$, $1 \leq i \leq n$, given by

$$(x_1, \ldots, x_n) \mapsto (x_i, 0, \ldots, 0).$$

Choose a basis $\{\alpha_1, \ldots, \alpha_n\}$ of K over k such that $\alpha_1 = 1$ and let $X = \sum_{i=1}^{n} x_i\alpha_i$. Then for each i, the corresponding function over K, $\tilde{F}_i : K \to K$, is given by

$$X \mapsto x_i,$$

where we have used the fact that $\alpha_1 = 1$. Notice each F_i is a linear transformation and has matrix A_i that has a 1 in the i-th position of the first row and 0's everywhere else. Let

$M \in K^{n\times n}$ be the Vandermonde matrix for the α_i's, i.e.

$$M = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^q & \alpha_2^q & \dots & \alpha_n^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \dots & \alpha_n^{q^{n-1}} \end{pmatrix},$$

so that $M(x_1,\dots,x_n)^T = (X, X^q, \dots, X^{q^{n-1}})^T$. Then we can write

$$\begin{aligned} \tilde{F_i}(X) &= (\alpha_1,\dots,\alpha_n)A_i(x_1,\dots,x_n)^T \\ &= (\alpha_1,\dots,\alpha_n)A_iM^{-1}M(x_1,\dots,x_n)^T \\ &= (\alpha_1,\dots,\alpha_n)\begin{pmatrix} & \mathrm{Row}_i M^{-1} & \\ 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}\begin{pmatrix} X \\ X^q \\ \vdots \\ X^{q^{n-1}} \end{pmatrix} \\ &= \mathrm{Row}_i M^{-1}(X, X^q, \dots, X^{q^{n-1}})^T. \end{aligned}$$

Next consider $F : k^n \to k^n$ given by

$$(x_1,\dots,x_n) \mapsto \left(\prod_{i=1}^n x_i^{e_i}, 0, \dots, 0\right).$$

The corresponding map over K is $\tilde{F} : K \to K$ given by

$$X \mapsto \prod_{i=1}^n x_i^{e_i},$$

where again we have used the fact that $\alpha_1 = 1$. Then

$$\begin{aligned}\tilde{F}(X) &= \prod_{i=1}^{n}(\tilde{F}_i(X))^{e_i} \\ &= \prod_{i=1}^{n}(\mathrm{Row}_i M^{-1}(X, X^q, \ldots, X^{q^{n-1}})^T)^{e_i} \\ &= \prod_{i=1}^{n}\left(\sum_{j=1}^{n} m_{ij} X^{q^{j-1}}\right)^{e_i},\end{aligned}$$

where $m_{ij} = [M^{-1}]_{ij}$. Generalizing from monomials to polynomials, if F is given by a polynomial in the first component:

$$(x_1, \ldots, x_n) \mapsto \left(\sum_{k=1}^{t}\left(\prod_{i=1}^{n} x_i^{e_{ik}}\right), 0, \ldots, 0\right),$$

then

$$\tilde{F}(X) = \sum_{k=1}^{t}\prod_{i=1}^{n}\left(\sum_{j=1}^{n} m_{ij} X^{q^{j-1}}\right)^{e_{ik}}.$$

Finally, if in F, a polynomial appears in the ℓ-th component, then in $\tilde{F}$, we simply multiply by α_ℓ, i.e.

$$(x_1, \ldots, x_n) \mapsto \left(0, \ldots, 0, \sum_{k=1}^{t}\left(\prod_{i=1}^{n} x_i^{e_{ik}}\right), 0, \ldots, 0\right),$$

corresponds to

$$\tilde{F}(X) = \alpha_\ell \sum_{k=1}^{t}\prod_{i=1}^{n}\left(\sum_{j=1}^{n} m_{ij} X^{q^{j-1}}\right)^{e_{ik}}. \tag{1.2}$$

Therefore, given any polynomial map $F : k^n \to k^n$, we sum the univariate maps corresponding to each component (multiplying by the appropriate basis element) to get the univariate polynomial that represents the system. In particular, for a system of quadratic polynomials,

the corresponding $\tilde{F}(X)$ can be written as

$$\tilde{F}(X) = \sum_{0 \le i \le j \le n-1} a_{ij} X^{q^i + q^j} + \sum_{0 \le i \le n-1} b_i X^{q^i} + c, \quad a_{ij}, b_i, c \in K,$$

where the total number of terms is $O(n^2)$. Since each coefficient in K can be expressed as an element of k^n, we see that the total space (number of elements in k) required to store the univariate polynomial is $O(n^3)$, which is the same as the corresponding multivariate system.

We also observe that the above technique may be extended to multivariate systems in $k[x_1, \ldots, x_n]^m$, where $n \neq m$. In this case, we simply let $M = \max\{n, m\}$ and define K as a degree M extension of k.

Complexity of polynomial factorization. Notice that $\tilde{F}(X)$ will be a sparse polynomial since by expanding the product in (1.2), we see that the only exponents appearing will be sums of q-th powers. Thus we make an important distinction regarding the complexity of finding the roots of univariate polynomials over finite fields. For the dense representation of a polynomial (a list of all coefficients including zeros), roots may be found in polynomial time (in the size of the input). See [VG03] for a discussion of several factorization methods.

For the sparse representation of a polynomial (a list of only the nonzero coefficients and the degrees), the problem becomes much harder. To illustrate this difference, consider the polynomial

$$f(X) = 1 + X + X^{2^v}.$$

Since there are only 3 nonzero coefficients, the input size is $O(v)$, but if we wanted to actually factor f, we would have to represent f as

$$f(X) = 1 + X + \sum_{i=2}^{2^v - 1} a_i X^i + X^{2^v}, \quad a_i \in K,$$

where the input size is now $O(2^v)$. We can then factor f with complexity that is polynomial

in 2^v, which is exponential in v.

In general, we have shown above that there is a one-to-one correspondence between a system of m quadratic polynomials in n variables and a univariate polynomial of sparse size $O(M^3)$, where $M = \max\{m, n\}$. This correspondence also establishes a correspondence between solutions. Therefore, since solving a quadratic system is NP-complete, solving a sparse univariate polynomial is also NP-complete.

1.2.2 Matsumoto-Imai Cryptosystem (MI)

Having discussed the necessary theory behind the mixed field systems, we are now ready to introduce the first such system: the Matsumoto-Imai cryptosystem (MI). Although it first appeared in a Japanese journal in the mid-80's, Matsumoto and Imai formally introduced (to the English reading world) what they called the C^* cryptosystem in 1988 [MI88]. They were the first to recognize the cryptographic significance of the correspondence discussed in the previous section and effectively use it to build a multivariate cryptosystem.

We will use the same set-up as in Section 1.2.1, with the added restriction that k has characteristic two. Choose an integer θ between 0 and n such that $\gcd(q^\theta + 1, q^n - 1) = 1$, and let $\tilde{F} : K \to K$ be given by

$$X \mapsto X^{q^\theta+1}$$

(k must have characteristic two since otherwise, no θ can satisfy the gcd requirement). Using the extended Euclidean algorithm, we can compute t such that

$$(q^\theta + 1)t \equiv 1 \mod (q^n - 1).$$

Notice

$$(X^{q^\theta+1})^t = XX^{(q^\theta+1)t-1} = X,$$

thus $\tilde{F}^{-1}(X) = X^t$ and $\tilde{F}$ is an easily invertible univariate map over K. Finally, we define

the public key of the MI cryptosystem as the polynomial map $\bar{F}$ given by

$$\bar{F} = L_1 \circ \pi \circ \tilde{F} \circ \pi^{-1} \circ L_2, \tag{1.3}$$

where $L_1 : k^n \to k^n$ and $L_2 : k^n \to k^n$ are invertible affine transformations that function as the private key. Since the number of possibilities for θ is small, keeping it secret increases the complexity of an attack by at most of factor of n, and it is therefore not considered part of the private key.

Encryption. Given plaintext $(x_1, \ldots, x_n) \in k^n$, the ciphertext is

$$(y_1, \ldots, y_n) = \bar{F}(x_1, \ldots, x_n).$$

Decryption. Given ciphertext $(y_1, \ldots, y_n) \in k^n$, the plaintext is recovered by computing

$$(x_1, \ldots, x_n) = L_2^{-1} \circ \pi \circ \tilde{F}^{-1} \circ \pi^{-1} \circ L_1^{-1}(y_1, \ldots, y_n).$$

Notice that the MI cryptosystem may be thought of as a multivariate analog to RSA since both rely on properties of exponentiation in quotient rings.

Example 1.2.1. To give a flavor of what multivariate cryptosystems look like, we now present a very small example of the MI cryptosystem. Let $k = \mathbb{F}_4$ be the finite field of four elements with primitive element a, and let K be a degree 5 extension of k. Let $\theta = 3$, and define the central map $F = \pi \circ \tilde{F} \circ \pi^{-1}$ where

$$\tilde{F}(X) = X^{q^3+1} \in K[X].$$

Then $\tilde{F}^{-1}(X) = X^{362}$. Pick invertible affine transformations $L_1 : k^5 \to k^5$ and $L_2 : k^5 \to k^5$

as

$$L_1 = \begin{pmatrix} 0 & 1 & 1 & a & 0 \\ 0 & a & a^2 & 1 & a^2 \\ a^2 & a^2 & 1 & a & 0 \\ 0 & a^2 & a & 0 & a \\ 0 & a & 1 & a^2 & a^2 \end{pmatrix} + \begin{pmatrix} a^2 \\ a \\ a^2 \\ 1 \\ a^2 \end{pmatrix}, \quad L_2 = \begin{pmatrix} a & 0 & 1 & a^2 & a^2 \\ 0 & a & a & a^2 & a \\ 1 & a^2 & 1 & 1 & 0 \\ a & a & 1 & a & 0 \\ 1 & 1 & a & 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ a \end{pmatrix}.$$

Finally, the public key is the 5-tuple of polynomials

$$(\bar{f}_1, \ldots, \bar{f}_5) = \bar{F}(x_1, \ldots, x_5) = L_1 \circ \pi \circ \tilde{F} \circ \pi^{-1} \circ L_2(x_1, \ldots, x_5). \tag{1.4}$$

In particular,

$$\begin{aligned} (\bar{f}_1, \ldots, \bar{f}_5) \;=\; & (ax_1x_2 + a^2x_1x_3 + a^2x_1x_5 + x_1 + x_2^2 + a^2x_2x_4 + a^2x_2x_5 + a^2x_2 + \\ & a^2x_3^2 + ax_3x_4 + a^2x_3 + x_4^2 + ax_4x_5 + ax_5^2 + ax_5 + a, \\ & a^2x_1x_2 + x_1x_4 + ax_1x_5 + ax_1 + x_2^2 + x_2x_3 + x_2x_4 + ax_2 + ax_3x_4 + \\ & x_3x_5 + x_3 + a^2x_4 + x_5^2 + x_5 + a^2, \\ & x_1^2 + a^2x_1x_2 + a^2x_1x_3 + a^2x_1x_5 + a^2x_1 + ax_2^2 + x_2x_3 + x_2x_4 + a^2x_2x_5 + \\ & x_2 + x_3^2 + a^2x_3x_4 + ax_3x_5 + ax_3 + a^2x_4^2 + a^2x_4x_5 + a^2x_5^2 + a, \\ & x_1^2 + ax_1x_2 + x_1x_3 + ax_1x_4 + x_1x_5 + ax_1 + a^2x_2^2 + x_2x_3 + x_2x_4 + \\ & x_2x_5 + x_2 + x_3^2 + x_3x_5 + x_3 + ax_4^2 + ax_4x_5 + a^2x_4 + x_5^2, \\ & x_1^2 + ax_1x_2 + x_1x_3 + x_1x_4 + a^2x_1x_5 + a^2x_1 + a^2x_2x_3 + ax_2x_4 + \\ & ax_3^2 + x_3x_4 + a^2x_3x_5 + x_3 + a^2x_4^2 + x_4x_5 + ax_4 + a^2x_5^2 + x_5 + a^2). \end{aligned}$$

The private key consists of the pair of transformations L_1 and L_2. Consider the plaintext $(1, a, a^2, a^2, a) \in k^5$. Encryption gives the ciphertext

$$(a, a, a^2, a^2, a) = \bar{F}(1, a, a^2, a^2, a).$$

To decrypt, a user inverts the compositions of (1.4) by using the private key to compute

$$L_2^{-1} \circ \pi \circ \tilde{F}^{-1} \circ \pi^{-1} \circ L_1^{-1}(a, a, a^2, a^2, a)$$

and recover the plaintext $(1, a, a^2, a^2, a)$.

Clearly the above example is quite small, and should not be considered secure. The authors originally suggested in [MI88] that $1 \leq m \leq 32$, $32 \leq n \leq 64$, and $64 \leq mn$, where $q = 2^m$ is the size of k and $[K : k] = n$. In particular, they proposed an implementation that used $m = 8$ and $n = 32$. This system was thought to be secure for seven years until 1995 when Jacques Patarin revealed his linearization equations attack [Pat95], which we will discuss in Section 2.1.

1.2.3 The Minus Variant and Sflash Signature Scheme

Even though the original MI system was broken, variants have been proposed to avoid the system's weakness. Most significant is the Minus variant (MI^-) proposed by Shamir [Sha93], on which the Sflash signature scheme [PCG01, ACDG03] is based. In general, Minus can be applied to any MPKC, and simply creates a signature scheme by removing several polynomials from the public key $\bar{F}$. Given an MI system with public key $\bar{F} = (\bar{f}_1, \ldots, \bar{f}_n)$, the public key of the corresponding MI^- system is the $(n - r)$-tuple of polynomials

$$\bar{F}^- = (\bar{f}_1, \ldots, \bar{f}_{n-r}),$$

where we have deleted the last r components from $\bar{F}$. The private key is L_1 and L_2, as before.

Document signing. Given a document $(y_1, \ldots, y_{n-r}) \in k^{n-r}$, randomly choose (and keep secret) r elements of k and append them to the document, yielding the n-tuple $(y_1, \ldots, y_n) \in k^n$. Then use the private key to compute the signature (equivalent to the

decryption operation):

$$(x_1, \ldots, x_n) = L_2^{-1} \circ \pi \circ \tilde{F}^{-1} \circ \pi^{-1} \circ L_1^{-1}(y_1, \ldots, y_n). \tag{1.5}$$

Signature verification. Given the document $(y_1, \ldots, y_{n-r}) \in k^{n-r}$ and its signature $(x_1, \ldots, x_n) \in k^n$, simply use the public key to check that

$$\bar{F}^{-}(x_1, \ldots, x_n) = (y_1, \ldots, y_{n-r}).$$

The Sflash signature scheme implements this idea by using the SHA-1 hash function to compute the hash value of the document, and then manipulates the hash value to create a digital signature via (1.5). As mentioned previously, the Sflash signature system was a final selection of the NESSIE (New European Schemes for Signatures, Integrity, and Encryption) project [NES03]. Recently, Dubois et al. [DFS07, DFSS07] broke the scheme; however, Ding et al. [DYCCD07] subsequently showed how to modify the system to circumvent the attack.

1.2.4 Hidden Field Equations (HFE)

After breaking the MI cryptosystem in 1995 [Pat95], Patarin developed the second mixed field system, the Hidden Field Equations (HFE) cryptosystem, in 1996 [Pat96]. HFE generalizes MI by using a polynomial over the extension field K instead of a monomial. Even though we will no longer be able to invert the central map map by performing a simple exponentiation, inversion can still be done efficiently as long as we restrict the degree of the polynomial. Too see this, we start by considering the extension field part of the MI central map:

$$\tilde{F}(X) = X^{q^\theta + 1}.$$

Given ciphertext $(y_1, \ldots, y_n) \in k^n$, if we let $Y = \pi^{-1} \circ L_1^{-1}(y_1, \ldots, y_n) \in K$, we see from (1.3) that every preimage of Y must be a root of $\tilde{F}(X) - Y$. Hence we must factor the polynomial $X^{q^\theta+1} - Y$, which can be done efficiently as long as $q^\theta + 1$ is not too large. From

the set of preimages, say $\{X_1, \ldots, X_m\}$, we can then finish the decryption by computing

$$(x_{i1}, \ldots, x_{in}) = L_2^{-1} \circ \pi(X_i), \quad 1 \leq i \leq m.$$

If there are m preimages, we will obtain m possible plaintexts, and so we must be able to distinguish the correct one. One possible idea is to use a secure hash function to compute the hash value of a plaintext and transmit it along with the ciphertext. Then, among the set of possible plaintexts, the correct one is the one that has the matching hash value.

This "inversion" technique is easily generalized to polynomials. We use the same set-up as Section 1.2.1, and do not require k to have characteristic two. Let

$$\tilde{F}(X) = \sum_{i=0}^{r_2-1} \sum_{j=0}^{i} a_{ij} X^{q^i+q^j} + \sum_{i=0}^{r_1-1} X^{q^i} + c,$$

with $a_{ij}, b_i, c \in K$ random. The role of r_1 and r_2 is to force the degree of $\tilde{F}(X)$ to be less than a degree bound, d, which determines the complexity of the factorization step. Notice that each term of $\tilde{F}$ has q-Hamming weight at most two, so $\pi \circ \tilde{F}$ is in fact a quadratic system in $k[x_1, \ldots, x_n]^n$. The public key of an HFE cryptosystem is the polynomial map $\bar{F}$ given by

$$\bar{F} = L_1 \circ \pi \circ \tilde{F} \circ \pi^{-1} \circ L_2,$$

where $L_1 : k^n \to k^n$ and $L_2 : k^n \to k^n$ are invertible affine transformations that, along with the coefficients of the map $\tilde{F}$, function as the private key.

Encryption. Given plaintext $(x_1, \ldots, x_n) \in k^n$, the ciphertext is

$$(y_1, \ldots, y_n) = \bar{F}(x_1, \ldots, x_n).$$

Decryption. Given ciphertext $(y_1, \ldots, y_n) \in k^n$, the plaintext is recovered by

1. Computing $Y = \pi^{-1} \circ L_1^{-1}(y_1, \ldots, y_n) \in K$.

2. Factoring (see [VG03]) the univariate polynomial $\tilde{F}(X) - Y$ to find the set of roots $\{X_1, \ldots, X_m\} \subset K$. The complexity of this step depends on d, the degree of $\tilde{F}$.

3. Computing $(x_{i1}, \ldots, x_{in}) = L_2^{-1} \circ \pi(X_i)$, $1 \leq i \leq m$, and deciding which one is the actual plaintext (this distinguishing step may vary in different implementations).

The original recommended parameters for HFE were $q = 2$, $n = 128$, and $r_2 = 13$. However, the system was broken by the minrank attack of Kipnis and Shamir [KS99], with later improvements by Courtois [Cou01]. In 2003, Faugére and Joux [FJ03] broke HFE using only Gröbner basis techniques. Since HFE is just a generalization of MI using a polynomial instead of a monomial, an interesting open question is whether the attack of Dubois et al. [DFSS07] on MI can be generalized to an attack on HFE.

Similar to the situation with MI, several variants have been proposed [Pat96] including HFE$^-$ (a signature scheme similar to MI$^-$) and HFEv (a signature scheme that combines HFE with the Oil-Vinegar concept of Section 1.2.6 by introducing vinegar variables). Quartz, which combines these two ideas, has not yet been broken. Baena et al. [BCD08] have recently proposed the Square-Vinegar signature scheme, which improves upon HFEv$^-$ by changing the field characteristic and reducing the degree of the central map. Subsequently, Chen et al. [CCDWY08] proposed an efficient encryption scheme that modifies the HFE system over fields of odd characteristic.

1.2.5 Triangular Encryption Schemes

Having discussed the mixed field systems, we now turn our focus to single field systems. The new framework we propose in Section 1.3 in fact combines ideas from two single field systems: Triangular and Oil-Vinegar systems.

Triangular maps make up one family of easily inverted multivariate maps. A trian-

gular map $F : k^n \to k^n$ has the form:

$$F(x_1, \ldots, x_n) = \begin{pmatrix} x_1 \\ x_2 + g_2(x_1) \\ \vdots \\ x_{n-1} + g_{n-1}(x_1, x_2, \ldots, x_{n-2}) \\ x_n + g_n(x_1, x_2, \ldots, x_{n-2}, x_{n-1}) \end{pmatrix}^T,$$

where each $g_i \in k[x_1, \ldots, x_n]$ is quadratic. Given $(y_1, \ldots, y_n) \in k^n$, it is easy to find $(x_1, \ldots, x_n) \in k^n$ such that $F(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ by iteratively solving for each component, i.e.

$$\begin{aligned} x_1 &= y_1, \\ x_2 &= y_2 - g_2(x_1), \\ &\vdots \\ x_{n-1} &= y_{n-1} - g_{n-1}(x_1, x_2, \ldots, x_{n-1}), \\ x_n &= y_n - g_n(x_1, x_2, \ldots, x_{n-2}, x_{n-1}). \end{aligned}$$

Triangular maps have the following important connection to algebraic geometry: taking the closure of the set of triangular maps under composition yields a group known as the group of tame transformations. In general an invertible polynomial map may not be tame. This is the subject of the Nagata problem [Nag72]. The famous Jacobian conjecture addresses the question of when a polynomial map is invertible: a polynomial map $F : \mathbb{C}^n \to \mathbb{C}^n$ is invertible if and only if the determinant of the Jacobian of F is nonzero. This problem has been studied by many people and is still wide open.

Early attempts to create triangular systems were unsuccessful, with Fell and Diffie declaring that by using their design, "there seems, however, to be no way to build such a system that is both secure and has a public key of practical size" [FD85]. Later systems of Tsujii et al. [TIFKM88] and Shamir [Sha93] were also broken. Particularly notable among the attacks are the linear algebra attacks of Coppersmith et al. [CSV93, CSV97].

T.T. Moh, who has much experience working with the Jacobian conjecture, proposed

a triangular encryption scheme in 1999 [Moh99]. Notice that because the transformations L_1 and L_2 are linear, they cannot hide the linearity of the first equation in F, so a system cannot be secure if it simply has a triangular map as its central map. Composing triangular maps can solve this problem; however, composition in general makes the degree of the map grow very quickly, which is problematic since central maps should be quadratic. Moh cleverly created a quadratic map by composing two triangular maps, one having degree eight, through the use of injections (basically adding new variables which are set to zero.) Unfortunately, Moh's original system is susceptible to a minrank attack [GC00], and later modified systems [MCY04, Moh07] are vulnerable to linearization equation attacks [NJHD07]. In Section 2.2.3, we will present Moh's original system in the context of the minrank attack and give a detailed description of the attack.

Another idea that attempted to avoid the problem of the linearity of the first polynomial (and the simplicity of the next few polynomials) was the TTS system [YC04], which simply discarded the initial polynomials and used the remaining system to create a signature scheme. Ding et al. showed the system was insecure [DSY06], but Yang and Chen have proposed another TTS system that is yet to be broken [YC05].

Wang et al. [WC04] proposed a generalization of triangular maps that they called tractable rational maps. They define a tractable rational map $F : k^n \to k^n$ as having the form:

$$F(x_1, \ldots, x_n) = \begin{pmatrix} r_1(x_1) \\ r_2(x_2) \cdot \frac{p_2(x_1)}{q_2(x_1)} + \frac{f_2(x_1)}{g_2(x_1)} \\ \vdots \\ r_{n-1}(x_{n-1}) \cdot \frac{p_{n-1}(x_1,x_2,\ldots,x_{n-2})}{q_{n-1}(x_1,x_2,\ldots,x_{n-2})} + \frac{f_{n-1}(x_1,x_2,\ldots,x_{n-2})}{g_{n-1}(x_1,x_2,\ldots,x_{n-2})} \\ r_n(x_n) \cdot \frac{p_n(x_1,x_2,\ldots,x_{n-2},x_{n-1})}{q_n(x_1,x_2,\ldots,x_{n-2},x_{n-1})} + \frac{f_n(x_1,x_2,\ldots,x_{n-2},x_{n-1})}{g_n(x_1,x_2,\ldots,x_{n-2},x_{n-1})} \end{pmatrix}^T,$$

where p_i, q_i, f_i, and g_i are polynomials, and r_i is a permutation polynomial over k. As in the triangular case, we can find preimages by iteratively solving for each component. However,

notice that the rational functions limit the invertibility of F to the set

$$\{(x_1, \ldots, x_n) \in k^n : (p_i q_i g_i)(x_1, \ldots, x_n) \neq 0 \text{ for } i = 2, \ldots, n\}.$$

Rather than composing two maps as Moh did, they introduce the idea of using basic injections and projections to effectively discard the weak top part of the triangle while still being able to compute unique preimages by exploiting other structure. Although the initial system was broken [JJMR05], the authors showed how to avoid the problem [WC06], and later, using a similar structure, Wang et al. [WYHL06] proposed the MFE cryptosystem, which we will discuss in Section 1.3.2.

1.2.6 Oil-Vinegar Systems

The second type of single field MPKC that is interesting for our purposes is called an Oil-Vinegar signature scheme. Patarin's oil-vinegar polynomial scheme [Pat97] finds its roots in his linearization equation attack [Pat95] on the Matsumoto-Imai cryptosystem. An *oil-vinegar polynomial* $f \in k[\check{x}_1, \ldots, \check{x}_v, x_1, \ldots, x_o]$ has the form:

$$f = \sum_{i=1}^{o} \sum_{j=1}^{v} a_{ij} x_i \check{x}_j + \sum_{i=1}^{v} \sum_{j=1}^{v} b_{ij} \check{x}_i \check{x}_j + \sum_{i=1}^{o} c_i x_i + \sum_{j=1}^{v} d_j \check{x}_j + e,$$

where $a_{ij}, b_{ij}, c_i, d_j, e \in k$. The variables $x_1, \ldots, x_o$ are called *oil variables* and the variables $\check{x}_1, \ldots, \check{x}_v$ are called *vinegar variables*. The important property of these polynomials is that they have no $x_i x_j$ terms (i.e. there are no terms quadratic in the oil variables). So, if we substitute v field values for the vinegar variables, f becomes linear in the oil variables. Basic oil-vinegar systems may be used for signatures as follows: let the private key be given by $F = (f_1, \ldots, f_o)$, where each f_i is a random oil-vinegar polynomial, along with an invertible affine transformation $L : k^{o+v} \to k^{o+v}$. The public key is the polynomial map $\bar{F}$ given by

$$\bar{F} = F \circ L. \tag{1.6}$$

Document signing. Given a document $(y_1, \ldots, y_o) \in k^o$, choose $(\check{x}'_1, \ldots, \check{x}'_v) \in k^v$ at random and attempt to compute $(x_1, \ldots, x_o)$ that satisfies the linear system

$$F(\check{x}'_1, \ldots, \check{x}'_v, x_1, \ldots, x_o) = (y_1, \ldots, y_o).$$

A solution will exist as long as the system is nonsingular, which will be the case with probability approximately $1 - \frac{1}{q}$. (Recall that a random $o \times o$ matrix over a finite field with q elements will be invertible with probability $\left(1 - \frac{1}{q}\right) \ldots \left(1 - \frac{1}{q^o}\right)$, and this expression is dominated by the first term when q is large.) If the resulting matrix for the linear system is singular, simply choose a different $(\check{x}'_1, \ldots, \check{x}'_v) \in k^v$ and try again. With high probability, one should be able to compute a solution $(x'_1, \ldots, x'_o) \in k^o$ in very few attempts. Finally, the signature is

$$(z_1, \ldots, z_{o+v}) = L^{-1}(\check{x}'_1, \ldots, \check{x}'_v, x'_1, \ldots, x'_o).$$

Signature verification. Given document $(y_1, \ldots, y_o) \in k^o$ and signature $(z_1, \ldots, z_{o+v}) \in k^{o+v}$, simply use the public key to check that

$$\bar{F}(z_1, \ldots, z_{o+v}) = (y_1, \ldots, y_o).$$

Kipnis and Shamir [KS98] first broke the system in the case where $o = v$ using the observation that the matrices corresponding to the quadratic forms of the private key have a special form (i.e. a large block of zeros). This allows attackers to separate the oil and vinegar variables and generate an equivalent system that can be used to create forgeries. Subsequently, Kipnis et al. [KPG99] proposed an unbalanced ($o < v$) scheme, extended the original attack to this case, and gave parameters they believed would be good for a secure system. Later, Ding and Schmidt proposed a more efficient "multi-layer" unbalanced oil-vinegar scheme, called Rainbow [DS05].

