Markus Kröll BSc

Analysis of a Key Agreement Protocol Based on Higher Order Diophantine Equations

MASTER THESIS

written to obtain the academic degree of a

Master of Science (MSc)

Master's programme Mathematical Computer Science

submitted to the university

Graz University of Technology

Supervisor:
O.Univ.-Prof. Dr.phil. Robert Tichy

Department of Analysis
and Computational Number Theory

Graz, September 2014

EIDESSTATTLICHE ERKLÄRUNG

AFFIDAVIT

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Das in TUGRAZonline hochgeladene Textdokument ist mit der vorliegenden Masterarbeit identisch.

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present master's thesis.

Datum/Date

Unterschrift/Signature

This document is set in Palatino, compiled with pdfLaTeX2e and Biber.

The LaTeX template from Karl Voit is based on KOMA script and can be found online: https://github.com/novoid/LaTeX-KOMA-template

Abstract

In 2011, Harry Yosh [42] proposed a new cryptographic key-exchange protocol based on Diophantine equations. Other than previously presented security protocols using Diophantine equations, Yosh imposed very little restrictions on the used parameters. This thesis aims to analyze Yosh's protocol as well as to restrict the set of public and private keys in order to maintain security and enable an efficient implementation of the key exchange. After presenting a modern version of the proof of Hilbert's tenth problem, which points out the hardness of solving Diophantine equations, a brief review of existing cryptographic schemes based on Diophantine equations is given. We then begin the study on Yosh's protocol in its general form over a unitary ring and establish minimal requirements for security. In order to use the protocol over a finite field $\mathbb{F}_q$, we use results from algebraic geometry to show explicit estimates on the number of q-rational points of an $\mathbb{F}_q$-definable hypersurface. To use the protocol over the integers, we introduce a broad class of integral Diophantine equations, which can be constructed from a given solution. We end with an example of the protocol over the integers and show that the public key has to be chosen very large for the protocol to be secure.

Kurzfassung

Harry Yosh führte 2011 ein neues kryptographisches Schlüsselaustauschprotokoll [42] ein, welches auf Diophantischen Gleichungen aufbaut. Im Gegensatz zu anderen bekannten Protokollen, welche auf Diophantischen Gleichungen basieren, gab Yosh wenig Einschränkungen für die Parameter, die im Ablauf seines Protokolls benötigt werden. Das Ziel dieser Arbeit ist sowohl Yosh's Protokoll zu analysieren, als auch die Menge von privaten und öffentlichen Schlüsseln so weit zu reduzieren, um Sicherheit und eine effektive Implementation des Schlüsselaustauschs zu ermöglichen. Nach der Präsentation einer modernen Version des Beweises von Hilbert's zehntem Problem, welches die Schwierigkeit des Lösens von Diophantischen Gleichungen darstellt, wird ein Überblick über bereits exisitierende kryptographische Protokolle basierend auf Diophantischen Gleichungen gegeben. Danach beginnen wir die Analyse der allgemeinen Version von Yosh's Protokoll über einem unitären Ring, und führen minimale Anforderungen zur Sicherheit ein. Um das Protokoll über einem endlichen Körper $\mathbb{F}_q$ durchzuführen, beweisen wir explizite Abschätzungen über die Anzahl von q-rationalen Punkten einer $\mathbb{F}_q$-definierbaren Hyperfläche. Dafür benötigen wir Resultate der Algebraischen Geometrie. Um das Protokoll über den ganzen Zahlen durchzuführen, führen wir eine Klasse von ganzzahligen Diophantischen Gleichungen ein, welche aus einer vordefinierten Lösung konstruiert werden können. Abschließend geben wir ein Beispiel des Protokolls über den ganzen Zahlen und zeigen, dass der öffentliche Schlüssel sehr groß gewählt werden muss, um die Sicherheit des Protokolls zu gewähren.

Contents

1 Introduction

In 1994, Peter Shor developed a quantum algorithm, called Shor's algorithm [39], solving both factorization as well as the discrete logarithm problem with the use of quantum computers. Since then, the continual progress in the area of quantum computing poses a threat to the security of widely used cryptographic techniques such as the RSA cryptosystem or the Diffie-Hellman key exchange method.

Public key cryptosystems are usually built on mathematical problems which are believed to be hard to solve. This way there are operations within these cryptosystems which can be computed very efficiently with publicly available knowledge, whereas other operations are feasible only for participants holding secret information. With the exception of certain families of Diophantine equations, higher order Diophantine equations are believed to be hard to solve. In addition to that, the following problem is even undecidable: Given any Diophantine equation, is there a universal algorithm deciding whether this equation is solvable. This is known as Hilbert's tenth problem, and it was proved by Matijasevič in 1970, that no such algorithm exists [9].

Public Key cryptosystems that are based on Diophantine equations may offer an alternative to those which are based on factorization or the discrete logarithm problem. As we will see, there are already many such cryptosystems. In 2011, Harry Yosh proposed the use of multidimensional Diophantine equations over the integers for the agreement on a key, see [42]. A key agreement protocol is a cryptographic protocol, where two or more participants establish a fresh key, and each of the participants influences the outcome. As with any other security protocol, no third party should be able to recreate the established key based on the exchanged messages.

In the following, an analysis of the key agreement protocol by Harry Yosh will be given. The security of the protocol is not only based on the Diophantine equation it uses, but also on the size of families of parameters used by its participants. As a small change in the underlying parameters may cause a huge increase in the data that needs to be transmitted or an increase in the number of computations, the efficiency of the protocol is analyzed as well.

In the first chapter, a modern proof of the negative solution to Hilbert's tenth problem is given. The impossibility of constructing an algorithm that decides the solvability of any general Diophantine equation does not mean that there is no efficient way of finding all solutions for a given family of Diophantine equations. However, the key agreement protocol presented in the following works with any non-linear Diophantine equation in at least 3 unknowns, in contrast to other cryptographic protocols based on Diophantine equations, which only use a very special family of equations.

In [18], Noriko Hirata-Kohno and Attila Pethő extend the brief observations made by Yosh concerning the security of the protocol as well as the usage of finite fields. Their results will serve as a foundation for this thesis. Amongst other things they proposed the use of a certain family of Diophantine equations over the finite fields. In Chapter 3, we establish that these equations are hard to solve by proving different estimates on the number of solutions of absolutely irreducible affine varieties over finite fields.

1.1 Notions and Notations

Let K be a field and let

$$f = \sum_{i \in I} a_i X_1^{\lambda_{i,1}} \cdots X_n^{\lambda_{i,n}} \in K[X_1, \dots, X_n]$$

be a multivariate polynomial for a finite index set I. We say that f is absolutely irreducible if it is irreducible on the algebraic closure $\bar{K}$. We will denote by $\deg f$ the total degree of f, i.e.

$$\deg f = \mathsf{max}\{\lambda_{i,1} + \cdots + \lambda_{i,n} \mid i \in I\}.$$

Moreover, if we write $\deg_{X_j} f$ for some $j \in \{1, \dots, n\}$, we mean the degree of f as a polynomial over $K[X_1, \dots, X_{j-1}, X_{j+1}, \dots, X_n]$.
We say that f is homogeneous, if

$$\lambda_{i,1} + \cdots + \lambda_{i,n} = \lambda_{j,1} + \cdots + \lambda_{j,n} \text{ for all } i, j \in I.$$

Otherwise we will say that f is inhomogeneous.
A Diophantine equation is an equation of the form

$$f = 0,$$

where $f \in \mathbb{Z}[X_1, \dots, X_n]$ for $n \geq 2$. We say that a Diophantine equation is linear, if $\deg f = 1$. Linear Diophantine equations are easy to solve, as shown in section 5.4.2. If $f = 0$ is a Diophantine equations with $\deg f > 1$, we call it a higher order Diophantine equation.
A finite field with q elements is always denoted by $\mathbb{F}_q$, where q is some prime power.

2 Hilbert's Tenth Problem

In 1900 David Hilbert published a list of 23 unsolved mathematical problems. The tenth problem on his list was the following:

> Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

It was proved by Yuri Matiyasevich in 1970 [9] that there is no algorithm which takes any polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$ and decides whether the Diophantine equation $f = 0$ has solutions or not in finitely many steps. In the following, we will present a proof given by Yuri Manin [25] of the negative answer to Hilbert's Tenth problem which is based on so called D-sets.

First the notion of Diophantine sets is introduced. With the use of D-sets, we can show that the class of Diophantine sets equals the class of recursively enumerable sets, which will lead to the desired result.

2.1 Principal Definitions

2.1.1 Diophantine Sets

Definition. *A set $\mathcal{M} \subseteq \mathbb{N}_0^n$, $n \in \mathbb{N}_0$, is called a Diophantine set, if there is some polynomial $D \in \mathbb{Z}[Y_1, \ldots, Y_n, X_1, \ldots, X_m]$ such that*

$$(a_1, \ldots, a_n) \in \mathcal{M} \Leftrightarrow (\exists x_1, \ldots, x_m \in \mathbb{N}_0)(D(a_1, \ldots a_n, x_1, \ldots, x_m) = 0]$$

holds.

For a Diophantine set $\mathcal{M}$ as given in the definition above, we will call

$$D(a_1, \ldots a_n, x_1, \ldots, x_m) = 0$$

its Diophantine representation.
Relations of the form $D(a_1, \ldots a_n, x_1, \ldots, x_m) = 0$ describe in fact families of Diophantine equations. The variables $a_1, \ldots, a_n$ are parameters and the $x_1, \ldots, x_m$ are unknowns. Fixing a certain tuple of parameters results in a single Diophantine equation.
In order to examine if certain sets are Diophantine or not, we first have to see what happens to Diophantine under basic set operations.

Proposition 2.1.1. *Let $\mathcal{M}_1, \mathcal{M}_2 \subseteq \mathbb{N}_0^n$ be Diophantine sets with Diophantine representations D_1 respectively D_2. Then $\mathcal{M}_1 \cup \mathcal{M}_2$ and $\mathcal{M}_1 \cap \mathcal{M}_2$ are also Diophantine.*

Proof. Let $(a_1, \dots, a_n) \in \mathbb{N}_0^n$. The integers are an integral domain, so

$$\begin{aligned}
&(\exists x_1, \dots, x_m, y_1, \dots, y_l \in \mathbb{N}_0) \\
&[(D_1(a_1, \dots, a_n, x_1, \dots, x_m) = 0) \vee (D_2(a_1, \dots, a_n, y_1, \dots, y_l) = 0)] \\
&\Leftrightarrow \\
&(\exists x_1, \dots, x_m, y_1, \dots, y_l \in \mathbb{N}_0)[D_1(a_1, \dots, a_n, x_1, \dots, x_m) D_2(a_1, \dots, a_n, y_1, \dots, y_l) = 0].
\end{aligned}$$

This means that the union is Diophantine with the representation $D_1 D_2$. Similarly the intersection of $\mathcal{M}_1$ and $\mathcal{M}_2$ is Diophantine, defined by the representation

$$(D_1(a_1, \dots, a_n, x_1, \dots, x_m))^2 + (D_2(a_1, \dots, a_n, y_1, \dots, y_l))^2 = 0.$$

□

Proposition 2.1.2. *Let $\mathcal{M}_1 \subseteq \mathbb{N}_0^n, \mathcal{M}_2 \subseteq \mathbb{N}_0^m$ be Diophantine sets with Diophantine representations D_1 respectively D_2. Then $\mathcal{M}_1 \times \mathcal{M}_2$ and the projection of $\mathcal{M}_1$ to its first k coordinates, $k \leq n$ are Diophantine.*

Proof. For the direct product, we have

$$\begin{aligned}
&(x_1, \dots, x_n, y_1, \dots, y_m) \in \mathcal{M}_1 \times \mathcal{M}2 \\
&\Leftrightarrow (\exists u_1, \dots, u_r, v_1, \dots, v_s)[(D_1(x_1, \dots, x_n, u_1, \dots, u_r))^2 + (D_2(y_1, \dots, y_m, v_1, \dots, v_s))^2 = 0],
\end{aligned}$$

thus the direct product is Diophantine. Next assume that $\mathcal{M}_1'$ is the projection of $\mathcal{M}_1$ to its first k coordinates for some fixed $k \leq n$. Then for all $(x_1, \dots, x_k) \in \mathbb{N}_0^k$ we have

$$(x_1, \dots, x_k) \in \mathcal{M}_1' \Leftrightarrow (\exists y_1, \dots, y_r, x_{k+1}, \dots, x_n)[D(x_1, \dots, x_k, x_{k+1}, \dots, x_n, y_1, \dots y_r) = 0],$$

thus the projection is Diophantine as well. □

A relation on k non-negative integers is a subset of $\mathbb{N}_0^k$. If a relation is a Diophantine set, we call it a Diophantine relation. Similarly, we call a function Diophantine, if its graph is a Diophantine set. The terms of Diophantine sets and Diophantine relations are usually interchangeable. For example, take the relation $\leq$ over the non-negative integers. The set S of pairs (a, b) with $a \leq b$ can be seen as a Diophantine set since

$$(a, b) \in S \Leftrightarrow (\exists x_1 \in \mathbb{N}_0)[D(a, b, x) = 0],$$

for $D = Y_1 - Y_2 + X_1 \in \mathbb{Z}[Y_1, Y_2, X_1]$. This also equals the relation $\leq$, so we can either say that the set S is Diophantine or the relation $\leq$ is, meaning the same thing.
We can generalize this and say that a property P, i.e. a logical expression P, is Diophantine, if the set of all numbers having this property is Diophantine. For example, for the set of even numbers $E \subset \mathbb{N}_0$ we have

$$a \in E \Leftrightarrow (\exists x \in \mathbb{N}_0)[D(a, x) = 0]$$

for the polynomial $D = 2X - Y \in \mathbb{Z}[Y, X]$, so the property 'is an even number' is Diophantine. When it is clear which polynomial D is used, we can simplify the notation and write

$$\mathsf{Even}(s) \Leftrightarrow \exists x[2x = a].$$

The domain of x as given above will always be $\mathbb{N}_0$, so we will only use this simplified notation. This definition of an even number shows that the property 'is an even number' is Diophantine. Disjunction and conjunction of properties correspond to union and intersection of sets, so according to Proposition 2.1.1 the disjunction and conjunction of two Diophantine properties is again Diophantine. The following examples of Diophantine relations use this fact and will come into effect later on:

$$\begin{aligned} a < b &\Leftrightarrow \exists x[a + x + 1 = b], \\ a|b &\Leftrightarrow \exists x[ax = b], \end{aligned} \tag{2.1}$$

Let $\mathsf{rem}(b, c)$ denote the remainder of b divided by c. Then from the above relations, we get that

$$a = \mathsf{rem}(b, c) \Leftrightarrow (a < c) \wedge (c|(b - a)) \tag{2.2}$$

is Diophantine, which will be used in the next section, and also shows that

$$a \equiv b \mod c \Leftrightarrow \mathsf{rem}(a, c) = \mathsf{rem}(b, c)$$

is Diophantine.

Note that we have constructed equation (2.2) with the use of Proposition 2.1.1. For Diophantine Relations $\mathcal{R}_1$ and $\mathcal{R}_2$, $\mathcal{R}_1 \wedge \mathcal{R}_2$ is also Diophantine, since this corresponds to the intersection of the sets. We will use this fact heavily to construct Diophantine sets and relations in the following sections.

2.1.2 Recursively Enumerable Sets

So far we have not introduced a way of knowing what the term 'algorithmically computable' means yet. For this matter, we will make use of the well known Church-Turing-Thesis, which states that algorithmic computability is equivalent to computability by a Turing machine.

Definition. *A Turing machine M is a 7-tuple $M = (Q, \Gamma, \Box, \Sigma, F, q_{\mathsf{start}}, \delta)$ where*

- *Q is a finite set of states, and $q_{\mathsf{start}} \in Q$ is the initial state. Further $F \subset Q$ is the set of final states.*
- *Γ is the finite set of tape symbols, with $\Box \in \Gamma$ the blank symbol*
- *$\Sigma \subset \Gamma \setminus \{\Box\}$ is the set of input symbol*
- *$\delta : (Q \setminus F) \times \Gamma \to Q \times \Gamma \times \{\mathsf{L}, \mathsf{S}, \mathsf{R}\}$ is the transition function*

Assume that $x \in (\Sigma \setminus \{\Box\})^*$. Then a Turing machine M can take this as an input, and if M halts on this input, one can derive $M(x) \in F$. For details we refer to [1]. This leads to the fact that a Turing machine can distinguish between two different cases for the term 'computable'.

Definition. *Let $L \subset (\Sigma \setminus \{\square\})^*$ be a language and let M be a Turing machine. Suppose that for the set F of final states we have $\{0,1\} \subseteq F$. Then*

- *M decides L, if for $x \in L$ we have $M(x) = 1$ and for $x \notin L$ we have $M(x) = 0$. We call L recursive, if there exists a Turing machine that decides L.*
- *M accepts L, if for $x \in L$ we have $M(x) \in F$ and for $x \notin L$ M will never halt. We call L recursively enumerable, if there exists a Turing machine that accepts L.*

It follows directly from this definition that every recursive set is recursively enumerable. Indeed, assume that a Turing machine M decides L. Then, we can construct a Turing machine M' which accepts L by copying M, and for every state in which M goes to the final state 0, M' instead enters a state where it goes to the right without ever halting. It is not true that every recursively enumerable set is recursive, as the Halting problem, among many others, gives a set which can be accepted by a Turing machine, but never decided. We therefore have the following theorem, which is crucial to the answer of Hilbert's tenth problem.

Theorem 2.1.3. *Let $\mathcal{R}$ be the class of all recursive languages, and $\mathcal{R}_{\mathcal{E}}$ the class of all recursively enumerable languages. Then $\mathcal{R} \subsetneq \mathcal{R}_{\mathcal{E}}$.*

The introduction of primitive recursive functions allows us to further characterize recursively enumerable subsets of non-negative integers.

Definition. *Let*

$$\begin{aligned} \mathsf{suc} : \mathbb{N}_0 \to \mathbb{N}_0, x \mapsto x+1, \\ 1^{(n)} : \mathbb{N}_0^n \to \mathbb{N}_0, (x_1, \dots, x_n) \mapsto 1, \\ \mathsf{pr}_i^n : \mathbb{N}_0^n \to \mathbb{N}_0, (x_1, \dots, x_n) \mapsto x_i, \end{aligned}$$

denote the basic functions for $n \in \mathbb{N}_0$. The primitive recursive functions are constructed from the basic functions by applying composition, juxtaposition and recursion.

The composition of two functions is defined in the usual way. For juxtaposition and recursion let $f_1 : \mathbb{N}_0^{k_1} \to \mathbb{N}_0^n, f_2 : \mathbb{N}_0^{k_2} \to \mathbb{N}_0^m$. For $k_1 = k_2$, the juxtaposition of the functions f_1 and f_2 is given by

$$\begin{aligned} g : \mathbb{N}_0^{k_1} \to \mathbb{N}_0^{n+m} \\ (x_1, \dots, x_{k_1}) \mapsto (f_1(x_1, \dots, x_{k_1}), f_2(x_1, \dots, x_{k_1})), \end{aligned}$$

and for $k_2 = k_1 + 2$, $n = m = 1$ the recursion obtained from f_1 and f_2 is a function g given by the equation

$$g(x_1, \dots, x_{k_1}, k) = \begin{cases} f_1(x_1, \dots, x_{k_1}) & : k = 0 \\ f_2(x_1, \dots, x_{k_1}, g(x_1, \dots, x_{k_1}, k-1), k) & : k > 1. \end{cases}$$

We want to be able to compare recursively enumerable sets with Diophantine sets. In order to do so, we first note that the basic functions from the definition above are

Diophantine:

$$
\begin{aligned}
y = \mathsf{suc}(x) &\Leftrightarrow y - x - 1 = 0\\
y = 1^{(n)}(x_1, \dots, x_n) &\Leftrightarrow y - 1 = 0\\
y = \mathsf{pr}_i^n(x_1, \dots, x_n) &\Leftrightarrow y - x_i = 0
\end{aligned}
$$

In addition to that, is is easy to show that any polynomial function is a primitive recursive function. Moreover, the primitive recursive functions can describe the recursively enumerable sets, as seen in the following theorem. For a proof of this theorem see [40].

Theorem 2.1.4. *A set $R \in \mathbb{N}_0^n$ is recursively enumerable if and only if there is a primitive recursive function f such that*

$$R = \{(x_1, \dots, x_n) \in \mathbb{N}_0^n \mid \exists y_1, \dots, y_m \in \mathbb{N}_0 \textit{ such that } f(x_1, \dots, x_n, y_1, \dots, y_m) = 0\}.$$

This theorem allows us to do two things. First, as we did with Diophantine sets, we can identify recursively enumerable sets with primitive recursive functions. Second, any Diophantine set is recursively enumerable. This follows from the fact that every polynomial is a primitive recursive function and the definition of Diophantine sets.
In order to proof Hilbert's tenth problem, we want to establish that the class of Diophantine sets equals the class of recursively enumerable sets. To do so, a third class of sets is introduced, the so called D-sets.

Definition. *Let $E \subseteq \mathbb{N}_0^n$. The set $G \subseteq \mathbb{N}_0^n$ obtained by bounded universal quantification on the i-th coordinate, if*

$$(x_1, \dots, x_n) \in E \Leftrightarrow \forall k \in \{1, \dots, x_i\}[(x_1, \dots, x_{i-1}, k, x_{i+1}, \dots, x_n) \in G].$$

As in [25], D-sets are defined as follows:

Definition. *Let $\mathfrak{D}$ be the class of Diophantine sets. Let $\mathfrak{C}$ be the smallest class containing $\mathfrak{D}$ which is closed under taking finite unions, finite intersections, finite direct products, projections, and applying the bounded universal quantifier. A set $C \in \mathfrak{C}$ is called a D-set.*

In the next section, we will establish that the D-Sets equal the recursively enumerable sets. Then, we will show that all recursively enumerable sets are Diophantine.

2.2 Recursively Enumerable Sets are D-Sets

Lemma 2.2.1. *The class of all recursively enumerable sets is closed with respect to direct product, union, intersection and projection.*

Proof. Let R_1, R_2, R_3 be recursively enumerable sets with primitive recursive functions

$$\begin{aligned} f_1 &: \mathbb{N}_0^{n+a} \to \mathbb{N}_0, \\ f_2 &: \mathbb{N}_0^{n+b} \to \mathbb{N}_0, \\ f_3 &: \mathbb{N}_0^{m+c} \to \mathbb{N}_0, \end{aligned}$$

for $n, m, a, b, c \in \mathbb{N}_0$ such that

$$\begin{aligned} R_1 &= \{(x_1, \dots, x_n) \in \mathbb{N}_0^n \mid \exists y_1, \dots, y_a \in \mathbb{N}_0 \text{ with } f_1(x_1, \dots, x_n, y_1, \dots, y_a) = 0\}, \\ R_2 &= \{(x_1, \dots, x_n) \in \mathbb{N}_0^n \mid \exists y_1, \dots, y_b \in \mathbb{N}_0 \text{ with } f_2(x_1, \dots, x_n, y_1, \dots, y_b) = 0\}, \\ R_3 &= \{(x_1, \dots, x_m) \in \mathbb{N}_0^m \mid \exists y_1, \dots, y_c \in \mathbb{N}_0 \text{ with } f_3(x_1, \dots, x_m, y_1, \dots, y_c) = 0\}. \end{aligned}$$

Closure under projection follows from the definition. For the other operations, like in Proposition 2.1.1, we have

$$\begin{aligned} R_1 \cup R_2 = \{(x_1, \dots, x_n) \in \mathbb{N}_0^n \mid \exists y_1, \dots, y_a, y'_1 \dots, y'_b \in \mathbb{N}_0 \\ \text{with } f_1(x_1, \dots, x_n, y_1, \dots, y_a) f_2(x_1, \dots, x_n, y'_1, \dots, y'_b) = 0\}, \\ R_1 \cap R_2 = \{(x_1, \dots, x_n) \in \mathbb{N}_0^n \mid \exists y_1, \dots, y_a, y'_1 \dots, y'_b \in \mathbb{N}_0 \\ \text{with } (f_1(x_1, \dots, x_n, y_1, \dots, y_a))^2 + (f_2(x_1, \dots, x_n, y'_1, \dots, y'_b))^2 = 0\}, \\ R_1 \times R_2 = \{(x_1, \dots, x_n, z_1, \dots, z_m) \in \mathbb{N}_0^{n+m} \mid \exists y_1, \dots, y_a, y'_1 \dots, y'_c \in \mathbb{N}_0 \\ \text{with } (f_1(x_1, \dots, x_n, y_1, \dots, y_a))^2 + (f_3(u_1, \dots, u_m, y'_1, \dots, y'_c))^2 = 0\}, \end{aligned}$$

and since the product and the sum of primitive recursive functions is again primitive recursive, the sets $R_1 \cup R_2, R_1 \cap R_2$ and $R_1 \times R_2$ are recursively enumerable. □

We need to introduce the so called Gödel function, which is defined by

$$\begin{aligned} \mathsf{gd} &: \mathbb{N}_0^3 \to \mathbb{N}_0, \\ (u, k, t) &\mapsto \mathsf{rem}(1 + kt, u). \end{aligned}$$

With the use of this function, we may encode arbitrarily long sequences $(y_1, \dots, y_N)$ with the pair (u, t).

Indeed, choose some $X \in \mathbb{N}_0$ large enough such that $X \geq N$ and for all $k \in \{1, \dots, N\}$ we have $1 + kN! > y_k$ and set $t = X!$. Consider the system of equations

$$\begin{aligned} u &\equiv y_1 \mod 1 + t \\ u &\equiv y_2 \mod 1 + 2t \\ &\dots \\ u &\equiv y_N \mod 1 + Nt. \end{aligned}$$

For all $i, j \in \{1, \dots, N\}$, we have $\gcd(1 + it, 1 + jt) = \gcd(1 + iX!, 1 + jX!) = 1$, since any prime p dividing the greatest common divisor would also divide $(i - j)X!$, meaning that $p < X$, but no such p could divide $1 + iX!$. Therefore, according to the Chinese Remainder Theorem, there is a unique solution $u \in \mathbb{N}_0$ to this system of equations with $u < \prod_{i=1}^N (1 + it)$. Thus (u, t) encodes the N-tuple $(y_1, \dots, y_N)$.

By (2.2), the remainder function and thus also the Gödel function are Diophantine. Moreover, it can be shown that this function is primitive recursive.

Lemma 2.2.2. *The class of all recursively enumerable sets is closed with respect to the bounded universal quantifier.*

Proof. Let E be a recursively enumerable set with primitive function f with domain $\mathbb{N}_0^{n+m}$. Let $G \subseteq \mathbb{N}_0^n$ be obtained from E by the use of the bounded universal quantifier. We define a function g by

$$g(x_1, \dots, x_n, u_1, \dots, u_m, t_1, \dots, t_m) = \sum_{k=1}^{x_n} (f(x_1, \dots, x_{n-1}, k, \mathsf{gd}(u_1, k, t_1), \dots, \mathsf{gd}(u_m, k, t_m)))^2.$$

Since f and gd are primitive recursive, so is g. We will show that

$$G = \{(x_1, \dots, x_n) \in \mathbb{N}_0^n \mid \exists u_1, \dots, u_m, t_1, \dots, t_m \\ \text{with } g(x_1, \dots, x_n, u_1, \dots, u_m, t_1, \dots, t_m) = 0\},$$

meaning that G is recursively enumerable.
First, assume that for a tuple $(x_1, \dots, x_n) \in \mathbb{N}_0^n$, there are some u_j, t_j such that

$$g(x_1, \dots, x_n, u_1, \dots, u_m, t_1, \dots, t_m) = 0.$$

This means that for all $k \in \{1, \dots, x_n\}$

$$f(x_1, \dots, x_{n-1}, k, \mathsf{gd}(u_1, k, t_1), \dots, \mathsf{gd}(u_m, k, t_m)) = 0,$$

and hence $(x_1, \dots, x_n) \in G$ by the definition of the bounded universal quantifier.
So now assume that $(x_1, \dots, x_n) \in G$. Then, for all $k \in \{1, \dots, x_n\}$ there are some $y_{i,k}$, $i \in \{1, \dots, m\}$, such that

$$f(x_1, \dots, x_{n-1}, k, y_{1,k}, \dots, y_{m,k}) = 0.$$

By the definition of gd, there are pairs (u_i, t_i) with $\mathsf{gd}(u_i, k, t_i) = y_{i,k}$ for all i, k. Therefore there exist u_i, t_i such that

$$g(x_1, \dots, x_n, u_1, \dots, u_m, t_1, \dots, t_m) = 0,$$

which completes the proof. □

Lemma 2.2.3. *Every D-set is recursively enumerable.*

Proof. Every Diophantine set it recursively enumerable. The class of D-sets is obtained by closing the Diophantine sets under direct product, union, intersection, projection and the bounded universal quantifier. Thus, by Lemma 2.2.1 and Lemma 2.2.2, every D-set is recursively enumerable. □

To prove the other direction, we use the characterization of recursively enumerable sets as given in Theorem 2.1.4.

Lemma 2.2.4. *Let $f : \mathbb{N}_0^{d_f} \to \mathbb{N}_0^{i_f}, g : \mathbb{N}_0^{d_g} \to \mathbb{N}_0^{i_g}$ be primitive recursive functions whose graphs Γ_f, Γ_g are D-sets.*

1. *Let $d_f = q, i_f = r, d_g = p, i_g = q$. Further let $h_1 : \mathbb{N}_0^p \to \mathbb{N}_0^r$ be the primitive recursive function, which is the composition of f and g. Then Γ_{h_1}, the graph of h_1, is a D-set.*
2. *Let $d_f = p, i_f = q, d_g = p, i_g = r$. Further let $h_2 : \mathbb{N}_0^p \to \mathbb{N}_0^{r+q}$ be the primitive recursive function, which is the juxtaposition of f and g. Then Γ_{h_2}, the graph of h_2, is a D-set.*

Proof. 1. By definition, we have

$$\begin{aligned}\Gamma_{h_1} &= \{(x_1, \dots, x_p, y_1, \dots, y_r) \mid h_1(x_1, \dots, x_p) = (y_1, \dots, y_r)\} \\ &= \{(x_1, \dots, x_p, y_1, \dots, y_r) \mid \exists z_1, \dots, z_z \in \mathbb{N}_0 \text{ with} \\ &\qquad [g(x_1, \dots, x_p) = (z_1, \dots, z_q) \text{ and } f(z_1, \dots, z_q) = (y_1, \dots, y_r)]\}.\end{aligned}$$

Hence Γ_{h_1} is the projection of $(\Gamma_g \cap \mathbb{N}_0^r) \times (\mathbb{N}_0^p \cap \Gamma_f)$ to the first r and last q coordinates. Since D-sets are closed under finite direct products, intersections and projections, Γ_{h_1} is also a D-set.

2. For juxtaposition, we first define a function

$$\begin{aligned}\mathsf{perm}_{p,q,r} : \mathbb{N}_0^{p+q+r} &\to \mathbb{N}_0^{p+q+r} \\ (x_1, \dots, x_p, y_1, \dots, y_q, z_1, \dots, z_r) &\mapsto (x_1, \dots, x_p, z_1, \dots, z_r, y_1, \dots, y_q).\end{aligned}$$

It is easy to see that the image of a Diophantine set under $\mathsf{perm}_{p,q,r}$ is again Diophantine. By the definition of juxtaposition, the graph is given by

$$\begin{aligned}\Gamma_{h_2} &= \{(x_1, \dots, x_r, y_1, \dots, y_q, z_1, \dots z_r)) \mid h_1(x_1, \dots, x_r) = (y_1, \dots, y_q, z_1, \dots z_r)\} \\ &= \{(x_1, \dots, x_r, y_1, \dots, y_q, z_1, \dots z_r)) \mid \\ &\qquad f(x_1, \dots, x_r) = (y_1, \dots, y_q) \text{ and } g(x_1, \dots, x_r) = (z_1, \dots z_r)\}.\end{aligned}$$

Therefore $\Gamma_{h_2} = (\Gamma_f \times \mathbb{N}_0^r) \cap \mathsf{perm}_{p,q,r}(\Gamma_g \times \mathbb{N}_0^q)$. Again since D-sets are closed under intersection and direct product, Γ_{h_2} is a D-set.

