

Inhaltsverzeichnis

1. Public-Key-Kryptographie	1
1.1 RSA	2
1.2 Diskreter Logarithmus	4
1.2.1 Diffie-Hellman-Schlüsselaustausch	5
1.2.2 ElGamal-Verschlüsselung	6
1.2.3 ElGamal-Signatur	7
1.3 Geeignete Gruppen	8
2. Elliptische Kurven	11
2.1 Affine Kurven	12
2.2 Projektive Kurven	15
2.3 Elliptische Kurven	22
3. Elliptische Kurven über endlichen Körpern	55
3.1 Der Frobenius	55
3.2 Punkte zählen	57
3.3 Der Schoof-Algorithmus	63
3.4 Supersinguläre elliptische Kurven	66
4. Das Problem des diskreten Logarithmus für elliptische Kurven	75
4.1 Allgemeine Methoden	76
4.1.1 Enumerationsverfahren	76

4.1.2	Babystep-Giantstep-Algorithmus (BSGS)	76
4.1.3	Pohlig-Hellman-Verfahren	77
4.1.4	Pollard- ρ -Methode	79
4.1.5	Pollard- λ -Methode	82
4.2	Spezielle Methoden	82
4.2.1	Der MOV-Algorithmus	83
4.2.2	Anomale Kurven oder SSSA-Algorithmus	89
5.	Praktische Konsequenzen	97
5.1	Geeignete elliptische Kurven	97
5.2	Vergleich mit anderen Public Key-Verfahren	98
5.2.1	RSA	98
5.2.2	DL-Verfahren in \mathbb{F}_q^\times	102
5.3	ECDSA	104
6.	Anhang: Mathematische Grundlagen	111
6.1	Ganze Zahlen	111
6.2	Kongruenzen	114
6.3	Gruppen	117
6.4	Ringe und Körper	122
6.5	Polynome	125
6.6	Endliche Körper	128
6.7	Algebraisch abgeschlossene Körper	130
6.8	Einheitswurzeln	131
6.9	p -adische Zahlen	131
6.10	Komplexität	134
	Literaturverzeichnis	137
	Sachverzeichnis	141