1997

Combinatorial designs, sequences and cryptography

Marc Michel Gysin
University of Wollongong

UNIVERSITY OF WOLLONGONG

Combinatorial Designs, Sequences and Cryptography

A thesis submitted in fulfillment of the
requirements for the award of the degree

Doctor of Philosophy

from

UNIVERSITY OF WOLLONGONG

by

Marc Michel Gysin, MSc (Hons), University of Wollongong

School of Information Technology and Computer Science
October 1997

Dedicated to
My parents Christine and Balthasar

Declaration

I hereby declare that this submission is my own work and that to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of a university or other institute of higher learning, except where due acknowledgement is made in the text.

The word "we" is used stylistically in order to give the reader a sense of familiarity and involvement, and does not imply that the results are joint work with others.

Marc Michel Gysin
July 17, 1997

Acknowledgments

I am pleased to acknowledge the assistance of a variety of parties. I especially would like to thank my supervisor, Professor Jennifer Seberry, whose inspirations and academic support contributed a lot towards this thesis. My thanks go also to everybody in the Centre for Computer Security Research for their friendship and moral support. Finally, I would like to acknowledge everybody whose involvement made it possible to run many combinatorial searches on a variety of machines.

Abstract

A major part of this thesis is about sequences with low, zero or constant autocorrelation function and their implications to combinatorial designs and cryptography. We discuss sequences with zero (periodic or nonperiodic) autocorrelation function and we show an array of constructions, also called multiplications, that give many new infinite families of such sequences. We introduce cyclotomy and show how such sequences together with a search through incidence matrices of cyclotomic or generalised cosets can be used to find a variety of new combinatorial designs. These designs include new weighing matrices, orthogonal designs and D–optimal designs.

In particular we give:

- T–matrices of order n for
$$n = 13, 19, 31, 37, 41, 42, 43, 61, 66, 86, 87.$$
- Weighing matrices $W(4n, 4n-2)$ and $W(4n, 2n-1)$ for
$$n = 25, 31, 37, 41, 61, 71, 73, 157.$$
- D–optimal designs of order
$$v = \frac{n}{2} = 31, 33, 37, 41, 43, 61, 73, 85, 91, 93, 113, 145, 157, 181.$$

We review some of the Stanton–Sprott–Whiteman constructions for difference sets and show how they can be applied to construct supplementary difference sets. We also give many other infinite families of supplementary difference sets and pairwise balanced designs with $\lambda = 1$.

The thesis concludes with some discussions about low autocorrelation in cryptography and a presentation of a small one–key cryptosystem.

Preface

Why study sequences with special autocorrelation function? It turns out that there is a strong connection in between such sequences and various combinatorial designs. This is shown in Chapter 1. In this chapter we also define a variety of combinatorial designs and study further connections between them. One interesting class of such designs are supplementary difference sets (SDS). They are strongly related to D–optimal designs. D–optimal designs have their applications in statistics. Another class are Hadamard matrices which have entries ± 1 and their rows and columns are mutually orthogonal. Necessary conditions on the order n for a Hadamard matrix are that $n = 1, 2$ or $n \equiv 0 \bmod 4$. It is conjectured that these conditions are also sufficient. Weighing matrices and orthogonal designs are generalisations of Hadamard matrices and we will study those throughout this thesis. Chapter 1 contains mainly preliminaries and none of the theorems or definitions presented there are new.

In Chapter 2 we examine a variety of concatenations of such sequences. These concatenations are also called “multiplications”. We examine multiplications which preserve certain properties about the autocorrelation function. In Section 2.2 we give important “ad–hoc” constructions which lead to new sequences, also called ternary complementary pairs (TCP's). Section 2.3 examines more multiplications. Most of these multiplications are obtained via computer–searches. Many of these multiplications can be applied recursively. From these results we obtain new weighing matrices and new orthogonal designs. Finally, in Section 2.4, we present a powerful construction via so called 4–NPAF sequences. We obtain 4–NPAF sequences on the computer and from these we construct new orthogonal designs and new weighing matrices. There are many joint papers arising from this chapter ([GysSeb96], [1GysSeb97], [2GysSeb97]). Section 2.2 is joint work with my supervisor. Theorem 4 is mainly but not only due to my supervisor as well as Lemma 6. The reverse can be said about Lemma 8. The rest of this section is joint work. Section 2.3 is mostly my work except for Lemmas 9, 10 and

Corollary 5 which are due to my supervisor and myself. The main idea in Section 2.4 is due to my supervisor. In particular, Definition 12 and Lemma 15 are my supervisor's idea. My contributions are the computer-searches and many of the corollaries, tables and other lemmas. My overall contribution to Section 2.4 is worth about 50%.