□

Lemma 2.2.5. *Let $f : \mathbb{N}_0^n \to \mathbb{N}_0, g : \mathbb{N}_0^{n+2} \to \mathbb{N}_0$ be primitive recursive functions whose graphs Γ_f, Γ_g are D-sets. Then the graph Γ_h, where h is the function defined recursively from f and g, is a D-set.*

Proof. First we write the graph Γ_h as a union $\Gamma_h = \Gamma_1 \cup \Gamma_2$, where

$$\begin{aligned}(x_1, \dots, x_{n+1}, y) \in \Gamma_h \text{ with } x_{n+1} = 0 &\Leftrightarrow (x_1, \dots, x_{n+1}, y) \in \Gamma_1, \\ (x_1, \dots, x_{n+1}, y) \in \Gamma_h \text{ with } x_{n+1} \geq 1 &\Leftrightarrow (x_1, \dots, x_{n+1}, y) \in \Gamma_2.\end{aligned}$$

By the definition of the recursion of two functions, we have $x_{n+1} = 0$ for $(x_1, \dots, x_{n+1}, y) \in \Gamma_1$ iff $f(x_1, \dots, x_n) = y$, and this holds iff $(x_1, \dots, x_n, y) \in \Gamma_f$. Hence

$$\Gamma_1 = \mathsf{perm}_{n,1,1}(\Gamma_f \times \mathbb{N}_0) \cap \mathsf{perm}_{n,1,1}(\mathbb{N}_0^{n-1} \times \{0\}),$$

therefore Γ_1 is a D-set. So it remains to prove that Γ_2 is also one. In order to do so, we introduce a set E, which is the projection of $E' \subseteq \mathbb{N}_0^{n+4}$ to its first $n+2$ coordinates, where the E' is defined by

$$\begin{aligned}(x_1,\dots,x_n,y,z,u,t) \in E' \Leftrightarrow z = \mathsf{gd}(u,y,t) \\ \text{and } \mathsf{gd}(u,0,t) = f(x_1,\dots,x_n) \\ \text{and } y \geq 1, \text{ for } k \in \{2,\dots,y\} \\ \mathsf{gd}(u,k,t) = g(x_1,\dots,x_n,k-1,\mathsf{gd}(u,k-1,t))\end{aligned}$$

We denote the first equation of the equivalence above E_1, the second E_2 and the third E_3. We claim that $\Gamma_2 \subseteq E$. Let $(x_1,\dots,x_n,y,z) \in \Gamma_2$. Further let $(a_1,\dots,a_y)$ be the sequence defined by $a_i = h(x_1,\dots,x_n,i)$ for $i \in \{1,\dots,y\}$. By the definition of the function gd, we can find u,t such that $\mathsf{gd}(u,k,t) = a_k$. Since $(x_1,\dots,x_n,y,z) \in \Gamma_2$, we have $h(x_1,\dots,x_n,y) = z$ and thus equation E_1 is true. Also E_2 is satisfied, since

$$\mathsf{gd}(u,0,t) = h(x_1,\dots,x_n,0) = f(x_1,\dots,x_n).$$

It is easy to show that E_3 holds by using induction on k, so indeed $\Gamma_2 \subseteq E$.
Next we claim that $E \subseteq \Gamma_2$. To show this, let $(x_1,\dots,x_n,y,z,u,t) \in E$. Then E_1, E_2, E_3 define the recursion of f and g which is h, and since by E_3 we have $y \geq 1$, $(x_1,\dots,x_n,y,z) \in \Gamma_2$ and thus $\Gamma_2 \subseteq E$.
Since $\Gamma_2 = E$, it suffices to show that sets which are determined by E_1, E_2, E_3 are D-sets, proving that Γ_2 is a D-set. E_1 is Diophantine and thus the corresponding set is a D-set. The set determined by E_2 is the projection to the first $n+4$ coordinates of the intersection of the D-sets given by the relations

$$k-1=0, w = \mathsf{gd}(u,k,t) \text{ and } f(x_1,\dots,x_n) - w = 0,$$

thus E_2 describes a D-set. So let us consider the set that arises from equation E_3. Let F be the set

$$(x_1,\dots,x_n,x_{n+1},u,t) \in F \Leftrightarrow \mathsf{gd}(u,x_{n+1}+1,t) = g(x_1\dots,x_{n+1},\mathsf{gd}(u,x_{n+1},t)).$$

This is a D-set, as it is the projection to the first $n+3$ of the intersection of the sets

$$\begin{aligned}w_1 &= \mathsf{gd}(u,x_{n+1}+1,t),\\ w_2 &= \mathsf{gd}(u,x_{n+1},t),\\ w_3 &= g(x_1,\dots,x_{n+1},w_2) = w_1.\end{aligned}$$

So

$$(x_1,\dots,x_{n+1},u,t) \in E_3 \Leftrightarrow \forall k \in \{1,\dots,x_{n+1}-1\} : (x_1,\dots,x_n,k,u,t) \in F$$

and thus E_3 is a D-set. □

Theorem 2.2.6. *The class of all D-sets equals the class of all recursively enumerable sets.*

Proof. From Lemma 2.2.3, every D-set is recursively enumerable, so we have to show that the converse is also true. Let E be a recursively enumerable set. By Theorem 2.1.4, the set E is the projection of

$$(\mathbb{N}_0^n \times \{0\}) \cap \{(x_1,\dots,x_n,y) \in \mathbb{N}_0^{n+1} \mid f(x_1,\dots,x_n) = y\}$$

to its first n coordinates, for some primitive recursive function f. So it suffices to show that every graph of a recursive function is a D-set. Every recursive function arises from the basic functions by applying composition, juxtaposition and recursion. So by Lemma 2.2.4 and Lemma 2.2.5, and the fact that the basic recursive functions describe D-sets, the graph of every recursive function is indeed a D-set. □

Since we have shown that D-sets are the same as recursively enumerable sets, we want to deduce the equality of the class of D-sets and Diophantine sets. For this, we will need to show that exponentiation as well as the factorial relation are both Diophantine.

2.3 Pell's equation

We will first establish that the exponential relation, i.e. the set of all triples (k, m, n) with $m = k^n$ is Diophantine. To do so, we will work with a certain kind of Pell's equation. Pell's equation is a Diophantine equation of the form

$$x^2 - dy^2 = 1. \tag{2.3}$$

This equation is trivial when d is a square, so this case is omitted.
Solutions to (2.3) are connected with properties of the ring $\mathbb{Z}[\sqrt{d}]$. In order to work with it, we will give the following definition.

Definition. *Let L/K be a finite field extension, and let μ_a be the K-linear map*

$$\begin{aligned}\mu_a : L &\to L,\\ x &\mapsto ax\end{aligned}$$

for some $a \in L$. We define the norm of a as $N_{L/K}(a) := \det \mu_a$.

We will only need the norm function for an algebraic number field $K/\mathbb{Q}$, which we will simply denote as N. An algebraic number field is a finite Galois extension, so we can use the well-known fact that

$$N(x) = \prod_{\sigma \in G} \sigma x \text{ for } G = \mathrm{Gal}(K/\mathbb{Q}).$$

Let $\mathcal{O}_K$ be the ring of integers of K. Then for all $a \in \mathcal{O}_K$, we have $|N(a)| = 1$ if and only if a is a unit.

2.3.1 Fundamental Units

Let K be a field and denote by $\mu(K)$ the roots of unit of K. For certain $d \in \mathbb{Z}$, we will show that solutions to (2.3) have a finite set of generators.

Theorem 2.3.1 (Dirichlet's Unit Theorem). *Let K be an algebraic number field with $[K : \mathbb{Q}] = r_1 + 2r_2$, where r_1 denotes the number of real and r_2 the number of pairs of conjugate complex embeddings. Let $\mathcal{O}_K$ be the ring of integers of K. Then there are some $\zeta \in \mu(\mathcal{O}_K)$ and $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1} \in \mathcal{O}_K^\times$ such that every $\varepsilon \in \mathcal{O}_K^\times$ has a unique representation*

$$\varepsilon = \zeta^d \prod_{i=1}^{r_1+r_2-1} \varepsilon_i^{k_i}, \quad \textit{with } d \in \{0, \ldots, \operatorname{ord}(\zeta) - 1\}, k_1, \ldots, k_{r_1+r_2-1} \in \mathbb{Z}.$$

This means that

$$\mathcal{O}_K^\times \cong \mu(\mathcal{O}_K) \times \mathbb{Z}^{r_1+r_2-1}.$$

We denote a tuple $(\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1})$ as the fundamental units of $\mathcal{O}_K$. We can use the Unit Theorem to prove the following:

Proposition 2.3.2. *Let $d \in \mathbb{N}_0$ be square-free with $d \equiv 2, 3 \mod 4$. Then the equation*

$$x^2 - dy^2 = 1$$

has an infinite set of solutions $S \subset \mathbb{Z}^2$, and there is some solution $(\alpha, \beta) \in S$ such that there is a unique $k \in \mathbb{Z}$ with

$$a + b\sqrt{d} = \pm(\alpha + \beta\sqrt{d})^k$$

for all $(a, b) \in S$.

Proof. Denote by K the quadratic number field $\mathbb{Q}(\sqrt{d})$. Since d is positive, $K \subset \mathbb{R}$, hence $\mu(K) = \{-1, 1\}$. Moreover there are two real embeddings

$$\sigma : a + b\sqrt{d} \mapsto a \pm b\sqrt{d},$$

and with $[K : \mathbb{Q}] = 2$ we have no complex embeddings. Thus, by Dirichlet's Unit Theorem, $\mathcal{O}_K^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. With $d \equiv 2, 3 \mod 4$ we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. The set of units equals the set of algebraic integers $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$ with $1 = N_K(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$, so the units are in a one-to-one correspondence with the set S.

□

We call a pair (α, β), as given in the proposition above, a fundamental solution. Next we consider the Pell equation

$$x^2 - (a^2 - 1)y^2 = 1, \tag{2.4}$$

for some positive integer $a > 1$. We claim that $(x, y) = (a, 1)$ is the fundamental solution to the above equation. To show this, we can not work with the abovementioned proposition, since for the case $a \equiv 3 \mod 4$, we have that $d = a^2 - 1$ is not square-free. In fact, we will only show that $(a, 1)$ generates the positive integer solutions of the above equation. So consider solutions to (2.4) given by $\chi_1 = x_1 + y_1\sqrt{d}, \chi_2 = x_2 + y_2\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ with $1 \leq \chi_1, \chi_2$. It is easy to see that for any $x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ solving (2.4) we have

- $x, y > 0 \Leftrightarrow x + y\sqrt{d} > 1$,
- $x > 0$ and $y < 0 \Leftrightarrow 0 < x + y\sqrt{d} < 1$,
- $x < 0$ and $y > 0 \Leftrightarrow -1 < x + y\sqrt{d} < 0$,
- $x, y < 0 \Leftrightarrow x + y\sqrt{d} < -1$,

so $x_1, x_2, y_1, y_2 > 0$. If we have $1 \leq \chi_1 < \chi_2$, it follows that $1 \leq x_1 < x_2$ and $0 \leq y_1 < y_2$, so the set of all $\alpha = x + y\sqrt{d} > 1$ with $x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d}) = N(\alpha) = 1$ is well-ordered. We claim that the smallest α in this set is the fundamental solution to (2.4). Indeed, on the one hand for any $n \in \mathbb{N}_0$ we have $N(\alpha^n) = N(\alpha)^n = 1$, so α^n is a solution. On the other hand for a solution with $1 \leq \beta$, there is some n such that

$$\alpha^n \leq \beta < \alpha^{n+1},$$

so $1 \leq \alpha^{-n}\beta < \alpha$ and $N(\alpha^{-n}\beta) = 1$. By the minimality of α we have $\alpha^{-n}\beta = 1$ and thus $\beta = \alpha^n$. Therefore, in order to show that $(a, 1)$ is the fundamental solution, we need to prove that $a + \sqrt{d}$ is minimal among solutions to the Pell equation above which are greater than 1. Assume that $\chi = x_3 + y_3\sqrt{d}$ is a solution with $1 < \chi_3 < a + \sqrt{d}$. But then $x_3 < a$ and $y_3 < 1$, which is not possible, so $(a, 1)$ is indeed the fundamental solution.

2.3.2 The Functions $X_a(n)$ and $Y_a(n)$

Since $(a, 1)$ is the fundamental solution of (2.4), the coefficients (x, y) of any solution $(a + \sqrt{d})^n$ can be expressed through $(a, 1)$.

Definition. *Let $a, n \in \mathbb{N}_0$ with $a > 1$. We denote by $(X_a(n), Y_a(n)) \in \mathbb{N}_0^2$ the unique pair solving the system of equations*

$$x^2 - (a^2 - 1)y^2 = 1, \tag{2.5}$$

$$x + y\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^n. \tag{2.6}$$

Note that it follows from the definition above that both $X_a(n)$ and $Y_a(n)$ are strictly increasing functions in n. Moreover, by the previous section, $X_a(n)$ and $Y_a(n)$ are well-defined. In fact, they form a bijective map from $\mathbb{N}_0$ to solution pairs over the non-negative integers of (2.4): For every $(x_o, y_o) \in \mathbb{N}_0^2$ with $x_0^2 - (a^2 - 1)y_0^2 = 1$ there is a unique $n \in \mathbb{N}_0$ with $(x_o, y_o) = (X_a(n_o), Y_a(n_o))$.
Taking conjugates in the ring $\mathbb{Z}[\sqrt{d}]$ is a ring homomorphism, so from (2.6) we derive the equivalent equation

$$x - y\sqrt{a^2 - 1} = (a - \sqrt{a^2 - 1})^n. \tag{2.7}$$

We will now prove some properties of the functions $Y_a(n)$ and $X_a(n)$.

Lemma 2.3.3. *Let $a > 1$. Then for all $n, m \in \mathbb{N}_0$ with $n \geq m$ we have the following equations:*

$$X_a(n \pm m) = X_a(n)X_a(m) \pm dY_a(n)Y_a(m) \tag{2.8}$$

$$Y_a(n \pm m) = Y_a(n)X_a(m) \pm X_a(n)Y_a(m) \tag{2.9}$$

$$X_a(2n) = 2X_a(n)^2 - 1 \tag{2.10}$$

$$Y_a(2n) = 2X_a(n)Y_a(n) \tag{2.11}$$

Proof. From (2.6), we obtain

$$\begin{aligned} X_a(n+m) + Y_a(n+m)\sqrt{d} &= (a+\sqrt{d})^{n+m} \\ &= (a+\sqrt{d})^n(a+\sqrt{d})^m \\ &= (X_a(n)+Y_a(n)\sqrt{d})(X_a(m)+Y_a(m)\sqrt{d}). \end{aligned}$$

Noting that $\overline{(a+\sqrt{s})} = a - \sqrt{s} = (a+\sqrt{s})^{-1}$, we use the same method to obtain

$$X_a(n-m) + \sqrt{d}Y_a(n-m) = (X_a(n)+\sqrt{d}Y_a(n))(X_a(m)-\sqrt{d}Y_a(m)).$$

Every element in $\alpha \in \mathbb{Z}[\sqrt{d}]$ can uniquely be written as $\alpha = x + y\sqrt{d}$, so by separating the above equations into integers and elements in $\sqrt{d}\mathbb{Z}$, we obtain the first two equations. Equation (2.11) follows by setting $m = n$. For equation (2.10), we have

$$X_a(2n) = X_a(n+n) = X_a(n)^2 + dY_a(n)^2 = X_a(n)^2 + (X_a(n)^2 - 1).$$

□

By definition, we have

$$X_a(n) + Y_a(n)\sqrt{a^2-1} = (a+\sqrt{a^2-1})^n$$

for all $n \in \mathbb{N}_0$. Thus, for all $a \geq 2$, $X_a(0) = 1, X_a(1) = a$ and $Y_a(0) = 0, Y_a(1) = 1$. By setting $m = 1$ in (2.8) and (2.9), we can represent X and Y as the linear recurrences

$$X_a(0) = 1, \quad X_a(1) = a, \quad X_a(n+1) = 2aX_a(n) - X_a(n-1), \tag{2.12}$$

$$Y_a(0) = 0, \quad Y_a(1) = 1, \quad Y_a(n+1) = 2aY_a(n) - Y_a(n-1). \tag{2.13}$$

These recurrences even hold for $a = 1$, by setting $X_1(n) = 1$ and $Y_1(n) = n$. This allows us to prove the following:

Lemma 2.3.4. *Let $a, b \geq 1$ and $n, k \in \mathbb{N}_0$. then*

$$Y_a(n) \equiv Y_b(n) \mod (a-b), \tag{2.14}$$

$$Y_a(n) \equiv n \mod (a-1), \tag{2.15}$$

$$(2a-1)^n \leq Y_a(n+1) < (2a)^n, \tag{2.16}$$

$$X_a(n) - (a-k)Y_a(n) \equiv k^n \mod (2ak - k^2 - 1). \tag{2.17}$$

Proof. We show the first equation by induction on $n \in \mathbb{N}_0$. For $n \in \{0, 1\}$ there is nothing to show, so assume that $n \geq 2$. By (2.13), $Y_a(n)$ is a polynomial in a and n. Hence, also by the above recurrence,

$$\begin{aligned} Y_a(n) - Y_b(n) &\equiv 2(a-b)(Y_a(n-1) - Y_b(n-1) - (Y_a(n-2) - Y_b(n-2)) \\ &\equiv 0 \mod (a-b). \end{aligned}$$

For equation (2.15), we set $b = 1$. The third equation is easily proved by induction with (2.13). For the fourth equation, we again use induction on n and the equations (2.12) and (2.13). For $n \in \{0, 1\}$ there is nothing to show, so assume that $n \geq 2$. Then

$$\begin{aligned} X_a(n+1) - (a-k)Y_a(n+1) &\equiv 2a(X_a(n) - (a-k)Y_a(n)) - (X_a(n-1) - (a-k)Y_a(n-1)) \\ &\equiv 2ak^n - k^{n-1} \equiv k^{n-1}(2ak-1) \\ &\equiv k^2k^{n-1} \equiv k^{n+1} \mod (2ak - k^2 - 1). \end{aligned}$$

□

The following two lemmas are crucial to prove Proposition 2.3.7:

Lemma 2.3.5. *With the notations above, we have*

$$n|m \text{ if and only if } Y_a(n)|Y_a(m) \text{ and} \tag{2.18}$$

$$Y_a^2(n)|Y_a(m) \text{ if and only if } nY_a(n)|m. \tag{2.19}$$

Proof. By definition $Y_a(n)$ and $X_a(n)$, for any $n \in \mathbb{N}_0$, form a solution to the Pell equation $x^2 - (a^2-1)y^2 = 1$, thus $\gcd(X_a(n), Y_a(n)) = 1$. By (2.9)

$$Y_a(n \pm m) \equiv Y_a(m)X_a(n) \mod Y_a(n),$$

and thus $Y_a(n)|Y_a(n \pm m)$ if and only if $Y_a(n)|Y_a(m)$. For unique $q, r \in \mathbb{Z}$ with $0 \leq r < n$ we can write $m = qn + r$ and thus

$$Y_a(n)|Y_a(m) \quad \Leftrightarrow \quad Y_a(n)|Y_a(qn+r) \quad \Leftrightarrow \quad Y_a(n)|Y_a(r).$$

Hence $Y_a(n)|Y_a(m)$ if and only if $Y_a(r) = 0$ and this holds if and only if $n|m$. For equation (2.19), we have

$$\begin{aligned} X_a(jn) + Y_a(jn)\sqrt{d} &= (a+\sqrt{d})^{jn} = (X_a(n) + Y_a(n)\sqrt{d})^j \\ &= \sum_{i=0}^{j} \binom{j}{i} (X_a(n))^{j-i}(Y_a(n)\sqrt{d})^i \\ &= \sum_{i \text{ even}} (X_a(n))^{j-i}(Y_a(n)\sqrt{d})^i + \sqrt{d} \sum_{i \text{ odd}} (X_a(n))^{j-i}(Y_a(n)\sqrt{d})^{i-1}. \end{aligned}$$

and hence

$$Y_a(nj) = \sum_{i \text{ odd}} (X_a(n))^{j-i}(Y_a(n)\sqrt{d})^{i-1} \equiv jX_a(n)^{j-1}Y_a(n) \mod (Y_a(n))^2.$$

Now assume that $(Y_a(n))^2|Y_a(m)$. Then $Y_a(n)|Y_a(m)$ and by the first part of the lemma, there is some $k \in \mathbb{Z}$ with $n = km$. Now

$$kX_a(n)^{k-1}Y_a(n) \equiv Y_a(m) \equiv 0 \mod (Y_a(m)^2)$$

and thus $(Y_a(n))^2|kY_a(m)$, meaning that $nY(n)|m$. For the other direction, suppose that $nY(n)|m$, and again let $k = Y(n)$. Then

$$Y_a(nY_a(n)) \equiv Y_a(n)X_a(n)^{Y_a(n)-1}Y_a(n) \equiv 0 \mod (Y_a(n))^2,$$

so $(Y_a(n))^2|Y_a(nY_a(n))$, and by (2.18) and the fact that $nY_a(n)|m$, $Y_a(nY_a(n))|Y_a(m)$ and thus $(Y_a(n))^2|Y_a(m)$. □

Lemma 2.3.6. *With the notations above, for $a \geq 2$, $n \in \mathbb{N}_0$*

$$Y_a(n-1) + Y_a(n) < X_a(n), \tag{2.20}$$
$$Y_a(4ni \pm m) \equiv \pm Y_a(m) \mod X_a(n), \tag{2.21}$$
$$Y_a(4ni + 2n \pm m) \equiv \mp Y_a(m) \mod X_a(n), \tag{2.22}$$
$$Y_a(k) \equiv \pm Y_a(m) \mod X_a(n) \text{ if and only if } k \equiv \pm m \mod 2n, \tag{2.23}$$

where the signs $\pm$ *do not correspond in equation* (2.23)*.*

Proof. By (2.9), we have

$$2Y_a(n-1) \leq aY_a(n-1) < aY_a(n-1) + X_a(n-1) = Y_a(n),$$

hence $Y_a(n-1) < Y_a(n) - Y_a(n-1)$ and it follows that

$$Y_a(n-1) + Y_a(n) < 2Y_a(n) - Y_a(n-1) \leq aY_a(n) - Y_a(n-1) = X_a(n),$$

so $Y_a(n-1) + Y_a(n) < X_a(n)$.
Next by Lemma 2.3.3,

$$Y_a(2n) \equiv 0 \text{ and } X_a(2n) \equiv -1 \mod X_a(n).$$

So by (2.9) and using $2n$ instead of n, we derive

$$Y_a(2n \pm m) \equiv \mp Y_a(m) \mod X_a(n)$$

and thus for all $i \in \mathbb{N}_0$ we have

$$\begin{aligned} Y_a(4ni \pm m) &= Y_a(i(2n+2n) \pm m) = Y_a(2n + \overbrace{2n + \cdots + 2n \pm m}^{:=m'}) \equiv -Y_a(m') = \\ &= Y_a(2n + \overbrace{\underbrace{2n + \cdots + 2n}_{2i-1 \text{ terms}}}^{:=m''} \pm m) \equiv Y_a(m'') \equiv \ldots \equiv Y_a(2n + 2n \pm m) \equiv -Y_a(2n \pm m) \\ &\equiv \pm Y_a(m) \mod X_a(n). \end{aligned}$$

Equation (2.22) follows along the same lines. For the last equation of the lemma, first assume that $k = 2nj \pm m$ for some $j \in \mathbb{N}_0$. With the two equations derived above, we have

$$Y_a(k) = \begin{cases} Y_a(4ni \pm m) \equiv \pm Y_a(m) & \text{for } j = 2i \\ Y_a(4ni + 2n \pm m) \equiv \mp Y_a(m) & \text{for } j = 2i+1 \end{cases}$$

for some $i \in \mathbb{N}_0$, so $Y_a(k) \equiv \pm Y_a(m) \mod X_a(m)$.
So assume now that $Y_a(k) \equiv \pm Y_a(m) \mod X_a(n)$. Let $0 \leq k', m' \leq n$ be representants of $\pm k$ and $\pm m$ modulo $2n$. Then there is some $i \in \mathbb{N}_0$ such that $k = \pm k' + i(2n)$ and like we showed before

$$Y_a(k) = Y_a(2n + \cdots + 2n \pm k') \equiv \pm Y_a(k') \mod X_a(n).$$

Likewise it follows that $Y_a(m) \equiv \pm Y_a(m')$ and thus by assumption $Y_a(k') \equiv \pm Y_a(m')$ mod $X_a(n)$. Suppose that $k' \neq m'$. Then, since $Y_a(n)$ is strictly increasing in n and by (2.20),

$$0 < |Y_a(k' \pm Y_a(m')| \leq |Y_a(k' + Y_a(m')| \leq Y_a(n-1) + Y(n) < X_a(n),$$

contradicting $X : a(n) | (Y_a(k') \pm Y_a(m'))$. So $k' = m'$ and hence $k \equiv \pm m \mod 2n$. □

We are now able to show that both functions $X_a(n)$ and $Y_a(n)$ are Diophantine.

Proposition 2.3.7. *Let $a \geq 2$. Then $c = Y_a(n)$ and $d = X_a(n)$ are Diophantine relations.*

Proof. We will prove first that for all $(c, a, n) \in \mathbb{N}_0$, $c = Y_a(n)$ holds if and only if there are $d, e, f, g, h, i, j \in \mathbb{N}_0$ such that

$$\begin{array}{llllll} (1) & d^2 - (a^2-1)c^2 = 1, & (4) & e = (j+1)2c^2, & (7) & h \equiv c \mod f, \\ (2) & f^2 - (a^2-1)e^2 = 1, & (5) & g \equiv a \mod f, & (8) & h \equiv n \mod 2c, \\ (3) & i^2 - (g^2-1)h^2 = 1, & (6) & g \equiv 1 \mod 2c, & (9) & n \leq c. \end{array}$$

This would mean that $c = Y_a(n)$ is the finite intersection of Diophantine relations and thus Diophantine. So first assume that for some $d, e, f, g, h, i, j \in \mathbb{N}_0$ the equations $(1) - (9)$ are true. Then, by definition of $X_a(n)$ and $Y_a(n)$, there are some $n_1, n_2, n_3 \in \mathbb{N}_0$ such that

$$d = X_a(n_1),\ c = Y_a(n_1),\ f = X_a(n_2),\ e = Y_a(n_2),\ i = X_g(n_3) \text{ and } h = Y_g(n_3).$$

So to prove that $c = Y_a(n)$, it suffices to show that $n_1 = n$. By relation (4) and (2.22), we have

$$c^2 | e \;\Leftrightarrow\; (Y_a(n_1))^2 | Y_a(n_2) \;\Leftrightarrow\; n_1 Y_a(n_1) | n_2 \;\Rightarrow\; Y_a(n_1) | n_2 \;\Leftrightarrow\; c | n_2.$$

By (2.14), $Y_g(n_3) \equiv Y_1(n_3) \mod g-1$, and with $g - 1 \equiv 0 \mod 2c$ it follows that $Y_g(n_3) \equiv Y_1(n_3) \mod 2c$, hence

$$n \equiv h = Y_g(n_3) \equiv Y_1(n_3) = n_3 \mod 2c.$$

Also with (2.14) we have $Y_a(n_3) \equiv Y_g(n_3) \mod f$, therefore

$$Y_a(n_3) \equiv Y_g(n_3) = h \equiv c = Y_a(p) \mod X_a(n_2)$$

and thus by (2.23) $n_3 \equiv \pm n_1 \mod 2n_2$. With $c | n_2$ and $n \equiv n_3 \mod 2c$ it follows that $n \equiv \pm n_1 \mod 2c$, and since $0 \leq n_1, b \leq c$, it follows that $n = n_1$. For the equivalence to be true is is not necessary that $d = X_a(n)$, but this is also true by relation (1).
For the other direction, assume that $c = Y_a(n)$ and let $d = X_a(n)$. By definition (1) holds and (9) by the monotonicity of Y_a. By setting $n_2 = nY_a(n), f = X_a(2n_2)$ and $e = Y_a(2n_2$, (2) holds. By (2.19),

$$nY_a(n) | nY_a(n) \Leftrightarrow c^2 = (Y_a(n))^2 | Y_a(nY_a(n)) = Y_a(n_2),$$

and by (2.11) $2X_a(n_2)Y_a(n_2) | Y_a(2n_2)$ and thus $2c^2 | e$, so there is some $j \in \mathbb{N}_0$ with $e = (j+1)2c^2$, which is (4). By setting $g = a + f^2(f^2 - a)$, $i = X_g(n)$, $h = Y_g(n)$ we have (5) and (3), and (5) together with (2) and (4) gives (6). By (2.15),

$$h = Y_g(n) \equiv n \mod g-1 \text{ and } g - 1 \equiv 0 \mod 2c$$

we have (8). By (2.14),

$$h = Y_g(n) \equiv Y_a(n) = n \mod g-a \text{ and } g - a \equiv 0 \mod f$$

we have (7).

Now that we have proven that $c = Y_a(n)$ is a Diophantine equation, it follows immediately that $d = X_a(n)$ is Diophantine as well. By definition

$$d = X_a(n) \Leftrightarrow d^2 - (a^2-1)(Y_a(n))^2 = 1,$$

and the right-hand side is Diophantine.

□

2.4 Exponentiation, Binomial Coefficient and Factorial are Diophantine

We are now able to show that both exponentiation and the binomial coefficient are Diophantine. To do so, we use the properties of the Diophantine functions $X_a(n)$ and $Y_a(n)$ developed in the previous section.

Theorem 2.4.1. *The exponential relation $m = k^n$ is Diophantine.*

Proof. We can assume that $n \geq 1$ and $k \geq 2$. We will show that for $a \geq Y_k(n+1)$ we have

$$k^n = \mathsf{rem}(X_a(n) - (a-k)Y_a(n), 2ak - k^2 - 1).$$

Since the remainder function and both $X_a(n) - (a-k)Y_a(n)$ and $2ak - k^2 - 1$ are Diophantine, the exponential relation is Diophantine as well. For all $k \geq 2$, $k < (2k-1)$ and thus with (2.16) and the assumption that $a \geq Y_k(n+1)$ we have

$$k \leq k^n < (2k-1)^n \leq Y_k(n+1) \leq a$$

and thus $k+1 \leq a$. With this we have

$$a < ak < ak + k - 1 = ak + (k+1)k - k^2 - 1 \leq ak + ak - k^2 - 1 = 2ak - k^2 - 1.$$

Lemma 2.3.4 gives us the congruence

$$X_a(n) - (a-k)Y_a(n) \equiv k^n \mod (2ak - k^2 - 1),$$

and since $0 < k^n < a < (2ak - k^2 - 1)$, k^n has to be the remainder of $(2ak - k^2 - 1)$ divided by $X_a(n) - (a-k)Y_a(n)$. □

Similar to the Gödel function in 2.2, we introduce a code representing tuples of arbitrary length over $\mathbb{N}_0$ to show that the binomial coefficient is Diophantine.

Definition. *Let $(a_1, \dots, a_n) \in \mathbb{N}_0$. We call (a, b, c) the positional code of the tuple $(a_1, \dots, a_n)$, if*

$$(a_n a_{n-1} \dots a_1)_b = a$$

and $c = n$, that means $a_1, \dots, a_n$ are the digits in the b-ary representation of a of length n.

The b-ary representation of a number a is always the same, but to uniquely determine a tuple corresponding to a and b, the length of the tuple must be given. Otherwise, the corresponding tuple can be arbitrarily long with any amount of leading zeros. When asking for a specific element in the tuple, however, the length of the tuple can be omitted. Consider the function

$$\begin{aligned}\mathsf{Elem} : \mathbb{N}_0^3 &\to \mathbb{N}_0,\\ (a,b,d) &\mapsto a_d,\end{aligned}$$

where a_d is the d-th digit in the b-ary representation of a, i.e.

$$a = a_n b^{n-1} + \dots + a_{d+1}b^d + a_d b^{d-1} + a_{d-1}b^{d-2} + \dots + a_1 = Ab^d + a_d b^{d-1} + B,$$

for unique $A, B, a_i \in \mathbb{N}_0$ with $B < b^{d-1}$ and $a_i < b$ for all $i \in \{1, \dots, n\}$. With Theorem 2.4.1, it is easy to see that this function is Diophantine:

$$e = \mathsf{Elem}(a,b,d) \Leftrightarrow \exists x,y,z[(d = z+1) \wedge (a = xb^d + eb^z + y) \wedge (e < b) \wedge (y < b^x)].$$

Proposition 2.4.2. *The binomial coefficient relation $m = \binom{a}{b}$ is Diophantine.*

Proof. To prove this, we will use the b-ary representation of non-negative integers. First note that for large enough $d \in \mathbb{N}_0$, the code $((d+1)^n, d, n+1)$ stands for the $n+1$-tuple

$$\left(\binom{n}{0}, \binom{n}{1}, \dots, \binom{n}{n}\right).$$

This means that we can describe the binomial relation with the function Elem, which we have shown to be Diophantine. Indeed, we have

$$\begin{aligned}(2^n+2)^n &= ((2^n+1)+1)^n\\ &= \binom{n}{0}(2^n+1)^0 + \binom{n}{1}(2^n+1)^1 + \ldots + \binom{n}{m}(2^n+1)^m + \ldots \binom{n}{n}(2^n+1)^n,\end{aligned}$$

and since $2^n + 1 > \binom{n}{k}$ for all $0 \le k \le n$,

$$m = \binom{a}{b} \Leftrightarrow m = \mathsf{Elem}((2^n+2)^n, 2^n+1, m+1)$$

□

Lemma 2.4.3. *Let $k, n \in \mathbb{N}_0$ with $n > (2k)^{(k+1)}$. Then*

$$k! = \left\lfloor \frac{n^k}{\binom{n}{m}} \right\rfloor.$$

Proof. By the definition of the floor-function, it suffices to show that $k! \le n^k / \binom{n}{m} < k! + 1$. For the left-hand side, we have

$$k! < k! \frac{1}{(1-1/n)\dots(1-(k-1)/n)} = \frac{n^k}{\binom{n}{m}}.$$

For the right hand side, first note that

$$\frac{1}{(1-k/n)^k} = \left(1+\frac{k}{n}\sum_{i=0}^{\infty}\left(\frac{k}{n}\right)^i\right)^k < \left(1+\frac{k}{n}\sum_{i=0}^{\infty}\left(\frac{1}{2}\right)^i\right)^k = \left(1+\frac{2k}{n}\right)^k$$
$$= \sum_{j=0}^{k}\binom{k}{j}\left(\frac{2k}{n}\right)^j < 1+\frac{2k}{n}\sum_{j=0}^{k}\binom{k}{j} < 1+\frac{k2^{k+1}}{n}.$$

Therefore,

$$\frac{n^k}{\binom{n}{m}} = \frac{1}{(1-1/n)\dots(1-(k-1)/n)} < k!\frac{1}{(1-k/n)^k}$$
$$< k! + \frac{k!k2^{k+1}}{n} < k! + \frac{(2k)^{k+1}}{n} < k!+1.$$

□

Proposition 2.4.4. *The factorial relation $m = k!$ is Diophantine.*

Proof. According to the previous lemma, it sufficed to show that $\lfloor n^k/\binom{n}{m}\rfloor$ is Diophantine. This is true, since the floor of a fraction is Diophantine as

$$z = \lfloor x/y \rfloor \Leftrightarrow yz \le x \le y(z+1), \tag{2.24}$$

and as we have seen, both n^k and $\binom{n}{m}$ are Diophantine as well. □

2.5 D-Sets are Diophantine

D-sets are defined to be the closure of Diophantine sets with respect to finite unions, finite intersections, finite direct products, projections and the application of the bounded universal quantifier. As we have seen in 2.1.1, in order to show that the class of Diophantine sets equals the class of D-sets, it suffices to show that Diophantine sets are closed under the bounded universal quantifier. So for this section, fix a nonempty Diophantine set $D \subseteq \mathbb{N}_0^{n+1}$ and assume that $E \subseteq \mathbb{N}_0^{n+1}$ is the result of applying the bounded universal quantifier on D, i.e.

$$(x_1,\dots,x_n,y) \in E \Leftrightarrow (\forall k \in \{1,\dots,y\}\exists y_1,\dots,y_m \in \mathbb{N}_0)[f(x_1,\dots,x_n,k,y_1,\dots,y_m)=0],$$

where f is the Diophantine representation of D. We denote by $d = \deg f$ and by c the sum of the absolute values of the coefficients of f. Next we need to define the following sets. Let

$$X = (x_1,\dots,x_n,y,Y,N,K,Y_1,\dots,Y_m) \in \mathbb{N}_0^{n+m+4},$$

and define the sets $E_1, E_2, E_3, E_{3+i} \subseteq \mathbb{N}_0^{n+m+4}$ for $i \in \{1, \ldots, m\}$ by

$$X \in E_1 \Leftrightarrow N \geq c(x_1 \cdots x_n y Y)^d \text{ and } Y < \min_{i \in \{1,\ldots,m\}} Y_i \tag{2.25}$$

$$X \in E_2 \Leftrightarrow 1 + KN! = \prod_{k=1}^{y} (1 + kN!) \tag{2.26}$$

$$X \in E_3 \Leftrightarrow f(x_1, \ldots, x_n, K, Y_1, \ldots, Y_m) \equiv 0 \mod (1 + KN!) \tag{2.27}$$

$$X \in E_{3+i} \Leftrightarrow \prod_{j<Y} (Y_i - j) \equiv 0 \mod (1 + KN!). \tag{2.28}$$

Further we define E' as the projection of $\cap_{i=1}^{m+3} E_i$ to the first $n + 1$ coordinates.

