UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

STUDIES ON DEEP HOLES AND DISCRETE LOGARITHMS

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

DOCTOR OF PHILOSOPHY

By

JINCHENG ZHUANG
Norman, Oklahoma
2014

STUDIES ON DEEP HOLES AND DISCRETE LOGARITHMS

A DISSERTATION APPROVED FOR THE
SCHOOL OF COMPUTER SCIENCE

BY

Dr. Qi Cheng, Chair

Dr. Sudarshan Dhall

Dr. Changwook Kim

Dr. Ralf Schmidt

Dr. Krishnaiyan Thulasiraman

To my grandparents and parents.

Acknowledgements

It is with great encouragements and help from my advisor, teachers, friends and family that I have been able to accomplish the work in this dissertation.

First and formost, I wish to express my gratitude to my advisor, Professor Qi Cheng. I learned so much from him through discussions during classes, meetings, and lunch hours. His critical and creative instruction has cultivated my approach to research. His passion and determination has encouraged me to explore and work. His optimism and humour has affected me to enjoy work and life. His guidance and support has helped me to persist during all these years. He has been a fantastic professor, advisor and friend. I am grateful for having had the opportunity to work with him.

I also wish to thank my dissertation committee members: Professors Sudarshan Dhall, Changwook Kim, Ralf Schmidt, and Krishnaiyan Thulasiraman. They have given me valuable suggestions and comments in the general exam and during the revision of this dissertation. My thanks also go to the other faculty and staff in the school of computer science at OU. In addition, I would like to thank all my teachers and mentors along these years.

Parts of Chapter 3 are from joint work with Prof. Qi Cheng and Dr. Jiyou Li and previously appeared in [13]. Parts of Chapter 4 are from joint work with Prof. Qi Cheng and Prof. Daqing Wan and previously appeared

in [16]. It has been a pleasure to work with them. I want to thank them for helpful discussions. I would like to thank professor E. Thomé for informing me of the update of their paper. I want to thank my friends for their help during my graduate research. I also want to thank the staff in the OU Writing Center for the suggestions concerning the revision of this dissertation. Some experiments have been performed using Sage and PARI, I want to thank the developers of these software.

Last but not least, I am grateful to my family for their lasting love and support. In particular, I want to thank my grandparents, my parents and my sister.

Table of Contents

1 Introduction **1**
- 1.1 Error-correcting codes and deep holes for linear codes 2
- 1.2 Cryptography and discrete logarithms over finite fields 5

2 Background **8**
- 2.1 Basic field theory 8
- 2.2 Error-correcting codes 10
  - 2.2.1 Linear codes 10
  - 2.2.2 Generalized Reed-Solomon codes 14
- 2.3 Some results related to additive combinatorics 15
- 2.4 Cryptography 17
  - 2.4.1 Asymmetric cryptography 17
  - 2.4.2 The discrete logarithm problem over finite fields 18
- 2.5 Smoothness of integers and polynomials 18
- 2.6 Lattice theory 19
  - 2.6.1 Basic concepts 20
  - 2.6.2 Computational problems 22
  - 2.6.3 Lattices and groups 23

3 The Deep Hole Problem of Generalized Reed-Solomon Codes **25**
- 3.1 Statement of the problem 25
- 3.2 Related work 27
- 3.3 A criterion for deep holes of MDS codes 29
- 3.4 Classifying deep holes using deep hole trees 30
  - 3.4.1 Construction of the deep hole tree 30
  - 3.4.2 Some lemmas 37
  - 3.4.3 The main theorem and the proof 47

4 The Discrete Logarithm Problem over Finite Fields **51**
- 4.1 Statement of the problem 51
- 4.2 Related work 53
  - 4.2.1 Generic attacks 53
  - 4.2.2 Index calculus method 54

4.2.3 Number field sieve and function field sieve 59
4.2.4 Recent breakthroughs 60
4.3 Right cosets of $PGL_2(\mathbf{F}_q)$ in $PGL_2(\mathbf{F}_{q^2})$ 62
4.4 Where does the computation of the original BGJT algorithm really happen? 69
4.5 Finding primitive elements and discrete logarithms of linear factors 71
4.5.1 Using SNF of relation matrices to determine group structures 71
4.5.2 Finding the discrete logarithm of the linear factors . . 73
4.5.3 The tale of two lattices 77
4.5.4 Huang-Narayanan's method to determine primitive elements 85
4.5.5 Finding the discrete logarithms of linear polynomials by SNF 86
4.5.6 Examples 87
4.6 Traps to the original BGJT-algorithm and a solution 102
4.6.1 The trap to the QPA-descent 102
4.6.2 The trap-avoiding descent 105

5 Conclusions and future work **109**

A Discrete logarithms of elements in the factor base of $\mathbf{F}_{16^{22}}$ **118**

B Discrete logarithms of elements in the factor base of $\mathbf{F}_{16^{22}}$ with another base **123**

C Discrete logarithms of elements in the factor base of $\mathbf{F}_{16^{24}}$ **129**

D Table of $h_0(x)$ and $h_1(x)$ **138**

List of Tables

4.1 Modular exponentiation in $\mathbf{Z}/11\mathbf{Z}$ 52
4.2 Discrete logarithms in $\mathbf{Z}/11\mathbf{Z}$ 52
4.3 Modular exponentiation in $\mathbf{F}_{2^3}$ 52
4.4 Discrete logarithms in $\mathbf{F}_{2^3}$ 53

A.1 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$ . . . 119
A.2 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$ (continued) 120
A.3 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$ (continued) 121
A.4 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$ (continued) 122

B.1 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$ with another base 125
B.2 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$ with another base (continued) 126
B.3 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$ with another base (continued) 127
B.4 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$ with another base (continued) 128

C.1 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$ . . . 130
C.2 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$ (continued) 131
C.3 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$ (continued) 132
C.4 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$ (continued) 133
C.5 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$ (continued) 134
C.6 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$ (continued) 135

C.7 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$ (continued) . . . 136
C.8 Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$ (continued) . . . 137

D.1 Representation of $\mathbf{F}_{q^{2k}}$ for $q = 2^{10}$ and prime extension degree 139
D.2 Representation of $\mathbf{F}_{q^{2k}}$ for $q = 2^{10}$ and prime extension degree (continued) . . . 140

List of Figures

1.1 Original communication channel model 1
1.2 Communication channel model with noise 2
1.3 Binary symmetric channel 3
1.4 Communication channel model with encoder and decoder . . . 4
1.5 Communication channel model with eavesdropper 5
1.6 Communication channel model with encryption and decryption 5

2.1 Encoding procedure 10
2.2 Decoding procedure 13
2.3 Deep holes in $\mathbf{R}^2$ 14
2.4 Lattice generated by $\mathbf{b}_1, \mathbf{b}_2$ 21
2.5 Lattice generated by $\mathbf{b}'_1, \mathbf{b}'_2$ 21

3.1 Expected deep hole tree for $p = 7, k = 2$ 35
3.2 Full deep hole tree for $p = 7, k = 2$ 36
3.3 Expected and full deep hole tree for $p = 11, k = 5$ 37
3.4 Expected and full deep hole tree for $p = 13, k = 7$ 38

Abstract

Error-correcting codes and cryptography are two important areas related to information communication. Generalized Reed-Solomon codes and cryptosystems based on the discrete logarithm problem are important representatives of these two fields, respectively.

For a linear code, deep holes are defined to be vectors that are further away from codewords than all other vectors. The problem of deciding whether a received word is a deep hole for generalized Reed-Solomon codes is co-NP-complete [14, 31].

In the recent breakthrough paper by Barbulescu, Gaudry, Joux and Thomé [6, 7], a quasi-polynomial time algorithm (QPA) was proposed for the discrete logarithm problem over finite fields of small characteristics. The time complexity analysis of the algorithm is based on several heuristics presented in their paper.

In this dissertation, we shall study the deep hole problem of generalized Reed-Solomon codes and the discrete logarithm problem over finite fields. On the one hand, we shall classify deep holes for generalized Reed-Solomon codes $RS_q(D, k)$ in a special case. On the other hand, we shall show that some of the heuristics in BGJT-algorithm are problematic in their original forms [6], in particular, when the field is not a Kummer extension. We

propose a solution to the algorithm in non-Kummer cases, without altering the quasi-polynomial time complexity.

Chapter 1

Introduction

In this dissertation, we consider problems concerning deep holes of generalized Reed-Solomon codes and discrete logarithms over finite fields.

The motivation for the studies stems from the increasing requirements for transmitting messages over realistic channels, which are often imperfect. This can be illustrated by the following example. Suppose Alice and Bob want to communicate over a channel. For the sake of simplicity, we assume that all the information has been transformed into digital signals. We start from considering the following abstract channel model as in Figure 1.1, which includes a source (Alice), a destination (Bob), and a channel.

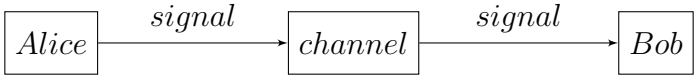

Figure 1.1: Original communication channel model

There are two fundamental issues of consideration:

- Correctness: In reality, there is noise in the channel, which may inter-

rupt the transmitted signal. If Alice sends the message in the original form, the message received by Bob may not be the same as sent by Alice.

- Privacy: The openness of the channel implies that other people, say Eve, may get the message over the channel. If Alice sends the message in the plain text form, then Eve can get the text and understand its meaning.

The main tools developed to solve these problems are error-correcting code theory and cryptography.

1.1 Error-correcting codes and deep holes for linear codes

In this section, the problem of transmitting information over noisy channels is considered as in Figure 1.2. In a seminal paper published in 1948 [66], Shannon established information theory to solve this problem.

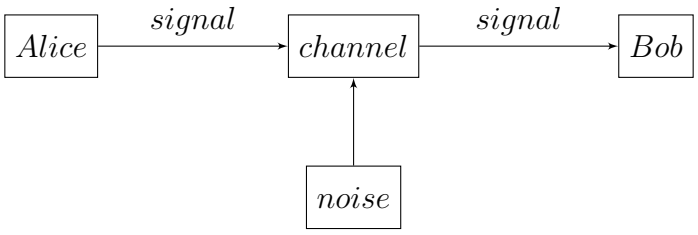

Figure 1.2: Communication channel model with noise

Because of the existence of noise, it may happen that a signal 0 is sent but a signal 1 is received.

Example 1. *The memoryless binary symmetric channel is defined as follows. The alphabet is* $\mathbf{F}_2 = \{0, 1\}$. *The symmetric channel means that it flips each input bit with crossover probability* $0 \leqslant p \leqslant 1$. *Thus the transmission of a single bit can be described pictorially as in Figure 1.3.*

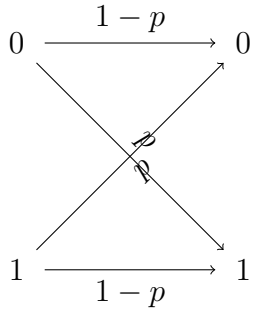

Figure 1.3: Binary symmetric channel

The memoryless channel means that the probability of flipping each bit is independent from other signals. In other words, let $\mathbf{t} = t_1 t_2 \cdots t_n \in \mathbf{F}_2^n, \mathbf{r} = r_1 r_2 \cdots r_n \in \mathbf{F}_2^n$, *we have*

$$P\{\mathbf{r} \quad received \mid \mathbf{t} \quad transmitted\} = \prod_{i=1}^{n} P\{r_i \quad received \mid t_i \quad transmitted\},$$

where $P\{E\}$ *denotes the probability that the event* E *happens.*

In order to detect and correct possible errors of signals during the transmission, the encoding and decoding procedures are introduced as in Figure 1.4.

The encoding procedure is a map that transforms signal alphabets into codewords, and the decoding is the inverse procedure. One of the funda-

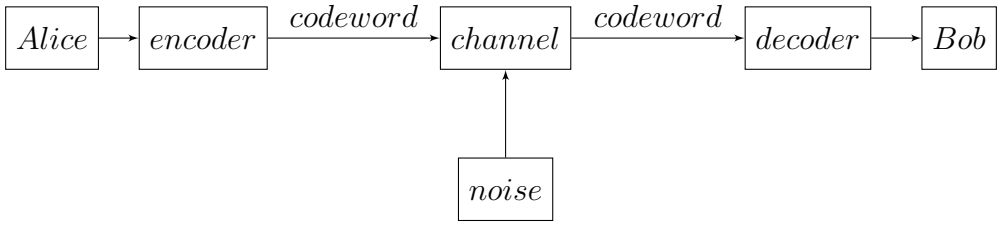

Figure 1.4: Communication channel model with encoder and decoder

mental results of Shannon [66] is the Noisy-Channel Coding theorem. Informally speaking, the theorem asserts that under certain conditions, there exist codes that make the error probability at the receiver arbitrarily small. A large number of codes have been designed. Hamming pioneered this field [32]. Reed and Solomon [59] introduced Reed-Solomon codes in 1960, which is of importance both in theory and in practice.

For the sake of usefulness, there should exist an efficient decoding algorithm. In practice, the maximum-likelihood decoding is used, which aims to minimize the error probability. In certain cases, such as the binary symmetric channel with crossover probability $p < 1/2$, the maximum-likelihood decoding is equivalent to the nearest-codeword decoding. In the nearest-codeword decoding, a received word is decoded as the closest codeword under the measure of Hamming distance. A deep hole of a code is one word which has the largest distance to the code. In this dissertation, we classify deep holes in a special case for generalized Reed-Solomon codes.

1.2 Cryptography and discrete logarithms over finite fields

Confidentiality is a significant concern in the practice of communication. In a paper published in 1949 [67], Shannon considered the problem of secure communication. Figure 1.5 shows a simplified model.

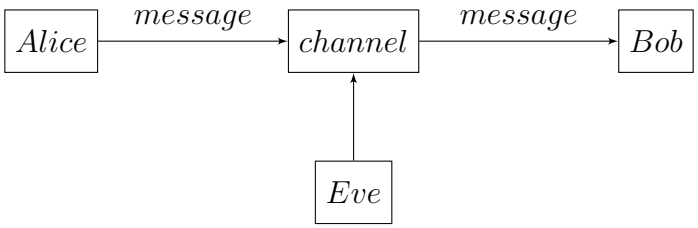

Figure 1.5: Communication channel model with eavesdropper

Since there exists a third party over the channel, the encryption and decryption procedures are introduced to keep the message secure as shown in Figure 1.6. The goal of an encryption procedure is to make the transformed message look random to the third party, while the receiver can recover the original message with the decryption procedure.

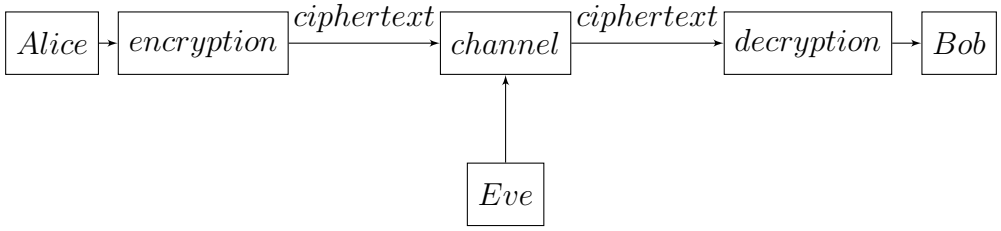

Figure 1.6: Communication channel model with encryption and decryption

The encryption procedure and its inverse are important components of

cryptography. In the early era, the confidentiality was usually achieved with some physical aid. In the modern era, cryptography has put its feet on more solid foundations [26], such as information theory, computational complexity, and mathematics.

There are two main branches of ciphers: one is the symmetric-key (or private-key) cipher and the other is the asymmetric-key (or public-key) cipher. Symmetric-key ciphers are implemented as either stream ciphers or block ciphers. The considerable advantage of the symmetric-key cipher is its speed. One of the drawbacks of the symmetric-key cipher is that the two participants need to share a key before the communication, which is a problem if there are many users since N users need $\binom{N}{2}$ keys.

In 1976, Diffie and Hellman [20] pioneered the public-key cryptography. In public-key cryptography, each participant has a pair of keys: one is the public key and the other is the private key. The public-key ciphers are usually built on some hard computational problems, among which the integer factorization and discrete logarithms problem over finite fields are two commonly used ones. For example, Diffie and Hellman [20] designed a key-exchange scheme based on the discrete logarithms over finite fields. Rivest, Shamir, and Adleman [60] developed a cryptosystem based on the integer factorization. ElGamal [23] established a cryptosystem based on the discrete logarithm problem.

For the sake of security, cryptanalysis efforts have been made to consider the hardness (or weakness) of these problems underlying these cryptosystems. In particular, many algorithms have been designed to attack the discrete logarithm problem over finite fields. Shor [68] designed a randomized algorithm to solve the discrete logarithm in polynomial time on a hypothetical quantum

computer. Many classical algorithms to compute discrete logarithms have been developed during the last decades, such as index calculus methods, the number field sieve, and the function field sieve. The state-of-the-art general purpose algorithm runs in sub-exponential time on classical computer models such as Turing machines. Recently, a quasi-polynomial time algorithm [6, 7] was proposed for the discrete logarithm problem over finite fields of small characteristics on classical computer models. In this dissertation, we shall study the original form of this algorithm [6]. Some heuristics are shown to be problematic and a solution is proposed.

Chapter 2

Background

2.1 Basic field theory

Definition 1. *A field* $\mathbf{F}$ *is a commutative ring with identity in which each nonzero element has an inverse. In other words, the set of units* $\mathbf{F}^* = \mathbf{F} \setminus \{0\}$ *is an abelian group under multiplication.*

Example 2. *We can check that the following are fields:*

1. *Fields with infinite elements:* $\mathbf{Q}, \mathbf{R}, \mathbf{C}$*, i.e., the fields of rational numbers, real numbers and complex numbers.*

2. *Fields with finite elements:* $\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/11\mathbf{Z}$*. In general,* $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ *is a field, where* p *is a prime number.*

Definition 2. *A field with finite elements is called a finite field or a Galois field.*

Definition 3. *Let* $\mathbf{F}$ *be a given field. The characteristic of* $\mathbf{F}$*, denoted by* $ch(\mathbf{F})$*, is defined as the smallest positive integer* n *such that* $n * 1_{\mathbf{F}} = 0$ *if such an integer exists and is defined as* 0 *otherwise.*

Proposition 1. *Let* $\mathbf{F}$ *be a given field. Then* $ch(\mathbf{F})$ *is either* 0 *or a prime* p*.*

Example 3. *We have the following cases:*

1. $ch(\mathbf{Q}) = 0$*, where* $\mathbf{Q}$ *is the rational number field.*
2. *Let* p *be a prime number. Then* $ch(\mathbf{F}_p) = p$*.*
3. *Let* p *be a prime number,* $\mathbf{F}_p[x]$ *be the integral domain of polynomials in the variable* x *with coefficients in* $\mathbf{F}_p$ *and* $\mathbf{F}_p(x)$ *be the fraction field of* $\mathbf{F}_p[x]$*. We have* $ch(\mathbf{F}_p(x)) = p$*.*

Definition 4. *Let* $\mathbf{F}$ *be a given field. The intersection of all subfields of* $\mathbf{F}$*, denoted by* $\mathbf{K} \subset \mathbf{F}$*, is called the prime subfield of* $\mathbf{F}$*.*

Proposition 2. *We have the following conclusions:*

1. *If* $ch(\mathbf{F}) = 0$*, then the prime subfield* $\mathbf{K}$ *of* $\mathbf{F}$ *is isomorphic to* $\mathbf{Q}$*.*
2. *If* $\mathbf{F}$ *is a finite field, i.e.,* $|\mathbf{F}| < \infty$*, then the prime subfield* $\mathbf{K}$ *of* $\mathbf{F}$ *is isomorphic to* $\mathbf{F}_p$*, where* $p = ch(\mathbf{F})$*. Furthermore, if the field extension degree* $[\mathbf{F} : \mathbf{K}] = k$*, then* $|\mathbf{F}| = p^k$*.*

Proposition 3. *We have the following conclusions:*

1. *If* $\mathbf{F}_q$ *is a finite field with order* $q \in \mathbf{Z}$*, then* $q = p^k$*, where* $p = ch(\mathbf{F}_q)$*.*
2. *Conversely, for each* $q = p^k$ *where* p *is a prime and* k *is a positive integer, there exists a unique finite field of order* q *up to isomorphism. The field is the splitting field of* $f(X) = X^q - X$ *over* $\mathbf{F}_p$*. All the elements of* $\mathbf{F}_q$ *are roots of* $f(X)$*. Furthermore,* $\mathbf{F}_q^*$ *is cyclic.*

2.2 Error-correcting codes

Basically, error-correcting codes add some useful redundant information to detect and correct errors. More information on error-correcting codes can be found in books such as [50].

2.2.1 Linear codes

In this section, we shall give a concise description of the linear codes [50]. We assume the alphabet of the codes is a finite field $\mathbf{F}_q$. We shall first consider the sending side.

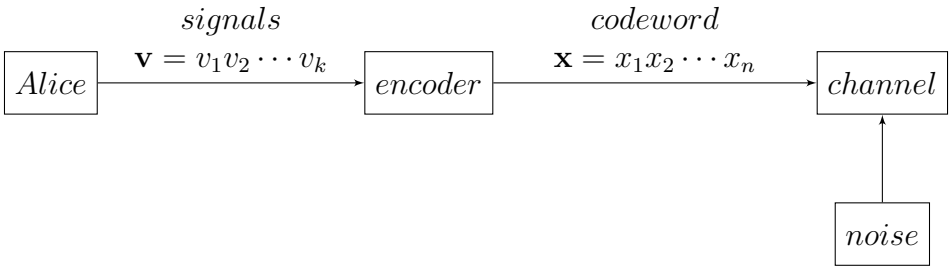

Figure 2.1: Encoding procedure

As indicated in Figure 2.1, the sent message is divided by blocks. Each message block is of length k, which is encoded as a codeword of length $n \geqslant k$.

Example 4. *In this example, the codeword consists of two parts: the first part is the same as the message block, i.e., $x_i = v_i$ for $1 \leqslant i \leqslant k$; the second part contains the useful redundant symbols, which are called check symbols. Given the parity check matrix H of the form*

$$H = [A|I_{n-k}], \tag{2.1}$$

where A is an $(n-k)*n$ matrix and I_{n-k} is an $(n-k)*(n-k)$ unit matrix, the check symbols are determined so that

$$H \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = 0,$$

where the computation is performed in the given field $\mathbf{F}_q$.

Remark 1. *In general, a parity check matrix may not have the form given in (2.1).*

Example 5. *Suppose $k = 1, n = 3$ and the linear code is defined over $\mathbf{F}_2$. Let the parity check matrix be*

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

Since $k = 1$, each block consists of one symbol. Also each codeword $x_1x_2x_3$ satisfies the conditions:

$$x_1 + x_2 = 0, \quad x_1 + x_3 = 0.$$

Thus, we have the following encoding table:

message	*codeword*
0	*000*
1	*111*

This is known as a repetition code.

Example 6. *Suppose $k = 2, n = 4$ and the linear code is defined over $\mathbf{F}_2$. Let the parity check matrix be*

$$H = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

Each message block includes two symbols in this case. Each codeword $x_1x_2x_3x_4$ satisfies:

$$x_2 + x_3 = 0, \quad x_1 + x_4 = 0.$$

Thus, we have the following encoding table:

message	*codeword*
00	*0000*
01	*0110*
10	*1001*
11	*1111*

The general definition of linear codes is given below.

Definition 5. *A linear code of length n and rank k, denoted by $[n, k]_q$, is a linear subspace with dimension k of the vector space $\mathbf{F}_q^n$ where $\mathbf{F}_q$ is the finite field with q elements. The code has rate (or efficiency) $R = k/n$.*

Remark 2. *Let $[n, k]_q$ be a given linear code. The elements in the code are called codewords. Elements in $\mathbf{F}_q^n$ are called codes or vectors.*

Remark 3. *Since we can regard a $[n, k]_q$ linear code as a vector space over $\mathbf{F}_q$ of dimension k, there exists a linearly independent basis $\mathbf{b}_1, \ldots, \mathbf{b}_k$ such*

that each codeword $\mathbf{u}$ *can be written as*

$$\mathbf{u} = \sum_{i=1}^{k} (c_i \mathbf{b}_i), \quad c_i \in \mathbf{F}_q, 1 \leqslant i \leqslant k.$$

The matrix G *whose rows are* $\mathbf{b}_1, \ldots, \mathbf{b}_k$ *is called a generator matrix. In the sequel, we assume that the rows of a generator matrix form a basis for the code.*

Definition 6. *A linear code* $[n, k]_q$ *is called maximum distance separable (in short, MDS) if it attains the Singleton bound, i.e.,* $d = n - k + 1$.

Now we turn our attention to the receiver's side shown in Figure 2.2.

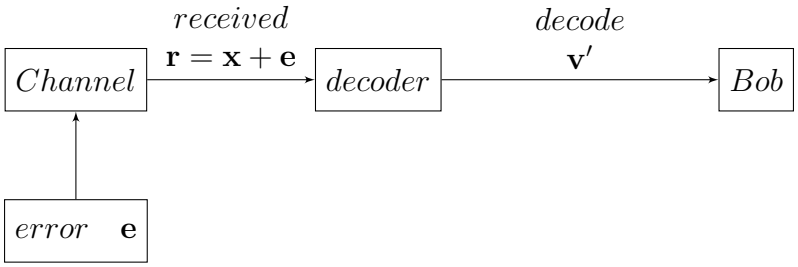

Figure 2.2: Decoding procedure

At the receiver's end, the received message is a mixture of the transmitted message and the error vector $\mathbf{e}$ introduced during the transmission. Given $\mathbf{r} = \mathbf{x} + \mathbf{e}$, the decoder needs to decode $\mathbf{r}$ as $\mathbf{v}'$ such that it minimizes the error. This is called the maximum likelihood decoding.

Definition 7. *The Hamming distance between two words* $\mathbf{u}, \mathbf{v} \in \mathbf{F}_q^n$*, denoted by* $d(\mathbf{u}, \mathbf{v})$*, is the number of their distinct coordinates.*

Example 7. *Over* $\mathbf{F}_2^3$*, we have* $d(101, 001) = 1$*,* $d(010, 100) = 2$*,* $d(000, 111) = 3$.

Definition 8. *The error distance of a received word* $\mathbf{u} \in \mathbf{F}_q^n$ *to the code* $[n,k]_q$ *is defined as its minimum Hamming distance to codewords.*

Definition 9. *The minimum distance of a code, which is denoted by* d*, is the smallest distance between any two distinct codewords of the code. The covering radius of a code is the maximum distance from any vector in* $\mathbf{F}_q^n$ *to the nearest codeword.*

Definition 10. *A deep hole of a code* $[n,k]_q$ *is a vector in* $\mathbf{F}_q^n$ *achieving the covering radius.*

Example 8. *In Euclidean space* $\mathbf{R}^2$*, the analogous deep holes are shown in Figure 2.3.*

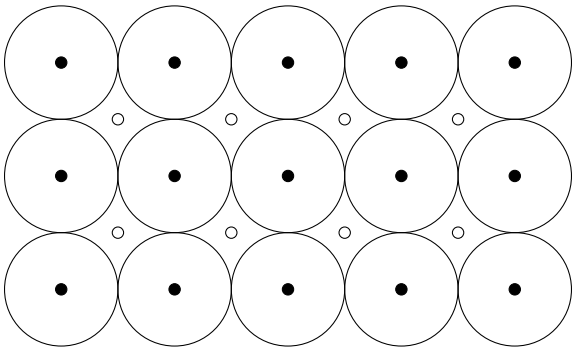

Figure 2.3: Deep holes in $\mathbf{R}^2$

2.2.2 Generalized Reed-Solomon codes

Generalized Reed-Solomon codes are of special interest and importance both in theory and practice of error-correcting codes.

Definition 11. *Let* $\mathbf{F}_q$ *be a finite field with* q *elements and characteristic* p*. Let* $D = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbf{F}_q$ *be the evaluation set and* $v_i \in \mathbf{F}_q^*, 1 \leqslant i \leqslant n$*, be*

the column multipliers. The set of codewords of the generalized Reed-Solomon code $RS_q(D,k)$ of length n and dimension k over $\mathbf{F}_q$ is defined as

$$RS_q(D,k) = \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) \in \mathbf{F}_q^n \mid f(x) \in \mathbf{F}_q[x], deg(f) \leqslant k-1\}.$$

The generalized Reed-Solomon codes are MDS codes and the minimum distance $d = n - k + 1$ and the covering radius $\rho = n - k$. We shall write generalized Reed-Solomon codes as GRS codes for short. If $D = \mathbf{F}_q^*$, it is called *primitive*. If $D = \mathbf{F}_q$, it is called a *singly-extended* GRS code. A GRS code is called *normalized* if its column multipliers are all equal to 1. In this dissertation, we shall work on the normalized GRS without loss of generality.

The encoding algorithm of the GRS code can be described by the linear map: $\varphi : \mathbf{F}_q^k \to \mathbf{F}_q^n$, in which a message $(a_1, \ldots, a_k)$ is mapped to a codeword $(f(\alpha_1), \ldots, f(\alpha_n))$, where $f(x) = a_k x^{k-1} + a_{k-1} x^{k-2} + \cdots + a_1 \in \mathbf{F}_q[x]$.

Efforts have been made to obtain an efficient decoding algorithm for GRS codes. Given a received word $\mathbf{u} \in \mathbf{F}_q^n$, if the error distance is smaller than $n - \sqrt{nk}$, then the list decoding algorithm of Sudan [70] and Guruswami-Sudan [30] solves the decoding in polynomial time. However, in general, the maximum likelihood decoding of GRS codes is NP-hard [31].

2.3 Some results related to additive combinatorics

In this section, we introduce some additive combinatorics results that we shall use later. The first theorem is about the estimation of the size of restricted sum sets, which was first proved by Dias da Silva and Hamidoune [69]. Then

Alon et al. [5] gave a simple proof using the polynomial method.

Theorem 1. *[5, 69] Let* $\mathbf{F}$ *be a field with characteristic* p *and* n *be a positive integer. Then for any finite subset* $S \subset \mathbf{F}$ *we have*

$$|n^{\wedge}S| \geqslant \min\{p, n|S| - n^2 + 1\},$$

where $n^{\wedge}S$ *denotes the set of all sums of* n *distinct elements of* S*.*

Brakemeier [9] and Gallardo et al. [25] established the following theorem:

Theorem 2. *[9, 25] Let* n *be a positive integer and* $S \subset \mathbf{Z}/n\mathbf{Z}$*. If* $|S| > \frac{n}{2}+1$*, then*

$$2^{\wedge}S = \mathbf{Z}/n\mathbf{Z},$$

where $2^{\wedge}S$ *denotes the set of all sums of* 2 *distinct elements of* S*.*

Example 9. *Let* $n = 7$*.*

1. *If* $S_1 = \{1, 2, 3\}$*, then* $2^{\wedge}S_1 = \{3, 4, 5\} \neq \mathbf{Z}/7\mathbf{Z}$*.*
2. *If* $S_2 = \{0, 2, 3, 6\}$*, then* $2^{\wedge}S_2 = \{1, 2, 3, 5, 6\} \neq \mathbf{Z}/7\mathbf{Z}$*.*
3. *If* $S_3 = \{0, 1, 2, 3, 4\}$*, then* $2^{\wedge}S_3 = \{0, 1, 2, 3, 4, 5, 6\} = \mathbf{Z}/7\mathbf{Z}$*.*
4. *If* $S_4 = \{0, 1, 3, 5, 6\}$*, then* $2^{\wedge}S_4 = \{0, 1, 2, 3, 4, 5, 6\} = \mathbf{Z}/7\mathbf{Z}$*.*

Theorem 2 implies the following corollary:

Corollary 1. *Let* $\mathbf{F}_p$ *be a prime finite field,* $S \subset \mathbf{F}_p^*$*. If* $|S| > \frac{p+1}{2}$*, then each element of* $\mathbf{F}_p^*$ *is the product of two distinct elements of* S*.*

Proof: Let g be a generator of $\mathbf{F}_p^*$. Let $S' = \{e | g^e \in S\} \subset \mathbf{Z}/(p-1)\mathbf{Z}$. For any given element $\alpha = g^a \in \mathbf{F}_p^*$, we need to show that there exist two distinct

elements $b \neq c$ such that $g^a = g^b g^c$, where $b, c \in S'$. This is equivalent to $a = b + c$, which follows from Theorem 2. □

2.4 Cryptography

Cryptography stems from the necessity of confidentiality, authentication and integrity of information communication. There are three most important primitives, namely symmetric ciphers, asymmetric ciphers, and hash functions.