However, these are signature schemes, and our goal is to build a secure cryptosystem.

1.3 New Framework: Combining Triangular and Oil-Vinegar Schemes

Recall that the difficulty in creating a secure triangular system is that it is hard to hide the triangular structure, especially the top equations. Though attempts have been made to use high degree "lock polynomials" through composition with another triangular map ([Moh99], [MCY04], [Moh07]), these have been shown to be insecure ([GC00], [DS03], [NJHD07]). However, this method is not the only way to achieve the necessary hiding of the triangular structure. We propose a new way of introducing lock polynomials to completely hide the triangular system by combining the triangular system with a series of oil-vinegar systems.

Figure 1.1: Combining Triangular and Oil-Vinegar Systems

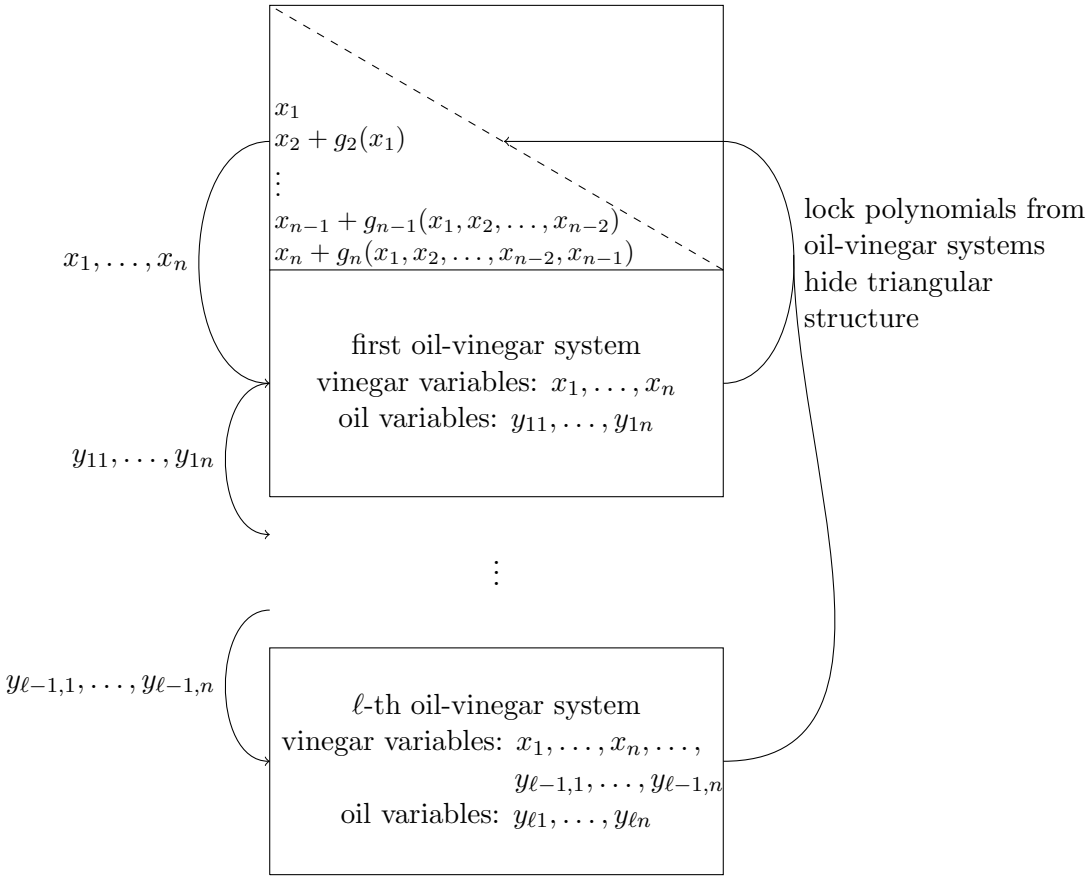


Figure 1.1 presents an informal description of the framework. By combining triangular and oil-vinegar systems, we can eliminate the individual deficiencies of each type of system. We avoid the security weaknesses of the triangular system by using the oil-vinegar systems to construct lock polynomials that will completely hide the triangular structure. Furthermore, by using the triangular system's variables as an initial set of vinegar variables, we build an encryption scheme that uses oil-vinegar systems, and are no longer limited to using them only for digital signature schemes.

1.3.1 A general framework

We now develop the technical details of the framework. Let k be a finite field with q elements, and let $\mathbb{F}$ be a degree d extension of k. Notice that although we are working in an extension field, our polynomials will be multivariate, as opposed to the univariate polynomials used to build mixed field systems such as Matsumoto-Imai and HFE. Our approach might be called an "intermediate" (or as Wang et al. [WYHL06] say, "medium") field construction.

Intermediate field construction. In particular, fix a basis $\{\alpha_1, \ldots, \alpha_d\}$ of $\mathbb{F}$ over k. We identify $\mathbb{F}$ with k^d, via the natural map $\pi : \mathbb{F} \to k^d$ given by

$$\pi(a_1\alpha_1 + \cdots + a_d\alpha_d) = (a_1, \ldots, a_d).$$

Similarly we can view a polynomial $f \in \mathbb{F}[X_1, \ldots, X_n]$ component-wise over k by writing $X_i = x_{i1}\alpha_1 + \cdots + x_{id}\alpha_d$, and then $f = f_1\alpha_1 + \cdots + f_d\alpha_d$ with $f_i \in k[x_{11}, \ldots, x_{nd}]$. Finally, we can extend π to the polynomial rings via

$$f \in \mathbb{F}[X_1, \ldots, X_n] \mapsto (f_1, \ldots, f_d) \in k[x_{11}, \ldots, x_{nd}]^d.$$

Although this set-up looks similar to that of Section 1.2.1, notice that we are working with a multivariate polynomial ring over a degree d intermediate extension as opposed to a

univariate polynomial ring over a degree n extension.

As mentioned above, the public key will be given by $\bar{F} = L_1 \circ F \circ L_2$, where L_1 and L_2 are invertible affine transformations. Suppose $(Y_1, \ldots, Y_n) = \phi(X_1, \ldots, X_n)$ is a triangular system when viewed component-wise over the base field k:

$$\begin{aligned} Y_1 &= X_1 + \phi_1(X_1) \\ Y_2 &= X_2 + \phi_2(X_1, X_2) \\ &\vdots \\ Y_n &= X_n + \phi_n(X_1, \ldots, X_n). \end{aligned} \tag{1.7}$$

More specifically, viewing each polynomial as having d components:

$$Y_i = \begin{pmatrix} Y_{i1} \\ Y_{i2} \\ \vdots \\ Y_{id} \end{pmatrix}^T = \begin{pmatrix} x_{i1} + \phi_{i1}(x_{11}, \ldots, x_{i-1,d}) \\ x_{i2} + \phi_{i2}(x_{11}, \ldots, x_{i-1,d}, x_{i1}) \\ \vdots \\ x_{id} + \phi_{id}(x_{11}, \ldots, x_{i-1,d}, x_{i1}, \ldots, x_{i,d-1}) \end{pmatrix}^T . \tag{1.8}$$

where each ϕ_{ij} is quadratic. To invert, we solve iteratively for $x_{11}, \ldots, x_{1d}, \ldots, x_{n1}, \ldots, x_{nd}$.

Oil-Vinegar layers. Similar to Rainbow [DS05], we will define several, say ℓ, layers of oil-vinegar systems. However, in our framework, we make the following relaxation: rather than requiring an oil-vinegar system with o oil variables and v vinegar variables to have o oil-vinegar polynomials, we allow more general systems, with t ($\geq o$) polynomials, as long as at least o of them are true oil-vinegar polynomials.

We now build the central map $F : \mathbb{F}^{n+\ell o} \to \mathbb{F}^{n+\ell t}$. Let $\{X_1, \ldots, X_n\}$ be the initial set of vinegar variables, and define the first oil-vinegar system:

$$Y_{n+i} = f_{n+i}(X_1, \ldots, X_n, X_{n+1}, \ldots, X_{n+o}), \quad 1 \leq i \leq t,$$

where $X_{n+1}, \ldots, X_{n+o}$ are the oil variables. In the next layer,

$$Y_{n+i} = f_{n+i}(X_1, \ldots, X_{n+o}, X_{n+o+1}, \ldots, X_{n+2o}), \quad t+1 \leq i \leq 2t,$$

$\{X_1, \ldots, X_{n+o}\}$ is the set of vinegar variables, and $\{X_{n+o+1}, \ldots, X_{n+2o}\}$ is the set of oil variables. Similarly, we create the other layers, ending with the ℓ-th layer,

$$Y_{n+i} = f_{n+i}(X_1, \ldots, X_{n+(\ell-1)o}, X_{n+(\ell-1)o+1}, \ldots, X_{n+\ell o}), \quad (\ell-1)t+1 \leq i \leq \ell t,$$

where $\{X_1, \ldots, X_{n+(\ell-1)o}\}$ is the set of vinegar variables, and $\{X_{n+(\ell-1)o+1}, \ldots, X_{n+\ell o}\}$ is the set of oil variables. (Here, we are assuming that each oil-vinegar system has t polynomials. We could be more general by letting the i-th system have t_i polynomials.)

We will use these oil-vinegar systems to completely mask the triangular system (1.7). Decryption will be done in two stages:

1. Unmask the triangular system and solve it for the initial set of vinegar variables.

2. Sequentially solve the oil-vinegar systems for the oil-variables.

Lock polynomials. The question is then, how can we use the oil-vinegar polynomials to mask the triangular system? The oil-vinegar polynomials will of course be quadratic, and we won't achieve much by simply adding linear combinations of them to the triangular polynomials (this is in fact what L_1 does), so we need to examine nonlinear combinations. However, any nonlinear polynomial in $\mathbb{F}[Y_{n+1}, \ldots, Y_{n+lt}]$ will, in general, have degree at least four as a polynomial in $\mathbb{F}[X_1, \ldots, X_{n+lo}]$.

Suppose we can define the f_i in each oil-vinegar system in such a way that there exists nonlinear polynomials

$$g_i \in \mathbb{F}[Y_{n+(i-1)t+1}, \ldots, Y_{n+it}], \quad 1 \leq i \leq \ell, \tag{1.9}$$

such that each $g_i(f_{n+(i-1)t+1}, \ldots, f_{n+it})$, $1 \leq i \leq \ell$, factors as a product of quadratic factors

in $\mathbb{F}[X_1, \ldots, X_{n+\ell o}]$. If we have n such quadratic factors, say $\psi_1, \ldots, \psi_n$, then we can use them as lock polynomials by adding one factor to each Y_i in the triangular system (1.7). That is, let

$$Y_i = f_i(X_1, \ldots, X_{n+\ell o}) = X_i + \phi_i(X_1, \ldots, X_i) + \psi_i(X_1, \ldots, X_{n+\ell o}) \quad 1 \leq i \leq n. \tag{1.10}$$

(Even more generally, we could add n_i quadratic factors to each Y_i:

$$Y_i = f_i(X_1, \ldots, X_{n+lo}) = X_i + \phi_i(X_1, \ldots, X_i) + \sum_{j=1}^{n_i} \psi_{ij}, \quad 1 \leq i \leq n,$$

so we would need a total of $\sum_{i=1}^{n} n_i$ factors.)

Appending the oil-vinegar systems to the updated triangular system gives our central map:

$$F(X_1, \ldots, X_{n+\ell o}) = (f_1, \ldots, f_{n+\ell t}).$$

Notice that as long as at least one of the variables $X_{i+1}, \ldots, X_{n+\ell o}$ are present in each ψ_i, the triangular structure of the first n equations is destroyed. Also, we make the observation that we can shrink the size of the triangular system, and hence the number of necessary quadratic factors, to $n-1$, if one of the ψ_i can be viewed as an oil-vinegar polynomial in $X_1, \ldots, X_n$ with a single oil variable X_n.

Now, in order to unmask and decrypt the triangular part, we must be able to compute the values of the ψ_i. Say there exist functions h_i in the rational function field over $\mathbb{F}$ in ℓ variables such that

$$h_i(g_1, \ldots, g_\ell) = \psi_i, \quad 1 \leq i \leq n.$$

Then during decryption, we simply use L_1^{-1} to compute $Y_{n+1}, \ldots, Y_{n+\ell t}$ from the ciphertext, substitute the values into $g_1, \ldots, g_\ell$, then evaluate each h_i, and substitute for each ψ_i in (1.10), restoring the original triangular structure. There is actually much freedom in the h_i

since we can view them as functions of the transformed ciphertext values $Y_{n+1}, \ldots, Y_{n+\ell t} \in \mathbb{F}$, so we are not limited to polynomials, but may also compute inverses and roots (depending on the characteristic of the field). However, we must note that computing inverses will require that the involved Y_i's are nonzero.

Framework summary. So, our proposed framework, which is simply a masked triangular system combined with a series of oil-vinegar systems, requires the existence of two crucial sets of functions:

- Polynomials $f_{n+(i-1)t+j} \in \mathbb{F}[X_1, \ldots, X_{n+io}]$ and $g_i \in \mathbb{F}[Y_{n+(i-1)t+1}, \ldots, Y_{n+it}]$ such that each $g_i(f_{n+(i-1)t+1}, \ldots, f_{n+it})$ factors into quadratic polynomials (the ψ_i's) in $\mathbb{F}[X_1, \ldots, X_{n+io}]$.
- Rational functions h_i which, upon evaluation at the transformed ciphertext values $(Y_{n+1}, \ldots, Y_{n+\ell t}) \in \mathbb{F}^{\ell t}$, yield the value of ψ_i. We require that there must not exist linear relationships involving the ψ_i and Y_j.

Notice that masking the triangular system and adding oil-vinegar polynomials has introduced two possibilities for decryption failure:

- We may not be able to compute inverses needed when evaluating the h_i.
- For any of the oil-vinegar systems, after we have computed the values of the vinegar variables, the remaining linear system in the oil variables may not be solvable.

Obviously, any practical cryptosystem must keep decryption failures to a minimum, so for any implementation, the probability of either of the above two problems occurring must be small. One possible solution is to make use of the embedding ($\nearrow$) modifier for MPKCs, first introduced in [DWY07].

1.3.2 Example: MFE cryptosystem

The MFE cryptosystem [WYHL06], although built using tractable rational maps, can be viewed (with slight modification) as an instance of our new framework. In fact, it

was this system that provided the inspiration to try to develop a more general system that avoids the known flaws of MFE.

We now present the central map of the MFE system in the context of our proposed framework, working only with polynomials over the extension field for ease of exposition. Let $\mathbb{F}$ have characteristic two. MFE's central map will be $F : \mathbb{F}^{12} \to \mathbb{F}^{15}$, where there are three oil-vinegar systems, given by $(Y_4, \ldots, Y_7), (Y_8, \ldots, Y_{11})$, and $(Y_{12}, \ldots, Y_{15})$.

To motivate the definition of the functions g_i and ψ_i, define the following matrices:

$$M_1 = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}, \quad M_2 = \begin{pmatrix} X_5 & X_6 \\ X_7 & X_8 \end{pmatrix}, \quad M_3 = \begin{pmatrix} X_9 & X_{10} \\ X_{11} & X_{12} \end{pmatrix},$$

and

$$Z_3 = M_1 M_2 = \begin{pmatrix} Y_4 & Y_5 \\ Y_6 & Y_7 \end{pmatrix}, \quad Z_2 = M_1 M_3 = \begin{pmatrix} Y_8 & Y_9 \\ Y_{10} & Y_{11} \end{pmatrix},$$

$$Z_1 = M_2^T M_3 = \begin{pmatrix} Y_{12} & Y_{13} \\ Y_{14} & Y_{15} \end{pmatrix}.$$

The g_i and ψ_i come from relationships between determinants. First notice that $\det(Z_3) = \det(M_1)\det(M_2)$, so letting $g_1 = \det(Z_3)$, $\psi_3 = \det(M_1)$, and $\psi_1 = \det(M_2)$, we have

$$g_1 = Y_4Y_7 + Y_5Y_6 = (X_1X_4 + X_2X_3)(X_5X_8 + X_6X_7) = \psi_3\psi_1. \tag{1.11}$$

Similarly $\det(Z_2) = \det(M_1)\det(M_3)$ and $\det(Z_1) = \det(M_2)\det(M_3)$ give

$$\begin{aligned} g_2 &= Y_8Y_{11} + Y_9Y_{10} &&= (X_1X_4 + X_2X_3)(X_9X_{12} + X_{10}X_{11}) &&= \psi_3\psi_2, \\ g_3 &= Y_{12}Y_{15} + Y_{13}Y_{14} &&= (X_5X_8 + X_6X_7)(X_9X_{12} + X_{10}X_{11}) &&= \psi_1\psi_2. \end{aligned}$$

Also,

$$\begin{aligned} h_1 &= (g_1g_3g_2^{-1})^{1/2} &&= ((\psi_3\psi_1)(\psi_1\psi_2)(\psi_3\psi_2)^{-1})^{1/2} &&= \psi_1, \\ h_2 &= g_3h_1^{-1} &&&&= \psi_2, \\ h_3 &= g_1h_1^{-1} &&&&= \psi_3. \end{aligned} \tag{1.12}$$

Finally, the central map $F : \mathbb{F}^{12} \to \mathbb{F}^{15}$ is given by

$$\begin{aligned}
Y_1 &= X_1 + \phi_1(X_1) + \psi_1 \\
Y_2 &= X_2 + \phi_2(X_1, X_2) + \psi_2 \\
Y_3 &= X_3 + \phi_3(X_1, X_2, X_3) + \psi_3 \\
Y_4 &= X_1X_5 + X_2X_7 & Y_5 &= X_1X_6 + X_2X_8 \\
Y_6 &= X_3X_5 + X_4X_7 & Y_7 &= X_3X_6 + X_4X_8 \\
Y_8 &= X_1X_9 + X_2X_{11} & Y_9 &= X_1X_{10} + X_2X_{12} \\
Y_{10} &= X_3X_9 + X_4X_{11} & Y_{11} &= X_3X_{10} + X_4X_{12} \\
Y_{12} &= X_5X_9 + X_7X_{11} & Y_{13} &= X_5X_{10} + X_7X_{12} \\
Y_{14} &= X_6X_9 + X_8X_{11} & Y_{15} &= X_6X_{10} + X_8X_{12}
\end{aligned}$$

The public key is the polynomial map $\bar{F} : \mathbb{F}^{12} \to \mathbb{F}^{15}$ given by

$$\bar{F} = L_1 \circ F \circ L_2,$$

where $L_1 : \mathbb{F}^{15} \to \mathbb{F}^{15}$ and $L_2 : \mathbb{F}^{12} \to \mathbb{F}^{12}$ are random invertible affine transformations that function as the private key.

Notice that the framework definition suggests that MFE's central map should be $F : \mathbb{F}^{16} \to \mathbb{F}^{16}$ (since $n = 4, o = t = 4$, and $\ell = 3$), however, it is given as $F : \mathbb{F}^{12} \to \mathbb{F}^{15}$. This is because the third oil-vinegar system does not utilize any new input variables, therefore shrinking the number of input variables by four. Also, ψ_3 is actually an oil-vinegar polynomial in $X_1, \ldots, X_4$ with single oil variable X_4, so the triangular system only needs three polynomials.

Encryption. Given plaintext $(X'_1, \ldots, X'_{12}) \in \mathbb{F}^{12}$, the ciphertext is

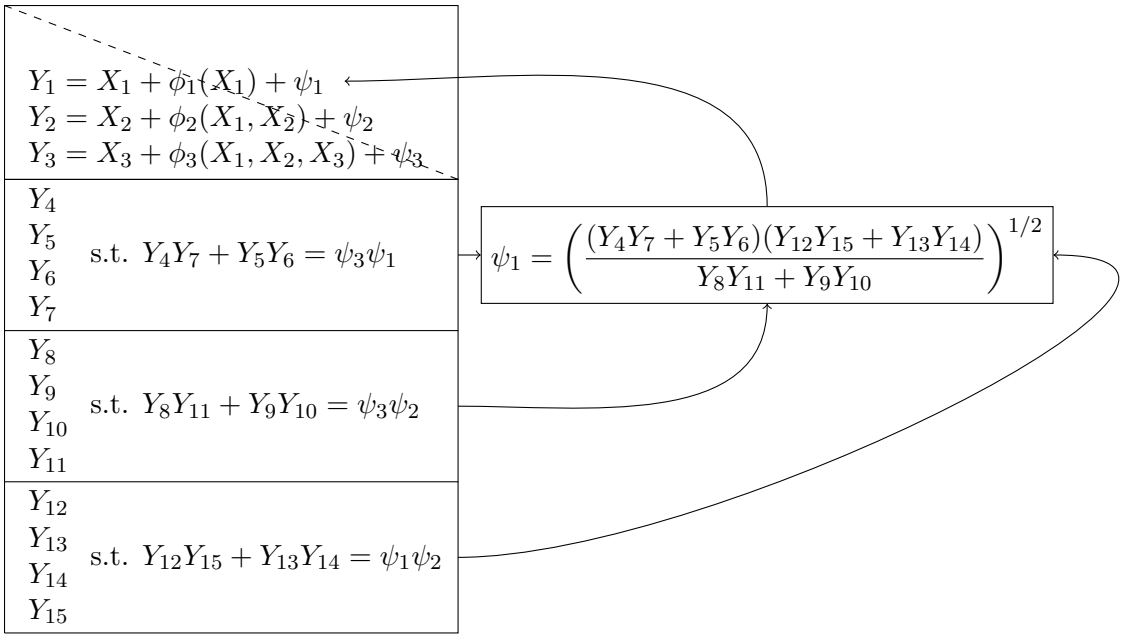
$$(Y'_1, \ldots, Y'_{15}) = \bar{F}(X'_1, \ldots, X'_{12}).$$

Decryption. Given ciphertext $(Y'_1, \ldots, Y'_{15}) \in \mathbb{F}^{12}$, the plaintext is recovered as follows. First, calculate $(Y_1, \ldots, Y_{15}) = L_1^{-1}(Y'_1, \ldots, Y'_{15})$, then use h_1, h_2, and h_3 to calculate ψ_1, ψ_2, and ψ_3. Adding these to Y_1, Y_2, and Y_3 respectively, restores the triangular structure of the first three polynomials and enables us to recover X_1, X_2, and X_3. Figure 1.2 describes the process of computing ψ_1 and restoring the triangular structure to the equation for Y_1. We then use $\psi_3 = X_1X_4 + X_2X_3$ to compute X_4. Using the values of the initial oil variables $X_1, \ldots, X_4$, we solve in sequence the first two oil-vinegar systems to recover the values of the remaining variables, $X_5, \ldots, X_{12}$. Finally, we compute the plaintext

$$(X'_1, \ldots, X'_{12}) = L_2^{-1}(X_1, \ldots, X_{12}).$$

(Note that the last system is not used in decryption, but is necessary for the g_i and ψ_i polynomials.)

Figure 1.2: MFE Decryption



Weakness of MFE. The creators of the MFE specifically defined $Z_1 = M_2^T M_3$ instead of $Z_1 = M_2 M_3$. Otherwise linearization equations (equations linear in both X and Y) exist. For instance, the relationship

$$Z_3 M_3 = M_1 Z_1 \ (= M_1 M_2 M_3)$$

yields four linearization equations.

However, Ding et al. [DHNW07] showed that other types of linearization equations still exist, called high order linearization equations, where the degree in Y is higher than one. Their second order linearization equations are derived by examining $M_3 M_3^* M_1^* M_1 M_2$, where M_i^* is the adjoint of M_i. In particular,

$$M_3 M_3^* M_1^* M_1 M_2 = M_3 (M_1 M_3)^* (M_1 M_2) = M_3 Z_2^* Z_3$$

and

$$M_3 M_3^* M_1^* M_1 M_2 = \det(M_3) \det(M_1) M_2 = \det(Z_2) M_2,$$

therefore,

$$M_3 Z_2^* Z_3 = \det(Z_2) M_2.$$

This equation gives four equations that are linear in X and quadratic in Y. They show that enough of these second order linearization equations exist to break MFE.

We observe that in both cases, the linearization equation attacks result from the fact that the Z matrices are defined as a product of 2×2 matrices. So, while the determinant relationships are crucial in giving the nice expressions for the g_i and ψ_i, the underlying matrix relationships are the critical weakness of the system.

1.3.3 Polynomial Identities

Although the original form of MFE has been broken, our general framework may be used to create other systems. For instance, notice that each of three g_i in MFE can be

viewed as the right hand side of the Diophantine equation (over a polynomial ring):

$$AB = CD + EF, \tag{1.13}$$

where C, D, E, F are oil-vinegar polynomials in 8 variables. In particular, for $\psi_3\psi_1 = g_1$ in MFE, we have

$$(X_1X_4 + X_2X_3)(X_5X_8 + X_6X_7) = Y_4Y_7 + Y_5Y_6,$$

where $Y_i \in \mathbb{F}[X_1, \ldots, X_8]$. So, solutions to equations like (1.13) will possibly yield families of cryptosystems in our proposed framework. This is in fact the case, and in Chapter 4 we will construct a cryptosystem based on a Diophantine equation of the form

$$AB = CD + EF + GH + IJ + KL, \tag{1.14}$$

where $C, D, \ldots, J$ are oil-vinegar polynomials in 8 oil and 8 vinegar variables, and there are no restrictions on K or L. In the context of our framework, we rewrite (1.14) as

$$\psi_1\psi_2 = f_1f_2 + \cdots + f_9f_{10}, \tag{1.15}$$

where each polynomial has degree two, and

1. $\psi_1 \in \mathbb{F}[X_1, \ldots, X_n]$, $\psi_2 \in \mathbb{F}[Y_1, \ldots, Y_n]$,
2. $f_i \in \mathbb{F}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$, $1 \leq i \leq 8$, are oil-vinegar polynomials, and
3. $f_i \in \mathbb{F}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$, $i = 9, 10$.