Lemma 2.5.1. *Let E, E' be given as above. Then $E \subseteq E'$.*

Proof. Let $(x_1, \ldots, x_n, y) \in E$ and $y_{1,k}, \ldots, y_{m,k} \in \mathbb{N}_0$, $k \in \{1, \ldots, y\}$ such that for the Diophantine representation f of D we have $f(x_1, \ldots, x_n, k, y_{1,k}, \ldots, y_{m,k}) = 0$. Set

$$Y = \max \left(\{y\} \cup \{y_{i,k} \mid 1 \leq i \leq m, 1 \leq k \leq y\} \right).$$

Recall the function gd. For any tuple $a_1, \ldots, a_n$ one can find u, t such that $\text{gd}(u, k, t) = a_k$ for all $k \in \{1, \ldots, n\}$. It is easy to show that for a given t, one can find arbitrarily large $t' \geq t$ such that there is an u' with the same property, i.e. $\text{gd}(u', k, t') = a_k$. Assume now that we have some N, Y_i such that

$$\text{gd}(Y_i, k, N!) = \text{rem}(1 + kN!, Y_i) = y_{i,k}$$

for all $i \in \{1, \ldots, m\}$ and $k \in \{1, \ldots, n\}$. Then

$$Y_i + (1 + kN!) = q(1 + kN!) + y_{i,k} + (1 + kN!) = (q + 1)(1 + kN!) + y_{i,k},$$

thus for given N we can choose Y_i arbitrarily large by subsequently adding the term $(1 + kN!)$. This means that we can choose N, Y_i such that (2.25) is satisfied. For our given y and N, choose K such that (2.26) is fulfilled. We still need to show that

$$(x_1, \ldots, x_n, y, Y, N, K, Y_1, \ldots, Y_m) \in \bigcap_{i=3}^{m+3} E_i.$$

By definition of the function gd, we have $(1 + kN!) | (Y_i - y_{i,k})$ and with $y_{i,k} \leq Y$ we have $(1 + kN!) | \prod_{j<Y} (Y_i - y_{i,k})$. For any $1 \leq k_1 < k_2 \leq y$ we have $\gcd(1 + k_1 N!, 1 + k_2 N!) = 1$ and thus E_{3+1} for all $i \in \{1, \ldots, m\}$. To show that E_3 holds, first note that since $(1 + KN!) \equiv 0 \equiv (1 + kN!) \mod 1 + kN!$ by E_1 and $\gcd(1 + kN!, N!) = 1$, we have $k \equiv K \mod 1 + kN!$. Moreover, we have $\text{rem}(1 + kN!, Y_i) = y_{i,k}$ and thus $Y_i \equiv y_{i,k} \mod 1 + kN!$. This means that

$$f(x_1, \ldots, x_n, K, Y_1, \ldots, Y_m) \equiv f(x_1, \ldots, x_n, k, y_{1,k}, \ldots, y_{m,k}) \equiv 0 \mod 1 + kN!$$

for all $k \in \{1, \ldots, y\}$ and again, since the $(1 + kN!)$ are pairwise coprime, E_3 follows. □

Lemma 2.5.2. *Let E, E' be given as above. Then $E' \subseteq E$.*

Proof. Let $(x_1,\dots,x_n,y,Y,N,K,Y_1,\dots,Y_m) \in \bigcap_{i=3}^{m+3} E_i$ such that $(x_1,\dots,x_n,y) \in E'$. We need to show that there are $y_{1,k},\dots,y_{m,k}$ for each $k \in \{1,\dots,y\}$ such that

$$f(x_1,\dots,x_n,y,y_{1,k},\dots,y_{m,k}) = 0. \tag{2.29}$$

We claim that the choice $y_{i,k} = \mathrm{rem}(Y_i, p_k)$ fulfills this requirements, where p_j is any fixed prime divisor of $1+kN!$. By E_2 and E_{3+i} we have

$$p_k|(1+kN!)|(1+KN!)|\prod_{j<Y} Y_i + j,$$

for all $i \in \{1,\dots,m\}$ and thus $p_k|(Y_i - j)$ for some $j < Y$. Since $y_{i,k}$ is defined to be the remainder of Y_i divided by p_k, it follows that $y_{i,k} < Y$. Since f is a polynomial, we have $f(x_1,\dots,x_n,k,y_{1,k},\dots,x_{m,k}) \le c(x_1\cdots x_n kY)^d$ and by E_1 this is bounded from above by N. By definition of the p_k, we have $p_k > N$ and thus

$$f(x_1,\dots,x_n,k,y_{1,k},\dots,y_{m,k}) < p_k. \tag{2.30}$$

Both congruences E_3 and $k \equiv K \mod 1+kN!$ also hold modulo p_k, and with $y_{i,k} \equiv Y_i \mod p_k$ we have that

$$f(x_1,\dots,x_n,k,y_{1,k},\dots,y_{m,k}) = f(x_1,\dots,x_n,K,Y_1,\dots,Y_m) \equiv 0 \mod p_k,$$

so with (2.30) we have (2.29) and thus the claim follows. □

Theorem 2.5.3. *The class of Diophantine sets equals the class of D-Sets.*

Proof. By the definition of D-sets, every Diophantine set is a D-set. As we have established before, to show that every D-set is Diophantine, it suffices to show that the class of Diophantine sets is closed under the bounded universal quantifier. With the two previous lemmas, the set E, which we obtain by applying the quantifier is equal to E'. The sets E_1, E_2, E_3 and E_{3+i}, $i \in \{1,\dots,m\}$ are given by the equations (2.25)-(2.28). Since both exponentiation and the factorial function are Diophantine, these sets are Diophantine as well, and as E' is a projection of the intersection of E_1, E_2, E_3 and E_{3+i}, it follows that E is Diophantine as well. □

2.6 Hilbert's Tenth Problem is Unsolvable

Let $D \in \mathbb{Z}[X_1,\dots,X_n]$ and assume that we are interested in the positive integer solutions of

$$D(X_1,\dots,X_n) = 0. \tag{2.31}$$

Next consider the system of equations

$$\begin{aligned} D(X_1,\dots,X_n) &= 0, \\ X_1 &= Y_{1,1}^2 + Y_{1,2}^2 + Y_{1,3}^2 + Y_{1,4}^2, \\ &\vdots \\ X_n &= Y_{n,1}^2 + Y_{n,2}^2 + Y_{n,3}^2 + Y_{n,4}^2. \end{aligned} \tag{2.32}$$

Since every natural number can be written as the sum of four squares, every solution of (2.32) is a solution to (2.31). This means that we can reduce Hilbert's tenth problem from finding solutions over the integers to finding solutions over the non-negative integers.

Theorem 2.6.1. *Assume that Hilbert's tenth problem is solvable over the positive integers. Then every Diophantine set is recursive.*

Proof. Let D be a Diophantine set, and let $f \in \mathbb{Z}[X_1, \dots, X_{n+m}]$ be its Diophantine representation, i.e.

$$D = \{(x_1, \dots, x_n) \in \mathbb{N}_0^n \mid \exists y_1, \dots, y_m \in \mathbb{N}_0 \text{ with } f(x_1, \dots, x_n, y_1, \dots, y_m) = 0\}.$$

Let $(x_1, \dots, x_n) \in \mathbb{N}_0^n$. Then, since Hilbert's tenth problem is solvable over $\mathbb{N}_0$, there is an algorithm that decides in finitely many steps whether there are some $y_1, \dots, y_m \in \mathbb{N}_0$ such that

$$D(x_1, \dots, x_n, y_1, \dots, y_m) = 0. \tag{2.33}$$

By the Church-Turing-Thesis, there is some Turing machine M such that

$$M((x_1, \dots, x_n)) = \begin{cases} 1 & : \exists y_1, \dots, y_m \in \mathbb{N}_0 \text{ satisfying (2.33)} \\ 0 & : \text{ otherwise,} \end{cases}$$

meaning that M decides D and thus D is recursive.

□

We can now use the fact that D-sets, Diophantine sets and recursively enumerable sets are the same to show that Hilbert's tenth problem has no solution.

Corollary 2.6.2. *Hilbert's tenth problem over the integers is unsolvable.*

Proof. Assume for the sake of a contradiction that Hilbert's tenth problem over the integers is solvable. Then, as we have deduced above, Hilbert's Tenth problem over the non-negative integers is solvable. Let $\mathcal{D}$ be the class of all Diophantine sets, $\mathcal{R}$ the class of all recursive languages and $\mathcal{R}_\mathcal{E}$ the class of all recursively enumerable languages. Then by Theorem 2.6.1 we have $\mathcal{D} \subset \mathcal{R}$, but since we have proved that the classes of D-sets, $\mathcal{R}_\mathcal{E}$ and $\mathcal{D}$ coincide, we have $\mathcal{R}_\mathcal{E} \subseteq \mathcal{R}$, contradicting 2.1.3. □

3 Number of Solutions of Equations over Finite Fields

The key exchange protocol that we are going to present in Chapter 5 can be implemented either over the integers or over a finite field. For the case of finite fields, we need to establish a bound on the number of solutions over $\mathbb{F}_q$ for certain polynomials. To do so, some notions from Algebraic Geometry are introduced.

3.1 Varieties over Finite Fields

In the following, let K always denote an algebraically closed field.

3.1.1 Definitions and Notation

Definition. *Let K be an algebraically closed field, and denote by $\mathbb{A}^n = K^n$ the affine n-space. For polynomials $f_1 \dots, f_m \in K[X_1, \dots, X_n]$ we define the affine algebraic set $V(f_1, \dots f_m) \subseteq \mathbb{A}^n$ as*

$$V(f_1, \dots f_m) = \{\mathbf{x} \in \mathbb{A}^n \mid f_1(\mathbf{x}) = \dots = f_m(\mathbf{x}) = 0\}.$$

We say that the polynomials in the above equation define the affine algebraic set $V(f_1, \dots, f_m)$. The set of such polynomial is not unique in general. Therefore, for any algebraic set $V \subseteq \mathbb{A}^n$ and any $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ with $V = V(f_1, \dots, f_m)$, we say that $f_1, \dots, f_m$ are the defining polynomials of V.
It is easy to show that for a set S of polynomials, we have $V(S) = V((S))$, where (S) is the ideal generated by S. In fact, for any affine algebraic set $X \subset A^n$, we define the ideal of X to be the ideal $I(X) \trianglelefteq K[X_1, \dots, X_n]$ with $V(I(X)) = X$.

Moreover, for any ideals $I, J \trianglelefteq K[X_1, \dots, X_n]$ we have $V(I) \cup V(J) = V(IJ)$ and $V(I) \cap V(J) = V(I + J)$. Therefore, we can identify affine algebraic sets as the closed sets of a topology, which we call the Zariski topology. This allows us to define irreducible algebraic sets via topology.

Definition. *Let X be a topological space. Then X is said to be reducible, if $X = X_1 \cup X_2$, where $X_1, X_2 \subsetneq X$ are closed sets. Otherwise, we call X irreducible.*

An irreducible affine algebraic set is called an affine variety. Note that an affine algebraic set $X \subset \mathbb{A}^n$ is an affine variety if and only if $I(X) \trianglelefteq K[X_1, \dots, X_n]$ is prime.

By Hilbert's Basis Theorem, $K[X_1, \dots, X_n]$ is a Noetherian ring and thus every affine algebraic set is a Noetherian topological space, i.e. every descending chain of closed sets is stationary. Similar to prime decomposition in a unique factorization domain, we can factor any algebraic set into so called irreducible components.

Proposition 3.1.1. *Every Noetherian topological space X can be written as a finite union*

$$X = X_1 \cup \cdots \cup X_m,$$

where $X_1, \ldots, X_m$ are irreducible closed subsets of X. If $X_i \not\subset X_j$ for all $i \neq j$, then the union is unique up to permutation.

Proof. First we show existence. We assume that X can not be written as a union as given above, so X is not irreducible and thus we can assume that $X = X_1 \cup X_2$ for $X_1, X_2 \subsetneq X$. This means that, without loss of generality, X_1 can not be written as a union as given above. Repeating this argument r times leads to a descending chain $X_r \subsetneq \ldots \subsetneq X_1 \subsetneq X$, which can not be arbitrarily long since X is a Noetherian topological space. To show uniqueness, assume that $X = X_1 \cup \ldots \cup X_m = Y_1 \cup \ldots Y_k$. This means that $X_1 \subseteq Y_1 \cup \ldots \cup Y_k$ and hence $X_1 = (Y_1 \cap X_1) \cup \ldots (Y_k \cap X_1)$. Since X_1 is irreducible, we have $X_1 = Y_1 \cap X_1$ without loss of generality. This means that $X_2 \cup \ldots \cup X_m = Y_2 \cup \ldots Y_k$, and we are done by induction. □

A crucial feature of every algebraic set is its dimension. This can again be defined by the means of topology.

Definition. *Let X be an irreducible topological space, and assume that*

$$\emptyset \neq X_1 \subsetneq X_2 \subsetneq \cdots \subsetneq X_{n-1} \subsetneq X_n = X$$

is the longest chain of irreducible closed subsets of X. Then we define n to be the dimension of X.

This means that we can define the dimension of an affine variety V as the longest chain of subvarieties. For an affine algebraic set with irreducible components $V_1, \ldots, V_k$, we define the dimension as the maximum of the dimensions of $V_1, \ldots, V_k$. Note that this is a valid definition, since the number of irreducible components is finite and the decomposition is unique by Proposition 3.1.1. Moreover, the dimension of an affine variety is finite by the fact that $K[X_1, \ldots, X_n]$ is Noetherian.

It is an immediate consequence of this definition, that for affine varieties X and Y with $X \subsetneq Y$ we have $\dim X < \dim Y$. One can show that for any irreducible $f \in K[X_1, \ldots, X_n] \setminus K$, we have $\dim V(f) = n - 1$. We call such an affine variety a hypersurface. Moreover, if $f_1, \ldots, f_d \in K[X_1, \ldots, X_n]$ such that the f_i are pairwise coprime, then $\dim V(f_1, \ldots, f_d) = n - d$.

In 3.2 we will make an estimate on the number of points of algebraic curves over a finite field. In higher dimensions, an algebraic curve is defined as follows:

Definition. *Let $C \subset \mathbb{A}^n$. Then C is called an algebraic curve, if it is an affine variety of dimension 1.*

We also introduce the notion of the degree.

Definition. *Let $V \subset \mathbb{A}^n$ be an affine variety. We define the degree of V as*

$$\deg V = \max\{\#(V \cap L) \mid L \subset \mathbb{A}^n \text{ linear with } \operatorname{codim}(L) = \dim(V) \text{ and } \#(V \cap L) < \infty\}.$$

In general, let $W \subset \mathbb{A}^n$ be an affine algebraic set, and $C_1, \ldots, C_h$ its irreducible components. Then

$$\deg W = \sum_{i=1}^{h} \deg C_i.$$

Note that, by definition, it follows that for a zero-dimensional affine variety, the degree of the affine variety equals the number of its points. Moreover, $\deg \mathbb{A}^n = \#(\mathbb{A}^n \cap \{0\}) = 1$. Also note that for any affine varieties $U, V \subseteq \mathbb{A}^n$, we have $\deg U \leq \deg V$ if $U \subseteq V$ and $\deg(A \cup B) \leq \deg A + \deg B$.

We call an affine variety with dimension $n-1$ a hypersurface. An absolutely irreducible hypersurface has an absolutely irreducible polynomial as its defining polynomial, and the degree of a hypersurface can be seen immediately.

Proposition 3.1.2. *Let $H \subset \mathbb{A}^n$ be a hypersurface with defining polynomial f. Then the degree of H equals the degree of f.*

Proof. Let $\deg f = d$. As every hypersurface has dimension $n-1$, we need to intersect it with a linear subspace L of dimension 1. After a change of coordinates, we may assume that L is given by the equation $X_2 = X_3 = \cdots X_n = 0$. This means that for a point $P \in \mathbb{A}^n$, we have $P \in H \cap L$ if and only if $P = (k, 0, \cdots, 0)$ for some $k \in K$ and $f(P) = 0$. This means that P needs to be a zero of the polynomial $f(X, 0, \ldots, 0) \in K[X]$, and since K is algebraically closed, there are exactly d such points. □

We will also need to introduce the notion of affine linear varieties.

Definition. *Let K be a field and $\mathbb{A}^n = K^n$ the affine n-space with underlying vector space $\mathbb{V}$. We say that L is an affine linear variety, if there is some linear subspace $S \subseteq \mathbb{V}$ and some $a \in \mathbb{A}^n$ such that $L = a + S$. We further define the dimension $\dim L = \dim_K S$, where $\dim_K S$ is the dimension of the K-vector space S..*

Note that the dimension of an affine linear variety is well defined. If we have $L = a + S$, then the subspace S is unique, whereas we can choose any $s \in S$ and have $L = (a + s) + S$.

Definition. *Let L_1, L_2 be affine linear varieties. Then we say that L_1 and L_2 are parallel, if they have the same defining linear subspace S, i.e. $L_1 = a_1 + S$ and $L_1 = a_2 + S$ for some $a_1, a_2 \in \mathbb{A}^n$ and some linear subspace S.*

3.1.2 Basic Inequalities

In this section we develop three basic inequalities, which will be needed frequently later on. To do so, we will make use of the general version of Bezout's inequality, as given in [12]. Moreover, we will follow [5] to prove the important Theorem 3.3.11. As we will mostly work with affine varieties over $\mathbb{A}^n = \bar{\mathbb{F}}_q{}^n$ which are defined by polynomials over $\mathbb{F}_q$, we will call such varieties $\mathbb{F}_q$-varieties.

Theorem 3.1.3 (Bezout's inequality)**.** *Let $V, W \subset \mathbb{A}^n$ be affine varieties. Then*

$$\deg (V \cap W) \leq \deg V \deg W.$$

The next lemma is given in [17].

Lemma 3.1.4. *Let $V_i \subset \mathbb{A}^n$, $i \in \{1, \dots, n\}$ be affine subvarieties. Then*

$$\deg\left(\bigcap_{i=1}^{n} V_i\right) \leq \deg V_1 (\max_{i>1} \deg V_i)^{\dim V_1}$$

Proof. We prove this by induction on n. For $n = 1$, set $V_2 = \mathbb{A}^n$. Then

$$\deg V_1 (\max_{i>1} \deg V_i)^{\dim V_1} = \deg V_1 (\deg \mathbb{A}^n)^{\dim V_1} = \deg V_1.$$

So assume that $n > 1$ and let $V_1 = C_1 \cup \cdots \cup C_h$ be the decomposition of V_1 into irreducible components. For some fixed $j \in \{1, \dots, h\}$ we want to show that

$$\deg\left(C_j \cap \bigcap_{i=2}^{n+1} V_i\right) \leq \deg C_j (\max_{i>1} \deg V_i)^{\dim C_j}. \tag{3.1}$$

For the case $C_j \subseteq V_2$ we are done by the induction hypothesis, so assume that $C_j \not\subseteq V_2$. Then, since C_j is irreducible, we have $\dim (C_j \cap V_2) < \dim C_j$. Again, by the induction hypothesis we have

$$\deg\left(C_j \cap \bigcap_{i=2}^{n+1} V_i\right) = \deg\left((C_j \cap V_2) \cap \bigcap_{i=3}^{n+1} V_i\right) \leq \deg (C_j \cap V_2) (\max_{i>2} \deg V_i)^{\dim (C_j \cap V_2)}.$$

With the Bezout inequality we have

$$\begin{aligned} \deg (C_j \cap V_2) (\max_{i>2} \deg V_i)^{\dim (C_j \cap V_2)} &\leq \deg (C_j \cap V_2) (\max_{i>2} \deg V_i)^{\dim C_j - 1} \\ &\leq \deg C_j (\max_{i>1} \deg V_i)^{\dim C_j} \end{aligned}$$

and hence 3.1 follows. The dimensions of the C_i are bounded by $\dim V_1$, and therefore

$$\begin{aligned} \deg\left(\bigcap_{i=1}^{n+1} V_i\right) &= \deg\left(V_1 \cap \bigcap_{i=2}^{n+1} V_i\right) = \deg\left(\left(C_1 \cap \bigcap_{i=2}^{n+1} V_i\right) \cup \cdots \cup \left(C_h \cap \bigcap_{i=2}^{n+1} V_i\right)\right) \\ &\leq \sum_{j=1}^{h} \deg\left(C_j \cap \bigcap_{i=2}^{n+1} V_i\right) \leq \left(\sum_{j=1}^{h} \deg C_j\right) (\max_{i>1} \deg V_i)^{\dim V_1}. \end{aligned}$$

□

The next lemma gives the first estimate on the number of $\mathbb{F}_q$-points of an affine variety.

Lemma 3.1.5. *Let $V \subset \mathbb{A}^n$ be an $\mathbb{F}_q$-variety with $\dim V = r \geq 0$ and $\deg V = \delta > 0$. Then*

$$\#(V \cap \mathbb{F}_q^n) \leq \delta q^r.$$

Proof. For all $x \in \mathbb{F}_q$ and $i \in \{1, \ldots, n\}$, we have $f_i(x) = 0$ for $f_i = X_i^q - X_i \in \mathbb{F}_q[X_1, \ldots, X_n]$. Let

$$W_i = \{(x_1, \ldots, x_n) \in \mathbb{A}^n \mid f_i(X_1, \ldots, X_n)\}.$$

Then we can write

$$V \cap \mathbb{F}_q^n = V \cap W_1 \cap \cdots \cap W_n$$

and thus by Lemma 3.1.4 and since $V \cap \mathbb{F}_q^n$ is zero-dimensional, we have

$$\#(V \cap \mathbb{F}_q^n) = \deg\left(V \cap W_1 \cap \cdots \cap W_n\right) \leq \deg V(\max_{i>1} \deg W_i)^r = \delta q^r.$$

□

Lemma 3.1.6. *Let $\delta \in \mathbb{N}$ and $f_1, \ldots, f_m \in \mathbb{F}_q[X_1, \ldots, X_n]$, $m \geq 2$ such that $\deg f_i \leq \delta$ and $\gcd f_1, \ldots, f_m = 1$ over $\bar{\mathbb{F}}_q[X_1, \ldots, X_n]$. Further let $V \subset \mathbb{A}^n$ be the variety defined by $f_1, \ldots, f_m$. Then*

$$|V \cap \mathbb{F}_q^n| \leq \delta^2 q^{n-2}.$$

Proof. We prove this by induction on m. Assume that $m = 2$. Then $\gcd\left(f_1, f_2\right) = 1$ and thus $V(f_1, f_2) = n - 2$. Moreover, by Bezout's inequality we have

$$\deg V(f_1, f_2) = \deg\left(V(f_1) \cap V(f_2)\right) \leq \deg f_1 \deg f_2 \leq \delta^2,$$

hence by Lemma 3.1.5 we deduce that $|V(f_1, f_2) \cap \mathbb{F}_q^n| \leq \delta^2 q^{n-2}$. Assume now that $m \geq 3$ and consider the polynomial $v = \gcd\left(f_1, \ldots, f_{m-1}\right)$ and let $d = \deg v$. Moreover, we define the polynomials $w_i \in \bar{\mathbb{F}}_q[X_1, \ldots, X_n]$ with $v = f_i w_i$ for all $i \in \{1, \ldots, m-1\}$. Then, by the definition of the greatest common divisor, $\gcd\left(w_1, \ldots, w_{m-1}\right) = 1$.
Assume that for some $\mathbf{x} \in \mathbb{F}_q^n$ we have $\mathbf{x} \in V$. Then either $v(\mathbf{x}) = 0 = f_m(\mathbf{x})$ or $w_i(\mathbf{x}) = 0 = f_m(\mathbf{x})$ for all $i \in \{1, \ldots, m-1\}$. For the first case, $\mathbf{x} \in V(v, f_m)$. Again by Bezout's inequality we have $\deg V(v, f_m) \leq d\delta$ and thus $|V(v, f_m) \cap \mathbb{F}_q^n| \leq d\delta q^{n-2}$. For the case $w_i(\mathbf{x}) = 0 = f_m(\mathbf{x})$ for all possible i, we use the fact that $\deg w_i \leq \delta - d$ and the induction hypothesis to obtain $|V(w_1, \ldots, w_{m-1}, f_m) \cap \mathbb{F}_q^n| \leq (\delta - d)^2 q^{n-2}$. Therefore

$$\begin{aligned} |V \cap \mathbb{F}_q^n| &\leq |V(v, f_m) \cap \mathbb{F}_q^n| + |V(w_1, \ldots, w_{m-1}, f_m) \cap \mathbb{F}_q^n| \\ &\leq d\delta q^{n-1} + (\delta - d)^2 q^{n-2} \leq \delta^2 q^{n-2} \end{aligned}$$

since $0 \leq d \leq \delta$. □

3.1.3 The Projective Space

Definition. *Let K be a field. The projective n space $\mathbb{P}^n$ is the set of all linear subspaces of the K-vector space K^{n+1} of dimension 1.*

Let the relation $\sim \in K^{n+1} \times K^{n+1}$ be defined as

$$a \sim b \text{ if and only if } \exists \lambda \in K : a = \lambda b$$

for $a, b \in K^{n+1}$. This is an equivalence relation, and since one-dimensional subspaces of K^{n+1} are spanned by single vectors, we can write

$$\mathbb{P}^n = (K^{n+1} \setminus \{\mathbf{0}\}) / \sim .$$

We will denote an equivalence class of $\mathbb{P}^n$ by $(a_0 : a_1 : \ldots : a_n)$ and call this a point in $\mathbb{P}^n$. Similar to affine spaces, we define a projective algebraic set $V \subset \mathbb{P}^n$ as the zero-set of homogeneous polynomials, i.e. V is a projective algebraic set if there is a subset $M \subset K[X_0, X_1, \ldots, X_n]$ of homogeneous polynomials with

$$V = \{(a_0 : \ldots : a_n) \in \mathbb{P}^n \mid f(a_0, \ldots, a_n) = 0\}.$$

Note that this definition makes sense for homogeneous polynomials: If $\deg f = d$, then $f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d f(a_0, \ldots, a_n)$ and therefore $f(a_0, \ldots, a_n) = 0$ if and only if $f(\lambda a_0, \ldots, \lambda a_n) = 0$ for any $\lambda \in K$.

The Zariski topology on $\mathbb{P}^n$ is defined to be the topology whose closed sets are projective algebraic sets. Affine varieties and the dimension of affine algebraic sets are defined via topology, and we define projective varieties and the dimension of projective algebraic sets analogously.

The notion of an algebraic curve was introduced in section 3.1.1. We will only need affine and projective algebraic curves in the plane.

Definition. *Let $C \subset \mathbb{P}^2$. Then C is a plane projective curve, if there is a homogeneous $f \in K[X, Y, Z]$ such that $C = V(f)$. If $C' \subset \mathbb{A}^2$, then C' is a plane affine curve if there is some $f' \in K[X, Y]$ such that $C = V(f')$.*

Note that every plane affine and projective curve is also an algebraic curve. We can classify curves in smooth and singular curves. The following definition is only given for plane projective curves, the definition for affine curves is analogously. We say that a plane curve is (absolutely) irreducible, if its defining polynomial is (absolutely) irreducible.

Definition. *Let $C \subset \mathbb{P}^2$ be a plane projective curve and $F \in K[X, Y, Z]$ homogeneous such that $C = V(F)$. Let $P = (x : y : 1)$ be a point on C and let $f = F(X, Y, 1) \in K[X, Y]$. Further let*

$$f = \sum_{i,j \geq 0} c_{i,j} (X - x)^i (Y - y)^j, \quad c_{i,j} \in K$$

be the Taylor expansion of f at the point (x, y). Then

$$\mathsf{ord}_P(C) = \min\{i + j | c_{i,j} \neq 0\}$$

is the order of the point P of C. C is called singular at the point P, if $\operatorname{ord}_P(C) > 1$ *and regular otherwise. If there exists a point P of C such that P is singular, then C is called singular, and C is called smooth otherwise.*

It is easy to show that there are only finitely many singular points for a given singular plane curve.

Definition. *Let $f \in K[X_1, \dots, X_n]$ be a non-homogeneous polynomial with* $\deg f = d$. *Then*

$$f^h = X_0^d f(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}) \in K[X_0, X_1, \dots, X_n]$$

is the homogenization of f.
Let $V \subset \mathbb{A}^n$ be an affine variety with a subset of polynomials $F \subset K[X_1, \dots, X_n]$ defining the variety, i.e. $V(F) = V$. Then the projective closure of V is the projective variety

$$V' = \{P \in \mathbb{P}^n \mid \forall f \in F : f^h(P) = 0\}.$$

It follows from the definition that for a polynomial f in n variables of degree d, the homogenization f^h is a polynomial in $n+1$ variables of degree d. Moreover, irreducibility is invariant under homogenization:

Proposition 3.1.7. *Let $f \in K[X_1, \dots, X_n]$ be irreducible. Then its homogenization $f^h \in K[X_0, X_1, \dots, X_n]$ is irreducible.*

Proof. Let $d = \deg f = \deg f^h$ and assume that f^h factors into $f^h = pq$. Assume that p is not homogeneous. Then p has a term t with $\deg t < \deg p$, meaning that $\deg tq < \deg p + \deg q = \deg f^h$, which is a contradiction since the term with the highest degree of tq appears in f^h. Therefore we can assume that p and q are homogeneous. Thus

$$f = f^h(1, X_1, \dots, X_n) = p(1, X_1, \dots, X_n)q(1, X_1, \dots, X_n),$$

so, without loss of generality, $p(1, X_1, \dots, X_n)$ is a unit. This is only possible if $p = cX_0^m$ for some $c \in K$ and $m \in \mathbb{N}$, hence $X_0 | f^h$, which is not possible by the construction of the homogenization. It follows that f^h is irreducible. □

3.1.4 The Non-singular Model of a Curve

Definition. *Let X be a topological space. A presheaf $\mathcal{F}$ of rings on X consists of the following:*

- *For every open $U \subset X$ a ring $\mathcal{F}(U)$*
- *For all pairs U, V with $U \subset V \subset X$ a map $\rho_{U,V} : \mathcal{F}(U) \to \mathcal{F}(V)$*

Moreover $\rho_{U,V}$ needs to satisfy the following:

- *$\rho_{U,U}$ is the identity map for all $U \subset X$*
- *For any $U \subset V \subset W$ we have $\rho_{V,U} \circ \rho_{W,V} = \rho_{W,U}$.*

A presheaf $\mathcal{F}$ is called a sheaf, if it has the subsequent property:

- *Let $U \subset X$ be open with an open cover $U \subset \bigcup_{i\in I} U_i$ such that for all $s_i \in \mathcal{F}(U_i)$ and $s_j \in \mathcal{F}(U_j)$, $i, j \in I$, we have $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$. Then there is a unique $s \in \mathcal{F}(U)$ such that $s|_{U_i} = s_i$ for all $i \in I$.*

Note that a presheaf is in fact a functor $\mathcal{F}$ from topological spaces to sets. Moreover, instead of rings, we can define a presheaf with categories. In the following, we will usually take the ring of K-valued functions as the underlying ring for sheaves, i.e. for every open U we have $\mathcal{F}(U) : U \to K$. We will denote such sheaves as sheaves of K-valued functions. We will also denote pairs $(X, \mathcal{O}_X)$ as ringed spaces, if X is a topological space and $\mathcal{O}_X$ is a sheaf of rings on X.

Definition. *Let $(X, \mathcal{O}_X)$, $(Y, \mathcal{O}_Y)$ be ringed spaces where $\mathcal{O}_X$ and $\mathcal{O}_Y$ are sheaves of K-valued functions, and let $f : X \to Y$ be a function. For any open set $U \subset Y$ and any function $\varphi : U \to K$ we denote by $f^*\varphi$ the composition $\varphi \circ f : f^{-1}(U) \to K$. Then f is called a morphism, if*

- *f is continuous and*
- *for every open $U \subset Y$ we have $f^*\mathcal{O}_Y(U) \subset \mathcal{O}_X(f^{-1}(U))$.*

We can extend the definition of affine varieties to ringed spaces.

Definition. *Let $(X, \mathcal{O}_X)$ be a ringed space. Then $(X, \mathcal{O}_X)$ is called an affine variety, if*

- *X is irreducible*
- *$\mathcal{O}_X$ is a sheaf of K-valued functions*
- *X is isomorphic to an irreducible topological space in the Zariski topology.*

Definition. *Let $(X, \mathcal{O}_X)$ be a ringed space. Then $(X, \mathcal{O}_X)$ is called a prevariety, if*

- *X is irreducible*
- *$\mathcal{O}_X$ is a sheaf of K-valued functions*
- *There exists a finite open cover $X \subset \bigcup_{i\in I} U_i$*

such that $(U_i, \mathcal{O}_X|_{U_i})$ is an affine variety for all $i \in I$.

Every affine variety is a prevariety by the trivial finite open cover $X \subset X$. We can usually write X for a prevariety and affine varietiy instead of $(X, \mathcal{O}_X)$, if we omit the structure of $\mathcal{O}_X$.

Definition. *Let X be a prevariety. Then X is a variety, if for every prevariety Y and all morphisms $f_1, f_2 : Y \to X$, the set $\{P \in Y \mid f_1(P) = f_2(P)\}$ is closed in Y.*

Now we are able to introduce the birational map.

Definition. *Let X and Y be varieties. A rational map from X to Y, denoted by $f : X \dashrightarrow Y$ is a morphism $f : U \to Y$, where $\emptyset \neq U \subset X$ is open. A rational map f is called birational, if there is some rational map $g : Y \dashrightarrow X$ with $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$.*

By definition, if there is a birational map $f : X \dashrightarrow Y$, then there are nonempty open subsets $U \subset X$ and $V \subset Y$ such that $U \simeq V$.

It is often necessary to work with a non-singular algebraic curve. To do so, it is possible to construct a curve which is birationally equivalent to a given one, but where the singularities are resolved. The following Theorem is given in [11].

Theorem 3.1.8. *Let C be a projective curve. Then there exists a non-singular projective curve X and a birational map $f : X \dashrightarrow C$ which is onto. Moreover, if X' is a non-singular curve with birational map $f' : X' \dashrightarrow C$, then there is a unique isomorphism $g : X \to X'$ such that $f' \circ g = f$.*

A birational map f is onto in the usual sense: For every point $P \in C$ there is some $P' \in X$ such that $f(P') = P$. For any plane projective curve, we will denote the non-singular curve X from the above theorem as the non-singular model of C, which is unique up to isomorphism. For a plane affine curve C', the non-singular model is the non-singular model of the projective closure of C'. Let now C be a plane projective curve with non-singular model X and birational map $f : X \dashrightarrow C$. One can show that for a non-singular point $P \in C$, there is a unique $P' \in X$ such that $f(P') = P$. Moreover, if P is singular, there are finitely many such points $P' \in X$. It can also be shown that for an irreducible f defining C, the polynomial f' defining its non-singular model X is also irreducible.

