Springer

1st edition

Due 2018-08-01
1st ed. 2018, 253 p. 4 illus.

Printed book
Hardcover

Printed book
Hardcover
ISBN 978-3-319-93048-0
Ca. $ 109,00

Planned

Discount group
Professional Books (2)

Product category
Monograph

Computer Science : Data Structures, Cryptology and Information Theory

Guo, F., Susilo, W., Mu, Y., University of Wollongong, Wollongong, NSW, Australia

Introduction to Security Reduction

- **Security proofs are essential to public-key cryptography**
- **Illustrates important notions in security reductions**
- **Suitable for researchers and graduate students engaged with public-key cryptography**

This monograph illustrates important notions in security reductions and essential techniques in security reductions for group-based cryptosystems. Using digital signatures and encryption as examples, the authors explain how to program correct security reductions for those cryptographic primitives. Various schemes are selected and re-proven in this book to demonstrate and exemplify correct security reductions. This book is suitable for researchers and graduate students engaged with public-key cryptography.

Order online at springer.com/booksellers
Springer Customer Service Center LLC
233 Spring Street
New York, NY 10013
USA
T: +1-800-SPRINGER NATURE
(777-4643) or 212-460-1500
customerservice@springernature.com

Prices and other details are subject to change without notice. All errors and omissions excepted. Americas: Tax will be added where applicable. Canadian residents please add PST, QST or GST. Please add $5.00 for shipping one book and $ 1.00 for each additional book. Outside the US and Canada add $ 10.00 for first book, $5.00 for each additional book. If an order cannot be fulfilled within 90 days, payment will be refunded upon request. Prices are payable in US currency or its equivalent.

Preface

Security reduction is a very popular approach for proving security in public-key cryptography. With security reduction, roughly speaking, we can show that breaking a proposed scheme is as difficult as solving a mathematical hard problem. However, how to program a correct security reduction using an adversary's adaptive attack is rather complicated. The reason is that there is no universal security reduction for all proposed schemes.

Security reductions given in cryptographic research papers are often hard for beginners to fully comprehend. To aid the beginners, some cryptography textbooks have illustrated how to correctly program security reductions with simpler examples. However, security reductions mentioned in research papers and previous textbooks are usually for specific schemes. The difference in security reductions for different schemes leads to confusion for the beginners. There is a need for a book that systematically introduces how to correctly program a security reduction for a cryptosystem, not for a specific scheme. With this in mind, we wrote this book, which we hope will help the reader understand how to correctly program a security reduction.

The contents of this book, especially the foundations of security reductions, are based on our understanding and experience. The reader might find that the explanations of concepts are slightly different from those in other sources, because we have added some "condiments" to help the reader understand these concepts. For example, in a security reduction, the adversary is not a black-box adversary but a malicious adversary who has unbounded computational power.

We thought this book would be completed within one year, but we underestimated its difficulty. It has taken more than four years to complete the writing of this book. There must still be errors that have not yet been found. We welcome any comments and suggestions.

University of Wollongong, Australia *Fuchun Guo, Willy Susilo, and Yi Mu*
May 2018

Contents

1 Guide to This Book ... 1

2 Notions, Definitions, and Models ... 5
- 2.1 Digital Signatures ... 5
- 2.2 Public-Key Encryption ... 7
- 2.3 Identity-Based Encryption ... 9
- 2.4 Further Reading ... 11

3 Foundations of Group-Based Cryptography ... 13
- 3.1 Finite Fields ... 13
  - 3.1.1 Definition ... 13
  - 3.1.2 Field Operations ... 14
  - 3.1.3 Field Choices ... 14
  - 3.1.4 Computations over a Prime Field ... 15
- 3.2 Cyclic Groups ... 16
  - 3.2.1 Definitions ... 16
  - 3.2.2 Cyclic Groups of Prime Order ... 17
  - 3.2.3 Group Exponentiations ... 17
  - 3.2.4 Discrete Logarithms ... 18
  - 3.2.5 Cyclic Groups from Finite Fields ... 19
  - 3.2.6 Group Choice 1: Multiplicative Groups ... 19
  - 3.2.7 Group Choice 2: Elliptic Curve Groups ... 20
  - 3.2.8 Computations over a Group ... 22
- 3.3 Bilinear Pairings ... 22
  - 3.3.1 Symmetric Pairing ... 23
  - 3.3.2 Asymmetric Pairing ... 24
  - 3.3.3 Computations over a Pairing Group ... 25
- 3.4 Hash Functions ... 25
- 3.5 Further Reading ... 26