Solving general identities of this form is the subject of Chapter 3.

1.3.4 Cremona Transformations

Solutions of identities like (1.15) supply the first necessary set of functions required by the framework (i.e. polynomials that factor into the quadratic ψ_i's). Recall that the

framework also requires the existence of rational functions h_i, which, upon evaluation at the transformed ciphertext values yield the value of ψ_i.

Cremona transformations [Kli72, GH78] from algebraic geometry are one possible candidate for the necessary rational functions, and in fact have been used previously in MPKC (by MFE and also in the construction of the ℓ-IC family of cryptosystems). Consider the following important example.

Example 1.3.1. Let (x_0, x_1, x_2) be homogeneous coordinates of the projective plane $\mathbb{P}^2$. Define the quadratic map τ by

$$(x_0, x_1, x_2) \stackrel{\tau}{\longmapsto} (x_0', x_1', x_2') = (x_1x_2, x_0x_2, x_0x_1).$$

Notice that τ is invertible on $\{(x_0, x_1, x_2) : x_0x_1x_2 \neq 0\}$ and the inverse map is given by

$$(x_0', x_1', x_2') \stackrel{\tau^{-1}}{\longmapsto} (x_1'x_2', x_0'x_2', x_0'x_1')$$

since

$$\begin{aligned} \tau^{-1} \circ \tau(x_0, x_1, x_2) &= \tau^{-1}(x_1x_2, x_0x_2, x_0x_1) \\ &= (x_0x_2x_0x_1, x_1x_2x_0x_1, x_1x_2x_0x_2) \\ &= x_0x_1x_2(x_0, x_1, x_2) \\ &= (x_0, x_1, x_2). \end{aligned}$$

Affine transformation. If we move to three-dimensional affine space, the inverse map becomes slightly more complicated. Let $(x_0, x_1, x_2) \in k^3$, and define τ in the same way, i.e.

$$(x_0, x_1, x_2) \stackrel{\tau}{\longmapsto} (x_0', x_1', x_2') = (x_1x_2, x_0x_2, x_0x_1).$$

In this case, we no longer benefit from the equivalence of projective points, but τ is still invertible on $\{(x_0, x_1, x_2) : x_0x_1x_2 \neq 0\}$ as long as square roots are possible in k. We define

τ^{-1} by

$$(x_0', x_1', x_2') \stackrel{\tau^{-1}}{\longmapsto} \left(\left(\frac{x_1' x_2'}{x_0'} \right)^{1/2}, \left(\frac{x_0' x_2'}{x_1'} \right)^{1/2}, \left(\frac{x_0' x_1'}{x_2'} \right)^{1/2} \right) = (x_0, x_1, x_2).$$

This map is precisely the map used to recover the values of the ψ_i in MFE:

$$(g_2, g_1, g_3) = (\psi_2\psi_3, \psi_1\psi_3, \psi_1\psi_2) \stackrel{\tau^{-1}}{\longmapsto} (\psi_1, \psi_2, \psi_3), \tag{1.16}$$

where the i-th component of τ^{-1} is in fact h_i as defined in (1.12).

Chains of oil-vinegar systems. We will use the basic structure of (1.16) in the construction of the cryptosystem of Chapter 4, extending it slightly by adding more oil-vinegar systems. To illustrate this idea, suppose we append a fourth oil-vinegar system $(Y_{16}, Y_{17}, Y_{18}, Y_{19})$ to MFE that introduces new oil variables $X_{13}, X_{14}, X_{15}, X_{16}$, and satisfies

$$g_4 = Y_{16}Y_{19} + Y_{17}Y_{18} = \psi_1\psi_4,$$

where the vinegar variables of this system are the variables of ψ_1, i.e. X_5, X_6, X_7, X_8. Then given the values of $Y_{16}, \ldots, Y_{19}$, we can compute the value of ψ_4 by using τ^{-1} to compute ψ_1, and setting

$$h_4 = \frac{g_4}{\psi_1} \quad (= \psi_4).$$

We can also easily solve for the values of the oil variables. This process can be extended in any number of ways. For one example, consider Figure 1.3, where we have appended three additional oil-vinegar systems:

system	oil variables	vinegar variables
4	$X_{13}, X_{14}, X_{15}, X_{16}$	X_5, X_6, X_7, X_8
5	$X_{17}, X_{18}, X_{19}, X_{20}$	$X_9, X_{10}, X_{11}, X_{12}$
6	$X_{21}, X_{22}, X_{23}, X_{24}$	X_1, X_2, X_3, X_4

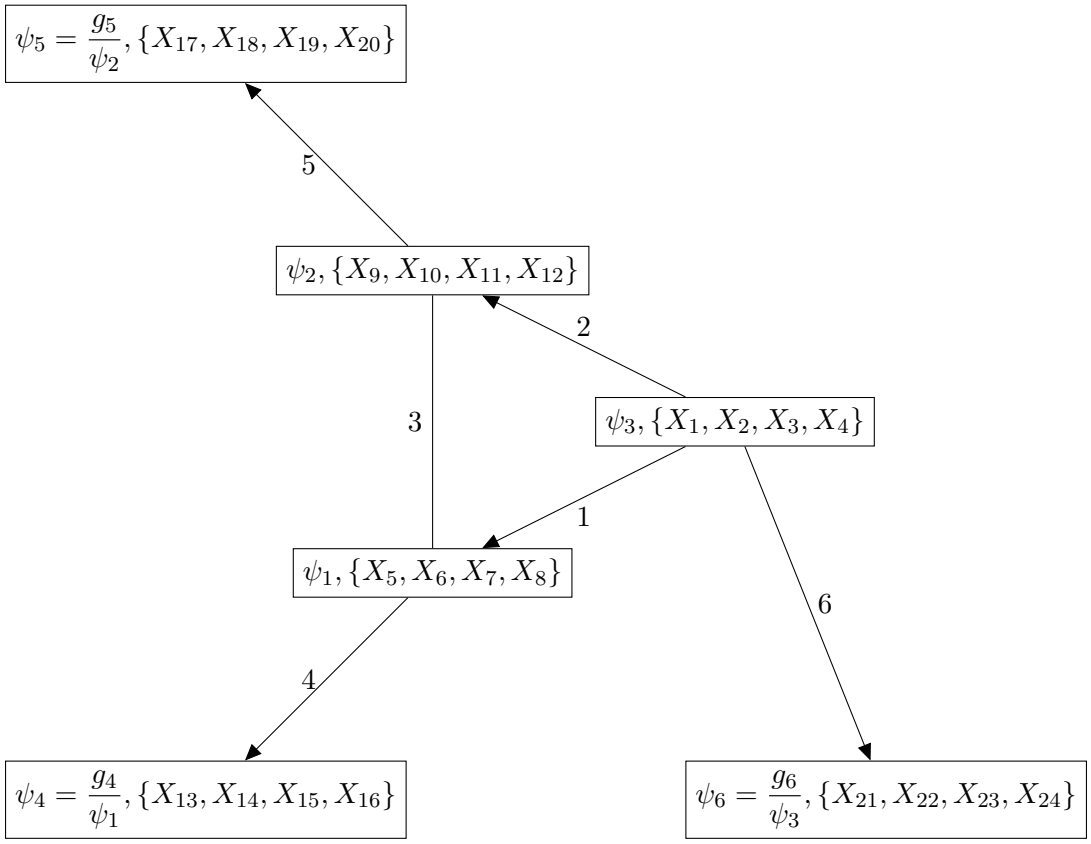
(1.17)

that satisfy

$$g_4 = \psi_1\psi_4, \quad g_5 = \psi_2\psi_5, \quad g_6 = \psi_3\psi_6. \tag{1.18}$$

(The heads of the arrows indicate the oil variables for each system.) During decryption, after we have computed the values of ψ_1, ψ_2, ψ_3, we can use (1.18) to easily compute the values of ψ_4, ψ_5, ψ_6. Similarly, after we have solved for the values of the vinegar variables $X_1, \ldots, X_{12}$, we can solve the three new oil-vinegar systems (1.17) for the oil variables $X_{13}, \ldots, X_{24}$.

Figure 1.3: Chain of Oil-Vinegar Systems



Chapter 2

Linear Algebra Attacks

Before designing a new cryptosystem, it is crucial to understand the existing attacks on MPKCs so that the weaknesses these attacks exploit may be avoided. Attacks on MPKCs can be grouped into two categories: attacks based on linear algebra, and attacks based on algebraic system solving. While this chapter addresses the linear algebra attacks in detail, we begin with some brief comments about algebraic system solving attacks.

Recall that the public key of an MPKC is a polynomial map $\bar{F} : k^n \to k^m$. Given a ciphertext $(y_1, \ldots, y_m) \in k^m$, algebraic system solving attacks predominantly employ Gröbner basis techniques in an attempt to solve the multivariate polynomial system

$$\bar{F}(x_1, \ldots, x_n) - (y_1, \ldots, y_m) = 0 \tag{2.1}$$

for a preimage $(x_1, \ldots, x_n) \in k^n$. Important advances have been made since Buchberger introduced his original algorithm in 1965 [Buc65], most notably Faugére's F_4 [Fau99] and F_5 [Fau02] algorithms. In fact, the most significant example of the effectiveness of an algebraic system solving attack against an MPKC is Faugére's success at breaking HFE for certain parameters [FJ03]. The XL algorithm [CKPS00], designed to solve overdetermined multivariate systems, has also been the focus of recent research. However, Gröbner basis methods are not the only tool available for solving multivariate systems such as (2.1); Ding

et al. have proposed the Zhuang-Zi algorithm [DGS06b], which relies on the univariate-multivariate correspondence of Section 1.2.1.

Though Gröbner basis attacks are quite powerful, attacks based on linear algebra have been far more destructive to the security of MPKCs; indeed, almost every MPKC that has been broken has fallen prey to the power of linear algebra attacks. In this chapter, we will discuss the three types of linear algebra attacks: linearization equation attacks, rank attacks, and the separation of oil and vinegar variables attack.

2.1 Linearization Equation Attacks

As mentioned in Section 1.2.2, linearization equations were first used by Patarin [Pat95] in his attack on the MI cryptosystem. We follow the presentation of Ding et al. [DGS06a].

First, consider the following argument. Let $Y \in K$ be the output of the central map of the MI cryptosystem, i.e. $Y = X^{q^\theta+1}$. Raising both sides to the $q^\theta - 1$ power, we have

$$Y^{q^\theta-1} = (X^{q^\theta+1})^{q^\theta-1} = X^{q^{2\theta}-1}.$$

Multiplying by XY,

$$XY^{q^\theta} = X^{q^{2\theta}}Y,$$

and we write

$$XY^{q^\theta} - X^{q^{2\theta}}Y = 0. \tag{2.2}$$

Observe that since q-th power maps are k-linear, when we move to the corresponding multivariate system over the ground field k, (2.2) becomes linear in both the input variables $(x_1, \ldots, x_n) = \pi(X)$ and the output variables $(y_1, \ldots, y_n) = \pi(Y)$. So, in addition to satisfying the original quadratic MI equation, the pair $(X, Y) \in K \times K$ also satisfies the k-linear equation (2.2). With this in mind, we introduce the following general definition.

Definition 2.1.1 ([DGS06a], Definition 2.3.1)**.** *Let $\mathcal{G} = \{g_1, \ldots, g_m\}$ be any set of m*

polynomials in $k[x_1, \ldots, x_n]$. *A linearization equation for* $\mathcal{G}$ *is any polynomial in* $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ *of the form*

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}x_iy_j + \sum_{i=1}^{n} b_ix_i + \sum_{j=1}^{m} c_jy_j + d, \tag{2.3}$$

such that we obtain the zero polynomial in $k[x_1, \ldots, x_n]/(x_1^q - x_1, \ldots, x_n^q - x_n)$ *(i.e. the zero function on* k^n*) upon substituting in* g_j *for* y_j*, for* $j = 1, \ldots, m$.

The set of all such polynomials forms a vector space, called the linearization equation space of $\mathcal{G}$. Given sufficiently many linearization equations for the set $\mathcal{G} = \{\bar{f}_1, \ldots, \bar{f}_m\}$, where $\bar{f}_i$ is the i-th component of the public key $\bar{F}$, substituting the ciphertext $(y_1, \ldots, y_m) = \bar{F}(x_1, \ldots, x_n)$ into each linearization equation yields a linear system in the x_i. If we get n linearly independent equations, we can uniquely solve for the plaintext $(x_1, \ldots, x_n) \in k^n$. On the other hand, if we get fewer than n, say ℓ, linearly independent equations, we can substitute these expressions for ℓ of the variables, hence reducing the number of unknowns and possibly being able to solve a reduced instance of (2.1).

To find the space of linearization equations, notice that substituting the quadratic public polynomials $\bar{f}_1, \ldots, \bar{f}_m \in k[x_1, \ldots, x_n]$ for the y_j in (2.3), expanding, and reducing powers greater than q if needed, we get a polynomial of the form

$$\sum_{1\le i\le j\le \ell\le n} \alpha_{ij\ell}x_ix_jx_\ell + \sum_{1\le i\le j\le n} \beta_{i,j}x_ix_j + \sum_{1\le i\le n} \gamma_ix_i + \delta, \tag{2.4}$$

where the $\alpha_{ij\ell}, \beta_{ij}, \gamma_i, \delta$ are all linear equations in the unknowns a_{ij}, b_i, c_j, d. Since this must be the zero function on k^n (i.e. the zero polynomial in the quotient ring), the $\alpha_{ij\ell}, \beta_{ij}, \gamma_i$, and δ must all be identically zero, giving $\frac{(n+1)(n+2)(n+3)}{6}$ linear equations in the $(n+1)(m+1)$ unknowns a_{ij}, b_i, c_j, d. Solving this linear system gives the space of linearization equations.

For the MI cryptosystem, it can be shown that the dimension of the linearization equation space is at least $n - \gcd(\theta, n) \ge \frac{2n}{3}$, so each ciphertext will produce at least $\frac{2n}{3}$ independent linearization equations, allowing us to eliminate two-thirds of the variables,

making the system (2.1) quite easy to solve.

As discussed in Example 1.3.2, Ding et al. [DHNW07] generalized linearization equations to allow for higher degrees in the y_i variables. Their degree two high order linearization equation (HOLE) attack successfully breaks the MFE cryptosystem.

2.2 Rank Attacks

Some of the most devastating attacks on multivariate public key cryptosystems have exploited a property of quadratic polynomials called the rank. In this section, we introduce the concept of rank, then proceed to discuss the minrank and dual rank attacks on MPKCs.

2.2.1 Rank defined

We first define rank in the case where k has odd characteristic. A quadratic form

$$f = \sum_{i=1}^{n} \sum_{j=i}^{n} \alpha_{ij} x_i x_j, \quad \alpha_{ij} \in k$$

can be written as $f = \mathbf{x}^T A \mathbf{x}$, where $\mathbf{x} = (x_1, \ldots, x_n)^T$ and $A \in k^{n \times n}$ is symmetric. We define the *rank* of f to be the rank of A. If f is a general quadratic polynomial, then we define the *rank* of f to be the rank of the homogeneous quadratic part of f.

Also, we make the important observation that given a matrix A for a quadratic form, if we perform a change of variables $\mathbf{x} \mapsto L\mathbf{x}$, then the matrix of the new quadratic form is $L^T A L$.

In the case where k has characteristic two, we must be more careful. First notice that a squared term is actually linear, and will not contribute to the rank. A quadratic form

$$f = \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \alpha_{ij} x_i x_j, \quad \alpha_{ij} \in k$$

can be written as $f = \mathbf{x}^T A \mathbf{x}$, where this time A is an uppertriangular matrix with $A_{ij} = \alpha_{ij}$. Then, we define the rank of f to be the rank of $A + A^T$.

We make a few observations:

- If a variable x_i does not appear in the polynomial f, then the row and column of A which correspond to x_i are zero, and f does not have full rank.
- If $f = \alpha_{ij} x_i x_j$ (with $0 \neq \alpha_{ij} \in k$), then it is easy to see that f has rank 2. In fact, if $f = \sum \alpha_{ij} x_i x_j$ where all the variables are distinct, then the rank of f is twice the number of terms of f
- Let $f = \left(\sum_{i=1}^{n} \alpha_i x_i \right) \left(\sum_{j=1}^{n} \beta_j x_j \right)$ be squarefree. Then $\text{rank}(f) = 2$.
- More generally, if $f = \sum \ell_i \ell_j$, where each ℓ_r is a linear polynomial, then $\text{rank}(f) \leq 2t$ where t is the number of products in the sum.

The last two facts follow from the results of the next section.

2.2.2 Equivalence classes of bilinear forms

This section presents some important results from [MS83]. Let k have characteristic two. Suppose we have a quadratic form $A(\mathbf{x}) = \mathbf{x}^T A \mathbf{x}$ where $A \in k^{n \times n}$ is uppertriangular with zero diagonal. There is a one-to-one correspondence between these quadratic forms and symplectic forms (i.e. bilinear forms $B(\mathbf{x}, \mathbf{y})$ satisfying $B(\mathbf{x}, \mathbf{x}) = 0$ and $B(\mathbf{x}, \mathbf{y}) = B(\mathbf{y}, \mathbf{x})$). In matrix form, we write $B(\mathbf{x}, \mathbf{y})$ as $\mathbf{x}^T B \mathbf{y}$ where $B \in k^{n \times n}$ is symmetric with zero diagonal. In particular, this correspondence is given by

$$A \longleftrightarrow B = A + A^T.$$

Theorem 2.2.1 (Dickson's Theorem)**.** *For every symplectic form $B(\mathbf{x}, \mathbf{y})$, there exists a linear transformation, L, such that under the transformation $\mathbf{u} = L^{-1}\mathbf{x}, \mathbf{v} = L^{-1}\mathbf{y}$, the matrix B becomes $L^T B L$ having the form*

$$L^T B L = \begin{pmatrix} 0 & 1 & & & & & & & \\ 1 & 0 & & & & & & & \\ & & 0 & 1 & & & & & \\ & & 1 & 0 & & & & & \\ & & & & \ddots & & & & \\ & & & & & 0 & 1 & & \\ & & & & & 1 & 0 & & \\ & & & & & & & 0 & 0 \\ & & & & & & & 0 & 0 \\ & & & & & & & & & \ddots \end{pmatrix},$$

where the diagonals above and below the main diagonal each have $\operatorname{rank}(B)/2$ *ones with zeros everywhere else.*

Examining the quadratic form $\mathbf{x}^T A\mathbf{x}$ under this transformation, we have

$$\begin{aligned} \mathbf{x}^T A\mathbf{x} &\leftrightarrow \mathbf{x}^T(A + A^T)\mathbf{y} \\ &= \mathbf{u}^T L^T(A + A^T)L\mathbf{v} \\ &= \mathbf{u}^T(L^T AL + L^T A^T L)\mathbf{v} \\ &= \mathbf{u}^T(\tilde{A} + \tilde{A}^T)\mathbf{v} \\ &\leftrightarrow \mathbf{u}^T \tilde{A}\mathbf{u}, \end{aligned}$$

and we say that A is *equivalent* to $\tilde{A}$. Notice that $\tilde{A}$ may no longer be uppertriangular, but $\tilde{A} + \tilde{A}^T$ must have the form specified by Dickson's Theorem so

- $\tilde{A}_{i,i+1} + \tilde{A}_{i+1,i} = 1, \quad i = 1, 3, \ldots, \operatorname{rank}(A + A^T) - 1,$
- $\tilde{A}_{i,i} = 0$ for all i, and
- $\tilde{A}_{i,j} + \tilde{A}_{j,i} = 0$ for all other i, j.

Thus we have the following important corollary:

Corollary 2.2.1. *Every quadratic form given by* $A \in k^{n\times n}$ *can be transformed via a linear*

transformation into the form

$$\sum_{i=1}^{r} x_{2i-1}x_{2i},$$

where $r = \text{rank}(A + A^T)$.

2.2.3 Minrank Attack

The minrank attack has been successfully applied to several MPKCs. Here we present the attack of Goubin and Courtois [GC00] on the single field TTM system of Moh. Kipnis and Shamir [KS99] first used the minrank attack against the mixed field HFE system, but since the system we will propose in Chapter 4 more closely resembles a single field system, we examine the Goubin-Courtois attack. We first define the MinRank problem as follows:

Definition 2.2.1 (MinRank Problem)**.** *Given* $A_1, \ldots, A_m \in k^{n\times n}$*, and* $r < n$*, find a non-trivial linear combination of*

$$A = \alpha_1 A_1 + \cdots + \alpha_m A_m, \quad a_i \in k,$$

such that $\text{rank}(A) \leq r$.

There are several techniques to solve this problem, but we will not discuss them here, only stating the complexity as $O(q^{\lceil \frac{m}{n} \rceil r} m^3)$, where $q = |k|$ [GC00].

Instead of simply presenting the technical details of the attacks, we begin each explanation with a brief overview to help motivate the main ideas and strategies behind the attack, and then follow with a more complete description of each attack.

Defining TPM. Since presenting Moh's original TTM cryptosystem [Moh99] would require a great deal of space, we present a generalization called TPM, of which TTM is a particular instance, that Goubin and Courtois ultimately used to break TTM. The central

map of TPM is given by $F = (f_1, \ldots, f_{n-r+u}) : k^n \to k^{n-r+u}$ where

$$\begin{array}{lcllll}
f_1 & = & x_1 & + & g_1(& x_{n-r+1}, \ldots, x_n) \\
f_2 & = & x_2 & + & g_2(x_1; & x_{n-r+1}, \ldots, x_n) \\
f_3 & = & x_3 & + & g_3(x_1, x_2; & x_{n-r+1}, \ldots, x_n) \\
 & \vdots & & & & \\
f_{n-r} & = & x_{n-r} & + & g_{n-r}(x_1, \ldots, x_{n-r-1}; & x_{n-r+1}, \ldots, x_n) \\
f_{n-r+1} & = & & & g_{n-r+1}(x_1, \ldots, x_n) & \\
 & \vdots & & & & \\
f_{n-r+u} & = & & & g_{n-r+u}(x_1, \ldots, x_n), &
\end{array} \tag{2.5}$$

with g_i quadratic, $1 \leq i \leq n - r + u$. For simplicity, we introduce $m = n + u - r$. Then the public key is the m polynomials of the map $\bar{F} = L_1 \circ F \circ L_2$, where $L_1 : k^m \to k^m$ and $L_2 : k^n \to k^n$ are random invertible affine transformations. Thus we can view $\bar{F} = (\bar{f}_1, \ldots, \bar{f}_m)$ as combinations of the central map polynomials $f_1, \ldots, f_m$, under the change of variables specified by L_2. Moh's TTM cryptosystem can be viewed as an instance of TPM with $n = 64$, $u = 38$, and $r = 2$.

We now make two crucial observations: the quadratic part of f_1 only has r variables, and the variable x_{n-r} appears only in the last u polynomials. We will use the minrank and dual rank attacks, respectively, to exploit these weaknesses and break the system. We can think of the two attacks as duals of each other: the minrank attack exploits the fact that one central map polynomial contains a small subset of the variables, while the dual rank attack exploits the fact that one variable appears in a small subset of the central map polynomials.

Attack overview. We may assume L_1 and L_2 are invertible linear transformations, since the affine parts may be absorbed into the central map (see [Wol05, Section 4.4.6]). As mentioned above, the minrank attack exploits the fact that the quadratic part of f_1 involves only the r variables $x_{n-r+1}, \ldots, x_n$. Let $[L_2\mathbf{x}]_i$ be the i-th component of $L_2(x_1, \ldots, x_n)^T$.

Composing f_1 with L_2 gives

$$f_1 \circ L_2(x_1, \ldots, x_n) = [L_2\mathbf{x}]_1 + g_1([L_2\mathbf{x}]_{n-r+1}, \ldots, [L_2\mathbf{x}]_n).$$

If we can find a basis for the space spanned by the last r components of $L_2\mathbf{x}$ (a space of linear polynomials having dimension r), then setting each of these components to a field value will cause $g_1([L_2\mathbf{x}]_{n-r+1}, \ldots, [L_2\mathbf{x}]_n)$ to be constant, thus giving a linear equation for $f_1 \circ L_2$ (there are q^r possible choices). Since the public polynomials $\bar{f}_1, \ldots, \bar{f}_m$ are linear combinations (via L_1) of $f_i \circ L_2$, $1 \leq i \leq m$, we will be able to find a linear combination of the public polynomials that is actually a linear polynomial, i.e. we can find α_i, $1 \leq i \leq m$ such that

$$\sum_{i=1}^{m} \alpha_i \bar{f}_i = \sum_{i=1}^{n} \beta_i x_i + \gamma. \tag{2.6}$$

Then plugging in the ciphertext $(y_1, \ldots, y_m) \in k^m$ for $(\bar{f}_1, \ldots, \bar{f}_n)$, (2.6) gives a linear expression involving the x_i, therefore giving us the value of $[L_2\mathbf{x}]_1$. Substituting this expression into the public polynomials is equivalent to setting $g_2([L_2\mathbf{x}]_1; [L_2\mathbf{x}]_{n-r+1}, \ldots, [L_2\mathbf{x}]_n)$ constant, and the equation for $f_2 \circ L_2$ becomes linear. Hence we can do another search for a linear equation among the public polynomials. We will continue this process until we have solved for all the variables.