3.2 The Weil Bound for Plane Affine Curves

In this section, we will assume that all given curves are irreducible.

3.2.1 The Genus of a Curve

Definition. *Let C be a smooth projective curve. A divisor on C is a formal sum $D = \sum_{P \in C} n_P P$, where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many P.*

Denote the set of all divisors on C by $\mathrm{Div}(C)$. We define the degree of a divisor $D = \sum n_P P$ to be $\mathrm{deg} D = \sum n_P$. Let $C \in \mathbb{P}^n$ be a smooth projective curve and denote by $k'(C)$ the quotient field of the domain $K[X_0, \ldots, X_n]/I(C)$. We define the function field of C by

$$k(C) = \{f \in k'(C) \mid \exists g, h \in K[X_0, \ldots, X_n]/I(C) : \\ g, h \text{ homogeneous}, \deg g = \deg h \text{ and } f = \frac{g}{h}\}.$$

For a Divisor $D = \sum n_P P$, the vector space of multiples of $-D$ is defined to be

$$\mathcal{L}(D) = \{f \in k(C) \mid \forall P \in C : \mathrm{ord}_P(f) \geq -n_P\},$$

and the dimension of D is defined to be $\dim D = \dim_K \mathcal{L}(D)$, where $\dim_K$ denotes the dimension of a K-vector space.

Definition. *Let C be a smooth projective curve. We define the genus g of C by*

$$g = \sup\{\deg D - \dim D + 1 \mid D \in \mathrm{Div}(C)\}.$$

It can be shown that the genus is always finite. The genus of a singular projective curve is defined as the genus of its non-singular model, and the genus of an affine curve is the genus of its projective closure.

3.2.2 The Weil Bound

A famous estimate on the number of $\mathbb{F}_q$ points of an absolutely irreducible smooth projective curve is given by the Hasse-Weil bound, which was proved in [41]. It uses the genus of the curve for an upper bound.

Theorem 3.2.1 (Hasse-Weil bound)**.** *Let C be a smooth, absolutely irreducible projective curve defined over $\mathbb{F}_q$ of genus g, and denote by N the number of $\mathbb{F}_q$-points of C. Then*

$$|N - q - 1| \leq 2g\sqrt{q}.$$

We want to use the Hasse-Weil bound to estimate the number of points of a plane affine curve. In addition to that, we want to eliminate the genus from the inequality. To do so, we will use the following upper bound on the genus of a plane projective curve, which is given in [11].

Proposition 3.2.2. *Let C be a plane projective curve and $f \in K[X, Y, Z]$ with $C = V(f)$ and $\deg f = d$. Further let g be the genus of C. Then*

$$g \leq \frac{(d-1)(d-2)}{2} - \sum_{P \in C} \frac{\mathrm{ord}_P(C)(\mathrm{ord}_P(C) - 1)}{2}. \tag{3.2}$$

Note that the right-hand side of the inequality is finite, since there are only finitely many singular points. We are therefore able to give a version of the Hasse-Weil bound for (possibly singular) plane absolutely irreducible affine curves.

Corollary 3.2.3. *Let C be a plane absolutely irreducible affine curve over a finite field $\mathbb{F}_q$ with $C = V(f)$ and $\deg f = d$. Denote by N the number of $\mathbb{F}_q$-points of C. Then*

$$|N - q| < (d-1)(d-2)\sqrt{q} + d. \tag{3.3}$$

Proof. Let C' be the homogenization of C and X be the non-singular model of C'. Further denote by $N^{(1)}$ the number of $\mathbb{F}_q$-points of C' and $N^{(2)}$ the number of $\mathbb{F}_q$-points of X. By the Weil bound, we have

$$|N^{(2)} - q - 1| \leq 2g\sqrt{q}.$$

Moreover, by the definition of the non-singular model, we have

$$|N^{(2)} - N^{(1)}| \leq \sum_{P \in C'} (\mathrm{ord}_P(C') - 1) \leq \sum_{P \in C'} \mathrm{ord}_P(C')(\mathrm{ord}_P(C') - 1)$$

and therefore with (3.2) we obtain

$$|N^{(1)} - q - 1| \leq |N^{(2)} - N^{(1)}| + |N^{(2)} - q - 1| \leq (d-1)(d-2)\sqrt{q}.$$

As the projective closure of the plane affine curve has at most d additional points at infinity, $N \leq N^{(1)} \leq N + d$ and thus $|N - N^{(1)} + 1| \leq d - 1$. Hence

$$|N - q| \leq |N - N^{(1)} + 1| + |N^{(1)} - q - 1| < (d-1)(d-2)\sqrt{q} + d.$$

□

3.3 Absolutely Irreducible Surfaces

Following [5], we are going to use estimates on the number of points and irreducible factors of polynomials restricted to linear affine varieties of dimension 2 to show Theorem 3.3.11. Unless stated otherwise, we are now going to assume that $\mathbb{A}^n = \bar{\mathbb{F}}_q{}^n$ for a finite field $\mathbb{F}_q$.

3.3.1 Affine Linear Varieties

We are going to characterize affine linear varieties by their defining equations.

Definition. *Let L be an affine linear variety in $\mathbb{A}^n$ of dimension $m \in \mathbb{N}$. A parametrization P of L is an equation of the form*

$$P : \mathbf{X} = \mathbf{n} + \mathbf{v}_1 Y_1 + \cdots + \mathbf{v}_m Y_m, \tag{3.4}$$

with $\mathbf{X} = (x_1, \ldots, x_n)$ and $\mathbf{v}_i = (v_{1,i}, \ldots, v_{n,i})$ for all $i \in \{1, \ldots, m\}$, such that for all $l \in L$ there are some $Y_1, \ldots, Y_m \in K$ with $l = \mathbf{x}$ and such that (3.4) holds.

Note that if L is given by $L = a + S$ and $s_1, \ldots, s_m \in K^n$ is a basis of S, then

$$\mathbf{X} = a + s_1 Y_1 + \cdots + s_m Y_m$$

is a parametrization of L. Conversely, for every parametrization

$$\mathbf{X} = \mathbf{n} + \mathbf{v}_1 Y_1 + \cdots + \mathbf{v}_m Y_m,$$

of L, we have $L = \mathbf{n} + \mathsf{span}(\mathbf{v}_1, \ldots, \mathbf{v}_m)$.

The main technique that is used in [5] and [37] to show bounds on the number of hypersurfaces in $\bar{\mathbb{F}}_q{}^n$ intersected with $\mathbb{F}_q^n$ is to analyze the number of factors of a polynomial f restricted to affine linear varieties of dimension 2 with a certain parametrization.

Definition. *Let L be an affine linear variety in $\mathbb{A}^n$ with parametrization*

$$P : X_i = \eta_i + \nu_{i,1}Y_1 + \cdots + \nu_{i,m}Y_m$$

for $i \in \{1, \ldots, n\}$ and let $f \in K[X_1, \ldots, X_n]$. Then a restriction of f to L is given by

$$f_{L,P} = f(\eta_1 + \nu_{1,1}Y_1 + \cdots + \nu_{1,m}Y_m, \ldots, \eta_n + \nu_{n,1}Y_1 + \cdots + \nu_{n,m}Y_m) \in K[Y_1, \ldots, Y_m].$$

Note that such a restriction is not unique, since it depends on the chosen parametrization. However, it can be shown that the number of irreducible factors of f_L is always the same.

Let

$$P : X_i = \eta_i + \nu_{i,1}Y_1 + \cdots + \nu_{i,m}Y_m, \qquad i \in \{1, \ldots, n\}$$

be the parametrization for some L, and let $f \in K[X_1, \ldots, X_n]$. Then $\mathbf{X} = T_1\mathbf{y_0} + n_1$, where $\mathbf{y_0} = (Y_1, \ldots, Y_m, 0, \ldots, 0) \in K^n$ and $T_1 = (v_1, \ldots, v_m, v_{m+1}, \ldots, v_n)$ where $v_{m+1}, \ldots, v_n \in K^n$ such that T_1 is invertible. This means that $f_{L,P} = f(T_1\mathbf{y_0} + n_1)$. Next let Q be another parametrization on L such that $Q : \mathbf{X} = T_2\mathbf{y_0} + n_2$. Then there is an invertible $T \in K^{n \times n}$ and some $n \in K^n$ such that

$$f_{L,P}(\mathbf{y_0}) = f(T_1\mathbf{y_0} + n_1) = f(T(T_2\mathbf{y_0} + n_2) + n) = f_{L,Q}(T\mathbf{y_0} + n). \tag{3.5}$$

Theorem 3.3.1. *Let L be an affine linear variety in $\mathbb{A}^n$, $f \in K[X_1, \ldots, X_n]$ and let P_1, P_2 be two parametrizations of L. Further let N_i be the number of irreducible factors of the polynomial f_{L,P_i} for $i \in \{1, 2\}$. Then $N_1 = N_2$.*

Proof. Let $g \in K[X_1, \ldots, X_n]$, $T \in K^{n \times n}$ be a regular matrix and $n \in K^n$. We will first show that g is irreducible if and only if $h := g(T\mathbf{X} + n)$ is irreducible. So assume that g is irreducible. Further let $h = h_1^{\alpha_1} \cdots h_k^{\alpha_k}$, where the h_i are irreducible. Since T is invertible, there is some matrix $\tilde{T}$ and some $\tilde{n} \in Kn$ such that $h(\tilde{T}\mathbf{X} + \tilde{n}) = g(\mathbf{X})$. Thus

$$g(\mathbf{X}) = h(\tilde{T}\mathbf{X} + \tilde{n}) = h_1(\tilde{T}\mathbf{X} + \tilde{n})^{\alpha_1} \cdots h_k(\tilde{T}\mathbf{X} + \tilde{n})^{\alpha_k},$$

and by the irreducibility of g we have without loss of generality $h(\tilde{T}\mathbf{X} + \tilde{n}) = C \cdot h_1(\tilde{T}\mathbf{X} + \tilde{n})$ for some $C \in K$. But this means that $h(\mathbf{X}) = C \cdot h_1(\mathbf{X})$, hence h is irreducible. If we assume that h is irreducible, we can show that g is irreducible analogously.
To prove the theorem, let

$$f_{L,P_1} = \left(f_{L,P_1}^{(1)}\right)^{\alpha_1} \cdots \left(f_{L,P_1}^{(N_1)}\right)^{\alpha_{N_1}} \text{ and } f_{L,P_1} = \left(f_{L,P_2}^{(1)}\right)^{\beta_1} \cdots \left(f_{L,P_2}^{(N_2)}\right)^{\beta_{N_2}},$$

where the $f_{L,P_i}^{(l)}$ are irreducible for all $i \in \{1, 2\}$ and $l \in \mathbb{N}$. If $N_1 = N_2$ we are done, so without loss of generality assume that $N_1 \leq N_2$. Then, by (3.5) we have

$$\left(f_{L,P_1}^{(1)}(\mathbf{y_0})\right)^{\alpha_1} \cdots \left(f_{L,P_1}^{(N_1)}(\mathbf{y_0})\right)^{\alpha_{N_1}} = \left(f_{L,P_2}^{(1)}(T\mathbf{y_0} + n)\right)^{\beta_1} \cdots \left(f_{L,P_2}^{(N_2)}(T\mathbf{y_0} + n)\right)^{\beta_{N_2}},$$

and since $f_{L,P_2}^{(i)}(T\mathbf{y_0} + n)$ is irreducible for all $1 \leq i \leq N_2$, we have $N_1 = N_2$. □

When restricting a polynomial to an affine linear variety, we will only be interested in the number of irreducible factors. The theorem above shows that this number does not change for the choice of parametrization, and thus we will write f_L instead of $f_{L,P}$. This allows us to make the following definitions:

Definition. *Let $f \in \mathbb{F}_q[X_1, \dots, X_n]$ with $\deg f = \delta > 0$ and let $L \subset \mathbb{A}^n$ be a linear affine variety with $\dim L = 2$. Further denote by f_L be the restriction of f to L.*

- *$M_T^{(2)}$ is the set of all linear affine varieties of dimension 2.*
- *As a subset of $M_T^{(2)}$, we denote by $M^{(2)}$ the set of all planes with the parametrization*

$$M^{(2)} = \left\{ \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix}^t \in \mathbb{F}_q^n \;\middle|\; \exists X, Y \in \mathbb{F}_q \text{ with } \begin{pmatrix} \nu_1 \\ \nu_2 \\ \vdots \\ \nu_n \end{pmatrix}^t + \begin{pmatrix} 1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix}^t X + \begin{pmatrix} 0 \\ \eta_2 \\ \vdots \\ \eta_n \end{pmatrix}^t Y = \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix}^t \right\}, \tag{3.6}$$

where $\nu_1, \nu_j, \omega_j, \eta_j \in \mathbb{F}_q$ for all $j \in \{2, \dots, n\}$ and $(\eta_2, \dots, \eta_n) \neq \mathbf{0}$.

- *E is the number of planes through a given point and $E^{(2)}$ is the number of planes through two given distinct points.*
- *$\nu(L)$ is the number of the absolutely irreducible factors of f_L over $\mathbb{F}_q$.*
- *For $j \in \{0, \dots, n\}$, we define Π_j as the set of planes $L \in M^{(2)}$ such that $|\nu(L) - 1| = j$.*
- *Π_{q-1} is the set of planes where f vanishes identically*

Moreover we define

$$A := |M^{(2)}|, \quad B = \sum_{j=1}^{\delta-1} j|\Pi_j|, \quad C = |\Pi_{q-1}|, \quad D = |M_T^{(2)}| - |M^{(2)}|.$$

When we are going to make a sum over all j, where $j = |\nu(L) - 1|$ is for some polynomial f and some linear affine plane, and include the planes where f is identically zero, then we will simply write $\sum_{j=1}^{q-1}$.

3.3.2 Estimates on the Restriction to Planes

Lemma 3.3.2. *With the notations from the definition above, we have*

$$|M_T^{(2)}| = \frac{q^n(q^n-1)(q^n-q)}{q^2(q^2-1)(q^2-q)}, \quad E = \frac{(q^n-1)(q^n-q)}{(q^2-1)(q^2-q)} \text{ and } E^{(2)} = \frac{q^n-q}{q^2-q}.$$

Proof. To count the elements in $M_T^{(2)}$, we observe that there are $q^n(q^n-1)(q^n-q)$ parametrizations of the form

$$\begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix}^t = \begin{pmatrix} \nu_1 \\ \nu_2 \\ \vdots \\ \nu_n \end{pmatrix}^t + \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix}^t X + \begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_n \end{pmatrix}^t Y,$$

since the vector $(v_1, \dots, v_n) \in \mathbb{F}_q^n$ is arbitrary and the other two vectors have to be chosen linearly independent. Moreover for every affine linear plane L, there are $q^2(q^2 - 1)(q^2 - q)$ different parametrizations describing L. The other two equalities can be proven along the same lines. □

The following theorem can be found in [21, Theorem 5]. In the theorem, $\triangle_X(p)$ denotes the discriminant of a polynomial p with respect to X.

Theorem 3.3.3. *Let K be a field and let $f \in K[X_1, \dots, X_n]$ be absolutely irreducible. Further let $\Phi \in K[V_1, \dots, V_n, W_2, \dots, W_n]$ with $\deg \Phi \leq 2\delta^2$ such that for all $(v_1, \dots, v_n, \omega_2, \dots, \omega_n) \in K^{2n/1}$ and*

$$\chi := f(X + v_1, \omega_2 X + Z_2 Y + v_2, \dots, \omega_n X + Z_n Y + v_n) \in \bar{K}[X, Y, Z_2, \dots, Z_n]$$

the following holds:

$$\Phi(v_1, \dots, v_n, \omega_2, \dots, \omega_n) \neq 0 \Rightarrow \mathrm{lc}_X(\chi) \in \bar{K} \text{ and } \triangle_X \left(\chi(X, 0, Z_2, \dots, Z_n\right) \neq 0.$$

Then there exists a polynomial $\Psi \in \bar{K}[\mathbb{Z}_2, \dots, Z_n] \setminus \bar{K}$ with $\deg \Psi \leq 3\delta^4/2 - 2\delta^3 + \delta^2/2$ such that for all $\eta = (\eta_2, \dots, \eta_n) \in \bar{K}^{n-1}$ with $\Psi(\eta) \neq 0$ the polynomial $\chi(X, Y, \eta_2, \dots, \eta_n)$ is absolutely irreducible.

We use the existence of such an Φ as above, which is also proved in [21], to deduce the following corollary.

Corollary 3.3.4. *Let $f \in \mathbb{F}_q[X_1, \dots, X_n]$ be absolutely irreducible with $\deg f = \delta > 0$. Then there are at most $(3\delta^4/2 - 2\delta^3 + 5\delta^2/2)\frac{q^{3n-3}}{q^3(q-1)}$ planes $L \in M^{(2)}$ such that f_L is not absolutely irreducible.*

Proof. With the notations from Theorem 3.3.3, we set $K = \mathbb{F}_q$ and define the polynomial

$$\Xi := \Phi(V_1, \dots, V_n, W_2, \dots, W_n)\Psi(Z_2, \dots, Z_n) \in \bar{\mathbb{F}}_q[V_1, \dots, V_n, W_2, \dots, W_n, Z_2, \dots, Z_n].$$

For any $(v, \omega, \eta) \in \bar{\mathbb{F}}_q^{3n-2}$ with $\Xi(v, \omega, \eta) \neq 0$, the polynomial $\chi(X, Y, \eta)$ is absolutely irreducible. So the only possible candidates for $L \in M^{(2)}$ such that f_L is not absolutely irreducible are those, for which $f_L = \chi(X, Y, \eta)$ is not absolutely irreducible and therefore $\Xi(v, \omega, \eta) = 0$. As Ξ defines a hypersurface of dimension $3n - 3$ and of degree less or equal than $(3\delta^4/2 - 2\delta^3 + 5\delta^2/2)$, by Lemma 3.1.5, there are at most $(3\delta^4/2 - 2\delta^3 + 5\delta^2/2)(q^{3n-3})$ different parametrizations of the form 3.6 describing a suitable plane $L \in M^{(2)}$. Since there are $q^3(q - 1)$ equivalent parametrizations for every plane, we are done. □

Assume now that we have given an absolutely irreducible polynomial $f \in \mathbb{F}_q[X_1, \dots, X_n]$ with $\deg f = \delta = 2$. Then it follows from the corollary above, that

$$B = \sum_{j=1}^{\delta-1} j|\Pi_j| = |\Pi_1| \leq (3\delta^4/2 - 2\delta^3 + 5\delta^2/2)\frac{q^{3n-6}}{(q-1)}. \tag{3.7}$$

This is a special case of the following proposition, which is proved in [5, Proposition 4.1].

Proposition 3.3.5. *Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ be a polynomial of degree $\delta > 1$. Then*

$$B \leq \left(2\delta^{13/3} + 3\delta^{11/3}\right) \frac{q^{3n-3}}{q^3(q-1)}. \tag{3.8}$$

The estimates of the following lemma are crucial for the proof of Theorem 3.3.8.

Lemma 3.3.6. *Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ with $\deg f = \delta > 0$ and let $L \subset \mathbb{A}^n$ be an $\mathbb{F}_q$-plane. Further suppose that f is not equivalent to a polynomial in $\mathbb{F}_q[X_1, \ldots, X_{n-2}]$. Then the following inequalities hold:*

$$\frac{B}{A} \leq \left(2\delta^{13/3} + 3\delta^{11/3}\right) \frac{q^{n-2}}{q^{n-1}-1}, \tag{3.9}$$

$$\frac{C}{A} \leq \frac{\delta^2}{q^2}, \tag{3.10}$$

$$\frac{D}{A} \leq \frac{4}{3q^2}, \tag{3.11}$$

$$\frac{A}{E} \leq q^{n-2}. \tag{3.12}$$

Proof. For the first inequality, let L be a linear affine variety of dimension 2 which omits to a parametrization as in (3.6). Then there are $q^3(q-1)$ equivalent parametrizations for L. Moreover, there are $q^n q^{n-1}(q^{n-1}-1) = q^{2n-1}(q^{n-1}-1)$ different possible parametrizations, thus

$$A = \frac{q^{2n-1}(q^{n-1}-1)}{q^3(q-1)}. \tag{3.13}$$

With Proposition 3.3.5, it follows that

$$\frac{1}{(2\delta^{13/3} + 3\delta^{11/3})} \frac{B}{A} \leq \frac{q^{3n-3}}{q^3(q-1)} \frac{q^3(q-1)}{q^{2n-1}(q^{n-1}-1)} = \frac{q^{n-2}}{q^{n-1}-1}$$

and thus (3.9) follows. With (3.13), equation (3.12) follows directly by Lemma 3.3.2. To obtain an upper bound for C/A, consider a plane $L \in M^{(2)}$. After a linear change of coordinates, we may assume that L is of the form $X_1 = \ldots = X_{n-2} = 0$. The plane L has q^{n-2} parallels of the form $X_1 = c_1, \ldots, X_{n-2} = c_{n-2}$ with $c_i \in \mathbb{F}_q$ for all $1 \leq i \leq n-2$. We can write f as

$$f = \sum_{i,j} p_{i,j}(X_1, \ldots, X_{n-2}) X_{n-1}^i X_n^j$$

for some finite index set $I \subset \mathbb{N}$ and polynomials $p_{i,j} \in \mathbb{F}_q[X_1, \ldots, X_{n-2}]$. Assume that L' is a plane parallel to L given by $X_1 = c_1, \ldots, X_{n-2} = c_{n-2}$ such that f_L vanishes on L'. This means that $p_{i,j}(c_1, \ldots, c_{n-2}) = 0$ for all $i, j \in I$. Assume that the $p_{i,j}$ have some common nontrivial factor h. Then $f = h \in \mathbb{F}_q[X_1, \ldots, X_{n-2}]$ since f is absolutely irreducible, contradicting our assumptions. Therefore by Lemma 3.1.6, and by the fact that the degree of every $p_{i,j}$ is bounded from above by δ, there are at most $\delta^2 q^{n-2}$ tuples $(c_1, \ldots, c_{n-2})$ such that $p_{i,j}(c_1, \ldots, c_{n-2}) = 0$ for all $p_{i,j}$. But this means that there are at most $\delta^2 q^{n-2}$ parallels L' to L such that $f_{L'} = 0$. Next, for $L \in M_{(2)}$ let $[L]_P$ be the equivalence class $\{K \in M_{(2)} \,|\text{L is parallel to } K\}$ and let D be the number of equivalence classes. Then

$$\frac{C}{A} \leq \frac{\delta^2 q^{n-4} D}{q^{n-2} D} = \frac{\delta^2}{q^2}.$$

For equation (3.11) we use the fact $D = |M_T^{(2)}| - A$ and thus have

$$\frac{D}{A} = \frac{1}{A} \frac{q^n(q^{n-1}-1)(q^{n-1}-q)}{q^2(q^2-1)(q^2-q)} \leq \frac{4}{3q^2}.$$

□

Let f be a polynomial in $\mathbb{F}_q[X,Y]$ of degree δ. In the following we will set $\omega(q,\delta) := (\delta-1)(\delta-2)q^{1/2} + \delta + 1$. The next lemma is from [36, lemma 5].

Lemma 3.3.7. *Let $f \in \mathbb{F}_q[X,Y]$ with $\deg f = \delta$ and $\nu = \nu(\mathbb{F}_q[X,Y])$. Further let N be the number of zeroes of f over $\mathbb{F}_q$. Then*

$$|N - \nu q| \leq \omega(q,\delta) + \delta^2.$$

Proof. For the proof set $\omega'(q,\delta) := \omega(q,\delta) - 1$. If f is absolutely irreducible then we are done by Corollary 3.2.3, so assume that f factors into

$$f = c f_1^{\alpha_1} \cdots f_\nu^{\alpha_\nu} f_{\nu+1}^{\alpha_{\nu+1}} \cdots f_k^{\alpha_k},$$

where the $f_i \in \mathbb{F}_q[X,Y]$ are absolutely irreducible for $i \in \{1,\ldots,\nu\}$, $f_j \in \bar{\mathbb{F}}_q[X,Y]$ are irreducible for $j \in \{\nu+1,\ldots,k\}$ and $c \in \bar{\mathbb{F}}_q$ such that every polynomial in the factorization has a coefficient equal to 1. Let $d_i = \deg f_i$ for each $i \in \{1,\ldots,k\}$. Further let V_i be the plane affine curve $V(f_i)$, $V_{i,j}$ be the affine variety $V(f_i, f_j)$, $N_i = |V_i \cap \mathbb{F}_q^2|$ and $N_{i,j} = |V_{i,j} \cap \mathbb{F}_q^2|$ for $i,j \in \{1,\ldots,k\}$. Then for $i,j \in \{1,\ldots,\nu\}$, we can deduce from Corollary 3.2.3 that we have

$$|N_i - q| < \omega'(q, d_i)$$

and by Bezout's inequality and Lemma 3.1.5 we obtain

$$N_{i,j} \leq d_i d_j.$$

Let $j \in \{\nu+1,\ldots,k\}$. As $f_j \in \bar{\mathbb{F}}_q[X,Y]$, there are some $\xi_{j,1},\ldots,\xi_{j,m} \in \bar{\mathbb{F}}_q$ such that $f_j \in (\mathbb{F}_q[\xi_{j,1},\ldots,\xi_{j,m}])[X,Y]$ and $1, \xi_{j,1},\ldots,\xi_{j,m}$ are linearly independent. Moreover, since f_j contains a term with coefficient 1, we can write it as

$$f_j = f_{j,0} + \xi_{j,1} f_{j,1} + \cdots + \xi_{j,m} f_{j,m},$$

where $f_{j,0} \in \mathbb{F}_q[X,Y]$ and $m \geq 1$. By the irreducibility of f_j, the $f_{j,r}$ are coprime for $r \in \{0,\ldots,m\}$ and therefore by Lemma 3.1.6 we have

$$N_j \leq d_j^2.$$

With the identity $\sum_i \omega'(q,\delta_i) \leq \omega'(q, \sum_i \delta_i)$ we have

$$N \geq \sum_{i=1}^{\nu} N_i - \sum_{\substack{i,j=1 \\ i \neq j}}^{\nu} N_{i,j} \geq \nu q - \sum_{i=1}^{\nu} \omega'(q,d_i) - \sum_{\substack{i,j=1 \\ i \neq j}}^{\nu} d_i d_j > \nu q - \omega'(q,\delta) - \delta^2.$$

On the other hand we obtain

$$N \leq \sum_{i=1}^{\nu} N_i + \sum_{i=\nu+1}^{k} N_i \leq \nu q + \sum_{i=1}^{\nu} \omega'(q, d_i) + \sum_{i=\nu+1}^{k} d_i^2 < \nu q + \omega'(q, \delta) + \delta^2,$$

so we have

$$-\omega'(q, \delta) - \delta^2 < N - \nu q \leq \omega'(q, \delta) + \delta^2.$$

□

We are now able to show the following theorem, which is the general version of Theorem 3.3.11, since no restrictions on the size of the finite field are given.

Theorem 3.3.8. *Let $H \subset \mathbb{A}^n$ be a hypersurface of degree δ and let $N = |H \cap \mathbb{F}_q^n|$. Then*

$$|N - q^{n-1}| \leq (\delta - 1)(\delta - 2)q^{n-3/2} + 5\delta^{13/3} q^{n-2}.$$

Proof. Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ be the defining polynomial of H, and assume that f is not equivalent to a polynomial in $n-2$ variables. First assume that $\delta = 1$. By the definition of a hypersurface, N is the number of zeroes of f over $\mathbb{F}_q^n$, and since the degree of the hypersurface equals the degree of f, the polynomial has total degree 1 and thus $N = q^{n-1}$. So we only need to prove the theorem for $\delta \geq 2$. By Lemma 3.3.7 it follows that

$$|N(f_L) - q| \leq |N(f_L) - \nu q| + |\nu(L) - 1| q \leq \omega(q, \delta) + \delta^2 + jq,$$

where $j = |\nu(L) - 1|$. Hence

$$\begin{aligned}
\sum_{L \in M^{(2)}} |N(f_L) - q| &\leq \sum_{j=0}^{q-1} \left(\sum_{L \in \Pi_j} |N(f_L) - q| \right) \\
&\leq \sum_{j=0}^{\delta-1} \left(\sum_{L \in \Pi_j} |N(f_L) - q| \right) + \sum_{L \in \Pi_{q-1}} |N(f_L) - q| \\
&= \left(\sum_{j=0}^{\delta-1} |\Pi_j| \right) (\omega(q, \delta) + \delta^2 + jq) + \sum_{L \in \Pi_{q-1}} (q^2 - q) \\
&\leq A(\omega(q, \delta) + \delta^2) + q \sum_{j=1}^{\delta-1} j|\Pi_j| + q(q-1)|\Pi_{q-1}| \\
&= A(\omega(q, \delta) + \delta^2) + Bq + Cq(q-1).
\end{aligned}$$

Moreover since $|N(f_L) - q| \leq q^2$ we have $\sum_{M_T^{(2)} \setminus M^{(2)}} |N(f_L) - q| \leq Dq^2$. Further by Lemma 3.3.2 we can write $q^{n-1} = q|M_T^{(2)}|/E = (1/E) \sum_{L \in M_T^{(2)}} q$. For the case $\delta \geq 3$ and with Lemma 3.3.6 we conclude that

$$\begin{aligned}
|N - q^{n-1}| &= \frac{1}{E}\left(\sum_{L\in M^{(2)}} |N(f_L) - q| + \sum_{M_T^{(2)}\setminus M^{(2)}} |N(f_L) - q|\right)\\
&\leq \frac{1}{E}\left(A((\omega(q,\delta) + \delta^2) + Bq + Cq(q-1) + Dq^2\right)\\
&= \frac{A}{E}\left(\omega(q,\delta) + \delta^2 + \frac{B}{A}q + \frac{C}{A}q(q-1) + \frac{D}{A}q^2\right)\\
&\leq q^{n-2}\left(\omega(q,\delta) + \delta^2 + (2\delta^{13/3} + 3\delta^{11/3})\frac{4}{3} + \delta^2 + \frac{4}{3}\right).
\end{aligned}$$

Since we have $5\delta^{13/3} \geq \delta + 1 + 2\delta^2 + 4/3 + (2\delta^{13/3} + 3\delta^{11/3})(4/3)$ for $\delta \geq 3$, we are done. For the case $\delta = 2$ we use the inequality

$$\frac{B}{A}q \leq (3\delta^4/2 - 2\delta^3 + 5\delta^2/2)\frac{4}{3}$$

which is a consequence of (3.7). With this inequality we have

$$\begin{aligned}
|N - q^{n-1}| &\leq q^{n-2}\left(\omega(q,\delta) + \delta^2 + (3\delta^4/2 - 2\delta^3 + 5\delta^2/2)\frac{4}{3} + \delta^2 + \frac{4}{3}\right)\\
&\leq (\delta-1)(\delta-2)q^{n-3/2} + (2\delta^4 + 3\delta)q^{n-2}\\
&\leq (\delta-1)(\delta-2)q^{n-3/2} + 5\delta^{13/3}q^{n-2}.
\end{aligned}$$

We still have to treat the case where f is equivalent to a polynomial in $n-2$ variables. We will do this by induction on n. For $n = 1$ and $n = 2$ there is nothing to show since f can not have only $n-2$ variables, and the theorem is true by the arguments above. Therefore assume that $n > 2$, and that f is equivalent to a polynomial g in $n-2$ variables. If we denote the number of zeroes of g in $\mathbb{F}_q^{n-2}$ by N', then $N = N'q^2$, so by the induction hypothesis we have

$$\begin{aligned}
|N - q^{n-1}| = |q^2N' - q^2q^{n-3}| &= q^2|N' - q^{n-3}|\\
&\leq q^2\left((\delta-1)(\delta-2)q^{n-7/2} + 5\delta^{13/3}q^{n-4}\right)\\
&\leq (\delta-1)(\delta-2)q^{n-3/2} + 5\delta^{13/3}q^{n-2}.
\end{aligned}$$

□

3.3.3 Improved Estimate with a Condition on the Field

With two more lemmas, we can improve the estimate given in the previous theorem, by assuming a lower bound on the number of elements in the finite field $\mathbb{F}_q$. The first lemma is from [36, lemma 6].