Chapter 3 introduces cyclotomy, cyclotomic cosets and their connection with SDS. The cyclotomic cosets can be looked at as a partition of the numbers 1 to $q - 1$, where $q = p^{\alpha}$ is a prime power. The information given in such partitions very often helps us to find sequences with special autocorrelation function and/or combinatorial designs, for orders n, which without these techniques would be hard to find. Since cyclotomy and the cyclotomic cosets are only defined for prime powers n, we are motivated to find similar partitions for any number n. We call this generalised cyclotomy and this is shown in Section 3.3. From cyclotomy and generalised cyclotomy we obtain a lot of new sequences, new weighing matrices and new orthogonal designs for comparatively high orders n. As indicated, these orders n are not necessarily prime powers. Since cyclotomy is intimately related with SDS, we examine how we can get more SDS from generalised cyclotomy. This is shown in Section 3.6. In this section we give further constructions of SDS. In particular, we also examine the Stanton-Sprott-Whiteman constructions for difference sets (DS) and give similar constructions for SDS. Many papers contributed to Chapter 3. These were [GysSeb95], [Gysin97], [3GysSeb97] and [4GysSeb97]. Many of the results in Section 3.3 are consequences of extensive computer-searches. These searches are based on an idea given in [GerSeb79] and [HunWal72]. Many of the computational results and the numerical consequences are new and they are given in Lemmas 21, 22 and 23 and Tables 3.1 to 3.9. These computer-searches have been carried out by myself. Section 3.6 is mainly my own work. Most of the theorems, lemmas and corollaries presented there are new. However, the results in Section 3.6.1 are covered by a paper given by S. Furino, [Furino91].

Finally, in Chapter 4, we give another answer to the question *Why study sequences with special autocorrelation function?* Here we reveal more about the connections between such sequences and pseudo-random sequences. Pseudo-random sequences are of greatest importance in cryptography. In the following sections we present a one-key cryptosystem where the key defines the encryption-mechanism in some way. The encryption algorithm itself is still public. The encryption-mechanism is based on a finite linear automaton and this automaton depends directly on the secret key. We study the relevant properties of this cryptosystem. The work presented in this chapter is from on a paper *A one-key cryptosystem based on a finite nonlinear automaton*, [Gysin95], and it is entirely my own work.

Publications Arising from this Thesis

[**GysSeb95**] M. Gysin and J. Seberry, On the weighing matrices of order $4n$ and weight $4n-2$ and $2n-1$, *Australasian Journal of Combinatorics*, 12, 157–174, 1995.

[**Gysin95**] M. Gysin, A one–key cryptosystem based on a finite nonlinear automaton, *Cryptography Policy and Algorithms Conference, Brisbane, Australia, 1995*, Springer Verlag, LNCS 1029, Berlin Heidelberg 1996.

[**GysSeb96**] M. Gysin and J. Seberry, Multiplications of ternary complementary pairs, *Australasian Journal of Combinatorics*, 14, 165–180, 1996.

[**Gysin97**] M. Gysin, New D–optimal designs via cyclotomy and generalised cyclotomy, *Australasian Journal of Combinatorics*, 15, 247–255, 1997.

[**1GysSeb97**] M. Gysin and J. Seberry, On 4–NPAF$(1, 2w)$ sequences, accepted for publication in *Bulletin of the Institute of Combinatorics and its Applications.*

[**2GysSeb97**] M. Gysin and J. Seberry, On ternary complementary pairs, *IEEE Transactions on Information Theory*, submitted.

[**3GysSeb97**] M. Gysin and J. Seberry, An experimental search and new combinatorial designs via a generalisation of cyclotomy, accepted for publication in *Journal of Combinatorial Mathematics and Combinatorial Computing.*

[**4GysSeb97**] M. Gysin and J. Seberry, On supplementary difference sets over rings with short orbits, *Finite Fields and Their Applications*, submitted.

