

Índice

Prólogo	13
Presentación	17
Capítulo I. Introducción y preliminares	21
1 Criptografía basada en curvas elípticas	23
2 Contenido y estructura de la obra	25
Capítulo II. Criptografía con curvas elípticas: ECC	29
1 Definición de curva elíptica	29
2 Estructura de grupo	35
3 Curvas elípticas sobre cuerpos finitos	38
4 Curvas elípticas sobre cuerpos primos	41
5 Curvas elípticas sobre cuerpos binarios	44
6 Curvas elípticas de Edwards y de Montgomery	49
7 Orden de una curva elíptica definida sobre un cuerpo finito y orden de un punto	53
8 Representación de los puntos de una curva elíptica	56
9 Patentes relacionadas	57
Capítulo III. Seguridad de la ECC	61
1 Métodos generales	61
2 Métodos para curvas específicas	72
3 Desafíos para atacar el ECDLP	73
Capítulo IV. Generación de curvas elípticas	75
1 Características del procedimiento Brainpool	76
2 Algoritmos del procedimiento Brainpool	83
3 Resultados empíricos sobre Brainpool	86
4 Características del procedimiento SafeCurves	87
5 La curva del millón de dólares	94

Capítulo V. Protocolos con curvas elípticas	97
1 Protocolos de acuerdo de clave	97
2 Protocolos de cifrado y descifrado	103
3 Algoritmo de firma digital ECDSA	109
Capítulo VI. Cifrado ECIES	113
1 Criptosistema DHIES	113
2 ECIES	114
3 Diferencias en las versiones estándar de ECIES	118
4 Seguridad de ECIES	123
5 Ejemplo de implementación de ECIES	129
6 Otros esquemas de cifrado híbrido	135
Capítulo VII. Implementación ECC en Java	139
1 El lenguaje Java	139
2 Funcionalidad ECC en el modelo JCA/JCE	146
3 Curvas elípticas disponibles en SunEC	148
4 Ejemplos de código con el proveedor SunEC	152
5 Bibliotecas criptográficas de terceras empresas	156
Capítulo VIII. Implementación ECC en Java Card	159
1 Funcionalidad ECC en Java Card	159
2 Características criptográficas adicionales	161
3 Ejemplos de código con NetBeans	163
Capítulo IX. Emparejamientos bilineales	179
1 Protocolos de Diffie-Hellman	180
2 Emparejamientos bilineales	183
3 Protocolos basados en emparejamientos	187
4 Emparejamiento de Tate	195
Capítulo X. Implementación de algoritmos para ECC	201
1 Aritmética de puntos	202
2 Algoritmos eficientes para ejecutar la multiplicación escalar	205
3 Algoritmos de multiplicación escalar que incluyen contramedidas	213

Capítulo XI. Ataques por canal lateral y por inducción de fallos	223
1 Ataques por canal lateral	224
2 Ataques por inducción de fallos	238
3 Ataques combinados	246
Apéndices	249
Apéndice A. Tarjetas inteligentes	251
1 La norma ISO/IEC 7816	252
2 Estructura de ficheros en una tarjeta inteligente	254
3 Comunicación con la tarjeta inteligente	254
Apéndice B. Java Card	259
1 Java Card API	261
2 Java Card Runtime Environment	263
3 Java Card Virtual Machine	268
4 Programación en Java Card	269
5 Limitaciones del lenguaje Java Card	270
6 Características criptográficas en Java Card	271
Bibliografía	275
Glosario de términos	295
Índice temático	301