Lemma 3.3.9. *Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ with $\deg f = \delta$, N be the number of zeroes of f in $\mathbb{F}_q^n$ and $L \subset \mathbb{A}^n$ be a linear affine variety of dimension 2. Then*

$$\sum_{L\in M_T^{(2)}} (N(f_L) - Nq^{2-n})^2 \leq \delta E q^{n-1}.$$

Proof. We have

$$\sum_{L\in M_T^{(2)}} N(f_L) = \sum_{\substack{\mathbf{x}\in\mathbb{F}_q^n\\ f(\mathbf{x})=0}} \sum_{\substack{L\in M_T^{(2)}\\ \mathbf{x}\in L}} 1 = \sum_{\substack{\mathbf{x}\in\mathbb{F}_q^n\\ f(\mathbf{x})=0}} E = NE$$

and

$$\begin{aligned}\sum_{L\in M_T^{(2)}} (N(f_L))^2 &= \sum_{\substack{\mathbf{x}\in\mathbb{F}_q^n\\ f(\mathbf{x})=0}} \sum_{\substack{\mathbf{y}\in\mathbb{F}_q^n\\ f(\mathbf{y})=0}} \sum_{\substack{\mathbf{x},\mathbf{y}\in\mathbb{F}_q^n\\ x,y\in L}} 1 = \sum_{\substack{\mathbf{x},\mathbf{y}\in\mathbb{F}_q^n\\ f(\mathbf{y})=f(\mathbf{x})=0\\ \mathbf{x}\neq\mathbf{y}}} E^{(2)} + \sum_{\substack{\mathbf{x},\mathbf{y}\in\mathbb{F}_q^n\\ x,y\in L}} E\\ &= N(N-1)E^{(2)} + NE \leq N^2E^{(2)} + NE.\end{aligned}$$

Therefore we have

$$\begin{aligned}\sum_{L\in M_T^{(2)}} (N(f_L) - Nq^{2-n})^2 &= \sum_{L\in M_T^{(2)}} (N(f_L))^2 + 2Nq^{2-n} \sum_{L\in M_T^{(2)}} N(f_L) - N^2q^{2(2-n)} \sum_{L\in M_T^{(2)}} 1\\ &= \sum_{L\in M_T^{(2)}} (N(f_L))^2 + 2N^2q^{2-n}E - N^2q^{2(2-n)}|M_T^{(2)}|.\end{aligned}$$

By Lemma 3.3.2 we have $q^{2-n} = E/|M_T^{(2)}|$. Moreover we have $|M_T^{(2)}|E^{(2)} < E^2$ and thus

$$\sum_{L\in M_T^{(2)}} (N(f_L))^2 + 2N^2q^{2-n}E - N^2q^{2(2-n)}|M_T^{(2)}| \leq N^2E^{(2)} + NE - N^2\frac{E^2}{|M_T^{(2)}|} \leq NE.$$

Since $N \leq \delta q^{n-1}$ by Lemma 3.1.5, it follows that $NE \leq \delta E q^{n-1}$, which finished the proof. □

Lemma 3.3.10. *Let $q > 15\delta^{\frac{13}{3}}$ and let $f \in \mathbb{F}_q[X_1, \dots, X_n]$ with $\deg f = \delta$. Then*

$$\sum_{j=1}^{q-1} j|\Pi_j| \leq 4\delta E q^{n-3}.$$

Proof. First note that by Lemma 3.3.7 we have

$$|N(f_L) - q| = |(q - \nu(L)q) - (N(f_L) - \nu(L)q| \geq jp - \omega(q,\delta) - \delta^2$$

and thus with Theorem 3.3.8 we deduce

$$\begin{aligned}|N(f_L) - Nq^{2-n}| &\geq |N(f_L) - q| - 2^{q-2}|N - q^{n-1}|\\ &\geq jp - \omega(q,\delta) - \delta^2 - \omega(q,\delta) - 5\delta^{13/3} \geq \frac{1}{2}jq,\end{aligned}$$

where the last inequality holds since $q > 15\delta^{\frac{13}{3}}$. Therefore, with the previous lemma we have

$$\frac{q^2}{4}\sum_{j=1}^{q-1} j^2|\Pi_j| = \sum_{L\in M_T^{(2)}} (\frac{1}{2}jq)^2 \leq \sum_{L\in M_T^{(2)}} (N(f_L) - Nq^{2-n})^2 \leq \delta E q^{n-1}$$

and thus $\sum_{j=1}^{q-1} j|\Pi_j| \leq 4\delta E q^{n-3}$. □

Now we are able to prove the following theorem:

Theorem 3.3.11. *Let $q > 15\delta^{\frac{13}{3}}$ and let $f \in \mathbb{F}_q[X_1, \dots, X_n]$ be absolutely irreducible with* $\deg f = \delta$. *Further let N be the number of zeroes of f in $\mathbb{F}_q^n$. Then*

$$|N - q^{n-1}| \leq (\delta - 1)(\delta - 2)q^{n-3/2} + (5\delta^2 + \delta + 1)q^{n-2}.$$

Proof. We can assume that f is not equivalent to a polynomial in $n-2$ variables, since the case where it is equivalent to such a polynomial can be treated analogously as in the proof of Theorem 3.3.8. Moreover note that for the case $\delta = 1$ we have $N = q^{n-1}$ and the inequality holds, so we can assume that $\delta \geq 2$. Similar to the proof of Theorem 3.3.8 we have

$$\begin{aligned}\sum_{L \in M_T^{(2)}} |N(f_L) - q| &\leq \sum_{j=0}^{\delta-1} \left(\sum_{L \in \Pi_j} (\omega(q, \delta + \delta^2 + jq) \right) + \sum_{L \in \Pi_{q-1}} (q^2 - q) \\ &\leq \left(\sum_{j=0}^{\delta-1} |\Pi_j| \right) (\omega(q, \delta + \delta^2) + q \sum_{j=0}^{\delta-1} j|\Pi_j| + q(q-1)|\Pi_{q-1}| \\ &\leq (A + D)(\omega(q, \delta + \delta^2) + 2q \sum_{j=0}^{q-1} j|\Pi_j|\end{aligned}$$

and thus by Lemma 3.3.10 it follows that

$$\sum_{L \in M_T^{(2)}} |N(f_L) - q| \leq (A + D)(\omega(q, \delta + \delta^2) + 8\delta E q^{n-2}.$$

Therefore we have

$$\begin{aligned}|N - q^{n-1}| = |\frac{1}{E} \sum_{L \in M_T^{(2)}} N(f_L) - \frac{1}{E} \sum_{L \in M_T^{(2)}} q| &\leq \frac{1}{E} \sum_{L \in M_T^{(2)}} |N(f_L) - q| \\ &\leq \frac{1}{E} \left((A + D)(\omega(q, \delta + \delta^2) + 8\delta E q^{n-2} \right) \\ &\leq q^{n-2}((\delta - 1)(\delta - 2)q^{1/2} + 5\delta^2 + \delta + 1).\end{aligned}$$

□

3.4 A Family of Collision-Free Functions

In order to construct a Diophantine Equation over a finite field which is hard to solve, as we need to do in 5.3, we are going to prove the following theorem, as given in [3], by Bérczes, Folláth and Pethő.

Theorem 3.4.1. *Let $\gamma \in \mathbb{F}_q^*$, $A, B \in \mathbb{F}_q[X_1, \dots, X_n]$ homogeneous with* $\deg A < \deg B = D$ *and* $\deg_{X_i} B = D$ *for all $i \in \{1 \dots, n\}$. Further suppose that there are $k, l \in \{1, \dots, n\}$ with $k < l$ and*

$$B(0, \dots 0, X_k, 0, \dots, 0, X_l, 0, \dots, 0) \in \mathbb{F}_q[X_k, X_l] \tag{3.14}$$

has no multiple zeroes. Set $F := A + B$ and let $P_{coll}(F, \gamma)$ be the probability that $F(\mathbf{x}) = \gamma$, where $\mathbf{x}$ is chosen uniformly at random from $\mathbb{F}_q^n$. If $q > 5D^{13/3}$, then

$$P_{coll}(F, \gamma) \leq \frac{3}{q}. \tag{3.15}$$

Moreover, $F + \gamma$ is absolutely irreducible over $\mathbb{F}_q$.

We will use Theorem 3.3.11 to establish the bound of the collision probability P_{coll}. We only need to show that a polynomial $F + \gamma$ as given above is absolutely irreducible.

Lemma 3.4.2. *Let K be a field with algebraic closure $\bar{K}$. Further let $A, B \in K[X]$ such that B has no multiple zeroes in $\bar{K}$ and $\deg A \neq \deg B \geq 1$. For some $n \geq 4$ we define*

$$G := Y^n + AY^{n-1} + B \in K[X, Y].$$

Then G is absolutely irreducible.

Proof. For the sake of a contradiction assume that G is reducible, i.e. there are $U, V \in \bar{K}[X, Y]$ with $G = UV$. Then U and V are of the form

$$\begin{aligned} U &= Y^k + a_{k-1}Y^{k-1} + \cdots + a_1 Y + a_0, \\ V &= Y^{n-k} + b_{n-k-1}Y^{n-k-1} + \cdots + b_1 Y + b_0, \end{aligned}$$

with polynomials a_i, b_j such that

$$a_i \in \begin{cases} \bar{K}[X] & : 0 \leq i \leq k-1 \\ \{1\} & : i = k \\ \{0\} & : k+1 \leq i \leq n-2 \end{cases} \quad \text{and} \quad b_j \in \begin{cases} \bar{K}[X] & : 0 \leq j \leq n-k-1 \\ \{1\} & : j = n-k \\ \{0\} & : n-k+1 \leq j \leq n-2. \end{cases}$$

We first assume that $\min\{k, n-k\} \geq 2$. With U, V, a_i and b_j defined as above, we have

$$G = UV = \sum_{i=0}^{n} c_i Y_i \text{ with } c_i = \sum_{j=0}^{i} a_j b_{i-j}. \tag{3.16}$$

By equating coefficients we see that $a_0 b_0 = B$, so we can assume without loss of generality that $\deg a_0 \geq 1$. Since $\bar{K}$ is algebraically closed, we choose some $\alpha \in \bar{K}$ with $a_0(\alpha) = 0$. By assumption B has no multiple root, therefore $b_0(\alpha) \neq 0$. By a simple inductive argument, it follows that $a_i(\alpha) = 0$ for all $i \neq k$. Thus $U(\alpha, Y) = Y_K$. We have $\min\{k, n-k\} \geq 2$ and thus $n - k - 2 \geq 0$, so we can write

$$\begin{aligned} Y^n + A(\alpha)Y^{n-1} + B(\alpha) &= G(\alpha, Y) = U(\alpha, Y)V(\alpha, Y) \\ &= Y^n + b_{n-1}(\alpha)Y^{n-1} + \cdots + b_1(\alpha)Y + b_0(\alpha). \end{aligned}$$

This is a contradiction since $0 = B(\alpha) \neq b_0(\alpha)$.
Assume now that $\min\{k, n-k\} = 1$, and without loss of generality that $k = 1$. Then $U = Y + a_0$ and $V = Y^{n-1} + b_{n-2}Y^{n-2} + \cdots + b_1 Y + b_0$. By (3.16) we obtain $B = a_0 b_0$ and $a_0 b_i = -b_{i-1}$ for all $i \in \{1, \ldots, n-2\}$. This means that $a_0^2 | B$, and since B has no multiple

roots, $a_0 \in \bar{K}$. Moreover, from $a_0 b_i = -b_{i-1}$ it follows that $b_{n-k-2} = (-a_0)^k b_n - 2$ for all $k \in \{1, \dots, n-2\}$, thus

$$\begin{aligned} Y^n + AY^{n-1} + B = G = UV \\ = Y^n + (a_0 + b_{n-2})Y^{n-1} + a_0(-a_0)^{n-2} b_{n-2}. \end{aligned}$$

But this means that $\deg A = \deg B$, which is a contradiction. □

Lemma 3.4.3. *Let K be a field, $\gamma \in K$, $A, B \in K[X_1, \dots, X_n]$ homogeneous with $\deg A < \deg B = D$ and $\deg_{X_i} B = D$ for all $i \in \{1 \dots, n\}$. Further suppose that there are $k, l \in \{1, \dots, n\}$ with $k < l$ and*

$$B(0, \dots 0, X_k, 0, \dots, 0, X_l, 0, \dots, 0) \in K[X_k, X_l]$$

has no multiple zeroes. Set $F := A + B$. Then the polynomial $F + \gamma$ is absolutely irreducible.

Proof. Assume that the polynomial $g := F + \gamma$ is reducible, i.e. there are $U, V \in \bar{K}[X_1, \dots, X_n]$ such that $g = UV$ and $\deg U, \deg V \geq 1$. Fix some indices $i, j \in \{1, \dots, n\}$ such that

$$B_0 := B(0, \dots 0, X_k, 0, \dots, 0, X_l, 0, \dots, 0)$$

has no multiple roots and set

$$\begin{aligned} A_0 &= A(0, \dots 0, X_i, 0, \dots, 0, X_j, 0, \dots, 0), \\ U_0 &= U(0, \dots 0, X_i, 0, \dots, 0, X_j, 0, \dots, 0), \\ V_0 &= V(0, \dots 0, X_i, 0, \dots, 0, X_j, 0, \dots, 0), \\ F_0 &= A_0 + B_0 \text{ and } \ g_0 = F_0 + \gamma. \end{aligned}$$

Since $\deg U \geq 1$ there is some $k \in \{1, \dots, n\}$ such that $\deg_{X_k} U \geq 1$. Since $\deg_{X_s} B = D$ for all s and $\deg A < \deg B$, $\deg_{X_s} g = D$. Moreover, since $g - \gamma$ is homogeneous, we have $\deg_{X_s} V < n$ and $\deg_{X_s} U > 0$. By repeating this argument, we can deduce that $1 \leq \deg_{X_s} U, \deg_{X_s} V \leq D - 1$ for all $s \in \{1, \dots, n\}$. This means that $g_0 = U_0 V_0$ is a nontrivial factorization of g_0. With $r = \deg X_j A_0$ we can write g_0 as

$$\begin{aligned} g_0 &= B_0 + A_0 + \gamma \\ &= X_j^D \left(B_0 \left(\frac{X_i}{X_j}, 1 \right) + \frac{1}{X_j^{D-r}} A_0 \left(\frac{X_i}{X_j}, 1 \right) + \gamma \frac{1}{X_j^D} \right) \\ &= \gamma X_j^D \left(b + aY^{D-r} + Y^D \right), \end{aligned}$$

where

$$X := \frac{X_i}{X_j}, Y := \frac{1}{X_j}, a = \frac{1}{\gamma} A_0(X, 1) \text{ and } \ b = \frac{1}{\gamma} B_0(X, 1).$$

Since $g_0 = U_0 V_0$, we set $K_1 = \deg_{X_j} U_0$, $K_2 = \deg_{X_j} V_0$ and obtain

$$\begin{aligned} g_0 &= \gamma X_j^{K_1} X_j^{K_2} \left(\frac{1}{\gamma X_j^{K_1}} U_0 \right) \left(\frac{1}{\gamma X_j^{K_2}} V_0 \right) \\ &= \gamma X_j^D U_0'(X, Y) V_0'(X, Y) \end{aligned}$$

for some nontrivial polynomials U_0' and V_0'. But this gives a factorization of $b + aY^{D-r} + Y^D$, which is absolutely irreducible by Lemma 3.4.2. □

Proof of Theorem 3.4.1. Assume that we have given $f = A + B + \gamma \in \mathbb{F}_q[X_1, \dots, X_n]$ as in the theorem. Then by Lemma 3.4.3, f is absolutely irreducible. By Theorem 3.3.11, we have

$$|N - q^{n-1}| \leq (D-1)(D-2)q^{n-3/2} + (5D^2 + D + 1)q^{n-2},$$

where N denotes the number of zeroes of f in $\mathbb{F}_q^n$. Thus

$$|N| \leq q^{n-1} + (D-1)(D-2)q^{n-3/2} + (5D^2 + D + 1)q^{n-2}.$$

As the collision of $F = A + B$ with γ equals a root of f, we have

$$\begin{aligned} P_{coll}(F, \gamma) = \frac{|N|}{|\mathbb{F}_q^n|} &\leq \frac{1}{q} + \frac{(D-1)(D-2)}{q^{3/2}} + \frac{(5D^2 + D + 1)}{q^2} \\ &\leq \frac{1}{q} + \frac{1}{q}\underbrace{\left(\frac{(D-1)(D-2)}{q^{1/2}}\right)}_{<1} + \frac{1}{q}\underbrace{\left(\frac{(5D^2 + D + 1)}{q}\right)}_{<1} < \frac{3}{q}. \end{aligned}$$

□

4 Cryptographic protocols based on Diophantine Equations

The proof that Hilbert's Tenth Problem has not solution means that there is no single algorithm taking any Diophantine equation as input and solving it. This does not mean that all Diophantine equations are hard to solve. On the contrary, most equations with a single variable or zero-dimensional systems of Diophantine equations can be solved efficiently. However, in spite of great efforts, there are many Diophantine equations for which there is no known method of solving them in polynomial time or even better. This fact is a reason for studying the use of Diophantine equations in the construction of public key cryptosystems.

Kerkhoff's principle for designing a cryptographic protocol states that an adversary, who tries to break a protocol, has knowledge of everything except for the private keys, i.e. the exact execution of a protocol is known. In order for a public key system to work, a message encrypted by the public key has to be linked to the private key in a way to decrypt the message. However, the public key can not give away any information of the private key, even with the knowledge of how the private key was chosen. This idea is realized through so called one-way-functions.

Definition. *A function $f : X \mapsto Y$ is called a one-way function, if for all $x \in X$ $f(x) = y$ can be computed in polynomial time, but for any probabilistic polynomial time algorithm A, we have*

$$Pr[A(f(X_n)) \in f^{-1}(f(X_n))] < n^{-\omega(1)}$$

where X_n denotes the uniform distribution over X^n.

Informally this means that f is easy to compute, but there is no efficient way of computing the inverse f^{-1}. Although it is believed that one-way functions exist, e.g. simple multiplication, it is a fact yet to be proved. A trapdoor function is a special case of a one-way function, where additional information on the function f ensures the computation of the inverse of f in polynomial time. To use a trapdoor function f in a public key cryptosystem, assume that p is the private key only known to the participant Alice. Alice uses the private key to compute the inverse $f^{-1}(m)$ for some message m, which she can do in a short amount of time assuming that p is the additional information required to invert a trapdoor function.

The hardness of solving certain Diophantine equations offers a chance of constructing possible candidates for trapdoor functions. For example, in section 4.2 we note that the problem of finding a non-negative solution to the equation

$$X_1 s_1 + \cdots + X_n s_n = C$$

is NP complete. The coefficients of this equation form the public key of a cryptosystem, and since it was constructed from the private key in a way that the solution of the equation for the holder of the private key is easy, this forms a trapdoor function based on Diophantine equations.

4.1 Ong-Schnorr-Shamir Signature Scheme

The Ong-Schnorr-Shamir cryptosystem for obtaining signatures was first proposed in 1984, [33]. It is a fairly simple protocol, which can be implemented and executed rather efficiently. Part of the security is based on the assumption that finding a single solution to a quadratic Diophantine equation over the ring $\mathbb{Z}_n$ is difficult. However, this assumption turned out to be false.

4.1.1 The Protocol

Assume that Alice wants to sign a message $M \in \mathbb{Z}_n$ where n is chosen arbitrarily. The signature scheme follows the subsequent protocol:

Ong-Schnorr-Shamir signature scheme

Key generation *Alice chooses two large primes p and q and sets $n = pq$. Further she chooses some $u \in \mathbb{Z}_n^*$, publishes n and $k := -u^{-2} \mod n$ while keeping u secret.*

Signature generation *Given a message $M \in \mathbb{Z}_n$, Alice selects a random $X_1 \in \mathbb{Z}_n^*$ and sets $X_2 := MX_1^{-1}$. Further she computes*

$$S_1 := (X_2 + X_1)/2,$$
$$S_2 := (X_2 - X_1)u/2.$$

The pair (S_1, S_2) acts as a signature for M.

Signature verification *To verify that (S_1, S_2) is a signature for M, Bob checks whether*

$$S_1^2 + kS_2^2 \equiv M \mod n. \tag{4.1}$$

To verify that a signature given by Alice indeed fulfills (4.1), we note that $X_1X_2 = M$, and thus

$$S_1^2 + kS_2^2 \equiv (X_2 + X_1)^2/4 - u^{-2}(X_2 - X_1)^2u^2/4 \equiv X_1X_2 \equiv M \mod n.$$

Note that as in other signature schemes, there is no one-to-one correspondence between signatures (S_1, S_2) and messages M, since there are n^2 possible pairs (S_1, S_2) and only n possible messages $M \in \mathbb{Z}_n$.

4.1.2 Cryptoanalysis of the Scheme

It can be shown that from the data given by the public key, the scheme cannot be broken by finding the private key, assuming that the factorization of n is a one-way function.

Proposition 4.1.1. *Finding the secret key u^{-1} is at least as hard as factoring n.*

Proof. Assume that we have given n and an algorithm to efficiently compute the secret key with the knowledge of the public key. Pick some $u \in \mathbb{Z}_n^*$ uniformly at random, and compute $k \equiv -u^{-2} \mod n$. Since (n, k) forms a public key for the signature scheme, we can compute $u' \in \mathbb{Z}_n^*$ such that $-(u')^{-2} \equiv k \mod n$. The equations $x^2 \equiv k \mod p$ and $x^2 \equiv k \mod q$ both have two solutions, thus it is easy to show using the Chinese Remainder Theorem that $x^2 \equiv k \mod n$ has exactly four solutions x_1, x_2, x_3, x_4, where the probability that $x_i \equiv \pm x_j$ is $\frac{1}{2}$ for $i, j \in \{1, 2, 3, 4\}$. Therefore $u \not\equiv \pm u'$ with probability $\frac{1}{2}$. Since

$$-(u')^{-2} \equiv -u^{-2} \Leftrightarrow (u' - u)(u' + u) \equiv 0 \mod n,$$

and n has only two prime factors, after choosing m different $u \in \mathbb{Z}_n^*$, we can indeed factorize n with probability $1 - \frac{1}{2^m}$. □

So the security of the Ong-Schnorr-Shamir signature scheme relies on the difficulty of solving the quadratic Diophantine equation

$$x^2 + ky^2 - m \equiv 0 \mod n \tag{4.2}$$

over $\mathbb{Z}$ for given m and k. However, Pollard [34] found a way of solving this equation efficiently using a probabilistic algorithm. His main idea was the reduction of the above equation to one with a smaller k and a new m. By iterating this process, an equation of the form $x^2 \pm y^2 \equiv m \mod n$ has to be solved, which can be done efficiently. This breaks the protocol, even with the given difficulty of finding the private key. The outline of the algorithm given by Pollard given in [34] is as follows:

1. If $n = p^k$ for some prime p, then solve (4.2) by computing square roots in $\mathbb{Z}_n^*$.
2. Replace m by a smaller m' such that $-k$ is a quadratic residuo modulo m_0, and where $0 < m' \leq \sqrt{4|k|/3}$ if $k > 0$ and $0 < |m'| \leq \sqrt{|k|}$ otherwise.
3. If m' is a perfect square, or $m' = k$, solve $x^2 + ky^2 \equiv m' \mod n$ with $y = 0$ or $x = 0$, go to step 5.
4. Apply the steps above recursively to solve $(x')^2 - m'(y')^2 \equiv -k \mod n$ such that $\gcd(y', n) = 1$. Solve $x^2 + ky^2 = m' \mod n$ with $x := x'(y')^{-1} \mod n$, $y := (y')^{-1} \mod n$.
5. Solve the recursive steps in 2-4 to obtain a solution to (4.2).

The time complexity of Pollard's algorithm is given $\mathcal{O}((\log n)^2 \log\log |k|)$, so a signature can be forged very efficiently. A first attempt of repairing the OSS scheme tried to run the protocol not over $\mathbb{Z}_n$, but instead used algebraic integers and executed the protocol over

$$\mathbb{Z}_{n,d} := \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}, 0 \leq a, b \leq n\}$$

for some fixed $d \in \mathbb{Z}$. The idea was that Pollard's algorithm only works over an Euclidean domain, which $\mathbb{Z}_{n,d}$ is not for any d with $d > 73$ or $d < -11$. However, Pollard's algorithm can be extended to algebraic integers, making this approach for a signature scheme insecure.

4.1.3 Extensions of OSS

The OSS scheme can be extended to protocols which are similar to the one in 4.1.1, but which are not vulnerable to any known algorithm solving

$$x^2 - ky^2 \equiv m \mod n.$$

Two signature schemes of this kind are treated in [29]. The first one presented exploits the fact that when solving the equation above algorithmically, there is no control over the structure of the solution. The base of the signature scheme is to set $x := r + \frac{m}{r}$ for some random $r\mathbb{Z}_n$, and publish a hash value of x along with the signature.
The second signature scheme takes advantage of the fact that Pollard-like algorithms take k as an input. By taking a non-polynomial function $k(x)$ instead of k, it is impossible for such algorithms to forge signatures.

4.2 Lin-Chang-Lee Cryptosystem

In [24], Lin, Chang and Lee proposed a public key cipher scheme, whose trapdoor function is based on certain Diophantine equations in n variables which are believed to be difficult to solve.

4.2.1 The Protocol

Let $w \in \mathbb{N}$ with $w = 2^b - 1$ for some positive integer b. A message M that is encrypted is assumed to be nb bits long. Further we assume that M can be broken down into n sub-messages of the form $m_1, \dots, m_n$.

Lin-Chang-Lee public key cryptosystem

Key Generation

1. *Choose n pairs $(q_1, k_1), \dots, (q_n, k_n) \in \mathbb{Z}^2$ such that $\gcd(q_i, q_j) = 1$ for $i \neq j$, $k_i > w$, $q_i > k_i w(q_i \mod k_i)$ and $q_i \not\equiv 0 \mod k_i$ for all $i \in \{1, \dots, n\}$.*
2. *For all $i \in \{1, \dots, n\}$ compute $R_i \equiv q_i \mod k_i$, $N_i = \lceil q_i/(k_i R_i) \rceil$,*

$$Q_i = \prod_{i \neq j} q_i \text{ and } Q = \prod_{i=1}^{n} q_i.$$

3. *For all $i \in \{1, \dots, n\}$, set $b_i \equiv Q_i^{-1} R_i \mod q_i$ and compute $s_i = Q_i b_i N_i \mod Q$.*

4. *Publish the key* $(s_1, \ldots, s_n)$. *The private key is given by the set of pairs* $(q_1, k_1), \ldots, (q_n, k_n)$, *all other parameters need not to be stored.*

Encryption

A message $M = (m_1, \ldots, m_n)$ *is encrypted to the ciphertext*

$$C = \sum_{i=1}^{n} m_i s_1 \tag{4.3}$$

Decryption

The i-th block of the message M can be decrypted by $m_i = \lfloor k_i C / q_i \rfloor$.

4.2.2 Cryptoanalysis

Lin et al. base the security of their public key cryptosystem on the difficulty of solving linear Diophantine equations over positive integers. They claim that in order to break the protocol, an attacker has to solve

$$X_1 s_1 + \cdots + X_n s_n = C$$

and obtain the message. In fact it can be shown that this problem is NP-complete, by reducing the integer knapsack problem to solving linear Diophantine equations with positive integers. However, in [8], Cusick showed that the cipher can be broken without solving any Diophantine equations. The major weakness of the cryptosystem is the construction of the public key, where any two numbers share a large common factor. To see this, define $G_i = \gcd(s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$ for all $i \in \{1, \ldots, n\}$ and $G = \gcd(s_1, \ldots, s_n)$. By (4.3) this leads to the equations $C \equiv m_i s_i \mod G_i$ and by defining $t_i = G_i / G$ we get

$$C/G \equiv m_i s_i / G \mod t_i. \tag{4.4}$$

Now

$$C/G \equiv x s_i / G \mod t_i$$

is a linear congruence in a single variable x for all $i \in \{1, \ldots, n\}$ and since we have $\gcd(s_i/G, G_i/G) = 1$, any solutions are congruent modulo t_i. Assume that x_0 is the smallest positive solution to the above equation. In [8], Cusick proves the following lemma:

Lemma 4.2.1. *Given any choice of the public key* $S = (s_1, \ldots, s_n)$, *we have* $t_i \geq w$ *for all* $i \in \{1, \ldots, n\}$.

From (4.4) it follows that $x = m_i \leq w$ is a solution and by the above lemma we have $t_i \geq w$, so by solving the above linear congruence one obtains in fact $x_0 = m_i$. Doing so for all $i \in \{1, \ldots, n\}$, we have retrieved the message $M = (m_1, \ldots, m_n)$.

4.3 Pre-conditions For Designing Asymmetric Cryptosystem Based On Diophantine Equation Hard Problem

The negative answer to Hilbert's Tenth Problem in section 2.6 concludes that there is no algorithm that decides whether any Diophantine equation is solvable or not. When building a cryptosystem that is based on some kind of Diophantine equation, solvability is usually a triviality, since a solution is mostly part of a private key and thus always given. In addition to that, restrictions to the appearing Diophantine equation may limit the number of non-zero coefficients or the degree of the polynomial. In [2], the so called Diophantine Equation Hard Problem is introduced, addressing the solvability of Diophantine equations from the following different perspective:

Definition. *Let $f = v_1X_1 + \cdots + v_nX_n - u \in \mathbb{Z}[X_1, \ldots, X_n]$ and fix a solution $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$. We call $\mathbf{x}$ the prf-solution to f. The Diophantine Equation Hard Problem (DEHP) is the problem of determining a prf-solution given f.*

Note that if a linear $f \in \mathbb{Z}[X_1, \ldots, X_n]$ as above is solvable, it has infinitely many solutions. For cryptography and consequent implementation purposes, one limits or even fixes the lengths of the parameters of such solutions, resulting in a finite solution space. As we will see in Proposition 5.4.6, this solution space is exponential in the size of the bound, which is the cause of the difficulty of the DEHP.

4.3.1 The Protocol

Assume that we have given a message $M \in \mathbb{Z}$ with bit length $2n$ and $M < 2^{2n-1} + 2^{2n-2}$.

AA$_\beta$ public key cryptosystem

Key Generation

Alice chooses two distinct primes p, q with bit lengths of n and $pq > 2^{2n-1} + 2^{2n-2}$. She computes $e_{A1} = p^2q$ and chooses some representant e_{A2} of an $e \in \mathbb{Z}_{pq}^*$ such that e_{A2} has bit length $3n$.

Encryption

Bob chooses some $k_1 \in \mathbb{Z}$ with bit length $4n$ and computes the ciphertext $C = k_1e_{A1} + M^2e_{A2}$.

Decryption

Set $W \equiv Ce^{-1} \equiv M^2 \mod pq$. With the knowledge of p,q and by the Chinese Remainder Theorem, the four square roots M_1, M_2, M_3, M_4 of $W \mod pq$ are computed. Select the $i \in \{1, 2, 3, 4\}$ such that

$$k_1' = \frac{C - M_i^2}{e_{A1}} \in \mathbb{Z}$$

and set $M_i = M$.

Asbullah and Ariffin prove that the decryption works for the choice of the above parameters, and that there are no decryption errors.

4.3.2 Cryptoanalysis

The security of the protocol has been analyzed in [28]. With the bounds on k_1 and the message M in the encryption process, the underlying instance of the DEHP is the solution of

$$C = k_1 e_{A1} + M^2 e_{A2}$$

for unknowns k_1 and M^2, since the other parameters are public and thus known to an adversary. Despite the simple nature of this equation, no known attack for this equation can retrieve the secret parameters within a feasible amount of time. Indeed, the parameters of the protocol where chosen such that the Euclidean Algorithm or Gaussian Lattice Reduction lead to a solution, but not efficiently enough to break the protocol. It is shown that encryption of the AA_β protocol has time complexity of $\mathcal{O}(n^2)$.

4.4 Multivariate Public Key Cryptosystems from Diophantine Equations

As many other public key systems, multivariate public key cryptosystems (MPKC) are based on the idea of a trapdoor function. In the case of MPKCs, this trapdoor function takes the form of a multivariate polynomial system of equations over a finite field k, where the polynomials are usually quadratic. The public key is represented by a map

$$\bar{F} : k^n \to k^m, \bar{F} = L_1 \circ F \circ L_2$$

where $n, m \in \mathbb{N}$ with $m \geq n$, $L_1 : k^m \to k^m$ and $L_2 : k^n \to k^n$ are random invertible affine transformations and the so-called central map $F : k^n \to k^m$ is an invertible nonlinear multivariate polynomial map. The functions L_1, L_2 and in some cases F form the private key of this cryptosystem. Two recent MPKCs are so called triangular and oil-vinegar systems. In [13], Gao and Heindl offer a framework which is a mixture of both, as discussed in the next section. To present this, we first need to make the following definition:

Definition. *Let k be a finite field. We call $f \in k[\check{x}_1, \dots, \check{x}_v, x_1, \dots, x_o]$ an oil-vinegar polynomial if it is of the form*

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

We call $x_1, \dots, x_o$ the oil variables and $\check{x}_1, \dots, \check{x}_v$ the vinegar variables.

4.4.1 General Framework

Let $k, \mathbb{F}$ be finite fields with $[\mathbb{F} : k] = d$ and $l, t \in \mathbb{N}$, where l is the number of layers of oil-vinegar systems and t is the number of polynomials of a system. First we describe how the public key is constructed. For the function $\bar{F}$, both L_1, L_2 are randomly chosen, so that we only have to construct the central map $F : \mathbb{F}^{n+lo} \to \mathbb{F}^{n+lt}$. To do so, let f_i be oil-vinegar polynomials such that there are nonlinear

$$g_i \in \mathbb{F}[Y_{n+(i-1)t+1}, \dots, Y_{n+it}], \qquad i \in \{1, \dots, l\},$$

where each $g_i(f_{n+(i-1)t+1}, \dots, f_{n+it})$ is a product of quadratic factors in $\mathbb{F}[X_1, \dots, X_{n+lo}]$. Let $\psi_1, \dots, \psi_n$ be n such quadratic factors. We define the first triangular system by

$$Y_i = f_i(X_1, \dots, X_{n+lo}) = X_i + \phi_i(X_1, \dots, X_i) + \psi_i(X_1, \dots, X_{n+lo}), \quad i \in \{1, \dots, n\}, \tag{4.5}$$

where every ϕ_i is a quadratic polynomial. Next, by setting $X_1, \dots, X_n$ the initial vinegar and $X_{n+1}, \dots, X_{n+o}$ the oil variables, we have the first oil-vinegar system

$$Y_{n+i} = f_{n+1}(X_1, \dots, X_n, X_{n+1}, \dots, X_{n+o}), \quad i \in \{1, \dots, t\}. \tag{4.6}$$

In this way, l layers are constructed, where the j-th layer is given by

$$Y_n + i = f_{n+i}(X_1, \dots, X_{n+(j-1)o}, X_{n+(j-1)o+1}, \dots, X_{n+jo}) \quad i \in \{(j-1)t + 1, jt\} \tag{4.7}$$

for $j \in \{2, \dots, l\}$, with vinegar variables $X_1, \dots, X_{n+(j-1)o}$ and with oil variables $X_{n+(j-1)o+1}, \dots, X_{n+jo}$. The central map is then given as

$$F(X_1, \dots, X_{n+lo}) = (f_1, \dots, f_{n+lt}).$$

In order to conduct the decryption, we need to assume that there are functions h_i such that

$$h_i(g_1, \dots, g_l) = \psi_i$$

for all $i \in \{1, \dots, n\}$. The decryption of a ciphertext $C \in k^m$ is performed as follows: First compute

$$(Y_1, \dots, Y_{n+lt}) = L_1^{-1}(C)$$

and compute the value of ψ_i by substituting $Y_{n+1}, \dots, Y_{n+lt}$ into $g_1, \dots, g_l$ and evaluating the h_i. This way, (4.5), (4.6) and (4.7) form a triangular system of equations, which can be solved iteratively. With the resulting $X_1, \dots, X_{n+lo}$ we finish the decryption by

$$M = L_2^{-1}(X_1, \dots, X_{n+lo}).$$

Unfortunately, this framework includes two possibilities for decryption failure. First, one may not be able to compute inverses for evaluating the h_i. Second, for any oil-vinegar system, the linear systems in the oil variables may not be solvable.

4.4.2 An Instance Based on Diophantine Equations

Gao and Heindl show how to construct a cryptosystem based on the above framework and on Diophantine equations of the form

$$AB = CD + EF + GH + IJ + KL,$$

where $C, D, \dots, J$ are oil-vinegar polynomials and there are no restrictions on K and L. The equation can be rewritten as

$$\psi_1\psi_2 = f_1 f_2 + \dots + f_9 f_{10},$$

where $deg\psi_1 = \deg \psi_2 = \deg f_i = 2$ for $i \in \{1, \dots, 10\}$ and

- $\psi_1 \in \mathbb{F}[X_1, \dots, X_n]$, $\psi_2 \in \mathbb{F}[Y_1, \dots, Y_n]$,
- $f_i \in \mathbb{F}[X_1, \dots, X_n, Y_1, \dots, Y_n]$ for all $i \in \{1, \dots, 10\}$ and further f_i are oil-vinegar polynomials for $i \in \{1, \dots, 8\}$.

Without going into detail, the central map is constructed to be of the form $F : \mathbb{F}^{45} \to \mathbb{F}^{74}$ consisting of one triangular system and 7 layers of oil-vinegar systems.