2.4.1 Asymmetric cryptography

In a seminal paper [20], Diffie and Hellman proposed a new kind of cryptography which is called asymmetric or public-key cryptography. In such systems, there exits a private key and a public key, hence the name.

The security of such systems relies on the concept of one-way functions, which is easy to compute in one way but hard to compute inversely. The existence of such functions implies that $P \neq NP$. Although nobody can prove the existence of such functions currently, people believe that there are some qualified candidates. The discrete logarithm problem over finite fields is one of the most important candidates, besides the integer factorization problem and others. The hardness of discrete logarithm problem underpins the security of the widely adopted Diffie-Hellman key exchange protocol [20] and ElGamal's cryptosystem [23].

2.4.2 The discrete logarithm problem over finite fields

Definition 12. *Let $\mathbf{F}_q$ be a finite field of characteristic p. Given $\alpha, \beta \in \mathbf{F}_q^*$, the discrete logarithm problem is to find an integer x such that $\alpha^x = \beta$.*

Remark 4. *In this dissertation, we only consider the case when α is a primitive element of $\mathbf{F}_q$.*

The state-of-the-art general-purpose methods for solving the discrete logarithm problem over finite fields are the number field sieve algorithm and the function field sieve algorithm, which originated from the index-calculus method. All these algorithms run in sub-exponential time. Let

$$L_N(\alpha) = \exp(O((\log N)^{\alpha}(\log\log N)^{1-\alpha})).$$

For a finite field $\mathbf{F}_q$, successful efforts have been made to reduce the heuristic complexity of these algorithms from $L_q(1/2)$ to $L_q(1/3)$. See [1, 2, 19, 28, 41, 42, 52, 58].

A sequence of breakthrough results [27, 37, 38] obtained recently on the discrete logarithm problem over finite fields culminated in a discovery of a quasi-polynomial time algorithm for small characteristic fields [6, 7]. For a finite field $\mathbf{F}_{q^{2k}}$ with $k < q$, their algorithm runs in heuristic time $q^{O(\log k)}$. This result, if correct, essentially removes the discrete logarithm over small characteristic fields from hard problems in cryptography.

2.5 Smoothness of integers and polynomials

Most efficient algorithms on the discrete logarithm problem over finite fields rely on smoothness of integers or polynomials. The basic idea is to reduce

the discrete logarithm of a bigger norm element to discrete logarithms of elements of smaller norm.

Definition 13. *An integer* $n = \prod_{i=1}^{k} p_i^{e_i}$ *is* B*-smooth if* $p_i < B$ *for a chosen upper bound* B *for all* $1 \leqslant i \leqslant k$*. A polynomial of degree* n *over a finite field* $\mathbf{F}_q$ *is* m*-smooth if all its irreducible factors have degrees* $\leqslant m$*. Denote the probability that a random polynomial of degree* n *(*$\geqslant m$*) over* $\mathbf{F}_q$ *is* m*-smooth by* $p(n, m)$*.*

Remark 5. *In [1], the author attributed the term smoothness to R. Rivest.*

Odlyzko [55] showed that

$$p(n, m) = exp((1 + o(1))\frac{n}{m}\log_e \frac{m}{n}),$$

in the case when $ch(\mathbf{F}_q) = 2, n \to \infty$ and $n^{\frac{1}{100}} \leqslant m \leqslant n^{\frac{99}{100}}$. Lovorn [49] generalized the conclusion to any prime power q. Car [12] obtained an asymptotic result in terms of Dickman function when m is large compared with n. Panario et al. [57] showed that the Dickman function approaches the number of smooth polynomials when $m \geqslant (1 + \epsilon)(\log n)^{1/k}$ for a positive integer k.

2.6 Lattice theory

In this section, we shall give a brief introduction to the lattice theory. More information about lattice theory can be found in books such as [53] and [34].

2.6.1 Basic concepts

Definition 14. *A lattice in* $\mathbf{R}^m$ *is the set*

$$\mathcal{L} = \{\sum_{i=1}^{n} x_i \mathbf{b}_i | x_i \in \mathbf{Z}\},$$

where $n \leqslant m$ *and* $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ *are linearly independent vectors over* $\mathbf{R}$ *and* $\mathbf{b}_i \in \mathbf{R}^n$ *for* $1 \leqslant i \leqslant n$.

Remark 6. *Given a lattice* $\mathcal{L}$ *defined as above, we call* m, n *the dimension and rank of the lattice* $\mathcal{L}$*, respectively. If* $m = n$*, we call it a full rank lattice. And we call the set of vectors* $\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_n$ *a lattice basis and write*

$$B = [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n],$$

where $\mathbf{b}_i$ *is written as a column vector for* $1 \leqslant i \leqslant n$*. Equivalently, we say the basis generates the lattice.*

Geometrically, the lattice consists of the intersection points of an infinite, regular n-dimensional grid.

Example 10. *Let* $m = n = 2$*, i.e., we consider a full rank lattice in* $\mathbf{R}^2$*. Let the lattice basis be*

$$\mathbf{b}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad \mathbf{b}_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

The lattice is generated by $B = [\mathbf{b}_1, \mathbf{b}_2] \in \mathbf{R}^{2\times 2}$*. Pictorially, it is shown in Figure 2.4.*

Example 11. *Let* $m = n = 2$*, i.e., we consider a full rank lattice in* $\mathbf{R}^2$*. Let*

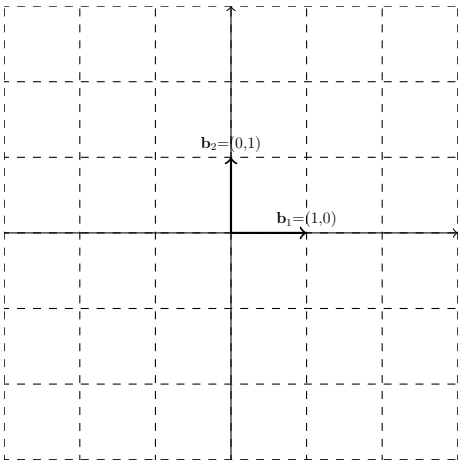

Figure 2.4: Lattice generated by $\mathbf{b}_1, \mathbf{b}_2$

the lattice basis be

$$\mathbf{b}_1' = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad \mathbf{b}_2' = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

The lattice is generated by $B' = [\mathbf{b}_1', \mathbf{b}_2'] \in \mathbf{R}^{2\times 2}$. *Pictorially, it is shown in Figure 2.5.*

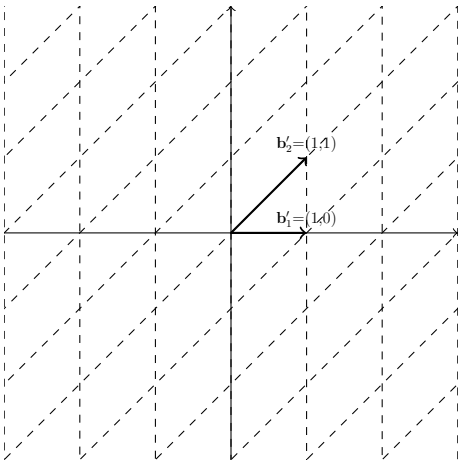

Figure 2.5: Lattice generated by $\mathbf{b}_1', \mathbf{b}_2'$

Remark 7. *Graphically, the intersection sets are the same as the last example. One can check that the lattice generated by* B *is the same as the one*

generated by B'. In this case, we call B and B' equivalent, in other words, equivalent bases generate the same lattice.

Definition 15. *The determinant of a lattice $\mathcal{L}(B)$ is the n-dimensional volume of the fundamental parallelepiped $P(B)$, which is spanned by the basis vectors. In other words,*

$$P(B) = \{B\mathbf{x} : 0 \leqslant x_i \leq 1\}.$$

We denote the determinant of $\mathcal{L}$ by $\det(\mathcal{L})$.

2.6.2 Computational problems

Minkowski's convex body theorem [53, page 12] asserts that given any convex set in $\mathbf{R}^n$, which is symmetric with respect to the origin and with volume greater than $2^n \det(\mathcal{L})$, there exists a non-zero lattice point in the set. As a corollary, Minkowski's first theorem implies that the length of the shortest vector in $\mathcal{L}$ satisfies

$$\lambda_1 < \sqrt{n} \det(\mathcal{L})^{1/n}.$$

While no known efficient algorithm can find the shortest vector, or even a vector within the Minkowski's bound, there are polynomial-time algorithms to approximate the shortest vector in a lattice. The Lenstra-Lenstra-Lovasz (LLL) algorithm can find in polynomial-time a vector whose length is at most $(2/\sqrt{3})^n$ times the length of the shortest vector of a lattice [53, page 33]. The Block-Korkine-Zolotarev (BKZ) algorithm [53] can achieve a better approximation factor.

2.6.3 Lattices and groups

Let $\mathcal{L}(B)$ be a rank n lattice and let $\mathcal{L}(B')$ be a full rank sublattice of $\mathcal{L}(B)$. Since each column vector of B' is a linear combination of column vectors of B, there exists a nonsingular integer matrix $T \in \mathbf{Z}^{n\times n}$ such that

$$B' = B * T.$$

Recall that how we define the congruent classes of integers as an additive group. Let $m \in \mathbf{Z}$, then $G = \langle m \rangle$ is a subgroup of $\mathbf{Z}$. Two integers a, b are equivalent if $a - b \in G$. If they are equivalent, we denote this by

$$a \equiv b \pmod{m}.$$

Following a similar procedure, we define an equivalent relation on $\mathcal{L}(B)$ as follows: given two lattice points $\mathbf{u}, \mathbf{v} \in \mathcal{L}(B)$, $\mathbf{u}$ is equivalent to $\mathbf{v}$ if and only if $\mathbf{u} - \mathbf{v} \in \mathcal{L}(B')$. If they are equivalent, then we denote this by

$$\mathbf{u} \equiv \mathbf{v} \pmod{\mathcal{L}(B')}.$$

Furthermore, we can define an operation on the equivalent classes as follows:

$$[\mathbf{u}] + [\mathbf{v}] = [\mathbf{u} + \mathbf{v}].$$

One can check that the quotient $G = \mathcal{L}(B)/\mathcal{L}(B')$ is an additive group with respect to the defined operation. And the map

$$\phi : \mathcal{L}(B) \to G = \mathcal{L}(B)/\mathcal{L}(B')$$

given by

$$\mathbf{u} \mapsto [\mathbf{u}],$$

is a group homomorphism, where $ker(\phi) = \mathcal{L}(B')$.

Remark 8. *There are different representations for the elements of G. Two well known ways are Hermite Normal Form (HNF) and Smith Norm Form (SNF).*

Definition 16. *A square nonsingular integer matrix $T \in \mathbf{Z}^{n\times n}$ is in HNF if it satisfies the following conditions:*

- *T is upper triangular, i.e., $t_{i,j} = 0$ if $i > j$,*
- *All diagonal elements of T are strictly positive, i.e., $t_{i,i} > 0$ for $1 \leqslant i \leqslant n$,*
- *All non diagonal elements are reduced modulo the corresponding diagonal element on the same row, i.e., $0 \leqslant t_{i,j} < t_{i,i}$ if $i < j$.*

Definition 17. *A matrix $T \in \mathbf{Z}^{n\times n}$ is in SNF if it satisfies the following conditions:*

- *T is diagonal, i.e., $t_{i,j} = 0$ if $i \neq j$,*
- *All diagonal elements are non negative, i.e., $t_{i,i} \geqslant 0$ for $1 \leqslant i \leqslant n$,*
- *$t_{i,i} | t_{i+1,i+1}$ for $1 \leqslant i < n$.*

Chapter 3

The Deep Hole Problem of Generalized Reed-Solomon Codes

3.1 Statement of the problem

Definition 18. *Given a generalized Reed-Solomon code $RS_q(D, k)$ with $|D| = n$, deep holes of $RS_q(D, k)$ are vectors in $\mathbf{F}_q^n$ whose distance with the code is $n - k$. The deep hole problem is to determine all the deep holes.*

Remark 9. *The problem of deciding whether a received word is a deep hole for generalized Reed-Solomon codes is co-NP-complete [14, 31].*

Definition 19. *Given a word $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbf{F}_q^n$, the Lagrange interpolating polynomial of $\mathbf{u}$ is defined as:*

$$u(x) = \sum_{i=1}^{n} u_i \frac{\prod_{j \neq i}(x - \alpha_j)}{\prod_{j \neq i}(\alpha_i - \alpha_j)} \in \mathbf{F}_q[x],$$

where $D = \{\alpha_1, \ldots, \alpha_n\}$ *is the evaluation set.*

Remark 10. *The Lagrange interpolating polynomial is the only polynomial in* $\mathbf{F}_q[x]$ *of degree less than* n *that satisfies* $u(\alpha_i) = u_i, 1 \leqslant i \leqslant n$.

Definition 20. *We say that a function* $u(x)$ *generates a vector* $\mathbf{u} \in \mathbf{F}_q^n$ *if*

$$\mathbf{u} = (u(\alpha_1), u(\alpha_2), \ldots, u(\alpha_n)).$$

We have the following conclusions:

1. If $deg(u) \leqslant k-1$, then $\mathbf{u} \in RS_q(D, k)$ by definition and $d(\mathbf{u}, RS_q(D, k)) = 0$.

2. If $deg(u) = k$, then it can be shown that $\mathbf{u}$ is a deep hole by the following proposition [45], i.e., $d(\mathbf{u}, RS_q(D, k)) = n - k$.

Proposition 4. *[45] For* $k \leqslant deg(u) \leqslant n - 1$, *we have the inequality*

$$n - deg(u) \leqslant d(u, RS_q(D, k)) \leqslant n - k.$$

When the degree of $u(x)$ becomes larger than k, the situation becomes complicated for GRS codes. However, in the case of singly-extended GRS codes defined over fields with odd characteristic, the situation seems to be much simpler. Cheng and Murray [14] conjectured in 2007 that the vectors generated by polynomial of degree k are the only possible deep holes.

Conjecture 1. *[14] Let* q *be an odd prime power. A word* $\mathbf{u}$ *is a deep hole of* $RS_q(\mathbf{F}_q, k)$ *if and only if* $\deg(u) = k$.

There is an analogous conjecture for deep holes of primitive Reed-Solomon codes by Wu and Hong [76].

Conjecture 2. *[76] Let q be an odd prime power. A word $\mathbf{u}$ is a deep hole of $RS_q(\mathbf{F}_q^*, k)$ if and only if it satisfies one of the following conditions:*

1. $u(x) = ax^k + f_{\leqslant k-1}(x), a \neq 0,$

2. $u(x) = bx^{q-2} + f_{\leqslant k-1}(x), b \neq 0,$

where $f_{\leqslant k-1}(x)$ denotes a polynomial with degree not larger than $k-1$.

Remark 11. *Parts of the content in this chapter are joint work with Qi Cheng and Jiyou Li and previously appeared in [13].*

3.2 Related work

Cheng and Murray [14] got the first result related to Conjecture 1 by reducing the problem to the existence of rational points on a hypersurface over $\mathbf{F}_q$.

Theorem 3. *[14] Let $\mathbf{u} \in \mathbf{F}_q^q$ such that $1 \leqslant \delta := \deg(u) - k \leqslant q - 1 - k$. If $q \geqslant \max(k^{7+\epsilon}, \delta^{\frac{13}{3}+\epsilon})$ for some constant $\epsilon > 0$, then $\mathbf{u}$ is not a deep hole.*

Following an approach similar to one in Cheng and Wan [15], Li and Wan [47] improved Theorem 3 with Weil's character sum estimate.

Theorem 4. *[47] Let $\mathbf{u} \in \mathbf{F}_q^q$ such that $1 \leqslant \delta := \deg(u) - k \leqslant q - 1 - k$. If*

$$q > \max((k+1)^2, \delta^{2+\epsilon}), k > (\frac{2}{\epsilon} + 1)\delta + \frac{8}{\epsilon} + 2$$

for some constant $\epsilon > 0$, then $\mathbf{u}$ is not a deep hole.

Liao [48] established the following result:

Theorem 5. *[48] Let $r \geqslant 1$ be an integer. For any received word $\mathbf{u} \in \mathbf{F}_q^q, r \leqslant \delta := \deg(u) - k \leqslant q - 1 - k$, if*

$$q > \max(2\binom{k+r}{2} + \delta, d^{2+\epsilon}), k > (\frac{2}{\epsilon} + 1)\delta + \frac{2r+4}{\epsilon} + 2$$

for some constant $\epsilon > 0$, then $d(\mathbf{u}, RS_q(\mathbf{F}_q, k)) \leqslant q - k - r$, which implies that $\mathbf{u}$ is not a deep hole.

Cafure, Matera, and Privitelli [11] proved the following result with tools of algebraic geometry:

Theorem 6. *[11] Let $\mathbf{u} \in \mathbf{F}_q^q$ such that $1 \leqslant \delta := \deg(u) - k \leqslant q - 1 - k$. If*

$$q > \max((k+1)^2, 14\delta^{2+\epsilon}), k > (\frac{2}{\epsilon} + 1)\delta,$$

for some constant $\epsilon > 0$, then $\mathbf{u}$ is not a deep hole.

Using Weil's character sum estimate and Li-Wan's new sieve [46] for distinct coordinates counting, Zhu and Wan [77] showed the following result:

Theorem 7. *[77] Let $r \geqslant 1$ be an integer. For any received word $\mathbf{u} \in \mathbf{F}_q^q, r \leqslant \delta := \deg(u) - k \leqslant q - 1 - k$, there are positive constants c_1 and c_2 such that if*

$$\delta < c_1 q^{1/2}, (\frac{\delta + r}{2} + 1)\log_2(q) < k < c_2 q,$$

then $d(\mathbf{u}, RS_q(\mathbf{F}_q, k)) \leqslant q - k - r$, which implies that $\mathbf{u}$ is not a deep hole.

3.3 A criterion for deep holes of MDS codes

By definition, deep holes of a linear code are words that have a maximum distance to the code. In the case of MDS codes, there is another way to characterize the deep hole, which connects the concept of deep holes with the MDS codes. The following is well known:

Proposition 5. *Let $\mathbf{F}_q$ be a finite field with characteristic p. Suppose G is a generator matrix for an MDS code $C = [n, k]_q$ with covering radius $\rho = n-k$, then $\mathbf{u} \in \mathbf{F}_q^n$ is a deep hole of C if and only if*

$$G' = \left[\begin{array}{c} G \\ \hline \mathbf{u} \end{array}\right]$$

generates another MDS code.

We give a proof below for the sake of completeness.

Proof: $\Rightarrow$ Suppose $\mathbf{u}$ is a deep hole of $C = [n, k]_q$. We show that G' is a generator matrix for another MDS code. Equivalently, we show that any $k+1$ columns of G' are linearly independent.

Assume there exist $k+1$ columns of G' which are linearly dependent. Without loss of generality, we assume that the first $k+1$ columns of G' are linear dependent. Consider the submatrix consisting of the intersection elements of the first $k+1$ rows and the first $k+1$ columns of G'. Hence there exist $a_1, \ldots, a_k \in \mathbf{F}_q$, not all zero, such that

$$(u_1, \ldots, u_{k+1}) = a_1\mathbf{r}_{1,k+1} + \cdots + a_k\mathbf{r}_{k,k+1},$$

where $\mathbf{r}_{i,k+1}$ is the vector consisting of the first $k+1$ elements of the i-th row

of G for $1 \leqslant i \leqslant k$. Let $\mathbf{v} = a_1\mathbf{r}_1 + \cdots + a_k\mathbf{r}_k \in C$, where $\mathbf{r}_i$ is the i-th row of G for $1 \leqslant i \leqslant k$. We have

$$d(\mathbf{u}, \mathbf{v}) \leqslant n - (k+1) < \rho,$$

which is a contradiction to the assumption that u is a deep hole of C.

$\Leftarrow$ Now suppose G' is a generator matrix for an MDS code, i.e., any $k+1$ columns of G' are linearly independent. We show that $d(\mathbf{u}, C) = n - k$.

Assume that $d(\mathbf{u}, C) < n - k$. Equivalently, there exist $a_1, \ldots, a_k \in \mathbf{F}_q$ such that $\mathbf{u}$ and $\mathbf{v} = a_1\mathbf{r}_1 + \cdots + a_k\mathbf{r}_k$ have more than k common coordinates, where $\mathbf{r}_i$ is the i-th row of G for $1 \leqslant i \leqslant k$. Without loss of generality, we assume that the first $k+1$ coordinates of $\mathbf{u}$ and $\mathbf{v}$ are the same. Consider the submatrix consisting of the first $k+1$ columns of G'. Since the rank of the matrix is less than $k+1$, thus the first $k+1$ columns of G' are linearly dependent, which contradicts to the assumption. □

3.4 Classifying deep holes using deep hole trees

3.4.1 Construction of the deep hole tree

Let $\mathbf{F}_q = \{\alpha_1, \alpha_2, \cdots, \alpha_q = 0\}$. The polynomials in $\mathbf{F}_q[x]$ of degree less than q form a $\mathbf{F}_q$-linear space, with a basis

$$\{1, x, \ldots, x^{k-1}, \prod_{i=1}^{k}(x - \alpha_i), \ldots, \prod_{i=1}^{q-1}(x - \alpha_i)\}.$$

Given a polynomial $f(x) \in \mathbf{F}_q[x]$ with degree $q-1$ we have

$$f(x) = l(x) + c_1 \prod_{i=1}^{k}(x-\alpha_i) + \cdots + c_{q-k}\prod_{i=1}^{q-1}(x-\alpha_i),$$

where $l(x)$ is of degree less than k. We want to determine when $f(x)$ generates a deep hole of $RS_q(\mathbf{F}_q, k)$. By Proposition 5, $f(x)$ generates a deep hole if and only if

$$G' = \left[\begin{array}{c} G \\ \hline \mathbf{u} \end{array}\right]$$

generates an MDS code, where G is the generator matrix of $RS_q(\mathbf{F}_q, k)$, and $\mathbf{u} = (f(\alpha_1), \ldots, f(\alpha_q))$.

Observe that the function, which generates a deep hole for $RS_q(D_2, k)$, also generates a deep hole for $RS_q(D_1, k)$ if $D_1 \subset D_2$. Instead of considering the deep holes for $RS_q(\mathbf{F}_q, k)$ at the first step, we propose to consider a smaller evaluation set at the beginning and make it increase gradually. To be more precise, firstly we determine c_1 over $D_1 = \{\alpha_1, \ldots, \alpha_{k+1}\}$, then we determine c_2 over $D_2 = \{\alpha_1, \ldots, \alpha_{k+2}\}$ based on the knowledge of c_1, so on and so forth. We present the result as a tree, which we shall call a *deep hole tree*.

Remark 12. *Wu and Hong [75] showed that if $D = \mathbf{F}_q \setminus \{\gamma_1, \ldots, \gamma_r\}$ then $f_{\gamma_i}(x) = \frac{1}{x-\gamma_i}$ generates a deep hole for $RS_q(D, k)$, where $1 \leqslant i \leqslant r$.*

Definition 21. *Let $RS_q(D, k)$ be a given code with $D = \mathbf{F}_q \setminus \{\gamma_1, \ldots, \gamma_r\}$. We will call deep holes generated by $f(x) = x^k$ and $f_{\gamma_i}(x) = \frac{1}{x-\gamma_i}$,$1 \leqslant i \leqslant r$, expected deep holes.*

We can also obtain the expected deep holes from Proposition 5.

Proposition 6. *Let $RS_q(D,k)$ be a given code with $D = \{\alpha_1, \ldots, \alpha_n\}$. We have*

1. *If $f(x) = x^k \in \mathbf{F}_q[x]$, then $f(x)$ generates a deep hole.*
2. *If $f(x) = \frac{1}{x-\gamma}$, $\gamma \in \mathbf{F}_q \setminus D$, then $f(x)$ generates a deep hole.*

Proof: Let the generator matrix of $RS_q(D,k)$ be

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix}.$$

Case 1. Let $f(x) = x^k$. Consider the matrix

$$G' = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \\ \alpha_1^{k} & \alpha_2^{k} & \cdots & \alpha_n^{k} \end{bmatrix}.$$

For any subset $\{\beta_1, \ldots, \beta_{k+1}\} \subset D$, the submatrix of G' corresponding to the subset is given by

$$M = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_{k+1} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{k-1} & \beta_2^{k-1} & \cdots & \beta_{k+1}^{k-1} \\ \beta_1^{k} & \beta_2^{k} & \cdots & \beta_{k+1}^{k} \end{bmatrix}.$$

Since $\det(M) = \prod_{1 \leqslant i < j \leqslant k+1}(\beta_j - \beta_i) \neq 0$, any $k+1$ columns of G' are linearly independent. From Proposition 5, $f(x) = x^k$ generates a deep hole.

Case 2. Let $f(x) = \frac{1}{x-\gamma}$, where $\gamma \in \mathbf{F}_q \setminus D$. Consider the matrix

$$G' = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \\ \frac{1}{\alpha_1-\gamma} & \frac{1}{\alpha_2-\gamma} & \cdots & \frac{1}{\alpha_n-\gamma} \end{bmatrix}.$$

For any subset $\{\beta_1, \ldots, \beta_{k+1}\} \subset D$, the submatrix of G' corresponding to the subset is given by

$$M = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_{k+1} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{k-1} & \beta_2^{k-1} & \cdots & \beta_{k+1}^{k-1} \\ \frac{1}{\beta_1-\gamma} & \frac{1}{\beta_2-\gamma} & \cdots & \frac{1}{\beta_{k+1}-\gamma} \end{bmatrix}.$$

Since $\prod_{i=1}^{k+1}(\beta_i - \gamma)\det(M) = (-1)^k \prod_{1 \leqslant i < j \leqslant k+1}(\beta_j - \beta_i)$, we deduce $\det(M) \neq 0$. From Proposition 5, $f(x) = \frac{1}{x-\gamma}$ generates a deep hole.

□

Motivated by Proposition 6, we construct the *expected deep hole tree* as follows:

1. The root node is 1 without loss of generality, i.e., $c_1 = 1$.

2. There are $p-k-1$ branches of the tree, each with distinct length in $[2, p-k]$. And we designate the sequence of nodes in a branch with length l as $\mathbf{b}_l$.

   - If $l = p-k$, then $\mathbf{b}_{p-k} = (0, \ldots, 0)$.
   - If $2 \leqslant l \leqslant p-k-1$, then $\mathbf{b}_l = (c_1, \ldots, c_l)$, where $f = \frac{1}{x-\alpha_{l+1}}$ is equivalent to $c_1 \prod_{i=1}^{k}(x-\alpha_i) + \cdots + c_l \prod_{i=1}^{k+l-1}(x-\alpha_i)$.

Proposition 7. *The expected deep hole tree is a subtree of the full deep hole tree.*

Proof: This follows from Remark 12. □

Now we can construct the full deep hole tree based on the expected deep hole tree.

1. The root node is 1 without loss of generality, i.e., $c_1 = 1$.

2. The children $\{c_{i+1}\}$ of a node $c_i, 1 \leqslant i \leqslant q-k-1$ are defined as follows: given the ancestors $(c_1, \ldots, c_i)$, for $\gamma \in \mathbf{F}_q$, if γ is the child of c_i in the expected deep hole tree, then keep it; otherwise, if

$$c_1 \prod_{i=1}^{k}(x-\alpha_i) + \cdots + c_i \prod_{i=1}^{k+i-1}(x-\alpha_i) + \gamma \prod_{i=1}^{k+i}(x-\alpha_i)$$

   satisfies the property of the function which generates a deep hole as in Proposition 5, then γ is a child of c_i.

That is, we keep the nodes of the expected deep hole tree and add additional ones if necessary. Now we illustrate the procedure to construct the deep hole tree by some examples.

Example 12. *Let $p = 7, k = 2$. The evaluation set is ordered such that $\alpha_i = i, 1 \leqslant i \leqslant 7$. The expected deep hole tree is shown in Figure 3.1.*

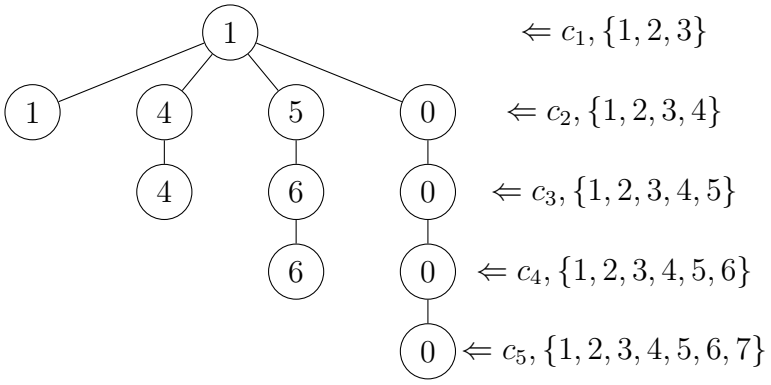

Figure 3.1: Expected deep hole tree for $p = 7, k = 2$

Remark 13. *We notice the following in Figure 3.1:*

1. *The root corresponds to the evaluation set $D_1 = \{1, 2, 3\}$. The expected deep holes are generated by functions equivalent to $\prod_{i=1}^{2}(x - i)$.*

2. *In depth 2, the evaluation set is $D_2 = \{1, 2, 3, 4\}$. One of the expected deep holes is generated by the function $\prod_{i=1}^{2}(x-i)+\prod_{i=1}^{3}(x-i)$, which is equivalent to $f_5 = \frac{1}{x-5}$.*

3. *In depth 3, the evaluation set is $D_3 = \{1, 2, 3, 4, 5\}$. One of the expected deep holes is generated by the function $\prod_{i=1}^{2}(x - i) + 4\prod_{i=1}^{3}(x - i) + 4\prod_{i=1}^{4}(x - i)$, which is equivalent to $f_6 = \frac{1}{x-6}$.*

4. *In depth 4, the evaluation set is $D_4 = \{1, 2, 3, 4, 5, 6\}$. One of the expected deep holes is generated by the function $\prod_{i=1}^{2}(x-i)+5\prod_{i=1}^{3}(x-i) + 6\prod_{i=1}^{4}(x - i) + 6\prod_{i=1}^{5}(x - i)$, which is equivalent to $f_0 = \frac{1}{x}$.*

5. *In depth 5, the evaluation set is* $D_5 = \{1, 2, 3, 4, 5, 6, 7\}$. *One of the expected deep holes is generated by the function* $\prod_{i=1}^{2}(x - i)$.