4 Foundations of Security Reduction 29
4.1 Introduction to Basic Concepts 29
4.1.1 Mathematical Primitives and Superstructures 29
4.1.2 Mathematical Problems and Problem Instances 30
4.1.3 Cryptography, Cryptosystems, and Schemes 31
4.1.4 Algorithm Classification 1 31
4.1.5 Polynomial Time and Exponential Time 32
4.1.6 Negligible and Non-negligible 32
4.1.7 Insecure and Secure 33
4.1.8 Easy and Hard 33
4.1.9 Algorithm Classification 2 34
4.1.10 Algorithms in Cryptography 34
4.1.11 Hard Problems in Cryptography 35
4.1.12 Security Levels 35
4.1.13 Hard Problems and Hardness Assumptions 36
4.1.14 Security Reductions and Security Proofs 36
4.2 An Overview of Easy/Hard Problems 37
4.2.1 Computational Easy Problems 37
4.2.2 Computational Hard Problems 42
4.2.3 Decisional Easy Problems 43
4.2.4 Decisional Hard Problems 44
4.2.5 How to Prove New Hard Problems 45
4.2.6 Weak Assumptions and Strong Assumptions 47
4.3 An Overview of Security Reduction 47
4.3.1 Security Models 47
4.3.2 Weak Security Models and Strong Security Models 49
4.3.3 Proof by Testing 49
4.3.4 Proof by Contradiction 50
4.3.5 What Is Security Reduction? 50
4.3.6 Real Scheme and Simulated Scheme 51
4.3.7 Challenger and Simulator 51
4.3.8 Real Attack and Simulation 52
4.3.9 Attacks and Hard Problems 52
4.3.10 Reduction Cost and Reduction Loss 53
4.3.11 Loose Reduction and Tight Reduction 53
4.3.12 Security Level Revisited 54
4.3.13 Ideal Security Reduction 55
4.4 An Overview of Correct Security Reduction 56
4.4.1 What Should Bob Do? 56
4.4.2 Understanding Security Reduction 57
4.4.3 Successful Simulation and Indistinguishable Simulation 57
4.4.4 Failed Attack and Successful Attack 58
4.4.5 Useless Attack and Useful Attack 59
4.4.6 Attack in Simulation 59
4.4.7 Successful/Correct Security Reduction 60

4.4.8 Components of a Security Proof 60
4.5 An Overview of the Adversary 61
4.5.1 Black-Box Adversary 61
4.5.2 What Is an Adaptive Attack? 61
4.5.3 Malicious Adversary 62
4.5.4 The Adversary in a Toy Game 63
4.5.5 Adversary's Successful Attack and Its Probability 63
4.5.6 Adversary's Computational Ability 64
4.5.7 The Adversary's Computational Ability in a Reduction 64
4.5.8 The Adversary in a Reduction 66
4.5.9 What the Adversary Knows 66
4.5.10 What the Adversary Never Knows 67
4.5.11 How to Distinguish the Given Scheme 67
4.5.12 How to Generate a Useless Attack 68
4.5.13 Summary of Adversary 69
4.6 An Overview of Probability and Advantage 69
4.6.1 Definitions of Probability 69
4.6.2 Definitions of Advantage 71
4.6.3 Malicious Adversary Revisited 73
4.6.4 Adaptive Choice Revisited 73
4.6.5 Useless, Useful, Loose, and Tight Revisited 74
4.6.6 Important Probability Formulas 74
4.7 An Overview of Random and Independent 75
4.7.1 What Are Random and Independent? 76
4.7.2 Randomness Simulation with a General Function 76
4.7.3 Randomness Simulation with a Linear System 79
4.7.4 Randomness Simulation with a Polynomial 81
4.7.5 Indistinguishable Simulation and Useful Attack Together 82
4.7.6 Advantage and Probability in Absolutely Hard Problems 83
4.8 An Overview of Random Oracles 83
4.8.1 Security Proof with Random Oracles 84
4.8.2 Hash Functions vs Random Oracles 84
4.8.3 Hash List 85
4.8.4 How to Program Security Reductions with Random Oracles 86
4.8.5 Oracle Response and Its Probability Analysis 86
4.8.6 Summary of Using Random Oracles 88
4.9 Security Proofs for Digital Signatures 89
4.9.1 Proof Structure 89
4.9.2 Advantage Calculation 90
4.9.3 Simulatable and Reducible 91
4.9.4 Simulation of Secret Key 91
4.9.5 Partition 92
4.9.6 Tight Reduction and Loose Reduction Revisited 92
4.9.7 Summary of Correct Security Reduction 93
4.10 Security Proofs for Encryption Under Decisional Assumptions 94