Attack details. The question that remains is how to find the space spanned by the last r components of $L_2\mathbf{x}$: this is where the MinRank problem fits in. We follow the basic outline of [DGS06a], but provide greater detail to give more clarity. Notice that if we consider the matrix A_1 of the quadratic form corresponding to f_1 (disregarding the linear and constant terms) as in Section 2.2.1, we expect it to satisfy $\text{rank}(A_1) \leq r$. In particular we can write A_1 in the form

$$A_1 = \begin{pmatrix} 0 & 0 \\ 0 & A_1' \end{pmatrix}, \tag{2.7}$$

where $A_1' \in k^{r \times r}$ is symmetric with zero diagonal. After applying the linear change, L_2, of variables, A_1 becomes $L_2^T A_1 L_2$ hence $\text{rank}(L_2^T A_1 L_2) \leq r$. Since the public polynomials are constructed by multiplying the vector of central map polynomials by the matrix L_1, there must be some combination of the matrices B_i of the quadratic forms corresponding to the public polynomials, $\bar{f}_i$, $1 \leq i \leq m$, such that

$$L_2^T A_1 L_2 = \sum_{i=1}^{m} \lambda_i B_i, \quad \lambda_i \in k. \tag{2.8}$$

This is clearly an instance of the MinRank problem. If r is small enough and odd (see the comments section below for how to handle the even case), we should be able to solve the MinRank problem and find $cL_2^T A_1 L_2$, i.e. the left side of (2.8) up to a constant multiple. The kernel of this matrix will have dimension $n - r$, and we can compute a basis of column vectors $v_1, \ldots, v_{n-r}$. Completing this basis to a basis for the whole space, $v_1, \ldots, v_n$, we have the nonsingular matrix

$$L = (v_1, \ldots, v_n).$$

Lemma 2.2.1. *The space spanned by the last r components of $L_2\mathbf{x}$ is the same as the space spanned by the last r components of $L^{-1}\mathbf{x}$.*

Proof. Notice that

$$L^T (cL_2^T A_1 L_2) L = E,$$

where $E \in k^{n \times n}$ has the same form as A_1 in (2.7). Since L_1 and L_2 are invertible, we can rewrite this as

$$A_1 L_2 \mathbf{x} = c^{-1} (L_2^T)^{-1} (L^T)^{-1} E L^{-1} \mathbf{x}.$$

Notice that the structure of A_1 (and E) makes the first $n - r$ components of the above vectors 0 (actually, we are interested only in the last $n - r$ components). Define $(L_2\mathbf{x})_r$ and $(L^{-1}\mathbf{x})_r$ to be the last r components of the vectors $L_2\mathbf{x}$ and $L^{-1}\mathbf{x}$, respectively. Also, let A_1' and E' be the $r \times r$ submatrices of rank r of A_1 and E, respectively. Finally, let $\tilde{L}$ be

the $r \times r$ matrix given by the last r rows and columns of $(L_2^T)^{-1}(L^T)^{-1}$. Then we have

$$A_1'(L_2\mathbf{x})_r = c^{-1}\tilde{L}E'(L^{-1}\mathbf{x})_r.$$

But since A_1 has rank r, A_1' is invertible, hence

$$(L_2\mathbf{x})_r = c^{-1}(A_1')^{-1}\tilde{L}E'(L^{-1}\mathbf{x})_r,$$

and we have shown that the last r components of $L_2\mathbf{x}$ are in the span of the last r components of $L^{-1}\mathbf{x}$. The reverse inclusion is done similarly. □

Using this Lemma, it is now clear that we can compute the required basis for the space spanned by the last r components of $L_2\mathbf{x}$. Suppose it is given by $\{b_{n-r+1}, \ldots, b_n\}$, where

$$b_i = x_i + \sum_{j=1}^{n-r} \alpha_{ij}x_j, \quad n-r+1 \leq i \leq n, \alpha_{ij} \in k. \tag{2.9}$$

We now explain more explicitly the process stated in the overview. Consider the first component of the central map under the change of variables, i.e. the first component of $F \circ L_2$:

$$f_1 \circ L_2\mathbf{x} = [L_2\mathbf{x}]_1 + g_1([L_2\mathbf{x}]_{n-r+1}, \ldots, [L_2\mathbf{x}]_n).$$

Now, each $[L_2\mathbf{x}]_i$, $n-r+1 \leq i \leq n$, can be written as a sum of the b_i:

$$[L_2\mathbf{x}]_i = \sum_{j=n-r+1}^{n} \beta_{ij}b_j, \quad \beta_{ij} \in k,$$

so setting the b_i to field values (we have q^r choices) will make g_1 constant, and therefore f_1 becomes linear. Equivalently, setting the b_i to field values in (2.9) gives linear expressions for x_i, $n-r+1 \leq i \leq n$, in terms of x_j, $1 \leq j \leq n-r$, so substituting these in for x_i, g_1 becomes constant, and thus f_1 becomes linear. Observe that from the perspective of algebraic geometry, we are restricting functions to a subspace of dimension r, which is

equivalent to setting the variables to be constant. Of course the public polynomials are just combinations of the central map polynomials (via L_1) after the base change (L_2), so to find the combination that yields a linear polynomial, we make the substitution of the x_i, $n-r+1 \leq i \leq n$ in $\bar{F}$ by the linear expressions of (2.9), and then do Gaussian reduction on the new public polynomials to find a linear polynomial. This gives us another linear equation, which we substitute (equivalent to setting another of the variables constant), and Gaussian reduction will give us another linear polynomial, and so on, until we have a total of n linear equations which we can then solve, and check to see if we have the right plaintext.

Notice that we have q^r choices for field values to plug in, however the complexity for this attack is clearly dominated by the step that finds a solution to the MinRank problem: $O(q^{\lceil \frac{m}{n} \rceil r} m^3)$.

Comments. The above method works if r is odd, however, we must make a slight modification in the case where r is even. Notice that g_2 involves only one additional variable, x_1. By Dickson's Theorem, we know that rank must be an even number and hence $\text{rank}(g_2) = \text{rank}(g_1) = r$. Thus solving the MinRank problem will actually give

$$c_1 L_2^T A_1 L_2 + c_2 L_2^T A_2 L_2 = \sum_{i=1}^{m} \lambda_i B_i, \quad \lambda_i \in k.$$

The subsequent process remains the same up until the point of searching for a combination of the public polynomials that yields a linear polynomial. As before, after substituting for the $x_{n-r+1}, \ldots, x_n$, g_1 becomes constant, but g_2 will be a quadratic function of $[L_2\mathbf{x}]_1$, so we search for combinations that are linear and also have squared terms. Once we find such equations, we can make them linear since we know the simple structure of f_1 and f_2.

2.2.4 Dual Rank Attack

Attack overview. As mentioned before, the dual rank attack is based on the fact that x_{n-r} appears in the quadratic parts of only the last u central map polynomials of TPM (2.5). This means it shouldn't be too hard to find some combination of the public polynomials that

doesn't involve the variable $[L_2\mathbf{x}]_{n-r}$ (actually, we will just guess random combinations until we find one). Suppose one such combination is given by $\sum_{i=1}^{m} \alpha_i \bar{f}_i$, and let $P = \sum_{i=1}^{m} \alpha_i B_i$ be the sum of the matrix representations of the corresponding quadratic forms. Utilizing the kernel of P, we can quickly construct a new combination that doesn't involve the variables $[L_2\mathbf{x}]_{n-r}$ or $[L_2\mathbf{x}]_{n-r-1}$, and can continue the process until we have a combination that involves only $[L_2\mathbf{x}]_{n-r+1}, \ldots, [L_2\mathbf{x}]_n$. Notice that we have in fact constructed a solution to the MinRank problem, since this final combination represents $f_1 \circ L_2$ up to a constant. We finish the attack using the techniques of the previous section.

Attack details. Let A_{n-r} be the matrix of the quadratic form corresponding to f_{n-r} in (2.5). Notice $\ker A_{n-r} \supseteq \{\mathbf{x} \in k^n : x_1 = \cdots = x_{n-r-1} = x_{n-r+1} = \cdots = x_n = 0\}$ has dimension ≥ 1, and the matrix $L_2^T A_{n-r} L_2$ corresponding to $f_{n-r} \circ L_2$ has a kernel of the same dimension. Therefore, we should be able to find some combination of the B_i (matrices of the quadratic forms corresponding to the public polynomials) with kernel of dimension ≥ 1. Choose $(\alpha_1, \ldots, \alpha_m) \in k^m$ at random, and let $P = \sum_{i=1}^{m} \alpha_i B_i$. We will consider $V = \ker P$. Notice

$$\begin{aligned}
P &= \sum_{i=1}^{m} \alpha_i \sum_{j=1}^{m} \ell_{ij} L_2^T A_j L_2 \quad \text{where } \ell_{ij} = [L_1]_{ij} \\
&= L_2^T \left(\sum_{i=1}^{m} \alpha_i \sum_{j=1}^{m} \ell_{ij} A_j \right) L_2 \\
&= L_2^T \left(\sum_{j=1}^{m} A_j \sum_{i=1}^{m} \alpha_i \ell_{ij} \right) L_2 \\
&= L_2^T \left(\sum_{j=1}^{m} \gamma_j A_j \right) L_2 \quad \text{where } \gamma_j = \sum_{i=1}^{m} \alpha_i \ell_{ij}.
\end{aligned}$$

Thus $\text{rank}(P) = \text{rank}\left(\sum_{j=1}^{m} \gamma_j A_j\right)$. Now, if our choice of $(\alpha_1, \ldots, \alpha_n) \in k^n$ results in $\gamma_j = 0$ for $n - r + 1 \leq j \leq m$ (i.e. for the last u indices), then

$$\dim V = \dim \ker \sum_{j=1}^{m} \gamma_j A_j = \dim \ker \sum_{j=1}^{n-r} \gamma_j A_j \geq 1$$

since in the definition of TPM (2.5), x_{n-r} does not appear in the polynomials $f_1, \ldots, f_{n-r}$. This means V contains the kernel corresponding to $\ker A_{n-r}$ under the change of variables (i.e. $\ker L_2^T A_{n-r} L_2$). We need to make sure we have the smallest possible kernel, in other words, the kernel that corresponds to exactly $\ker A_{n-r}$, so whenever we find $\dim V \geq 1$, we compute the solution space Λ for the λ_i in

$$PV = \left(\sum_{i=1}^{m} \lambda_i B_i\right) V = 0. \tag{2.10}$$

The V we want has the property that $\dim(\Lambda) = n - r$. To see this, notice that

$$\ker \left(\sum_{j=1}^{n-r} \gamma_j A_j\right) \supseteq \ker A_{n-r},$$

and again, this is since dimension is unchanged under the change of variables. Recall that $m = n + u - r$, so the probability of guessing the right kernel is $\frac{q^{m-u}}{q^m} = q^{-u}$, so it takes about q^u tries to find the right kernel. Similar to the minrank attack, we will see that this initial step is the most costly step of the attack.

The goal now is to build a chain of $n - r$ kernels which corresponds to

$$\ker A_{n-r} \subseteq \ker A_{n-r-1} \subseteq \cdots \subseteq \ker A_2 \subseteq \ker A_1, \tag{2.11}$$

where the last kernel is the same as the kernel of the matrix in (2.8). The last step in the attack will be the same as the minrank attack, performing a search of size q^r. We find the next kernel in the chain as follows. Compute a basis for Λ (the solution space of the λ_i in

(2.10)). Write the i-th basis vector as $(\lambda_{i1}, \ldots, \lambda_{im}) \in \Lambda$, and let

$$\tilde{f}_i = \sum_{j=1}^{m} \lambda_{ij} \bar{f}_i, \quad 1 \leq i \leq n-r.$$

Let $\tilde{B}_i$ be the matrices of the quadratic parts of these polynomials, so $\tilde{B}_1, \ldots, \tilde{B}_{n-r}$ each correspond to some combination of $A_1, \ldots, A_{n-r}$ under the change of variables. It is easy to see from the definition of TPM (2.5) that we are left with $n-r$ quadratic polynomials with the variable x_{n-r-1} appearing in only one. This puts us back in a similar position to where we started, only now we only have $n-r$ matrices $\tilde{B}_1, \ldots, \tilde{B}_{n-r}$ and $u = 1$. As before, we choose random $(\alpha_1, \ldots, \alpha_{n-r}) \in k^{n-r}$, and compute $P = \sum_{i=1}^{n-r} \alpha_i \tilde{B}_i$ and $V = \ker P$. When $\dim V \geq 1$, we compute the solution space Λ to

$$\left(\sum_{i=1}^{n-r} \lambda_i \tilde{B}_i \right) V = 0.$$

This time we want $\dim \Lambda = n-r-1$, and the probability of guessing the right kernel is $\frac{q^{n-r-1}}{q^{n-r}} = q^{-1}$, so we will have the kernel after about q guesses. Continuing, by using the basis elements of the new Λ, we compute the $n-r-1$ new matrices $\tilde{B}_1, \ldots, \tilde{B}_{n-r-1}$, and repeat the process $n-r-2$ more times. The end result is that we have found the necessary chain of kernels (2.11), and we finish the attack by doing a search of size q^r (notice $r \leq u$) and applying the techniques of the previous section. The complexity of this attack can be shown to be approximately: $O(nm^3q^u)$ [YC04].

Comments. We can make an improvement to our attack strategy. Recall that if a variable x_t does not appear in a central map polynomial, then its matrix has rank $< n$. So, if x_t appears only in one equation in the central map, then when we form linear combinations of pairs of polynomials from the public key, these pairs (for the most part) will have rank $< n$. To see this, suppose x_t appears only in the central map polynomial f_t. We can write

public polynomials $\bar{f}_i$ and $\bar{f}_j$ as

$$\bar{f}_i = \alpha_i f_t + \sum_{k \neq t} \beta_{ik} f_k \quad \text{and} \quad \bar{f}_j = \alpha_j f_t + \sum_{k \neq t} \beta_{jk} f_k,$$

where we assume α_i and α_j are nonzero (this is why we used the phrase "for the most part"). Then

$$\bar{f}_i + \frac{\alpha_i}{\alpha_j} \bar{f}_j$$

has no term with $[L_2\mathbf{x}]_t$ and hence its matrix has rank $< n$. We can generalize this so that if a variable x_t only appears in u central map polynomials, then we can find combinations of $u+1$ public polynomials that have less than full rank, i.e.

$$\bar{f}_1 + \alpha_2 \bar{f}_2 + \cdots + \alpha_{u+1} \bar{f}_{u+1}$$

has no $[L_2\mathbf{x}]_t$ term, as long as the α_i's are chosen correctly. So we really only need to consider combinations of $(u+1)$ of the public matrices, as opposed to all m of them. This reduces the attack complexity to $O(n^3 q^u)$ [YC04].

The main idea of this attack (finding a chain of kernels) was first proposed by Coppersmith et al. [CSV93, CSV97] to break Shamir's Birational Permutation signature scheme [Sha93]. Goubin and Courtois later showed how to apply this idea to attack TPM [GC00], but they take a slightly different approach after finding each kernel of (2.11), resulting in a complexity of $O(n^6 q^u)$.

2.2.5 Similarities between the two attacks

The rank attacks exploit the fact that the TPM system uses polynomials that have ranks near both ends of the spectrum. While the minrank attack begins by finding a polynomial with *small* rank, the dual rank attack begins by finding a polynomial with *almost full* rank. Notice that in both attacks, the final step involves a search of size q^r. This suggests that at the heart of the attacks we are able to use rank distinguish the

triangular part (the first $n-r$ equations) from the u random quadratics that are appended, and find expressions of the first $n-r$ variables in terms of the last r.

2.3 Separation of Oil and Vinegar Variables Attack

Recall from Section 1.2.6 that Kipnis and Shamir [KS98] first used their separation of oil and vinegar variables attack to break Patarin's original balanced oil-vinegar signature scheme (i.e. $o = v$). Subsequently, Kipnis et al. [KPG99] proposed an unbalanced ($o < v$) scheme, showed how to extend the attack, and gave parameters to construct a secure system. Although originally developed to attack oil-vinegar signature systems, the separation of oil and vinegar variables attack has been used to break other schemes, notably a version of the triangular signature scheme TTS [DSY06]. Since the system we propose in Chapter 4 combines ideas from triangular and oil-vinegar systems, it is important to understand this attack.

2.3.1 Kipnis-Shamir attack on balanced oil-vinegar

We first consider the Kipnis-Shamir attack on an oil-vinegar scheme with $o = v$, say both equal to n, giving a total of $2n$ variables. The central map $F = (f_1, \ldots, f_n)$ is an n-tuple of oil-vinegar polynomials with each $f_i(x_1, \ldots, x_n, \check{x}_1, \ldots, \check{x}_n) \in k[x_1, \ldots, x_n, \check{x}_1, \ldots, \check{x}_n]$ quadratic, and the public key is given by $\bar{F} = F \circ L$ where $L : k^{2n} \to k^{2n}$ is an invertible affine transformation. Notice that in the presentation of oil-vinegar systems in Section 1.2.6, we listed the vinegar variables $\check{x}_1, \ldots, \check{x}_n$ before the oil variables $x_1, \ldots, x_n$ in the f_i so that the definition of the new framework of Section 1.3 would be more natural. Kipnis and Shamir use the original notation of the oil variables preceding vinegar variables, which we follow here.

Let $\mathbf{x} = (x_1, \ldots, x_n, \check{x}_1, \ldots, \check{x}_n)^T$, and write the homogeneous quadratic part of each f_i as $f_i = \mathbf{x}^T A_i \mathbf{x}$ as in Section 2.2.1. Observe that since f_i is an oil-vinegar polynomial and

has no terms that are quadratic in the oil variables, A_i must have the form:

$$A_i = \begin{pmatrix} 0 & A_{i1} \\ A_{i2} & A_{i3} \end{pmatrix},$$

where $A_{i1}, A_{i2}, A_{i3} \in k^{n \times n}$, $1 \leq i \leq n$. Assume for now that L is an invertible linear transformation; we will explain later how to modify the attack when L is affine. The matrices, B_i, corresponding to the public polynomials are be given by $B_i = L^T A_i L$. Define the *oil subspace*, $\mathcal{O}$ to be the set of all vectors in k^{2n} with zeros in the last n positions, and define the *vinegar space*, $\mathcal{V}$, to be the set of all vectors in k^{2n} with zeros in the first n positions.

We now make an important observation: *knowledge of the transformed oil subspace, $L^{-1}\mathcal{O}$, will allow us to create forgeries.* Notice $L^{-1}\mathcal{O}$ is simply the set of vectors

$$\{\bar{\mathbf{o}} \in k^{2n} : L\bar{\mathbf{o}} \in \mathcal{O}\}.$$

Suppose we have in fact found $L^{-1}\mathcal{O}$, and let $\{v_1, \ldots, v_n\}$ be a basis of column vectors. Complete this to a basis $V = \{v_1, \ldots, v_{2n}\}$ for the whole space k^{2n}. Notice that we can think of V in matrix form as

$$V = L^{-1} \begin{pmatrix} * & * \\ 0 & * \end{pmatrix},$$

where the $*$'s denote some $n \times n$ submatrices. Then we have

$$\begin{aligned} V^T B_i V &= \left(L^{-1} \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right)^T B_i L^{-1} \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \\ &= \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} (L^T)^{-1} B_i L^{-1} \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \\ &= \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} A_i \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \\ &= \begin{pmatrix} 0 & * \\ * & * \end{pmatrix}. \end{aligned}$$

So, $V^T B_i V$ is the matrix corresponding to some oil-vinegar polynomial, and thus $F' = \bar{F} \circ V$ is an oil-vinegar system. But notice that

$$F' \circ V^{-1} = \bar{F}, \tag{2.12}$$

has the same form as (1.6), so we can use the new oil-vinegar map F' along with the invertible transformation V^{-1} to create valid signatures in the exact same way a legitimate user does.

Now, proving that we can in fact find $L^{-1}\mathcal{O}$ requires the following lemma:

Lemma 2.3.1 ([KS98], Lemma 4)**.** *Viewing A_i as a linear mapping, if A_i is invertible, then A_i maps $\mathcal{O}$ onto $\mathcal{V}$, and A_i^{-1} maps $\mathcal{V}$ onto $\mathcal{O}$. Furthermore, for any other invertible A_j, $A_i^{-1} A_j$ has $\mathcal{O}$ as an invariant subspace.*

Proof. Let $\mathbf{o} \in \mathcal{O}$,

$$A_i \mathbf{o} = \begin{pmatrix} 0 & * \\ * & * \end{pmatrix} \begin{pmatrix} * \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ * \end{pmatrix} \in \mathcal{V},$$

so A_i maps $\mathcal{O}$ into $\mathcal{V}$. But since A_i is invertible, it must map $\mathcal{O}$ to a subspace of dimension

n, so we have $A_i\mathcal{O} = \mathcal{V}$. Inverting, we must have $A_i^{-1}\mathcal{V} = \mathcal{O}$, and since this holds for any i, we conclude that $A_i^{-1}A_j\mathcal{O} = \mathcal{O}$ for any i, j. □

Notice that under the change of variables L, as f_i transforms to $f_i \circ L$, the corresponding matrix A_i transforms to $L^T A_i L$. However, viewing A_i as a linear transformation, it becomes $L^{-1}A_i L$. We reconcile this difference by considering the product $A_i^{-1}A_j$, where A_i is invertible. Applying L to both quadratic forms, the matrix of the product is

$$(L^T A_i L)^{-1} L^T A_j L = L^{-1} A_i^{-1} A_j L.$$

On the other hand, as linear maps, the matrix of the product is

$$(L^{-1} A_i L)^{-1} L^{-1} A_j L = L^{-1} A_i^{-1} A_j L.$$

Both right-hand side expressions are the same, giving the following corollaries:

Corollary 2.3.1. *If B_i and B_j are invertible, then $B_i^{-1}B_j$ has $L^{-1}\mathcal{O}$ as an invariant subspace.*

Proof. From above, $B_i^{-1}B_j = (L^T A_i L)^{-1}(L^T A_j L) = L^{-1}A_i^{-1}A_j L$. Thus

$$B_i^{-1}B_j L^{-1}\mathcal{O} = L^{-1}A_i^{-1}A_j L L^{-1}\mathcal{O} = L^{-1}A_i^{-1}A_j\mathcal{O} = L^{-1}\mathcal{O},$$

□

Corollary 2.3.2 ([KS98], Theorem 7)**.** *Consider only the B_i that are invertible. Define $T = k[B_i^{-1}B_j \text{ for all } i, j]$, the polynomial ring in all the $B_i^{-1}B_j$ for all i, j. Then the transformed oil space, $L^{-1}\mathcal{O}$ is an invariant subspace of every element of T.*

2.3.2 Implementation

We have reduced the problem of forging a signature to finding a common invariant subspace of a set of matrices. As with the MinRank problem, we don't explicitly discuss

how to solve this problem, but do make a few comments. Kipnis and Shamir present two methods for using the $B_i^{-1}B_j$ to compute $L^{-1}\mathcal{O}$. Their first approach is probabilistic. They state that heuristically, a basis of T should have $t = O(n^2)$ matrices. Define a vector $\mathbf{r}$ of $2n$ formal variables that represents an element of $L^{-1}\mathcal{O}$, and let M be the $2n \times t$ matrix with columns given by the product of each basis matrix with $\mathbf{r}$. Since the oil subspace has dimension n, M has rank n and therefore any $n+1$ rows must be linearly dependent, in particular the first $n+1$ rows. The resulting linear equation has $n+1$ unknown coefficients, and fixing one of them to be 1 gives n more unknowns in addition to the $2n$ components of $\mathbf{r}$. Each of the t components of the resulting row vector must be zero, and they describe how to solve this overdetermined quadratic system of t equations in $3n$ variables by linearization and choosing random vectors.

The second approach is to use characteristic polynomials of the $B_i^{-1}B_j$. Ding et al. [DGS06a] give a more complete treatment of this method, including notes on implementation in characteristic two.

We have presented the attack for the case where L is a linear transformation. In general, L is affine, but notice that in the composition $\bar{F} = F \circ L$, the quadratic parts of the polynomials are *not* affected by the affine part of L, i.e. the column vector making up the affine part of L only affects the linear and constant terms. Thus we simply perform the attack as stated above, except the new oil-vinegar map F' is constructed by composing the homogeneous quadratic part of $\bar{F}$ with V, leaving the linear and constant parts unchanged. We can then forge signatures in a similar way.

Before moving to the unbalanced case, we note that the balanced attack also applies to oil-vinegar systems with $v < o$.

2.3.3 Generalization to the unbalanced case $v > o$ with $v \approx o$

Define the $\mathcal{O}$ to be the set of all vectors in k^{o+v} with zeros in the last v positions, and define $\mathcal{V}$ to be the set of all vectors in k^{o+v} with zeros in the first o positions. In this

case, the matrix A_i of f_i has the form

$$A_i = \begin{pmatrix} 0 & A_{i1} \\ A_{i2} & A_{i3} \end{pmatrix},$$

where $A_{i1}, A_{i2} \in k^{o \times v}$, $A_{i3} \in k^{v \times v}$, $1 \leq i \leq o$.

Notice that since $v > o$, Lemma 2.3.1 no longer holds, since A_i only maps $\mathcal{O}$ *into* $\mathcal{V}$ (in particular, into an o-dimensional subspace). Kipnis et al. [KPG99] give a probabilistic generalization of the balanced attack to this case with complexity $o^4 q^{v-o-1}$.

2.3.4 Attacks when $o \not\approx v$

Based on the above complexity, v should clearly be larger than o, but it is not totally clear how large v should be. Braeken et al. [BWP05] examined the case when $v \geq 2o$, in particular $v = 2o$ and $v = 3o$ for small q and recommended values for o to construct secure systems. Continuing to increase v to $v \geq o^2$ is not a viable solution, as Kipnis et al. [KPG99] showed that in almost all cases, the resulting system was not secure.

2.3.5 Attacking general multivariate systems

Both the balanced and unbalanced attacks find $L^{-1}\mathcal{O}$ and use it to create an equivalent oil-vinegar system (2.12) which can be used to forge signatures. In general, forging a signature is a simpler problem than finding the plaintext that corresponds to a given ciphertext. Given a document P and the public key $F(x_1, \ldots, x_n)$ of a signature scheme, as the authors of [DSY06] eloquently comment in their work that breaks a version of TTS, "we need to know how to find a (not THE) solution for the equation $F(x_1, \ldots, x_n) = P$." For instance, in an oil-vinegar scheme, we know that the vast majority of choices for the vinegar vector $(\check{x}_1, \ldots, \check{x}_v) \in k^v$ will yield a valid signature $(\check{x}_1, \ldots, \check{x}_v, x_1, \ldots, x_o) \in k^{o+v}$, and to forge a signature, we only need to find one solution.

For this reason, applying the separation of oil and vinegar variables attack to a multivariate encryption scheme $\bar{F} = L_1 \circ F \circ L_2$ becomes a more difficult problem. Naively,

we would at least need to search through the space $L_2^{-1}\mathcal{O}$, thus increasing the complexity of the attack (similar to searching through the space of the last r components of $L_2\mathbf{x}$ in the minrank attack). However, while performing the security analysis on the MFE cryptosystem, Wang et al. [WYHL06] still use the complexity given in Section 2.3.3, and we follow their example in the cryptanalysis of our new system in Section 4.3.

Applying the separation of oil and vinegar variables attack to a general system involves partitioning variables of the central map into oil variables $x_1, \ldots, x_o$ and vinegar variables $\check{x}_1, \ldots, \check{x}_v$, where no $x_i x_j$ term appears in any central map polynomial. From Section 2.3.3, the complexity of this attack depends on the size of the minimal vinegar set. Wang et al. mention using a maximal clique-finding algorithm to find this set, but give no explanation. To actually accomplish this, construct the graph with vertices given by the central map variables and edges occuring whenever the product of two variables does *not* appear in any polynomial. Recall that a clique is a set of vertices that has the property that any pair of vertices in the set has an edge between them [DW01]. Therefore, computing the clique number (size of a maximal clique) of this graph is equivalent to computing the maximal oil set, and taking its complement in the set of all variables gives the minimal vinegar set. (Wang et al. state that the size of the minimal vinegar set for MFE is 9, but computations with Magma [MAGMA] show that it is actually 8, since a maximal oil set is given by $\{X_1, X_3, X_7, X_8\}$.)