Example 13. *Let* $p = 7, k = 2$. *The evaluation set is ordered such that* $\alpha_i = i, 1 \leqslant i \leqslant 7$. *The full deep hole tree is shown in Figure 3.2.*

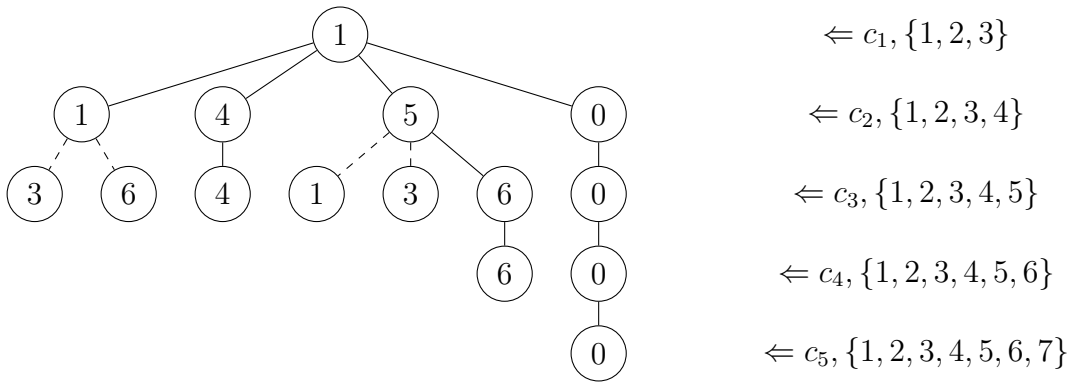

Figure 3.2: Full deep hole tree for $p = 7, k = 2$

Remark 14. *There are four more nodes here than the expected deep hole tree. They are all in depth three.*

1. *The first additional deep hole is generated by the function* $\prod_{i=1}^{2}(x-i)+\prod_{i=1}^{3}(x-i)+3\prod_{i=1}^{4}(x-i)$.

2. *The second additional deep hole is generated by the function* $\prod_{i=1}^{2}(x-i)+\prod_{i=1}^{3}(x-i)+6\prod_{i=1}^{4}(x-i)$.

3. *The third additional deep hole is generated by the function* $\prod_{i=1}^{2}(x-i)+5\prod_{i=1}^{3}(x-i)+\prod_{i=1}^{4}(x-i)$.

4. *The fourth additional deep hole is generated by the function* $\prod_{i=1}^{2}(x-i)+5\prod_{i=1}^{3}(x-i)+3\prod_{i=1}^{4}(x-i)$.

Example 14. *Let $p = 11, k = 5$. The evaluation set is ordered such that $\alpha_i = i, 1 \leqslant i \leqslant 11$. The expected deep hole tree and full deep hole tree are shown in Figure 3.3.*

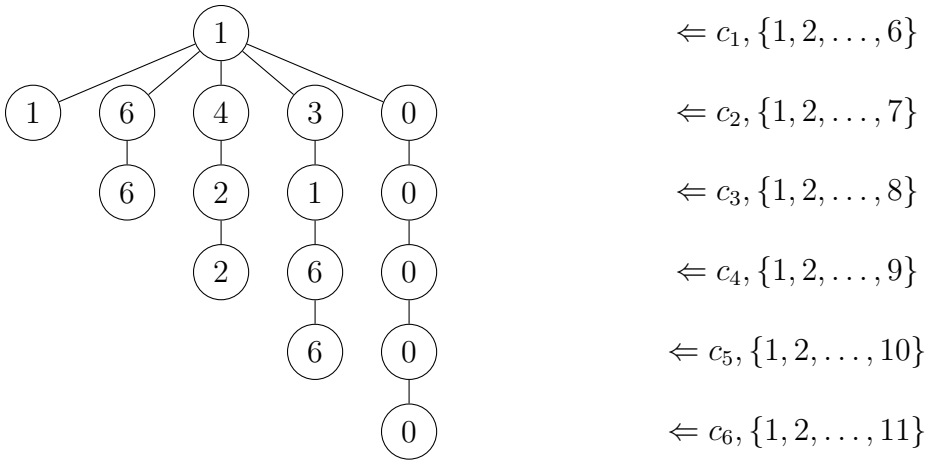

Figure 3.3: Expected and full deep hole tree for $p = 11, k = 5$

Example 15. *Let $p = 13, k = 7$. The evaluation set is ordered such that $\alpha_i = i, 1 \leqslant i \leqslant 13$. The expected and full deep hole trees are shown in Figure 3.4.*

3.4.2 Some lemmas

Lemma 1. *In depth $d = 2$, the nodes are the same in both the expected deep hole tree and full deep hole tree.*

Proof: We show that in depth $d = 2$, the nodes are the same in both the expected deep hole tree and full deep hole tree.

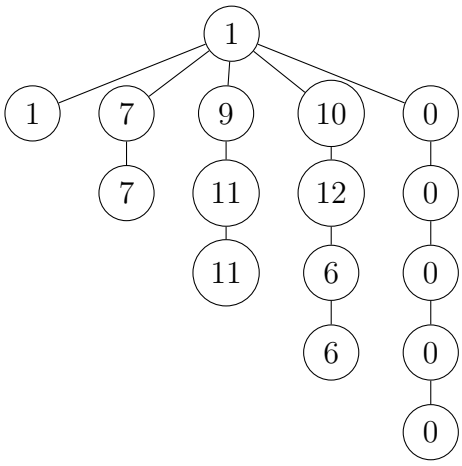

Figure 3.4: Expected and full deep hole tree for $p = 13, k = 7$

In depth $d = 2$, the evaluation set is $D = \{\alpha_1, \alpha_2, \ldots, \alpha_{k+2}\}$. Designate the set of nodes in depth 2 of the expected deep hole tree as S. Firstly, we show that $|S| = p - (k + 1)$. This follows from the fact that the equivalent functions of the form

$$f(x) = \prod_{i=1}^{k}(x - \alpha_i) + c_2 \prod_{i=1}^{k+1}(x - \alpha_i), \quad c_2 \in \mathbf{F}_p,$$

for $f(x) = x^k$ and $f_\delta(x) = \frac{1}{x-\delta}$ take the same value at $\beta \in D \setminus \{\alpha_{k+2}\}$ but pairwise different values at α_{k+2}, where $\delta \in \mathbf{F}_p \setminus D$.

Next, we show that if $c_2 \notin S$ then $f(x) = \prod_{i=1}^{k}(x - \alpha_i) + c_2 \prod_{i=1}^{k+1}(x - \alpha_i)$ does not generate a deep hole. Consider the following matrix

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{k+2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_{k+2}^{k-1} \\ f(\alpha_1) & f(\alpha_2) & \cdots & f(\alpha_{k+2}) \end{bmatrix},$$

where $f(i) = 0, 1 \leqslant i \leqslant k, f(\alpha_{k+1}) = \prod_{i=1}^{k}(\alpha_{k+1}-\alpha_i), f(\alpha_{k+2}) = \prod_{i=1}^{k}(\alpha_{k+2}-\alpha_i) + c_2 \prod_{i=1}^{k+1}(\alpha_{k+2} - \alpha_i)$.

Case 1. If

$$\begin{aligned} f(\alpha_{k+2}) &= \prod_{i=1}^{k}(\alpha_{k+2} - \alpha_i) + c_2 \prod_{i=1}^{k+1}(\alpha_{k+2} - \alpha_i) \\ &= \prod_{i=1}^{k}(\alpha_{k+2} - \alpha_i)[1 + c_2(\alpha_{k+2} - \alpha_{k+1})] \\ &= 0, \end{aligned}$$

i.e., $c_2 = \frac{1}{\alpha_{k+1}-\alpha_{k+2}}$, then there are $k+1$ columns of G, namely, the first k columns and the last column, which are linearly dependent. Thus $f(x)$ does not generate a deep hole in this case.

Case 2. Suppose $f(\alpha_{k+2}) \neq 0$. For any $k-1$ elements $\{\beta_1, \ldots, \beta_{k-1}\} \subset \{\alpha_1, \ldots, \alpha_k\}$, consider the submatrix

$$G' = \begin{bmatrix} 1 & \cdots & 1 & 1 & 1 \\ \beta_1 & \cdots & \beta_{k-1} & \alpha_{k+1} & \alpha_{k+2} \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_{k-1}^{k-1} & \alpha_{k+1}^{k-1} & \alpha_{k+2}^{k-1} \\ 0 & \cdots & 0 & f(\alpha_{k+1}) & f(\alpha_{k+2}) \end{bmatrix}.$$

Thus $\det(G') = 0$ is equivalent to

$$f(\alpha_{k+1}) \prod_{i=1}^{k-1}(\alpha_{k+2} - \beta_i) = f(\alpha_{k+2}) \prod_{i=1}^{k-1}(\alpha_{k+1} - \beta_i),$$

that is,

$$\frac{f(\alpha_{k+2})}{f(\alpha_{k+1})} = \prod_{i=1}^{k-1} \frac{\alpha_{k+2} - \beta_i}{\alpha_{k+1} - \beta_i}$$
$$= \prod_{i=1}^{k-1} (1 + \frac{\alpha_{k+2} - \alpha_{k+1}}{\alpha_{k+1} - \beta_i}).$$

Hence for each subset $\{\beta_1, \ldots, \beta_{k-1}\} \subset \{\alpha_1, \ldots, \alpha_k\}$, there is a unique c_2 such that $\det(G') = 0$.

In total, there are $k+1$ elements of candidate c_2 such that the corresponding $f(x)$ does not generate a deep hole. This implies that if $c_2 \notin S$ then $f(x)$ does not generate a deep hole.

In conclusion, in depth $d = 2$, the nodes in the full deep hole tree are exactly those in the expected deep hole tree. □

Lemma 2. *Let p be an odd prime, $k \geqslant \frac{p-1}{2}, d \geqslant 2$ be a positive integer and $D_d = \{\alpha_1, \ldots, \alpha_{k+d}\} \subset \mathbf{F}_p, \delta \in \mathbf{F}_p \setminus D_d$. For any $\gamma \in \mathbf{F}_p$, there exists a subset $\{\beta_1, \ldots, \beta_k\} \subset D_d$ such that the matrix*

$$A = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \frac{1}{\beta_1 - \delta} & \cdots & \frac{1}{\beta_k - \delta} & \gamma \end{bmatrix}$$

is singular.

Proof: Note that $\det(A) = \det(A') + \det(A'')$, where

$$A' = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \frac{1}{\beta_1-\delta} & \cdots & \frac{1}{\beta_k-\delta} & 0 \end{bmatrix}, A'' = \begin{bmatrix} 1 & \cdots & 1 & 0 \\ \beta_1 & \cdots & \beta_k & 0 \\ \vdots & \ddots & \vdots & 0 \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & 0 \\ \frac{1}{\beta_1-\delta} & \cdots & \frac{1}{\beta_k-\delta} & \gamma \end{bmatrix}.$$

Since

$$\prod_{i=1}^{k}(\beta_i - \delta)\det(A') = \begin{vmatrix} \beta_1 - \delta & \cdots & \beta_k - \delta & 1 \\ \beta_1(\beta_1 - \delta) & \cdots & \beta_k(\beta_k - \delta) & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1}(\beta_1 - \delta) & \cdots & \beta_k^{k-1}(\beta_k - \delta) & \delta^{k-1} \\ 1 & \cdots & 1 & 0 \end{vmatrix}$$

$$= \begin{vmatrix} \beta_1 & \cdots & \beta_k & 1 \\ \beta_1^2 & \cdots & \beta_k^2 & 2\delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^k & \cdots & \beta_k^k & k\delta^{k-1} \\ 1 & \cdots & 1 & 0 \end{vmatrix}$$

$$= (-1)^k \begin{vmatrix} 1 & \cdots & 1 & 0 \\ \beta_1 & \cdots & \beta_k & 1 \\ \beta_1^2 & \cdots & \beta_k^2 & 2\delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^k & \cdots & \beta_k^k & k\delta^{k-1} \end{vmatrix}$$

$$= (-1)^k \begin{vmatrix} 1 & \cdots & 1 & \frac{d}{dx}1\Big|_{x=\delta} \\ \beta_1 & \cdots & \beta_k & \frac{d}{dx}x\Big|_{x=\delta} \\ \beta_1^2 & \cdots & \beta_k^2 & \frac{d}{dx}x^2\Big|_{x=\delta} \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^k & \cdots & \beta_k^k & \frac{d}{dx}x^k\Big|_{x=\delta} \end{vmatrix}$$

$$= (-1)^k \frac{d}{dx} \begin{vmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & x \\ \beta_1^2 & \cdots & \beta_k^2 & x^2 \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^k & \cdots & \beta_k^k & x^k \end{vmatrix} \Bigg|_{x=\delta}$$

$$= (-1)^k \frac{d}{dx} \left[\prod_{1 \leqslant i < j \leqslant k} (\beta_j - \beta_i) \prod_{i=1}^{k} (x - \beta_i) \right] \Bigg|_{x=\delta},$$

thus

$$\begin{aligned} \det(A') &= \frac{(-1)^k}{\prod_{i=1}^k (\beta_i - \delta)} \prod_{1 \leqslant i < j \leqslant k} (\beta_j - \beta_i) \frac{d}{dx} \left[\prod_{i=1}^{k} (x - \beta_i) \right] \Bigg|_{x=\delta} \\ &= \frac{(-1)^k}{\prod_{i=1}^k (\beta_i - \delta)} \prod_{1 \leqslant i < j \leqslant k} (\beta_j - \beta_i) \prod_{i=1}^{k} (\delta - \beta_i) \sum_{i=1}^{k} \frac{1}{\delta - \beta_i} \\ &= \prod_{1 \leqslant i < j \leqslant k} (\beta_j - \beta_i) \sum_{i=1}^{k} \frac{1}{\delta - \beta_i}. \end{aligned}$$

It follows that

$$\begin{aligned} \det(A) &= \det(A') + \det(A'') \\ &= \prod_{1 \leqslant i < j \leqslant k} (\beta_j - \beta_i) \sum_{i=1}^{k} \frac{1}{\delta - \beta_i} + \gamma \prod_{1 \leqslant i < j \leqslant k} (\beta_j - \beta_i). \end{aligned}$$

Hence $\det(A) = 0$ is equivalent to

$$\sum_{i=1}^{k} \frac{1}{\delta - \beta_i} + \gamma = 0.$$

Designate the set $\{\frac{1}{\delta-\beta_i} \mid i \in D_d\}$ as S_1 with cardinality $k + d$. Since $\frac{p-1}{2} \leqslant k, 2 \leqslant d$, from Theorem 1, we conclude that

$$\begin{aligned} |k^{\wedge} S_1| &\geqslant \min\{p, k|S_1| - k^2 + 1\} \\ &= p, \end{aligned}$$

which implies that for each $\gamma \in \mathbf{F}_p$, there exists a subset $\{\beta_1, \ldots, \beta_k\} \subset D_k$ such that $\sum_{i=1}^{k} \frac{1}{\delta-\beta_i} + \gamma = 0$. □

Lemma 3. *Let p be an odd prime, $k \geqslant \frac{p-1}{2}, d \geqslant 2$ be a positive integer and $D_{d+1} = \{\alpha_1, \ldots, \alpha_{k+d+1} = \delta\} \subset \mathbf{F}_p$. For any $\delta' \in \mathbf{F}_p, \delta' \notin D_{d+1}, \gamma \in \mathbf{F}_p, \gamma \neq \frac{1}{\delta-\delta'}$, there exists a subset $\{\beta_1, \ldots, \beta_k\} \subset D_{d+1} \setminus \{\delta\}$ such that the matrix*

$$B = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \frac{1}{\beta_1-\delta'} & \cdots & \frac{1}{\beta_k-\delta'} & \gamma \end{bmatrix}$$

is singular.

Proof: Note that $\det(B) = \det(B') + \det(B'')$, where

$$B' = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \frac{1}{\beta_1-\delta'} & \cdots & \frac{1}{\beta_k-\delta'} & \frac{1}{\delta-\delta'} \end{bmatrix}, B'' = \begin{bmatrix} 1 & \cdots & 1 & 0 \\ \beta_1 & \cdots & \beta_k & 0 \\ \vdots & \ddots & \vdots & 0 \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & 0 \\ \frac{1}{\beta_1-\delta'} & \cdots & \frac{1}{\beta_k-\delta'} & \gamma - \frac{1}{\delta-\delta'} \end{bmatrix}.$$

Since

$$(\delta-\delta')\prod_{i=1}^{k}(\beta_i-\delta')\det(B') = \begin{vmatrix} \beta_1-\delta' & \cdots & \beta_k-\delta' & \delta-\delta' \\ \beta_1(\beta_1-\delta') & \cdots & \beta_k(\beta_k-\delta') & \delta(\delta-\delta') \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1}(\beta_1-\delta') & \cdots & \beta_k^{k-1}(\beta_k-\delta') & \delta^{k-1}(\delta-\delta') \\ 1 & \cdots & 1 & 1 \end{vmatrix}$$

$$= \begin{vmatrix} \beta_1 & \cdots & \beta_k & \delta \\ \beta_1^2 & \cdots & \beta_k^2 & \delta^2 \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^k & \cdots & \beta_k^k & \delta^k \\ 1 & \cdots & 1 & 1 \end{vmatrix}$$

$$= (-1)^k \begin{vmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \beta_1^2 & \cdots & \beta_k^2 & \delta^2 \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^k & \cdots & \beta_k^k & \delta^k \end{vmatrix}$$

$$= (-1)^k \prod_{1\leqslant i<j\leqslant k} (\beta_j - \beta_i) \prod_{i=1}^{k} (\delta - \beta_i),$$

we have

$$\begin{aligned}\det(B') &= \frac{(-1)^k}{(\delta-\delta')\prod_{i=1}^{k}(\beta_i-\delta')} \prod_{1\leqslant i<j\leqslant j} (\beta_j - \beta_i) \prod_{i=1}^{k} (\delta - \beta_i) \\ &= \frac{1}{\delta-\delta'} \prod_{1\leqslant i<j\leqslant k} (\beta_j - \beta_i) \prod_{i=1}^{k} \frac{\beta_i - \delta}{\beta_i - \delta'},\end{aligned}$$

and

$$\det(B'') = (\gamma - \frac{1}{\delta-\delta'}) \prod_{1\leqslant i<j\leqslant k} (\beta_j - \beta_i).$$

Hence

$$\begin{aligned}\det(B) &= \frac{1}{\delta-\delta'} \prod_{1\leqslant i<j\leqslant k} (\beta_j - \beta_i) \prod_{i=1}^{k} \frac{\beta_i - \delta}{\beta_i - \delta'} + (\gamma - \frac{1}{\delta-\delta'}) \prod_{1\leqslant i<j\leqslant k} (\beta_j - \beta_i) \\ &= \prod_{1\leqslant i<j\leqslant k} (\beta_j - \beta_i) \left[\frac{1}{\delta-\delta'} \prod_{i=1}^{k} \frac{\beta_i - \delta}{\beta_i - \delta'} + \frac{\gamma(\delta-\delta')-1}{\delta-\delta'} \right] \\ &= \frac{\prod_{1\leqslant i<j\leqslant k}(\beta_j - \beta_i)}{\delta-\delta'} \left[\prod_{i=1}^{k} \frac{\beta_i - \delta}{\beta_i - \delta'} + \gamma(\delta-\delta') - 1 \right].\end{aligned}$$

It follows that $\det(B) = 0$ is equivalent to

$$\prod_{i=1}^{k} (1 + \frac{\delta' - \delta}{\beta_i - \delta'}) = 1 - \gamma(\delta - \delta').$$

If $|D_d| = k+2$, we consider the dual version of the equality. From Corollary 1, there exist two distinct elements $x, y \in D_d$ such that $(1 + \frac{\delta'-\delta}{x-\delta'})(1 + \frac{\delta'-\delta}{y-\delta'}) = \theta$ for any $\theta \in \mathbf{F}_p^*$, hence there exist k distinct elements in D_d such

that

$$\prod_{i=1}^{k}(1+\frac{\delta'-\delta}{\alpha_i-\delta'})=1-\gamma(\delta-\delta'),$$

for any $\gamma \neq \frac{1}{\delta-\delta'}$.

If $|D_d| > k+2$, we select a subset $D' \subset D_d$ such that $|D'| = k+2$, then apply the same argument as above. □

Lemma 4. *Let p be an odd prime, $k \geqslant \frac{p-1}{2}, d \geqslant 2$ be a positive integer and $D_{d+1} = \{\alpha_1, \ldots, \alpha_{k+d+1} = \delta\} \subset \mathbf{F}_p$. For any $\gamma \in \mathbf{F}_p, \gamma \neq \delta^k$, there exists a subset $\{\beta_1, \ldots, \beta_k\} \subset D_{d+1} \setminus \{\delta\}$ such that the matrix*

$$C = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \beta_1^k & \cdots & \beta_k^k & \gamma \end{bmatrix}$$

is singular.

Proof: Note that $\det(C) = \det(C') + \det(C'')$, where

$$C' = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \beta_1^k & \cdots & \beta_k^k & \delta^k \end{bmatrix}, C'' = \begin{bmatrix} 1 & \cdots & 1 & 0 \\ \beta_1 & \cdots & \beta_k & 0 \\ \vdots & \ddots & \vdots & 0 \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & 0 \\ \beta_1^k & \cdots & \beta_k^k & \gamma-\delta^k \end{bmatrix}.$$

Since

$$\det(C') = \prod_{1 \leqslant i < j \leqslant k} (\beta_j - \beta_i) \prod_{i=1}^{k} (\delta - \beta_i),$$

$$\det(C'') = \prod_{1 \leqslant i < j \leqslant k} (\beta_j - \beta_i)(\gamma - \delta^k),$$

we have

$$\frac{1}{\prod_{1 \leqslant i < j \leqslant k} (\beta_j - \beta_i)} \det(C) = \prod_{i=1}^{k} (\delta - \beta_i) + \gamma - \delta^k.$$

Thus $\det(C) = 0$ is equivalent to

$$\prod_{i=1}^{k} (\delta - \beta_i) = \delta^k - \gamma.$$

Denote $S = \{\delta - \alpha \mid \alpha \in D\}$. If $|D_d| = k + 2$, we consider the dual version of the equality. From Corollary 1, there exist two distinct elements $x, y \in S$ such that $xy = \theta$ for any $\theta \in \mathbf{F}_p^*$, hence there exist k distinct elements in S such that

$$\prod_{i=1}^{k} (\delta - \beta_i) = \delta^k - \gamma,$$

for any $\gamma \neq \delta^k$.

If $|D_d| > k+2$, we select a subset $S' \subset S$ such that $S = k+2$, then apply the same argument as above. □

3.4.3 The main theorem and the proof

In this section, we establish the following theorem:

Theorem 8. *Let $p > 2$ be a prime number, $k \geqslant \frac{p-1}{2}$, $D = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ with $k < n \leqslant p$. The only deep holes of $RS_p(D, k)$ are generated by functions*

which are equivalent to the following:

$$f(x) = x^k, \quad f_\delta(x) = \frac{1}{x-\delta},$$

where $\delta \in \mathbf{F}_p \setminus D$. *Here two functions* $f(x)$ *and* $g(x)$ *are equivalent if and only if there exists* $a \in \mathbf{F}_p^*$ *and* $h(x) \in \mathbf{F}_p[x]$ *with degree less than* k *such that*

$$g(x) = af(x) + h(x).$$

The basic idea of the proof of Theorem 8 is reducing the problem to some additive number theory problems.

Proof: Proceed by induction on the depth of the full deep hole tree.

Basis case. This follows from Lemma 1.

Inductive step. We show that if the set of nodes of the full deep hole tree coincide with the nodes of the expected deep hole tree in the same depth $d \geqslant 2$, then there are no additional nodes in depth $d+1$ except the expected ones. Denote the corresponding evaluation set by $D_d = \{\alpha_1, \ldots, \alpha_{k+d}\}$ in depth d and $D_{d+1} = \{\alpha_1, \ldots, \alpha_{k+d}, \alpha_{k+d+1} = \delta\}$ in depth $d+1$. In order to show there are no new nodes in depth $d+1$, there are three cases to consider.

Case 1: We show the branch, which corresponds to the function $f = \frac{1}{x-\delta}$, will not grow in depth $d+1$. It suffices to show that there exists $\{\beta_1, \ldots, \beta_k\} \subset$

$\{\alpha_1, \ldots, \alpha_{k+d}\}$ such that for any $\gamma \in \mathbf{F}_p$ and matrix

$$A = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \frac{1}{\beta_1-\delta} & \cdots & \frac{1}{\beta_k-\delta} & \gamma \end{bmatrix},$$

we have $\det(A) = 0$. This follows from Lemma 2.

Case 2: We show that the branch, which corresponds to the function $f = \frac{1}{x-\delta'}$, where $\delta' \notin D_{k+1}$, has only one child in depth $d+1$. It suffices to show that there exists $\{\beta_1, \ldots, \beta_k\} \subset D_d$ such that for any $\delta' \notin D_{d+1}, \gamma \in \mathbf{F}_p, \gamma \neq \frac{1}{\delta-\delta'}$ and matrix

$$B = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \frac{1}{\beta_1-\delta'} & \cdots & \frac{1}{\beta_k-\delta'} & \gamma \end{bmatrix},$$

we have $\det(B) = 0$. This follows from Lemma 3.

Case 3: We show that the branch, which corresponds to the function $f = x^k$ has only one child in depth $d+1$. It suffices to show that there exists

$\{\beta_1, \ldots, \beta_k\} \subset D_d$ such that for any $\gamma \neq \delta^k$ and matrix

$$C = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \beta_1 & \cdots & \beta_k & \delta \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{k-1} & \cdots & \beta_k^{k-1} & \delta^{k-1} \\ \beta_1^k & \cdots & \beta_k^k & \gamma \end{bmatrix}$$

we have $\det(C) = 0$. This follows from Lemma 4.

From the principle of induction, the theorem is proved. □

Chapter 4

The Discrete Logarithm Problem over Finite Fields

4.1 Statement of the problem

We start by defining the discrete logarithm problem over finite fields.

Definition 22. *Let $\mathbf{F}_q$ be a finite field of characteristic p and $g \in \mathbf{F}_q$ be a primitive element. Then for each $\alpha \in \mathbf{F}_q^*$, there exists an integer n such that $g^n = \alpha$, which is denoted by $\log_g(\alpha)$. The discrete logarithm problem over finite fields is determining $log_g(\alpha)$ given α.*

Example 16. *Let $p = 11$ be a prime number. One can check that 2 is a primitive root of $\mathbf{Z}/11\mathbf{Z}$, i.e., $(\mathbf{Z}/11\mathbf{Z})^* = \langle 2 \rangle$. It is easy to compute the power of 2 modulo 11 using modular exponentiation. The result is shown in Table 4.1.*

Conversely, we can compute the discrete logarithms of elements based on 2. The result is shown in Table 4.2.

x	1	2	3	4	5	6	7	8	9	10
$2^x \pmod{11}$	2	4	8	5	10	9	7	3	6	1

Table 4.1: Modular exponentiation in $\mathbf{Z}/11\mathbf{Z}$

x	1	2	3	4	5	6	7	8	9	10
$\log_2(x) \pmod{11}$	10	1	8	2	4	9	7	3	6	5

Table 4.2: Discrete logarithms in $\mathbf{Z}/11\mathbf{Z}$

Example 17. *Consider* $\mathbf{F}_{2^3} = \mathbf{F}_2[x]/(f(x))$*, where* $f(x) = x^3+x+1 \in \mathbf{F}_2[x]$ *is irreducible. Let* g *be a root of* $f(x)$*. We compute the power of* g *using modular exponentiation and discrete logarithms of* $\alpha \in \mathbf{F}_{2^3}^*$*. The results are shown in Table 4.3 and Table 4.4, respectively.*

x	g^x
1	g
2	g^2
3	$g+1$
4	g^2+g
5	g^2+g+1
6	g^2+1
7	1

Table 4.3: Modular exponentiation in $\mathbf{F}_{2^3}$

From the above examples, we can see that computing exponentiations and discrete logarithms are inverse operations. If the field size is not too large then both computations are easy. However, in the general case, computing exponentiation is easy and computing discrete logarithms is hard in the sense that we have a polynomial-time algorithm for the former problem (such as exponentiating by squaring) but no such an algorithm for the latter problem. Because of this property, the discrete logarithm problem over finite fields is considered a candidate of one-way function used to construct cryptographic schemes. For example Diffie and Hellman proposed a key exchange protocol

α	$\log_g(\alpha)$
g	1
g^2	2
$g+1$	3
g^2+g	4
g^2+g+1	5
g^2+1	6
1	7

Table 4.4: Discrete logarithms in $\mathbf{F}_{2^3}$

[20] based on the hardness of discrete logarithm problem over finite fields. ElGamal proposed a cryptosystem [23] based on the hardness of discrete logarithm problem over finite fields .

Remark 15. *Parts of the content in this chapter are joint work with Qi Cheng and Daqing Wan and previously appeared in [16].*

4.2 Related work

Denote

$$L_N(\alpha) = \exp(O((\log N)^{\alpha}(\log\log N)^{1-\alpha})),$$

$$L_{N,c}(\alpha) = \exp((c+o(1))((\log N)^{\alpha}(\log\log N)^{1-\alpha})).$$

4.2.1 Generic attacks

Consider the problem of solving discrete logarithms over a cyclic group G with $|G| = N$. Let g be a primitive element of G. In the first step, we assume G is a general group, that is, we do not have additional information on the structure of G.

Shanks [65] proposed the well known baby-step giant-step algorithm,

which is deterministic. The basis idea of the algorithm is that we can write $\log_g(\alpha) = i_0 m + j_0$, where $m = \lceil \sqrt{N} \rceil$ and $0 \leqslant i_0 \leqslant m-1, 0 \leqslant j_0 \leqslant m$. The algorithm consists of two steps:

- Giant-step: compute a list of $L = \{\alpha g^{-j} \mid 0 \leqslant j \leqslant m\}$ and sort the list,
- Baby-step: for each $0 \leqslant i \leqslant m-1$, compute g^{im}; if $g^{i_0 m} = \alpha g^{-j_0} \in L$, stop and return i_0, j_0.

From the baby-step, we get the relation $g^{i_0 m} = \alpha g^{-j_0}$, which implies

$$i_0 m = \log_g(\alpha) - j_0.$$

Thus we have

$$\log_g(\alpha) = i_0 m + j_0.$$

The running time of Shanks' algorithm is $O(\sqrt{N})$. The space requirement is $O(\sqrt{N})$.

Pollard [58] proposed two probabilistic algorithms, namely, the so called kangaroo method and rho method. Both of the algorithms run in expected time $O(\sqrt{N})$ with less space.

4.2.2 Index calculus method

In [55] and [56], the author attributed the basic ideas of index calculus method to Western and Miller [74] and Kraitchik [51]. And the author attributed the invention of the index calculus method to Adleman [1], Merkle [52], and Pollard [58]. This algorithm is a probabilistic one. It is based on the

fundamental property of discrete logarithms that

$$\log \prod_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \log \alpha_i.$$

If we get one relation about a set of variables $\alpha_1, \ldots, \alpha_m$ of the form

$$\prod_{i=1}^{m} \alpha_i^{e_i} = 1,$$

then it implies

$$\sum_{i=1}^{m} e_i \log_g \alpha_i = 0.$$

If we get sufficiently many such relations, we can solve the linear system to get the discrete logarithms $\log_g \alpha_i$ for $1 \leqslant i \leqslant m$. In the index calculus method, this set is called a factor base. The concept of smoothness also plays an important role in the calculus method.

The general framework consists of three phases:

- Phase 1. Finding relations among the logarithms of elements in the factor base (such as via guessing and checking),
- Phase 2. Solving the linear equations to get the logarithms of elements in the factor base,
- Phase 3. Finding individual logarithm by reducing it to the factor base.