4.10.1 Proof Structure . . . 94
4.10.2 Classification of Ciphertexts . . . 95
4.10.3 Classification of the Challenge Ciphertext . . . 96
4.10.4 Simulation of the Challenge Ciphertext . . . 96
4.10.5 Advantage Calculation 1 . . . 97
4.10.6 Probability P_T of Breaking the True Challenge Ciphertext . . 98
4.10.7 Probability P_F of Breaking the False Challenge Ciphertext . . 98
4.10.8 Advantage Calculation 2 . . . 99
4.10.9 Definition of One-Time Pad . . . 100
4.10.10 Examples of One-Time Pad . . . 101
4.10.11 Analysis of One-Time Pad . . . 103
4.10.12 Simulation of Decryption . . . 103
4.10.13 Simulation of Challenge Decryption Key . . . 104
4.10.14 Probability Analysis for P_F . . . 105
4.10.15 Examples of Advantage Results for A_F^K and A_F^I . . . 106
4.10.16 Advantage Calculation 3 . . . 108
4.10.17 Summary of Correct Security Reduction . . . 109

4.11 Security Proofs for Encryption Under Computational Assumptions . 109
4.11.1 Random and Independent Revisited . . . 109
4.11.2 One-Time Pad Revisited . . . 110
4.11.3 Solution to Hard Problem Revisited . . . 110
4.11.4 Simulation of Challenge Ciphertext . . . 111
4.11.5 Proof Structure . . . 112
4.11.6 Challenge Ciphertext and Challenge Hash Query . . . 113
4.11.7 Advantage Calculation . . . 114
4.11.8 Analysis of No Advantage . . . 115
4.11.9 Requirements of Decryption Simulation . . . 116
4.11.10 An Example of Decryption Simulation . . . 116
4.11.11 Summary of Correct Security Reduction . . . 118

4.12 Simulatable and Reducible with Random Oracles . . . 119
4.12.1 H-Type: Hashing to Group . . . 119
4.12.2 C-Type: Commutative . . . 121
4.12.3 I-Type: Inverse of Group Exponent . . . 122

4.13 Examples of Incorrect Security Reductions . . . 123
4.13.1 Example 1: Distinguishable . . . 124
4.13.2 Example 2: Useless Attack by Public Key . . . 126
4.13.3 Example 3: Useless Attack by Signature . . . 128

4.14 Examples of Correct Security Reductions . . . 130
4.14.1 One-Time Signature with Random Oracles . . . 130
4.14.2 One-Time Signature Without Random Oracles . . . 133
4.14.3 One-Time Signature with Indistinguishable Partition . . . 136

4.15 Summary of Concepts . . . 139
4.15.1 Concepts Related to Proof . . . 139
4.15.2 Preliminaries and Proof by Contradiction . . . 140
4.15.3 Security Reduction and Its Difficulty . . . 141

4.15.4 Simulation and Its Requirements 142
4.15.5 Towards a Correct Security Reduction 144
4.15.6 Other Confusing Concepts 146

5 Digital Signatures with Random Oracles 147
5.1 BLS Scheme 147
5.2 BLS$^+$ Scheme 149
5.3 BLS$^\#$ Scheme 152
5.4 BB^{RO} Scheme 155
5.5 ZSS Scheme 157
5.6 ZSS$^+$ Scheme 160
5.7 ZSS$^\#$ Scheme 162
5.8 BLS^G Scheme 165

6 Digital Signatures Without Random Oracles 173
6.1 Boneh-Boyen Scheme 173
6.2 Gentry Scheme 177
6.3 GMS Scheme 180
6.4 Waters Scheme 185
6.5 Hohenberger-Waters Scheme 189

7 Public-Key Encryption with Random Oracles 193
7.1 Hashed ElGamal Scheme 193
7.2 Twin Hashed ElGamal Scheme 195
7.3 Iterated Hashed ElGamal Scheme 198
7.4 Fujisaki-Okamoto Hashed ElGamal Scheme 202

8 Public-Key Encryption Without Random Oracles 209
8.1 ElGamal Scheme 209
8.2 Cramer-Shoup Scheme 211

9 Identity-Based Encryption with Random Oracles 215
9.1 Boneh-Franklin Scheme 215
9.2 Boneh-Boyen^{RO} Scheme 218
9.3 Park-Lee Scheme 221
9.4 Sakai-Kasahara Scheme 224

10 Identity-Based Encryption Without Random Oracles 229
10.1 Boneh-Boyen Scheme 229
10.2 Boneh-Boyen$^+$ Scheme 233
10.3 Waters Scheme 237
10.4 Gentry Scheme 242

References 249