Chapter 3

Polynomial Identities

Let $\mathbb{F}$ be a finite field of characteristic p. As discussed in Section 1.3.3, our goal is to construct quartic identities of the form

$$AB = f_1 f_2 + f_3 f_4 + \ldots f_{n-1} f_n + f_{n+1} f_{n+2} + \cdots + f_{n+t-1} f_{n+t} \tag{3.1}$$

where each polynomial has degree two, and

1. $A \in \mathbb{F}[X_1, \ldots, X_n]$, $B \in \mathbb{F}[Y_1, \ldots, Y_n]$.
2. $f_i \in \mathbb{F}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$, $1 \leq i \leq n$, are oil-vinegar polynomials.
3. $f_i \in \mathbb{F}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$, $n+1 \leq i \leq n+t$.

Furthermore, since ultimately we will build cryptosytems out of these identities, we introduce a restriction on the ranks of the polynomials:

4. $A, B, f_1, \ldots, f_{n+t}$ each have rank ≥ 4.

In this chapter, we explore several ideas to attack this problem. We begin by considering an approach based on classical number theory: parameterization; and continue by examining a more computational approach utilizing Gröbner bases. The last three sections focus on more algebraic/geometric ideas: Plücker coordinates, determinants, and Grassmann coordinates.

3.1 Parameterization

An initial approach to solving this problem is to parameterize the solutions, much like one can parameterize, for instance, the rational points on a circle. Suppose we are given the equation of a circle $x^2 + y^2 = 1$. Using $(-1, 0)$ as an initial solution, we parameterize all solutions as

$$(x, y) = (-1, 0) + \lambda(a, b).$$

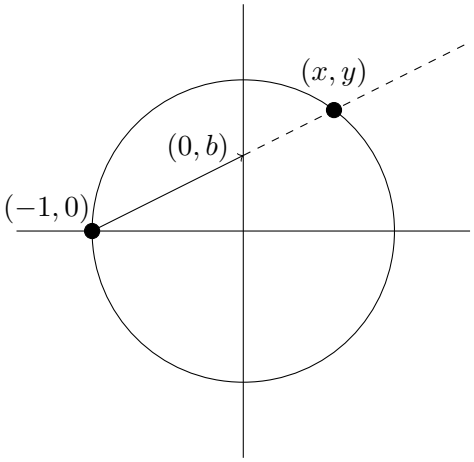
So, we have $(-1 + \lambda a)^2 + (\lambda b)^2 = 1$, and solving for λ gives $\lambda = \frac{2a}{a^2+b^2}$. Since (a, b) is a direction vector, we can fix $a = 1$ and let $b \in \mathbb{Q}$ vary, giving

$$(x, y) = (-1, 0) + \frac{2}{1 + b^2}(1, b). \tag{3.2}$$

Notice (3.2) misses the point $(-1, 0)$ since we fixed $a = 1$. To avoid this problem, we could allow $a = 0$, or we could use another initial point and take the union of the points from the new parameterization with those from the original parameterization (3.2).

Geometrically, as depicted in Figure 3.1, we draw the ray with tail $(-1, 0)$ in the direction $(1, b)$. The point (x, y) specified by (3.2) is given by the other point where this ray intersects the circle.

Figure 3.1: Parameterization of Points on the Unit Circle



We can quickly generalize this idea to rational functions. Suppose we want to find solutions of $x^2 + y^2 = 1$ where $x, y \in \mathbb{F}(t_1, \ldots, t_n)$. The parameterization (3.2) still holds, where we let $b \in \mathbb{F}(t_1, \ldots, t_n)$ vary.

We now develop a parameterization for the polynomial equation

$$\sum_{i=1}^{T} F_i G_i = 0,$$

where $F_i, G_i \in \mathbb{F}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$. Notice that initial solutions may often be easy to find; for instance, if $\mathbb{F} = \mathbb{F}_2$, an initial solution to $F_1 G_1 + F_2 G_2 = 0$ is given by $(F_1, F_2, G_1, G_2) = (1, 1, 1, 1)$. Now, suppose in general we have initial solution $F_i = \alpha_i$ and $G_i = \beta_i$, $1 \leq i \leq T$. A new solution will be of the form $F_i = \alpha_i + \lambda f_i$, $G_i = \beta_i + \lambda g_i$, with $f_i, g_i \in \mathbb{F}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$, $1 \leq i \leq T$. Since a new solution must satisfy the original equation, we have

$$\begin{aligned} 0 &= \sum_{i=1}^{T} (\alpha_i + \lambda f_i)(\beta_i + \lambda g_i) \\ &= \sum_{i=1}^{T} \lambda(\alpha_i g_i + \beta_i f_i) + \lambda^2 f_i g_i. \end{aligned} \tag{3.3}$$

Hence,

$$\lambda = \frac{\sum_{i=1}^{T} \alpha_i g_i + \beta_i f_i}{\sum_{i=1}^{T} f_i g_i} = \frac{\lambda_1}{\lambda_2}.$$

Clearing denominators in (3.3), we have the parameterization

$$F_i = \alpha_i \lambda_2 + \lambda_1 f_i, \; G_i = \beta_i \lambda_2 + \lambda_1 g_i, \quad 1 \leq i \leq T, \tag{3.4}$$

where $f_i, g_i \in \mathbb{F}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ are arbitrary and

$$\lambda_1 = \sum_{i=1}^{T} \alpha_i g_i + \beta_i f_i, \quad \lambda_2 = \sum_{i=1}^{T} f_i g_i. \tag{3.5}$$

To satisfy the requirement of (3.1) that each polynomial must be quadratic, we observe

that

$$\alpha_i, \beta_i \in k \text{ and } f_i, g_i \text{ linear polynomials}, \quad 1 \leq i \leq T,$$

are *sufficient* conditions. We do not claim, however, that these are *necessary* conditions, since that would require proving that $\alpha_i, \beta_i, f_i, g_i$ of higher degrees can never yield quadratic F_i and G_i in (3.4).

Recall that we are specifically interested in the rank of the solution polynomials; the following proposition addresses this issue:

Proposition 3.1.1. *Suppose* $\mathbb{F}$ *has characteristic two. Let* $\alpha_i, \beta_i, f_i,$ *and* g_i *be as above. Then* $\operatorname{rank}(\alpha_i\lambda_2+\lambda_1 f_i) \leq 2(T-1)$, and similarly, *rank*$(\beta_i\lambda_2+\lambda_1 g_i) \leq 2(T-1)$, *for* $1 \leq i \leq T$.

Proof. Expanding using (3.5), notice

$$\alpha_i\lambda_2 + \lambda_1 f_i = \alpha_i \sum_{j=1}^{T} f_j g_j + f_i \sum_{j=1}^{T} (\alpha_j g_j + \beta_j f_j)$$

Note that adding a squared term won't change the rank (since it has rank zero), so

$$\begin{aligned}
\operatorname{rank}(\alpha_i\lambda_2 + \lambda_1 f_i) &= \operatorname{rank}\left(\alpha_i \sum_{j=1}^{T} f_j g_j + \beta_i f_i^2 + f_i \sum_{j=1}^{T} (\alpha_j g_j + \beta_j f_j)\right) \\
&= \operatorname{rank}\left(\alpha_i \sum_{\substack{j=1 \\ j\neq i}}^{T} f_j g_j + \ f_i \sum_{\substack{j=1 \\ j\neq i}}^{T} (\alpha_j g_j + \beta_j f_j)\right) \\
&= \operatorname{rank}\left(\sum_{\substack{j=1 \\ j\neq i}}^{T} (\alpha_i f_j + \alpha_j f_i)(g_j + \frac{\beta_j}{\alpha_i} f_i)\right) \\
&\leq 2(T-1),
\end{aligned}$$

where we have assumed $\alpha_i \neq 0$ and have used the properties of rank discussed in Section 2.2. On the other hand, if $\alpha_i = 0$, $\operatorname{rank}(\alpha_i\lambda_2 + \lambda_1 f_i) = \operatorname{rank}(\lambda_1 f_i) \leq 2$. □

An important consequence of this proposition is that in order to achieve ranks greater than 4 with this method, we must have $T \geq 4$. Furthermore, a major drawback of

this method is that there seems to be no straightforward way to enforce the other restrictions of (3.1) on the parameterized solution (3.4).

3.2 Gröbner Basis Approach

We next explore a computational approach for solving (3.1), focusing on a simpler instance, namely the identity used by the MFE cryptosystem:

$$AB = CD + EF, \tag{3.6}$$

where A, B, C, D, E, F satisfy the requirements of (3.1). Writing $x_1, \ldots, x_4$ for $X_1, \ldots, X_4$ and $y_1, \ldots, y_4$ for $X_5, \ldots, X_8$ in (1.11), we can rewrite the specific solution used by MFE (when $\mathbb{F}$ has characteristic two) as:

$$(x_1x_4+x_2x_3)(y_1y_4+y_2y_3) = (x_1y_1+x_2y_3)(x_3y_2+x_4y_4)+(x_1y_2+x_2y_4)(x_3y_1+x_4y_3). \tag{3.7}$$

Why study such an apparently simple identity? A brief discussion of the size of the systems needed to naively find solutions to such an equation should suffice. Recall two important formulas:

1. The number of terms of degree k in a polynomial in n variables is at most $\binom{n+k-1}{k}$.
2. The total number of terms in a polynomial of degree d in n variables is at most $\binom{n+d}{d}$.

So, if we assign an unknown to the coefficient of each term of (3.6), this gives a total of $6\binom{n+2}{2}$ unknowns. Notice that the total degree of (3.6) is 4, giving a total of $\binom{n+4}{4}$ terms. Equating the coefficients of corresponding terms on both sides of the equation gives $\binom{n+4}{4}$ quadratic equations in the unknown coefficients. So, if $n = 8$, solving (3.6) requires solving a quadratic system of 495 equations in 270 unknowns – a difficult task even over $\mathbb{F}_2$. As n increases the problem becomes even more daunting.

3.2.1 Over $\mathbb{F}_2[x_1, \ldots, x_4, y_1, \ldots, y_4]$

We are interested in completely characterizing the solutions to (3.6) over the ring $\mathbb{F}_2[x_1, \ldots, x_4, y_1, \ldots, y_4]$, in particular, to see whether there are other solutions, in addition to the MFE solution, which might be suitable for building a cryptosystem. Before we consider the computational aspects of this problem, we address the notion of equivalent solutions.

First consider invertible linear transformations of variables. If we compose the central map $\tilde{F}$ of an MPKC with a change of variables T, the public key becomes $\bar{F} = L_1 \circ (\tilde{F} \circ T) \circ L_2$. However, we can simply redefine $L_2 := T \circ L_2$, absorbing T into L_2, and we can think of the two maps $\tilde{F}$ and $\tilde{F} \circ T$ as being equivalent. On the other hand, if we compose the central map $\tilde{F}$ of an MPKC with an invertible linear transformation S on the left, the public key becomes $\bar{F} = L_1 \circ (S \circ \tilde{F}) \circ L_2$. Redefining $L_1 := L_1 \circ S$, S is absorbed into L_1, and we can think of the two maps $\tilde{F}$ and $S \circ \tilde{F}$ as being equivalent. (See [WP05b] for a more general discussion of the idea of equivalent keys for MPKCs.) With this in mind, we introduce the following definition of equivalence:

Definition 3.2.1. *Two solutions* (A, B, C, D, E, F) *and* (A', B', C', D', E', F') *of* (3.6) *are equivalent if there exist invertible linear transformations* S *and* T *such that*

$$(A', B', C', D', E', F') = S(A \circ T, B \circ T, C \circ T, D \circ T, E \circ T, F \circ T).$$

We can use this definition of equivalence to significantly reduce the complexity of our problem. Notice that the first restriction of (3.1) requires A to be a quadratic in $\mathbb{F}_2[x_1, \ldots, x_4]$ and B to be a quadratic in $\mathbb{F}_2[y_1, \ldots, y_4]$, so we can write $A = A(\mathbf{x})$ and $B = B(\mathbf{y})$. Since rank 2 solutions are not suitable, A and B must both have rank 4, and hence by Corollary 2.2.1, we can find two invertible changes of variables $T_1, T_2 \in \mathbb{F}_2^{4\times 4}$ such that

$$A(T_1\mathbf{x}) = x_1x_2 + x_3x_4 \quad \text{and} \quad B(T_2\mathbf{y}) = y_1y_2 + y_3y_4.$$

Therefore, given any solution $(A, B, C, D, E, F) \in \mathbb{F}_2[x_1, \ldots, x_4, y_1, \ldots, y_4]^6$ of (3.6) satisfying the requirements of (3.1), if we define the linear transformation T by the matrix

$$T = \begin{pmatrix} T_1 & 0 \\ 0 & T_2 \end{pmatrix} \in \mathbb{F}_2^{8\times 8}$$

and compose each component of the solution with T, we get an equivalent solution of the form

$$(x_1x_2 + x_3x_4, y_1y_2 + y_3y_4, C \circ T, D \circ T, E \circ T, F \circ T). \tag{3.8}$$

From now on, we will only study solutions of this form, effectively eliminating A and B and reducing our problem to finding solutions (C, D, E, F) of the equation

$$(x_1x_2 + x_3x_4)(y_1y_2 + y_3y_4) = CD + EF. \tag{3.9}$$

We now consider transformations of the solution vector (C, D, E, F). Consider in particular an invertible linear transformation S given by

$$(C, D, E, F)^T \overset{S}{\longmapsto} (C', D', E', F')^T,$$

such that the new vector also satisfies (3.9). Since $CD + EF = C'D' + E'F'$, we call L an invariant transformation. For example, one can swap C and D, swap E and F, or swap (C, D) and (E, F), yet leave the quantity $CD+EF$ unchanged. These three transformations are not the only invariant transformations, although the others are less trivial, for instance,

$$(C, D, E, F)^T \mapsto (C + E, D, E, D + F)^T.$$

Observe that the set of invariant transformations in fact forms a group G under function composition. In the next section, we determine the group of invariant transformations and work toward the goal of designing equations for use in Gröbner basis computation that

eliminate redundant solutions due to the invariant transformations.

Before we state our main theorem, we address one more issue regarding equivalence: the transformation T of (3.8) is not unique. Consider for instance the transformation T' that maps $x_1 \mapsto x_1 + x_2$ and $x_3 \mapsto x_3 + x_4$, while fixing the other variables. Then composing the components of (A, B, C, D, E, F) with the map $T' \circ T$ yields a solution having the same general form as (3.9). Thus during computation, we must also take into account invertible linear transformations of variables that are invariant for both $x_1x_2 + x_3x_4$ and $y_1y_2 + y_3y_4$. This type of invariant transformation as well as the invariant transformations of the solution vector (C, D, E, F) can be viewed as invariants of the quadratic form $z_1z_2 + z_3z_4 \in \mathbb{F}_2[z_1, z_2, z_3, z_4]$.

The following theorem, which we prove in Section 3.2.3, completely characterizes solutions of (3.6) over $\mathbb{F}_2[x_1, \ldots, x_4, y_1, \ldots, y_4]$:

Theorem 3.2.1. *Any solution* $(A, B, C, D, E, F) \in \mathbb{F}_2[x_1, \ldots, x_4, y_1, \ldots, y_4]^6$ *satisfying the requirements of* (3.1) *is equivalent to the MFE solution* (3.7).

3.2.2 Invariants of the equation $z_1z_2 + z_3z_4$

Let $\mathbf{z} = (z_1, z_2, z_3, z_4)^T$. Suppose we have quadratic form $Q(\mathbf{z}) = z_1z_2 + z_3z_4$. Our goal is to describe the invariant group of Q. In matrix form, $Q(\mathbf{z}) = \mathbf{z}^T Q\mathbf{z}$ where $Q \in \mathbb{F}_2^{4\times4}$ is uppertriangular with $Q_{12} = Q_{34} = 1$ and $Q_{ij} = 0$ for all other i, j. We seek linear transformations, $L \in \mathbb{F}_2^{4\times4}$, such that $Q(L\mathbf{z}) = Q(\mathbf{z})$, i.e. $\mathbf{z}^T L^T QL\mathbf{z} = z_1z_2 + z_3z_4$. This yields the following equations:

- $[L^TQL]_{ii} = 0$, $1 \le i \le 4$,
- $[L^TQL]_{12} + [L^TQL]_{21} = 1$,
- $[L^TQL]_{34} + [L^TQL]_{43} = 1$, and
- $[L^TQL]_{ij} + [L^TQL]_{ji} = 0$ for all other i, j.

Solving this quadratic system for the 16 entries of L yields the invariant group, G, having 72 matrices (out of the 20160 invertible matrices in $\mathbb{F}_2^{4\times 4}$). This group has an abelian subgroup of order 8 generated by the matrices corresponding to the following three transformations of order 2:

$$\begin{aligned}(z_1, z_2, z_3, z_4) &\overset{\tau_1}{\longmapsto} (z_2, z_1, z_3, z_4),\\ (z_1, z_2, z_3, z_4) &\overset{\tau_2}{\longmapsto} (z_1, z_2, z_4, z_3),\\ (z_1, z_2, z_3, z_4) &\overset{\tau_3}{\longmapsto} (z_3, z_4, z_1, z_2).\end{aligned}$$

Let $H = \langle \tau_1, \tau_2, \tau_3 \rangle$. Letting τ_4 be any element in $G \backslash H$, for instance,

$$(z_1, z_2, z_3, z_4) \overset{\tau_1}{\longmapsto} (z_1 + z_3, z_2, z_3, z_2 + z_4),$$

it is straightforward to show (by examining cosets $Ha, a \in G$) that

$$G = \langle \tau_1, \tau_2, \tau_3, \tau_4 \rangle.$$

Recall that we want to introduce equations that attempt to eliminate (during Gröbner basis computation) redundant solutions caused by the invariant transformations $S \in G$. Notice redundant solutions due to τ_1 (interchanging the first and second positions) can be excluded by imposing an order requiring $C \geq D$ (in lex order in the coefficients of C and D). The question then becomes, how can we design equations that accomplish this ordering? Consider the first several coefficients of C and D:

$$\begin{array}{lccccccc} C: & c_1 & c_2 & c_3 & \ldots & c_i & \ldots \\ D: & d_1 & d_2 & d_3 & \ldots & d_i & \ldots . \end{array}$$

To enforce $C \geq D$, notice that If $d_1 = 1$, then c_1 must also be 1; but if $d_1 = 0$, then c_1 can be either 0 or 1. So, the first coefficient of C and D must satisfy

$$d_1(c_1 - 1) = 0.$$

If $c_1 = d_1$, then to break the tie, move to the next coefficient, where we get an equation similar to the above, but with c_2 and d_2. However, if $c_1 \neq d_1$, the above equation handles the situation, and the equation with c_2 and d_2 should vanish. Thus, the coefficients of C and D must satisfy

$$(c_1 - d_1 + 1)(d_2(c_2 - 1)) = 0.$$

We can continue in this fashion, supposing $c_j = d_j$, $1 \leq j < i$. Then if $d_i = 1$, we must have $c_i = 1$, so the coefficients of C and D must satisfy

$$\left(\prod_{j<i} (c_j - d_j + 1) \right) c_i(d_i - 1) = 0.$$

In this process, the i-th equation has degree $i + 1$; hence we will not be able to completely ensure $C \geq D$ unless we allow equations with very large degree, significantly hampering computation. Therefore, for practical purposes, we introduce these equations only up to a small i, say 5.

We can introduce similar equations to enforce the restriction $E \geq F$ in an attempt to remove redundant solutions due to τ_2. Finally, we can introduce equations to enforce $C \geq E$ in an attempt to remove redundant solutions due to τ_3. Even though we have not succeeded at eliminating all redundant solutions due to invariant transformations, introducing these equations eliminates much of the redundancy and significantly decreases the time required for computation.

3.2.3 Gröbner basis computation

From the discussion at the beginning of Section 3.2, we saw that unless we could reduce the system of 495 equations in 270 variables, a solution via Gröbner basis techniques would be elusive. By forcing A and B to have the form $A = x_1x_2+x_3x_4$ and $B = y_1y_2+y_3y_4$, we have eliminated the $2\binom{8+2}{2} = 90$ unknowns from the left-hand side of (3.6). Further, AB is a now homogeneous quartic, so we only need to consider homogeneous quadratic polynomials C, D, E, F; hence reducing the number of variables to $4\binom{8+2-1}{2} = 144$ and the number of equations to the number of possible terms of degree 4, i.e. $\binom{8+4-1}{4} = 330$. Since over $\mathbb{F}_2$, squared terms are actually linear, the coefficients of x_i^2 and y_i^2 must be zero. Finally, the second restriction of (3.1) requires C, D, E, F to be oil-vinegar polynomials, so considering the x_i's as vinegar variables and y_i's as oil variables, there can be no terms of the form y_iy_j. Therefore, the total number of variables is reduced to $4\left(\binom{8+2-1}{2} - 8 - \binom{4}{2}\right) = 88$ and the total number of equations is reduced to 164. Now, since each coefficient is an element of $\mathbb{F}_2$, it must statisfy the equation $z^2 + z = 0$. By letting z run through all 88 coefficient variables, we introduce 88 additional equations that will ensure the total degree of the polynomials used during computation is kept low.

I employed the following strategy for computing the solutions to the system of 252 equations in 88 variables using Magma:

1. *Compute the Gröbner basis under a grevlex ordering.* Although a lex ordering is required to subsequently enumerate the solutions, the idea was to determine if there were coefficients that are forced to be zero, and could thus be eliminated. Since the system was large, I had to specialize 4 of the variables and thus compute 16 separate Gröbner bases. In each case, I found that the $4\binom{4}{2} = 24$ variables corresponding to the x_ix_j terms must be zero.

2. *Compute the Gröbner basis of the new system (64 variables) under a lex ordering.* The system was still too large, although now I only had to specialize 2 variables, hence computing 4 Gröbner bases. Also, in this stage, I employed the strategies of Section

3.2.2 to enforce an order on the solution components.

3. *Enumerate and examine all solutions.* Enumerating the solutions described by the 4 Gröbner bases in the previous step gave a total of 264 solutions. However, equivalent solutions can be eliminated (i.e. equivalent by an invariant transformation of the solution vector that was not excluded in the previous step, or by an invariant transformation of the variables). In fact, of the 264 solutions, only 24 are distinct up to an invariant transformation on the solution vector, and all 24 of these are equivalent via a transformation of variables to the MFE solution, thus proving Theorem 3.2.1.

3.2.4 Over more general polynomial rings

The above then tells us there is no new solution to the equation (3.6) over the ring $\mathbb{F}_2[x_1, \ldots, x_4, y_1, \ldots, y_4]$. What happens if we enlarge the ring to $\mathbb{F}_2[x_1, \ldots, x_n, y_1, \ldots, y_n]$ with $n > 4$? We have not been successful so far, and the main difficulty is in the Gröbner basis computation. Another direction is to relax the equation (3.6) to

$$AB = F_1G_1 + \cdots + F_TG_T,$$

where $T \geq 3$ and $F_i, G_i \in \mathbb{F}[x_1, \ldots, x_n, y_1, \ldots, y_n]$.

Much work is yet to be done to solve such problems. The resulting polynomial systems are extremely large, and require much reduction before progress can be made. As a result, I turned to other ideas in my search for polynomial identities. Old results from algebraic geometry were especially enlightening, especially the subjects of Plücker and Grassmann Coordinates.

3.3 Plücker Coordinates

Algebraic geometry provides perhaps the most interesting perspective from which to view the equation $AB = CD + EF$ over the polynomial ring $\mathbb{F}[x_1, \ldots, x_4, y_1, \ldots, y_4]$.

Let $P = (x_1, x_2, x_3, x_4)$ and $Q = (y_1, y_2, y_3, y_4)$ be two distinct points in three-dimensional projective space $\mathbb{P}^3$. We define Plücker coordinates as

$$p_{ij} = \begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix} = x_i y_j - x_j y_i. \tag{3.10}$$

Notice that there are six distinct coordinates as $p_{ij} = -p_{ji}$, so we only consider indices $i < j$. We can also think of them as the 2×2 minors of the matrix

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \end{pmatrix}.$$

We will see that they in fact give an isomorphism between the space of lines in $\mathbb{P}^3$ and the quadric in $\mathbb{P}^5$ defined by

$$p_{12}p_{34} - p_{13}p_{24} + p_{14}p_{23} = 0. \tag{3.11}$$

Notice that this identity is exactly the identity (3.7) used in MFE. Showing that Plücker coordinates satisfy (3.11) can be done in several ways. Two of them are instructive for our purposes; we discuss them here, and generalize the second using a more general structure in Section 3.5.

First, consider a Gröbner basis approach (see [CLO96]) over the polynomial ring in 14 variables:

$$\mathbb{F}[x_1, \ldots, x_4, y_1, \ldots, y_4, p_{12}, \ldots, p_{34}].$$

Consider the ideal

$$I = \langle p_{ij} - (x_i y_j - x_j y_i) : 1 \leq i < j \leq 4 \rangle.$$

Computing with Magma and using a lex ordering with

$$x_1 > \cdots > x_4 > y_1 > \cdots > y_4 > p_{12} > \cdots > p_{34},$$

we see that the last polynomial in the Gröbner basis of I is in fact the Plücker quadric (3.11).

A second approach (see [HP47]) to proving the identity (3.11) involves Laplace expansions of matrix determinants:

$$\begin{aligned}
p_{12}p_{34} - p_{13}p_{24} + p_{14}p_{23} &= \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix} \begin{vmatrix} x_3 & x_4 \\ y_3 & y_4 \end{vmatrix} - \begin{vmatrix} x_1 & x_3 \\ y_1 & y_3 \end{vmatrix} \begin{vmatrix} x_2 & x_4 \\ y_2 & y_4 \end{vmatrix} + \\
&\quad \begin{vmatrix} x_1 & x_4 \\ y_1 & y_4 \end{vmatrix} \begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix} \\
&= x_1 \left(y_2 \begin{vmatrix} x_3 & x_4 \\ y_3 & y_4 \end{vmatrix} - y_3 \begin{vmatrix} x_2 & x_4 \\ y_2 & y_4 \end{vmatrix} + y_4 \begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix} \right) - \\
&\quad y_1 \left(x_2 \begin{vmatrix} x_3 & x_4 \\ y_3 & y_4 \end{vmatrix} - x_3 \begin{vmatrix} x_2 & x_4 \\ y_2 & y_4 \end{vmatrix} + x_4 \begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix} \right) \\
&= x_1 \begin{vmatrix} x_2 & x_3 & x_4 \\ y_2 & y_3 & y_4 \\ y_2 & y_3 & y_4 \end{vmatrix} - y_1 \begin{vmatrix} x_2 & x_3 & x_4 \\ x_2 & x_3 & x_4 \\ y_2 & y_3 & y_4 \end{vmatrix} \\
&= 0,
\end{aligned}$$

where the last equality follows from the fact that both matrices have duplicate rows and hence have zero determinants.