Historically, Adleman [1] published the first subexponential time algorithm for the discrete logarithm over finite fields. The original algorithm solves this problem in a prime field, that is, the field size is a prime. The asymptotic running time is $L(1/2)$. Adleman's algorithm relies on similar ideas used by Morrison and Brillhart [54] for factoring integers. They both

make use of the concepts of a factor base and smoothness of an element over the factor base. We describe a modified version of Adleman's algorithm briefly according to the general framework. Suppose we are going to solve the discrete logarithm in $\mathbf{F}_q$ where q is a prime and $q-1=\prod_{i=1}^{i=n} p_i^{e_i}$. Suppose $\mathbf{F}_q^* = \langle g \rangle$ and we want to compute $\log_g(\alpha)$. The plan is to solve $\log_g(\alpha) \pmod{p_j^{e_j}}, 1 \leqslant j \leqslant n$ first, then calculate $\log_g(\alpha) \pmod{q-1}$ using Sun Zi Theorem (Chinese Remainder Theorem).

1. Choose a bound $B = L(1/2, c)$, where c is a small constant. The factor base includes all positive prime numbers less than B. Randomly guess an integer e and test whether g^e is B-smooth. If so, we get

$$g^e = \prod_{p<B} p^{e_p},$$

   which implies

$$e = \sum_{p<B} e_p \log_g(p).$$

   Repeat this until enough linear equations are collected.

2. Solve the linear equations using Gaussian elimination over $\mathbf{Z}_{p_j^{e_j}}$. Thus we get the discrete logarithms of elements in the factor base.

3. To compute the target $\log_g(\alpha)$, we repeat choosing a random integer m until αg^m is B-smooth. If so, then we can compute $\log_g(\alpha)$ from the knowledge of the discrete logarithms of elements in the factor base.

Hellman and Reyneri [33] generalized Adleman's algorithm to a field of fixed characteristic $p \in \mathbf{Z}$. The asymptotic running time of their algorithm is $L(1/2)$. In a field of composite order $|\mathbf{F}_q| = p^k$, the elements are represented

as polynomials. In this case, Hellman and Reyneri [33] make use of smoothness of a polynomial. Consider the field $\mathbf{F}_{2^k} = \mathbf{F}_2[x]/(f(x))$ for example, where $f(x) \in \mathbf{F}_2[x]$ is irreducible with degree k. Suppose $\mathbf{F}_{2^k}^* = \langle g \rangle$ and we want to determine $\log_g(\alpha)$. We still follow the general framework to describe the modified algorithm.

1. Choose a polynomial degree bound $B = L(1/2, c)$, where c is a small constant. The factor base consists of all irreducible polynomials with degree less than B. Randomly guess an integer $0 < e < 2^k - 1$ and test whether g^e is B-smooth. If so, we get

$$g^e = \prod_{\deg(p_i(x)) < B} p_i(x)^{e_{p_i(x)}},$$

   which gives the relation

$$e = \sum_{\deg p_i(x) < B} e_{p_i(x)} \log_g(p_i(x)).$$

   Continue the procedure until we collect enough relations.

2. Solve the linear system over $\mathbf{Z}/(2^k - 1)\mathbf{Z}$ to find the discrete logarithms of elements in the factor base.

3. To compute the target $\log_g(\alpha)$, we repeat choosing a random integer m until αg^m is B-smooth. If so, then we can compute $\log_g(\alpha)$ from the knowledge of the discrete logarithms of elements in the factor base.

To improve the time complexity of Adleman's algorithm, one can speed up the process of finding relations, which plays an essential role in the algorithm. Blake, Mullin, and Vanstone [8] proposed to do so using the idea

of systematic equations. Generalizing the concept of systematic equations, Coppersmith [19] developed the first algorithm with asymptotic time $L(1/3)$ for a field of characteristic 2. Coppersmith's algorithm takes advantage of the Frobenius map and the special representation of the field. Explicitly, let $\mathbf{F}_{2^n} = \mathbf{F}_2[x]/(P(x))$, where $P(x) = x^n + Q(x)$ is irreducible over $\mathbf{F}_2$ of degree n and $Q(x)$ is a low degree polynomial. He chooses k a power of 2 near $\sqrt{n}$ and computes $n = rk - s$, where $0 \leqslant s < k$. Coppersmith then generates his systematic equations through the following way: firstly, he chooses a pair of low degree polynomials $A(x)$ and $B(x)$ such that $\gcd(A(x), B(x)) = 1$. Let $C(x) = x^r A(x) + B(x)$ and $D(x) = C(x)^k$. Then, he reduces the following:

$$\begin{aligned} D(x) &= C(x)^k \mod P(x) \\ &= x^{rk} A(x)^k + B(x)^k \mod P(x) \\ &= x^s Q(x) A(x)^k + B(x)^k \mod P(x). \end{aligned}$$

Both sides of the systematic equation have degrees $O(\sqrt{n})$. Thus the probability for both sides to be smooth is much higher than gx^e for a randomly chosen $0 \leqslant e < 2^k - 1$.

Semaev [64] generalized Coppersmith's algorithm to any field of fixed characteristic.

Adleman and Demarrais [3] developed the first subexponential algorithm for discrete logarithms over all finite fields $\mathbf{F}_{p^n}$ with expected running time $L(1/2)$. Their algorithm consists of two subroutines, both of which are some variations of the index calculus method.

- If $n < p$, they represent the field $\mathbf{F}_{p^n}$ as $\mathcal{O}/(p)$, where $\mathcal{O}$ is some number ring and (p) is the prime ideal generated by p. An element $\alpha \in \mathcal{O}$ is

smooth if the prime ideals in the factorization of (α) have norms below a given bound.

- When $n \geqslant p$, they represent $\mathbf{F}_{p^n}$ by $\mathbf{F}_p[x]/(f(x))$, where $f(x) \in \mathbf{F}_p[x]$ is irreducible with degree n. The element $g(x) \in \mathbf{F}_p[x]/(f(x))$ is smooth if its irreducible factors all have degree less than a given bound.

4.2.3 Number field sieve and function field sieve

The state-of-the-art general-purpose methods for solving the discrete logarithm problem over finite fields are the number field sieve and the function field sieve, which originated from the index-calculus algorithm. All these algorithms run in subexponential time. For a finite field $\mathbf{F}_q$, successful efforts have been made to reduce the heuristic complexity of these algorithms from $L_q(1/2)$ to $L_q(1/3)$.

The number field sieve technique was originally developed to factor big integers N [10, 44]. The generalized number field sieve is the state-of-the-art general-purpose algorithm for factorization.

Inspired by the technique of number field sieve to factor large integers, Gordon [28] introduced the idea of using the number field sieve to solve discrete logarithms in a finite field $\mathbf{F}_p$ of prime order. The asymptotic running time of Gordon's algorithm is $L_p(1/3)$.

Let m be an integer and $f(x) \in \mathbf{Z}[x]$ be an irreducible monic polynomial such that $(p, \Delta_f) = 1$ and $f(m) \equiv 0 \pmod{p}$. Also, let $\alpha \in \mathbf{C}$ be a root of $f(x)$, which is used to construct a number field $K = \mathbf{Q}(\alpha)$. Let $\mathcal{O}_K$ be the ring of algebraic integers in K. Choosing $\mathfrak{p} = (p, \alpha - m)$, Gordon represents

the filed as

$$\mathbf{F}_p \cong \mathcal{O}/\mathfrak{p}.$$

Subsequently, the number field sieve method was investigated further by [40, 61, 62, 63, 72, 73].

Adleman [2] firstly applied the function field sieve to solve discrete logarithms in a field of small characteristic, which is an analogous of the number field sieve. Later, Adleman and Huang [4] made an improvement on the function field sieve. Function field sieve was further studied in [29, 39].

Joux and Lercier [41] developed some variations of function field sieve, which applies to $\mathbf{F}_{q^n}$ where q is a medium-sized prime power. The expected running time is $L(1/3)$. Their key idea is to speed up the sieving stage by an efficient representation of the field.

Joux, Lercier, Smart and Vercauteren [42] studied several variations of the number field sieve, which applies to the case $\mathbf{F}_{p^n}$, where p is a medium to large prime. The asymptotic running time is $L(1/3)$ if n is not too big.

Remarkably, the combination of the above two algorithms solve the discrete logarithms in $\mathbf{F}_{p^n}$ in all cases with heuristic time complexity $L_{p^n}(1/3)$.

4.2.4 Recent breakthroughs

Joux [38] designed the first algorithm with heuristic running time $L(1/4)$ to compute discrete logarithms in a field of small characteristic. Joux's approach combines the features of of Coppersmith's algorithm [19] and Joux-Lercier's method [41] and Joux's pinpointing technique [37]. Joux's $L(1/4)$ algorithm relies on three basic ideas as follows:

1. Joux represents the field $\mathbf{F}_{q^k}$ as $\mathbf{F}_q[x]/(f(x))$ where $f(x)$ is an irre-

ducible factor of $h_1(x)x^q - h_0(x)$, where $h_0(x)$ and $h_1(x)$ are of low degree. The advantage of this representation is that in such a field one has the relation

$$x^q = \frac{h_0(x)}{h_1(x)}.$$

2. Observing the well known fact that

$$X^q - X = \prod_{\alpha \in \mathbf{F}_q} (X - \alpha),$$

Joux uses this equation as his source systematic equation.

3. To amplify the initial systematic equations, Joux makes use of the following homographies:

$$X \to \frac{aX + b}{cX + d}.$$

Also, Gologlu, Granger, McGuire, and Zumbragel [27] made an improvement in the case when characteristic is 2.

Finally, these sequence of breakthrough results [27, 37, 38] recently on the discrete logarithm problem over finite fields culminated in a discovery of a quasi-polynomial algorithm for small characteristic fields, which we call BGJT-algorithm [6, 7]. For a finite field $\mathbf{F}_{q^{2k}}$ with $k < q$, their algorithm runs in heuristic time $q^{O(\log k)}$. This result, if correct, essentially removes the discrete logarithm over small characteristic fields from hard problems in cryptography.

4.3 Right cosets of $PGL_2(\mathbf{F}_q)$ in $PGL_2(\mathbf{F}_{q^2})$

Both [7] and [38] need to compute the right cosets of $PGL_2(\mathbf{F}_q)$ in $PGL_2(\mathbf{F}_{q^2})$ as the preliminary. In this section, we presents an classification of such right cosets.

Proposition 8. *Let $b \in \mathbf{F}_{q^2}, c \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ be variables. Given*

$$v = \frac{b^q - b}{c - c^q} \in \mathbf{F}_q, w = \frac{1 - bc^q}{c - c^q} \in \mathbf{F}_{q^2}, \tag{4.1}$$

let $(b_1, c_1), (b_2, c_2)$ be any two pairs satisfying (4.1). Let

$$A_1 = \begin{pmatrix} 1 & b_1 \\ c_1 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & b_2 \\ c_2 & 1 \end{pmatrix}.$$

If both A_1 and A_2 are not singular, then they are in the same right coset of $PGL_2(\mathbf{F}_q)$ in $PGL_2(\mathbf{F}_{q^2})$.

Proof: From (4.1), we deduce

$$\begin{cases} (c - \frac{w^q}{v})^{q+1} = (\frac{w^q}{v})^{q+1} - \frac{1}{v} \\ b = -vc + w + w^q. \end{cases}$$

Without loss of generality, assume $\gamma^{q+1} = (\frac{w^q}{v})^{q+1} - \frac{1}{v}, \zeta_1^{q+1} = \zeta_2^{q+1} = 1$ and

$$c_1 = \frac{w^q}{v} + \zeta_1\gamma, c_2 = \frac{w^q}{v} + \zeta_2\gamma,$$

where ζ_1, ζ_2 are two distinct $(q+1)$-th roots of unity. Hence

$$b_1 = -vc_1 + w + w^q = w - v\zeta_1\gamma,$$

$$b_2 = -vc_2 + w + w^q = w - v\zeta_2\gamma.$$

It follows that

$$A_1 = \begin{pmatrix} 1 & w - v\zeta_1\gamma \\ \frac{w^q}{v} + \zeta_1\gamma & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & w - v\zeta_2\gamma \\ \frac{w^q}{v} + \zeta_2\gamma & 1 \end{pmatrix}.$$

Since A_2 is not singular, we deduce

$$A_2^{-1} = \frac{1}{\det(A_2)} \begin{pmatrix} 1 & -w + v\zeta_2\gamma \\ -\frac{w^q}{v} - \zeta_2\gamma & 1 \end{pmatrix}.$$

Thus,

$$\begin{aligned} A_1A_2^{-1} &= \frac{1}{\det(A_2)} \begin{pmatrix} (v\zeta_1\gamma - w)(\frac{w^q}{v} + \zeta_2\gamma) + 1 & -v(\zeta_1\gamma - \zeta_2\gamma) \\ \zeta_1\gamma - \zeta_2\gamma & (v\zeta_2\gamma - w)(\frac{w^q}{v} + \zeta_1\gamma) + 1 \end{pmatrix} \\ &= \frac{1}{\det(A_2)} \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}. \end{aligned}$$

Note that $m_{12} = -vm_{21}, m_{11} - m_{22} = (w^q + w)m_{21}$. The last step is to prove $\frac{m_{11}}{m_{21}} \in \mathbf{F}_q$. Let $\delta = \frac{m_{11}}{m_{21}}$. Note that

$$\begin{aligned} \delta \in \mathbf{F}_q &\iff \delta = \delta^q \\ &\iff m_{11}m_{21}^q = m_{11}^q m_{21} \\ &\iff m_{11}m_{21}^q \in \mathbf{F}_q. \end{aligned}$$

Since $\gamma^{q+1} = (\frac{w^q}{v})^{q+1} - \frac{1}{v} = \frac{w^{q+1} - v}{v^2}$, we have $\frac{w^{q+1}}{v} = v\gamma^{q+1} + 1$. Hence

$$m_{11} = w^q\zeta_1\gamma + v\zeta_1\gamma\zeta_2\gamma - w\zeta_2\gamma - v\gamma^{q+1}.$$

Thus

$$m_{11}m_{21}^q = \gamma^{q+1}\{(w^q + w) - (w\zeta_1^q\zeta_2 + w^q\zeta_1\zeta_2^q) + v(\zeta_2\gamma + \zeta_2^q\gamma^q) - v(\zeta_1\gamma + \zeta_1^q\gamma^q)\}.$$

Since

$$\gamma^{q+1} \in \mathbf{F}_q,$$

$$w^q + w \in \mathbf{F}_q, w\zeta_1^q\zeta_2 + w^q\zeta_1\zeta_2^q \in \mathbf{F}_q,$$

$$\zeta_2\gamma + \zeta_2^q\gamma^q \in \mathbf{F}_q, \zeta_1\gamma + \zeta_1^q\gamma^q \in \mathbf{F}_q,$$

we deduce $m_{11}m_{21}^q \in \mathbf{F}_q$, which implies $\frac{m_{11}}{m_{21}} \in \mathbf{F}_q$ and $\frac{m_{22}}{m_{21}} \in \mathbf{F}_q$. Thus

$$A_1A_2^{-1} = \frac{\zeta_1\gamma - \zeta_2\gamma}{\det(A_2)} \begin{pmatrix} \frac{m_{11}}{m_{21}} & -v \\ 1 & \frac{m_{22}}{m_{21}} \end{pmatrix}$$
$$\in PGL_2(q),$$

which implies that A_1 and A_2 are in the same right coset of of $PGL_2(\mathbf{F}_q)$ in $PGL_2(\mathbf{F}_{q^2})$. □

Remark 16. *Following an approach similar to this one, one can also prove that A_1 and A_2 are in the same left coset of of $PGL_2(\mathbf{F}_q)$ in $PGL_2(\mathbf{F}_{q^2})$.*

Proposition 9. *Let $\mathbf{F}_{q^2}^* = \langle g \rangle$. Each representative of a right coset of $PGL_2(\mathbf{F}_q)$ in $PGL_2(\mathbf{F}_{q^2})$ is equivalent to one of the following four types:*

1. $\begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix}$, *where* $b, c \in \mathbf{F}_{q^2}$.

2. $\begin{pmatrix} 1 & b_1 \\ g & d_2 g \end{pmatrix}$, *where* $b_1, d_2 \in \mathbf{F}_q$.

3. $\begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix}$, *where* $c, d \in \mathbf{F}_{q^2}$.

4. $\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix}$, *where* $c, d \in \mathbf{F}_{q^2}$.

Proof: We determine the equivalence relation case by case. Let

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_1 + a_2 g & b_1 + b_2 g \\ c_1 + c_2 g & d_1 + d_2 g \end{pmatrix}$$

be a representative of a right coset of $PGL_2(\mathbf{F}_q)$ in $PGL_2(\mathbf{F}_{q^2})$, where

$$a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in \mathbf{F}_q.$$

First of all, if $a = 0$, then the matrix can be reduced to type (3) after dividing b since $b \neq 0$. In the following, we assume $a \neq 0$. Without loss of generality, we assume $a = 1$ and consider the matrix

$$\begin{pmatrix} 1 & b_1 + b_2 g \\ c_1 + c_2 g & d_1 + d_2 g \end{pmatrix}.$$

We have the following cases:

Case I. $b_2 \neq 0$

Subtracting $\frac{d_2}{b_2}$ times the first row from the second row, the matrix be-

comes

$$\begin{pmatrix} 1 & b \\ c' & d_1' \end{pmatrix},$$

where $c' \in \mathbf{F}_{q^2}, d_1' \in \mathbf{F}_q$.

1. If $d_1' = 0$, the matrix is equivalent to type (4).

2. If $d_1' \neq 0$, the matrix is equivalent to type (1) since we can divide the second row by d_1'.

Case II. $b_2 = 0$

If $b_1 = 0$, then the matrix is equivalent to type (4).

If $b_1 \neq 0$, then the matrix becomes

$$\begin{pmatrix} 1 & b_1 \\ c' = c_1' + c_2' g & d_2 g \end{pmatrix}$$

after subtracting d_1/b_1 times first row from the second row.

1. If $d_2 = 0$, then the matrix can be reduced to type (4).

2. Assume $d_2 \neq 0$.

   (a) If $c_1' = 0, c_2' = 0$, then the matrix can be reduced to type (3).

   (b) If $c_1' = 0, c_2' \neq 0$, then the matrix can be reduced to type (2) by dividing the second row by c_2'.

   (c) If $c_1' \neq 0$, subtracting $\frac{1}{c_1'}$ times the second row from the first row, we get

$$\begin{pmatrix} -\frac{c_2'}{c_1'} g & b' \\ c' & d_2 g \end{pmatrix}.$$

Dividing the matrix by g, we get

$$\begin{pmatrix} -\frac{c_2'}{c_1'} & b'g^{-1} \\ c'g^{-1} & d_2 \end{pmatrix}.$$

i. If $c_2' = 0$, the matrix can be reduced to type (3).

ii. If $c_2' \neq 0$, dividing the first row by $-\frac{b_2'}{b_1'}$ and the second row by d_2, the matrix is reduced to type (1).

□

Proposition 10. *Let*

$$\begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ c_1 + c_2 g & d_1 + d_2 g \end{pmatrix}$$

be one representative of a right coset of $PGL_2(\mathbf{F}_q)$ *in* $PGL_2(\mathbf{F}_{q^2})$*, where* $c_1, c_2, d_1, d_2 \in \mathbf{F}_q$*. Then it is equivalent to one of the following types:*

1. $\begin{pmatrix} 0 & 1 \\ g & \beta_2 g \end{pmatrix}$, *where* $\beta_2 \in \mathbf{F}_q$.

2. $\begin{pmatrix} 0 & 1 \\ 1 + \alpha_2 g & \beta_2 g \end{pmatrix}$, *where* $\alpha_2, \beta_2 \in \mathbf{F}_q$.

Proof: There are two cases to consider.

1. Assume $c_1 = 0$. If $d_1 \neq 0$, subtracting d_1 times the first row from the second row, we get

$$\begin{pmatrix} 0 & 1 \\ c_2 g & d_2 g \end{pmatrix}.$$

If $d_1 = 0$, then the matrix is of the above form already. Since $c_2 \neq 0$, after dividing the second row by c_2, the matrix is reduced to type (1).

2. Assume $c_1 \neq 0$. If $d_1 \neq 0$, subtracting d_1 times the first row from the second row, we get

$$\begin{pmatrix} 0 & 1 \\ c_1 + c_2 g & d_2 g \end{pmatrix}.$$

If $d_1 = 0$, then the matrix is of the above form already. Dividing the second row by c_1, we get

$$\begin{pmatrix} 0 & 1 \\ 1 + c_2 g & \frac{d_2}{c_1} g \end{pmatrix}.$$

Thus the matrix is reduced to type (2).

□

Similarly, we have the following conclusion.

Proposition 11. *Let*

$$\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c_1 + c_2 g & d_1 + d_2 g \end{pmatrix}$$

be one representative of a right coset of $PGL_2(\mathbf{F}_q)$ in $PGL_2(\mathbf{F}_{q^2})$. Then it is equivalent to one of the following types:

1. $\begin{pmatrix} 1 & 0 \\ \alpha_2 g & g \end{pmatrix}$, *where* $\alpha_2 \in \mathbf{F}_q$.

2. $\begin{pmatrix} 1 & 0 \\ \alpha_2 g & 1+\beta_2 g \end{pmatrix}$, *where* $\alpha_2, \beta_2 \in \mathbf{F}_q$.

4.4 Where does the computation of the original BGJT algorithm really happen?

Suppose that we need to compute discrete logarithm in the field $\mathbf{F}_{q^{2k}}$, where $q > k > 1$. A main technique in [6], which bases on smooth polynomials, is to find a nice ring generator ζ of $\mathbf{F}_{q^{2k}} = \mathbf{F}_{q^2}[\zeta]$ over $\mathbf{F}_{q^2}$ satisfying

$$x^q = h_0(x)/h_1(x),$$

where h_1 and h_0 are polynomials of very small degree. In many places of the computation, polynomial degrees can be dropped quickly by replacing x^q with $h_0(x)/h_1(x)$, which allows an effective attack based on smoothness.

The main issue with this approach is that the computation really takes place in the ring $\mathbf{F}_{q^2}[x]/(x^q h_1(x) - h_0(x))$, where in the analysis of [6], the computation is assumed to be in $\mathbf{F}_{q^2}[x]/(f(x))$, where $f(x)$ is the minimal polynomial of ζ over $\mathbf{F}_{q^2}$. Since $f(x)$ divides $x^q h_1(x) - h_0(x)$, there is a natural surjective ring homomorphism

$$\mathbf{F}_{q^2}[x]/(x^q h_1(x) - h_0(x)) \to \mathbf{F}_{q^2}[x]/(f(x)).$$

But the former ring, which is a direct sum of the latter field (if $f(x)$ is a simple factor of $x^q h_1(x) - h_0(x)$) and a few other rings, is much larger in many cases. The computation thus can be affected by the other rings, rendering several

conjectures in [6, 38] problematic.

Interestingly, for the Kummer extension of the form $\mathbf{F}_{q^2}[x]/(x^{q-1} - a)$, everything is fine. This is because the difference between the ring $\mathbf{F}_{q^2}[x]/(x^q - ax)$ and the field is rather small. The discrete logarithm of x, which is a zero divisor in the former ring, can be computed easily in the latter field, since it belongs to a subgroup of a small order (dividing $(q-1)(q^2-1)$) in the field. This is consistent with all announced practical implementations.

However, in case of more difficult non-Kummer extensions, we discover that there are multiple problems.

1. First, if $x^q h_1(x) - h_0(x)$ has linear factors over $\mathbf{F}_{q^2}$, the discrete logarithms of these linear factors cannot be computed in polynomial time, invalidating a basic assumption in [6]. One can verify that most of polynomials given in [38, Table 1] have linear factors.

2. Second, even at the stage of finding discrete logarithms of linear elements, we show that there are additional serious restrictions on the choice of $h_0(x)$ and $h_1(x)$. For example, if $x^q h_1(x) - h_0(x)$ has another irreducible factor over $\mathbf{F}_{q^2}$ of degree k_i satisfying $\gcd(k_i, k) > 1$, we do not see how the algorithm can work. We propose to select $h_0(x)$ and $h_1(x)$ such that $x^q h_1(x) - h_0(x)$ has only one irreducible factor $f(x)$ over $\mathbf{F}_{q^2}$ of degree k, and all other irreducible factors over $\mathbf{F}_{q^2}$ have degrees bigger than one and relatively prime to k. Under these assumptions, we give an algorithm which will find the discrete logarithm of any linear element in polynomial time, under a heuristic assumption supported by our theoretical results and numerical data.

3. For a non-linear element, a clever idea, the so-called QPA-descent, was

proposed in [6] to reduce its degree, until its relation to linear factors can be found. While the above two problems about linear factors can be fixed under our newly improved heuristic assumptions, another serious problem is that there are *traps* in the QPA-descent. For these traps, the QPA-descent described in [6] will not work at all. They will also block the descent of other elements, hence severely affecting the usefulness of the new algorithm.

4.5 Finding primitive elements and discrete logarithms of linear factors

4.5.1 Using SNF of relation matrices to determine group structures

Firstly, we recall the definition of the finitely generated group [21].

Definition 23. *Let G be a group written multiplicatively. It is finitely generated if there exists $\{g_1, \ldots, g_n\} \subset G$ such that for any $\alpha \in G$, there exist $e_1, \ldots, e_m \in \mathbf{Z}$ such that*

$$\alpha = \prod_{i=n}^{m} g_i^{e_i}.$$

The following is the well known fundamental theorem of finitely generated abelian groups [21]:

Theorem 9. *Let G be a finitely generated abelian group. Then there is an isomorphism*

$$G \cong \mathbf{Z}^r \times \mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n_s\mathbf{Z},$$

where $r, s \geqslant 0$, $n_1 \geqslant 2$ *and* $n_i | n_{i+1}$ *for* $1 \leqslant i \leqslant s-1$. *Furthermore, the* r *and* n_i *are uniquely determined by* G. *The integer* r *is called the free rank or Betti number of* G *and* $n_1, n_2, \ldots, n_s$ *are called the invariant factors of* G. *The isomorphic expression of* G *is called the invariant factor decomposition of* G.

Let G be a finite abelian group of order $|N|$. Enge [24] developed an algorithm to determine the structure of G. The basic idea is to compute the SNF of the relation lattice. We describe this method briefly. Let the factor base $S = \{g_1, g_2, \ldots, g_n\}$ be sufficiently large such that it generates G. Consider the group homomorphism

$$\phi : \mathbf{Z}^n \to G$$

given by

$$(e_1, e_2, \ldots, e_n) \mapsto \prod_{i=1}^{n} g_i^{e_i}.$$

Since S generates G, ϕ is surjective and its kernel Γ is a full-dimensional lattice of determinant N such that $G \cong \mathbf{Z}^n/\Gamma$. Thus the object of determining the structure of G is reduced to determining the structure of $\mathbf{Z}^n/\Gamma$.

Enge's algorithm thus consists of two phases:

1. Collecting relations to construct a relation matrix A which approaches Γ well by some criterion.

2. Computing the SNF of A to find the invariant factors of G and the generators.

4.5.2 Finding the discrete logarithm of the linear factors

We first review the new algorithm in [6, 7]. Suppose that the discrete logarithm is sought over the field $\mathbf{F}_{q^{2k}}$ with $k < q$. For other small characteristic fields, for example, $\mathbf{F}_{p^k}$ ($p < k$), one first embeds it into a slightly larger field:

$$\mathbf{F}_{p^k} \rightarrow \mathbf{F}_{q^k} \rightarrow \mathbf{F}_{q^{2k}}$$

where $q = p^{\lceil \log_p k \rceil}$. A quasi-polynomial time algorithm for $\mathbf{F}_{q^{2k}}$ implies a quasi-polynomial time algorithm for $\mathbf{F}_{p^k}$. We assume that

$$\mathbf{F}_{q^{2k}} = \mathbf{F}_{q^2}[\zeta]$$

where $\zeta^q = \frac{h_0(\zeta)}{h_1(\zeta)}$. Here h_0 and h_1 are polynomials over $\mathbf{F}_{q^2}$ relatively prime to each other, and of a constant degree. In particular, $\deg(h_0) < q + \deg(h_1)$. To find such a nice ring generator ζ, one searches over all the polynomials $h_0(x)$ and $h_1(x)$ of a constant degree in $\mathbf{F}_{q^2}[x]$, until $h_1(x)x^q - h_0(x)$ has an irreducible factor $f(x)$ of degree k with multiplicity one. Let the factorization be

$$x^q h_1(x) - h_0(x) = f(x) \prod_{i=1}^{l} (f_i(x))^{a_i} \tag{4.2}$$

where the polynomials $f(x)$ and $f_i(x)$'s are irreducible and pair-wise prime. Denote the degree of $f_i(x)$ by k_i.

Remark 17. *In practice, it is enough to search only a quadratic polynomial h_0 (not necessarily monic) and a monic linear polynomial h_1 in $\mathbf{F}_{q^2}[x]$. However, proving the existence of such polynomials for any constant degree such*

that $x^q h_1(x) - h_0(x)$ has the desired factorization pattern seems to be out of reach by current techniques.

For simplicity we assume that $h_1(x)$ is monic and linear. Most of the known algorithms start by computing the discrete logarithms of elements in a special set called a factor base, which usually contains small integers, or low degree polynomials. In the new approach [6, 7, 38], the factor base consists of the linear polynomials $\zeta + \alpha$ for all $\alpha \in \mathbf{F}_{q^2}$, and an algorithm is designed to compute the discrete logarithms of all the elements in the factor base. It is conjectured that this algorithm runs in polynomial time. One starts the algorithm with the identity:

$$\prod_{\alpha \in \mathbf{F}_q} (x - \alpha) = x^q - x.$$

Then apply the Möbius transformation

$$x \mapsto \frac{ax + b}{cx + d}$$

where the matrix $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{F}_{q^2}^{2\times 2}$ is nonsingular. We have

$$\prod_{\alpha \in \mathbf{F}_q} (\frac{ax + b}{cx + d} - \alpha) = (\frac{ax + b}{cx + d})^q - \frac{ax + b}{cx + d}.$$

Clearing the denominator:

$$\begin{aligned} & (cx+d)\prod_{\alpha\in\mathbf{F}_q}((ax+b)-\alpha(cx+d)) \\ = \;& (ax+b)^q(cx+d)-(ax+b)(cx+d)^q \\ = \;& (a^qx^q+b^q)(cx+d)-(ax+b)(c^qx^q+d^q). \end{aligned}$$

Multiplying both sides by $h_1(x)$ and replacing $x^q h_1(x)$ by $h_0(x)$, we obtain

$$\begin{aligned} & h_1(x)(cx+d)\prod_{\alpha\in\mathbf{F}_q}((ax+b)-\alpha(cx+d)) \\ = \;& (a^qh_0(x)+b^qh_1(x))(cx+d)-(ax+b)(c^qh_0(x)+d^qh_1(x)) \\ & \pmod{x^qh_1(x)-h_0(x)}. \end{aligned}$$

If the right-hand side can be factored into a product of linear factors over $\mathbf{F}_{q^2}$, we obtain a relation of the form

$$\lambda^{e_0}\prod_{i=1}^{q^2}(x+\alpha_i)^{e_i}=\prod_{i=1}^{q^2}(x+\alpha_i)^{e_i'} \pmod{x^qh_1(x)-h_0(x)}, \qquad (4.3)$$

where λ is a multiplicative generator of $\mathbf{F}_{q^2}$, $\alpha_1 = 0, \alpha_2, \alpha_3, \ldots, \alpha_{q^2}$ is a natural ordering of elements in $\mathbf{F}_{q^2}$, and e_i's and e_i''s are non-negative integers.