4.4.3 Cryptoanalysis

When trying to break the protocol with attack strategies based on either linear algebra or algebraic attacks, which have proven to be useful at analyzing other multivariate public key cryptosystems, the cryptosystem seems to be secure for the choice of at least $|k| = 2^{16}$ and $d = [\mathbb{F} : k] = 1$. A higher choice of any of those two variables may increase security, but will decrease efficiency of the cryptosystem.

5 The Key Exchange Protocol by Harry Yosh

Let R be a ring with unity, and assume that there exist some $a \in R, b \in \mathbb{N}$ such that the function

$$\begin{aligned} T_{a,b} : & R[X] \to R[X] \\ & X \mapsto (X + a)^b \end{aligned}$$

is invertible. In the key exchange protocol proposed by Harry Yosh, two participants Alice and Bob want to agree on a secret with the use of public key cryptography. The public key of Alice consists of a multidimensional Diophantine equation, and her secret is a predetermined solution to this equation. As we will see, this cryptographic protocol can be executed for the cases $R = \mathbb{Z}$ and $R = \mathbb{F}_q$.

5.1 The Protocol

Yosh's key exchange protocol

1. *Alice chooses a polynomial $f \in R[X_1, \ldots, X_n] \setminus R$ and some $\mathbf{r} = (r_1, \ldots, r_n) \in R^n$, such that $\mathbf{r}$ is a solution to the Diophantine equation*

$$f(X_1, \ldots, X_n) = 0. \tag{5.1}$$

   She publishes f and keeps $\mathbf{r}$ a secret.
2. *Bob chooses some $g \in R[X_1, \ldots, X_n]$ and parameters $a_1, \ldots, a_m, b_1, \ldots, b_m \in R$ such that T_{a_i,b_i} is invertible for all $i \in \{1, \ldots, m\}$, where $T_{a,b}$ is defined as*

$$\begin{aligned} T_{a,b} : R[X_1, \ldots, X_n] &\to R[X_1, \ldots, X_n], \\ q &\mapsto (q + a)^b. \end{aligned}$$

   He computes

$$h' = T_{a_m,b_m} \circ \cdots \circ T_{a_1,b_1}(g) = (\ldots(g + a_1)^{b_1} + a_2)^{b_2} + \cdots + a_m)^{b_m} \tag{5.2}$$

   and chooses a representative h of h' in $R[X_1, \ldots, X_n]/(f)$. Bob publishes both g and h.
3. *Alice now computes both $s = g(\mathbf{r})$ and $u = h(\mathbf{r})$ and sends u to Bob.*
4. *In the last step, Bob computes*

$$T^{-1}_{a_1,b_1} \circ \cdots \circ T^{-1}_{a_m,b_m}(u) = s.$$

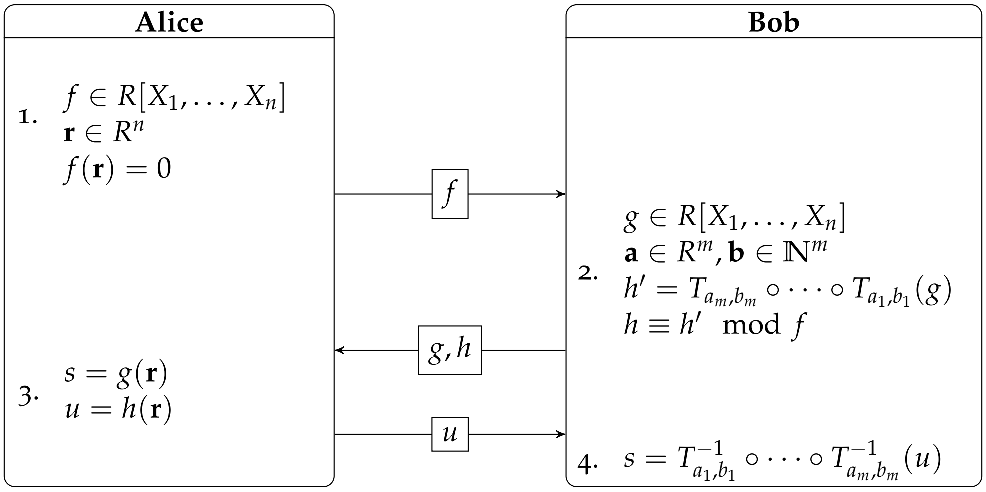
Alice
Bob
1. $f \in R[X_1, \ldots, X_n]$
$\mathbf{r} \in R^n$
$f(\mathbf{r}) = 0$
f
2. $g \in R[X_1, \ldots, X_n]$
$\mathbf{a} \in R^m, \mathbf{b} \in \mathbb{N}^m$
$h' = T_{a_m,b_m} \circ \cdots \circ T_{a_1,b_1}(g)$
$h \equiv h' \mod f$
g, h
3. $s = g(\mathbf{r})$
$u = h(\mathbf{r})$
u
4. $s = T^{-1}_{a_1,b_1} \circ \cdots \circ T^{-1}_{a_m,b_m}(u)$

Figure 5.1: After finishing the protocol, Alice and Bob share a secret $s \in R$.

Theorem 5.1.1. *After running the protocol above, Alice and Bob have a shared secret s.*

Proof. Alice first calculates s by $s = g(\mathbf{r})$. Since $h \equiv h' \mod f$, there is some $q \in R[X_1, \ldots, X_n]$ such that $h = h' + fq$. Thus

$$u = h(\mathbf{r}) = h'(\mathbf{r}) + f(\mathbf{r})q(\mathbf{r}) = h'(\mathbf{r}), \tag{5.3}$$

and with (5.2) we get

$$T^{-1}_{a_1,b_1} \circ \cdots \circ T^{-1}_{a_m,b_m}(u) = T^{-1}_{a_1,b_1} \circ \cdots \circ T^{-1}_{a_m,b_m}(h'(\mathbf{r})) = g(\mathbf{r}) = s.$$

□

A simplification of Yosh' protocol was made in [18] by using only 2 parameters a and b for the function $T_{a,b}$. It was originally defined as

$$T'_{a,b,c}(x) = (x + a)^b + c,$$

which would lead to

$$\begin{aligned} &T_{a'_m,b'_m,c_m} \circ \cdots \circ T_{a'_1,b'_1,c_1}(g) = \\ &(\ldots(g + a'_1)^{b'_1} + c_1 + a'_2)^{b'_2} + \cdots + c_{m-1} + a'_m)^{b'_m} + c_m \end{aligned}$$

in (5.2). But this equals $T_{a_{m+1},b_{m+1}} \circ \cdots \circ T_{a_1,b_1}(g)$ with $a_1 = a'_1$, $a_j = a'_j + c_{j-1}$, $a_{m+1} = c_m$, $b_k = b'_k$, $b_{m+1} = 1$ for $j \in \{2, \ldots, m\}$, $k \in \{1, \ldots, m\}$, so the third parameter c is obsolete.

A single protocol run between Alice and Bob established exactly one secret s, and both participants have exactly one public key. Thus a single protocol run is represented by the parameters used to exchange the secret s.

Remark *We denote the parameters of a given protocol run as $(f, \mathbf{r}, g, h, \mathbf{a}, \mathbf{b})$, where $f = 0$ is a Diophantine equation as in 5.1, $\mathbf{r} \in R^n$ a solution to this Diophantine equation and g, h, $\mathbf{a}$,$\mathbf{b}$ are chosen as in step 2 of the protocol, where $\mathbf{a} = (a_1, \ldots, a_m)$ and $\mathbf{b} = (b_1, \ldots, b_m)$ for some $m \in \mathbb{N}$. Note that from $(f, \mathbf{r}, g, h, \mathbf{a}, \mathbf{b})$, $\mathbf{r}$, $\mathbf{a}$ and $\mathbf{b}$ are kept secret, whereas f, g and h can be assumed to be available for any attacker. Furthermore, we will always denote by n the number of variables and by m the number of a_i, b_i as chosen in step 2 of the protocol, unless indicated otherwise.*

5.2 Security Essentials

In Yosh's brief analysis of the protocol, two possible points for an attack of the protocol were given. First of all, an attacker observes the system

$$\begin{aligned} f(X_1, \ldots, X_n) &= 0, \\ h(X_1, \ldots, X_n) &= u. \end{aligned} \tag{5.4}$$

By solving the system (5.4) an attacker knows the solution $\mathbf{r} \in R^n$, so he can compute $g(\mathbf{r}) = s$. However, if this system is positive-dimensional, it is hard to solve in general as we have seen in Chapter 2. A second strategy that Yosh proposed for a possible attack was to decipher the sequence

$$T_{a_m,b_m} \circ \cdots \circ T_{a_1,b_1}(g) \equiv h \tag{5.5}$$

and thus retrieve the numbers $a_1, b_1, \ldots, a_m, b_m$. With these numbers, an attacker can compute the secret s like in step 4 of the protocol, since u is part of the public information of sender and recipient. Similar to (5.5), an attacker can also try to decipher

$$T_{a_m,b_m} \circ \cdots \circ T_{a_1,b_1}(s) = u. \tag{5.6}$$

Note that this equation follows immediately from (5.3) and (5.2). A notable difference between the two equations above is, that h is only one representative of the left-hand side of (5.5), whereas equality holds for the equation above. In addition to that, s adds another unknown to equation (5.6) in comparison to (5.5). The equation (5.6) is further analyzed in 5.4.1.

Lemma 5.2.1. *Let $f \in R[X_1, \ldots, X_n] \setminus R$, where R is a field and assume that for $\mathbf{r} = (r_1, \ldots, r_n) \in R^n$ we have $f(\mathbf{r}) = 0$ and $f(X_1, r_2, \ldots, r_n) \neq 0$. Then there exist $n-1$ protocol runs with parameters $(f, \mathbf{r}, g_i, h_i, \mathbf{a_i}, \mathbf{b_i})$, $i \in \{2, \ldots, n\}$, such that the system of polynomial equations*

$$\begin{aligned} f(x_1, \ldots, x_n) &= 0, \\ h_i(x_1, \ldots, x_n) &= u_i, \ i \in \{2, \ldots, n\} \end{aligned} \tag{5.7}$$

has only finitely many solutions.

Proof. Let $f_0 \in R[X_2, \dots, X_n], f_1 \in R[X_1, \dots, X_n]$ be the unique polynomials such that $f = f_0 + X_1 f_1$. Further let

$$G := \{(x_2, \dots, x_n) \in R^{n-1} | (x_1, \dots, x_n) \in R^n \setminus V(f_0, f_1)\},$$

where $V(f_0, f_1)$ is the affine variety $V(f_0, f_1) = \{\mathbf{x} \in R^n \mid f_0(\mathbf{x}) = f_1(\mathbf{x}) = 0\}$. Since $f \neq 0$, at least one of the polynomials f_0, f_1 is not equal to 0, hence G contains infinitely many points. Note that $(r_2, \dots, r_n) \in G$.

Now consider the choice of the h_i. For any $g_i \in R[X_i]$, consider the equation $0 = h_i(x_i) - u_i$. When we choose $h = h'$, we have

$$\begin{aligned} 0 &= h_i(x_i) - u_i = h_i(x_i) - h_i(r_i) = h_i'(x_i) - h_i'(r_i) \\ &= (\dots(g_i(x_i) + a_1)^{b_1} + \dots + a_m)^{b_m} - (\dots(g_i(r_i) + a_1)^{b_1} + \dots + a_m)^{b_m} \end{aligned}$$

and thus $h_i(x_i) - u_i = 0$ if and only if $g_i(x_i) - g_i(r_i) = 0$. We claim that we can fix parameters $(f, \mathbf{r}, g_i, h_i, \mathbf{a_i}, \mathbf{b_i})$, $i \in \{2, \dots, n\}$ such that

$$V(h_2 - u_2, \dots, h_n - u_n) \subseteq G.$$

Indeed, if we set for example $g_i = X_i$ for all $i \in \{2, \dots, n\}$, then $h_i(x_i) - u_i = 0$ if and only if $x_i = r_i$ and

$$V(h_2 - u_2, \dots, h_n - u_n) = \{(r_2, \dots, r_n)\} \subset G.$$

So for any $(a_2, \dots, a_n) \in V(h_2 - u_2, \dots, h_n - u_n)$, we have $f(X_1, a_2, \dots, a_n) \in R[X_1] \setminus \{0\}$, and thus $f(X_1, a_2, \dots, a_n) = 0$ has only finitely many solutions, since $V(h_2 - u_2, \dots, h_n - u_n)$ is finite, as every polynomial h_i is a polynomial in only one unknown. It follows that (5.7) has only finitely many solutions.

□

Assume that $\mathbf{a}, \mathbf{b}$ and g are chosen such that $\gcd(f, h - u) \in R$. Then the system

$$\begin{aligned} f(X_1, X_2) &= 0, \\ h(X_1, X_2) &= u, \end{aligned}$$

is obviously zero dimensional, thus it can be solved within a short amount of time. This gives a lower bound for n, namely $n \geq 3$.
In many instances it is convenient to reuse the public key of a protocol. In the case of Yosh's key exchange protocol, this may be done at most $n - 2$ times.

Proposition 5.2.2. *The protocol can be used at most $n - 2$ times using the same parameters f and $\mathbf{r}$.*

Proof. Assume that Alice has run the protocol (not necessarily with the same partner Bob) i times using the pair f and $\mathbf{r}$. At the i-th run, an adversary observes the system as in (5.4):

$$\begin{aligned} f(x_1, \dots, x_n) &= 0, \\ h_i(x_1, \dots, x_n) &= u_i. \end{aligned}$$

It follows that after $n-1$ protocol runs, n equations in n unknowns are given, leading to a system of equations

$$\begin{aligned} f(x_1,\ldots,x_n) &= 0, \\ h_1(x_1,\ldots,x_n) &= u_1, \\ &\vdots \\ h_{n-1}(x_1,\ldots,x_n) &= u_n - 1. \end{aligned}$$

By Lemma 5.2.1, this system may be zero-dimensional and thus vulnerable to an attack. □

Next we define bounds on $\mathbf{a}, \mathbf{b}$ used in a protocol with parameters $(f, \mathbf{r}, g, h, \mathbf{a}, \mathbf{b})$.

Definition. *k Let R be a ring with unity and absolute value $|\cdot|$, $\mathcal{T}, \mathcal{S} \in \mathbb{N}$, and let*

$$\hat{\mathcal{B}}(R) = \{b \in \mathbb{N} \mid T_b \textit{ is invertible}\}$$

where $T_b : R[X] \to R[X]$ with $x \mapsto x^b$. Further let $P(\mathcal{T}, \mathcal{S})$ be the set of all parameters $(f, \mathbf{r}, g, h, \mathbf{a}, \mathbf{b})$ for protocol runs such that the number of steps for performing step 1-4 of the protocol is bounded by $\mathcal{T}$ and the number of bits needed to store $(f, \mathbf{r}, g, h, \mathbf{a}, \mathbf{b})$ is at most $\mathcal{S}$. We define

$$\begin{aligned} \mathcal{M}_{\mathcal{T},\mathcal{S}} &:= \max\{|a_i| \in \mathbb{N} \mid \exists (f, \mathbf{r}, g, h, \mathbf{a}, \mathbf{b}) \in P(\mathcal{T}, \mathcal{S}) \textit{ with } \mathbf{a} = (a_1, \ldots, a_i, \ldots, a_m)\}, \\ \mathcal{B}_{\mathcal{T},\mathcal{S}} &:= \max\{b_i \in \hat{\mathcal{B}}(R) \mid \exists (f, \mathbf{r}, g, h, \mathbf{a}, \mathbf{b}) \in P(\mathcal{T}, \mathcal{S}) \textit{ with } \mathbf{b} = (b_1, \ldots, b_i, \ldots, b_m)\}. \end{aligned}$$

Further define

$$\mathcal{B}_{\mathcal{T},\mathcal{S}}(R) := \{b \in \hat{\mathcal{B}}(R) \mid b \le \mathcal{B}_{\mathcal{T},\mathcal{S}}\}.$$

Note that in the above definition, we consider the size of the a_i as a natural number $|a_i|$. This makes sense, since we want to measure the a_i by the number of bits that are needed to represent them.

Let $\mathcal{T}, \mathcal{S} \in \mathbb{N}$ and $(f, \mathbf{r}, g, h, \mathbf{a}, \mathbf{b})$ be the parameters of a protocol run such that $(f, \mathbf{r}, g, h, \mathbf{a}, \mathbf{b}) \in P(\mathcal{T}, \mathcal{S})$. We want to investigate lower bounds on $\mathcal{T}$ and $\mathcal{S}$. To do so, we only cover step 2 of the protocol, since step 1 depends on the way of choosing f, and both step 3 and 4 can be executed efficiently.

So assume that $\deg_{X_i} g = t_i$. Then $u_i' = \deg_{X_i} h' = t_i b_1 b_2 \ldots b_m$. The upper bound on the number of terms for h' is given by $(u_1+1)\ldots(u_n+1)$, and since polynomials in sparse representations, e.g. polynomials with relatively few non-zero terms compared to their degree, are rare, we can assume that the number of non-zero terms of h' is

$$\mathcal{O}(u_1 \ldots u_n) = \mathcal{O}(t_1 \ldots t_n (b_1 b_2 \ldots b_m)^n).$$

We choose h such that $h \equiv h' \mod f$, thus there is some $H \in R[X_1, \ldots, X_n]$ such that $h = h' + Hf$. By assuming that $\deg_{X_i} f \le u_i'$ for any $i \in \{1, \ldots, n\}$, we can always choose H such that $\deg_{X_i} h \le u_i$. Since h is part of the public key, we cannot store h as $h' + Hf$, since the knowledge of h' might lead to an attack on the protocol as we will see later. Thus h needs to be stored in dense representation, which needs

$\mathcal{O}(t_1 \dots t_n(b_1 b_2 \dots b_m)^n)$ many bits.
For the sake of convenience we write $\mathcal{M}$ and $\mathcal{B}$ instead of $\mathcal{M}_{\mathcal{T},\mathcal{S}}$ and $\mathcal{B}_{\mathcal{T},\mathcal{S}}$ when not talking about certain bounds $\mathcal{S}$, $\mathcal{T}$.

A way for an attacker to retrieve the secret s is to find solutions to the Diophantine equation $f = 0$. Finding the solution $\mathbf{r}$ is not the only way of attacking the protocol. If the Diophantine equation has at least m solutions, the protocol can be broken if m of them are given, even without knowing $\mathbf{r}$.

Proposition 5.2.3. *Let $(f, \mathbf{r}, g, h, \mathbf{a}, \mathbf{b})$ be the parameters of a protocol run. If an adversary can compute m different solutions to the Diophantine equation (5.1), then he can also compute s in $\mathcal{O}(\mathcal{B}^{m+n})$.*

Proof. First note that if one of the computed solutions is in fact $\mathbf{r}$, then the adversary can compute s by simply following the protocol.
Let now $\mathbf{t} \in R^n$ such that $f(\mathbf{t}) = 0$. An adversary knows g, so he can compute $\beta = g(\mathbf{t})$. As a representative of h' in $R[X_1, \dots, X_n]/(f)$, h is of the form $h = h' + Sf$ for some $S \in R[X_1, \dots, X_n]$, hence $h(\mathbf{t}) = h'(\mathbf{t})$. This gives us the equation

$$(\dots(\beta + a_1)^{b_1} + a_2)^{b_2} + \dots + a_m)^{b_m} = h(\mathbf{t}). \tag{5.8}$$

Assume now that we have m different solutions to (5.1), $\mathbf{t}_1, \dots, \mathbf{t}_m \in R^n$ and fix some $b_1, \dots, b_m \in \{1, 3, 5, \dots, \mathcal{B}\}$. By defining

$$h_k = h(\mathbf{t}_k), \beta_k = g(\mathbf{t}_k) \text{ for } k \in \{1, \dots, m\}$$

and introducing integer variables $G_j^{(i)}$ for $i, j \in \{1, \dots, m\}$, we can transform the set of m equations of the form (5.8) into the following polynomial system:

$$A := \begin{cases} G_1^{(1)b_1} &= h_1, \\ &\vdots \\ G_m^{(1)b_1} &= h_m, \end{cases}$$
$$B := \left\{ G_j^{(i)} = G_j^{(i+1)b_{m-i}} + a_{(m+1-i)}, \; j \in \{1, \dots, m\}, i \in \{2, \dots, m-1\} \right\}$$
$$C := \begin{cases} G_1^{(m)} &= \beta_1 + a_1, \\ &\vdots \\ G_m^{(m)} &= \beta_m + a_1. \end{cases}$$

There are $m^2 + m$ unknowns, namely $a_i, G_j^{(i)}$ for $i, j \in \{1, \dots, m\}$. Moreover, there are m equations in the set A, $m(m-1)$ in the set B and again m in C, giving us $m^2 + m$ equations. This system is zero-dimensional, hence it can be solved in $\mathcal{O}(\mathcal{B}^n)$ steps using an algorithm based on Gröbner bases as in [23]. Since we have to solve the above system for any $b_1, \dots, b_m \in \mathcal{B}(R)$, this gives us a runtime of $\mathcal{O}(\mathcal{B}^n \mathcal{B}^m)$ □

5.2.1 Importance of Choosing a Representant h

In step 2 of Yosh's key exchange protocol, the public key part h is chosen as a representative of h' in $R[X_1, \dots, X_n]/(f)$. This not only leads to a possible reduction of the size of the public key, but also adds to the security of the protocol. In fact, we can show that if $h = h'$, an attacker can break the protocol in at most $\mathcal{O}(\mathcal{B}^{2mt}|\mathcal{B}(R)|^{m+1})$, where $t = \deg_{X_i} g$ for some $i \in \{1, \dots, n\}$ such that $t \geq 0$. As we will see later, $\mathcal{B}$, m and t have to be small positive integers for the protocol to be efficient, thus such an attack would be managable within a feasible amount of time. To do so, we have to establish how to efficiently compute $a \in R$, $r \in \mathcal{B}(R)$ and $h \in R[X_1, \dots, X_n]$ for a given $f \in R[X_1, \dots, X_n]$ such that

$$h^r + a = f. \tag{5.9}$$

For the rest of the chapter assume that $h' = h$ and that R is an integral domain.
First let $f, h \in R[X]$ with $f = a_n X^n + \dots + a_1 X + a_0$, $g = b_m X^m + \dots + b_1 X + b_0$ such that $f = h^r$ for some $r \in \mathbb{N}_{\geq 2}$ with $x \mapsto x^r$ invertible. Then $r|n$ and $b_m^r = a_n$. By expanding h^r we get

$$\begin{aligned} &(b_m X^m + \dots + b_1 X + b_0)^r = \\ &B_m X^n + B_{m-1} X^{n-1} + \dots + B_0 X^{n-m} + \mathcal{O}(X^{n-m-1}) \end{aligned} \tag{5.10}$$

where

$$B_i = b_m^{r-1} b_{m-i} + \sum_{\substack{k_1 m + \dots + k_{i-1}(m-i+1) = mr-i \\ k_1 + \dots + k_{i-1} = r,\ k \geq 0}} \binom{r}{k_1, \dots, k_{i-1}} b_1^{k_1} \dots b_{m-i+1}^{k_{m-i+1}} \tag{5.11}$$

for $i \in \{0, \dots, m\}$. By (5.10) and $f = h^r$ we get a system of equations

$$B_m = a_m, \dots, B_0 = a_{n-m}. \tag{5.12}$$

We want to solve this system for unknowns $b_m, \dots, b_0$. Since r is invertible, $b_m = \sqrt[r]{a_n}$. Moreover, by (5.11) every B_i is a polynomial in $b_m, \dots, b_{m-i}$, thus we immediately get a solution for b_{m-1} via the equation $B_{m-1} = a_{m-1}$, which leads to a solution for b_{m-2} via $B_{m-2} = a_{m-2}$ and so on. Hence we can solve the above system in $\mathcal{O}(m)$ steps. By [19] we can expand $(b_m X^m + \dots + b_1 X + b_0)^r$ in less than $r^2(m+1)^2$ steps, hence we can compute $\sqrt[r]{f} = h$ in

$$\mathcal{O}(r^2(m+1)^2) + \mathcal{O}(m) = \mathcal{O}(r^2 \left(\frac{n}{r}\right)^2) = \mathcal{O}(n^2).$$

The procedure above computes $\sqrt[r]{f} = h$ without needing the constant term of f, therefore to solve an equation of the form $f = a + h^r$, we can first compute h and then $a = f(0) - (h(0))^r$. To use this for an equation of the form (5.9), we can view any $f \in R[X_1, \dots, X_n]$ as a polynomial in X_i over $R[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n]$ where $i \in \{1, \dots, n\}$ such that $\deg_{X_i} f \geq 0$.

This leads to Algorithm 1.

Algorithm 1: Find all solutions for a_i, b_i to the nested equation $(\dots(g(X_1,\dots,X_n)+a_1)^{b_1}+a_2)^{b_2}+\cdots)^{b_{m-1}}+a_m = h(X_1,\dots,X_n)$

```
Let $LM(g) = X_1^{\beta_1}\dots X_n^{\beta_n}$
$j = 0$                                          /* global variable */
NestedRoot($0$,$h$,$j$)
Function NestedRoot($i$,$H$,$I$)
    Let $LM(H) = X_1^{\alpha_1}\dots X_n^{\alpha_n}$
    $D = \gcd(\alpha_1,\dots,\alpha_n)$
    for $r \in \{x \in \mathcal{B}(R)\} \mid x$ divides $D\}$ do
        if $\beta_i \nmid \frac{\alpha_i}{r}$ for any $i \in \{1,\dots,n\}$ then
            stop
        $G = \sqrt[r]{H}$
        $j = j+1$
        if $i < m-2$ then
            $b_{m-i-1}^{[I,j]} = r$
            $a_{m-i}^{[I,j]} = H(\mathbf{0}) - G(\mathbf{0})$
            NestedRoot($i+1$,$G$,$j$)
        else
            if $(G(X_1,\dots,X_n) - G(\mathbf{0})) = (g - g(\mathbf{0}))$ then
                $b_1^{[I,j]} = r$
                $a_2^{[I,j]} = H(\mathbf{0}) - G(\mathbf{0})$
                $a_1^{[I,j]} = G(\mathbf{0}) - g(\mathbf{0})$
```

Note that Algorithm 1 only works if m is known. For unknown m, one could run the algorithm for all $m \in \{1,\dots,K\}$ where

$$K = \max\{k \in \mathbb{N} \mid a^k \deg g \le \deg h\}$$

and $1 < a = \min \mathcal{B}(R)$. This is an upper bound for m, since by our assumption of h, we have $\deg h = \deg g b_1 \dots b_m$ for some $b_i \in \mathcal{B}(R)$. Thus the algorithm has to be run at most $(\log \deg h - \log \deg g) / \log a$ times. Further note that the step

$$G(X) = \sqrt[r]{H(X)}$$

may not be computed the way it is above for every r, since $H(X)$ is not an r-th power for all $r \in \{x \in \mathcal{B}(R)\} \mid x$ divides $D\}$ in general. Hence we need to add the step of checking that $G(X) \in R[X]$ and $G(X)^r = H(X)$, which does not increase the time for taking the r-th root of $\mathcal{O}(n^2)$.

Theorem 5.2.4. *Let $g, h \in R[X_1,\dots,X_n]$ with $\deg_{X_i} g = t$ for some $i \in \{1,\dots,n\}$ such that $t \ge 1$. Algorithm 1 finds all $a_i \in R$, $b_i \in \mathcal{B}(R)$, $i \in \{1,\dots,m\}$ with*

$$(\dots(g(X_1,\dots,X_n)+a_1)^{b_1}+a_2)^{b_2}+\cdots)^{b_{m-1}}+a_m = h(X_1,\dots,X_n) \tag{5.13}$$

in at most $\mathcal{O}(\mathcal{B}^{2mt}|\mathcal{B}(R)|^{m+1})$.

Proof. As we have seen before, for a given $h \in R[X_1, \dots, X_n]$ $\mathsf{NestedRoot}(0, h, j)$ computes all $b_{m-1} \in \mathcal{B}(R)$, $a_m \in R$ and $g_{m-1} \in R[X_1, \dots, X_n]$ such that

$$g_{m-1}^{b_{m-1}} + a_m = h.$$

For $i \in \{1, \dots\ m-2\}$ $\mathsf{NestedRoot}(i, g_{m-i}, j)$ gives us all solutions for

$$g_{m-i-1}^{b_{m-i-1}} + a_{m-1} = g_{m-i}$$

and thus we receive a_j, b_j, g_j such that

$$\begin{aligned} h &= g_{m-1}^{b_{m-1}} + a_m \\ &= (g_{m-2}^{b_{m-2}} + a_{m-1})^{b_{m-1}} + a_m \\ &\vdots \\ &= (\dots(g_1)^{b_1} + a_2)^{b_2} + \dots)^{b_{m-1}} + a_m. \end{aligned}$$

We have $g + a_1 = g_1$, hence $a_1 = g_1(\mathbf{0}) - g(\mathbf{0})$. Taking any root of h takes at most $(tb_1 \dots b_m)^2 = \mathcal{O}(\mathcal{B}^{2m})$ time, and since $\deg g_i < \deg h$ for $i \in \{1, \dots, m-1\}$, this gives an upper bound for any root calculation performed in the algorithm. By the nested character of the $\mathsf{NestedRoot}$ calls, the algorithm finds all solutions to 5.13 in

$$\mathcal{O}(\mathcal{B}^{2m})(|\mathcal{B}(R)| + \dots + |\mathcal{B}(R)|^m) = \mathcal{O}(\mathcal{B}^{2m})\frac{|\mathcal{B}(R)|^{m+1} - 1}{|\mathcal{B}(R)| - 1} = \mathcal{O}(\mathcal{B}^{2mt}|\mathcal{B}(R)|^{m+1}).$$

□

Algorithm 1 finds at most $\mathcal{B}^m$ pairs $(\mathbf{a}, \mathbf{b})$ satisfying (5.13). To choose one, let A be the set of all $a_{k_1}^{[I_1, I_2]}$ computed by the algorithm, where $k_1 \in \{1, \dots, m\}$ and $I_1, I_2 \in \mathbb{N}$. For any $i_1, i_2 \in \mathbb{N}$ such that there exists some $a_1^{[i_2, i_1]} \in A$, a solution to (5.13) is given by

$$\begin{aligned} \mathbf{a} &= (a_1^{[i_2,i_1]}, a_2^{[i_2,i_1]}, a_3^{[i_3,i_2]}, \dots, a_{m-1}^{[i_{m-1},i_{m-2}]}, a_m^{[i_m,i_{m-1}]}), \\ \mathbf{b} &= (b_1^{[i_2,i_1]}, b_2^{[i_3,i_2]}, \dots, b_{m-2}^{[i_{m-1},i_{m-2}]}, b_{m-1}^{[i_m,i_{m-1}]}). \end{aligned}$$

5.3 The Protocol over Finite Fields

We have to ensure that security of the protocol can still be given in finite fields. In 5.2 we established that the solution of the system of equations (5.4) breaks the protocol. Although the solution space over a field $\mathbb{F}_q$ is finite, the solution of systems of higher order congruence equations is NP-complete for $n \geq 3$, c.f. [14].
Next, we require the function $x \mapsto x^b$ to be invertible over $\mathbb{F}_q^*$. It is a well-known fact that this holds if and only if $\gcd(q-1, b) = 1$. The following lemma gives us a way of fixing a finite field suitable for the protocol:

Lemma 5.3.1. *Let p_1, p_2 be odd prime numbers with $p_2 | (2^{p_1} - 1)$. Then $p_2 > p_1$.*

Proof. Since

$$2^{p_1} \equiv 1 \mod p_2,$$

we have $\operatorname{ord}_{\mathbb{F}_{p_2}^*} 2 | p_1$, and since p_1 is prime $\operatorname{ord}_{\mathbb{F}_{p_2}^*} 2 = p_1$. Thus $p_1 | (p_2 - 1)$ and it follows that $p_2 > p_1$.

□

Now let $\mathcal{B}$ be an upper bound for the exponents $b_1, \dots, b_m$. For any prime number r, the smallest prime factor of $2^r - 1$ is at least r. Thus by choosing r prime with $r > \mathcal{B}$ and $q = 2^r$, every exponentiation we perform in the protocol is invertible in $\mathbb{F}_q^*$.

5.3.1 Choosing a Polynomial f

As in [18], we are going to use Theorem 3.4.1 to construct a Diophantine equation $f(X_1, \dots, X_n) = 0$ over a finite field, which can not be solved in a reasonable amount of time by guessing solutions $\mathbf{x} \in \mathbb{F}_q^n$ uniformly at random. In order to do so, we need to find homogeneous polynomials A and B that fulfill the requirements of the theorem.

Proposition 5.3.2. *Let $F = A + B \in \mathbb{F}_q[X_1, \dots, X_n]$ with*

$$A = \alpha_1 X_1^s + \dots + \alpha_n X_n^s,$$
$$B = \beta_1 X_1^r + \dots + \beta_n X_n^r,$$

where $\alpha_i, \beta_j \in \mathbb{F}_q^*$ for $i, j \in \{1, \dots, n\}$. Let $0 < s < r < q$ and further let $\gcd(r, q) = 1$. Then F satisfies all assumptions of Theorem 3.4.1.

Proof. The diagonal form of the homogeneous polynomials A and B ensures $\deg A < \deg B = r$ and $\deg_{X_i} B = r$ for all $i \in \{1 \dots, n\}$, so it remains to prove that

$$b(X_k, X_l) := B(0, \dots 0, X_k, 0, \dots, 0, X_l, 0, \dots, 0) = \beta_k X_k^r + \beta_l X_l^r \in \mathbb{F}_q[X_k, X_l]$$

has no multiple roots. The binary form $b(X_k, X_l)$ has no multiple roots at $(a, b) \in (\mathbb{F}_q^*)^2$ if and only if $\frac{\partial}{\partial X_k} b(X_k, X_l)|_{X_k = a, X_l = b} \neq 0$ or $\frac{\partial}{\partial X_l} b(X_k, X_l)|_{X_k = a, X_l = b} \neq 0$. Since $\gcd(r, q) = 1$ and both $a \neq 0$, $\beta_k \neq 0$ we have $\frac{\partial}{\partial X_k} b(X_k, X_l)|_{X_k = a, X_l = b} = \beta_k r a^{r-1} \neq 0$. □

Assume now that Alice and Bob want to execute Yosh's key exchange protocol over a finite field. First, they agree on a finite field $\mathbb{F}_q$, where $q = 2^r$ for some large enough prime r. Then with Algorithm 2, Alice can construct a suitable Diophantine equation over $\mathbb{F}_q$.

