Cryptography in a quantum world
Wehner, S.D.C.

Citation for published version (APA):

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: http://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE (Digital Academic Repository)

UvA-DARE is a service provided by the library of the University of Amsterdam (http://dare.uva.nl)

Download date: 03 Jan 2019
## Contents

### Acknowledgments

xv

## I  Introduction

1 Quantum cryptography 3

1.1 Introduction 3

1.2 Setting the state 5

1.2.1 Terminology 5

1.2.2 Assumptions 6

1.2.3 Quantum properties 7

1.3 Primitives 9

1.3.1 Bit commitment 9

1.3.2 Secure function evaluation 11

1.3.3 Secret sharing 17

1.3.4 Anonymous transmissions 18

1.3.5 Other protocols 19

1.4 Challenges 19

1.5 Conclusion 20

## II  Information in quantum states

2 Introduction 25

2.1 Quantum mechanics 25

2.1.1 Quantum states 25

2.1.2 Multipartite systems 27

2.1.3 Quantum operations 29

2.2 Distinguishability 32
3 State discrimination with post-measurement information

3.1 Introduction ............................................. 43
  3.1.1 Outline ........................................ 45
  3.1.2 Related work .................................... 46

3.2 Preliminaries ........................................... 47
  3.2.1 Notation and tools .............................. 47
  3.2.2 Definitions .................................... 47
  3.2.3 A trivial bound: guessing the basis ............. 48

3.3 No post-measurement information .................... 49
  3.3.1 Two simple examples ............................ 49
  3.3.2 An upper bound for all Boolean functions .......... 50
  3.3.3 AND function .................................. 50
  3.3.4 XOR function .................................. 51

3.4 Using post-measurement information ................. 54
  3.4.1 A lower bound for balanced functions ............. 54
  3.4.2 Optimal bounds for the AND and XOR function ..... 57

3.5 Using post-measurement information and quantum memory .... 63
  3.5.1 An algebraic framework for perfect prediction .... 63
  3.5.2 Using two bases ................................. 66
  3.5.3 Using three bases ............................... 70

3.6 Conclusion ............................................. 72

4 Uncertainty relations ..................................... 75

4.1 Introduction ............................................. 75

4.2 Limitations of mutually unbiased bases ............. 78
  4.2.1 MUBs in square dimensions ...................... 79
  4.2.2 MUBs based on Latin squares .................... 80
  4.2.3 Using a full set of MUBs ....................... 80

4.3 Good uncertainty relations ........................... 83
  4.3.1 Preliminaries .................................. 84
  4.3.2 A meta-uncertainty relation .................... 89
  4.3.3 Entropic uncertainty relations ................. 89

4.4 Conclusion ............................................. 91