Following the same notations in [6], let $\mathcal{P}_q$ be a set of representatives of the right cosets of $PGL_2(\mathbf{F}_q)$ in $PGL_2(\mathbf{F}_{q^2})$. Note that the cardinality of $\mathcal{P}_q$ is q^3+q. It was shown in [6, 38] that the matrices in the same coset produce the same relation (4.3).

Suppose that for some $1 \leqslant g \leqslant q^2$, $\zeta+\alpha_g$ is a known multiplicative generator of $\mathbf{F}_{q^2}[\zeta] = \mathbf{F}_{q^2}[x]/(f(x))$. Since (4.3) also holds modulo $f(x)$,

taking the discrete logarithm with respect to the base $\zeta + \alpha_g$, we obtain

$$e_0 \log_{\zeta+\alpha_g} \lambda + \sum_{1 \leqslant i \leqslant q^2, i \neq g} (e_i - e'_i) \log_{\zeta+\alpha_g}(\zeta+\alpha_i) \equiv e'_g - e_g \pmod{q^{2k}-1}. \quad (4.4)$$

The above equation gives us a linear relation among the discrete logarithm of linear factors. One hopes to collect enough relations such that the linear system formed by those relations is non-singular over $\mathbf{Z}/(q^{2k}-1)\mathbf{Z}$. It allows us to solve $\log_{\zeta+\alpha_g}(\zeta + \alpha_i)$ for all the $\zeta + \alpha_i$ in the factor base.

However, if for some $1 \leqslant z \leqslant q^2$,

$$(x + \alpha_z) | x^q h_1(x) - h_0(x),$$

the algorithm will unlikely compute $\log_{\zeta+\alpha_g}(\zeta + \alpha_z)$. It is because that $x + \alpha_z$ is zero or nilpotent (without loss of generality let $f_1 = x + \alpha_z$) in the $\mathbf{F}_{q^2}[x]/((x + \alpha_z)^{a_1})$ component of the ring

$$\mathbf{F}_{q^2}[x]/(x^q h_1(x) - h_0(x)) = \mathbf{F}_{q^2}[x]/(f(x)) \oplus \bigoplus_{i=1}^{l} \mathbf{F}_{q^2}[x]/(f_i(x)^{a_i}).$$

Hence in (4.3), if $e_z > 0$, e'_z is positive as well. Most likely we will have $e_z = e'_z$, so the coefficient for $\log_{\zeta+\alpha_g}(\zeta + \alpha_z)$ in (4.4) will always be 0.

Remark 18. *If $e'_z > e_z \geqslant 1$, it is possible to compute $\log_{\zeta+\alpha_g}(\zeta + \alpha_z)$. However, this requires the low degree polynomial in the right hand side of (4.3) to have the factor $(x + \alpha_z)^2$, which is unlikely. Our numerical data confirm that it never happens when q is sufficiently large.*

To compute the discrete logarithm of $\zeta + \alpha_z$, we have to use additional relations which hold for the field $\mathbf{F}_{q^2}[\zeta]$ but may not hold for the bigger ring

$\mathbf{F}_{q^2}[x]/(x^q h_1(x) - h_0(x))$. The equation

$$(\zeta + \alpha_z)^{q^{2k}-1} = 1$$

is such an example. But this does not help in computing its discrete logarithm in the field $\mathbf{F}_{q^2}[\zeta]$, if it is the only relation involving $\zeta + \alpha_z$.

In general, it is hard to find useful additional relations for $x + \alpha_z$, since for the algorithm to work, it is essential that we replace x^q by $h_0(x)/h_1(x)$ (not replace $f(x)$ by zero) in the relation generating stage. Hence it is not clear that the discrete logarithm of $\zeta + \alpha_z$ can be computed in polynomial time, invalidating a conjecture in [6].

Remark 19. *An exception is in the case of a Kummer extension, where the zero divisor x in the ring has a small order in the field.*

4.5.3 The tale of two lattices

To fix the above problem in a non-Kummer case, we can either change our factor base to not include the linear factors of $x^q h_1(x) - h_0(x)$, or we can search for h_0 and h_1 such that $x^q h_1(x) - h_0(x)$ does not have linear factors. In the following discussion, we will assume that $x^q h_1(x) - h_0(x)$ has no linear factor for simplicity. That is,

$$k_i := \deg(f_i) \geqslant 2 \ (1 \leqslant i \leqslant l).$$

In this case, the linear factors $x+\alpha_i$'s are invertible in the ring $\mathbf{F}_{q^2}[x]/(x^q h_1(x) - h_0(x))$ and equation (4.3) reduces to

$$\lambda^{e_0} \prod_{i=1}^{q^2} (x+\alpha_i)^{e_i - e_i'} = 1 \pmod{x^q h_1(x) - h_0(x)}. \tag{4.5}$$

We define two fundamental lattices in $\mathbf{Z}^{q^2+1}$:

$$\begin{aligned}
\mathcal{L}_1 &= \{(e_0, e_1, \ldots, e_{q^2}) | \lambda^{e_0} \prod_{i=1}^{q^2} (x+\alpha_i)^{e_i} = 1 \pmod{f(x)}\}, \\
\mathcal{L}_2 &= \{(e_0, e_1, \ldots, e_{q^2}) | \lambda^{e_0} \prod_{i=1}^{q^2} (x+\alpha_1)^{e_i} = 1 \pmod{x^q h_1(x) - h_0(x)}\}.
\end{aligned}$$

It is easy to see that $\mathcal{L}_2 \subseteq \mathcal{L}_1$. Consider the group homomorphism

$$\psi_1 : \mathbf{Z}^{q^2+1} \to (\mathbf{F}_{q^2}[x]/(f(x)))^*$$

given by

$$(e_0, e_1, \ldots, e_{q^2}) \mapsto \lambda^{e_0} \prod_{i=1}^{q^2} (x+\alpha_i)^{e_i}.$$

The group homomorphism ψ_2 is defined in the same way, except that modulo $f(x)$ is replaced by modulo $(x^q h_1(x) - h_0(x))$.

Cheng and Wan proved Theorem 10 and Theorem 11 in [13]. We include their proofs for the sake of completeness.

Theorem 10. *If* $\deg(h_1) \leqslant 2$, *then the maps* ψ_1 *and* ψ_2 *are surjective.*

Proof: It is enough to prove that ψ_2 is surjective. If not, the image H of ψ_2 would be a proper subgroup of $(\mathbf{F}_{q^2}[x]/(x^q h_1(x) - h_0(x)))^*$. We can then choose a non-trivial character χ of $(\mathbf{F}_{q^2}[x]/(x^q h_1(x) - h_0(x)))^*$ which is trivial on the subgroup H. Since χ is trivial on H which contains $\mathbf{F}_{q^2}^*$, we

can use the Weil bound as given in Theorem 2.1 in [71] and deduce that

$$1 + q^2 = |1 + \sum_{\alpha \in \mathbf{F}_{q^2}} \chi(x + \alpha)| \leqslant (q + \deg(h_1) - 2)\sqrt{q^2} \leqslant q^2.$$

This is a contradiction. It follows that ψ_2 must be surjective. □

Note that in the application of computing discrete logarithms, it is important that ψ_1 is surjective. As a corollary, we obtain

Corollary 2. *If* $\deg(h_1) \leqslant 2$, *then*

- *the group* $\mathbf{Z}^{q^2+1}/\mathcal{L}_1$ *is isomorphic to the cyclic group* $\mathbf{Z}/(q^{2k} - 1)\mathbf{Z}$,
- *the group* $\mathbf{Z}^{q^2+1}/\mathcal{L}_2$ *is isomorphic to*

$$\mathbf{Z}/(q^{2k} - 1)\mathbf{Z} \oplus \bigoplus_{i=1}^{l} \mathbf{Z}/(q^{2k_i} - 1)\mathbf{Z} \bigoplus (a \textit{ finite } p\textit{-group}).$$

In particular, the group $\mathbf{Z}^{q^2+1}/\mathcal{L}_2$ is not cyclic when $l \geqslant 1$. The relation generation stage only gives lattice vectors in $\mathcal{L}_2$, which is far from the $\mathcal{L}_1$ if $l \geqslant 1$. Thus, we need to add more relations to $\mathcal{L}_2$ in order to get close to $\mathcal{L}_1$.

Since $\lambda^{q^2-1} = 1$, the vector $(q^2 - 1, 0, \ldots, 0)$ is automatically in $\mathcal{L}_2$. Let $\mathcal{L}_2^*$ be the lattice in $\mathbf{Z}^{q^2+1}$ generated by $\mathcal{L}_2$ and the following q^2 vectors

$$(0, q^{2k} - 1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 0, q^{2k} - 1),$$

corresponding to the relations $(x + \alpha_i)^{q^{2k}-1} = 1$ modulo $f(x)$ for $\alpha_i \in \mathbf{F}_{q^2}$. It is clear that

$$\mathcal{L}_2^* = \mathcal{L}_2 + (q^{2k} - 1)\mathbf{Z}^{q^2+1}.$$

The next result gives the group structure for the quotient $\mathbf{Z}^{q^2+1}/\mathcal{L}_2^*$.

Theorem 11. *For $deg(h_1) \leqslant 2$, there is a group isomorphism*

$$\mathbf{Z}^{q^2+1}/\mathcal{L}_2^* \cong \mathbf{Z}/(q^{2k}-1)\mathbf{Z} \oplus \bigoplus_{1 \leqslant i \leqslant l} \mathbf{Z}/(q^{2\gcd(k,k_i)}-1)\mathbf{Z}.$$

Proof: Recall that

$$\mathbf{Z}^{q^2+1}/\mathcal{L}_2 \cong A \stackrel{\text{def}}{=} \mathbf{Z}/(q^{2k}-1)\mathbf{Z} \oplus \bigoplus_{i=1}^{l} \mathbf{Z}/(q^{2k_i}-1)\mathbf{Z} \bigoplus (\text{a finite } p\text{-group}).$$

It is clear that

$$A/(q^{2k}-1)A \cong \mathbf{Z}/(q^{2k}-1)\mathbf{Z} \oplus \bigoplus_{1 \leqslant i \leqslant l} \mathbf{Z}/(q^{2\gcd(k_i,k)}-1)\mathbf{Z}.$$

The kernel of the surjective composed homomorphism

$$\mathbf{Z}^{q^2+1} \longrightarrow \mathbf{Z}^{q^2+1}/\mathcal{L}_2 \cong A \longrightarrow A/(q^{2k}-1)A$$

is precisely $\mathcal{L}_2 + (q^{2k}-1)\mathbf{Z}^{q^2+1} = \mathcal{L}_2^*$. The desired isomorphism follows.

□

If $\gcd(k_i, k) > 1$ for some i, then $\mathcal{L}_2^*$ is still far from $\mathcal{L}_1$. We would like $\mathcal{L}_2^*$ to be as close to $\mathcal{L}_1$ as possible in a smooth sense. For us, the more interesting case is the following

Corollary 3. *Let $deg(h_1) \leqslant 2$. If $\gcd(k_i, k) = 1$ for all $1 \leqslant i \leqslant l$, we have an isomorphism*

$$\mathbf{Z}^{q^2+1}/\mathcal{L}_2^* \cong \mathbf{Z}/(q^{2k}-1)\mathbf{Z} \oplus (\mathbf{Z}/(q^2-1)\mathbf{Z})^l.$$

This corollary shows that under the same assumption, the lattice $\mathcal{L}_2^*$ is a smooth approximation of $\mathcal{L}_1$ in the sense that the quotient $\mathcal{L}_1/\mathcal{L}_2^*$ is a direct sum of small order cyclic groups.

The algorithm to compute the discrete logarithms in the factor base essentially samples vectors from the lattice $\mathcal{L}_2$. Let $\mathbf{r}_1, \mathbf{r}_2, \ldots$ be the vectors in $\mathcal{L}_2$ obtained by the relation-finding algorithm, i.e., from the relations in (4.5). Let $\hat{\mathcal{L}}_2$ be the lattice generated by those vectors. Let $\hat{\mathcal{L}}_1$ be the lattice generated by $\hat{\mathcal{L}}_2$ and the following q^2+1 vectors:

$$(q^2-1, 0, \ldots, 0), (0, q^{2k}-1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 0, q^{2k}-1).$$

Computing the Hermite (or Smith) Normal Form of $\hat{\mathcal{L}}_1$ is equivalent to solving the linear system $\hat{\mathcal{L}}_2$ in the ring $\mathbf{Z}/(q^{2k}-1)\mathbf{Z}$. It is in general difficult to find bases for the two lattices $\mathcal{L}_1$ and $\mathcal{L}_2$ directly. One can think that $\hat{\mathcal{L}}_1$ and $\hat{\mathcal{L}}_2$ are the approximations of $\mathcal{L}_1$ and $\mathcal{L}_2$, respectively. These approximations can be computed by the polynomial time algorithm. Obviously,

$$\begin{array}{c} \hat{\mathcal{L}}_2 \\ \\ \end{array} \begin{array}{c} \subseteq \mathcal{L}_2 \subseteq \\ \subseteq \hat{\mathcal{L}}_1 \subseteq \end{array} \mathcal{L}_2^* \subseteq \mathcal{L}_1.$$

These inclusions induce surjective group homomorphisms

$$\mathbf{Z}^{q^2+1}/\hat{\mathcal{L}}_2 \begin{array}{c} \rightarrow \mathbf{Z}^{q^2+1}/\mathcal{L}_2 \rightarrow \\ \rightarrow \mathbf{Z}^{q^2+1}/\hat{\mathcal{L}}_1 \rightarrow \end{array} \mathbf{Z}^{q^2+1}/\mathcal{L}_2^* \rightarrow \mathbf{Z}^{q^2+1}/\mathcal{L}_1.$$

If $\mathbf{Z}^{q^2+1}/\hat{\mathcal{L}}_2$ is cyclic, then its quotient $\mathbf{Z}^{q^2+1}/\mathcal{L}_2$ will be cyclic. This is false if $l \geqslant 1$ as we have seen before. Similarly, $\mathbf{Z}^{q^2+1}/\hat{\mathcal{L}}_1$ is not cyclic as its quotient

$\mathbf{Z}^{q^2+1}/\mathcal{L}_2^*$ is not cyclic if $l \geqslant 1$. Hence the conjecture in [35] also needs modification. It seems reasonable to hope that $\hat{\mathcal{L}}_1$ is a good approximation to $\mathcal{L}_2^*$ in the sense that the quotient $\mathcal{L}_2^*/\hat{\mathcal{L}}_1$ is a direct sum of small order cyclic groups. In the interesting case where $\gcd(k, k_i) = 1$ for all $1 \leqslant i \leqslant l$, our numerical data suggest the following heuristic is highly plausible.

Heuristic 1. *Assume that $x^q h_1(x) - h_0(x)$ does not have linear factors, and $\gcd(k, k_i) = 1$ for all $1 \leqslant i \leqslant l$. Then in the SNF of $\hat{\mathcal{L}}_1$, the diagonal elements are*

$$1, 1, \ldots, 1, s_1, \ldots, s_t, q^{2k} - 1,$$

where for $1 \leqslant i \leqslant t$, $s_i > 1$ and $s_i | q^2 - 1$.

Example 18. *Let $q = 16, k = 11$ and $\mathbf{F}_{q^2} = \langle \lambda \rangle$.*

In the first step, we choose the appropriate $h_0(x)$ and $h_1(x)$ as follows:

$$h_0(x) = \lambda * x^2 + \lambda^4 * x + 1,$$

$$h_1(x) = x + \lambda.$$

Thus we have the polynomial

$$h_1(x) * x^{16} - h_0(x) = x^{17} + \lambda * x^{16} + \lambda * x^2 + \lambda^4 * x + 1.$$

The two irreducible factors of $h_1(x) * x^{16} - h_0(x)$ over $\mathbf{F}_{q^2}$ are of degree 11 and 6, respectively.

After collecting the relations and generating the SNF, the SNF is given

by $[A|B]$*, where* B *is a zero matrix and*

$$A = \begin{bmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 15 & & & & \\ & & & & 15 & & & \\ & & & & & 255 & & \\ & & & & & & 309485009821345068724781055 & \end{bmatrix}_{257\times 257}.$$

Note that $16^{2\times 11} - 1 = 309485009821345068724781055$.

Example 19. *Let* $q = 16, k = 13$ *and* $\mathbf{F}_{q^2} = \langle\lambda\rangle$.

In the first step, we choose the appropriate $h_0(x)$ *and* $h_(x)$ *as follows:*

$$h_0(x) = \lambda * x^2 + \lambda^7 * x + 1,$$

$$h_1(x) = x + \lambda.$$

Thus we have the polynomial

$$h_1(x) * x^{16} - h_0(x) = x^{17} + \lambda * x^{16} + \lambda * x^2 + \lambda^7 * x + 1.$$

The two irreducible factors of $h_1(x) * x^{16} - h_0(x)$ *over* $\mathbf{F}_{q^2}$ *are of degree* 13 *and* 4*, respectively.*

After collecting the relations and generating the SNF, the SNF is given

by $[A|B]$*, where* B *is a zero matrix and*

$$A = \begin{bmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & 15 & & & & & \\ & & & & 15 & & & & \\ & & & & & 15 & & & \\ & & & & & & 15 & & \\ & & & & & & & 255 & \\ & & & & & & & & 2028240960365167042394725128601 5 \end{bmatrix}_{257\times 257}.$$

Note that $16^{2\times 13} - 1 = 2028240960365167042394725128601 5$.

Assuming the heuristics, $\mathbf{Z}^{q^2+1}/\hat{\mathcal{L}}_1$ is not much bigger than $\mathbf{Z}^{q^2+1}/\mathcal{L}_1$, namely,

$$\mathbf{Z}^{q^2+1}/\hat{\mathcal{L}}_1 \cong \mathbf{Z}/s_1\mathbf{Z} \oplus \mathbf{Z}/s_2\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/s_t\mathbf{Z} \oplus \mathbf{Z}/(q^{2k}-1)\mathbf{Z}.$$

We can find a generator for each component, as a product of linear polynomials from the computation of the SNF. Suppose that for $1 \leqslant i \leqslant t$, the generator for the i-th component is

$$\lambda^{e_{i0}} \prod_{1\leqslant j\leqslant q^2} (x+\alpha_j)^{e_{ij}}.$$

Since $s_i | q^2-1$, the above generator belongs to $\mathbf{F}_{q^2}$ in $\mathbf{F}_{q^2}[x]/(f(x))$. Assuming

that it is $\lambda^{e'_{i0}}$, we have

$$\lambda^{e_{i0}-e'_{i0}} \prod_{1 \leqslant j \leqslant q^2} (x+\alpha_j)^{e_{ij}} = 1 \pmod{f(x)}.$$

There are t such relations. Adding them to $\hat{\mathcal{L}}_1$, we will finally arrive at the lattice $\mathcal{L}_1$. It allows us to find a generator for $(\mathbf{F}_{q^2}[x]/(f(x)))^*$, and to solve the discrete logarithms for the factor base, with respect to this generator.

4.5.4 Huang-Narayanan's method to determine primitive elements

In the case of $G = \mathbf{F}_{p^k}^{\times}$, where p is a small prime, Huang and Narayanan [35] designed a polynomial-time algorithm to determine the primitive element of G based on a result of F.R.K Chung [17] and Joux's relation generation method [38].

Firstly, Huang and Narayanan embed the field $\mathbf{F}_{p^k}$ to $\mathbf{F}_{q^{2k}}$, where $q = p^m$ and $m = \lceil \log_p(k) \rceil$. The field $\mathbf{F}_{q^{2k}}$ is represented in the same way as in [38]. That is, one searches for appropriate polynomials $h_0(x), h_1(x) \in \mathbf{F}_{q^2}[x]$ of low degree such that the factorization of $h_1(x)x^q - h_0(x)$ over $\mathbf{F}_{q^2}[x]$ has an irreducible factor $I(x)$ of degree k. Let ζ be a root of $I(x)$. The field $\mathbf{F}_{q^{2k}}$ is represented by $\mathbf{F}_{q^2}[\zeta]$. They remark that an isomorphism between two explicit representations of a field of size p^n can be computed deterministically in time polynomial in n and $\log(p)$, which is due to Lenstra [43].

From a result of F.R.K Chung [17], let l be a prime power and t be a positive integer satisfying $(t-1)^2 < l$ and the field $\mathbf{F}_{l^t} = \mathbf{F}_l[\alpha]$. Then the set $\mathbf{F}_l + \alpha$ generates $\mathbf{F}_{l^t}^{\times}$. In the current case, Chung's result implies that $\mathbf{F}_{q^{2k}}^*$

is generated by $S = \mathbf{F}_{q^2} + \zeta$ since $k < q$ by construction. In practice, S is extended to the bigger set $F = S \cup \{h_1(x)\} \cup \{\lambda\}$, where $\mathbf{F}_{q^2} = \langle\lambda\rangle$.

Similarly as in [24], Huang and Narayanan also make use of the fact that

$$\mathbf{F}_{q^{2k}}^{\times} \cong \mathbf{Z}^{|F|}/\Gamma,$$

where Γ is the relation lattice satisfied by elements of F. Thus one can determine the generator of $\mathbf{F}_{q^{2k}}^{\times}$ by computing the SNF of a relation matrix M, which approaches Γ well.

To collect the needed relations, Huang and Narayanan propose to construct the relation matrix M via Joux's relation generation algorithm [38].

4.5.5 Finding the discrete logarithms of linear polynomials by SNF

Following the same notation as in the last section, suppose M is a good approximation of Γ such that the SNF $D = U * M * V$ determines the structure of $\mathbf{F}_{q^{2k}}^{\times}$ correctly. Suppose the relation is represented as columns of M and M is an $m \times n$ matrix. Then U is an $m \times m$ matrix and V is an $n \times n$ matrix. D has the form $[D_1|D_2]$, where

$$D_1 = \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & q^{2k}-1 \end{bmatrix}_{m \times m}$$

and D_2 is a zero matrix.

We observe that we can not only find the primitive element γ from the information of U^{-1}, but also the discrete logarithms of elements in F based on the found primitive element. Suppose the corresponding elements of i-th row of M and D are a_i and b_i, respectively. Since

$$D = U * M * V,$$

$$M = U^{-1} * D * V^{-1},$$

each a_i can be written as a product of b_j and vice versa. Notice that $b_i = 1$ for all $1 \leqslant i \leqslant m-1$, thus we have the expression

$$a_i = \gamma^{e_i},$$

which implies that $\log_\gamma(a_i) = e_i$, where e_i is the i-th element of the last row of U.

4.5.6 Examples

Example 20. *In this example, we want to find the primitive element of* $\mathbf{F}_{16^{2\times 11}}$ *and the discrete logarithms of linear polynomials.*

In the first step, we define $\mathbf{F}^*_{16^2} = \langle\lambda\rangle$ *and search for* $h_0(x), h_1(x) \in \mathbf{F}_{16^2}[x]$ *such that* $h_1(x) * x^{16} - h_0(x)$ *satisfies the conditions in Heuristic 1. Choose*

$$h_0(x) = \lambda * x^2 + \lambda^4 * x + 1, h_1(x) = x + \lambda.$$

We have

$$h_1(x) * x^{16} - h_0(x) = x^{17} + \lambda * x^{16} + \lambda * x^2 + \lambda^4 * x + 1.$$

There are two irreducible factors of $h_1(x) * x^{16} - h_1(x)$ *over* $\mathbf{F}_{16^2}$*:*

$$\begin{aligned} f_1(x) = x^6 &+ (\lambda^6 + \lambda^4 + \lambda^2 + 1) * x^5 + (\lambda^7 + \lambda^6 + \lambda^4 + 1) * x^4 \\ &+ (\lambda^7 + \lambda^5 + \lambda^4 + \lambda^2 + \lambda) * x^3 + \lambda^4 * x^2 \\ &+ (\lambda^7 + \lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1) * x + \lambda^7 + \lambda^4 + \lambda^3 + 1, \end{aligned}$$

$$\begin{aligned} f_2(x) = x^{11} &+ (\lambda^6 + \lambda^4 + \lambda^2 + \lambda + 1) * x^{10} + (\lambda^7 + \lambda^5 + \lambda^4 + \lambda^3 + g) * x^9 \\ &+ (\lambda^7 + \lambda^6 + \lambda^5 + \lambda^4 + \lambda) * x^8 + (\lambda^7 + \lambda^6 + \lambda^5 + \lambda^2 + \lambda + 1) * x^7 \\ &+ (\lambda^7 + \lambda^5 + \lambda^4 + \lambda^2 + 1) * x^6 + (\lambda^5 + \lambda^2 + 1) * x^5 \\ &+ (\lambda^6 + \lambda^5 + \lambda^3) * x^4 + (\lambda^7 + \lambda^6 + \lambda^4 + \lambda^2 + 1) * x^3 \\ &+ (\lambda^7 + \lambda^6 + \lambda^4 + 1) * x^2 + (\lambda^7 + \lambda^6 + \lambda^4) * x \\ &+ \lambda^7 + \lambda^6 + \lambda^4 + \lambda^3 + \lambda^2. \end{aligned}$$

We construct $\mathbf{F}_{16^{2\times 11}}$ *as* $\mathbf{F}_{16^2}[\zeta]$*, where* ζ *is a root of irreducible polynomial* $f_2(x) \in \mathbf{F}_{16^2}[x]$*.*

In the second stage, we choose the factor base $F = \{\lambda\} \cup S$*, where* $S = \mathbf{F}_{16^2} + \zeta$*. And we collect the relations among the elements in the factor base to construct the relation matrix* M*. There are two types of relations to consider.*

- *The first type is according to Joux's relation generation method. We collect all the Möbius twist relations from the systematic equation, that is, we run over all right cosets of* $PGL_2(\mathbf{F}_{16})$ *in* $PGL_2(\mathbf{F}_{16^2})$ *from our classification.*

- *The second type makes use of the following observation:* $\lambda^{255} = 1$ *and for each* $\alpha_i \in \mathbf{F}_{16^2}$*, there exists an* e_i *such that*

$$\lambda^{e_i} = (\zeta + \alpha_i)^{\frac{16^{2\times 11}-1}{16^2-1}}.$$

Finally, we compute the SNF of M*. In other words, we compute*

$$D = U * M * V.$$

We have $D = [D_1|D_2]$*, where* D_2 *is a zero matrix and*

$$D_1 = \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & 30948500982134506872478105 5 \end{bmatrix}_{257\times 257}.$$

Since $309485009821345068724781055 = 16^{22} - 1$*, we claim that we have found the primitive element of* $\mathbf{F}^*_{16^{22}}$*, which can be recovered from the last column of* U^{-1} *as follows*

[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0].

The corresponding element is

$$\gamma = \zeta + \lambda^{166}.$$

Furthermore, the discrete logarithms of elements in the factor base can be retrieved from the last row of U. The result is in Appendix A.

For instance, we can verify that

- $\log_\gamma(\lambda) = 20996433999644194858583185 3, \gamma^{\log(\lambda)} = \lambda$,
- $\log_\gamma(\zeta) = 6071087908206556447631818 1, \gamma^{\log_\gamma(\zeta)} = \zeta$,
- $\log_\gamma(\zeta + \lambda^{55}) = 115063015500116530915979577, \gamma^{\log_\gamma(\zeta+\lambda^{55})} = \zeta + \lambda^{55}$,
- $\log_\gamma(\zeta+\lambda^{197}) = 187986527916727874578311046, \gamma^{\log_\gamma(\zeta+\lambda^{197})} = \zeta+\lambda^{197}$,
- $\log_\gamma(\zeta+\lambda^{255}) = 267444368200903281347884604, \gamma^{\log_\gamma(\zeta+\lambda^{255})} = \zeta+\lambda^{255}$.

Example 21. *In this example, we want to find the primitive element of $\mathbf{F}_{16^{2\times 11}}$ and the discrete logarithms of linear polynomials following another approach.*

In the first step, we define $\mathbf{F}^*_{16^2} = \langle\lambda\rangle$ and search for $h_0(x), h_1(x) \in \mathbf{F}_{16^2}[x]$ such that $h_1(x) * x^{16} - h_0(x)$ satisfies the conditions in Heuristic 1. Choose

$$h_0(x) = \lambda * x^2 + \lambda^4 * x + 1, h_1(x) = x + \lambda.$$

We have

$$h_1(x) * x^{16} - h_0(x) = x^{17} + \lambda * x^{16} + \lambda * x^2 + \lambda^4 * x + 1.$$

There are two irreducible factors of $h_1(x) * x^{16} - h_1(x)$ *over* $\mathbf{F}_{16^2}$*:*

$$\begin{aligned} f_1(x) = x^6 &+ (\lambda^6 + \lambda^4 + \lambda^2 + 1) * x^5 + (\lambda^7 + \lambda^6 + \lambda^4 + 1) * x^4 \\ &+ (\lambda^7 + \lambda^5 + \lambda^4 + \lambda^2 + \lambda) * x^3 + \lambda^4 * x^2 \\ &+ (\lambda^7 + \lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1) * x + \lambda^7 + \lambda^4 + \lambda^3 + 1, \end{aligned}$$

$$\begin{aligned} f_2(x) = x^{11} &+ (\lambda^6 + \lambda^4 + \lambda^2 + \lambda + 1) * x^{10} + (\lambda^7 + \lambda^5 + \lambda^4 + \lambda^3 + g) * x^9 \\ &+ (\lambda^7 + \lambda^6 + \lambda^5 + \lambda^4 + \lambda) * x^8 + (\lambda^7 + \lambda^6 + \lambda^5 + \lambda^2 + \lambda + 1) * x^7 \\ &+ (\lambda^7 + \lambda^5 + \lambda^4 + \lambda^2 + 1) * x^6 + (\lambda^5 + \lambda^2 + 1) * x^5 \\ &+ (\lambda^6 + \lambda^5 + \lambda^3) * x^4 + (\lambda^7 + \lambda^6 + \lambda^4 + \lambda^2 + 1) * x^3 \\ &+ (\lambda^7 + \lambda^6 + \lambda^4 + 1) * x^2 + (\lambda^7 + \lambda^6 + \lambda^4) * x \\ &+ \lambda^7 + \lambda^6 + \lambda^4 + \lambda^3 + \lambda^2. \end{aligned}$$

We construct $\mathbf{F}_{16^{2\times 11}}$ *as* $\mathbf{F}_{16^2}[\zeta]$*, where* ζ *is a root of irreducible polynomial* $f_2(x) \in \mathbf{F}_{16^2}[x]$*.*

In the second stage, we choose the factor base $F = \{\lambda\} \cup S$*, where* $S = \mathbf{F}_{16^2} + \zeta$*. And we collect the relations among the elements in the factor base to construct the relation matrix* M*. There are there types of relations to consider.*

1. *Generate* 150 *relations by Joux's method.*

2. *Generate Frobenius relations. That is, for each* $\alpha \in \mathbf{F}_{16^2}$*, we have*

$$(\zeta + \alpha)^{16} = \zeta^{16} + \alpha^q = \frac{h_0(\zeta)}{h_1(\zeta)} + \alpha^{16},$$

which implies

$$h_1(\zeta) * (\zeta + \alpha)^{16} = h_0(\zeta) + \alpha^{16} * h_1(\zeta).$$

If the polynomial in the right-hand side factorizes into linear polynomial products, then we get a relation. In practice, we get 128 *Frobenius relations.*

3. *The last type of relation makes use of the following observation:* $\lambda^{255} = 1$ *and for each* $\alpha_i \in \mathbf{F}_{16^2}$*, there exists an* e_i *such that*

$$\lambda^{e_i} = (\zeta + \alpha_i)^{\frac{16^{2\times 11}-1}{16^2-1}}.$$

We compute the SNF of M *to get*

$$D = U * M * V.$$

Since the diagonal element of D *are*

$$1, 1, \ldots, 1, 309485009821345068724781055 (= 16^{22} - 1),$$

we claim that we have found the primitive element, which can be recovered from the message of the last column of U^{-1} *as follows:*

[-1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -21441445124877501493350844, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)].