We now focus on the aforementioned isomorphism. Let P and Q be two distinct points on the line $L \subset \mathbb{P}^3$. Define the map ω as

$$\omega(L) = (p_{12}, p_{13}, p_{14}, p_{23}, p_{24}, p_{34}) \in \mathbb{P}^5,$$

where p_{ij} are the Plücker coordinates defined in (3.10). It can be easily shown that ω is well-defined, as it does not depend on the choice of P and Q, and at least one coordinate is nonzero.

Theorem 3.3.1 (Theorem 8.6.11, [CLO96]). *The map*

$$\{\text{lines in } \mathbb{P}^3\} \xrightarrow{\omega} \{(z_{12}, z_{13}, z_{14}, z_{23}, z_{24}, z_{34}) \in \mathbb{P}^5 : z_{12}z_{34} - z_{13}z_{24} + z_{14}z_{23} = 0\},$$

which sends a line $L \subset \mathbb{P}^3$ to its Plücker coordinates $\omega(L)$, is a bijection.

Proof. Let $A = (x_1, x_2, x_3, x_4)$ and $B = (y_1, y_2, y_3, y_4)$ be two points on L. First, we show ω is injective. Suppose $\omega(L) = \lambda\omega(L')$ for some $\lambda \neq 0$, i.e. $p_{ij} = \lambda p'_{ij}$, $1 \leq i < j \leq 4$. Without loss of generality, assume $p_{12} \neq 0$. Then the point

$$P = (0, -p'_{12}, -p'_{13}, -p'_{14}) = \frac{1}{\lambda}(0, -p_{12}, -p_{13}, -p_{14}) = (0, -p_{12}, -p_{13}, -p_{14})$$

lies on both L and L' since $y_1A - x_1B = (0, -p_{12}, -p_{13}, -p_{14})$ is a point of L (a similar equation holds for L'). Also, the point

$$Q = (p'_{12}, 0, -p'_{23}, -p'_{24}) = \frac{1}{\lambda}(p_{12}, 0, -p_{23}, -p_{24}) = (p_{12}, 0, -p_{23}, -p_{24})$$

lies on both L and L' since $y_2A - x_2B = (p_{12}, 0, -p_{23}, -p_{24})$ is a point of L. Since two points determine a unique line, $L = L'$. Next, we show ω is surjective. Let $(p_{12}, p_{13}, p_{14}, p_{23}, p_{24}, p_{34})$ be on the quadric. Again, without loss of generality, assume $p_{12} \neq 0$, and let L be the line determined by the points

$$(0, -p_{12}, -p_{13}, -p_{14}) \quad \text{and} \quad (p_{12}, 0, -p_{23}, -p_{24}).$$

Then simple calculations show

$$\begin{aligned} \omega(L) &= p_{12}(p_{12}, p_{13}, p_{14}, p_{23}, p_{24}, \frac{1}{p_{12}}(p_{13}p_{24} - p_{14}p_{23})) \\ &= (p_{12}, p_{13}, p_{14}, p_{23}, p_{24}, p_{34}). \end{aligned}$$

□

So, we have established a bijection from the space of lines in $\mathbb{P}^3$ to a projective variety in $\mathbb{P}^5$ defined by a quadric with nice properties (in particular, with the properties specified at the outset in (3.1)). The natural question is then: can we generalize these ideas to higher dimensions in order to create more general polynomial identities? The first direction, addressed in Section 3.4, involves increasing the the number of variables and working directly with matrix determinants to try to find identities like the Plücker quadric (3.11). The second direction utilizes the generalization of Plücker coordinates known as Grassmann coordinates and is addressed in Section 3.5.

3.4 Determinants in Higher Dimensions

Recall that the key observation of the determinant proof of (3.11) was that matrices with duplicate rows (or columns) have zero determinant. The Plücker quadric exploited 3×3 matrices over $\mathbb{F}[x_1, \ldots, x_4, y_1, \ldots, y_4]$, so one idea is to add four new variables and consider 4×4 matrices over $R = \mathbb{F}[x_1, \ldots, x_4, y_1, \ldots, y_4, z_1, \ldots, z_4]$.

Since we are introducing more variables, it will be helpful to redefine Plücker coordinates to take into account the variables involved. Let

$$p_{xy}^{ij} = \begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix} = x_i y_j - x_j y_i, \quad 1 \leq i < j \leq 4.$$

Even though a 4×4 matrix in general has a quartic determinant, by expanding it along the first two columns, we can group it into an equation of the form

$$AB + f_1 f_2 + f_3 f_4 + f_5 f_6 + f_7 f_8 + f_9 f_{10},$$

i.e.,

$$\begin{vmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{vmatrix} = p_{ab}^{12}p_{cd}^{34} - p_{ab}^{13}p_{cd}^{24} + p_{ab}^{14}p_{cd}^{23} + p_{ab}^{23}p_{cd}^{14} - p_{ab}^{24}p_{cd}^{13} + p_{ab}^{34}p_{cd}^{12}.$$

Adding together two matrices (both having first, third, and fourth columns x, y, and z respectively, and each having second column y, and z respectively), we have

$$\begin{aligned} 0 &= \begin{vmatrix} x_1 & y_1 & y_1 & z_1 \\ x_2 & y_2 & y_2 & z_2 \\ x_3 & y_3 & y_3 & z_3 \\ x_4 & y_4 & y_4 & z_4 \end{vmatrix} + \begin{vmatrix} x_1 & z_1 & y_1 & z_1 \\ x_2 & z_2 & y_2 & z_2 \\ x_3 & z_3 & y_3 & z_3 \\ x_4 & z_4 & y_4 & z_4 \end{vmatrix} \\ &= (p_{xy}^{12} + p_{xz}^{12})p_{yz}^{34} - (p_{xy}^{13} + p_{xz}^{13})p_{yz}^{24} + (p_{xy}^{14} + p_{xz}^{14})p_{yz}^{23} + \\ &\quad (p_{xy}^{23} + p_{xz}^{23})p_{yz}^{14} - (p_{xy}^{24} + p_{xz}^{24})p_{yz}^{13} + (p_{xy}^{34} + p_{xz}^{34})p_{yz}^{12}. \end{aligned} \tag{3.12}$$

To put (3.12) in the required oil-vinegar form, define $\rho : R \to \mathbb{F}[X_1, \ldots, X_6, Y_1, \ldots, Y_6]$ as a ring isomorphism induced by

$$(x_1, \ldots, z_4) \mapsto (X_1, X_3, Y_5, Y_6, X_6, X_5, Y_1, Y_3, X_4 - X_6, X_2 - X_5, Y_4, Y_2)$$

and set

$$\begin{aligned} A &= X_1X_2 - X_3X_4 \\ B &= Y_1Y_2 - Y_3Y_4 \\ f_1 &= X_1(Y_1 + Y_4) - X_4Y_5 \\ f_2 &= X_5Y_2 - (X_2 - X_5)Y_3 \\ f_3 &= X_1(Y_2 + Y_3) - X_4Y_6 \end{aligned}$$

$$
\begin{aligned}
f_4 &= X_5Y_4 - (X_2 - X_5)Y_1 \\
f_5 &= X_3(Y_1 + Y_4) - X_2Y_5 \\
f_6 &= X_6Y_2 - (X_4 - X_6)Y_3 \\
f_7 &= X_3(Y_2 + Y_3) - X_2Y_6 \\
f_8 &= X_6Y_4 - (X_4 - X_6)Y_1 \\
f_9 &= Y_5(Y_2 + Y_3) - Y_6(Y_1 + Y_4) \\
f_{10} &= X_2X_6 - X_4X_5.
\end{aligned}
$$

which gives us the structure we want. We now make some comments on this system of equations:

- The rank of each polynomial is 4.
- There are 8 oil-vinegar polynomials $(f_1, \ldots, f_8)$. Viewing the X_i's as vinegar variables, we would need to solve for only 6 oil-variables $Y_1, \ldots, Y_6$. Along with f_9 and f_{10}, this leaves us with 4 extra equations, thus harming the information rate of any cryptosystem that uses this identity.
- When X_i, $1 \leq i \leq 6$, and f_i, $1 \leq i \leq 8$, take on values in $\mathbb{F}$, we hope to be able to solve uniquely the resulting linear system for the oil variables $Y_1, \ldots, Y_6$. In this case, the system is not solvable with probability approximately $\frac{2}{|\mathbb{F}|}$. On the other hand, if we let Y_i, $1 \leq i \leq 6$ take on values in $\mathbb{F}$, the resulting linear system is again not solvable with probability approximately $\frac{2}{|\mathbb{F}|}$.

Since our ultimate purpose for such a polynomial identity is to use it create a good cryptosystem, and the above comments reveal that such a system would be of low rank, have poor information rate, and be subject to a significant rate of decryption failure, we therefore conclude that we need to find a "better" identity. However, as we shall see, the idea of adding more variables and considering larger matrices is not without merit.

Consider the polynomial ring $R = \mathbb{F}[x_1, \ldots, x_4, y_1, \ldots, y_4, z_1, \ldots, z_4, w_1, \ldots, w_4]$.

Observe that the matrix

$$M_x = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ x_1 & x_1 & y_1 & z_1 & w_1 \\ x_2 & x_2 & y_2 & z_2 & w_2 \\ x_3 & x_3 & y_3 & z_3 & w_3 \\ x_4 & x_4 & y_4 & z_4 & w_4 \end{bmatrix}$$

has zero determinant since the first two columns are dependent. By Laplace expansion on the first row, the determinant is the sum of the determinants of the five 4×4 minors. We introduce the following notation:

$$|\mathbf{xyzw}| = \begin{vmatrix} x_1 & y_1 & z_1 & w_1 \\ x_2 & y_2 & z_2 & w_2 \\ x_3 & y_3 & z_3 & w_3 \\ x_4 & y_4 & z_4 & w_4 \end{vmatrix}.$$

We can write the other four minors in a similar way, so

$$\begin{aligned} |M_x| &= |\mathbf{xyzw}| - |\mathbf{xyzw}| + |\mathbf{xxzw}| - |\mathbf{xxyw}| + |\mathbf{xxyz}| \\ &= |\mathbf{xxzw}| - |\mathbf{xxyw}| + |\mathbf{xxyz}| \end{aligned}$$

Now define the matrices M_y, M_z, and M_w by replacing each of the x_i's in the first column of M_x by y_i, z_i, and w_i, respectively. (In the following equations, note that since each matrix has a duplicate column, the sign of the determinant is irrelevant, and we choose it to be

positive.) Then

$$\begin{aligned}
0 &= |M_x| + |M_y| + |M_z| + |M_w| \\
&= |\mathbf{xxzw}| + |\mathbf{xxyw}| + |\mathbf{xxyz}| + \\
&\quad |\mathbf{yyzw}| + |\mathbf{yxyw}| + |\mathbf{yxyz}| + \\
&\quad |\mathbf{zyzw}| + |\mathbf{zxzw}| + |\mathbf{zxyz}| + \\
&\quad |\mathbf{wyzw}| + |\mathbf{wxzw}| + |\mathbf{wxyw}| \\
&= |\mathbf{xxyw}| + |\mathbf{xxyz}| + |\mathbf{yxyw}| + |\mathbf{yxyz}| + |\mathbf{zxyz}| + |\mathbf{wxyw}| + \quad \text{(grouping } \mathbf{xy}\text{'s)} \\
&\quad |\mathbf{xxzw}| + |\mathbf{yyzw}| + |\mathbf{zyzw}| + |\mathbf{zxzw}| + |\mathbf{wyzw}| + |\mathbf{wxzw}| \quad \text{(grouping } \mathbf{zw}\text{'s)} \\
&= |\mathbf{xyxw}| + |\mathbf{xyxz}| + |\mathbf{xyyw}| + |\mathbf{xyyz}| + |\mathbf{xyzz}| + |\mathbf{xyww}| + \\
&\quad |\mathbf{zwxx}| + |\mathbf{zwyy}| + |\mathbf{zwyz}| + |\mathbf{zwxz}| + |\mathbf{zwyw}| + |\mathbf{zwxw}| \\
&= |\mathbf{xyxw}| + |\mathbf{xyxz}| + |\mathbf{xyyw}| + |\mathbf{xyyz}| + \quad (\text{since } |\mathbf{xyzz}| = |\mathbf{xyww}| = 0) \qquad (3.13) \\
&\quad |\mathbf{zwxw}| + |\mathbf{zwxz}| + |\mathbf{zwyw}| + |\mathbf{zwyz}| \quad (\text{since } |\mathbf{zwxx}| = |\mathbf{zwyy}| = 0) \qquad (3.14)
\end{aligned}$$

As before, we write determinants using Plücker coordinates and group terms to give an equation of the form (3.1) with $n = 8$ and $t = 2$. In particular, the first term of (3.13) becomes

$$|\mathbf{xyxw}| = p_{xy}^{12}p_{xw}^{34} + p_{xy}^{13}p_{xw}^{24} + p_{xy}^{14}p_{xw}^{23} + p_{xy}^{23}p_{xw}^{14} + p_{xy}^{24}p_{xw}^{13} + p_{xy}^{34}p_{xw}^{12}. \qquad (3.15)$$

So, defining

$$p_{ij} = p_{xw}^{ij} + p_{xz}^{ij} + p_{yw}^{ij} + p_{yz}^{ij}, \quad 1 \le i \le 4, \qquad (3.16)$$

the four determinants of (3.13) can be grouped as

$$p_{xy}^{12}p_{34} + p_{xy}^{13}p_{24} + p_{xy}^{14}p_{23} + p_{xy}^{23}p_{14} + p_{xy}^{24}p_{13} + p_{xy}^{34}p_{12}.$$

After performing a similar grouping for (3.14), we get the the identity

$$\begin{aligned} 0 &= (p_{xy}^{12} + p_{zw}^{12})p_{34} + (p_{xy}^{13} + p_{zw}^{13})p_{24} + (p_{xy}^{14} + p_{zw}^{14})p_{23} + \\ &\quad (p_{xy}^{23} + p_{zw}^{23})p_{14} + (p_{xy}^{24} + p_{zw}^{24})p_{13} + (p_{xy}^{34} + p_{zw}^{34})p_{12}. \end{aligned} \tag{3.17}$$

We now make two comments regarding this identity, and the system that arises from it:

- While the polynomials $p_{xy}^{ij} + p_{zw}^{ij}$ have rank 8, the polynomials p_{ij} only have rank 4, so the minimum rank of the system is 4.
- A cryptosystem based directly on (3.17) is susceptible to a linearization equations attack. In fact, for a random ciphertext, the average dimension of the linearization equation space is 15, with a maximum of at least 28.

However, we can construct an identity very similar to (3.17) that avoids these problems, and Chapter 4 presents the complete details of the new cryptosystem.

3.5 Grassmann Coordinates

While the previous section explained a seemingly ad hoc method of obtaining polynomial identities by expanding determinants and grouping terms nicely, the goal of this section is to develop a more concrete, algebraic approach to the subject using Grassmann coordinates. We will follow Hodge and Pedoe's [HP47] treatment of the material, culminating with a basis theorem that provides an excellent method for constructing polynomial identities. This basis theorem will give us a good foundation from which to build identities such as (3.15) and (3.17).

3.5.1 Preliminaries

Points in projective space. Consider n-dimensional project space, $\mathbb{P}^n$, over a base field $\mathbb{F}$. A *point*, A, in $\mathbb{P}^n$ is be represented as

$$A = [\alpha_0, \ldots, \alpha_n],$$

where the α_i's are not all zero. Recall that in projective space, two points $A = [\alpha_0, \ldots, \alpha_n]$ and $B = [\beta_0, \ldots, \beta_n]$ are equivalent if there exists a $\lambda \in \mathbb{F}$ such that $A = \lambda B$.

Linear subspaces. Let $A^0, \ldots, A^k$ be $k+1$ linearly independent points of $\mathbb{P}^n$. Then the set of all linear combinations of these points is a *linear subspace*, S_k, of dimension k. Further, the arbitrary points

$$A^0 = (\alpha_0^0, \ldots, \alpha_n^0), \ldots, A^k = (\alpha_0^k, \ldots, \alpha_n^k) \in \mathbb{P}^n,$$

determine a k-dimensional subspace S_k if and only if the matrix

$$A = \begin{pmatrix} \alpha_0^0 & \ldots & \alpha_n^0 \\ \vdots & & \vdots \\ \alpha_0^k & \ldots & \alpha_n^k \end{pmatrix}$$

has rank $k+1$, and we say $A^0, \ldots, A^k$ form a basis for S_k. Notice that if $L \in \mathbb{F}^{k+1 \times k+1}$ is an invertible transformation, then the matrix $B = LA$ defines the same subspace. For the remainder of the discussion, we will assume $k \neq 0$ and $k \neq n-1$, i.e., we consider only proper subspaces.

Grassmann coordinates Let S_k have basis $A^0, \ldots, A^k$. Choose $k+1$ distinct indices from $\{0, \ldots, n\}$: $i_0, \ldots, i_k$, and compute the determinant of the $k+1 \times k+1$ matrix formed

by selecting the i_0-th, ..., i_k-th columns from A:

$$p_{i_0 \dots i_k} = \begin{vmatrix} \alpha_{i_0}^0 & \dots & \alpha_{i_k}^0 \\ \vdots & & \vdots \\ \alpha_{i_0}^k & \dots & \alpha_{i_k}^k \end{vmatrix}. \tag{3.18}$$

Notice that the $p_{i_0 \dots i_k}$ are skew-symmetric in their indices, since swapping two indices is equivalent to swapping two columns in the matrix, resulting in a change of sign of the determinant. In fact, any permutation of the indices results in multiplying by a power of -1, so we only consider $\binom{n+1}{k+1}$ possible choices for the set of indices. We call an $\binom{n+1}{k+1}$-tuple $(\dots, p_{i_0 \dots i_k}, \dots)$ the *Grassmann coordinates* of S_k. Notice that the components cannot be all simultaneously zero, since this would imply $\operatorname{rank}(A) < k+1$; thus we can consider the Grassmann coordinates of S_k as a point in $\mathbb{P}^{\binom{n+1}{k+1}-1}$. Also, if we have an equivalent basis matrix $B = LA$, then upon taking determinants of submatrices, we find that the individual coordinates are equivalent up to a nonzero constant (i.e. $|L|$), and are thus equal as elements of $\mathbb{P}^{\binom{n+1}{k+1}-1}$.

It can be shown that distinct subspaces of $\mathbb{P}^n$ have distinct Grassmann coordinates. In particular, this gives the injection

$$\{S_k : S_k \text{ a subspace of } \mathbb{P} \text{ of dimension } k\} \hookrightarrow \mathbb{P}^{\binom{n+1}{k+1}-1}. \tag{3.19}$$

As with Plücker coordinates (simply Grassmann coordinates with $n = 3, k = 1$), we will see that there is actually an isomorphism via Grassmann coordinates from the set of k-dimensional subpaces of $\mathbb{P}^n$ to a projective variety in $\mathbb{P}^{\binom{n+1}{k+1}-1}$ defined by quadratic polynomials.

Quadratic relations. Consider $\mathbb{F}[\dots, P_{i_0 \dots i_k}, \dots]$, the polynomial ring in $\binom{n+1}{k+1}$ indeterminates that are skew-symmetric in their indices. We note first that it can be shown that

there is no linear relation

$$\sum_{i_0,\ldots,i_k} u_{i_0\ldots i_k} P_{i_0\ldots i_k}, \quad u_{i_0\ldots i_k} \in \mathbb{F},$$

that is identically zero when evaluated at the Grassmann coordinates of every S_k; however, there are quadratic relations (this is to be expected, considering (3.11)). Let $i_1, \ldots, i_k$ be distinct indices from $\{0, \ldots, n\}$, and $j_0, \ldots, j_{k+1}$ be distinct indices also from $\{0, \ldots, n\}$. Define

$$F_{i_1\ldots i_k, j_0\ldots j_{k+1}}(P) = \sum_{\lambda=0}^{k+1} (-1)^\lambda P_{i_1\ldots i_k j_\lambda} P_{j_0\ldots j_{\lambda-1} j_{\lambda+1}\ldots j_{k+1}}. \tag{3.20}$$

Then replacing, for any S_k, the indeterminate $P_{i_0\ldots i_k}$ with the corresponding Grassmann coordinate $p_{i_0\ldots i_k}$, we have

$$F_{i_1\ldots i_k, j_0\ldots j_{k+1}}(p) = 0. \tag{3.21}$$

The proof of (3.21) is a straightforward generalization of the determinant proof of (3.11).

Define the *generic k-dimensional subspace* as the subspace determined by the $k+1$ points $A^0, \ldots, A^k$, where the components $\alpha_0^i, \ldots, \alpha_n^i$ of A^i, $1 \le i \le k$, are indeterminates. Then, replacing the indeterminate $P_{i_0\ldots i_k}$ in (3.20) with the corresponding Grassmann coordinate $p_{i_0\ldots i_k}$ of the generic k-dimensional subspace, we see that $F_{i_1\ldots i_k, j_0\ldots j_{k+1}}(p)$ is in fact equal to zero as a polynomial in the ring

$$\mathbb{F}[\alpha_0^0, \ldots, \alpha_n^0, \ldots, \alpha_0^k, \ldots, \alpha_n^k].$$

Example 3.5.1. Let the points $A^0 = (x_0, x_1, x_2, x_3)$ and $A^1 = (y_0, y_1, y_2, y_3)$ be a basis for a one-dimensional subspace, $S_1 \subset \mathbb{P}^3$, so the Grassmann coordinates of S_1 are given by the 2×2 minors of the matrix

$$\begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 \end{pmatrix}.$$

Let $i_1 = 0, j_0 = 1, j_1 = 2, j_2 = 3$. Then (3.20) gives

$$p_{01}p_{23} - p_{02}p_{13} + p_{03}p_{12} = 0,$$

which is the same as (3.11), except our indices now start at 0 instead of 1.

We can now state two important theorems regarding Grassmann coordinates.

Theorem 3.5.1 (Theorem VII.6.II, [HP47]). *If* $(\dots, p_{i_0\dots i_k}, \dots)$ *are* $\binom{n+1}{k+1}$ *elements of* $\mathbb{F}$ *which are not all zero, which are skew-symmetric in the suffixes, and which satisfy* (3.21)*, then there is a* k*-dimensional subspace of* $\mathbb{P}^n$ *which has coordinates* $(\dots, p_{i_0\dots i_k}, \dots)$.

This theorem, along with the previous result (3.19), establishes in general the isomorphism

$$\{k\text{-dimensional subspaces of } \mathbb{P}^n\} \cong \mathbf{V} \subset \mathbb{P}^{\binom{n+1}{k+1}-1},$$

where $\mathbf{V}$ is the projective variety defined by the quadratics of (3.20). Notice Theorem 3.3.1 about Plücker coordinates is a special case of this isomorphism.

Theorem 3.5.2 (Basis Theorem, Theorem VII.7.I, [HP47]). *If* $F(P)$ *is any homogeneous polynomial in* $P_{i_0\dots i_k}$ *such that* $F(p) = 0$ *for all* S_k*, then*

$$F(P) = \sum_{i,j} A_{i_1\dots i_k, j_0\dots j_{k+1}}(P) F_{i_1\dots i_k, j_0\dots j_{k+1}}(P),$$

where $F_{i_1\dots i_k, j_0\dots j_{k+1}}(P)$ *is the quadratic form defined in* (3.20)*, and* $A_{i_1\dots i_k, j_0\dots j_{k+1}}(P)$ *is a homogeneous polynomial in* $P_{i_0\dots i_k}$.

3.5.2 Constructing more identities

We are interested in applying the above theorems to generic k-dimensional subspaces. If $(\dots, p_{i_0\dots i_k}, \dots)$ gives the Grassmann coordinates of a generic k-dimensional subspace, then we can rephrase Theorem 3.5.2 in the language of ideals to say that if

$f \in \mathbb{F}[\dots, P_{i_0 \dots i_k}, \dots]$ vanishes on $(\dots, p_{i_0 \dots i_k}, \dots)$, then

$$f \in \Big\langle \sum_{\lambda=0}^{k+1} (-1)^\lambda P_{i_1 \dots i_k j_\lambda} P_{j_0 \dots j_{\lambda-1} j_{\lambda+1} \dots j_{k+1}} \Big\rangle \subset \mathbb{F}[\dots, P_{i_0 \dots i_k}, \dots].$$

This gives us the power to build all sorts of polynomial identities. However, for the time being, we are interested in identities with quadratic polynomials, therefore limiting us to one-dimensional subspaces of $\mathbb{P}^n$.

Example 3.5.2. Let $n = 7$, and consider the generic subspace $S_1 \subset \mathbb{P}^7$ given by the matrix

$$\begin{pmatrix} x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \\ y_0 & y_1 & y_2 & y_3 & y_4 & y_5 & y_6 & y_7 \end{pmatrix}.$$

There are $\binom{7+1}{1+1} = 28$ Grassmann coordinates, and we wish to determine the number of quadratic relations (3.21). Fix $i_1 \in \{0, \dots, n\}$, and let $j_0, j_1, j_2 \in \{0, \dots, n\}$ be distinct. If one of the j's, without loss of generality j_0, is equal to i_1, then (3.20) becomes

$$\begin{aligned} F_{i_1, j_0 j_1 j_2}(p) &= \sum_{\lambda=0}^{2} (-1)^\lambda p_{i_1 j_\lambda} p_{j_0 \dots j_{\lambda-1} j_{\lambda+1} \dots j_{k+1}} \\ &= p_{i_1 j_0} p_{j_1 j_2} - p_{i_1 j_1} p_{j_0 j_2} + p_{i_1 j_2} p_{j_0 j_1} \\ &= p_{i_1 i_1} p_{i_1 j_2} - p_{i_1 j_1} p_{i_1 j_2} + p_{i_1 j_2} p_{i_1 j_1}, \end{aligned}$$

which is trivially zero since $p_{i_1 i_1} = 0$. Thus we get nontrivial relations only when the j's are distinct from i_1. This amounts to choosing 4 distinct indices from $\{0, \dots, n\}$, so there are $\binom{7+1}{4} = 70$ quadratic relations.

One way to make things more interesting, and in fact achieve the identity (3.15), is to restrict ourselves to a smaller space inside the generic space $S_1 \subset \mathbb{P}^n$.

