

Albrecht Beutelspacher · Jörg Schwenk ·
Klaus-Dieter Wolfenstetter

Moderne Verfahren der Kryptographie





Von RSA zu Zero-Knowledge

8., überarbeitete Auflage



Springer Spektrum

Inhaltsverzeichnis

	Ziele der Kryptographie	1
	1.1 Geheimhaltung	1
	1.2 Authentikation	2
	1.3 Anonymität	4
	1.4 Protokolle	5
	Literatur	6
	Kryptologische Grundlagen	9
	2.1 Verschlüsselung	9
	2.2 Asymmetrische Verschlüsselung	14
	2.3 Einwegfunktionen	16
	2.4 Kryptographische Hashfunktionen	17
	2.5 Trapdoor-Einwegfunktionen	18
	2.6 Commitment und Bit-Commitment	19
	2.7 Digitale Signatur	21
	2.8 Der RSA-Algorithmus	24
	Literatur	28
	Grundlegende Protokolle	31
	3.1 Passwortverfahren (Festcodes)	31
	3.2 Wechselcodeverfahren	33
	3.3 Challenge-and-Response	35
	3.4 Diffie-Hellman-Schlüsselvereinbarung	37
	3.5 Das ElGamal-Verschlüsselungsverfahren	39
	3.6 Das ElGamal-Signaturverfahren	40
	3.7 Shamirs No-Key-Protokoll	41
	3.8 Knobeln übers Telefon	44
	3.9 Blinde Signaturen	46
	Literatur	48
	Zero-Knowledge-Verfahren	51
	4.1 Interaktive Beweise	51
	4.2 Zero-Knowledge-Verfahren	56
	4.3 Alle Probleme in NP besitzen einen Zero-Knowledge-Beweis	65
	4.4 Es ist besser, zwei Verdächtige zu verhören	69

4.5	Witness Hiding	73
4.6	Nichtinteraktive Zero-Knowledge-Beweise	78
4.7	Das Random Oracle-Modell	84
	Literatur	86

Multiparty Computations	89
5.1 Secret Sharing Schemes	89
5.2 Wer verdient mehr?	92
5.3 Skatspielen übers Telefon	96
5.4 Secure Circuit Evaluation	99
5.5 Wie kann man sich vor einem allwissenden Orakel schützen?	104
Literatur	105

Anonymität	107
6.1 Das Dining-Cryptographers-Protokoll	107
6.2 MIXe	110
6.3 Elektronische Münzen	112
6.4 Elektronische Wahlen	114
Literatur	118

Vermischtes	121
7.1 Schlüsselmanagement durch Trusted Third Parties	121
7.2 Angriffe auf Protokolle	128
7.3 Oblivious Transfer	134
7.4 Quantenkryptographie	143
Literatur	146

Pairing-basierte Kryptosysteme	149
8.1 Elliptische Kurven in der Kryptographie	149
8.2 Die Gap-DH-Annahme	151
8.3 Bilineare Abbildungen	152
8.4 Neue Signaturverfahren	154
8.5 Identitätsbasierte Kryptographie	154
8.6 Generischer Einsatz von bilinearen Abbildungen	156
Literatur	156

Mathematische Grundlagen	157
9.1 Natürliche Zahlen	157
9.2 Modulare Arithmetik	161
9.3 Quadratische Reste	166
9.4 Der diskrete Logarithmus	169
9.5 Isomorphie von Graphen	173
9.6 Der Zufall in der Kryptographie	175

9.7	Komplexitätstheorie	177
9.8	Große Zahlen	180
	Literatur	182
Sachverzeichnis	183