The corresponding element is

$$\gamma = \lambda^{-1} * (\zeta + \lambda^{177})^{-21441445124877501493350844}.$$

Furthermore, the discrete logarithms of elements in the factor base can be read from the last row of U. The result is in Appendix B.

We verify the following instances:

- $\log_\gamma(\lambda) = 245160674446712564244728522, \gamma^{\log(\lambda)} = \lambda,$
- $\log_\gamma(\zeta) = 255670351189335847080296839, \gamma^{\log_\gamma(\zeta)} = \zeta,$
- $\log_\gamma(\zeta + \lambda^{100}) = 68291259138980224088221968, \gamma^{\log_\gamma(\zeta+\lambda^{100})} = \zeta + \lambda^{100},$
- $\log_\gamma(\zeta + \lambda^{177}) = 3, \gamma^{\log_\gamma(\zeta+\lambda^{177})} = \zeta + \lambda^{177},$
- $\log_\gamma(\zeta + \lambda^{186}) = 49529503067517771000507583, \gamma^{\log_\gamma(\zeta+\lambda^{186})} = \zeta + \lambda^{186}.$

Example 22. *In this example, we want to find the primitive element and discrete logarithms of linear polynomials in $\mathbf{F}_{16^{2\times 12}}$.*

In the first step, we define $\mathbf{F}_{16^2}^* = \langle\lambda\rangle$ *and search for* $h_0(x), h_1(x) \in \mathbf{F}_{16^2}[x]$ *such that* $h_1(x) * x^{16} - h_0(x)$ *satisfies the conditions in Heuristic 1. Choose*

$$h_0(x) = \lambda * x^2 + (\lambda^6 + \lambda^5 + \lambda^4 + \lambda^2) * x + 1, h_1(x) = x + \lambda.$$

We have

$$h_1(x) * x^{16} - h_0(x) = x^{17} + \lambda * x^{16} + \lambda * x^2 + (\lambda^6 + \lambda^5 + \lambda^4 + \lambda^2) * x + 1.$$

There are two irreducible factors of $h_1(x) * x^{16} - h_1(x)$ *over* $\mathbf{F}_{16^2}$*:*

$$\begin{aligned} f_1(x) = {} & x^5 + (\lambda^7 + \lambda^5 + \lambda^4 + \lambda) * x^4 + (\lambda^7 + \lambda^5 + \lambda^3 + 1) * x^3 \\ & + (\lambda^7 + \lambda^5 + \lambda^4 + \lambda^3) * x + \lambda^7 + \lambda^6 + \lambda^5 + \lambda^4 + \lambda^3 + \lambda, \end{aligned}$$

$$\begin{aligned} f_2(x) = {} & x^{12} + (\lambda^7 + \lambda^5 + \lambda^4) * x^{11} + (\lambda^7 + \lambda^5 + \lambda^3 + \lambda^2 + \lambda) * x^{10} \\ & + (\lambda^6 + \lambda^5 + \lambda^4 + \lambda^2 + \lambda) * x^9 + (\lambda^7 + \lambda^6 + \lambda^4 + \lambda^3 + \lambda) * x^8 \\ & + (\lambda^7 + \lambda^5 + \lambda^4 + \lambda^2) * x^7 + (\lambda^7 + \lambda^6 + \lambda^4 + 1) * x^6 \\ & + (\lambda^7 + \lambda^4 + \lambda + 1) * x^5 + (\lambda^6 + \lambda^4 + \lambda^2) * x^4 \\ & + (\lambda^7 + \lambda^2) * x^3 + (\lambda^7 + \lambda^5 + \lambda^4 + \lambda^3 + \lambda^2 + \lambda) * x^2 \\ & + (\lambda^6 + \lambda^3 + \lambda^2) * x + \lambda^7 + \lambda^6 + \lambda^5 + \lambda^3. \end{aligned}$$

We construct $\mathbf{F}_{16^{2\times 12}}$ *as* $\mathbf{F}_{16^2}[\zeta]$*, where* ζ *is a root of irreducible polynomial* $f_2(x) \in \mathbf{F}_{16^2}[x]$*.*

In the second stage, we choose the factor base $F = \{\lambda\} \cup S$*, where* $S = \mathbf{F}_{16^2} + \zeta$*. And we collect the relations among the elements in the factor base to construct the relation matrix* M*. There are two types of relations to consider.*

- *The first type is according to Joux's relation generation method. We*

collect all the Möbius twist relations from the systematic equation, that is, we run over all cosets of $PGL_2(\mathbf{F}_{16})$ in $PGL_2(\mathbf{F}_{16^2})$ from our classification.

- *The second type makes use of the following observation: $\lambda^{255} = 1$ and for each $\alpha_i \in \mathbf{F}_{16^2}$, there exists an e_i such that*

$$\lambda^{e_i} = (\zeta + \alpha_i)^{\frac{16^{24}-1}{16^2-1}}.$$

Next, we compute the SNF of M. Equivalently, we compute

$$D = U * M * V.$$

Since the diagonal element of D are

$$1, 1, \ldots, 1, 3, 3, 3, 3, 792281625142643375935439503 35(= 16^{24} - 1),$$

the relations are not sufficient to determine the actual structure of $\mathbf{F}^*_{16^{24}}$. However, it is not far away from it since we have only four small none-one components. Observe that $3|16^2 - 1$, thus these four elements actually lie in $\mathbf{F}_{16^2}$. Thus we can add these relations as follows.

1. *The element β_{252} corresponding to the 252-th diagonal element can be found from the 252-th column of U^{-1}, which is*

   [-15, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -42, 0, 0, 0, 0, 0, 0, 0,
   0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
   0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

-4760533332987710118711190636, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -5, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0].

Thus,

$$\beta_{252} = \lambda^{-15} * (z + \lambda^{16})^{-42} * (z + \lambda^{100})^{e} * (z + \lambda^{168}) * (z + \lambda^{189})^{-5},$$

where $e = -4760533332987710118711190636$*. Since* $\beta_{252} = \lambda^{255}$*, we add the following column vector to the relation matrix:*

[-15-255, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -42, 0, 0, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

-4760533332987710118711190636, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -5, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0].

2. *The element* β_{253} *corresponding to the 253-th diagonal element can be found from the 253-th column of* U^{-1}, *which is*

[-3, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -9, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
-23930764333874738583871355, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, -1, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0].

Thus,

$$\beta_{253} = \lambda^{-3} * (z + \lambda^{16})^{-9} * (z + \lambda^{100})^{e} * (z + \lambda^{188}) * (z + \lambda^{189})^{-1},$$

where $e = -23930764333874738583871355$. *Since* $\beta_{253} = \lambda^{170}$, *we add the following column vector to the relation matrix:*

[-3-170, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -9, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
-23930764333874738583871355, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, -1, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0].

3. *The element β_{254} corresponding to the 254-th diagonal element can be found from the 254-th column of U^{-1}, which is*

[-30, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -71, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
-9515460161743407776180350742, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -10, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0].

Thus,

$$\beta_{254} = \lambda^{-30} * (z+\lambda^{16})^{-71} * (z+g^{100})^{-9515460161743407776180350742} * (z+\lambda^{189})^{-10}.$$

Since $\beta_{254} = \lambda^{170}$, we add the following column vector to the relation matrix:

[-30-170, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -71, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
-95154601617434077618035074 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -10, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0].

4. *The element β_{255} corresponding to the 255-th diagonal element can be found from the 255-th column of U^{-1}, which is*

[585, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1365, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
186245504196192185205891589 24, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 195, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0].

Thus,

$$\beta_{255} = \lambda^{585} * (z+\lambda^{16})^{1365} * (z+\lambda^{100})^{18624550419619218520589158924} * (z+\lambda^{189})^{195}.$$

Since $\beta_{255} = \lambda^{170}$, *we add the following column vector to the relation matrix:*

[585-170, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1365, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 18624550419619218520589158924, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 195,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0].

Now, we compute the SNF of the new relation matrix M', *which consists of* M *and the four augmented relations, to get*

$$D' = U' * M' * V'.$$

Since the diagonal elements of D' *are*

$$1, 1, \ldots, 1, 79228162514264337593543950335 = 16^{24} - 1,$$

we claim that we have found the primitive element, which can be recovered from the message of the last column of U'^{-1} *as follows:*

[22, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 88, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
152674035219163120011070411, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0].

The corresponding element is

$$\gamma = \lambda^{22} * (z + \lambda^{16})^{88} * (z + \lambda^{100})^{152674035219163120011070411}.$$

Furthermore, the discrete logarithms of elements in the factor base can be read from the last row of U'*. The result is in Appendix C.*

For instance, we can verify that

- $\log_\gamma(\lambda) = 789174638377378107794516211118, \gamma^{\log(\lambda)} = \lambda$,
- $\log_\gamma(\zeta) = 628330903496446298221485457739, \gamma^{\log_\gamma(\zeta)} = \zeta$,
- $\log_\gamma(\zeta + \lambda^{73}) = 659951781013581735327974109 5, \gamma^{\log_\gamma(\zeta+\lambda^{73})} = \zeta + \lambda^{73}$,
- $\log_\gamma(\zeta + \lambda^{172}) = 238938262865528406620737793336, \gamma^{\log_\gamma(\zeta+\lambda^{172})} = \zeta + \lambda^{172}$,

- $\log_\gamma(\zeta + \lambda^{251}) = 769443310670972772035804211 82, \gamma^{\log_\gamma(\zeta+\lambda^{251})} = \zeta + \lambda^{251}$.

4.6 Traps to the original BGJT-algorithm and a solution

4.6.1 The trap to the QPA-descent

Now we review the QPA-descent. Suppose that we need to compute the discrete logarithm of $W(\zeta) \in \mathbf{F}_{q^{2k}}[\zeta]$, where W is a polynomial over $\mathbf{F}_{q^2}$ of degree $w > 1$. The QPA-descent, firstly proposed in [6], is to represent $W(\zeta)$ as a product of elements of smaller degree, e.g., $\leqslant w/2$, in the field $\mathbf{F}_{q^2}[x]/(f(x))$. To do this, one again starts with the identity:

$$\prod_{\alpha \in \mathbf{F}_q} (x - \alpha) = x^q - x.$$

Then apply the transformation

$$x \mapsto \frac{aW(x) + b}{cW(x) + d}$$

where the matrix $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{F}_{q^2}^{2\times 2}$ is nonsingular. We have

$$\prod_{\alpha \in \mathbf{F}_q} (\frac{aW(x) + b}{cW(x) + d} - \alpha) = (\frac{aW(x) + b}{cW(x) + d})^q - \frac{aW(x) + b}{cW(x) + d}.$$

Clearing the denominator:

$$\begin{aligned}
& (cW(x)+d)\prod_{\alpha\in\mathbf{F}_q}((aW(x)+b)-\alpha(cW(x)+d)) \\
= \;& (aW(x)+b)^q(cW(x)+d)-(aW(x)+b)(cW(x)+d)^q \\
= \;& (a^q\tilde{W}(x^q)+b^q)(cW(x)+d)-(aW(x)+b)(c^q\tilde{W}(x^q)+d^q),
\end{aligned}$$

where $\tilde{W}(x)$ is a polynomial obtained by raising the coefficients of $W(x)$ to the q-th power. Replacing x^q with $h_0(x)/h_1(x)$, we obtain

$$\begin{aligned}
& (cW(x)+d)\prod_{\alpha\in\mathbf{F}_q}((aW(x)+b)-\alpha(cW(x)+d)) \\
= \;& (a^q\tilde{W}(h_0(x)/h_1(x))+b^q)(cW(x)+d) \\
& -(aW(x)+b)(\tilde{W}(h_0(x)/h_1(x))+d^q h_1(x)) \\
& \pmod{x^q h_1(x)-h_0(x)}.
\end{aligned}$$

It was shown in [6] that matrices in the same right coset of $PGL_2(\mathbf{F}_q)$ of $PGL_2(\mathbf{F}_{q^2})$ generate the same equations. The denominator of the right-hand side is a power of $h_1(x)$. Denote the numerator of the right-hand side polynomial by $N_{m,W}(x)$. If the polynomial $N_{m,W}(x)$ is $w/2$-smooth, namely, it can be factored completely into a product of irreducible factors over $\mathbf{F}_{q^2}$, all have degree $w/2$ or less, we obtain a relation of the form

$$\prod_{i=1}^{q^2}(W(x)+\alpha_i)^{e_i}=\lambda^{e_0}\prod_{g(x)\in S}g(x)^{e'_g} \pmod{x^q h_1(x)-h_0(x)}, \tag{4.6}$$

where $S\subseteq\mathbf{F}_{q^2}[x]$ is a set of monic polynomials of degrees less than $w/2$ and with cardinality at most $3w$. Denote the vector $(e_1,e_2,\ldots,e_{q^2})$ by $\mathbf{v}_m$. Note

that it is a binary vector, and it is independent of $W(x)$. Collecting enough number of relations will allow us to represent $W(x)$ as a product of elements of smaller degrees. This process is the QPA-descent. A heuristic made in [6] is that repeating this process, one can represent any element in $\mathbf{F}_{q^2}[x]/(f(x))$ as a product of linear factors. Combining it with the fact that the discrete logarithm of the linear factors are known, one solves the discrete logarithm for any element.

However, the descent will not work if $W(x)$ is a factor of $x^q h_1(x) - h_0(x)$. Recall that $\alpha_1 = 0$.

Theorem 12. *If $W(x) | x^q h_1(x) - h_0(x)$, e_1 will always be 0 in (4.6).*

In other words, if $W(x)$ is a factor of $x^q h_1(x) - h_0(x)$, then it will never appear in the left-hand side of (4.6) as a factor. So the descent for $W(\zeta)$ is not possible.

Proof: The polynomial $W(x)$ is a zero divisor in the ring $\mathbf{F}_{q^2}[x]/(x^q h_1(x) - h_0(x))$. Hence if $W(x)$ appears in the left-hand side of (4.6) as a factor, it will also appear in the right-hand side. This contradicts to the requirement that the factors in the right-hand side have degrees smaller than the degree of $W(x)$. □

Note that the trap factor $W(\zeta)$ can appear in the descent paths of other elements, which essentially blocks the descents. It is especially troublesome if $x^q h_1(x) - h_0(x)$ has many small degree factors.

4.6.2 The trap-avoiding descent

Now we have discovered traps for the original QPA-descent. How can we work around them? From the above discussion, we assume that we work in a non-Kummer extension, and the polynomial $x^q h_1(x) - h_0(x)$ with the factorization as in (4.2) satisfies

- $\deg(h_0) \leqslant 2, \deg(h_1) \leqslant 1$,
- $k_i > 1$ for all $1 \leqslant i \leqslant l$; in other words, it is free of linear factors,
- $\gcd(k, k_i) = 1$ for all $1 \leqslant i \leqslant l$.

In the most interesting case where k is a prime, our numerical data show that the above requirements can be easily satisfied. For example, when $q = 1024$, the result is in Appendix D.

Heuristic 2. *Let q be a prime power and $k < q$ be a prime. Then there exist polynomials h_0 and h_1 satisfying the above requirements.*

Assume that the discrete logarithms of all linear polynomials have been computed. Suppose that we need to compute the discrete logarithm of $W(\zeta)$, where $W(x)$ is an irreducible polynomial of degree less than k, and it is relatively prime to $f(x)$. If $W(x)|x^q h_1(x) - h_0(x)$, we will search for an integer i such that $W(x)^i \pmod{f(x)}$ is relatively prime to $x^q h_1(x) - h_0(x)$. Such an i can be found easily by a random process.

Now we can assume that $\gcd(W(x), x^q h_1(x) - h_0(x)) = 1$. If there are not many traps, we will use a trap-avoiding strategy for the descent. The basic idea is simple. Whenever we find a relation (4.6), we will not use it unless the right-hand side is relatively prime to $x^q h_1(x) - h_0(x)$.

Definition 24. *Define the trap-avoiding descent lattice $\mathcal{L}(W)$ associated with $W(x)$ to be generated by*

$$\{\mathbf{v}_m | N_{m,W} \text{ is } w/2 - \text{smooth, and } \gcd(N_{m,W}, x^q h_1(x) - h_0(x)) = 1\}.$$

Note that we use less relations than [6] does, since we have to avoid traps. If the vector $(1, 0, \ldots, 0)$ is in the trap-avoiding descent lattice of $W(x)$, then $W(x)$ can be written as a product of low-degree polynomials in $\mathbf{F}_{q^2}[x]/(f(x))$ that are not traps. We believe that the following heuristic is very likely to be true.

Heuristic 3. *The trap-avoiding descent lattice for $W(x)$ contains the vector $(1, 0, \ldots, 0)$ if $\gcd(W(x), x^q h_1(x) - h_0(x)) = 1$.*

Remark 20. *The authors of [7] and [36] proposed their solutions for the traps.*

To provide a theoretical evidence, we will show that $(1, 0, \ldots, 0)$ is in its super lattice that is generated by $\mathbf{v}_m$ for all $m \in \mathcal{P}_q$, regardless whether $N_{m,W}(x)$ is $w/2$-smooth or not. This is a slight improvement over [6], where it is proved that $(q^3 - q, 0, \ldots, 0)$ is in the super lattice. To proceed, we first make some definitions following [6]. There are two matrices in consideration. The matrix $\mathcal{H}$ is composed by the binary row vectors $\mathbf{v}_m$ for all

$$m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{P}_q.$$

It is a matrix with q^3+q rows and q^2 columns. If we view m^{-1} as a map from $\mathbf{P}^1(\mathbf{F}_q)$ to $\mathbf{P}^1(\mathbf{F}_{q^2})$ given by

$$(\beta_1 : \beta_2) \to (-d\beta_1 + b\beta_2 : c\beta_1 - a\beta_2),$$

then the i-th component of v_m is 1 if there is a point $P \in \mathbf{P}^1(\mathbf{F}_q)$ such that $m^{-1}(P) = (\alpha_i : 1)$. We define a binary vector $\mathbf{v}_m^+ = (e_1, \ldots, e_{q^2}, e_{q^2+1})$ for $m \in \mathcal{P}_q$, where $(e_1, \ldots, e_{q^2}) = \mathbf{v}_m$, and

$$e_{q^2+1} = \begin{cases} 1 & \text{if } (a:c) \in \mathbf{P}^1(\mathbf{F}_q) \\ 0 & \text{otherwise.} \end{cases}$$

One can verify that the last component of $\mathbf{v}_m^+$ corresponds to whether there is a point $P \in \mathbf{P}^1(\mathbf{F}_q)$ such that $m^{-1}(P) = (1:0) = \infty$. The matrix $\mathcal{H}^+$ is composed of the vectors $\mathbf{v}_m^+, m \in \mathcal{P}_q$. $\mathcal{H}^+$ is a matrix with q^3+q rows and q^2+1 columns. All the row vectors have exactly $q+1$ coordinates which are 1's.

Denote the lattices generated by the row vectors of $\mathcal{H}$ and $\mathcal{H}^+$ by $\mathcal{L}(\mathcal{H})$ and $\mathcal{L}(\mathcal{H}^+)$, respectively. In [6], the authors showed that $\mathbf{v}_1 = (q^2+q, \ldots, q^2+q) \in \mathcal{L}(\mathcal{H}^+)$ and $\mathbf{v}_2 = (q^2+q, q+1, \ldots, q+1) \in \mathcal{L}(\mathcal{H}^+)$.

Theorem 13. *The vector* $(1, 0, \ldots, 0)$ *is in the lattice* $\mathcal{L}(\mathcal{H})$.

Proof: Fix a γ such that $\mathbf{F}_{q^2} = \mathbf{F}_q[\gamma]$. Firstly, observe that $\mathbf{v}_3 = (1, \ldots, 1, q) \in \mathcal{L}(\mathcal{H}^+)$. This follows from $\mathbf{v}_3 = \sum_{\beta \in \mathbf{F}_q} \mathbf{v}_{m_\beta} \in \mathcal{L}(\mathcal{H}^+)$, where

$$m_\beta = \begin{pmatrix} 1 & \beta\gamma \\ 0 & 1 \end{pmatrix} \in \mathcal{P}_q.$$

There are $q+1$ row vectors in $\mathcal{H}^+$ such that both the first and the last coordinates are 1. Since the projective linear map on a projective line is sharply 3-transitive, a third coordinate with value 1 will uniquely determine the coset in $\mathcal{P}_q$. Thus the sum of these $q+1$ vectors is $\mathbf{v}_4 = (q+1, 1, \ldots, 1, q+1) \in \mathcal{L}(\mathcal{H}^+)$.

From the above observations, we have

$$\mathbf{v}_5 = \mathbf{v}_2 - (q+1)\mathbf{v}_3 = (q^2-1, 0, \ldots, 0, 1-q^2) \in \mathcal{L}(\mathcal{H}^+),$$

$$\mathbf{v}_6 = \mathbf{v}_4 - \mathbf{v}_3 = (q, 0, \ldots, 0, 1) \in \mathcal{L}(\mathcal{H}^+).$$

We deduce

$$\mathbf{v}_7 = q\mathbf{v}_6 - \mathbf{v}_5 = (1, 0, \ldots, 0, q^2+q-1) \in \mathcal{L}(\mathcal{H}^+),$$

which implies $(1, 0, \ldots, 0) \in \mathcal{L}(\mathcal{H})$. □

Chapter 5

Conclusions and future work

Error-correcting codes and cryptography play important roles in information communication. Generalized Reed-Solomon codes and cryptography systems based on discrete logarithms are representatives of these areas, respectively. In this dissertation, we have studied the deep hole problem of generalized Reed-Solomon codes and the discrete logarithm problem over finite fields.

In the first part, we classify deep holes for Generalized Reed-Solomon codes $RS_q(D, k)$. Specifically, we give a characterization of deep holes when q is an odd prime, $|D| > k \geqslant \frac{p-1}{2}$. Generalizing the result to finite fields of composite order is a possible future work.

In the second part, we study the validation of the heuristics made in the quasi-polynomial time algorithm solving the discrete logarithms in the small characteristic fields [6]. We find that the heuristics are problematic in the cases of non-Kummer extensions. We propose a few modifications to the algorithm, including some extra requirements for the polynomials h_0 and h_1, and a trap-avoiding descent strategy. The modified algorithm relies on three improved heuristics.

Proposition 12. *If Heuristics 1, 2 and 3 hold, then the discrete logarithm problem over* $\mathbf{F}_{q^k}$ *(*$k < q$*) can be solved in time* $q^{O(\log(k))}$.

We believe that proving (or disproving) these heuristics offers interesting open problems that will help to understand the effectiveness of the new algorithm. Besides, it is interesting to explore the applications of the idea used to attack the discrete logarithms over finite fields to other problems.

Bibliography

[1] L. Adleman. A subexponential algorithm for the discrete logarithm problem with applications to cryptography. In *FOCS*, pages 55–60. IEEE Computer Society, 1979.

[2] L. Adleman. The function field sieve. In Leonard M. Adleman and Ming-Deh A. Huang, editors, *ANTS*, volume 877 of *Lecture Notes in Computer Science*, pages 108–121. Springer, 1994.

[3] L. Adleman and J. DeMarrais. A subexponential algorithm for discrete logarithms over all finite fields. In Douglas R. Stinson, editor, *CRYPTO*, volume 773 of *Lecture Notes in Computer Science*, pages 147–158. Springer, 1993.

[4] L. Adleman and M. Huang. Function field sieve method for discrete logarithms over finite fields. *Information and Computation*, 151:5–16, 1999.

[5] A. Alon, M. Nathanson, and I. Ruzsa. The polynomial method and restricted sums of congruence classes. *Journal of Number Theory*, 56(2):404–417, 1996.

[6] R. Barbulescu, R. Gaudry, A. Joux, and E. Thomé. A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. *CoRR*, abs/1306.4244v1, 2013.

[7] R. Barbulescu, R. Gaudry, A. Joux, and E. Thomé. A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. *CoRR*, abs/1306.4244v2, 2013.

[8] I. F. Blake, R. C. Mullin, and S. A. Vanstone. Computing logarithms in $GF(2^n)$. In G. R. Blakley and David Chaum, editors, *CRYPTO*, volume 196 of *Lecture Notes in Computer Science*, pages 73–82. Springer, 1984.

[9] W. Brakemeier. Eine anzahlformel von zahlen modulo n. *Monatshefte für Mathematik*, 85:277–282, 1978.

[10] J. P. Buhler, H. W. Lenstra Jr., and Carl Pomerance. Factoring integers with the number field sieve. volume 1554 of *Lecture Notes in Computer Science*, pages 50–94. Springer, 1993.

[11] A. Cafure, G. Matera, and M. Privitelli. Singularities of symmetric hypersurfaces and an application to Reed-Solomon codes. *Advances in Mathematics of Communications*, 6(1):69–94, 2012.

[12] M. Car. Théorèmes de densité dans $F_q[x]$. *Acta Arith.*, 48:145–165, 1987.

[13] Q. Cheng, J. Li, and J. Zhuang. On determining deep holes of generalized Reed-Solomon codes. In *ISAAC*, volume 8283 of *Lecture Notes in Computer Science*, pages 100–110. Springer, 2013.

[14] Q. Cheng and E. Murray. On deciding deep holes of Reed-Solomon codes. In *TAMC*, pages 296–305, 2007.

[15] Q. Cheng and D. Wan. On the list and bounded distance decodability of Reed-Solomon codes. *SIAM Journal on Computing*, 37(1):195–209.

[16] Q. Cheng, D. Wan, and J. Zhuang. Traps to the BGJT-algorithm for discrete logarithms. Cryptology ePrint Archive, Report 2013/673, 2013.

[17] F. R. K. Chung. Diameters and eigenvalues. *Journal of the American Mathematical Society*, 2(2):187–196, 1989.

[18] Henri Cohen, editor. *Algorithmic Number Theory, Second International Symposium, ANTS-II, Talence, France, May 18-23, 1996, Proceedings*, volume 1122 of *Lecture Notes in Computer Science*. Springer, 1996.

[19] D. Coppersmith. Fast evaluation of logarithms in fields of characteristic two. *IEEE Transactions on Information Theory*, 30(4):587–594, 1984.

[20] W. Diffie and M. Hellman. New directions in cryptogrphy. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[21] D. Dummit and R. Foote. *Abstract Algebra*. 3rd edition.

[22] Cynthia Dwork, editor. *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*, volume 4117 of *Lecture Notes in Computer Science*. Springer, 2006.

[23] T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[24] A. Enge. A general framework for subexponential discrete logarithm algorithms in groups of unknown order. In A. Blokhuis, J. W. P. Hirschfeld, D. Jungnickel, and J. A. Thas, editors, *Finite Geometries*, volume 3 of *Developments in mathematics*, pages 133–146. Kluwer Academic Publishers, 2001.

[25] L. Gallardo, G. Grekos, and J. Pihko. On a variant of the Erdös-Ginzburg-Ziv theorem. *Acta Arithmetica*, 89:331–336, 1999.

[26] O. Goldreich. *The Foundations of Cryptography - Volume 1, Basic Techniques*. Cambridge University Press, 2001.

[27] F. Göloglu, R. Granger, G. McGuire, and J. Zumbrägel. On the function field sieve and the impact of higher splitting probabilities. In Ran Canetti and Juan A. Garay, editors, *CRYPTO*, volume 8043 of *Lecture Notes in Computer Science*, pages 109–128. Springer, 2013.

[28] D. M. Gordon. Discrete logarithms in GF(p) using the number field sieve. *SIAM Journal on Discrete Mathematics*, 6(1):124–138, 1993.

[29] R. Granger, A. Holt, D. Page, N. Smart, and F. Vercauteren. Function field sieve in characteristic three. In Duncan A. Buell, editor, *ANTS*, volume 3076 of *Lecture Notes in Computer Science*, pages 223–234. Springer, 2004.

[30] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Transaction on Information Theory*, 45(6):1757–1767, 1999.

[31] V. Guruswami and A. Vardy. Maximum-likelihood decoding of Reed-Solomon codes is NP-hard. In *Proceeding of SODA*, 2005.

[32] R. Hamming. Error detecting and error correcting codes. *The Bell System Technical Journal*, 29(2):147–160, 1950.

[33] M. E. Hellman and J. M. Reyneri. Fast computation of discrete logarithms in GF(q). In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *CRYPTO*, pages 3–13. Plenum Press, New York, 1982.

[34] L. Hua. *Introduction to Number Theory*. Springer-Verlag, 1982.

[35] M. Huang and A. Narayanan. Finding primitive elements in finite fields of small characteristic. *CoRR*, abs/1304.1206, 2013.

[36] M. Huang and A. Narayanan. On the relation generation method of joux for computing discrete logarithms. *CoRR*, abs/1312.1674, 2013.

[37] A. Joux. Faster index calculus for the medium prime case application to 1175-bit and 1425-bit finite fields. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT*, volume 7881 of *Lecture Notes in Computer Science*, pages 177–193. Springer, 2013.

[38] A. Joux. A new index calculus algorithm with complexity $L(1/4 + o(1))$ in very small characteristic. Cryptology ePrint Archive, Report 2013/095, 2013.

[39] A. Joux and R. Lercier. The function field sieve is quite special. In Claus Fieker and David R. Kohel, editors, *ANTS*, volume 2369 of *Lecture Notes in Computer Science*, pages 431–445. Springer, 2002.

[40] A. Joux and R. Lercier. Improvements to the general number field sieve for discrete logarithms in prime fields. a comparison with the gaussian integer method. *Mathematics of Computation*, 72(242):953–967, 2003.

[41] A. Joux and R. Lercier. The function field sieve in the medium prime case. In Serge Vaudenay, editor, *EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 254–270. Springer, 2006.

[42] A. Joux, R. Lercier, N. Smart, and F. Vercauteren. The number field sieve in the medium prime case. In Dwork [22], pages 326–344.

[43] H. W. Lenstra Jr. Finding isomorphisms between finite fields. *Mathematics of Computation*, 56(193):329–347, 1991.

[44] A. K. Lenstra, H. W. Lenstra Jr., M. S. Manasse, and J. M. Pollard. The number field sieve. In Harriet Ortiz, editor, *STOC*, pages 564–572. ACM, 1990.

[45] J. Li and D. Wan. On the subset sum problem over finite fields. *Finite Fields and Their Applications*, 14:911–929, 2008.

[46] J. Li and D. Wan. A new sieve for distinct coordinate counting. *Science China Mathematics*, 53(9):2351–2362, 2010.

[47] Y. Li and D. Wan. On error distance of Reed-Solomon codes. *Science in China Series A: Mathematics*, 51:1982–1988, 2008.

[48] Q. Liao. On Reed-Solomon codes. *Chinese Annals of Mathematics, Series B*, 32B:89–98, 2011.

[49] R. Lovorn. *Rigourous, subexponential algorithms for discrete logarithm algorithms in* $\mathbf{F}(p^2)$. PhD thesis.

[50] F. Macwilliams and N. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, Netherlands, 1977.

[51] K. S. McCurley. The discrete logarithm problem. In *Cryptography and Computational Number Theory*, pages 49–74, 1990.

[52] R. Merkle. *Secrecy, authentication, and public key systems*. PhD thesis, Stanford University, 1979.

[53] D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems: A Cryptographic Perspective*. Kluwer Academic Publishers, 2002.

[54] M. A. Morrison and J. Brillhart. A method of factoring and the factorization of F_7. *Mathematics of computation*, 29(129):183–205.