Example 3.5.3. Let $n = 7$, and consider the subspace $S_1' \subset S_1$ given by the matrix

$$\begin{pmatrix} x_0 & x_1 & x_2 & x_3 & x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 & w_0 & w_1 & w_2 & w_3 \end{pmatrix},$$

where the second four components of the first point have been repeated. In this case, in addition to quadratic relations, the Grassmann coordinates also satisfy some linear relations. This fits our intuition, since if this smaller subspace $S_1' \subset \mathbb{P}^7$ is to be isomorphic to a projective variety in $\mathbb{P}^{27}$, the projective variety should be smaller than the one corresponding to S_1; this is accomplished by introducing more defining equations. Notice that for $0 \leq i < j \leq 4$, we have

$$\begin{aligned} & p_{ij} + p_{j,i+4} + p_{i+4,j+4} - p_{i,j+4} \\ &= (x_i y_j - x_j y_i) + (x_j w_i - x_i y_j) + (x_i w_j - x_j w_i) - (x_i w_j - x_j y_i) \\ &= 0. \end{aligned}$$

Denoting these 6 polynomials as G_{ij}, we can now write the identity (3.15) in terms of the "basis" polynomials of (3.20) and these additional linear relations:

$$\begin{aligned} & p_{xy}^{12} p_{xw}^{34} + p_{xy}^{13} p_{xw}^{24} + p_{xy}^{14} p_{xw}^{23} + p_{xy}^{23} p_{xw}^{14} + p_{xy}^{24} p_{xw}^{13} + p_{xy}^{34} p_{xw}^{12} \\ &= p_{01} p_{67} + p_{02} p_{57} + p_{03} p_{56} + p_{12} p_{47} + p_{13} p_{46} + p_{23} p_{45} \\ &= F_{0,567} + F_{1,467} + F_{2,457} + F_{3,456} + \\ &\quad p_{67} G_{01} + p_{57} G_{02} + p_{56} G_{03} + p_{47} G_{12} + p_{46} G_{13} + p_{45} G_{23}, \end{aligned}$$

where the first equality is simply a transition from notation used in Section 3.4 to the notation used in the current section.

We can similarly express (3.17) in terms of quadratic and linear relations on Grassmann coordinates of a linear subspace $S_1 \subset \mathbb{P}^{23}$. This is also the case with the identity used to build the new cryptosystem presented in Chapter 4.

3.5.3 Open questions

Using these tools, we see that we can construct various polynomial identities. However, the question remains: will such identities be useful for building multivariate public

key cryptosystem. As we will see in Chapter 4, the answer is definitely yes. However, I believe that there is much left to be explored regarding these types of polynomial identities, as evidenced by the following open questions:

- As in Example 3.5.2, one obvious way of creating more identities is to increase n, and so far only a few cases have been examined. What other values of n yield nice identities?

- As in Example 3.5.3, if we work with subspaces of S_k, other relations arise which become useful in constructing identities. How can we determine what other subspaces will yield profitable results?

- As mentioned before, $p_{i_0 \ldots i_k}$ is a degree $k+1$ polynomial in the components of the points $A^0, \ldots, A^k$. We have only considered the case $k = 1$. Can identities produced by using larger values of k be used in multivariate public key cryptography?

Clearly the above list is not exhaustive, and future exploration in these directions should prove to be interesting. As a final note, there is yet another perspective from which to view identities involving Plücker coordinates. Howard et al. [HMSV09] present the quadric relations and give an interesting way to view the identities through the process of "uncrossing" edges in a graph.

Chapter 4

Construction and Analysis of the New Cryptosystem

4.1 Polynomial Identity

In Section 3.4, we developed some new identities ((3.12) and (3.17)) that satisfied the requirements laid out at the beginning of Chapter 3. However, recall that these identities had some undesirable qualities in view of the fact that our goal is to construct a new cryptosystem. In particular, the second identity (3.17), had two problems: some of the polynomials had rank 4, and more importantly, linearization equations existed. A closer inspection of the identity reveals that these problems are caused by the fact that the right-hand side of (3.16), i.e.

$$p_{xw}^{ij} + p_{xz}^{ij} + p_{yw}^{ij} + p_{yz}^{ij}, \tag{4.1}$$

can be grouped as

$$(x_i + y_i)(w_j + z_j) - (x_j + y_j)(w_i + z_i). \tag{4.2}$$

Thus, although (4.1) is a sum of four rank 4 polynomials, the sum itself only has rank 4. Also, the fact that x_i and y_i can be grouped into a single term causes linearization equations to exist (similarly, the other terms of (4.2) cause more linearization equations to exist). We

can avoid this problem by simply removing one of the terms from (4.1). Notice that this deletion is valid since, for instance, removing the p_{xw}^{ij} term is equivalent to removing the $|\mathbf{xyxw}|$ and $|\mathbf{zwxw}|$ determinants from (3.13) and (3.14), respectively, and the identity (3.17) still holds.

We now more explicitly develop the identity that we will use to construct our new cryptosystem. Let $\mathbb{F}$ be a degree d extension of k having characteristic two. Define the polynomial ring

$$R = \mathbb{F}[x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4, z_1, z_2, z_3, z_4, w_1, w_2, w_3, w_4].$$

As discussed above, define

$$p^{ij}(x, y, z, w) = p_{xz}^{ij} + p_{yz}^{ij} + p_{yw}^{ij}, \quad 1 \leq i < j \leq 4,$$

where we have removed the p_{xw}^{ij} term from (4.1). Then the identity (3.17) becomes

$$\begin{aligned} 0 \;=\; & (p_{xy}^{12} + p_{zw}^{12})p^{34}(x, y, z, w) + (p_{xy}^{13} + p_{zw}^{13})p^{24}(x, y, z, w) + \\ & (p_{xy}^{14} + p_{zw}^{14})p^{23}(x, y, z, w) + (p_{xy}^{23} + p_{zw}^{23})p^{14}(x, y, z, w) + \\ & (p_{xy}^{24} + p_{zw}^{24})p^{13}(x, y, z, w) + (p_{xy}^{34} + p_{zw}^{34})p^{12}(x, y, z, w). \end{aligned} \tag{4.3}$$

To put (4.3) in the required oil-vinegar form, define $\rho : R \to \mathbb{F}[X_1, \ldots, X_8, Y_1, \ldots, Y_8]$ as a ring isomorphism induced by

$$\begin{aligned} & (x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4, z_1, z_2, z_3, z_4, w_1, w_2, w_3, w_4) \mapsto \\ & \quad (X_1, X_3, Y_1 + Y_5, Y_3 + Y_7, X_4, X_2, Y_5, Y_7, X_5, X_7, Y_4 + Y_8, Y_2 + Y_6, X_8, X_6, Y_8, Y_6), \end{aligned}$$

where, $\rho(x_1) = X_1, \rho(x_2) = X_3, \rho(x_3) = Y_1 + Y_5$, and so on. Then set

$$\begin{array}{rclcl}
\psi_1 & = & \rho(p_{xy}^{12} + p_{zw}^{12}) & = & X_1X_2 + X_3X_4 + X_5X_6 + X_7X_8 \\
\psi_2 & = & \rho(p^{34}(x,y,z,w)) & = & Y_1Y_2 + Y_3Y_4 + Y_5Y_6 + Y_7Y_8 \\
f_1 & = & \rho(p_{xy}^{13} + p_{zw}^{13}) & = & X_4Y_1 + X_8Y_4 + (X_1 + X_4)Y_5 + X_5Y_8 \\
f_2 & = & \rho(p^{24}(x,y,z,w)) & = & (X_2 + X_3)Y_2 + X_7Y_3 + X_2Y_6 + X_6Y_7 \\
f_3 & = & \rho(p_{xy}^{14} + p_{zw}^{14}) & = & X_8Y_2 + X_4Y_3 + X_5Y_6 + (X_1 + X_4)Y_7 \\
f_4 & = & \rho(p^{23}(x,y,z,w)) & = & X_7Y_1 + (X_2 + X_3)Y_4 + X_6Y_5 + X_2Y_8 \\
f_5 & = & \rho(p_{xy}^{23} + p_{zw}^{23}) & = & X_2Y_1 + X_6Y_4 + (X_2 + X_3)Y_5 + X_7Y_8 \\
f_6 & = & \rho(p^{14}(x,y,z,w)) & = & (X_1 + X_4)Y_2 + X_5Y_3 + X_4Y_6 + X_8Y_7 \\
f_7 & = & \rho(p_{xy}^{24} + p_{zw}^{24}) & = & X_6Y_2 + X_2Y_3 + X_7Y_6 + (X_2 + X_3)Y_7 \\
f_8 & = & \rho(p^{13}(x,y,z,w)) & = & X_5Y_1 + (X_1 + X_4)Y_4 + X_8Y_5 + X_4Y_8 \\
f_9 & = & \rho(p_{xy}^{34} + p_{zw}^{34}) & = & Y_1Y_7 + Y_2Y_8 + Y_3Y_5 + Y_4Y_6 \\
f_{10} & = & \rho(p^{12}(x,y,z,w)) & = & X_1X_7 + X_2(X_5 + X_8) + X_3X_5 + X_4(X_6 + X_7)
\end{array} \tag{4.4}$$

thus satisfying (3.1), i.e. $\psi_1\psi_2 = f_1f_2 + f_3f_4 + f_5f_6 + f_7f_8 + f_9f_{10}$.

We now examine the oil-vinegar part of (4.4): $f_1, \ldots, f_8$. First consider the case where $X_1, \ldots, X_8$ are the vinegar variables. This yields the following linear system:

$$\begin{bmatrix}
X_4 & 0 & 0 & X_8 & X_1 + X_4 & 0 & 0 & X_5 \\
0 & X_2 + X_3 & X_7 & 0 & 0 & X_2 & X_6 & 0 \\
0 & X_8 & X_4 & 0 & 0 & X_5 & X_1 + X_4 & 0 \\
X_7 & 0 & 0 & X_2 + X_3 & X_6 & 0 & 0 & X_2 \\
X_2 & 0 & 0 & X_6 & X_2 + X_3 & 0 & 0 & X_7 \\
0 & X_1 + X_4 & X_5 & 0 & 0 & X_4 & X_8 & 0 \\
0 & X_6 & X_2 & 0 & 0 & X_7 & X_2 + X_3 & 0 \\
X_5 & 0 & 0 & X_1 + X_4 & X_8 & 0 & 0 & X_4
\end{bmatrix}
\begin{bmatrix} Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \\ Y_5 \\ Y_6 \\ Y_7 \\ Y_8 \end{bmatrix}
=
\begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \\ f_8 \end{bmatrix}.$$

When X_i and f_i, $1 \leq i \leq 8$, take on values in $\mathbb{F}$, we hope to be able to solve uniquely the

above system for the oil variables $Y_1, \ldots, Y_8$. This will be possible whenever the coefficient matrix has nonzero determinant. The determinant is given by

$$\big((X_1 + X_5 + X_8)(X_2 + X_7) + (X_3 + X_6 + X_7)(X_4 + X_5)\big)^4.$$

On the other hand, if we view $Y_1, \ldots, Y_8$ as the oil variables, the determinant of the resulting linear system in $X_1, \ldots, X_8$ becomes

$$\big((Y_1 + Y_8)(Y_2 + Y_7) + (Y_3 + Y_6)(Y_4 + Y_5)\big)^4.$$

In both cases, the probability that the determinant is zero is $\frac{1}{|\mathbb{F}|} + \frac{1}{|\mathbb{F}|^2} - \frac{1}{|\mathbb{F}|^3}$.

4.2 Building a Cryptosystem

Although we now have an identity where each polynomial has rank 8 and no linearization equations exist, unfortunately, a cryptosystem based directly on (4.4) will be susceptible to a separation of oil and vinegar variables attack. Recall from Section 2.3.5 that a separation of oil and vinegar variables attack succeeds if the size of a maximal oil set is too large, but also that the size of a maximal oil set is inversely related to the number of distinct products appearing in the system of equations. A cryptosystem constructed by chaining together systems of the form (4.4) will have a large oil set since the absence of p_{xw}^{ij} terms from (4.3) results in a significant decrease in the number of distinct products in the system. To avoid this attack, we remove different products from each of the chained oil-vinegar systems by introducing three additional, slightly different subsystems.

Note that each permutation of x, y, z and w in (4.3) yields a new identity. In particular, when exchanging x with y, or z with w, the first factor of each term of (4.3) remains unchanged. We shall take advantage of this. Renaming each ψ_j and f_j in (4.4) as

$\psi_{1,j}$ and $f_{1,j}$ respectively, we define

$$\psi_{i,1} = \psi_{1,1} \quad \text{and} \quad f_{i,j} = f_{1,j}, \quad i = 2, \ldots, 4, \quad j = 1, 3, \ldots, 9.$$

Then, interchanging z with w in (4.3), we define

$$\begin{aligned}
\psi_{2,2} &= \rho(p^{34}(x, y, w, z)) \\
f_{2,2} &= \rho(p^{24}(x, y, w, z)) \\
f_{2,4} &= \rho(p^{23}(x, y, w, z)) \\
f_{2,6} &= \rho(p^{14}(x, y, w, z)) \\
f_{2,8} &= \rho(p^{13}(x, y, w, z)) \\
f_{2,10} &= \rho(p^{12}(x, y, w, z)).
\end{aligned}$$

Similarly, by interchanging x with y in (4.3), we define $\psi_{3,2}$ and $f_{3,j}$, $j = 2, 4, \ldots, 10$. Finally, by interchanging x with y, and z with w in (4.3), we define $\psi_{4,2}$ and $f_{4,j}$, $j = 2, 4, \ldots, 10$. Then we have four identities:

$$\psi_{i,1}\psi_{i,2} = f_{i,1}f_{i,2} + \cdots + f_{i,9}f_{i,10}, \quad 1 \leq i \leq 4. \tag{4.5}$$

Before introducing the central map of the new cryptosystem, we briefly comment on its intermediate field construction as outlined in Section 1.3. Since $\mathbb{F}$ is a degree d extension of k, we view each X_i, $1 \leq i \leq 24$, and Y_i, $1 \leq j \leq 32$, as a d-tuple. Thus the triangular portion of the central map will have the form described in (1.7) and (1.8).

Finally, using the four systems (4.5), we define the central map of the new cryptosystem,

$$(Z_1, \ldots, Z_{74}) = F(X_1, \ldots, X_{24}, Y_1, \ldots, Y_{32}),$$

by

$$
\begin{aligned}
Z_1 &= X_1 + \phi_1(X_1) + \psi_{1,1}(X_1, \ldots, X_8) \\
Z_2 &= X_2 + \phi_2(X_1, X_2) + \psi_{1,2}(Y_1, \ldots, Y_8) \\
Z_3 &= X_3 + \phi_3(X_1, \ldots, X_3) + \psi_{2,2}(Y_9, \ldots, Y_{16}) \\
Z_4 &= X_4 + \phi_4(X_1, \ldots, X_4) + \psi_{3,2}(Y_{17}, \ldots, Y_{24}) \\
Z_5 &= X_5 + \phi_5(X_1, \ldots, X_5) + \psi_{2,1}(X_9, \ldots, X_{16}) \\
Z_6 &= X_6 + \phi_6(X_1, \ldots, X_6) + \psi_{3,1}(X_{17}, \ldots, X_{24}) \\
Z_7 &= X_7 + \phi_7(X_1, \ldots, X_7) + \psi_{4,2}(Y_{25}, \ldots, Y_{32}) \\
Z_{7+i} &= f_{1,i}(X_1, \ldots, X_8, Y_1, \ldots, Y_8) && 1 \leq i \leq 10 \\
Z_{17+i} &= f_{2,i}(X_1, \ldots, X_8, Y_9, \ldots, Y_{16}) && 1 \leq i \leq 10 \\
Z_{27+i} &= f_{2,i}(Y_1, \ldots, Y_8, Y_9, \ldots, Y_{16}) && 1 \leq i \leq 8 \\
Z_{36} &= f_{2,10}(Y_1, \ldots, Y_8, Y_9, \ldots, Y_{16}) \\
Z_{36+i} &= f_{3,i}(X_1, \ldots, X_8, Y_{17}, \ldots, Y_{24}) && 1 \leq i \leq 10 \\
Z_{46+i} &= f_{2,i}(X_9, \ldots, X_{16}, Y_9, \ldots, Y_{16}) && 1 \leq i \leq 8 \\
Z_{55} &= f_{2,10}(X_9, \ldots, X_{16}, Y_9, \ldots, Y_{16}) \\
Z_{55+i} &= f_{3,i}(X_{17}, \ldots, X_{24}, Y_{17}, \ldots, Y_{24}) && 1 \leq i \leq 8 \\
Z_{64} &= f_{3,10}(X_{17}, \ldots, X_{24}, Y_{17}, \ldots, Y_{24}) \\
Z_{64+i} &= f_{4,i}(X_9, \ldots, X_{16}, Y_{25}, \ldots, Y_{32}) && 1 \leq i \leq 10
\end{aligned}
$$

Notice $f_{2,9}(Y_1, \ldots, Y_8, Y_9, \ldots, Y_{16})$ has been omitted from the central map to avoid redundancy as

$$f_{2,9}(Y_1, \ldots, Y_8, Y_9, \ldots, Y_{16}) = f_{2,9}(X_1, \ldots, X_8, Y_9, \ldots, Y_{16}) = Z_{26}. \tag{4.6}$$

Similarly, $f_{2,9}(X_9, \ldots, X_{16}, Y_9, \ldots, Y_{16}) = Z_{26}$ and $f_{3,9}(X_{17}, \ldots, X_{24}, Y_{17}, \ldots, Y_{24}) = Z_{45}$ are also omitted. Since the central map is from $\mathbb{F}^{56}$ to $\mathbb{F}^{74}$, the information rate of this cryptosystem is $\frac{56}{74} \approx .76$ (slightly smaller than the MFE information rate of .80).

4.2.1 Inverting the central map

Recall that decryption proceeds by unmasking the triangular system $(Z_1, \ldots, Z_7)$, and then solving the oil-vinegar systems. We start by focusing on the first three equations of the triangular system, as the first three ψ_i can be recovered by inverting a Cremona transformation as discussed in Section 1.3.4. Using the notation we introduced in Chapter 1 for the general framework, let

$$\begin{aligned} g_1 &= Z_8Z_9 + Z_{10}Z_{11} + Z_{12}Z_{13} + Z_{14}Z_{15} + Z_{16}Z_{17} \\ &= \psi_{1,1}(X_1, \ldots, X_8)\psi_{1,2}(Y_1, \ldots, Y_8), \\ g_2 &= Z_{18}Z_{19} + Z_{20}Z_{21} + Z_{22}Z_{23} + Z_{24}Z_{25} + Z_{26}Z_{27} \\ &= \psi_{2,1}(X_1, \ldots, X_8)\psi_{2,2}(Y_9, \ldots, Y_{16}), \\ g_3 &= Z_{28}Z_{29} + Z_{30}Z_{31} + Z_{32}Z_{33} + Z_{34}Z_{35} + Z_{26}Z_{36} \\ &= \psi_{2,1}(Y_1, \ldots, Y_8)\psi_{2,2}(Y_9, \ldots, Y_{16}). \end{aligned}$$

Note that Z_{26} appears in both g_2 and g_3 because of (4.6). Then, since

$$\psi_{2,1}(X_1, \ldots, X_8) = \psi_{1,1}(X_1, \ldots, X_8) \quad \text{and} \quad \psi_{2,1}(Y_1, \ldots, Y_8) = \psi_{1,2}(Y_1, \ldots, Y_8),$$

we have

$$\begin{aligned} h_1 &= (g_1g_2g_3^{-1})^{1/2} &&= \psi_{1,1}(X_1, \ldots, X_8) \\ h_2 &= g_1h_1^{-1} &&= \psi_{1,2}(Y_1, \ldots, Y_8) \\ h_3 &= g_2h_1^{-1} &&= \psi_{2,2}(Y_9, \ldots, Y_{16}). \end{aligned}$$

We can then substitute the transformed ciphertext values into h_1, h_2, h_3 and subsequently restore the triangular structure of Z_1, Z_2, Z_3, respectively. The next step is to unmask the

final four equations in the triangular portion. To do this, we define

$$\begin{aligned}
g_4 &= Z_{37}Z_{38} + Z_{39}Z_{40} + Z_{41}Z_{42} + Z_{43}Z_{44} + Z_{45}Z_{46} \\
&= \psi_{3,1}(X_1, \ldots, X_8)\psi_{3,2}(Y_{17}, \ldots, Y_{24}), \\
g_5 &= Z_{47}Z_{48} + Z_{49}Z_{50} + Z_{51}Z_{52} + Z_{53}Z_{54} + Z_{26}Z_{55} \\
&= \psi_{2,1}(X_9, \ldots, X_{16})\psi_{2,2}(Y_9, \ldots, Y_{16}), \\
g_6 &= Z_{56}Z_{57} + Z_{58}Z_{59} + Z_{60}Z_{61} + Z_{62}Z_{63} + Z_{45}Z_{64} \\
&= \psi_{3,1}(X_{17}, \ldots, X_{24})\psi_{3,2}(Y_{17}, \ldots, Y_{24}), \\
g_7 &= Z_{65}Z_{66} + Z_{67}Z_{68} + Z_{69}Z_{70} + Z_{71}Z_{72} + Z_{73}Z_{74} \\
&= \psi_{4,1}(X_9, \ldots, X_{16})\psi_{4,2}(Y_{25}, \ldots, Y_{32}).
\end{aligned}$$

Then, since $\psi_{3,1}(X_1, \ldots, X_8) = \psi_{1,1}(X_1, \ldots, X_8)$ and $\psi_{4,1}(X_9, \ldots, X_{16}) = \psi_{2,1}(X_9, \ldots, X_{16})$, we have

$$\begin{aligned}
h_4 &= g_4 h_1^{-1} &&= \psi_{3,2}(Y_{17}, \ldots, Y_{24}) \\
h_5 &= g_5 h_3^{-1} &&= \psi_{2,1}(X_9, \ldots, X_{16}) \\
h_6 &= g_6 h_4^{-1} &&= \psi_{3,1}(X_{17}, \ldots, X_{24}) \\
h_7 &= g_7 h_5^{-1} &&= \psi_{4,2}(Y_{25}, \ldots, Y_{32}).
\end{aligned}$$

Using $h_4, \ldots, h_7$, we can restore the triangular structure of $Y_4, \ldots, Y_7$, and easily recover $X_1, \ldots, X_7$. To recover X_8, we use the value of $h_1 = \psi_{1,1}(X_1, \ldots, X_8)$, as long as X_7 is nonzero.

We finish the inversion process by solving for the remaining variables $X_9, \ldots, X_{24}$

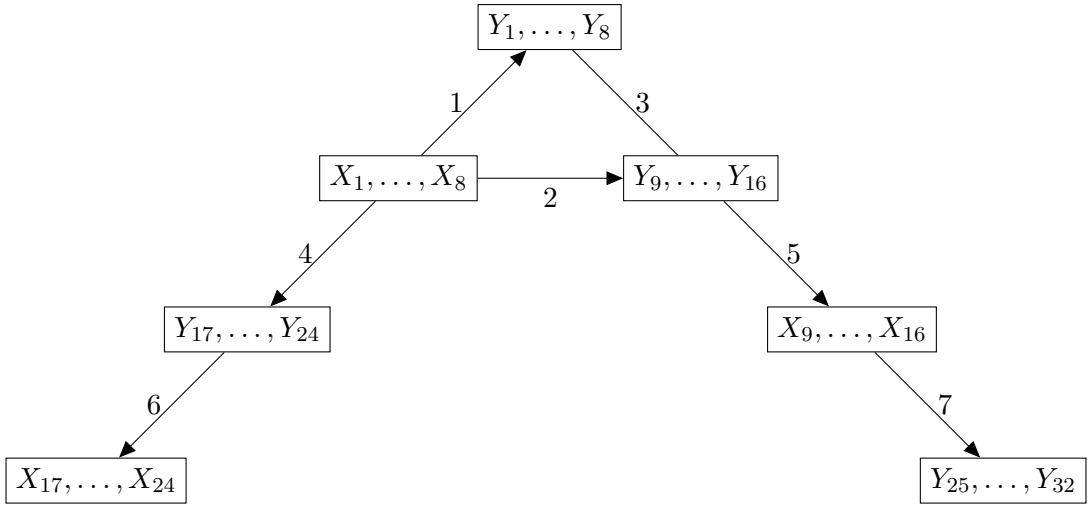
and $Y_1, \ldots, Y_{32}$, using 6 of the 7 oil-vinegar systems:

subsystem	oil-vinegar polynomials	oil variables	vinegar variables
1	$Z_8, \ldots, Z_{15}$	$Y_1, \ldots, Y_8$	$X_1, \ldots, X_8$
2	$Z_{18}, \ldots, Z_{25}$	$Y_9, \ldots, Y_{16}$	$X_1, \ldots, X_8$
4	$Z_{37}, \ldots, Z_{44}$	$Y_{17}, \ldots, Y_{24}$	$X_1, \ldots, X_8$
5	$Z_{47}, \ldots, Z_{54}$	$X_9, \ldots, X_{16}$	$Y_9, \ldots, Y_{16}$
6	$Z_{56}, \ldots, Z_{63}$	$X_{17}, \ldots, X_{24}$	$Y_{17}, \ldots, Y_{24}$
7	$Z_{65}, \ldots, Z_{72}$	$Y_{25}, \ldots, Y_{32}$	$X_9, \ldots, X_{16}$

(4.7)

Similar to Figure 1.3 in Chapter 1, Figure 4.1 illustrates the relationships between these oil-vinegar systems (the heads of the arrows indicate the oil variables for each system).

Figure 4.1: Chain of Oil-Vinegar Systems in the New Cryptosystem



4.2.2 Decryption failures

In this section, we let $N = |\mathbb{F}|$. From Section 1.3, we know that decryption may fail 1) if we are unable to perform a necessary inversion in $\mathbb{F}$ while computing the h_i's, or 2) if we are unable to solve an oil-vinegar subsystem. To compute h_1, h_2, h_3, notice that

we must have $\psi_{1,1}(X_1, \ldots, X_8)$, $\psi_{1,2}(Y_1, \ldots, Y_8)$, and $\psi_{2,2}(Y_9, \ldots, Y_{16})$ all nonzero. First consider when

$$\psi_{1,1}(X_1, \ldots, X_8) = X_1X_2 + X_3X_4 + X_5X_6 + X_7X_8 = 0.$$

If we let $M_1 = \begin{bmatrix} X_1 & X_3 \\ X_4 & X_2 \end{bmatrix}$, $M_2 = \begin{bmatrix} X_5 & X_7 \\ X_8 & X_6 \end{bmatrix} \in \mathbb{F}^{2\times 2}$, then

$$\begin{aligned}
P(\psi_{1,1}(X_1, \ldots, X_8) = 0) &= P(\det M_1 = \det M_2) \\
&= \sum_{\alpha\in\mathbb{F}} P(\det M_1 = \alpha \mid \det M_2 = \alpha)P(\det M_2 = \alpha) \\
&= \sum_{\alpha\in\mathbb{F}} (P(\det M_1 = \alpha))^2 \\
&= (P(\det M_1 = 0))^2 + \sum_{0\neq\alpha\in\mathbb{F}} (P(\det M_1 = \alpha))^2 \\
&= \left(\frac{N^3 + N^2 - N}{N^4}\right)^2 + (N-1)\left(\frac{N^3 - N}{N^4}\right)^2 \\
&= \frac{N^7 + N^4 - N^3}{N^8}.
\end{aligned}$$

When N is large, this probability is approximately $\frac{1}{N}$, and is the same for $\psi_{1,2}(Y_1, \ldots, Y_8)$ and $\psi_{2,2}(Y_9, \ldots, Y_{16})$.