A brief word about the papers, their contributions to this thesis, and my own contribution to the joint papers (the numbers of the theorems, definitions etc. refer to this thesis and *not* to the papers):

[GysSeb95] The main contribution of this paper is towards Section 3.5.1. Lemmas 21 and 22, Tables 3.1 and 3.2 are the main results. My personal contribution to this paper was the computer–search for the T– and JM–matrices. Similar searches have been used in [HunWal72] and others. I estimate my overall contribution to be worth about 20%.

[Gysin95] This paper is entirely my own work. The contribution here is a small one–key cryptosystem which is given in Section 4.2.

[GysSeb96] This paper is is given in Section 2.3. I believe that most of this paper is my own work. However, my supervisor's contribution has been towards Lemmas 9, 10 and Corollary 5. I would rate my contribution to be around 80%.

[Gysin97] This paper contributed about 90% towards Section 3.5.2. This paper is entirely my own work. However, the computer–search is, as the search of [GysSeb95], based on ideas given in [GerSeb79], [HunWal72] and others.

[1GysSeb97] This paper is given in Section 2.4. Definition 12 and Lemma 15 are due to my supervisor. My contributions are the computer–searches and many of the corollaries, tables and other lemmas. In short, I would say the main idea is my supervisor's, the implementation of the idea and pursuing it further are mine. I believe either contribution is around 50%.

[2GysSeb97] This paper is a 50% – 50% joint paper. It is given in Section 2.2. Many of the results presented there are due to this paper. However, some of the results and ideas stem from [GavLem94], so for example, Definition 10 and parts of Lemma 7. This paper is mostly a result of mutual inspirations. In other words, it is impossible to state who contributed exactly what to this paper. However, I believe the following statements are fair. Theorem 4 is mainly but not only due to my supervisor as well as Lemma 6. The reverse can be said about Lemma 8. The rest is joint work.

[3GysSeb97] This paper is mostly my work. The contribution of this paper to the thesis are towards Sections 3.3 and 3.4, some more D–optimal designs (Table 3.7) and the case 87 for JM–matrices (Table 3.2). The computer–search is again, as the searches in [GysSeb95] and [Gysin97], based on ideas given in [GerSeb79], [HunWal72] and others. I would rate my contribution to be around 80%.

[4GysSeb97] This paper is given in Section 3.6. Many of the theorems, lemmas and corollaries presented there are new. However, the results in Section 3.6.1 are covered by a paper given by S. Furino, [Furino91]. As for [3GysSeb97], I would rate my contribution to be worth around 80%.

Theorems, lemmas and corollaries which are in sections other than the ones arising from the above papers are not new. This is sometimes not mentioned explicitly, since the original references were hard to find.

Contents

Acknowledgments iv

Abstract v

Preface vi

Publications Arising from this Thesis ix

1 Combinatorial Designs and Sequences 1

1.1 Sequences with Zero Autocorrelation Function 1

1.2 Combinatorial Designs 5

1.2.1 Balanced Incomplete Block Designs 5

1.2.2 Weighing Matrices, Hadamard Matrices and Orthogonal Designs 7

1.2.3 Supplementary Difference Sets 9

1.2.4 D-Optimal Designs 11

1.3 Searching for Sequences and Combinatorial Designs 13

1.3.1 Exhaustive Search Algorithms 13

1.3.2 Heuristic Search Algorithms 14

2 Multiplications and Ternary Complementary Pairs **18**

2.1 Standard Multiplications and Constructions 18

2.2 More on Ternary Complementary Pairs 21

2.2.1 Some Extended Standard Constructions 22

2.2.2 Ternary Complementary Pairs with a Minimum Number of Zeros 25

2.3 Multiplications of Sequences via Computer 29

2.3.1 Multiplications "by Hand" 29

2.3.2 Multiplications via Computer 33

2.3.3 Results and Numerical Consequences 37

2.3.4 Some New Families of Weighing Matrices 41

2.4 Sequences of Type A, B, C, C and Orthogonal Designs 44
2.4.1 Existence of Sequences of Type A, B, C, C 45
2.4.2 Some New Families of Orthogonal Designs 48