Theorem 5.3.3. *Let $f \in \mathbb{F}_q[X_1, \dots, X_n] \setminus \mathbb{F}_q$ be constructed by Algorithm 2. The probability of finding a root $\mathbf{x}$ of f, when x runs uniformly through the elements of $\mathbb{F}_q^n$, is at most $\frac{3}{q}$.*

Algorithm 2: Construct a polynomial $f \in \mathbb{F}_q[X_1, \dots, X_n]$ and $\mathbf{r} \in \mathbb{F}_q^n$ with $f(r) = 0$.

```
  Input  : $v, M \in \mathbb{N}$
1 Choose $\alpha_i, \beta_i \in \mathbb{F}_q^*$ for $i \in \{1, \dots, n\}$
2 Choose $r \in \mathbb{N}$ odd with $3 \leq r < (\frac{q}{5})^{3/13}$
3 Choose $s \in \mathbb{N}$ with $1 \leq s < r$
4 Set $A = \alpha_1 X_1^s + \cdots + \alpha_n X_n^s$, $B = \beta_1 X_1^r + \cdots + \beta_n X_n^r$
5 Choose $\mathbf{r} \in \mathbb{F}_q^n$
6 $\gamma = A(\mathbf{r}) + B(\mathbf{r})$
7 if $\gamma = 0$ then
8     go to 5
9 $f = A + B - \gamma$
```

Proof. First, we choose the coefficients α_i, β_i of the polynomials A and B according to Proposition 5.3.2. Choosing r odd ensures that $\gcd(r, q) = 1$. Moreover $r < (\frac{q}{5})^{3/13}$ induces $r < q$ as well as $q > 5r^{13/3}$. With the **go to** loop we choose $\mathbf{r} \in \mathbb{F}_q^n$ randomly until we find a $\gamma \in \mathbb{F}_q^*$. By selecting $\mathbf{r}$ uniformly from $\mathbb{F}_q^n$, we obtain $\gamma \neq 0$ with high probability according to Lemma 5.3.4. Thus we can assume that the algorithm terminates. By Theorem 3.4.1, $P_{\text{coll}}(A + B, \gamma) \leq \frac{3}{q}$, and therefore the same probability holds for finding a root of f.

□

Note that we assume the termination of Algorithm 2 based on a probabilistic argument. By the Schwartz-Zippel Lemma below, the probability of $A(\mathbf{x}) + B(\mathbf{x}) \neq 0$ is at least

$$1 - rq^{n-1}\frac{1}{q^n} > 1 - \frac{1}{5^{3/13}q^{n-3/13}},$$

hence it is highly unlikely that $\gamma = 0$ occurs even once for any chosen q and $n \geq 2$.

Lemma 5.3.4 (Schwartz-Zippel). *Let $f \in \mathbb{F}_q[X_1, \dots, X_n]$ be non-zero with $\deg f = d$ the total degree of f. Then the number of zeros of f is at most dq^{n-1}.*

Proof. Since $V(f)$ is a hypersurface with $\dim V(f) = n - 1$ and $\deg V(f) = d$ by Proposition 3.1.2, the lemma follows directly from Lemma 3.1.5. □

Despite the analogy of the Schwartz-Zippel Lemma and the above theorem, there are two main advantages for polynomials chosen subject to the conditions of Theorem 3.4.1. First, for q sufficiently large, the probability of finding a uniformly chosen root $\mathbf{x}$ is always bounded by $\frac{3}{q}$, whereas the other bound, $\frac{d}{q}$ depends on the total degree d of the polynomial. Second, the polynomial f found by Algorithm 2 is absolutely irreducible, hence the equation $f = 0$ can not be solved via factoring f.

5.3.2 Finite Fields with Characteristic Greater than 2

Now let $\mathbb{F}_q$ be a finite field with $2 \nmid q$. This means that we can not use Lemma 5.3.1 to set $\mathcal{B}(\mathbb{F}_q)$.
Let $\mathcal{B}' = \{3, 5, \dots, \mathcal{B}\}$, which is the set of candidates for $\mathcal{B}(\mathbb{F}_q)$. There are no even numbers in $\mathcal{B}'$, since $2|(q-1)$ for every choice of q. First assume that q is a prime. Then

$$\mathcal{B}(\mathbb{F}_q) = \{b \in \mathcal{B}' \mid \gcd(q-1, b) = 1\}.$$

Since the greatest common divisor can be computed efficiently, this set is easy to build. If it is too small, we have to choose a different prime q.
Assume now that $q = p^n$ for a prime p. For small primes, it is easy to achieve a set $\mathcal{B}(\mathbb{F}_p)$ which is almost as large as $\mathcal{B}'$. Then we can choose an exponent $n \in \mathbb{N}$ such that $|\mathcal{B}(\mathbb{F}_p)| \leq 2|\mathcal{B}(\mathbb{F}_q)|$. Indeed, for an initial choice n_0, we have

$$\begin{aligned}\gcd(p^{n_0} - 1, p^{n_0+1} - 1) &= \gcd(p^{n_0} - 1, p^{n_0+1} - p^{n_0}) \\ &= \gcd(p^{n_0} - 1, p(p-1)) \\ &= \gcd(p^{n_0} - 1, p - 1),\end{aligned}$$

thus any divisor of $p^{n_0} - 1$ that is divisible by some $b \in \mathcal{B}(\mathbb{F}_p)$ can not be a divisor of $p^{n_0-1} - 1$ and vice versa. In the worst case, such divisors are evenly distributed, and we can choose $n \in \{n_o, n_o + 1\}$ and $q = p^n$ such that $|\mathcal{B}(\mathbb{F}_q)| = \frac{1}{2}|\mathcal{B}(\mathbb{F}_q)|$.

When we choose q to be a large prime, we may choose different polynomials A and B in Algorithm 2.

Proposition 5.3.5. *Let p be a prime and $q = p^k$ for some $k \in \mathbb{N}$. Further let $P \in \mathbb{Z}[X]$ be the irreducible polynomial*

$$P = X^n + \lambda_{n-1}X^{n-1} + \cdots + \lambda_1 X + \lambda_0$$

with $n < p$. Assume that P has no multiple roots over $\mathbb{C}$ and that $\bar{P} \equiv P \mod q$ has no multiple roots over $\mathbb{F}_q^*$. Let $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ be the roots of P, and define the multivariate polynomial

$$N_P := \prod_{i=1}^{n} (X_1 + \alpha_i X_2 + \alpha_i^2 X_3 + \cdots + \alpha_i^{n-1} X_n).$$

Then N_P is a homogeneous polynomial in $\mathbb{Z}[X_1, \dots, X_n]$ of degree n, and

$$\bar{N}_P(X_1, X_2, 0, \dots, 0) \equiv N_P(X_1, X_2, 0, \dots, 0) \mod q$$

has no multiple roots in $(\mathbb{F}_q^*)^2$.

Proof. The degree of N_P and the fact that it is homogeneous follow immediately from the definition. So we first show that N_P is an integral polynomial. Let $M = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ and let $\mathcal{O}_M$ be the ring of integers of M. For all $\sigma \in \mathsf{Gal}(M/\mathbb{Q})$, we have

$$\sigma\left(\prod_{i=1}^{n} (X_1 + \alpha_i X_2 + \cdots + \alpha_i^{n-1} X_n)\right) = \prod_{i=1}^{n} (X_1 + \sigma(\alpha_i) X_2 + \cdots + \sigma(\alpha_i)^{n-1} X_n)$$

and thus $\sigma(N_P) = N_P$, since σ only permutes the factors in the product. Therefore we have $N_P \in \mathbb{Q}[X_1, \dots, X_n]$. Moreover, $N_P \in \mathcal{O}_M[X_1, \dots, X_n]$ and thus N_P is integral since $\mathbb{Z}$ is integrally closed.
Next we have

$$\begin{aligned}
&N_P(X_1, X_2, 0, \dots, 0) = \prod_{i=0}^{n}(X_1 + \alpha_i X_2) = \\
&= X_1^n + X_1^{n-1}X_2 \left(\sum_{1 \le j \le n} \alpha_j \right) + \dots + X_1 X_2^{n-1} \left(\sum_{1 \le j_1 \le \dots \le j_{n-1} \le n} \alpha_{j_1} \cdots \alpha_{j_{n-1}} \right) + X_2^n \prod_{i=1}^{n} \alpha_i \\
&= X_1^n + X_1^{n-1}X_2\lambda_{n-1} + \dots + X_1 X_2^{n-1}\lambda_1 + X_2^n \lambda_0 \in \mathbb{Z}[X_1, \dots, X_n].
\end{aligned}$$

Assume that for $(a, b) \in (\mathbb{F}_q^*)^2$ we have

$$N_P(a, b, 0, \dots, 0) \equiv b^{n-1}\bar{P}\left(\frac{a}{b}\right) \equiv 0 \mod p.$$

Then, since $b \in \mathbb{F}_q^*$, $\bar{P}\left(\frac{a}{b}\right) \equiv 0 \mod p$. Now

$$\frac{\partial}{\partial X_1} \left(\prod_{i=1}^{n}(X_1 + \alpha_i X_2) \right) \Bigg|_{X_1 = a, X_2 = b} \equiv b^{n-1}\bar{P}'\left(\frac{a}{b}\right) \mod p,$$

and this can not be equal to 0, since $\bar{P}$ has no multiple roots. □

Let now $M = \mathbb{Q}(\alpha_1)$, where α_1 is defined as above. A polynomial as defined above is called norm form, since it is strongly related to the norm function of an algebraic number field. For $x = x_1 + \alpha_1 x_2 + \dots + \alpha_1^{n-1} x_n$ we have $x \in \mathbb{Z}[\alpha_1]$, and thus for the norm we have $\mathcal{N}_{M/\mathbb{Q}} \in \mathbb{Z}$. Moreover, we have

$$\begin{aligned}
\mathcal{N}_{M/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x) &= \prod_{i=1}^{n}(x_1 + \sigma_i(\alpha_1)x_2 + \sigma_i(\alpha_1)^2 x_3 + \dots + \sigma_i(\alpha_1)^{n-1} x_n) \\
&= \prod_{i=1}^{n}(x_1 + \alpha_i x_2 + \alpha_i^2 x_3 + \dots + \alpha_i^{n-1} x_n).
\end{aligned}$$

Every n-tuple $(x_1, \dots, x_n)$ corresponds uniquely to some $x \in \mathbb{Z}[\alpha_1]$ by setting $x = x_1 + \alpha_1 x_2 + \dots + \alpha_1^{n-1} x_n$. Thus, for every $(x_1, \dots, x_n) \in \mathbb{Z}^n$ we have

$$N_P(x_1, \dots, x_n) = \mathcal{N}_{M/\mathbb{Q}}(x) \in \mathbb{Z}.$$

With Proposition 5.3.5, we can find polynomials A and B satisfying the requirements of Theorem 3.4.1. By choosing polynomials P and Q, such that $\bar{Q}$ has no multiple roots and such that $\deg P < \deg Q < \left(\frac{q}{5}\right)^{3/13}$, we can set $A = N_P$ and $B = N_Q$.

5.3.3 Choosing a, b and h over $\mathbb{F}_q$

We want to fix $r \in \mathbb{N}$ such that the size of the finite field $\mathbb{F}_q$, $q = 2^r$ is large enough for the security of the key agreement protocol. By having $r \geq 127$, Theorem 5.3.3 ensures that the polynomial which is output by Algorithm 2 is a Diophantine equation which can be used as a public key. In chapter 5.2, we already concluded that $\mathcal{B}$ has to be a small positive integer. In the case of finite fields, we can abandon the bound $\mathcal{M}$ and choose $a_1, \ldots, a_m \in \mathbb{F}_q^*$. This way an adversary has no chance of obtaining the secret s with methods like we will discuss in section 5.4.1. To choose the representative h of h' in $\mathbb{F}_q[X_1, \ldots, X_n]/(f)$, we can choose some $V \in \mathbb{F}_q[X_1, \ldots, X_n]$ randomly with $1 \leq \deg V \leq \deg f$ and set $h = h' + Vf$.

5.4 The Protocol over $\mathbb{Z}$

It is well-known that the function $T_b : \mathbb{Z}[X] \to \mathbb{Z}[X], X \mapsto X^b$ is invertible if and only if b is odd. This means that $\mathcal{B}$ is some positive odd integer, $\mathcal{B}(\mathbb{Z}) = \{3, 5, \ldots, \mathcal{B}\}$ and clearly $|\mathcal{B}(\mathbb{Z})| = (\mathcal{B} - 1)/2$.

5.4.1 Security over $\mathbb{Z}$

Assume that we have given the equation

$$X_m^{b_m} = u,$$

with known $u \in \mathbb{Z}$ and unknowns $X_m \in \mathbb{Z}$, $b_m \in \mathbb{N}$, b_m odd, and assume we know that there exists at least one solution to this equation. By [4] (and assuming that $|u| > 16$), we can use a perfect-power classification algorithm to compute some $\bar{X}$ and $\bar{b}$ in $(\log |u|) \exp \mathcal{O}(\sqrt{\log \log |u| \log \log \log |u|})$ steps such that

$$\bar{X}^{\bar{b}} = u. \tag{5.14}$$

By Proposition 5.4.1, we can ensure that $\bar{b}$ is an odd integer by factoring out a maximal power of 2 and raising $\bar{X}$ by the same power. This allows us to uniquely compute $u' := u^{1/b_m}$. Now assume that $(f, \mathbf{r}, g, h, \mathbf{a}, \mathbf{b})$ are the parameters of a given protocol run. From equations (5.3) and (5.2) we can deduce that

$$(\ldots(s + a_1)^{b_1} + a_2)^{b_2} + \cdots)^{b_{m-1}} + a_m)^{b_m} = u. \tag{5.15}$$

Comparing this with what we have computed above, we can write $\bar{X}$ as $(\ldots(s + a_1)^{b_1} + \cdots)^{b_{m-1}} + a_m)$, leading to a similar equation

$$X_{m-1}^{b_{m-1}} + a_m = u' \Leftrightarrow X_{m-1}^{b_{m-1}} = u' - a_m. \tag{5.16}$$

with $X_{m-1} = (\ldots(s + a_1)^{b_1} + \cdots)^{b_{m-2}} + a_{m-1})$.

Proposition 5.4.1. *Let $k \in \mathbb{N}$ and $k = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$ its prime decomposition. Then k is a perfect power if and only if $D := \gcd(\alpha_1, \ldots, \alpha_m) > 1$. Moreover, the positive integer solutions to the equation*

$$X^b = k$$

are given by

$$b = \frac{D}{d}, X = k^{d/D},$$

where d runs over all positive divisors of D.

Proof. First assume that $D > 1$. By setting $\bar{k} := p_1^{\alpha_1/D} \dots p_m^{\alpha_m/D} \in \mathbb{N}$ we can write $k = \bar{k}^D$, meaning that k is a perfect power. If $k = \bar{k}^a$ for some $k, a \in \mathbb{Z}$ and $a > 1$, then, by the uniqueness of the prime decomposition in $\mathbb{Z}$, $a | \alpha_i$ for $i \in \{1, \dots, m\}$ and thus $a | D$, so $D > 1$.

□

In Definition 5.2, we have introduced positive integers $\mathcal{M}$ and $\mathcal{B}$, such that $\mathcal{M}$ is the upper bound of the absolute values of the a_i, i.e. $|a_i| \leq \mathcal{M}$ for $i \in \{1, \dots, n\}$ and $\mathcal{B}$ is a bound for the b_j, $j \in \{1, \dots, m\}$. This means that equation (5.16) has only finitely many solutions. So let $\bar{X}_{m-1}$, $\bar{b}_{m-1}$, a_m be such a solution. Again $\bar{X}_{m-1}$ is of the form

$$\bar{X}_{m-1} = (\dots(s + a_1)^{b_1} + a_2)^{b_2} + \cdots)^{b_{m-1}} + a_{m-1} = X_{m-2}^{b_{m-2}} - a_{m-1}.$$

By iterating this method, we can deduce Algorithm 3.

Algorithm 3: Find all possible solutions to the nested equation $(\dots(s + a_1)^{b_1} + a_2)^{b_2} + \cdots)^{b_{m-1}} + a_m = u$ with bounds on the unknowns

```
Input   : $u \in \mathbb{Z}$, $m, \mathcal{B}, \mathcal{M} \in \mathbb{N}$
Output: An array containing all possible solutions

$j = 0$                                          /* global variable */
Findpairs$_{<m}$ (1,$u$,0)

Function Findpairs$_{<m}$($i$,$c$,$I$)
    for $b \in \{3,5,7,\dots,\mathcal{B}\}$ do
        $x_0 = \lfloor c^{1/b} \rfloor$
        $k = 0$
        $x_k^- = x_0$
        while $c - (x_k^-)^b < \mathcal{M}$ do
            $j = j + 1$
            $y_{(i,b,[I,j])} = c - (x_k^+)^b$
            $j = j + 1$
            $y_{(i,b,[I,j])} = c - (x_k^-)^b$
            if $i + 1 < m$ then
                Findpairs$_{<m}$($i + 1$,$x_k^+$,$j - 1$)
                Findpairs$_{<m}$($i + 1$,$x_k^-$,$j$)
            else
                Findpairs$_{=m}$($x_k^+$,$j - 1$)
                Findpairs$_{=m}$($x_k^-$,$j$)
            $k = k + 1$
            $x_k^+ = x_0 + k$
            $x_k^- = x_0 - k$

Function Findpairsn($c$, $I$)
    for $-\mathcal{M} \leq k \leq \mathcal{M}$ do
        $y_{(m,k,I)} = k$
        $s_{(k,I)} = c - k$
```

Theorem 5.4.2. *Algorithm 3 finds all solutions to the equation*

$$(\dots(s+a_1)^{b_1}+a_2)^{b_2}+\cdots)^{b_{m-1}}+a_m=u, \tag{5.17}$$

with $|a_i| \leq \mathcal{M}$ and $b_i \in \{3,5,\dots,\mathcal{B}\}$, $i \in \{1,\dots,m\}$ in at most $\mathcal{O}((2\mathcal{B}\sqrt[3]{\mathcal{M}})^m(1+2\mathcal{M}))$ steps.

Proof. By setting $X_1 := (\dots(s+a_1)^{b_1}+a_2)^{b_2}+\cdots+a_{m-1})$ we can write equation (5.17) as

$$X_1^{b_{m-1}}+a_m=u. \tag{5.18}$$

First, the algorithm executes $\mathsf{Findpairs}_{<m}(1,u,0)$, which finds all values for $X_1 \in \mathbb{Z}$ and $a_m \in \{-M,\dots,M\}$ solving (5.18) as follows: We successively choose an integer $b \in \{3,5,\dots,\mathcal{B}\}$ for the exponent, thus solving the equation for every possible b_{m-1}. Since we require $-\mathcal{M} < a_m < \mathcal{M}$ and $a_m = u - X_1^{b_{m-1}}$, we find all possible X_1 by setting $x_0 = \lfloor c^{1/b} \rfloor$ and finding all possible $x_k^{+,-} = x_0 \pm k$, $k \in \mathbb{Z}$ such that $-\mathcal{M} < u-(x_k^{+,-})^b < \mathcal{M}$. By writing $X_1 = X_2^{b_{m-2}} + a_{m-1}$, we can find solutions for X_2, b_{m-2} and a_{m-1} the same way as above, thus every solution for X_1 is a new input for a function $\mathsf{Findpairs}_{<m}(2, X_1, I)$. Hence, for all $i \in \{1,\dots,m-2\}$ we find solutions for $X_i = X_{i+1}^{b_{m-i-1}} + a_{m-i}$, and it takes $2\mathcal{M}$ steps for the function $\mathsf{Findpairs}_{=m}$ to find all s, a_1 with $X_{m-1} = s + a_1$. Now we need to bound the number of steps of the algorithm. By definition $x_0 = \lfloor c^{1/b} \rfloor \leq c^{1/b}$ and thus $c - x_0^b \geq 0$. This gives us a chain of $(c-(x_k^-)^b)$ with $k \in \{1,\dots,K\}$ such that K is maximal with $(c-(x_k^-)^b) < \mathcal{M}$:

$$\begin{aligned} 0 \leq (c-(x_0^-)^b) < (c-(x_1^-)^b) < \cdots < (c-(x_k^-)^b) < \mathcal{M} \Leftrightarrow \\ -c \leq -(x_0^-)^b < -(x_1^-)^b < \cdots < (x_k^-)^b < \mathcal{M} - c. \end{aligned}$$

Hence the number the **while** loop is executing is equal to $\sqrt[b]{\mathcal{M}-c} - \sqrt[b]{-c}$ and this is bounded from above by $2\sqrt[b]{M}$. Since $b \in \{3,5,\dots,\mathcal{B}\}$, we get an upper bound

$$2\sqrt[3]{\mathcal{M}} + 2\sqrt[5]{\mathcal{M}} + \cdots + 2\sqrt[\mathcal{B}]{\mathcal{M}} \leq \mathcal{B}\sqrt[3]{\mathcal{M}} \tag{5.19}$$

for the number of steps of a single $\mathsf{Findpairs}_{<m}$ function. Every $\mathsf{Findpairs}_{<m}$ calls again two $\mathsf{Findpairs}_{<m}$ and after $m-1$ nested calls $\mathsf{Findpairs}_{=m}$, this gives us at most

$$\begin{aligned} \sum_{i=0}^{m-1} (2\mathcal{B}\sqrt[3]{\mathcal{M}})^i + (2\mathcal{B}\sqrt[3]{\mathcal{M}})^m 2\mathcal{M} &= \frac{(2\mathcal{B}\sqrt[3]{\mathcal{M}})^m - 1}{2\mathcal{B}\sqrt[3]{\mathcal{M}} - 1} + (2\mathcal{B}\sqrt[3]{\mathcal{M}})^m 2\mathcal{M} \\ &< (2\mathcal{B}\sqrt[3]{\mathcal{M}})^m (1+2\mathcal{M}) \end{aligned}$$

many steps. □

First of all, note that Algorithm 3 finds in fact the secret s, meaning that the knowledge of the parameters **a** and **b** is obsolete for breaking the protocol. If the $y_{(i,b,[I_1,I_2])}$ are stored, however, a solution to (5.15) can be given as follows: Choose some $(b_1,\dots,b_{m-1}) \in (\mathcal{B}(R))^{m-1}$. Further choose indices $I_j \in \mathbb{N}$ and some $k \in [-\mathcal{M},\mathcal{M}]$ such that the elements of

$$\mathbf{y} := (y_{(1,b_{m-1},[I_1,I_2])}, y_{(2,b_{m-2},[I_2,I_3])}, \dots, y_{(m-2,b_{m-1},[I_{m-2},I_{m-1}])}, y_{(m-1,b_{m-2},[I_{m-1},I_m])}, y_{(m,k,I_m)})$$

are in the output of Algorithm 3. Then the chosen b_i together with $\mathbf{a} = \mathbf{y}$ form a solution.
A disadvantage that the algorithm suffers is that the runtime depends on the knowledge of m. If m is known, it can be executed as above, leading to as many as $\mathcal{O}((2\mathcal{B}\sqrt[3]{\mathcal{M}})^m(1+2\mathcal{M}))$ solutions to equation (5.15). If m is not known, an adversary has to run the algorithm above for every $\hat{m} \leq m$ and then check for all such $\hat{m}$, if the result matches the parameters of the protocol.

Any perfect power with odd exponent in the interval $[u-\mathcal{M}, u+\mathcal{M}]$ is a solution to (5.16). If Algorithm 3 would be set not to loop over all $b \in \mathcal{B}(R)$ but over perfect powers in this interval, the runtime would be asymptotically the same, as we can see in Proposition 5.4.3. This also shows that the upper bound in (5.19) could instead be estimated asymptotically as $2\sqrt[3]{\mathcal{M}}$. The proof of the following proposition is a modification of the proof of [31, Theorem 1].

Proposition 5.4.3. *Let $u \in \mathbb{Z}$, $K \in \mathbb{N}$ and define*

$$P(u,K) = \{x \in [u-K, u+K] \mid x \text{ is a perfect power with odd exponent } e \leq \mathcal{B}\}.$$

Then $|P(u,K)| \approx \sqrt[3]{u+K} - \sqrt[3]{u-K} \leq 2\sqrt[3]{K}$.

Proof. Let $N_3^{\mathcal{B}}(x)$ denote the set of perfect powers less than or equal to x, where the exponent is odd and at most $\mathcal{B}$. It suffices to show that $|N_3^{\mathcal{B}}(x)| \approx \sqrt[3]{x}$. Since we can easily compute the exact size of $N_3^{\mathcal{B}}(x)$ for small x, we can assume that $\mathcal{B} \geq 3$ and $x \geq 8$. Next, we define the sets $A_n(x) := \{k^n \mid k \in \mathbb{N}, k^n \leq x\}$ for $n \in \mathbb{N}$ and set $M := \lfloor \log_2 x \rfloor - [\lfloor \log_2 x \rfloor \text{ is even}]$, where $[\cdot]$ is the Iverson bracket, cf. [16]. Then $2^M \in A_M(x)$ and $2^{M+1} \notin A_{M+1}(x)$ because $2^{M+1} > x$, so

$$M' := \max\{m \in \mathbb{N} \mid \emptyset \neq A_m(x) \subseteq N_3^{\mathcal{B}}(x)\} = \begin{cases} M, & \text{if } M < \mathcal{B} \\ \mathcal{B}, & \text{if } M \geq \mathcal{B}. \end{cases}$$

The elements of $N_3^{\mathcal{B}}(x)$ are all in some $A_n(x)$ for $n \in \{1, \dots, M'\}$, hence

$$N_3^{\mathcal{B}}(x) = \bigcup_{\substack{n=3,\\ n \text{ odd}}}^{M'} A_n(x). \tag{5.20}$$

Any set $A_n(x)$ contains $\lfloor \sqrt[n]{x} \rfloor$ elements, so with the assumption that $\mathcal{B} \geq 3$ and the fact that the union in (5.20) is in general not disjoint we get

$$\lfloor \sqrt[3]{x} \rfloor = A_3(x) \leq N_3^{\mathcal{B}}(x) \leq \sum_{\substack{n=3,\\ n \text{ odd}}}^{M'} \lfloor \sqrt[n]{x} \rfloor. \tag{5.21}$$

Now we can bound the sum on the right-hand side of (5.21) as follows:

$$\sum_{\substack{n=3,\\ n \text{ odd}}}^{M'} \lfloor \sqrt[n]{x} \rfloor \leq \lfloor \sqrt[3]{x} \rfloor + \sum_{n=4}^{M} \lfloor \sqrt[n]{x} \rfloor \leq \lfloor \sqrt[3]{x} \rfloor + \sum_{n=4}^{M} \sqrt[4]{x} \leq \lfloor \sqrt[3]{x} \rfloor + \sqrt[4]{x}(M-2),$$

and by L'Hospitals rule we get

$$1 \xleftarrow{x\to\infty} \frac{\lfloor\sqrt[3]{x}\rfloor}{\sqrt[3]{x}} \leq \frac{N_3^{\mathcal{B}}(x)}{\sqrt[3]{x}} \leq \frac{\lfloor\sqrt[3]{x}\rfloor}{\sqrt[3]{x}} + \frac{\sqrt[4]{x}(M-2)}{\sqrt[3]{x}} < \frac{\lfloor\sqrt[3]{x}\rfloor}{\sqrt[3]{x}} + \frac{\log_2 x}{\sqrt[12]{x}} \xrightarrow{x\to\infty} 1,$$

hence $N_3^{\mathcal{B}}(x) \to \sqrt[3]{x}$ for $x \to \infty$.

□

5.4.2 Choosing a Diagonal Polynomial

In order to make the protocol in chapter 5.1 secure, the polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$ has to be chosen such that $f = 0$ is hard to solve. Other than that, an efficient way for calculating a solution $\mathbf{r} \in \mathbb{Z}^n$ when defining the polynomial in the first step of the key-exchange is required, as well as a representation of the polynomial with feasible bit length in respect of an implementation. For all this, Hirata-Kohno and Pethő suggest to choose a diagonal polynomial of the form

$$f = c_1 X_1^{d_1} + \ldots + c_n X_n^{d_n} + c_0, \tag{5.22}$$

with $d_1, \ldots, d_n \geq 2$.

Algorithm 4: Construct a diagonal polynomial f and an $\mathbf{r} \in \mathbb{Z}^n$ with $f(r) = 0$.

```
     Input  : $v, M \in \mathbb{N}$
 1   Choose $d_1 \in \{2, \ldots, M\}$
 2   for $2 \leq i \leq n$ do
 3       Choose $d_i \in \{d_{i-1}, \ldots, M\}$
 4   Choose $r'_i \in \{-2^v, \ldots, 2^v\}$ for $\{1, \ldots, n\}$
 5   if $(r'_1, \ldots, r'_n) = \mathbf{0}$ then
 6       go to 4
 7   Choose $c_{m+1} \in \{-2^v, \ldots, 2^v\} \setminus \{0\}$
 8   $d = \gcd(r'_1, \ldots, r'_n)$
 9   Set $r_i = \frac{r'_i}{d}$ for $\{1, \ldots, n\}$
10   $\mathbf{R} = (r_1^{d_1}, \ldots, r_n^{d_n})^t$
11   Let $\mathbf{y_i} \in \mathbb{Z}^n, i \in \{0, \ldots, n\}$ with $(\mathbf{y_0}^t + q'_1\mathbf{y_1}^t + \cdots + q'_n\mathbf{y_n}^t)\mathbf{R} = c_{m+1}$
         for any $q'_i \in \mathbb{Z}$ for $\{1, \ldots, n\}$
12   Choose $q_i \in \mathbb{Z}$ for $\{1, \ldots, n\}$
13   $(c_1, \ldots, c_m) = \mathbf{y_0}^t + q_1\mathbf{y_1}^t + \cdots + q_n\mathbf{y_n}^t$
14   $\mathbf{r} = (r_1, \ldots, r_n)$
15   $f = c_1 X_1^{d_1} + \ldots + c_n X_n^{d_n} + c_{m+1}$
```

The idea of Algorithm 4 is to set the exponents and to choose a solution for the diagonal polynomial in a certain way, then use the solvability of linear Diophantine equations to compute the coefficients for f. The way this is done, there are infinitely many n-tuples of coefficients for fixed exponents and $\mathbf{r}$ with $f(\mathbf{r}) = 0$.

Lemma 5.4.4. *Let $f \in \mathbb{Z}[X_1, \dots, X_n]$ be given by*

$$f = c_1X_1 + c_2X_2 + \cdots + c_nX_n$$

with $c_i \neq 0$ for all $i \in \{1, \dots, n\}$ and let $c_0 \in \mathbb{Z} \setminus \{0\}$. Then the Diophantine equation $f - c_0 = 0$ is solvable if and only if $\gcd(c_1, \dots, c_n) | c_0$.

Proof. Let $d = \gcd(c_1, \dots, c_n)$. First, assume that that there are some $a_1, \dots, a_n \in \mathbb{Z}$ with

$$c_1a_1 + \cdots + c_na_n = c_0.$$

Then $d | c_1a_1 + \cdots + c_na_n$ and thus $d|c_0$. For the other direction, assume now that $d|c_0$. We claim that there exist some $a'_1, \dots, a'_n \in \mathbb{Z}$ such that

$$c_1a'_1 + \cdots + c_na'_n = d.$$

We prove this by induction on n. For $n = 2$ the lemma follows from the well-known Euclidean algorithm. So assume that $n > 2$ and let $d' = \gcd(c_1, \dots c_{n-1})$. By the induction hypothesis there are some $a''_1, \dots, a''_n \in \mathbb{Z}$ with

$$c_1a''_1 + \cdots + c_{n-1}a''_{n-1} = d'.$$

Since

$$d = \gcd(c_1, \dots, c_n) = \gcd(\gcd(c_1, \dots c_{n-1}), c_n),$$

there are some $a, b \in \mathbb{Z}$ with

$$d = ad' + bc_n = a(c_1a''_1 + \cdots + c_{n-1}a''_{n-1}) + bc_n,$$

hence our claim is proved. By multiplying $\frac{c_0}{d} \in \mathbb{Z}$ to (15), we obtain some $a_1, \dots, a_n \in \mathbb{Z}$ with

$$c_1a_1 + \cdots + c_na_n = c_0.$$

□

Theorem 5.4.5. *Algorithm 4 finds a pair $(f, \mathbf{r})$ with*

$$f = c_1X_1^{d_1} + \ldots + c_nX_n^{d_n} + c_0 \in \mathbb{Z}[X_1, \dots, X_n]$$

and $f(\mathbf{r})$ in polynomial time.

Proof. We start the proof by noting that the term 'Choose' in Algorithm 4 stands for a choice at random. At the start of the algorithm we choose the exponents d_i such that $2 \leq d_1 \leq \ldots \leq d_n \leq M$. Further we fix $c_{m+1}, r'_1, \dots, r'_n$ for some given bound. The if-statement in line 5 ensures that $0 \neq d = \gcd(r'_1, \dots, r'_n)$. Since $r_1, \dots, r_n$ are set such that $\gcd(r_1, \dots, r_n) = 1$ we have $\gcd(r_1^{d_1}, \dots, r_n^{d_n}) = 1$, hence the linear Diophantine equation

$$c_0 = c_1r_1^{d_1} + \cdots + c_1r_n^{d_n} \tag{5.23}$$

is solvable by Lemma 5.4.4. For solving this equation in polynomial time, we can use an algorithm introduced in [10], giving us $\mathbf{y_0}, \dots, \mathbf{y_n} \in \mathbb{Z}^n$ such that

$$(\mathbf{y_0}^t + q_1\mathbf{y_1}^t + \cdots + q_n\mathbf{y_n}^t) \begin{pmatrix} r_1^{d_1} \\ \vdots \\ r_n^{d_n} \end{pmatrix} = c_{m+1}$$

for any $q_1 \dots, q_n \in \mathbb{Z}$. By fixing the q_i we can set $(c_1, \dots, c_m) = \mathbf{y_0}^t + q_1\mathbf{y_1}^t + \cdots + q_n\mathbf{y_n}^t$ and hence we have both f and $\mathbf{r}$ with $f(\mathbf{r}) = 0$. □

Special cases of the Diophantine equation of diagonal form (5.22) have been studied extensively. First consider equations of the form $X_j^2 + C = X_i^n$, which have only finitely many solutions. In fact, for any C there is a computable $K(C)$ bounding all possible values for X_j. In practice, however, this bound is too large to solve the equation in a feasible amount of time by considering all X_j in this bound. Another special case of (5.22) is given by $X_j^2 + c_i X_i^2 = m$. This equation has infinitely many solutions. It is the Diophantine equation the OSS-Scheme in 4.1 is built on, and as we have seen, it can be solved quickly. However, unlike in the case of the OSS-scheme, only the solution $\mathbf{r}$ or m different solutions would break the protocol, as we have seen in Proposition 5.2.3, so we need control on the solutions of the equation $X_j^2 + c_i X_i^2 = m$. The fastest known way of finding a general solution is only pseudo-polynomial in c_i. In fact, if we set $c_1 = 1, c_2 = -1$, input any values for X_k for $k > 2$ and set $d_1 = d_2 = 2$, the resulting equation is of the form $X_1^2 - X_2^2 = n$. Finding solutions to this is as hard as factoring n.

By Kerckhoffs principle, it is safe to assume that an attacker knows that the solution $\mathbf{r}$ to $f = 0$ fulfills $\gcd \mathbf{r} = 1$. To avoid a brute force attack, i.e. test whether

$$c_1 r_1^{d_1} + \cdots + c_1 r_n^{d_n} - c_0 = 0$$

for all possible $\mathbf{r}$ with $|r_i| \leq 2^{v/d_i}$, we need to choose v larger than a certain bound.