Computing $h_4, \ldots, h_7$ requires only two additional conditions: $\psi_{3,2}(Y_{17}, \ldots, Y_{24}) \neq 0$ and $\psi_{2,1}(X_9, \ldots, X_{16}) \neq 0$. Again, each of these are zero with probabilty approximately $\frac{1}{N}$, so the total probability that we will not be able to unmask the triangular system is approximately $\frac{5}{N}$.

Recall that we can use h_1 to recover X_8 as long as X_7 is nonzero. However, if $X_7 = 0$, we can instead use Z_{17} as long as $X_2 \neq 0$. Hence we fail to recover X_8 with probability $\frac{1}{N^2}$.

We have already addressed in Section 4.1 the solvability of the oil-vinegar subsystems. Notice that in (4.7), we have 6 oil-vinegar systems, but only 4 distinct sets of vinegar variables. Hence the total probability of failing to invert the oil-vinegar systems is approximately $\frac{4}{N}$.

Therefore, we conclude that decryption failure occurs with total probability approximately $\frac{9}{N}$. Practical implementations may avoid this problem by choosing N large enough to ensure that decryption failure is negligible, or by using the embedding ($\nearrow$) modifier (see [DWY07, DYCCD07]).

4.3 Security and Efficiency

In the following, we show that our system is safe from known attacks on MPKCs. Throughout this section, q is the size of the base field, k, and d is the degree of $\mathbb{F}$ over k.

4.3.1 Attacks based on linear algebra.

We now consider the specific linear algebra-based attacks, examining the minrank and dual rank, separation of oil and vinegar variables, and finally, linearization equations attacks. These attacks have been perhaps the most devastating to attempts at building MPKCs.

Minrank attack. Recall from Section 2.2 that if a variable X_i does not appear in the quadratic part of a polynomial, then the associated matrix will not have full rank, since the i-th row and column are zero. So, loosely speaking, if an equation has too few variables, the associated matrix will have small rank. This is the foundation for the minrank attack. Since the public polynomials are just combinations of the central map polynomials (via L_1) after a change of variables (via L_2), if the matrix for a central map polynomial has low rank, r, then some combination of the public key polynomials also must have rank r. After such a combination is found, the system may be broken.

From [GC00], the complexity of the attack is $q^{\lceil \frac{m}{n} \rceil r}$, where m is the number of central map polynomials, n is the number of variables, and r is the smallest rank. Considering the ranks of the central map polynomials, viewed component-wise over k, the smallest rank is $8d$, hence the complexity of attack is $q^{\lceil \frac{74}{56} \rceil 8d} = q^{16d}$.

Dual rank attack. While minrank succeeds when an equation has too few vari-

ables, the dual rank attack is effective when a variable appears in too few equations. In this case, the matrix corresponding to the quadratic part of a polynomial in which the variable does not appear will have less than full rank. In particular, if a variable only appears in the quadratic part of u central map equations, then some combination of $(u+1)$ of the public polynomials must have less than full rank. Finding such a combination will again enable us to break the system. The complexity of this attack is at least $n^3 q^u$ [YC04].

In our case, viewing the central map polynomials component-wise over k, each of the $56d$ variables appears in at least $6d$ equations, so the complexity of the attack is $(56d)^3 q^{6d}$.

Separation of oil and vinegar variables attack. As mentioned in Section 2.3, the goal of this attack is to find the transformed oil space. Kipnis et al. [KPG99] give a complexity of $o^4 q^{v-o-1}$ where o and v are the number of oil and vinegar variables, respectively. Determining the transformed oil space may possibly lead to breaking the system, so we show that the complexity for our system is sufficiently high.

Recall that in an oil-vinegar system, no terms in the system may be quadratic in the oil variables. This means that given a system of polynomials, adding terms may result in a decrease of the size of the oil set, but never an increase, hence the vinegar set cannot possibly shrink by adding terms. So, disregarding the ϕ_i of the triangular system and viewing our central map F as a system of oil-vinegar polynomials with coefficients in $\mathbb{F}$, we can determine the size of the minimal vinegar set by computing the maximum size of an oil set. This can be done by finding the clique number of the graph with vertices given by the 56 variables and edges occuring whenever the product of two variables does *not* appear in any polynomials of F. Computation using Magma reveals that the clique number is 20, so the smallest vinegar set has 36 variables. This gives a complexity of $20^4 q^{15d}$.

Linearization equations attack. Computations using Magma verify that there are no first order linearization equations. Regarding second order linearization equations, we point out an important contrast between our new system and MFE. In MFE, each ψ_i has rank 4, and can therefore be expressed as the determinant of a 2×2 matrix. The f_i are defined as elements of the product of two of these matrices, and the identity (1.13) holds

by the multiplicative property of the determinant. Since the ψ_i in our system have rank 8, no simple matrix decomposition exists, as each ψ_i has an expression as the sum of two 2×2 determinants. Further, the f_i are not defined as elements of a matrix product, so the multiplicative property of the determinant is of no use.

However, the above argument obviously cannot completely rule out the possibility of second order linearization equations. A search for second order equations would involve solving a linear system in approximately $\binom{56d+1}{1}\binom{74d+2}{2}$ coefficients. So, for $d = 1$, naive Gaussian elimination would require $> 2^{51}$ field operations, and for $d = 2$, it would require $> 2^{60}$ field operations. The time and memory requirements for solving such a system (about 32 GB with Magma) have prevented us from performing the computation.

4.3.2 Algebraic attacks.

At the heart of these attacks are the F_4 and F_5 algorithms of Faugére [Fau99] and [Fau02], as well as the XL algorithm of Courtois et al. [CKPS00]. There have been some recent contributions to complexity estimates for these algorithms, assuming general systems.

Barget et al. [BFSY05] give the total number of operations in k for F_5 (and hence XL) as

$$O\left(\binom{n + d_{reg}}{n}^{\omega}\right),$$

where ω is the exponent in Gaussian reduction and d_{reg} is the degree of regularity of the ideal formed by the polynomials in the system, given by the degree of the first term with negative coefficient in the expansion of

$$\frac{\prod_{i=1}^{m}(1 - z^{d_i})}{(1 - z)^n}, \tag{4.8}$$

where d_i is the total degree of the i-th polynomial. But since each of our polynomials have total degree two, (4.8) simplifies to $(1 - z)^{m-n}(1 + z)^m$. For us, if we take the degree of $\mathbb{F}$ over k to be 1 (so $m = 74$ and $n = 56$), we have $d_{reg} = 15$. Hence the attack requires $2^{\omega \log \binom{71}{56}} > 2^{49\omega}$ operations in k. If we instead take the degree of $\mathbb{F}$ over k to be 2, d_{reg}

becomes 26, and the attack requires $> 2^{92\omega}$ operations.

One other attack of note in this category is the attack of Joux et al. [JJMR05] against an earlier tractable rational map cryptosystem of Wang and Chen [WC04]. The authors exploit the fact that within the central map, there is a smaller subsystem of 11 equations in 7 variables. However, because of the design of our system, there appears to be no such overdetermined subsystem.

4.3.3 Parameters

Based on the preceding discussion, Table 4.1 presents security levels for different choices of $q = |k|$ and $d = [\mathbb{F} : k]$, where the column F_5 gives the complexity of the algebraic system solving attack, and the column Rank/UOV gives the complexity of the linear algebra attacks. To compute the complexity of Faugére's F_5 algorithm, we have used $\omega = 2.3$.

Table 4.1: Security

Claimed	Input	Output	Parameters		Complexity		Key Size [kBytes]	
Security	[bits]	[bits]	q	d	F_5	Rank/UOV	Public	Private
2^{113}	896	1184	2^{16}	1	2^{114}	2^{113}	245	18
2^{212}	1792	2368	2^{16}	2	2^{213}	2^{212}	1907	70
2^{114}	1792	2368	2^{32}	1	2^{114}	2^{209}	490	36

Note that the complexity for F_5 is the same for the first and third systems even though input size is different. This is because the complexity estimate for F_5 depends only on the number of equations and the number of variables. However, while the second system has the same input size as the third, security is much higher because of the use of an intermediate field (i.e. $d > 1$).

4.3.4 Efficiency

Consider our proposed system with $q = 2^{16}$ and $d = 1$. We compare it to MFE-1, which was shown to have a significant advantage over RSA-1024 in decryption speed [WYHL06]. Since MFE-1 uses a degree 4 extension of $\mathbb{F}_{2^{16}}$, multiplications in the extension

field require 4^2 operations over the base field. A rough count of multiplications over $\mathbb{F}_{2^{16}}$ yields about 2400 for MFE-1 and 3200 for our system. We implemented both systems in a straightforward way using Magma on a 1600MHz UltraSPARC IIIi. The results are recorded in Table 4.2.

Table 4.2: Implementation Results

System	Input [bits]	Output [bits]	Encryption Time	Decryption Time	
				Central Map	Total
MFE-1	768	960	52ms	2ms	2.7ms
Our System	896	1184	94ms	1.4ms	2.3ms

As expected, encryption in our system is slower since it uses 74 equations in 56 variables over $\mathbb{F}_{2^{16}}$, whereas MFE-1 uses 60 equations in 48 variables. However, even though the multiplication count for our system is larger, decryption is actually faster. This is because the division and square root operations are slower in the large extension field of MFE-1; furthermore, decrypting MFE-1 requires converting back and forth between the base field and the extension field.

4.4 Future Directions

We have introduced a new framework for constructing multivariate public key cryptosystems that combines the ideas of triangular and oil-vinegar systems. Also, we have proposed a new cryptosystem that implements the framework, and we have shown the system to be secure against known MPKC attacks. The framework has much freedom and should provide a fertile ground for new research in the area of multivariate public key cryptography. In particular, we pose the following open questions:

- How can we find all quadratic solutions to the general Diophantine equations (1.13) and (1.14)?

  For the first equation, $AB = CD + EF$, we have completely characterized all solutions subject to the requirements laid out at the beginning of Chapter 3. However, it is

an open question to characterize all solutions in general. For the second equation, $AB = CD + EF + GH + IJ + KL$, we have found several solutions, and we can use the Basis Theorem (Theorem 3.5.2) to construct many more solutions. However, there is much work to be done to study this form.

- One solution to (1.14) gives several possible cryptosystems, depending on how we choose to arrange the oil-vinegar systems. How can we effectively choose the best one?

  The system proposed in Chapter 4 uses the configuration illustrated by Figure 4.1, but this is not the only possible arrangement. Starting from the triangle formed by the first three oil-vinegar systems, the remaining four systems may be arranged in many ways.

- What strategies can be formulated to help minimize the decryption failure rate?

  We mentioned the obvious solution of choosing $\mathbb{F}$ large enough so as to make decryption failure negligible. However, in applications where decryption failure is strictly prohibited, the embedding modifier of [DWY07] should be implemented. An explicit implementation is left for future work. Also, Section 4.2.2 showed decryption failure is in part tied to the arrangement of the oil-vinegar systems, so progress regarding the previous question may in be useful in minimizing decryption failure.

- What other polynomial identities may be used to construct cryptosystems in the proposed framework?

  Identities of the form (1.13) and (1.14) have been used to construct the MFE cryptosytem, and our new cryptosystem, respectively. However, more general identities of the form (3.1):

$$AB = f_1 f_2 + f_3 f_4 + \ldots f_{n-1} f_n + f_{n+1} f_{n+2} + \cdots + f_{n+t-1} f_{n+t}$$

  should be explored.

- Rather than having g_i in (1.9) factor into two distinct quadratics, can we find $g_i = \sum \alpha_{jk} Y_j Y_k = \psi_i$, or $g_i = \psi_i^2$? This would make h_i much simpler: $h_i = g_i$ and $h_i = g_i^{1/2}$, respectively, and the first type of decryption failure would become irrelevant.

- A further generalization of the framework would be to omit the g_i's and simply require the existence of rational functions $h_i \in \mathbb{F}(Y_{n+1}, \ldots, Y_{n+\ell t})$ such that each $h_i(f_{n+1}, \ldots, f_{n+\ell t})$ is quadratic in $X_1, \ldots, X_{n+\ell o}$, and could be used as a lock polynomial. Can other systems be successfully created using this generalization?

Bibliography

[ACDG03] Mehdi-Laurent Akkar, Nicolas Courtois, Romain Duteuil, and Louis Goubin, "A fast and secure implementation of Sflash," Public Key Cryptography - PKC 2003: 6th International Workshop on Practice and Theory in Public Key Cryptography. LNCS 2567, 267-278. Springer (2003)

[BCD08] John Baena, Crystal Clough, and Jintai Ding, "Square-Vinegar Signature Scheme," Post-Quantum Cryptography - PQCrypto 2008: Second International Workshop. LNCS 5299, 17-30 (2008)

[BFSY05] Magali Barget, Jean-Charles Faugére, Bruno Salvy, and Bo-Yin Yang, "Asymptotic Expansion of the Degree of Regularity for Semi-Regular Systems of Equations," Proceedings of MEGA'05: 8th International Symposium on Effective Methods in Algebraic Geometry (2005)

[Buc65] Bruno Buchberger, "Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalem Polynomideal (An algorithm for finding the basis elements in the residue class ring modulo a zero dimensional polynomial ideal)," Ph.D. thesis, Mathematical Institute, University of Innsbruck, Austria. English translation published in the Journal of Symbolic Computation 41 (2006)

[BWP05] An Braeken, Christopher Wolf, and Bart Preneel, "A Study of the Security of Unbalanced Oil and Vinegar Schemes," Topics in Cryptology - CT-RSA 2005: The Cryptographers' Track at RSA Conference 2005. LNCS 3376, 29-43. Springer (2005)

[CCDWY08] Chia-Hsin Owen Chen, Ming-Shing Chen, Jintai Ding, Fabian Werner, and Bo-Yin Yang, "Odd-Char Multivariate Hidden Field Equations," Cryptology ePrint Archive, Report 2008/543. http://eprint.iacr.org (2008)

[CKPS00] Nicolas Courtois, Alexander Kilmov, Jacques Patarin, and Adi Shamir, "Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations," Advances in Cryptology - EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques. LNCS 1807, 392-407 (2000)

[CLO96] David Cox, John Little, and Donal O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. 2nd ed. Springer (1996)

[Cou01] Nicolas Courtois, "The Security of Hidden Field Equations (HFE)," Topics in Cryptology - CT-RSA 2001: The Cryptographers' Track at RSA Conference 2001. LNCS 2020, 266-281. Springer (2001)

[CSV93] Don Coppersmith, Jacques Stern and Serge Vaudenay, "Attacks on the Birational Permutation Signature Schemes," Advances in Cryptology - CRYPTO'93: 13th Annual International Cryptology Conference. LNCS 773, 435-443. Springer (1994)

[CSV97] Don Coppersmith, Jacques Stern and Serge Vaudenay, "The Security of the Birational Permutation Signature Schemes," *Journal of Cryptology*. 10 no. 3, 207-221 (1997)

[DFS07] Vivien Dubois, Pierre-Alain Fouque, and Jacques Stern, "Cryptanalysis of Sflash with Slightly Modified Parameters," Advances in Cryptology - EUROCRYPT 2007: 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques. LNCS 4515, 264-275. Springer (2007)

[DFSS07] Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, and Jacques Stern, "Practical Cryptanalysis of Sflash," Advances in Cryptology - CRYPTO 2007: 27th International Cryptology Conference. LNCS 4622, 1-12. Springer (2007)

[DGS06a] Jintai Ding, Jason Gower, and Deiter Schmidt, *Multivariate Public Key Cryptosystems*. Springer (2006)

[DGS06b] Jintai Ding, Jason Gower, and Deiter Schmidt, "Zhuang-Zi: A new algorithm for solving multivariate polynomial equations over a finite field," Cryptology ePrint Archive, Report 2006/038. http://eprint.iacr.org (2006)

[DH76] Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, IT-22 (1976) no. 6 pp. 644-654.

[DHNW07] Jintai Ding, Lei Hu, Xuyun Nie, Jianyu Li and John Wagner, "High Order Linearization Equation (HOLE) Attack on Multivariate Public Key Cryptosystems," Public Key Cryptography - PKC 2007: 10th International Conference on Practice and Theory in Public-Key Cryptography. LNCS 4450, 233-248. Springer (2007)

[DS03] Jintai Ding and Dieter Schmidt, "The new TTM implementation is not secure," *Proceedings of International Workshop on Coding, Cryptography, and Combinatorics (CCC 2003)*. 106-121 (2003)

[DS05] Jintai Ding and Dieter Schmidt, "Rainbow, a New Multivariate Polynomial Signature Scheme," Applied Cryptography and Network Security: Third International Conference (ANCS 2005). LNCS 3531, 164-175. Springer (2005)

[DS06] Jintai Ding and Dieter Schmidt, "Multivariable Public Key Cryptosystems," Algebra and its applications: papers from the international conference held at Ohio University, Athens, OH, March 2226, 2005. Contemporary Mathematics 419, 79-94. AMS (2006)

[DSY06] Jintai Ding, Deiter Schmidt, and Zhijun Yin, "Cryptanalysis of the new TTS scheme in CHES 2004," *International Journal of Information Security*, 5 (2006) no. 4 pp. 231-240.

[DW01] Douglas West, *Introduction to Graph Theory*. 2nd ed. 4. Prentice Hall (2001)

[DWY07] Jintai Ding, Christopher Wolf, and Bo-Yin Yang, "ℓ-Invertible Cycles for Multivariate Quadratic Public Key Cryptography," Public Key Cryptography - PKC 2007: 10th International Conference on Practice and Theory in Public-Key Cryptography, LNCS 4450, 266-281, Springer (2007)

[DYCCD07] Jintai Ding, Bo-Yin Yang, Chen-Mou Cheng, Owen Chen, and Vivien Dubois, "Breaking the symmetry: a way to resist the new differential attack," Cryptology ePrint Archive, Report 2007/366. http://eprint.iacr.org (2007)

[Fau99] Jean-Charles Faugére, "A new efficient algorithm for computing Gröbner bases (F_4)," *Journal of Pure and Applied Algebra*. 139, 61-68 (1999)

[Fau02] Jean-Charles Faugére, "A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5)," ISSAC '02: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation. 75-83. ACM (2002)

[FD85] Harriet Fell and Whitfield Diffie, "Analysis of a Public Key Approach Based on Polynomial Substitution," Advances in Cryptology - CRYPTO '85: A Conference on the Theory and Application of Cryptographic Techniques. LNCS 218, 340-349. Springer (1885)

[FJ03] Jean-Charles Faugére and Antoine Joux, "Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases, Advances in Cryptology - CRYPTO 2003: 23rd Annual International Cryptology Conference. LNCS 2729, 44-60. Springer (2003)

[GC00] Louis Goubin and Nicolas Courtois, "Cryptanalysis of the TTM Cryptosystem," Advances in Cryptology - ASIACRYPT 2000: 6th International Conference on the Theory and Application of Cryptology and Information Security. LNCS 1976, 44-57. Springer (2000)

[GH78] Phillip Griffiths and Joseph Harris, *Principles of Algebraic Geometry*, pp. 496-498. Wiley & Sons (1978)

[GH08] Shuhong Gao and Raymond Heindl, "Multivariate Public Key Cryptosystems from Diophantine Equations," in review.

[GJ79] Michael Garey and David Johnson, *Computers and intractability: a guide to the theory of NP-completeness*, p. 251. Freeman (1979)

[HMSV09] Benjamin Howard, John Millson, Andrew Snowden, and Ravi Vakil, "The equations for the moduli space of n points on the line," *Duke Mathematical Journal* 146 (2), 175-226 (2009)

[HP47] William Hodge and Daniel Pedoe, *Methods of Algebraic Geometry*. Vol 1. Cambridge (1947)

[IM85] Hideki Imai and Tsutomu Matsumoto, "Algebraic methods for constructing asymmetric cryptosystems," Algebraic Algorithms and Error-Correcting Codes: 3rd International Conference (AAECC-3). LNCS 229, 108-229. Springer (1985)

[JJMR05] Antoine Joux, Sébastien Kunz-Jacques, Frédéric Muller, and Pierre-Michel Ricordel, "Cryptanalysis of the Tractable Rational Map Cryptosystem," Public Key Cryptography - PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography. LNCS 3386, 258-274. Springer (2005)

[Kli72] Morris Kline, *Mathematical Thought from Ancient to Modern Times*, pp. 932-944. Oxford (1972)

[KS98] Aviad Kipnis and Adi Shamir, "Cryptanalysis of the oil and vinegar signature scheme," Advances in Cryptology - CRYPTO '98: 18th Annual International Cryptology Conference. LNCS 1462, 257-266. Springer (1998)

[KS99] Aviad Kipnis and Adi Shamir, "Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization," Advances in Cryptology - CRYPTO '99: 19th Annual International Cryptography Conference. LNCS 1666, 19-30. Springer (1999)

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin, "Unbalanced oil and vinegar signature schemes," Advances in Cryptology - EUROCRYPT '99: International Conference on the Theory and Application of Cryptographic Techniques. LNCS 1592, 206-222. Springer (1999) (extended version available at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.45.9346)

[MAGMA] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.* 24 (3-4), 235-265 (1997)

[Moh99] Tzuong Tsieng Moh, "A public key system with signature and master key functions," *Communications in Algebra*. 27 no. 5, pp.2207-2222 (1999)

[Moh07] Tzuong Tsieng Moh, "Two New Examples of TTM," Cryptology ePrint Archive, Report 2007/144. http://eprint.iacr.org (2007)

[MCY04] Tzuong Tsieng Moh, Jiun-Ming Chen, and Bo-Yin Yang, "Building Instances of TTM Immune to the Goubin-Courtois Attack and the Ding-Schmidt Attack," Cryptology ePrint Archive, Report 2004/168. http://eprint.iacr.org (2004)

[MI88] Tsutomu Matsumoto and Hideki Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption," Advances in Cryptology - EUROCRYPT '88: Workshop on the Theory and Application of Cryptographic Techniques. LNCS 330, 419-453 (1988)

[MS83] Neil Sloane and Florence MacWilliams, "Weight distribution of second-order Reed-Muller codes," *The Theory of Error-Correcting Codes*, 434-444. North Holland (1983)

[Nag72] Masayoshi Nagata, "On Automorphism Group of $K[x, y]$," volume 5 of *Lectures on Mathematics*, Kyoto University, Kinokuniya, Tokyo.

[NES03] NESSIE: New European Schemes for Signatures, Integrity, and Encryption, "NESSIE project announces final selection of crypto algorithms," Information Society Technologies Programme of the European Commission (IST-1999-12324). https://www.cosic.esat.kuleuven.be/nessie/ (2003)

[NJHD07] Xuyun Nie, Xin Jiang, Lei Hu, and Jintai Ding, "Cryptanalysis of Two New Instances of TTM Cryptosystem," Cryptology ePrint Archive, Report 2007/381. http://eprint.iacr.org (2007)

[Pat95] Jacques Patarin, "Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt '88," Advances in Cryptology - CRYPTO '95: 15th Annual International Cryptology Conference. LNCS 963, 248-261. Springer (1995)

[Pat96] Jacques Patarin, "Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms," Advances in Cryptology - EUROCRYPT '96: International Conference on the Theory and Application of Cryptographic Techniques. LNCS 1070, 33-48 (1996) (extended version available at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.33.1805)

[Pat97] Jacques Patarin, "The oil and vinegar signature scheme," Presented at the Dagstuhl Workshop on Cryptography (1997)

[PCG01] Jacques Patarin, Nicolas Courtois, and Louis Goubin, "Flash, a fast multivariate signature algorithm," Topics in Cryptology - CT-RSA 2001: The Cryptographers' Track at the RSA Conference 2001. LNCS 2020, 298-307. Springer (2001)

[PG97] Jacques Patarin and Louis Goubin, "Trapdoor one-way permutations and multivariate polynomials," Information and Communications Security - ICIS '97: First International Conference. LNCS 1334, 356-368. Springer (1997) (extended version available at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.41.9400)

[PGC98] Jacques Patarin, Louis Goubin, and Nicolas Courtois, "Improved Algorithms for Isomorphisms of Polynomials," Advances in Cryptology - EUROCRYPT '98: International Conference on the Theory and Application of Cryptographic Techniques. LNCS 1403, 184-200. Springer (1998) (extended version available at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.23.5317)

[Riv90] Ronald L. Rivest, "Cryptography," *Handbook of Theoretical Computer Science*, Ed. J. van Leeuwen, Elsevier, 1990, pp.717-755.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, 21 (1978), pp. 120-126.

[Sha93] Adi Shamir, "Efficient Signature Schemes Based on Birational Permutations," Advances in Cryptology - CRYPTO'93: 13th Annual International Cryptology Conference. LNCS 773, 1-12. Springer (1993)

[Sho97] Peter Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*. 26 no. 5, 1484-1509 (1997)

[TIFKM88] Shigeo Tsujii, Toshiya Itoh, Atsushi Fujioka, Kaoru Kurosawa, Tsutomu Matsumoto, "A public-key cryptosystem based on the difficulty of solving a system of nonlinear equations." Systems and Computers in Japan 19, 1018 (1988)

[VG03] Joachim von zur Gathen, Jürgen Gerhard, *Modern Computer Algebra*. 2nd ed. Cambridge (2003)

[WC04] Lih-Chung Wang and Fei-Hwang Chang, "Tractable Rational Map Cryptosystem," Cryptology ePrint Archive, Report 2004/046. http://eprint.iacr.org (2004)

[WC06] Lih-Chung Wang and Fei-Hwang Chang, "Revision of Tractable Rational Map Cryptosystem," Cryptology ePrint Archive, Report 2004/046. http://eprint.iacr.org (2006)

[Wol05] Christopher Wolf, "Multivariate Quadratic Polynomials in Public Key Cryptography," Ph.D. thesis, Katholieke Universiteit Leuven, Belgium (2005)

[WP05a] Christopher Wolf and Bart Preneel, "Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations," Cryptology ePrint Archive, Report 2005/077. http://eprint.iacr.org (2005)

[WP05b] Christopher Wolf and Bart Preneel, "Large Superfluous Keys in Multivariate Quadratic Asymmetric Systems," Public Key Cryptography - PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography. LNCS 3386, 275-287. Springer (2005)

[WYHL06] Lih-Chung Wang, Bo-Yin Yang, Yuh-Hua Hu and Feipei Lai, "A Medium-Field Multivariate Public-Key Encryption Scheme," Topics in Cryptology - CT-RSA 2006: The Cryptographers' Track at the RSA Conference 2006. LNCS 3860, 132-149. Springer (2006)

[YC04] Bo-Yin Yang and Jiun-Ming Chen, "TTS: Rank Attacks in Tame-Like Multivariate PKCs," Cryptology ePrint Archive, Report 2004/061. http://eprint.iacr.org (2004)

[YC05] Bo-Yin Yang and Jiun-Ming Chen, "Building Secure Tame-like Multivariate Public-Key Cryptosystems: The New TTS," Information Security and Privacy: 10th Australasian Conference (ACISP 2005). LNCS 3574, 518-531. Springer (2005)