[55] A. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, editors, *EUROCRYPT*, volume 209 of *Lecture Notes in Computer Science*, pages 224–314. Springer, 1984.

[56] A. Oklyzko. Discrete logarithms: The past and the future. *Designs, Codes and Cryptography*, 19:129–145, 2000.

[57] D. Panario, X. Gourdon, and P. Flajolet. An analytic approach to smooth polynominals over finite fields. In Joe Buhler, editor, *ANTS*, volume 1423 of *Lecture Notes in Computer Science*, pages 226–236. Springer, 1998.

[58] J. Pollard. Monte carlo methods for index computations (mod p). *Mathematics of Computation*, 32(143):918–924, 1978.

[59] I. S. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.

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

[61] O. Schirokauer. Discrete logarithms and local units. *Philosophical Transactions: Physical Sciences and Engineering*, 345(1676):409–423, 1993.

[62] O. Schirokauer. Virtual logarithms. *Journal of Algorithms*, 57(2):140–147, 2005.

[63] O. Schirokauer, D. Weber, and T. Denny. Discrete logarithms: The effectiveness of the index calculus method. In Cohen [18], pages 337–361.

[64] I. A. Semaev. An algorithm for evaluation of discrete logarithms in some nonprime finite fields. *Mathematics of Computation*, 67(224):1679–1689, 1998.

[65] D. Shanks. Class number, a theory of factorization and genera. In *Proc. Symp. Pure Math. 20, 1969*, pages 415–440. AMS, Providence, R.I., 1971.

[66] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423 and 623–656, 1948.

[67] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[68] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[69] J. A. Dias Da Silva and Y. O. Hamidoune. Cyclic spaces for grassmann derivatives and additive theory. *Bulletin of the London Mathematical Society*, 26:140–146, 1994.

[70] M. Sudan. Decoding of Reed-Solomon codes beyond the error-correction bound. *Journal of Complexity*, 13:180–193, 1997.

[71] D. Wan. Generators and irreducible polynomials over finite fields. *Math. Comp.*, 66(219):1195–1212, 1997.

[72] D. Weber. An implementation of the general number field sieve to compute discrete logarithms mod p. In Louis C. Guillou and Jean-Jacques Quisquater, editors, *EUROCRYPT*, volume 921 of *Lecture Notes in Computer Science*, pages 95–105. Springer, 1995.

[73] D. Weber. Computing discrete logarithms with the general number field sieve. In Cohen [18], pages 391–403.

[74] A. E. Western and J. C. P. Miller. *Tables of Indices and Primitive Roots.* Cambridage University Press, 1968.

[75] R. Wu and S. Hong. On deep holes of generalized Reed-Solomon codes. 2012. arXiv:1205.7016.

[76] R. Wu and S. Hong. On deep holes of standard Reed-Solomon codes. *Science China Mathematics*, 55(12):2447–2455, 2012.

[77] G. Zhu and D. Wan. Computing error distance of Reed-Solomon codes. In *TAMC2012*, LNCS 7287, pages 214–224.

Appendix A

Discrete logarithms of elements in the factor base of $\mathbf{F}_{16^{22}}$

We define $\mathbf{F}^*_{16^2} = \langle\lambda\rangle$ and choose

$$h_0(x) = \lambda * x^2 + \lambda^4 * x + 1, h_1(x) = x + \lambda.$$

We have

$$h_1(x) * x^{16} - h_0(x) = x^{17} + \lambda * x^{16} + \lambda * x^2 + \lambda^4 * x + 1.$$

The primitive element of $\mathbf{F}^*_{16^{22}}$ is

$$\gamma = \zeta + \lambda^{166}.$$

The discrete logarithms of elements in the factor base can be retrieved from the last row of U.

α	$\log_\gamma(\alpha)$	α	$\log_\gamma(\alpha)$
λ	209964339996441948585831853	ζ	60710879082065564476318181
$\zeta+\lambda$	17976977313082885784218745	$\zeta+\lambda^2$	86011917882104584081826403
$\zeta+\lambda^3$	23601911278984985084942468 1	$\zeta+\lambda^4$	46933633336121228215957387
$\zeta+\lambda^5$	22117346539692306847334309 6	$\zeta+\lambda^6$	30872972099728839280648682 3
$\zeta+\lambda^7$	23876702086765680016334688 5	$\zeta+\lambda^8$	24922969256464713574666983 3
$\zeta+\lambda^9$	25572824825795882551669139 1	$\zeta+\lambda^{10}$	23886122028448505131295396 6
$\zeta+\lambda^{11}$	14101442532048636599709443 7	$\zeta+\lambda^{12}$	57351169457668833342818523
$\zeta+\lambda^{13}$	27263529857102704468516308 6	$\zeta+\lambda^{14}$	10071932231034085660814842 7
$\zeta+\lambda^{15}$	65842862513074489251190232	$\zeta+\lambda^{16}$	18971014656903429157106619 1
$\zeta+\lambda^{17}$	25987771529563571686964850 8	$\zeta+\lambda^{18}$	15284822392927108020433003 1
$\zeta+\lambda^{19}$	11083626367725082724877596 2	$\zeta+\lambda^{20}$	23104652983491943387117099 5
$\zeta+\lambda^{21}$	65568872696411869821050900	$\zeta+\lambda^{22}$	60307334715434746813891976
$\zeta+\lambda^{23}$	20021553615993227944425567 9	$\zeta+\lambda^{24}$	44503929244825116272604823
$\zeta+\lambda^{25}$	15141428857298721321004488 4	$\zeta+\lambda^{26}$	19151320890942937666165690 5
$\zeta+\lambda^{27}$	31678494587456828868072198	$\zeta+\lambda^{28}$	26283367828956737690753580 6
$\zeta+\lambda^{29}$	26136256137298922774083021 0	$\zeta+\lambda^{30}$	64544113481768992685091099
$\zeta+\lambda^{31}$	11081530902633488527199248 7	$\zeta+\lambda^{32}$	38272929298248650299635142
$\zeta+\lambda^{33}$	20959309994019805315335691 0	$\zeta+\lambda^{34}$	25409837623122724672735810 8
$\zeta+\lambda^{35}$	28652338119968084291646493 8	$\zeta+\lambda^{36}$	22570306120045532274804255 5
$\zeta+\lambda^{37}$	27753783588802968843034059 4	$\zeta+\lambda^{38}$	14475537437053308158513610 9
$\zeta+\lambda^{39}$	28280619967842009155137655 3	$\zeta+\lambda^{40}$	24259257388286578690429468 8
$\zeta+\lambda^{41}$	16447737556624980702755890 1	$\zeta+\lambda^{42}$	16790940196799634667542997
$\zeta+\lambda^{43}$	20178847635726887822587956 1	$\zeta+\lambda^{44}$	30789569200819010309977199
$\zeta+\lambda^{45}$	69602113679960600249155254	$\zeta+\lambda^{46}$	56896044191628709633519462
$\zeta+\lambda^{47}$	14678949729188153662054510 3	$\zeta+\lambda^{48}$	3447317785707529939588559
$\zeta+\lambda^{49}$	12284656140674766792017803 6	$\zeta+\lambda^{50}$	26406363633076937432415391 2
$\zeta+\lambda^{51}$	16306063251507711682872572 8	$\zeta+\lambda^{52}$	28673828347400375392885160 4
$\zeta+\lambda^{53}$	22165102259849777074405957 1	$\zeta+\lambda^{54}$	18018503144596819135536865 0
$\zeta+\lambda^{55}$	11506301550011653091597957 7	$\zeta+\lambda^{56}$	26320188212293601141493239 0
$\zeta+\lambda^{57}$	27544773170113136138842384 6	$\zeta+\lambda^{58}$	13751648811560513699507080 7
$\zeta+\lambda^{59}$	20163863504109484689284285 8	$\zeta+\lambda^{60}$	24842626503707132894679523 8
$\zeta+\lambda^{61}$	21664945781132831882194145	$\zeta+\lambda^{62}$	21221761531665158545318743
$\zeta+\lambda^{63}$	20409443512063114779858980 6	$\zeta+\lambda^{64}$	25455288912009636931412565 9

Table A.1: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$

α	$\log_\gamma(\alpha)$	α	$\log_\gamma(\alpha)$
$\zeta+\lambda^{65}$	289874636975270203885102287	$\zeta+\lambda^{66}$	38356433400535569851362782
$\zeta+\lambda^{67}$	12717678142815283739137857 1	$\zeta+\lambda^{68}$	11754390038894777413625202 7
$\zeta+\lambda^{69}$	17524330646691176371888039 1	$\zeta+\lambda^{70}$	10728824172380799458333137 2
$\zeta+\lambda^{71}$	57060669007602570552304555	$\zeta+\lambda^{72}$	28338929811091622870892315
$\zeta+\lambda^{73}$	13461254620400547729807065	$\zeta+\lambda^{74}$	27563283154234405560362002 4
$\zeta+\lambda^{75}$	28259710451466454684910022 9	$\zeta+\lambda^{76}$	24918209001240600113445107 3
$\zeta+\lambda^{77}$	44277451386825090602542608	$\zeta+\lambda^{78}$	25931437503993118314343671
$\zeta+\lambda^{79}$	30433064330311452235058665 3	$\zeta+\lambda^{80}$	35621348167969028340492880
$\zeta+\lambda^{81}$	22028808338995330289827873 0	$\zeta+\lambda^{82}$	37463523887513602799754496
$\zeta+\lambda^{83}$	31736067058981386973169537	$\zeta+\lambda^{84}$	18234715457703433745165843 0
$\zeta+\lambda^{85}$	18964598452345409788830817 8	$\zeta+\lambda^{86}$	73851516947168730695453792
$\zeta+\lambda^{87}$	28629185005402634508697105 2	$\zeta+\lambda^{88}$	21614246197010751111083987 2
$\zeta+\lambda^{89}$	29902237710882211694923526 2	$\zeta+\lambda^{90}$	10753839181025092578103633 2
$\zeta+\lambda^{91}$	13511496416292935376348712 8	$\zeta+\lambda^{92}$	27153252105349210113077196 9
$\zeta+\lambda^{93}$	12601723020913148518196227 9	$\zeta+\lambda^{94}$	12358955738961869136305296 6
$\zeta+\lambda^{95}$	26794655971351970653808180 9	$\zeta+\lambda^{96}$	13138639605703919728233832 5
$\zeta+\lambda^{97}$	63397409637910064344408164	$\zeta+\lambda^{98}$	26821448276839928951550100 3
$\zeta+\lambda^{99}$	62687163929754783208156355	$\zeta+\lambda^{100}$	22626206953014101926469134 2
$\zeta+\lambda^{101}$	29180857445075171979951785 7	$\zeta+\lambda^{102}$	28856235597618431660731260 2
$\zeta+\lambda^{103}$	27908455291007218976245492 2	$\zeta+\lambda^{104}$	79436210589444030171224 21
$\zeta+\lambda^{105}$	24435732935152099143752581 7	$\zeta+\lambda^{106}$	13884833905256949841649454 9
$\zeta+\lambda^{107}$	48040365524838535430231015	$\zeta+\lambda^{108}$	22756201873489933950365048 8
$\zeta+\lambda^{109}$	12452027321697776600007242 5	$\zeta+\lambda^{110}$	15229648401324218704420113 2
$\zeta+\lambda^{111}$	96375242006871962930490322	$\zeta+\lambda^{112}$	26745269671480518093741277 4
$\zeta+\lambda^{113}$	29231747761432347395067287 1	$\zeta+\lambda^{114}$	19770923644011604537308629 0
$\zeta+\lambda^{115}$	18592985699332267794381308 8	$\zeta+\lambda^{116}$	25217891144951304053146975 7
$\zeta+\lambda^{117}$	22349392205390891262933877 4	$\zeta+\lambda^{118}$	23197730899491416563127151 6
$\zeta+\lambda^{119}$	22115779321677756679496063 5	$\zeta+\lambda^{120}$	10130694878743813717687479 1
$\zeta+\lambda^{121}$	45985416084608851965672309	$\zeta+\lambda^{122}$	15153690476401380507093923 2
$\zeta+\lambda^{123}$	10604150579250089057799367 2	$\zeta+\lambda^{124}$	13464675362702676717156177 2
$\zeta+\lambda^{125}$	18000951522272012251790000 9	$\zeta+\lambda^{126}$	70291012123675837358325645
$\zeta+\lambda^{127}$	21811936904381002226561557 2	$\zeta+\lambda^{128}$	24554087598969235934826609 0

Table A.2: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$ (continued)

α	$\log_\gamma(\alpha)$	α	$\log_\gamma(\alpha)$
$\zeta+\lambda^{129}$	10800472781080893558381121 6	$\zeta+\lambda^{130}$	12384225256451216058248126
$\zeta+\lambda^{131}$	20396489126847859310804288 0	$\zeta+\lambda^{132}$	48787676106680171913341506
$\zeta+\lambda^{133}$	28638071221722904499243782 5	$\zeta+\lambda^{134}$	20308196758103421932887114
$\zeta+\lambda^{135}$	10496416312622601673627692 0	$\zeta+\lambda^{136}$	15034141859324414572622616 5
$\zeta+\lambda^{137}$	56890118196069214947473142	$\zeta+\lambda^{138}$	16417717880788328160692668 9
$\zeta+\lambda^{139}$	18097323238284550123957520 5	$\zeta+\lambda^{140}$	22247789295363713195212245 6
$\zeta+\lambda^{141}$	28659436816171175231787515 9	$\zeta+\lambda^{142}$	43688270978266751194323615
$\zeta+\lambda^{143}$	13194398233756211644253329 8	$\zeta+\lambda^{144}$	26524150578732746581178058 0
$\zeta+\lambda^{145}$	24888775045954719618138020 1	$\zeta+\lambda^{146}$	13916860716025393209614829 2
$\zeta+\lambda^{147}$	29298590882477203206797537 7	$\zeta+\lambda^{148}$	10841447469231376422237261 2
$\zeta+\lambda^{149}$	12660796348621758354580139	$\zeta+\lambda^{150}$	62594709934864216620976691
$\zeta+\lambda^{151}$	28367438581449766756455145 4	$\zeta+\lambda^{152}$	18085648591187744187778720 6
$\zeta+\lambda^{153}$	27023242343084091184022611 1	$\zeta+\lambda^{154}$	81941119355501810048530505
$\zeta+\lambda^{155}$	27302801458202435781468019 5	$\zeta+\lambda^{156}$	16197069458868592360148 91
$\zeta+\lambda^{157}$	16233375162017136779890862 9	$\zeta+\lambda^{158}$	16735420215771513660369406 4
$\zeta+\lambda^{159}$	12051106727135784575018341 9	$\zeta+\lambda^{160}$	23372147965090723601586665 7
$\zeta+\lambda^{161}$	19261418932558824472714135	$\zeta+\lambda^{162}$	27872276461258877060327198 9
$\zeta+\lambda^{163}$	24796494043408004169566402 9	$\zeta+\lambda^{164}$	94119770840604026593707304
$\zeta+\lambda^{165}$	17482300334944059072806242 2	$\zeta+\lambda^{166}$	1
$\zeta+\lambda^{167}$	27238788773203625893165745 1	$\zeta+\lambda^{168}$	86633665014398563099078298
$\zeta+\lambda^{169}$	71240618417126117077211982	$\zeta+\lambda^{170}$	69380423528369019607274203
$\zeta+\lambda^{171}$	29047341174576444439674614 1	$\zeta+\lambda^{172}$	30764701472202434332666168 1
$\zeta+\lambda^{173}$	42926023851516580244989 01	$\zeta+\lambda^{174}$	51100970268637288483849042
$\zeta+\lambda^{175}$	99823187350058002949074008	$\zeta+\lambda^{176}$	17875566314277572304828709 8
$\zeta+\lambda^{177}$	23042002055727396000512615 7	$\zeta+\lambda^{178}$	20991174563492088640595897 7
$\zeta+\lambda^{179}$	56710234708743977149294456	$\zeta+\lambda^{180}$	21239012496732273552254750 2
$\zeta+\lambda^{181}$	27921502021328722346159726 3	$\zeta+\lambda^{182}$	22275947749907929753879010 2
$\zeta+\lambda^{183}$	22955723036383831262441915 6	$\zeta+\lambda^{184}$	22417954237777146326226096 9
$\zeta+\lambda^{185}$	15349450678391771302006809 3	$\zeta+\lambda^{186}$	12050115319477251802756486 7
$\zeta+\lambda^{187}$	54594993515293880227016105	$\zeta+\lambda^{188}$	67047106912208099346143223
$\zeta+\lambda^{189}$	42590084650795238177614836	$\zeta+\lambda^{190}$	13493902354657064629321628 8
$\zeta+\lambda^{191}$	63788416473339949077139236	$\zeta+\lambda^{192}$	23853701612272776371687376 8

Table A.3: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$ (continued)

α	$\log_\gamma(\alpha)$	α	$\log_\gamma(\alpha)$
$\zeta+\lambda^{193}$	29500225573695610822217049 7	$\zeta+\lambda^{194}$	33452384403016975443261448
$\zeta+\lambda^{195}$	22675934423888537194729704 9	$\zeta+\lambda^{196}$	16441577059989401076351238 8
$\zeta+\lambda^{197}$	18798652791672787457831104 6	$\zeta+\lambda^{198}$	17564451870104741342345884 4
$\zeta+\lambda^{199}$	28908169580134404810617896	$\zeta+\lambda^{200}$	10538872637255088081544390 0
$\zeta+\lambda^{201}$	15563692748680804955636392 1	$\zeta+\lambda^{202}$	17619209562200159910310145 1
$\zeta+\lambda^{203}$	10886657591697592349157619 3	$\zeta+\lambda^{204}$	29424189956695436245559679 7
$\zeta+\lambda^{205}$	26736916897653266953872560 9	$\zeta+\lambda^{206}$	76169186974092165494542307
$\zeta+\lambda^{207}$	15640528020891991946800828 9	$\zeta+\lambda^{208}$	15770982848551649990162157 4
$\zeta+\lambda^{209}$	24401378369416601087149902	$\zeta+\lambda^{210}$	16957366136301436453944044 0
$\zeta+\lambda^{211}$	30465529870989522274729092 2	$\zeta+\lambda^{212}$	79581034891221809905127 78
$\zeta+\lambda^{213}$	19419869048777207220766931 2	$\zeta+\lambda^{214}$	20532767864657935340390007
$\zeta+\lambda^{215}$	53305984964867387236865971	$\zeta+\lambda^{216}$	38883929858903310463377543
$\zeta+\lambda^{217}$	90868289341404546199018233	$\zeta+\lambda^{218}$	30613480272809816229170027 0
$\zeta+\lambda^{219}$	18457665489051020393935076 0	$\zeta+\lambda^{220}$	22677028705851495451599182 8
$\zeta+\lambda^{221}$	10179366608172305409353807	$\zeta+\lambda^{222}$	10602371639065670323819257 6
$\zeta+\lambda^{223}$	27750967289403871061142599 8	$\zeta+\lambda^{224}$	91545332728896049056784 69
$\zeta+\lambda^{225}$	18631296245009225444341087 1	$\zeta+\lambda^{226}$	90403414721509610199939565
$\zeta+\lambda^{227}$	92886667564241681561277764	$\zeta+\lambda^{228}$	33510479531643077540876160
$\zeta+\lambda^{229}$	18300097661755352298808959 1	$\zeta+\lambda^{230}$	91265380486368272182676515
$\zeta+\lambda^{231}$	59002359565778703024889233	$\zeta+\lambda^{232}$	34264867479868460810734942
$\zeta+\lambda^{233}$	29745175522210459102209102 2	$\zeta+\lambda^{234}$	57218595182614053027230395
$\zeta+\lambda^{235}$	17865900497529808936866449 8	$\zeta+\lambda^{236}$	10247021853213831932531337 5
$\zeta+\lambda^{237}$	33461539298237214439353268	$\zeta+\lambda^{238}$	15611314150257822217211813 4
$\zeta+\lambda^{239}$	28587731262748460844694326 4	$\zeta+\lambda^{240}$	85494712539152191660715126
$\zeta+\lambda^{241}$	21628792072511708954025118	$\zeta+\lambda^{242}$	25081221901957417425310765 6
$\zeta+\lambda^{243}$	21958981407689031092610012 4	$\zeta+\lambda^{244}$	16194895569919753268909552 6
$\zeta+\lambda^{245}$	13073511916763329189882454 5	$\zeta+\lambda^{246}$	84290185480225124048542976
$\zeta+\lambda^{247}$	22376987982034302709888031 1	$\zeta+\lambda^{248}$	14957426591969177328029525 4
$\zeta+\lambda^{249}$	17636664355658522096561190 6	$\zeta+\lambda^{250}$	49703412344191105681997600
$\zeta+\lambda^{251}$	77624305010052315824933994	$\zeta+\lambda^{252}$	16108619132191809860202607
$\zeta+\lambda^{253}$	26830059208805028870429426 4	$\zeta+\lambda^{254}$	16168148772228800730459551
$\zeta+\lambda^{255}$	26744436820090328134788460 4		

Table A.4: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$ (continued)

Appendix B

Discrete logarithms of elements in the factor base of $\mathbf{F}_{16^{22}}$ with another base

We define $\mathbf{F}^*_{16^2} = \langle\lambda\rangle$ and choose

$$h_0(x) = \lambda * x^2 + \lambda^4 * x + 1, h_1(x) = x + \lambda.$$

We have

$$h_1(x) * x^{16} - h_0(x) = x^{17} + \lambda * x^{16} + \lambda * x^2 + \lambda^4 * x + 1.$$

The primitive element of $\mathbf{F}^*_{16^{22}}$ is

$$\gamma = \lambda^{-1} * (\zeta + \lambda^{177})^{-214414451248775014933508 44}.$$

The discrete logarithms of elements in the factor base can be retrieved from the last row of U.

α	$\log_\gamma(\alpha)$	α	$\log_\gamma(\alpha)$
λ	245160674446712564244728522	ζ	25567035118933584708029683 9
$\zeta+\lambda$	14312271094603845520856727 5	$\zeta+\lambda^2$	11700422371149654268411332
$\zeta+\lambda^3$	37418405030167078068454494	$\zeta+\lambda^4$	64157124908740452291313973
$\zeta+\lambda^5$	59290014694581809190099094	$\zeta+\lambda^6$	15475369300152803968947456 7
$\zeta+\lambda^7$	13501892447077708167829181 5	$\zeta+\lambda^8$	37165475098659344235916287
$\zeta+\lambda^9$	43596175006155616900512999	$\zeta+\lambda^{10}$	15746580406555867545532324
$\zeta+\lambda^{11}$	74226434922941803317076548	$\zeta+\lambda^{12}$	18889995827408215557762518 7
$\zeta+\lambda^{13}$	17934032502404877506480801 4	$\zeta+\lambda^{14}$	26294347964204229780948920 8
$\zeta+\lambda^{15}$	18630106221982036918612268 8	$\zeta+\lambda^{16}$	28074296622893217188287334 9
$\zeta+\lambda^{17}$	44537570606883223833960472	$\zeta+\lambda^{18}$	47525890739556801076509499
$\zeta+\lambda^{19}$	23978285308313198592459098	$\zeta+\lambda^{20}$	91917754247760122290558 20
$\zeta+\lambda^{21}$	24129675905248851737008285 0	$\zeta+\lambda^{22}$	17200207445400998949389904 4
$\zeta+\lambda^{23}$	21603423215262052030462782 6	$\zeta+\lambda^{24}$	27794338733725445979788622 2
$\zeta+\lambda^{25}$	10604991474799710646300345 1	$\zeta+\lambda^{26}$	17235024889557159944520868 5
$\zeta+\lambda^{27}$	19730618287518982568359081 2	$\zeta+\lambda^{28}$	82230899015227565528889459
$\zeta+\lambda^{29}$	90360508856614691582774480	$\zeta+\lambda^{30}$	30363647814517385664296546 1
$\zeta+\lambda^{31}$	18471297691531713136625009 8	$\zeta+\lambda^{32}$	15387215786408171879759348
$\zeta+\lambda^{33}$	10743321192363695812477323 5	$\zeta+\lambda^{34}$	17775488840320789335907388 7
$\zeta+\lambda^{35}$	16050741761649115357069078 2	$\zeta+\lambda^{36}$	20749768577212060837693987 0
$\zeta+\lambda^{37}$	11131384461694130488458971 6	$\zeta+\lambda^{38}$	19569869391632138953170081 6
$\zeta+\lambda^{39}$	29455772851300086648289957	$\zeta+\lambda^{40}$	86791224276969645656148162
$\zeta+\lambda^{41}$	53411828373357718099857214	$\zeta+\lambda^{42}$	46938099161694680002852703
$\zeta+\lambda^{43}$	19722595408318778046659098 4	$\zeta+\lambda^{44}$	13524202319624782524277053 1
$\zeta+\lambda^{45}$	24701049726177104301840693 6	$\zeta+\lambda^{46}$	29340847638037927133076971 3
$\zeta+\lambda^{47}$	14074240195783548647144927	$\zeta+\lambda^{48}$	25544636534887449413521681
$\zeta+\lambda^{49}$	23851311245127154612333958 9	$\zeta+\lambda^{50}$	10744638739214385326228481 3
$\zeta+\lambda^{51}$	83904274852733394929829962	$\zeta+\lambda^{52}$	26598440447716845468975999 6
$\zeta+\lambda^{53}$	26611968269059632640604164	$\zeta+\lambda^{54}$	27503005423449886616295926 0
$\zeta+\lambda^{55}$	14540069353220682369763338 3	$\zeta+\lambda^{56}$	25069597386942895739474395
$\zeta+\lambda^{57}$	25966369311974381456486219	$\zeta+\lambda^{58}$	97767382179440424780370198
$\zeta+\lambda^{59}$	40890148273304153517493382	$\zeta+\lambda^{60}$	27814968363296461556404078 2
$\zeta+\lambda^{61}$	26525104771995240472640740	$\zeta+\lambda^{62}$	55212125169498570189217737
$\zeta+\lambda^{63}$	52057644118912776804616834	$\zeta+\lambda^{64}$	17202035832134249997823457 1

Table B.1: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$ with another base

α	$\log_\gamma(\alpha)$	α	$\log_\gamma(\alpha)$
$\zeta+\lambda^{65}$	13045321065804662587191783	$\zeta+\lambda^{66}$	29313763248356176813029 1323
$\zeta+\lambda^{67}$	21950384240054147851777 7309	$\zeta+\lambda^{68}$	17370816958715358295839 2663
$\zeta+\lambda^{69}$	30499188446598820799715 2959	$\zeta+\lambda^{70}$	23654398543524502091862 5088
$\zeta+\lambda^{71}$	50999824672754506714174025	$\zeta+\lambda^{72}$	49040487145055091653989785
$\zeta+\lambda^{73}$	25740617431284273165962 3665	$\zeta+\lambda^{74}$	86916142926288897156366331
$\zeta+\lambda^{75}$	76575741693451191085290801	$\zeta+\lambda^{76}$	24408403746138757400297827
$\zeta+\lambda^{77}$	25879593249181307591296 3152	$\zeta+\lambda^{78}$	18611616658872108245099 2299
$\zeta+\lambda^{79}$	49890665498283796829214737	$\zeta+\lambda^{80}$	11298626746805110766604 7985
$\zeta+\lambda^{81}$	15780212523358210767623 4500	$\zeta+\lambda^{82}$	63973672119081157954335449
$\zeta+\lambda^{83}$	75850760194779005214740398	$\zeta+\lambda^{84}$	23869402901634048981034 1500
$\zeta+\lambda^{85}$	12440010258993529628232 0597	$\zeta+\lambda^{86}$	59235175165913832194019763
$\zeta+\lambda^{87}$	15447457216132798849702 0218	$\zeta+\lambda^{88}$	10941595361024792360662 5203
$\zeta+\lambda^{89}$	16778954119898761746371 9918	$\zeta+\lambda^{90}$	15469150211595327824505 2418
$\zeta+\lambda^{91}$	14520586569031201954031 0577	$\zeta+\lambda^{92}$	23887435354000321904726 2551
$\zeta+\lambda^{93}$	27698079477624147830808 5066	$\zeta+\lambda^{94}$	41911984029038103882539 99
$\zeta+\lambda^{95}$	61478754412602543315697036	$\zeta+\lambda^{96}$	29983535095276004527721 8860
$\zeta+\lambda^{97}$	26116168996848317187520 0311	$\zeta+\lambda^{98}$	22892792316276011967421 9742
$\zeta+\lambda^{99}$	27536016932382149423964 0010	$\zeta+\lambda^{100}$	68291259138980224088221968
$\zeta+\lambda^{101}$	17088365218561234028140 6848	$\zeta+\lambda^{102}$	25843923872589629087866 3963
$\zeta+\lambda^{103}$	59186257162111562019475773	$\zeta+\lambda^{104}$	12251171956915652545937 8489
$\zeta+\lambda^{105}$	69821419855716190789379023	$\zeta+\lambda^{106}$	89015834697375054765446976
$\zeta+\lambda^{107}$	10949962302149442196174 1905	$\zeta+\lambda^{108}$	91356123031449102950454032
$\zeta+\lambda^{109}$	39521610919314535485540215	$\zeta+\lambda^{110}$	28852106779657229423441 2858
$\zeta+\lambda^{111}$	17633366081214456270284 5163	$\zeta+\lambda^{112}$	69083283226211912692523191
$\zeta+\lambda^{113}$	26214585589532093288474619	$\zeta+\lambda^{114}$	22397384718294518574808 6825
$\zeta+\lambda^{115}$	81032285485774567858791332	$\zeta+\lambda^{116}$	35728974678018449457346963
$\zeta+\lambda^{117}$	10857391020838405343310 8776	$\zeta+\lambda^{118}$	10761368677694720385631 7994
$\zeta+\lambda^{119}$	20016539478109176900526 2230	$\zeta+\lambda^{120}$	25579355528598236818135 3334
$\zeta+\lambda^{121}$	30814744272474970499331 8031	$\zeta+\lambda^{122}$	11076523829663430514745 5388
$\zeta+\lambda^{123}$	16426460812038987330189 48	$\zeta+\lambda^{124}$	33738876733517376730227193
$\zeta+\lambda^{125}$	22927405759920171361855 6051	$\zeta+\lambda^{126}$	20143321466615190589163 7210
$\zeta+\lambda^{127}$	27996460591231049931925 9848	$\zeta+\lambda^{128}$	18110095100236380444932 3700

Table B.2: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$ with another base (continued)

