

Indice

Introduzione	i
I Le radici della crittografia	1
1 La segretezza nella comunicazione	3
1.1 Scritture celate, scritture rivelate	3
1.2 Il vocabolario della crittografia	8
1.3 Classificazione delle cifrature	12
2 Breve storia della crittografia	17
2.1 La trasposizione	18
2.2 La corrispondenza di Giulio Cesare	21
2.3 Macchine cifranti	29
2.4 Il vero modo di scrivere in cifra	35
2.5 La cifra indecifrabile	38
2.6 La guerra dei crittografi	52
3 Tempi moderni	61
3.1 Il cifrario perfetto	62
3.2 Il segreto diventa pubblico	69
3.3 Uno sguardo sul futuro	80
II Il ruolo della meccanica quantistica	83
4 Primi passi nel mondo quantistico	85
4.1 La polarizzazione della luce e i fotoni	85
4.2 L'esperimento di Stern e Gerlach e lo spin dell'elettrone	98
4.3 Somiglianze e differenze	105

5	Gli strumenti della meccanica quantistica	107
5.1	Osservabili e apparati di misura	108
5.2	Misure e loro risultati	118
5.3	Vietato copiare!	120
6	Obiezioni e contraddizioni	127
6.1	I gatti di Schrödinger	128
6.2	Il paradosso di Einstein, Podolsky e Rosen	131
6.3	Gli amici di Alice e la disuguaglianza di Bell	143
6.4	Un paradosso ben poco paradossale	153
III	La crittografia quantistica	157
7	Particelle e informazione	159
7.1	Le banconote quantistiche	161
7.2	Il primo protocollo di crittografia quantistica	165
7.3	La crittografia quantistica e lo spin	176
8	Un'analisi critica	185
8.1	L'efficienza di un protocollo	187
8.2	Come ridurre l'informazione di Eva aumentando la segretezza	193
9	Nuovi orizzonti	201
9.1	Le sfide sperimentali	201
9.2	Il teletrasporto e i gatti di Schrödinger	206
9.3	Qubit e parallelismo quantistico	210
IV	Appendici	217
A	Il cifrario a chiave pubblica RSA	219
B	Approfondimento sulla disuguaglianza di Bell	225
C	La logica del teletrasporto	229
	Bibliografia	235
	Indice analitico	241