Proposition 5.4.6. *Let $d_1, \dots, d_n, v \in \mathbb{N}$ with $d_j = \min_k d_k$ and $d_i = \max_k d_k$. The number of n-tuples $(r_1, \dots, r_n) \in \mathbb{Z}^n$ such that $\gcd(r_1, \dots, r_n) = 1$ and $|r_i|^{d_i} \leq 2^v$ for all $i \in \{1, \dots, n\}$ is in the interval*

$$\left[\frac{2^{\frac{n(v+1)}{d_i}}}{\zeta(n)}, \frac{2^{\frac{(n+1)v}{d_j}}}{\zeta(n)} + \mathcal{O}(2^{\frac{(n-1)v+n}{d_j}}) \right].$$

Proof. By the lemma in [32, page 1], the number $Z_k(t)$ of k-tuples $\mathbf{v} \in \{1, \dots, t\}^k$ such that $\gcd \mathbf{v} = 1$ is given by $t^k/\zeta(k) + \mathcal{O}(t^{k-1})$. We denote by $Z(\chi_1, \dots, \chi_n)$ the number of all all n-tuples $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{Z}^n$ with $\gcd \boldsymbol{v} = 1$ and $1 \leq v_i \leq \chi_i$ if $\chi_i \geq 0$ and $\chi_i \leq v_i \leq 0$ otherwise for all $i \in \{1, \dots, n\}$. Then

$$\frac{2^{\frac{nv}{d_i}}}{\zeta(n)} \leq Z\left(2^{\frac{v}{d_i}}, \dots, 2^{\frac{v}{d_i}}\right) \leq Z\left(2^{\frac{v}{d_1}}, \dots, 2^{\frac{v}{d_m}}\right) \leq Z\left(2^{\frac{v}{d_j}}, \dots, 2^{\frac{v}{d_j}}\right) \leq \frac{2^{\frac{nv}{d_j}}}{\zeta(n)} + \mathcal{O}(2^{\frac{(n-1)v}{d_j}}).$$

Next we consider $\hat{Z}_k(t)$, by which we denote the number of k-tuples $\mathbf{v} \in \{-t, \dots, t\}^k$ such that $\gcd \mathbf{v} = 1$. By the symmetry of the greatest common divisor, we have

$$\hat{Z}_n(t) = \sum_{\chi_1, \dots, \chi_n \in \{-t, t\}} Z(\chi_1, \dots, \chi_n) = \sum_{l=0}^{n} \binom{n}{l} Z_n(t) = 2^n Z_n(t),$$

since the cases where any number of $v_i = 0$ adds to the $\mathcal{O}(t^{n-1})$ term of $Z_n(t)$. Replacing Z with $\hat{Z}$ as we have replaced Z_k with $\hat{Z}_k$ leads to the desired result: Let $\hat{Z}(\chi_1, \dots, \chi_n)$ be the number of n-tuples $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{Z}^n$ with $\gcd v = 1$ and $|v_i| \leq \chi_i$ for all $i \in \{1, \dots, n\}$. Then

$$2^n Z_n\left(2^{\frac{v}{d_i}}\right) \leq Z\left(2^{\frac{v}{d_1}}, \dots, 2^{\frac{v}{d_m}}\right) \leq 2^n Z_n\left(2^{\frac{v}{d_j}}\right).$$

□

To avoid an attack, v has to be chosen such that the number of possibilities for $(r_1, \dots, r_n)$ is at least 2^{128}. By the proposition above, this means that

$$\frac{2^{\frac{n(v+1)}{d_i}}}{\zeta(n)} \geq 2^{128} \Leftrightarrow v \geq \frac{d_j}{n}(128 + \log_2(\zeta(n))) - 1,$$

where $0 < d_j = \max(d_1, \dots, d_n)$. Further, Hirata and Pethő suggest to choose the d_i to be small, namely $d_i \leq 7$. To omit trivial cases for f, we also require that $d_i \geq 2$ for all $i \in \{1, \dots, n\}$.

5.4.3 The Diagonal Polynomial is Irreducible

Let f be the diagonal polynomial from the previous section, and assume that f is primitive, such that there is some $k \in \{1, \dots, n\}$ with

$$d = \gcd(c_1, \dots, c_{k-1}, c_{k+1}, \dots, c_n, c_0) = 1.$$

If f is not of this form, we can change two coefficients of f in order to bring it to this form. Indeed, since $\gcd(r_1, \dots, r_n) = 1$, there is some r_j such that $d \nmid r_j$. For a fixed $i \in \{1, \dots, n\}$, setting

$$c_l = \begin{cases} c_l + k r_j^{d_j} & : l = i \\ c_l - k r_i^{d_i} & : l = j \\ c_l & : l \in \{1, \dots, n\} \setminus \{i, j\} \end{cases}$$

for some $k \in \mathbb{Z} \setminus \{0\}$ still solves the equation (5.23), so this again gives a valid diagonal polynomial.

With the assumption above, we can therefore show that f is in fact irreducible over $\mathbb{Z}$, excluding trivial attacks on the protocol by factoring f into smaller factors which may be easy to solve. To show irreducibility of f, we use the following proposition, which states a well-known fact about irreducibility:

Proposition 5.4.7. *Let K be a field and $n \in \mathbb{N}$ with $n \geq 2$. Further let $a \in K^*$. Assume that for all prime numbers p with $p|n$ we have $a \notin K^p$, and if $4|n$ we have $a \notin -4K^4$. Then*

$$X^n - a \in K[X]$$

is irreducible over K.

Next we are going to need the following lemma:

Lemma 5.4.8. *Let $c_0, c_1, \ldots, c_k \in \mathbb{Z} \setminus \{0\}$ and let*

$$g = c_0 + c_1 X_1^{d_1} + \cdots + c_k X_k^{d_k} \in \mathbb{Z}[X_1, \ldots, X_k]$$

be primitive for some exponents $d_i \geq 2$, $i \in \{1, \ldots, k\}$. Then

$$g \notin (\mathbb{Q}(X_1, \ldots, X_k))^p \text{ and } g \notin -4(\mathbb{Q}(X_1, \ldots, X_k))^4$$

for all prime numbers p.

Proof. Since g is primitive, it suffices to show the lemma for $\mathbb{Z}[X_1, \ldots, X_k]$ instead of $\mathbb{Q}(X_1, \ldots, X_k)$. So for the sake of a contradiction, assume that there is a polynomial $h \in \mathbb{Z}[X_1, \ldots, X_k]$ such that $g = h^p$ for some prime p. As $c_1 \neq 0$, we have that $M := X_1^{d_1/p} \sqrt[p]{c_1}$ has to be a monomial appearing in h. Moreover, since $X_1^{d_1}$ is the highest X_1-term in g, M is the highest X_1-term in h. The constant term of g is not equal to zero, so the same has to hold for h. Let $0 \neq c = h(0)$. As $X_1^{d_1}$ is the only monomial in g divisible by X_1, M is the only monomial of h divisible by X_1. But then $pc^{p-1} X_1^{d_1/p} \sqrt[p]{c_1} \in \mathbb{Z}[X_1, \ldots, X_k]$ is a monomial of $h^p = g$, a contradiction. We can show that $g \notin -4(\mathbb{Z}[X_1, \ldots, X_k])^4$ along the same lines. □

The assumption that f is primitive and Gauss's lemma allow us to prove that f is irreducible.

Theorem 5.4.9. *Let*

$$f = c_1 X_1^{d_1} + \ldots + c_n X_n^{d_n} + c_0 \in \mathbb{Z}[X_1, \ldots, X_n]$$

be a polynomial that was constructed in Algorithm 4. Then f is irreducible over $\mathbb{Z}$.

Proof. By our initial assumption and if necesarry after renumbering, we can write f as $f = c_1 X_1^{d_1} + g$ for a primitive $g \in \mathbb{Z}[X_1, \ldots, X_n]$. By Gauss's lemma, we can work in $\mathbb{Q}(X_1, \ldots, X_n)$ and thus f is irreducible by Proposition 5.4.7 and Lemma 5.4.8. □

5.4.4 Choosing a Non-diagonal Diophantine Equation

In Algorithm 4, an initially chosen solution $\mathbf{r}$ leads to a diagonal Diophantine equation via solving the linear equation

$$c_1 r_1^{d_1} + \cdots + c_1 r_n^{d_n} = c_0$$

for known $d_1, \ldots, d_n$ and c_0. This can be done efficiently by a multidimensional extension of the Euclidean algorithm. We can extend this idea to a more general class of Diophantine equations. Again we start by choosing a solution $\mathbf{r} = (r_1, \ldots, r_n)$ with $\gcd(r_1, \ldots, r_n) = 1$ and some $c_0 \in \mathbb{Z} \setminus \{0\}$. For some given $N \in \mathbb{N}$, we want to find $d_{i,j} \in \mathbb{N}_0$ and $c_i \in \mathbb{Z}$ with $i \in \{1, \ldots, N\}$ and $j \in \{1, \ldots, n\}$, so that we can define an $f \in \mathbb{Z}[X_1, \ldots, X_n]$ with

$$f = c_0 + \sum_{i=1}^{N} c_i X_1^{d_{i,1}} \ldots X_n^{d_{i,n}} \tag{5.24}$$

and $f(\mathbf{r}) = 0$. We can do this the following way:

Since $\gcd(r_1, \ldots, r_n) = 1$, we can find some nonempty multisets $R_1, \ldots, R_K$ for $K \in \{2, \ldots, n\}$ such that

$$\begin{gathered} R_1 \cup \ldots \cup R_K = R \text{ and} \\ \gcd\big(\prod_{r \in R_1} r, \ldots, \prod_{r \in R_K} r\big) = 1, \end{gathered}$$

where R is the multiset $\{r_1, \ldots, r_n\}$. The union does not need to be disjoint. Then we can choose the exponents $d_{i,j} \in \mathbb{N}_0$ such that for every monomial $X_{i_1}^{\lambda_1} \cdots X_{i_K}^{\lambda_K}$ of f we have $r_{i_1}, \ldots, r_{i_k} \in R_j$ for some $j \in \{1, \ldots, K\}$. Moreover, for all $j \in \{1, \ldots, K\}$, there has to be a monomial $X_{i_1}^{\lambda_1} \cdots X_{i_k}^{\lambda_k}$ in f with $r_{i_1}, \ldots, r_{i_k} \in R_j$. With this exponents, the following proposition shows that we can choose the coefficients of f the same way as we did in the previous section:

Proposition 5.4.10. *Assume that $f \in \mathbb{Z}[X_1, \ldots, X_n]$ is given as above with $\mathbf{r} = (r_1, \ldots, r_n) \in \mathbb{Z}^n$ and $\gcd(r_1, \ldots, r_n) = 1$. Then*

$$\gcd\big(r_1^{d_{1,1}} \cdots r_n^{d_{1,n}}, r_1^{d_{2,1}} \cdots r_n^{d_{2,n}}, \ldots, r_1^{d_{N,1}} \cdots r_n^{d_{N,n}}\big) = 1.$$

Proof. Let $R' = \{r_1^{d_{1,1}} \cdots r_n^{d_{1,n}}, r_1^{d_{2,1}} \cdots r_n^{d_{2,n}}, \ldots, r_1^{d_{N,1}} \cdots r_n^{d_{N,n}}\}$. Further let $r := r_1^{d_{j,1}} \cdots r_n^{d_{j,n}} \in R'$ and let $r_{j_1}, \ldots, r_{j_l}$ be the factors of r with $d_{j,j_1}, \ldots, d_{j,j_l} \geq 1$. By the choice of the exponents as given above, we have $r_{j_1}, \ldots, r_{j_l} \in R_s$ for some $s \in \{1, \ldots, K\}$. This means that for every R_s, there is some $r_1^{d_{j,1}} \cdots r_n^{d_{j,n}} \in R'$ such that $r_1^{d_{j,1}} \cdots r_n^{d_{j,n}} \mid \prod_{r \in R_s} r^{d_{j,1} \cdots d_{j,n}}$. It follows that

$$\gcd\big(r_1^{d_{1,1}} \cdots r_n^{d_{1,n}}, \ldots, r_1^{d_{N,1}} \cdots r_n^{d_{N,n}}\big) \mid \gcd\big(\prod_{r \in R_1} r^{d_{1,1} \cdots d_{1,n}}, \ldots, \prod_{r \in R_K} r^{d_{N,1} \cdots d_{N,n}}\big) = 1.$$

proving the proposition. □

Thus by defining $\mathbf{r}_i := r_1^{d_{i,1}} \dots r_n^{d_{i,n}}$, we have the linear Diophantine equation

$$c_1\mathbf{r}_1 + \cdots + c_N\mathbf{r}_N + c_0 = 0 \tag{5.25}$$

in the unknowns $c_1, \dots, c_N$ which is easy to solve. As long as we have the monomials of f corresponding to $\mathbf{r}_1, \dots, \mathbf{r}_N$ as constructed above, we can add any amount of arbitrary terms. Assume that we want to add the polynomial $g \in \mathbb{Z}[X_1, \dots, X_n]$ to $f \in \mathbb{Z}[X_1, \dots, X_n, c_1, \dots, c_N]$. We can do this by setting

$$c_0^{\text{new}} := c_0 + g(r_1, \dots, r_n),$$

and solving equation (5.25) with c_0^{new} instead of c_0. The partitioning of the multiset R into $R_1, \dots, R_K$ is assumed to be easy to compute, since $K \leq n$ is a small integer.

It is even possible to extend the approach above of constructing a Diophantine equation from a given solution to polynomials without a constant term. To see this, let $\mathbf{r} = (r_1, \dots, r_n) \in \mathbb{Z}^n$, such that for some $A, B_1, \dots, B_m \subseteq \{1, \dots, n\}$, $d_{k,l} \in \mathbb{N}_0$ with $k \in \{1, \dots, m+1\}$, $l \in \{1, \dots, n\}$ and

$$R_0 = \prod_{i \in A} r_i^{d_{0,i}}, R_j = \prod_{i \in B_j} r_i^{d_{j,i}} \qquad \text{for } j \in \{1, \dots, m\}$$

we have

$$\gcd(R_1, \dots, R_m) | R_0.$$

This allows us to find $c_0, c_1, \dots, c_m \in \mathbb{Z}$ with

$$c_0R_0 + c_1R_1 + \cdots + c_mR_m = 0.$$

Hence

$$c_0X_1^{d_{0,1}} \dots X_n^{d_{0,n}} + c_1X_1^{d_{1,1}} \dots X_n^{d_{1,n}} + \cdots + c_mX_1^{d_{m,1}} \dots X_n^{d_{m,n}} = 0 \tag{5.26}$$

is a Diophantine equation of the form $f = 0$ without constant term and $f(\mathbf{r}) = 0$. However, this equation is not wise to use in the cryptographic protocol, since we have established in section 5.2 that the knowledge of any solutions to the Diophantine equation $f = 0$ may decrease the security of the protocol. A trivial solution of (5.26) is always given by $(r_1, \dots, r_n) = \mathbf{0}$, and if f is not of the form $f = f' + g$, where g is a diagonal polynomial without constant term, than there are even infinitely many trivial solutions, which would break the protocol.

Comparing the general approach of a Diophantine equation $f = 0$ where f is given in (5.24) with the polynomial from the previous section, we see that the diagonal polynomial is a special case of this more general Diophantine equation with a very sparse representation. Other than that we have broader choice in equations and thus in public keys, by a weaker restriction on the number or structure of monomials.

5.4.5 Choosing a,b and h over $\mathbb{Z}$

Let $f = c_1X_1^{d_1} + \ldots + c_nX_n^{d_n} + c_0$ be the Diophantine equation for the key exchange protocol performed over the integers, as constructed in the previous section. We still need to define how to choose the other parameters and polynomials used in the protocol.

In 5.2 we established that the degree of h' is $\deg g b_1 \dots b_m$, meaning that the number of coefficients which are non-zero of the public key h is about $\mathcal{O}((\deg g \mathcal{B}^m)^n)$. This means that $\mathcal{B}, n$ and m have to be small integers, and g should be a linear or quadratic polynomial. Moreover, we have to expect that most of the coefficients of h have a size of about $\mathcal{M}^{b_1 \dots b_m}$. By Theorem 3 we can break the protocol in $\mathcal{O}((2\mathcal{B}\sqrt[3]{\mathcal{M}})^m(1+2\mathcal{M}))$. To counter this, the parameters $a_1, \dots, a_m$ should fulfill $|a_i| \geq 10^8$ for all $i \in \{1, \dots, m\}$ and hence $\mathcal{M} \geq 10^8$.

One way of choosing $h \equiv h' \mod f$ is to pick a polynomial $V \in \mathbb{Z}[X_1, \dots, X_n]$ at random and set $h = h' + Vf$. A very simple deterministic approach of computing a representative is the use of a pseudo-division algorithm for polynomials, as given by Knuth in [22].

Proposition 5.4.11. *Let R be a unique factorization domain, $u, v \in R[X]$ with*

$$u = u_m X^m + \dots + u_1 X + u_0, \quad v = v_n X^n + \dots + v_1 X + v_0$$

such that $v_n \neq 0$ and $m \geq n \geq 0$. Then there are unique polynomials q and r such that

$$v_n^{m-n+1} u = qv + r.$$

Now choose some $i \in \{1, \dots, n\}$ such that $\deg_{X_i} g \geq 1$, $\deg_{X_i} f \geq 1$ and note that $\tilde{R} := R[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n]$ is a unique factorization domain and $\tilde{R}[X_i] = R[X_1, \dots, X_n]$. We have $\deg_{X_i} f = d_i \leq 7$ and $k_i := \deg_{X_i} h' \geq (b_1 \dots b_m)$ so $k_i \geq d_i \geq 0$. With the above proposition, there are some $q, r \in R[X_1, \dots, X_n]$ such that

$$c_i^{k_i - d_i + 1} h' = qf + r \Leftrightarrow h' = qf + r - (c_i^{k_i - d_i + 1} - 1)h'$$

and thus $h' \equiv r - (c_i^{k_i - d_i + 1} - 1)h' \mod f$, where c_i is the leading coefficient of $h' \in \tilde{R}[X_i]$. The remainder r can be found with any polynomial division algorithm, since then factor v_n^{m-n+1} in the above proposition, which corresponds to $c_i^{k_i - d_i + 1}$, was chosen such that any division performed in such an algorithm stays within the chosen ring, thus in $\mathbb{Z}$. Both the deterministic and the random approach of choosing the representant $h \equiv h' \mod (f)$ can be done very fast. However, the random approach has the advantage of not adding any information about the structure of h. With the deterministic approach, an adversary could obtain more information in order to calculate any parameters which are kept secret.

5.4.6 An Example over $\mathbb{Z}$

As a first example, we use the smallest possible n, namely $n = 3$ and work over $\mathbb{Z}[X_1, X_2, X_3]$. Assume that Alice chooses some $\mathbf{r} = (9, 7, 5)$, $c_4 = 313$ and the exponents $(d_1, d_2, d_3) = (3, 5, 7)$. By Algorithm 4, the polynomial f is constructed by solving the linear Diophantine equation

$$c_1 9^3 + c_2 7^3 + c_3 5^7 = 313.$$

Since $\gcd \mathbf{r} = 1$, this equation has infinitely many solutions. Alice picks one such solution and thus retrieves $f \in \mathbb{Z}[X_1, X_2, X_3]$ with

$$\begin{aligned} f &= c_1 X_1^3 + c_2 X_2^3 + c_3 X_3^7 - c4, \\ c_1 &= 201,\ c_2 = 10042812,\ c_3 = -2160508. \end{aligned}$$

Bob selects a quadratic polynomial $g = X_1^2 + X_2 X_3 \in \mathbb{Z}[X_1, X_2, X_3]$. With the minimal choice for m and b_1, b_2, b_3 and the small a_1, a_2, a_3, which are clearly impractical to use in a protocol by Theorem 5.4.2 due to security reasons, he is given

$$\begin{aligned} m &= 3, \\ b_1 &= b_2 = b_3 = 3, \\ a_1 &= 131,\ a_2 = 250,\ a_3 = -19 \text{ and} \\ h' &= (((X_1^2 + X_2 X_3 + 131)^3 + 250)^3 - 19)^3 \end{aligned}$$

to compute $h \in \mathbb{Z}[X_1, X_2, X_3]/(f)$. With the fairly small parameters, h' is already very large. It is made up of 406 monomials, and the arithmetic mean of the coefficients is $5.44 \cdot 10^{54}$. The internal storage used for h' alone is 95.60 kilobytes in Mathematica. We set $h = h' + f$.

With the knowledge of g and h, Alice computes

$$\begin{aligned} s = g(9,7,5) &= 116, \\ u = h(9,7,5) &= 400758352336691378193916217914839 \\ &\quad\ 1228888425639437343836280702452 0. \end{aligned}$$

Finally, Bob can retrieve the secret s by computing

$$s = ((u^{1/3} + 19)^{1/3} - 250)^{1/3} - 131 = 116.$$

Taking into account the lower and upper bounds for all parameters established in section 5.4.5, we look at the size of parameters with larger f and a_i. Again, let $m = n = 3$. For the construction of f via Algorithm 4, a lower bound for v is given by

$$v \geq \frac{d_{\mathsf{max}}}{n}(128 + \log_2(\zeta(n))) - 1 = \frac{7}{3}(128 + \log_2(\zeta(3))) - 1 \approx 298.286,$$

so we choose $v = 299$. This gives the bounds

$$\begin{aligned} |r_1| \leq 2^{\frac{299}{3}} \approx 1.00 \cdot 10^{30},\ |r_2| \leq 2^{\frac{299}{5}} \approx 1.00 \cdot 10^{18}, \\ |r_3| \leq 2^{\frac{299}{7}} \approx 7.21 \cdot 10^{12},\ |c_4| \leq 2^{299} \approx 1.01 \cdot 10^{90}. \end{aligned}$$

So assume that Alice chooses coprime r_1, r_2, r_3 and c_4 with

$$\begin{aligned} r_1 &= 2145243202915256125330217571 55, \\ r_2 &= -907194993065307412, \\ r_3 &= -67353381470, \\ c_4 &= 412758574673874772. \end{aligned}$$

This leads again to infinitely many possible coefficients c_1, c_2, c_3. Alice selects such a tuple, and thus f is given by

$$\begin{aligned} f &= c_1 X_1^3 + c_2 X_2^3 + c_3 X_3^7 - c4, \\ c_1 &= -216075779524989596501529484579175432832572228, \\ c_2 &= -347162229807529816393497516153471869 1459421, \\ c_3 &= -478751726068037828369288275043894774920122 04. \end{aligned}$$

This choice of coefficients minimizes $|c_1| + |c_2| + |c_3|$, however it is a hard problem in general to find this minimum. For the choice of h', assume again that $b_1 = b_2 = b_3 = 3$ and use the same polynomial g. The minimal size for the a_i is given by 10^8, so let h' be given by

$$\begin{aligned} h' &= (((X_1^2 + X_2 X_3 + a_1)^3 + a_2)^3 - a_3)^3 \text{ with} \\ a_1 &= 38751531, \\ a_2 &= -849101056 \text{ and} \\ a_3 &= 26893070. \end{aligned}$$

Despite the increased size of the a_i, the internal storage used for h' by Mathematica is almost the same as before with 103.96 kilobytes.
The size of h' and thus h changes dramatically when m or n is increased. Indeed, as we have shown in 5.2, the degree of h' grows exponentially in n and m. So assume that $m = n = 4$ and let

$$\begin{aligned} g &= X_1^2 + X_2 X_3 + X_4, \\ h' &= (((g^3 + 250)^3 - 19)^3 - 77)^3. \end{aligned}$$

Then h' consists of 95284 monomials, and the internal storage of h' takes 29.27 megabytes.

6 Conclusions

The security of the key agreement protocol by Harry Yosh is based on the hardness of solving a system of higher degree Diophantine equations. Unlike with other cryptosystems based on Diophantine equations, Alice can choose the polynomial f fully arbitrarily. Although it is true that no general algorithm for solving such equations exist, there are many equations which are easy to solve. Hence the polynomial f must be chosen carefully, as it was done in 5.3.1 and 5.4.2.
Like in the Diffie-Hellman key exchange, both participants of the protocol are involved in setting the secret s, with Alice choosing an $\mathbf{r} \in R^n$ and Bob choosing some $g \in R[X_1, \ldots, X_n]$, resulting in $g(\mathbf{r}) = s$. However, they both need an extra step in exchanging the secret compared to other protocols, which is not only a disadvantage in efficiency, but also may cause a vulnerability of the security, since f, g, h and u are all publicly available.

The main drawback of the protocol is the amount of data that needs to be stored and transmitted. First consider the polynomial f. In 5.3.1, the polynomial is chosen to be of the form $f = A + B - \gamma$, where A and B are polynomials omitting to a sparse representation, however we cannot control the size of $\gamma \in \mathbb{F}_q$. In order to enable the hardness of solving the equation $f = 0$ when f is constructed to fulfill the requirements of 3.4.1, we need to choose $q \geq 2^{127}$.
Over the integers, by taking the sparse representation, the polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$ has only $n + 1$ many terms. However, the size of the coefficients may be very large, even with the use of [10] in Algorithm 4, which tries to keep the coefficients small.
Next we consider the polynomial h. As we have established in 5.2, the degree of h' is $tb_1 \ldots b_m$ and the number of non-zero coefficients is about $\mathcal{O}(t_1 \ldots t_n (b_1 \ldots b_m)^n)$, where $t = \deg g$ and $t_i = \deg_{X_i} g$ for all $i \in \{1, \ldots, n\}$. Hirata-Kohno and Pethő suggest to control the degree of one variable X_i through the choice of the representant h, in the best case however, this gives $\mathcal{O}(t_1 \ldots t_n (b_1 \ldots b_m)^{n-1})$ coefficients in h. Furthermore over the integers, small $a_1, \ldots, a_m$ would lead to insecurity, so they have to be chosen relatively large. For $\mathbf{a}$ as part of a protocol, assume that $a = \max\{|a_1|, \ldots, |a_m|\}$. We have to expect that most coefficients of h' have the size $a^{b_1 \cdots b_m}$. We set $a = 10^8$, $m = n = 3$, $b_1 = b_2 = b_3 = 3$ and $\deg_{X_i} g = 1$ for all $i \in \{1, \ldots, n\}$, corresponding to a minimal choice of the parameters. With this we still have to transmit about 1000 coefficients of the size 10^{72}.
Compared to other public key cryptosystems like RSA for key transmission or Diffie-Hellman, the number of steps which are needed to be performed in order to agree on a secret is fairly large as well. We can therefore say that, as long as key agreement protocols based on integer factorization or the discrete logarithm problem remain unbroken, the protocol by Harry Yosh provides a secure yet resource-intensive alternative.

Bibliography

[1] Sanjeev Arora and Boaz Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009 (cit. on p. 5).

[2] M. A. Asbullah and M. R. K. Ariffin. "Pre-conditions For Designing Asymmetric Cryptosystem Based On Diophantine Equation Hard Problem." In: 2012, pp. 198–203 (cit. on p. 53).

[3] A. Bérczes, J. Folláth, and A. Pethő. "On a family of collision-free functions." In: *Tatra Mountains Math. Publ.* 47.3 (2010), pp. 1–13 (cit. on p. 44).

[4] Daniel J. Bernstein. "Detecting Perfect Powers In Essentially Linear Time." In: *Math. Comp* 67 (1998), pp. 1253–1283 (cit. on p. 70).

[5] Antonio Cafure and Guillermo Matera. "Improved explicit estimates on the number of solutions of equations over a finite field." In: *Finite Fields and Their Applications* 12.2 (2006), pp. 155–185 (cit. on pp. 28, 35, 38).

[6] Henri Cohen. *Number theory. Volume I. , Tools and diophantine equations*. Graduate Texts in Mathematics. New York: Springer, 2007. ISBN: 978-0-387-49922-2.

[7] JHE Cohn. "The Diophantine equation $x^2 + C = y^n$." In: *Acta Arith* 65.4 (1993), pp. 367–381.

[8] Thomas W. Cusick. "Cryptanalysis of a Public Key System Based on Diophantine Equations." In: *Inf. Process. Lett.* 56.2 (Oct. 1995), pp. 73–75. ISSN: 0020-0190 (cit. on p. 52).

[9] Davis, Matijasevic, and Robinson. "Hilbert's Tenth Problem. Diophantine Equations: Positive Aspects of a Negative Solution." In: *Mathematical Developments Arising from Hilbert Problems, American Mathematical Society, 1976, 2 vols.* Vol. 2. 1976 (cit. on pp. 1, 3).

[10] Hamid Esmaeili. "Short solutions for a linear Diophantine equation." In: *Lecturas Matemáticas* 27 (2006), pp. 5–16 (cit. on pp. 76, 84).

[11] W. Fulton. *Algebraic curves: an introduction to algebraic geometry*. Advanced book classics. Addison-Wesley Pub. Co., Advanced Book Program, 1989 (cit. on pp. 33, 34).

[12] W. Fulton. *Intersection Theory*. Ergebnisse Der Mathematik Und Ihrer Grenzgebiete, 3. Folge, Bd. 2. Springer-Verlag GmbH, 1998 (cit. on p. 28).

[13] Shuhong Gao and Raymond Heindl. "Multivariate public key cryptosystems from diophantine equations." In: *Designs, Codes and Cryptography* 67.1 (2013), pp. 1–18 (cit. on p. 54).

[14] Michael R. Garey and David S. Johnson. *Computers and Intractability; A Guide to the Theory of NP-Completeness*. New York, NY, USA: W. H. Freeman & Co., 1990. ISBN: 0716710455 (cit. on p. 65).

[15] Andreas Gathmann. "Algebraic geometry." In: *University of Kaiserslautern* (2003).

[16] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. 2nd. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1994. ISBN: 0201558025 (cit. on p. 73).

[17] J. Heintz and C. P. Schnorr. "Testing Polynomials Which Are Easy to Compute (Extended Abstract)." In: *Proceedings of the Twelfth Annual ACM Symposium on Theory of Computing*. STOC '80. 1980, pp. 262–272 (cit. on p. 28).

[18] Noriko Hirata-Kohno and Attila Pethő. "On a key exchange protocol based on Diophantine equations." In: () (cit. on pp. 1, 58, 66).

[19] Ellis Horowitz and Sartaj Sahni. "The computation of powers of symbolic polynomials." In: *SIAM Journal on Computing* 4.2 (1975), pp. 201–208 (cit. on p. 63).

[20] James P Jones and YV Matuasevic. "Proof of Recursive Unsolvability of Hilbert's Tenth Problem." In: *American Mathematical Monthly* 98.8 (1991), pp. 689–709.

[21] Erich Kaltofen. "Effective Noether irreducibility forms and applications." In: *Journal of Computer and System Sciences* 50.2 (1995), pp. 274–295 (cit. on p. 38).

[22] Donald E. Knuth. *The Art of Computer Programming.* Vol. 2: *Seminumerical Algorithms*. 2nd ed. Addison-Wesley, Reading, Mass., 1988 (cit. on p. 81).

[23] D. Lazard. "Solving zero-dimensional algebraic systems." In: *Journal of Symbolic Computation* 13.2 (1992), pp. 117 –131 (cit. on p. 62).

[24] C. H. Lin et al. "A New Public-Key Cipher System Based Upon the Diophantine Equations." In: *IEEE Trans. Comp* 44 (1995), pp. 13–19 (cit. on p. 51).

[25] Yu. I. Manin. *A course in mathematical logic for mathematicians*. Second. Vol. 53. Graduate Texts in Mathematics. Springer, New York, 2010 (cit. on pp. 3, 7).

[26] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. *Handbook of Applied Cryptography*. 1st. Boca Raton, FL, USA: CRC Press, Inc., 1996. ISBN: 0849385237.

[27] L.J. Mordell. *Diophantine equations*. Pure and Applied Mathematics. Elsevier Science, 1969. ISBN: 9780080873428.

[28] Ariffin M. R. K., Asbullah M. A., and Abu N. A. *AA_β Public Key Cryptosystem – An Asymmetric Cryptosystem based on the Diophantine Equation Hard Problem*. [Online] Available as: `http://http://eprint.iacr.org/2011/467.pdf` (cit. on p. 54).

[29] David Naccache. "Can O.S.S. be Repaired? Proposal for a New Practical Signature Scheme." In: *Advances in Cryptology - EUROCRYPT '93*. Vol. 765. Lecture Notes in Computer Science. Springer, 1993, pp. 233–239 (cit. on p. 51).

[30] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer, 2006.

[31] MA Nyblom. "A counting function for the sequence of perfect powers." In: *Australian Mathematical Society Gazette* 33.5 (2006), pp. 338–343 (cit. on p. 73).

[32] J.E Nymann. "On the probability that k positive integers are relatively prime." In: *Journal of Number Theory* 4.5 (1972), pp. 469 –473 (cit. on p. 76).

[33] H. Ong, C. P. Schnorr, and A. Shamir. “An Efficient Signature Scheme Based on Quadratic Equations.” In: *Proceedings of the Sixteenth Annual ACM Symposium on Theory of Computing*. STOC ’84. New York, NY, USA: ACM, 1984, pp. 208–216 (cit. on p. 49).

[34] J Pollard and C Schnorr. “An efficient solution of the congruence $x^2 + ky^2 \equiv m \mod n$.” In: *Information Theory, IEEE Transactions on* 33.5 (1987), pp. 702–709 (cit. on p. 50).

[35] Hans Riesel. *Prime Numbers and Computer Methods for Factorization*. Cambridge, MA, USA: Birkhauser Boston Inc., 1985. ISBN: 0-8176-3291-3.

[36] Wolfgang M Schmidt. “A lower bound for the number of solutions of equations over finite fields.” In: *Journal of Number Theory* 6.6 (1974), pp. 448–480 (cit. on pp. 40, 42).

[37] Wolfgang M. Schmidt. *Equations over finite fields. An elementary approach*. Lecture Notes in Mathematics, Vol. 536. Springer-Verlag, Berlin-New York, 1976, pp. ix+276 (cit. on p. 35).

[38] T.N. Shorey and R. Tijdeman. *Exponential Diophantine Equations*. Cambridge Tracts in Mathematics. Cambridge University Press, 2008. ISBN: 9780521091701.

[39] Peter W Shor. “Algorithms for quantum computation: discrete logarithms and factoring.” In: *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*. IEEE. 1994, pp. 124–134 (cit. on p. 1).

[40] Robert I. Soare. *Recursively enumerable sets and degrees*. Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1987 (cit. on p. 7).

[41] André Weil. *Sur les courbes algébriques et les variétés qui s’en déduisent*. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948, pp. iv+85 (cit. on p. 34).

[42] Harry Yosh. “The key exchange cryptosystem used with higher order Diophantine equations.” In: *International Journal of Network Security & Its Applications* 3.2 (2011) (cit. on pp. iv, v, 1).