3 Cyclotomy and Generalised Cyclotomy 50
3.1 Cyclotomy and Supplementary Difference Sets 50
3.2 Cyclotomy and the Incidence Matrices 55
3.3 The Generalisation 58
3.4 The Experimental Search 60
3.5 Results and Numerical Consequences 60
3.5.1 Weighing Matrices and Orthogonal Designs 61
3.5.2 D-Optimal Designs 68
3.6 More Supplementary Difference Sets 71
3.6.1 Supplementary Difference Sets over Galois Domains 71
3.6.2 A More General Construction 76
3.6.3 Supplementary Difference Sets with Short Orbits 80
3.6.4 Twin Prime Power Constructions 83
3.6.5 Balanced Incomplete Block Designs and Pairwise Balanced Designs 87

4 Sequences and Cryptography 90
4.1 Pseudo-Random Sequences 90
4.2 A One-Key Cryptosystem Based on a Nonlinear Finite Automaton . . 91
4.2.1 Introduction 91
4.2.2 Mealy Machines and Extended Mealy Machines 92
4.2.3 An Example 94
4.2.4 The Real Implementation 96
4.2.5 Security and Statistics 97

Bibliography 101

A Partitions for the Composite Cases 107
A.1 T-Matrices 107
A.1.1 The Case $t = 42 = 2 \times 3 \times 7$, $y = 11 = (1, 2, 4)$ 107
A.1.2 The Case $t = 66 = 2 \times 3 \times 11$, $y = 5 = (1, 2, 5)$ 108
A.1.3 The Case $t = 86 = 2 \times 43$, $y = 11 = (1, 11)$ 108
A.1.4 The Case $t = 87 = 3 \times 29$, $y = 7 = (1, 7)$ 109
A.2 JM-Matrices 110

A.2.1 The Case $n = 33 = 3 \times 11$, $y = 4 = (1,4)$ 110

A.2.2 The Case $n = 35 = 5 \times 7$, $y = 4 = (4,4)$ 110

A.2.3 The Case $n = 39 = 3 \times 13$, $y = 4 = (1,4)$ 111

A.2.4 The Case $n = 55 = 5 \times 11$, $y = 4 = (4,4)$ 111

A.2.5 The Case $n = 66 = 2 \times 3 \times 11$, $y = 5 = (1,2,5)$ 112

A.2.6 The Case $n = 77 = 7 \times 11$, $y = 4 = (4,4)$ 112

A.3 D–Optimal Designs 113

A.3.1 The Case $v = 33 = 3 \times 11$, $y = 5 = (2,5)$ 113

A.3.2 The Case $v = 85 = 5 \times 17$, $y = 9 = (4,9)$ 113

A.3.3 The Case $v = 91 = 7 \times 13$, $y = 68 = (5,3)$ 114

A.3.4 The Case $v = 93 = 3 \times 31$, $y = 4 = (1,4)$ 115

A.3.5 The Case $v = 145 = 5 \times 29$, $y = 24 = (4,24)$ 116

List of Tables

2.1 TCP's up to length $n = 20$. 30

2.2 Multiplications of TCP's. 39

2.3 Sequences of type A,B,C,C. 46

2.4 From TCP's to sequences of type A, B, C, C. 47

2.5 Some other sequences of type A, B, C, C. 48

2.6 An orthogonal design $OD(4p; 1, 2w)$ exists. 49

3.1 T–matrices found via cyclotomy and generalised cyclotomy. 64

3.2 JM–matrices found via cyclotomy and generalised cyclotomy. 65

3.3 The first rows of particular T–matrices. 66

3.4 The first rows of particular JM–matrices. 67

3.5 The initial sets C_1 for constructing T–matrices. 68

3.6 The initial sets C_1 for constructing JM–matrices. 68

3.7 D–optimal designs found via cyclotomy and generalised cyclotomy. . . 69

3.8 The first rows of particular D–optimal designs. 70

3.9 The initial sets C_1 for constructing D–optimal designs. 70

3.10 Some PBD with $\lambda = 1$. 89

4.1 The automaton for the key $k = A0B3FF293C49B061_{hex}$. 95

4.2 One round of encryption. 95

4.3 Statistical tests in CBC mode. 99