α	$\log_\gamma(\alpha)$	α	$\log_\gamma(\alpha)$
$\zeta+\lambda^{129}$	10362256858151958561927694 4	$\zeta+\lambda^{130}$	25520804848092702918527872 9
$\zeta+\lambda^{131}$	26876189317792824479971843 0	$\zeta+\lambda^{132}$	62918530600723303569435719
$\zeta+\lambda^{133}$	34307722353387684169816680	$\zeta+\lambda^{134}$	20284460568668209375977782 6
$\zeta+\lambda^{135}$	54474716781140286048917955	$\zeta+\lambda^{136}$	21704086419500732964045946 0
$\zeta+\lambda^{137}$	13620757746123506176442848 8	$\zeta+\lambda^{138}$	30680185318399701525140978 6
$\zeta+\lambda^{139}$	21724946875405390449885933 5	$\zeta+\lambda^{140}$	1317592104461177030179659
$\zeta+\lambda^{141}$	17167769899226131596327447 1	$\zeta+\lambda^{142}$	45669043370126710306284780
$\zeta+\lambda^{143}$	19145084976308939408928226 2	$\zeta+\lambda^{144}$	15182526603617101446731388 0
$\zeta+\lambda^{145}$	24245048076158694710058872 4	$\zeta+\lambda^{146}$	16853225889166103566536368 8
$\zeta+\lambda^{147}$	46001997696396834415129293	$\zeta+\lambda^{148}$	22844487503677124317007353
$\zeta+\lambda^{149}$	16501350988086852731879067 1	$\zeta+\lambda^{150}$	51598955349120579196291939
$\zeta+\lambda^{151}$	22378448565252320669913232 6	$\zeta+\lambda^{152}$	25879683735614742395366986 4
$\zeta+\lambda^{153}$	29683754549864189712201523 9	$\zeta+\lambda^{154}$	25577027196686787896251442 5
$\zeta+\lambda^{155}$	29100991901105853235778488 5	$\zeta+\lambda^{156}$	30093046093371256837906149 9
$\zeta+\lambda^{157}$	23917040531048317600335481 6	$\zeta+\lambda^{158}$	35338581065788991302855186
$\zeta+\lambda^{159}$	81374545680450706377193796	$\zeta+\lambda^{160}$	15973549791184305688297380 3
$\zeta+\lambda^{161}$	26421170485646736887728980 5	$\zeta+\lambda^{162}$	12800306334222362494992697 6
$\zeta+\lambda^{163}$	15630463203160999172475273 1	$\zeta+\lambda^{164}$	85556503567264591078239641
$\zeta+\lambda^{165}$	15907902647915333612020420 8	$\zeta+\lambda^{166}$	11792128168783361665609549 4
$\zeta+\lambda^{167}$	36897129086682654192346059	$\zeta+\lambda^{168}$	48371388970228548293231920
$\zeta+\lambda^{169}$	54790314247026174674932188	$\zeta+\lambda^{170}$	23043119770187318545342554 2
$\zeta+\lambda^{171}$	19901677747777961433647511 9	$\zeta+\lambda^{172}$	27941639735875018275593688 4
$\zeta+\lambda^{173}$	26565614117563001733116415 4	$\zeta+\lambda^{174}$	18883100804010926316067583
$\zeta+\lambda^{175}$	23038886118138818396066467 2	$\zeta+\lambda^{176}$	98199271125411705493140117
$\zeta+\lambda^{177}$	3	$\zeta+\lambda^{178}$	14257055252475529327524876 3
$\zeta+\lambda^{179}$	43839382219727567115722204	$\zeta+\lambda^{180}$	26018800811480825006493186 8
$\zeta+\lambda^{181}$	18193824140505948779468055 7	$\zeta+\lambda^{182}$	19772644674899276684342564 3
$\zeta+\lambda^{183}$	14797840141823183608487832 4	$\zeta+\lambda^{184}$	28850252321597401295259452 1
$\zeta+\lambda^{185}$	99254748498175494329063262	$\zeta+\lambda^{186}$	49529503067517771000507583
$\zeta+\lambda^{187}$	25374367383861719788169842 0	$\zeta+\lambda^{188}$	18265661494451029463273626 2
$\zeta+\lambda^{189}$	11890650053122926054808676 4	$\zeta+\lambda^{190}$	30154155539957480164768714 7
$\zeta+\lambda^{191}$	15562107353801379850106475 9	$\zeta+\lambda^{192}$	18365737110999610235185527 7

Table B.3: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$ with another base (continued)

α	$\log_\gamma(\alpha)$	α	$\log_\gamma(\alpha)$
$\zeta+\lambda^{193}$	795125429918982020161037 63	$\zeta+\lambda^{194}$	227451768028285780430620127
$\zeta+\lambda^{195}$	309343018264006547584815426	$\zeta+\lambda^{196}$	241946350445695204771062252
$\zeta+\lambda^{197}$	205696605635317462614292499	$\zeta+\lambda^{198}$	89100991046833477813984036
$\zeta+\lambda^{199}$	120504295183975708730894969	$\zeta+\lambda^{200}$	203109136212029700466823060
$\zeta+\lambda^{201}$	75708409138614621737562364	$\zeta+\lambda^{202}$	133280859693258015441507444
$\zeta+\lambda^{203}$	112246037963627791938335312	$\zeta+\lambda^{204}$	267187970885747179529069048
$\zeta+\lambda^{205}$	304624787618803358524298191	$\zeta+\lambda^{206}$	116788135825489062673160323
$\zeta+\lambda^{207}$	105382678516271575792458311	$\zeta+\lambda^{208}$	230832595293942592532363531
$\zeta+\lambda^{209}$	227069453395107697837040463	$\zeta+\lambda^{210}$	79199699021640775261314565
$\zeta+\lambda^{211}$	42756922053006075634015213	$\zeta+\lambda^{212}$	205121426327140748767301122
$\zeta+\lambda^{213}$	102621957424082188651702118	$\zeta+\lambda^{214}$	40687680231356695413187713
$\zeta+\lambda^{215}$	178593835233410231480344304	$\zeta+\lambda^{216}$	15985714590584374092039955 2
$\zeta+\lambda^{217}$	139365109108623334979437542	$\zeta+\lambda^{218}$	5262938317090958824682725
$\zeta+\lambda^{219}$	202111551923737297717435720	$\zeta+\lambda^{220}$	10349266009687522698470 6387
$\zeta+\lambda^{221}$	195226179915492843929215243	$\zeta+\lambda^{222}$	22208257449946123443943 8879
$\zeta+\lambda^{223}$	103006090504657036013554682	$\zeta+\lambda^{224}$	29843987868021421392573 3386
$\zeta+\lambda^{225}$	25378257763922468039664937 9	$\zeta+\lambda^{226}$	29126902460135912912793380
$\zeta+\lambda^{227}$	18014710973590532657396965 6	$\zeta+\lambda^{228}$	23074846185139925293851372 0
$\zeta+\lambda^{229}$	10405542181425500943167537 9	$\zeta+\lambda^{230}$	20243213174442733438882871 0
$\zeta+\lambda^{231}$	79475369164356306161226882	$\zeta+\lambda^{232}$	22555411574129859300690929 3
$\zeta+\lambda^{233}$	30255460651632506769337877 8	$\zeta+\lambda^{234}$	25462460251537630277546283 5
$\zeta+\lambda^{235}$	15223990676718194678380117 7	$\zeta+\lambda^{236}$	19906253428057787772386765 5
$\zeta+\lambda^{237}$	29185766533400161277652129 2	$\zeta+\lambda^{238}$	16589850016987618079709027 6
$\zeta+\lambda^{239}$	22934995481865424831279550 6	$\zeta+\lambda^{240}$	25032822161327908717711648 9
$\zeta+\lambda^{241}$	10850760786089207425494571 7	$\zeta+\lambda^{242}$	79626510054879541240635569
$\zeta+\lambda^{243}$	25502565585556793296932674 6	$\zeta+\lambda^{244}$	20221417659910989353804145 4
$\zeta+\lambda^{245}$	22521014278059103413956580 5	$\zeta+\lambda^{246}$	14993817573038109672982546 9
$\zeta+\lambda^{247}$	34500298375756404642131589	$\zeta+\lambda^{248}$	26753641265053729392148737 6
$\zeta+\lambda^{249}$	20183868058509174519152079	$\zeta+\lambda^{250}$	23857613827173301387226720 5
$\zeta+\lambda^{251}$	21931622638974618060665259 6	$\zeta+\lambda^{252}$	22921817957885030462945804 3
$\zeta+\lambda^{253}$	72513519521903370374564186	$\zeta+\lambda^{254}$	23822816313418411479863659
$\zeta+\lambda^{255}$	61496084422620635236180111		

Table B.4: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{22}}$ with another base (continued)

Appendix C

Discrete logarithms of elements in the factor base of $\mathbf{F}_{16^{24}}$

We define $\mathbf{F}^*_{16^2} = \langle\lambda\rangle$ and we choose

$$h_0(x) = \lambda * x^2 + (\lambda^6 + \lambda^5 + \lambda^4 + \lambda^2) * x + 1, h_1(x) = x + \lambda.$$

We have

$$h_1(x) * x^{16} - h_0(x) = x^{17} + \lambda * x^{16} + \lambda * x^2 + (\lambda^6 + \lambda^5 + \lambda^4 + \lambda^2) * x + 1.$$

The primitive element of $\mathbf{F}^*_{16^{24}}$ is

$$\gamma = \lambda^{22} * (z + \lambda^{16})^{88} * (z + \lambda^{100})^{1526740352191631200110704 11}.$$

The discrete logarithms of elements in the factor base can be retrieved from the last row of U.

α	$\log_\gamma(\alpha)$
λ	78917463837737810779451621118
ζ	628330903496446298221485457 39
$\zeta + \lambda$	735258893035925618768277424 53
$\zeta + \lambda^2$	472300796961055407262909275 16
$\zeta + \lambda^3$	549177744297834269336369644 84
$\zeta + \lambda^4$	792354358861078462188542315 7
$\zeta + \lambda^5$	457172706681590789423606384 85
$\zeta + \lambda^6$	334146824237615651633793466 54
$\zeta + \lambda^7$	402558706382663463822074093 15
$\zeta + \lambda^8$	430607779114765903041683661 73
$\zeta + \lambda^9$	427181312796892336267825454 22
$\zeta + \lambda^{10}$	614312094814696082021225578 56
$\zeta + \lambda^{11}$	154205189882588328769644484 16
$\zeta + \lambda^{12}$	520331347995931725554463617 41
$\zeta + \lambda^{13}$	28651410788658624868720993 07
$\zeta + \lambda^{14}$	98978674930790608881610148 93
$\zeta + \lambda^{15}$	14112830488700460515374781089
$\zeta + \lambda^{16}$	31565952605284615774562307460
$\zeta + \lambda^{17}$	74899234251784049139464962555
$\zeta + \lambda^{18}$	97351932663966041108358729 37
$\zeta + \lambda^{19}$	37466249378068174722839537 05
$\zeta + \lambda^{20}$	51276010888349207343565164415
$\zeta + \lambda^{21}$	46724702733336032548408812110
$\zeta + \lambda^{22}$	45417240492128703795092645988
$\zeta + \lambda^{23}$	84733515823654393827257448 81
$\zeta + \lambda^{24}$	57200882769996519643647198217
$\zeta + \lambda^{25}$	42062867158594407944206868909
$\zeta + \lambda^{26}$	53314752603614214713380073497
$\zeta + \lambda^{27}$	67801570807285324778714467569
$\zeta + \lambda^{28}$	65111040054663487435376557373
$\zeta + \lambda^{29}$	17479223786687203510917239844
$\zeta + \lambda^{30}$	35093733237113190746143475037
$\zeta + \lambda^{31}$	32570827880458575097784800932
$\zeta + \lambda^{32}$	12641117537395985096198374631

Table C.1: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$

$\zeta + \lambda^{33}$	548996376115598413156349384 59
$\zeta + \lambda^{34}$	27419590524173778347287346224
$\zeta + \lambda^{35}$	52804964157720351665905091944
$\zeta + \lambda^{36}$	32342299631230719587973850129
$\zeta + \lambda^{37}$	76936061386306080119873186312
$\zeta + \lambda^{38}$	27220689991489861337888431391
$\zeta + \lambda^{39}$	72932342784228951083331645916
$\zeta + \lambda^{40}$	51634719174051252992090809 93
$\zeta + \lambda^{41}$	14303397013813561238733739956
$\zeta + \lambda^{42}$	16667521691891993395795895105
$\zeta + \lambda^{43}$	57014439471472481010709074059
$\zeta + \lambda^{44}$	38230243241529658763723141566
$\zeta + \lambda^{45}$	90891472219558327932539153 24
$\zeta + \lambda^{46}$	18413793106346570296254066967
$\zeta + \lambda^{47}$	58811658572606698138627374963
$\zeta + \lambda^{48}$	58081754185828197344720742188
$\zeta + \lambda^{49}$	72966112765085137900112962112
$\zeta + \lambda^{50}$	30658168281362004830752264659
$\zeta + \lambda^{51}$	78547887407583391577398155025
$\zeta + \lambda^{52}$	32782409185238606453628068269
$\zeta + \lambda^{53}$	51990384895874794696621036010
$\zeta + \lambda^{54}$	46744121179621417982657086030
$\zeta + \lambda^{55}$	44373611950153893781607418907
$\zeta + \lambda^{56}$	76496867816713383248579218811
$\zeta + \lambda^{57}$	45400616131679528146328715254
$\zeta + \lambda^{58}$	62123869816878840747381133015
$\zeta + \lambda^{59}$	93066150388973143720088829 0
$\zeta + \lambda^{60}$	73123534784655137115281820428
$\zeta + \lambda^{61}$	68010719292134552328447538869
$\zeta + \lambda^{62}$	39077434130981808413153624096
$\zeta + \lambda^{63}$	13479182764941489266572502498
$\zeta + \lambda^{64}$	44012268866734707601622948042

Table C.2: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$ (continued)

$\zeta + \lambda^{65}$	33485563897720043744760666730
$\zeta + \lambda^{66}$	28811251583862757756826394110
$\zeta + \lambda^{67}$	50381712729231411800736557829
$\zeta + \lambda^{68}$	78911470348976469058467873 08
$\zeta + \lambda^{69}$	71253612566594565723283184607
$\zeta + \lambda^{70}$	28437808527264401458993371965
$\zeta + \lambda^{71}$	46061211109812613778391041288
$\zeta + \lambda^{72}$	61483240293102006622862467207
$\zeta + \lambda^{73}$	65995178101358173532797410 95
$\zeta + \lambda^{74}$	48190888921109927390295438909
$\zeta + \lambda^{75}$	55989936308049697224625312022
$\zeta + \lambda^{76}$	50877871166489547030954202137
$\zeta + \lambda^{77}$	40956068935321194071525522395
$\zeta + \lambda^{78}$	51469665748251218919730758 77
$\zeta + \lambda^{79}$	14222848471115701707370933804
$\zeta + \lambda^{80}$	37348579112228888657856012299
$\zeta + \lambda^{81}$	74746784848432190071437398076
$\zeta + \lambda^{82}$	16127759585546392351104788516
$\zeta + \lambda^{83}$	74954697215415662372458125821
$\zeta + \lambda^{84}$	55658636605676470444596384889
$\zeta + \lambda^{85}$	14708148697267344188393374547
$\zeta + \lambda^{86}$	32035998220878016075856889033
$\zeta + \lambda^{87}$	20489723269347166249126654847
$\zeta + \lambda^{88}$	94137666152988792330756733 23
$\zeta + \lambda^{89}$	50955117320264787110432080509
$\zeta + \lambda^{90}$	79017352274004430263466176 62
$\zeta + \lambda^{91}$	91160994889022482078547697 13
$\zeta + \lambda^{92}$	16059240863801982139899752660
$\zeta + \lambda^{93}$	17591552596340728829482248 27
$\zeta + \lambda^{94}$	72354759919198512727358335583
$\zeta + \lambda^{95}$	53756203853116868920996274814
$\zeta + \lambda^{96}$	84435399087170470615584548 07

Table C.3: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$ (continued)

$\zeta + \lambda^{97}$	46513442261311289802432158526
$\zeta + \lambda^{98}$	70983211743762146886003854384
$\zeta + \lambda^{99}$	11208015826498350926223213152
$\zeta + \lambda^{100}$	63382530011411470074835160385
$\zeta + \lambda^{101}$	48261588098972167932261071419
$\zeta + \lambda^{102}$	18170789754285975728674455437
$\zeta + \lambda^{103}$	59604979622792231316799446071
$\zeta + \lambda^{104}$	10828268485134176768803062891
$\zeta + \lambda^{105}$	44906541314734542176013605 81
$\zeta + \lambda^{106}$	35463749158115443875622 4467
$\zeta + \lambda^{107}$	43786598502247468427610262652
$\zeta + \lambda^{108}$	45550133875011937859966834771
$\zeta + \lambda^{109}$	40426805794968671495292042340
$\zeta + \lambda^{110}$	70831593500600351493630884894
$\zeta + \lambda^{111}$	38211848688714283832772779989
$\zeta + \lambda^{112}$	50559173247880557268324805254
$\zeta + \lambda^{113}$	72761867963621550846111276770
$\zeta + \lambda^{114}$	53131979266488828611418770055
$\zeta + \lambda^{115}$	90926853792840224325044885 89
$\zeta + \lambda^{116}$	39059558238350676994040688686
$\zeta + \lambda^{117}$	57998087941268909937031889117
$\zeta + \lambda^{118}$	70663059378525708538943266 88
$\zeta + \lambda^{119}$	55430850414652056972279254955
$\zeta + \lambda^{120}$	76189912196933273000984417985
$\zeta + \lambda^{121}$	44365257402027681655849938372
$\zeta + \lambda^{122}$	31578669227499776635928761155
$\zeta + \lambda^{123}$	73346142737098850555132073374
$\zeta + \lambda^{124}$	10964682212185532349211175875
$\zeta + \lambda^{125}$	40935902046100394435467143521
$\zeta + \lambda^{126}$	68843551736314242138589242954
$\zeta + \lambda^{127}$	33549530699692743347412650386
$\zeta + \lambda^{128}$	52519598317449787246298140 84

Table C.4: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$ (continued)

$\zeta + \lambda^{129}$	48720013405934910184599067489
$\zeta + \lambda^{130}$	52810887224216171341505629833
$\zeta + \lambda^{131}$	69973286222071942108722018510
$\zeta + \lambda^{132}$	40120022074333217247940894555
$\zeta + \lambda^{133}$	65082174948570219261437338040
$\zeta + \lambda^{134}$	15137240274247981871381552261
$\zeta + \lambda^{135}$	72997232988609057750490144519
$\zeta + \lambda^{136}$	16957326851102048228374565848
$\zeta + \lambda^{137}$	74842503692180669082566904959
$\zeta + \lambda^{138}$	47784254542041912700501126872
$\zeta + \lambda^{139}$	14237362465375977488862393444
$\zeta + \lambda^{140}$	15494866232413153659878691929
$\zeta + \lambda^{141}$	35194116763538317561885818027
$\zeta + \lambda^{142}$	35478250996503101366591679877
$\zeta + \lambda^{143}$	16293509655131500790560009825
$\zeta + \lambda^{144}$	40483311535813431092200610602
$\zeta + \lambda^{145}$	63946247960775460702115826083
$\zeta + \lambda^{146}$	45708154259493184079324069607
$\zeta + \lambda^{147}$	53670251247571407089105595626
$\zeta + \lambda^{148}$	19978675019322247282247034342
$\zeta + \lambda^{149}$	49454873210696967199301318397
$\zeta + \lambda^{150}$	47311476144098852970104777757
$\zeta + \lambda^{151}$	70874229943316200053708158186
$\zeta + \lambda^{152}$	22696906826809709580994079639
$\zeta + \lambda^{153}$	38874215525524861393493298987
$\zeta + \lambda^{154}$	26919321661644114311155374107
$\zeta + \lambda^{155}$	53251123645128120067924131471
$\zeta + \lambda^{156}$	62960766233403049449501071566
$\zeta + \lambda^{157}$	29628696906149426734574566747
$\zeta + \lambda^{158}$	24947436124270621372066291143
$\zeta + \lambda^{159}$	63363038483596148789466937062
$\zeta + \lambda^{160}$	78560709418944366629852541000

Table C.5: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$ (continued)

$\zeta + \lambda^{161}$	140038050753185324818749304 54
$\zeta + \lambda^{162}$	11739171737333189280661232427
$\zeta + \lambda^{163}$	35647525880990763683938445106
$\zeta + \lambda^{164}$	12097242691103914294464212955
$\zeta + \lambda^{165}$	17548407743056291738406347200
$\zeta + \lambda^{166}$	31262491490678774063952856685
$\zeta + \lambda^{167}$	26887546081788951249033296959
$\zeta + \lambda^{168}$	73164552460333379527793867270
$\zeta + \lambda^{169}$	96522080522570543971763 8719
$\zeta + \lambda^{170}$	24281769713026219005112132883
$\zeta + \lambda^{171}$	13695690063475856495321861146
$\zeta + \lambda^{172}$	23893826286552840662073779336
$\zeta + \lambda^{173}$	59771669596121379938854176172
$\zeta + \lambda^{174}$	55040207046608453422185088350
$\zeta + \lambda^{175}$	31690877453464841957400227635
$\zeta + \lambda^{176}$	76889293533362156536054520830
$\zeta + \lambda^{177}$	45685901588350904393647104918
$\zeta + \lambda^{178}$	55934794697385194083775802463
$\zeta + \lambda^{179}$	63635657591138409339810039444
$\zeta + \lambda^{180}$	53055918281215512995956977848
$\zeta + \lambda^{181}$	73214485258330280479973912031
$\zeta + \lambda^{182}$	48652353886798566644595255794
$\zeta + \lambda^{183}$	51545977506340845920252296109
$\zeta + \lambda^{184}$	65306366887412850231462791436
$\zeta + \lambda^{185}$	77536022373477380043544676207
$\zeta + \lambda^{186}$	11070226367321982292028491344
$\zeta + \lambda^{187}$	66442894643482274238910382 73
$\zeta + \lambda^{188}$	23119982482729165770995406907
$\zeta + \lambda^{189}$	27661868189986431004226496778
$\zeta + \lambda^{190}$	35147526635142226592869398871
$\zeta + \lambda^{191}$	63847966888383655248944826632
$\zeta + \lambda^{192}$	60085599479128183147908509282

Table C.6: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$ (continued)

$\zeta + \lambda^{193}$	125129631227715779135883848 74
$\zeta + \lambda^{194}$	424301015339097821010645734 45
$\zeta + \lambda^{195}$	21010974084823022190139596 22
$\zeta + \lambda^{196}$	263208357033034481587322162 71
$\zeta + \lambda^{197}$	523353323816497926705059764 89
$\zeta + \lambda^{198}$	356712537611392786901773064 62
$\zeta + \lambda^{199}$	669598090202653179685720011 79
$\zeta + \lambda^{200}$	178228651612453184421812262 14
$\zeta + \lambda^{201}$	250537591284363409608755144 88
$\zeta + \lambda^{202}$	497833131568794158867068485 31
$\zeta + \lambda^{203}$	600138002701523129692610527 38
$\zeta + \lambda^{204}$	438476944939956962054105710 69
$\zeta + \lambda^{205}$	269949986167433227504769562 55
$\zeta + \lambda^{206}$	649319833268319075071489158 00
$\zeta + \lambda^{207}$	107874982785832066535749523 26
$\zeta + \lambda^{208}$	240497892394069910103558863 39
$\zeta + \lambda^{209}$	149316192804488054896048164 91
$\zeta + \lambda^{210}$	263033402718637582302069435 03
$\zeta + \lambda^{211}$	672998917353558361075177330 49
$\zeta + \lambda^{212}$	548041823646251157913842573 97
$\zeta + \lambda^{213}$	672056969138489724659192199 27
$\zeta + \lambda^{214}$	679516885714434392907599650 1
$\zeta + \lambda^{215}$	238301995660978308003039132 92
$\zeta + \lambda^{216}$	48152411340096926800927697 9
$\zeta + \lambda^{217}$	754648208847026830017731923 96
$\zeta + \lambda^{218}$	287301515423709163864581114 99
$\zeta + \lambda^{219}$	276780502972893090662543496 66
$\zeta + \lambda^{220}$	301490658736911084559702460 57
$\zeta + \lambda^{221}$	169589240088880419904842451 15
$\zeta + \lambda^{222}$	323610240727192589095706313 2
$\zeta + \lambda^{223}$	551746263939168093554477110 70
$\zeta + \lambda^{224}$	519612498140876328952412231 61

Table C.7: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$ (continued)

$\zeta + \lambda^{225}$	27419536717726951512925494753
$\zeta + \lambda^{226}$	43030034360240559345761960800
$\zeta + \lambda^{227}$	61608484891663412191407951286
$\zeta + \lambda^{228}$	51904222583728267581386869173
$\zeta + \lambda^{229}$	61156394747942852792210073448
$\zeta + \lambda^{230}$	28050394126071653871745143560
$\zeta + \lambda^{231}$	26663450942729852272874457543
$\zeta + \lambda^{232}$	67146953452324811886177106807
$\zeta + \lambda^{233}$	34617250485135966693590919545
$\zeta + \lambda^{234}$	68012893985383124432526071805
$\zeta + \lambda^{235}$	13111923774673046120000508735
$\zeta + \lambda^{236}$	18945241548530441951637018673
$\zeta + \lambda^{237}$	20832362322157966046021902755
$\zeta + \lambda^{238}$	38060105557851257663836313220
$\zeta + \lambda^{239}$	11020021046745233252368558399
$\zeta + \lambda^{240}$	41139993509923108868646860133
$\zeta + \lambda^{241}$	31111091371356149908269721282
$\zeta + \lambda^{242}$	71007746760749096783679520789
$\zeta + \lambda^{243}$	28867509349869515719580559645
$\zeta + \lambda^{244}$	57962624436187445128900557477
$\zeta + \lambda^{245}$	23364030560932846491908450395
$\zeta + \lambda^{246}$	33578001724187610824751722600
$\zeta + \lambda^{247}$	21851351944000328535515497397
$\zeta + \lambda^{248}$	10064820131698521099626242 26
$\zeta + \lambda^{249}$	69350035722045762069996350548
$\zeta + \lambda^{250}$	26672118556411224622331956213
$\zeta + \lambda^{251}$	76944331067097277203580421182
$\zeta + \lambda^{252}$	29753379441962528968367252 64
$\zeta + \lambda^{253}$	15139634842369290031879987383
$\zeta + \lambda^{254}$	19312232545952708515703701658
$\zeta + \lambda^{255}$	71604902619266588004240863616

Table C.8: Discrete logarithms of elements in the factor base in $\mathbf{F}_{16^{24}}$ (continued)

Appendix D

Table of $h_0(x)$ and $h_1(x)$

Let $q = 2^{10}, \mathbf{F}_{q^2}^* = \langle \lambda \rangle$, and consider extensions of $\mathbf{F}_{q^{2k}}$ such that the extension degree is prime and $512 < k < 1024$. We want to compute $h_0(x)$ and $h_1(x)$ over $\mathbf{F}_{q^2}[x]$ such that they satisfy the following properties:

- $\deg(h_0) \leq 2, \deg(h_1) \leq 1$;
- $k_i > 1$ for all $1 \leq i \leq l$; In other words, it is free of linear factors;
- $\gcd(k, k_i) = 1$ for all $1 \leq i \leq l$.

Extension Degree	h0	h1
521	$x^2 + \lambda^{333}$	$x + \lambda$
523	$x^2 + \lambda^{768}$	$x + \lambda$
541	$x^2 + \lambda^{2838}$	$x + \lambda$
547	$x^2 + \lambda^{1616}$	$x + \lambda$
557	$x^2 + \lambda^{2978}$	$x + \lambda$
563	$x^2 + \lambda^{399}$	$x + \lambda$
569	$x^2 + \lambda^{1266}$	$x + \lambda$
571	$x^2 + \lambda^{527}$	$x + \lambda$
577	$x^2 + \lambda^{437}$	$x + \lambda$
587	$x^2 + \lambda^{284}$	$x + \lambda$
593	$x^2 + \lambda^{843}$	$x + \lambda$
599	$x^2 + \lambda^{1244}$	$x + \lambda$
601	$x^2 + \lambda^{2216}$	$x + \lambda$
607	$\lambda^7 * x^2 + \lambda^{17} * x + \lambda^{406}$	x
613	$x^2 + \lambda^{296}$	$x + \lambda$
617	$x^2 + \lambda^{1714}$	$x + \lambda$
619	$x^2 + \lambda^{5864}$	$x + \lambda$
631	$x^2 + \lambda^{682}$	$x + \lambda$
641	$x^2 + \lambda^{4014}$	$x + \lambda$
643	$x^2 + \lambda^{2592}$	$x + \lambda$
647	$x^2 + \lambda^{600}$	$x + \lambda$
653	$x^2 + \lambda^{397}$	$x + \lambda$
659	$x^2 + \lambda^{717}$	$x + \lambda$
661	$x^2 + \lambda^{5081}$	$x + \lambda$
673	$x^2 + \lambda^{280}$	$x + \lambda$
677	$x^2 + \lambda^{1797}$	$x + \lambda$
683	$x^2 + \lambda^{302}$	$x + \lambda$
691	$x^2 + \lambda^{3802}$	$x + \lambda$
701	$x^2 + \lambda^{1934}$	$x + \lambda$
709	$x^2 + \lambda^{3655}$	$x + \lambda$
719	$x^2 + \lambda^{2543}$	$x + \lambda$
727	$x^2 + \lambda^{3964}$	$x + \lambda$
733	$x^2 + \lambda^{4427}$	$x + \lambda$
739	$x^2 + \lambda^{4661}$	$x + \lambda$
743	$x^2 + \lambda^{500}$	$x + \lambda$
751	$x^2 + \lambda^{1405}$	$x + \lambda$
757	$x^2 + \lambda^{1317}$	$x + \lambda + 1$

Table D.1: Representation of $\mathbf{F}_{q^{2k}}$ for $q = 2^{10}$ and prime extension degree

Extension Degree	h0	h1
761	$x^2 + \lambda^{3000}$	$x + \lambda$
769	$x^2 + \lambda^{1645}$	$x + \lambda$
773	$x^2 + \lambda^{1882}$	$x + \lambda$
787	$x^2 + \lambda^{3996}$	$x + \lambda$
797	$x^2 + \lambda^{2572}$	$x + \lambda$
809	$x^2 + \lambda^{551}$	$x + \lambda$
811	$x^2 + \lambda^{101}$	$x + \lambda$
821	$x^2 + \lambda^{1941}$	$x + \lambda$
823	$x^2 + \lambda^{1220}$	$x + \lambda + 1$
827	$x^2 + \lambda^{1607}$	$x + \lambda$
829	$x^2 + \lambda^{2918}$	$x + \lambda$
839	$x^2 + \lambda^{454}$	$x + \lambda$
853	$x^2 + \lambda^{1386}$	$x + \lambda$
857	$x^2 + \lambda^{1493}$	$x + \lambda$
859	$x^2 + \lambda^{404}$	$x + \lambda$
863	$x^2 + \lambda^{1063}$	$x + \lambda$
877	$x^2 + \lambda^{1898}$	$x + \lambda$
881	$x^2 + \lambda^{383}$	$x + \lambda$
883	$x^2 + \lambda^{1824}$	$x + \lambda$
887	$x^2 + \lambda^{4621}$	$x + \lambda$
907	$x^2 + \lambda^{40}$	$x + \lambda$
911	$x^2 + \lambda^{1784}$	$x + \lambda$
919	$x^2 + \lambda^{4419}$	$x + \lambda$
929	$x^2 + \lambda^{1119}$	$x + \lambda$
937	$x^2 + \lambda^{2433}$	$x + \lambda$
941	$x^2 + \lambda^{132}$	$x + \lambda$
947	$x^2 + \lambda^{1078}$	$x + \lambda$
953	$x^2 + \lambda^{1032}$	$x + \lambda$
967	$x^2 + \lambda^{1509}$	$x + \lambda$
971	$x^2 + \lambda^{1712}$	$x + \lambda$
977	$x^2 + \lambda^{2460}$	$x + \lambda$
983	$x^2 + \lambda^{2864}$	$x + \lambda$
991	$x^2 + \lambda^{1310}$	$x + \lambda + 1$
997	$x^2 + \lambda^{1421}$	$x + \lambda$
1009	$x^2 + \lambda^{3152}$	$x + \lambda$
1013	$x^2 + \lambda^{738}$	$x + \lambda$
1019	$x^2 + \lambda^{4900}$	$x + \lambda$
1021	$x^2 + x + \lambda^{306}$	$x + \lambda$

Table D.2: Representation of $\mathbf{F}_{q^{2k}}$ for $q = 2^{10}$ and prime extension degree (continued)