Contents

Abstract ii

Acknowledgments v

Notation viii

Chapter 1. Introduction 1
1.1. Algebraic curves 1
1.2. Precedent applications of algebraic curves 6
1.2.1. Algebraic-geometric codes 6
1.2.2. Elliptic curve cryptography 7
1.2.3. Factorization of large numbers 9
1.2.4. Sequences for stream ciphers 11
1.3. A new application to balanced arrays 12
1.4. A new application to balanced n-ary designs 14
1.5. Practical usages of balanced n-ary designs and balanced arrays 16
1.5.1. Block designs 16
1.5.2. Balanced fractional factorial designs 17
1.5.3. Weighing designs 19

Chapter 2. Algebraic Curves 21
2.1. Projective curves and affine curves 21
2.2. Curves over finite fields 24
2.3. Rational functions 25
2.4. Divisors 28
2.5. Vector space $L(D)$ 30

2.6. Riemann-Roch Theorem 31

Chapter 3. Balanced Arrays 33

3.1. Introduction 33

3.2. Symmetric sets of curves 35

3.3. A construction on an elliptic curve 39

Chapter 4. Balanced n-ary Designs 43

4.1. Introduction 43

4.2. Algebraic curves and balanced n-ary designs 47

Chapter 5. Concluding Remarks 53

Bibliography 55