

Contents

Introduction	1
1 Preliminaries and Overview	5
1.1 Notation and Conventions	5
1.2 Pseudorandom Generators	6
1.3 Public Key Encryption	7
1.3.1 IND-CPA security	8
1.3.2 Circular Security	9
1.4 Program Obfuscation	10
1.5 Related work and original results	13
1.5.1 Technical Overview	16
2 Separation from Virtual Black-Box Obfuscation	18
2.1 PKE from Obfuscation	18
2.2 Properties of Our Scheme	21
2.3 A PKE that is not n -Circular Secure	22
3 Separation from Indistinguishability Obfuscation	26
3.1 The Technical Details	27
Bibliography	30

<i>CONTENTS</i>	iii
Acknowledgements	34