Contents

List of Figures i

Acknowledgments iii

Abstract v

Resumé vii

List of Publications ix

1 Introduction 1
- 1.1 Cryptography muddled with quantum results 2
  - 1.1.1 Overview of the field 2
  - 1.1.2 Secure Two-Party Computation 3
- 1.2 Coin Flipping 7
  - 1.2.1 Problem Statement 7
  - 1.2.2 Impossibility of Classical Coin Flipping and Quantum Strong Coin Flipping 8
  - 1.2.3 Quantum Weak Coin Flipping 10
- 1.3 Contributions (informal) 13
  - 1.3.1 TDPG-to-Explicit-protocol Framework (TEF) and bias 1/10 | First Contribution 14
  - 1.3.2 Exact Unitaries for Mochon's assignments | Second Contribution 17
  - 1.3.3 Elliptic Monotone Align (EMA) Algorithm | Third Contribution 18
  - 1.3.4 Exact Unitaries for Mochon's assignments, a geometric approach | Fourth Contribution 21
- 1.4 Navigating the thesis 22

I Prior Art 23

2 Existence of (almost perfect) Quantum Weak Coin Flipping Protocols 25
- 2.1 WCF protocol as an SDP and its Dual 27
- 2.2 (Time Dependent) Point Games with EBM transitions/functions 31
- 2.3 (Time Dependent) Point Games with Valid functions 33
  - 2.3.1 Examples of valid line transitions 34
  - 2.3.2 Example of (Time Dependent) Point Games 35
- 2.4 Time Independent Point Games (TIPGs) 37
  - 2.4.1 A note on Visualising TDPG and TIPGs 38
- 2.5 Mochon's TIPG achieving bias $\epsilon = 1/(4k+2)$ 39
  - 2.5.1 The Ladder 40
  - 2.5.2 The Split (and The Raise) 45

3 Connection with Conic Duality 47
- 3.1 (Time Dependent) Point Games with valid transitions 47
  - 3.1.1 Formalising the equivalence between transitions and functions 47
  - 3.1.2 Operator monotone functions and valid functions 49
  - 3.1.3 Strictly valid functions are EBM functions 54
  - 3.1.4 From point games with valid functions to point games with EBM functions 56

II Primary Contributions 57

4 TDPG-to-Explicit-protocol Framework (TEF) and bias 1/10 59
4.1 Motivation and Conventions . . . 59
4.2 The Framework . . . 61
4.2.1 Important Special Case: The Blinkered Unitary . . . 64
4.3 Games and Protocols . . . 66
4.3.1 Mochon's Approach . . . 66
4.3.2 Bias $1/6$ . . . 68
4.3.3 Bias $1/10$ Game . . . 70
4.3.4 Bias $1/10$ Protocol . . . 71

5 Approaching bias $1/(4k+2)$ 79
5.1 Mochon's Assignments . . . 79
5.2 Equivalence to Monomial Assignments . . . 80
5.2.1 The origin can be shifted . . . 81
5.3 f_0 Unitary | Solution to Mochon's f-assignment . . . 82
5.3.1 The Balanced Case . . . 82
5.3.2 The Unbalanced Case . . . 85
5.4 m Unitary | Solution to Mochon's m-assignments . . . 87
5.4.1 The Balanced Case . . . 88
5.4.2 The Unbalanced Case . . . 94
5.5 Main Result . . . 97
5.5.1 Example: A bias $1/14$ protocol . . . 97

III Secondary Contributions 101

6 Elliptic Monotone Align (EMA) Algorithm 103
6.1 Canonical Forms Revisited . . . 103
6.1.1 The Canonical Projective Form (CPF) and the Canonical Orthogonal Form (COF) 103
6.1.2 From EBM to EBRM to COF . . . 105
6.2 Ellipsoids . . . 109
6.2.1 The inequality as containment of ellipsoids . . . 109
6.2.2 Convex Geometry Tools | Weingarten Map and the Support Function . . . 110
6.3 Elliptic Monotone Align (EMA) Algorithm . . . 110
6.3.1 Notation . . . 111
6.3.2 Lemmas for EMA . . . 114
6.3.3 The Algorithm . . . 122
6.4 Conclusion . . . 148

7 Approaching bias $1/(4k+2)$ | a geometric approach 153
7.1 Ellipsoid Picture . . . 153
7.1.1 Exact Formulae . . . 154
7.2 f_0 Unitary | Solution to the f_0-assignment . . . 156
7.2.1 The Balanced Case . . . 158
7.3 Extended Matrix Instances . . . 161
7.4 Weingarten Iteration | Isometric Iteration using the Weingarten Map . . . 163
7.4.1 The Finite Case . . . 163
7.4.2 The Divergent Case . . . 164
7.5 f_0 Unitary (cont.) . . . 168
7.5.1 The Unbalanced Case . . . 168

7.6 m Unitary | Solution to Mochon's Monomial Assignments 169
7.6.1 Simplest Monomial Problem 169
7.6.2 Balanced Monomial Problem 170
7.6.3 Unbalanced Monomial Problem 174

8 Conclusion and Outlook 179

IV Appendix 183

A Existence of almost perfect weak coin flipping 185
A.1 WCF protocol as an SDP and its Dual 185
A.2 (Time Dependent) Point Games with EBM transitions/functions 188
A.3 Time Independent Point Games (TIPGs) 189
A.4 Mochon's TIPG achieving bias $\epsilon = 1/(4k+2)$ 193

B TEF, Approaching $1/10$ and EMA 199
B.1 TEF functions = Valid functions = closure of EBM functions 199
B.2 Blink $m \to n$ Transition 200
B.3 Mochon's Assignments 204

C Approaching $1/(4k+2)$ 207
C.1 Restricted decomposition into f_0-assignments 207

D Approaching $1/(4k+2)$ | Geometric Approach 211
D.1 Known Results 211
D.2 Normals and the Weingarten Map (Curvature) 212
D.3 The $-1/x$ trick and monomial assignments 214
D.4 Existence of Solutions to Matrix Instances and their dimensions 215
D.5 Lemmas for the Contact and Component conditions 217

Bibliography 223