# Contents

1 Introduction .................................................. 1
   1.1 Tight Reductions ........................................ 4
   1.2 Digital Signatures ....................................... 6
   1.3 Contribution ............................................. 9
      1.3.1 Sufficient Conditions for the Impossibility of Tight Reductions. ......................... 9
      1.3.2 Tightly Secure Signatures in the Standard Model ............................................. 11
      1.3.3 Tightly Secure Signatures in the Random Oracle Model ................................. 12

2 Preliminaries ................................................. 15
   2.1 Notation .................................................... 15
   2.2 Complexity Theoretical Foundations ..................... 16
      2.2.1 Model of Computation ................................ 16
      2.2.2 Complexity Assumptions ............................ 20
   2.3 Cryptographic Foundations ............................... 25
      2.3.1 The Security Parameter and Symmetric Key Size ............................................. 25
      2.3.2 Asymmetric Key Size and Exact Security ..................................................... 27
      2.3.3 Basic Primitives ...................................... 28

3 Sufficient Conditions for the Impossibility of Tight Reductions in Cryptography .......... 33
   3.1 Warm-Up: Improved Bound for Digital Signatures ................................. 36
      3.1.1 Simple reductions from non-interactive complexity assumptions to breaking UF-SMA-security .............................................................. 38
      3.1.2 Lower Tightness Bound for $r$-simple reductions from any NICA to breaking UF-SMA-security .............................................................. 41
## Contents

3.1.3 Interpretation .............................................. 46  
3.2 Sufficient Conditions to Rule out Tight Reductions .... 47  
3.2.1 Definitions ............................................. 48  
3.2.2 Main Theorem to Rule Out Tight Reductions ........ 50  
3.3 Applications ............................................. 55  
3.4 Practical Implications ................................. 59  
3.5 Limitations: How to circumvent the bound ....... 60  

4 Efficient Tightly Secure Signatures in the Standard Model 63  
4.1 Security Notions for Digital Signatures in the Multi-User Setting ............................................. 66  
4.2 Generic Construction in the Standard Model .......... 67  
4.2.1 Description of the Scheme ......................... 68  
4.2.2 Proof of Security ...................................... 69  
4.2.3 Instantiation with Building Blocks from the Literature ...................................................... 72  

5 Practical Tightly Secure Signatures in the Random Oracle Model 75  
5.1 Intuition .................................................... 77  
5.2 Description of the Scheme ............................ 79  
5.3 Proof of Security ......................................... 81  
5.4 Efficiency of our Scheme ............................. 86  

6 Conclusion .................................................. 89  

Bibliography .................................................. 91