

Contents

Foreword

ix

A Efficient Distributed Computation Modulo a Shared Secret

Dario Catalano

1

1	Introduction	1
1.1	Previous Work	2
1.2	Organization of this Lecture	3
2	Preliminaries	4
2.1	The Network Model	4
2.2	Definitions and Notations	4
3	Building Blocks	5
3.1	Additive Sharing over \mathbb{Z}_q	6
3.2	Polynomial Sharing over \mathbb{Z}_q	6
3.3	Additive Sharing over \mathbb{Z}	7
3.4	Polynomial Sharing over \mathbb{Z}	8
4	Basic Protocols	9
4.1	Distributed Computation Modulo q	9
4.2	Joint Random Sharing over \mathbb{Z}_q	10
4.3	Joint Random Sharing of 0 in \mathbb{Z}_q	10
4.4	Computing Shares of the Inverse of a Shared Secret	11
4.5	Joint Random Invertible Element Sharing	11
5	A Different Approach	11
6	Converting among Different Secret Sharing Methods	12
6.1	Converting between Additive and Polynomial Shares	12
6.2	Converting between Integer Shares and \mathbb{Z}_q Shares	13
6.3	Computing Shares of the Binary Representation of a Secret	16
6.4	Approximate Truncation	16
7	Distributed Modular Reduction	17
7.1	Newton Iteration Method	17
7.2	First Step: Computing Shares of an Approximation of $1/p$	18

7.3	Second Step: the Modular Reduction Protocol	20
8	Exponentiation with a Shared Exponent	23
8.1	Set Membership	24
9	Generating Shared Random Primes	26
9.1	The Basic Miller-Rabin Algorithm	26
9.2	Generation of a Shared Candidate Prime	27
9.3	Distributed Miller-Rabin Primality Test	27
9.4	Generation of Shared Random Safe Primes	28
10	Efficient Generation of Shared RSA Keys	30
11	Computing Inverses over a Shared Modulus	30
11.1	The Basic Idea	30
11.2	The Full Protocol	31
11.3	A Fundamental Lemma	34
	References	36

B Multiparty Computation, an Introduction

Ronald Cramer and Ivan Damgård

41

1	Introduction	41
2	What is Multiparty Computation?	41
2.1	The MPC and VSS Problems	41
2.2	Adversaries and their Powers	42
2.3	Models of Communication	43
2.4	Definition of Security	44
3	Results on MPC	49
3.1	Results for Threshold Adversaries	49
3.2	Results for General Adversaries	50
4	MPC Protocols	51
4.1	The Passive Case	53
4.2	The Active Case	60
4.3	Realization of F_{Com} : Information Theoretic Scenario	65
4.4	Formal Proof for the F_{Com} Realization	75
5	The Cryptographic Scenario	76
5.1	Using Encryption to Implement the Channels	76
5.2	Cryptographic Implementations of Higher-Level Functionalities	77
6	Protocols Secure for General Adversary Structures	78
A	Formal Details of the General Security Model for Protocols	78
A.1	The Real-Life Execution	79
A.2	The Ideal Process	80
A.3	The Hybrid Models	82
A.4	Composing Protocols	83
A.5	Composing Interfaces	84
	References	85

C Foundations of Modern Cryptography*Giovanni Di Crescenzo***89**

1	Introduction	89
2	One-Way Functions	89
2.1	Definitions	90
2.2	Candidates from Number Theory	92
2.3	Weak vs. Strong One-Way Functions	94
3	Pseudo-Random Generators	98
3.1	Definitions	99
3.2	Constructions	100
3.3	A Cryptographic Application	103
4	Pseudo-Random Functions	103
4.1	Definitions	104
4.2	Constructions	105
4.3	Examples and Applications	108
5	Zero-Knowledge Protocols	109
5.1	Basic Definitions	110
5.2	Zero-Knowledge Proof Systems of Membership	111
5.3	Witness-Indistinguishable Proof Systems of Knowledge	116
5.4	Zero-Knowledge Proof Systems of Decision Power	119
5.5	Zero-Knowledge Transfers of Decision	124
	References	129

D Provable Security for Public Key Schemes*David Pointcheval***133**

1	Introduction	133
1.1	Provable Security	134
1.2	Exact Security and Practical Security	134
1.3	Outline of the Notes	135
1.4	Related Work	135
2	Security Proofs and Security Arguments	135
2.1	Computational Assumptions	135
2.2	“Reductionist” Security Proofs	136
2.3	Practical Security	136
2.4	The Random-Oracle Model	137
2.5	The General Framework	138
3	A First Formalism	138
3.1	Digital Signature Schemes	139
3.2	Public-Key Encryption	140
4	The Computational Assumptions	143
4.1	Integer Factoring and the RSA Problem	143
4.2	The Discrete Logarithm and the Diffie-Hellman Problems	145

5	Digital Signature Schemes	146
5.1	Provable Security	147
5.2	DL-Based Signatures	148
5.3	RSA-Based Signatures	154
6	Public-Key Encryption	163
6.1	History	163
6.2	A First Generic Construction	164
6.3	OAEP: the Optimal Asymmetric Encryption Padding.	167
6.4	REACT: a Rapid Enhanced-security Asymmetric Cryptosystem Transform	179
7	Conclusion	184
	References	185

E Efficient and Secure Public Key Cryptosystems

Tsuyoshi Takagi

191

1	Efficient Integer Arithmetic	191
1.1	Modular Exponentiation	191
1.2	Window Methods	192
1.3	Montgomery Multiplication	194
2	Fast Variants of RSA Cryptosystem	196
2.1	PKCS #1 Version 2.1	196
2.2	Multi-Exponent RSA	197
2.3	Size of Secret Primes	199
2.4	Comparison	200
3	Implementation Attack on RSA-CRT	201
4	EPOC Cryptosystem	204
4.1	EPOC-2 Cryptosystem	204
4.2	Reject Timing Attack on EPOC-2	207
4.3	Relation to Other Cryptosystems	212
4.4	Other Encryption Primitives	213
5	Elliptic Curve Cryptosystem	214
5.1	Scalar Multiplication	215
5.2	Efficient Coordinate System	217
6	Side Channel Attacks on ECC	218
6.1	SPA on ECC	218
6.2	DPA and Countermeasures	219
6.3	Goubin's Power-Analysis Attack	220
7	Zero-Value Point Attack on ECC	220
7.1	Non-Zero Digit Methods	226
7.2	Montgomery Ladder Method	226
7.3	Non-Zero Window Method	231
	References	231

Contemporary Cryptology

Catalano, D.; Cramer, R.; Damgård, I.; Di Crescenzo, G.;

Pointcheval, D.; Takagi, T.

2005, IX, 238 p., Softcover

ISBN: 978-3-7643-7294-1

A product of Birkhäuser Basel