

Índice general

1. Introducción	9
2. Conceptos básicos de paralelismo	11
2.1. Introducción	11
2.2. Modelos de computación paralela	11
2.2.1. Computadoras paralelas	11
2.2.2. Modelos de paralelismo	12
2.2.3. Relaciones entre modelos de paralelismo	14
2.3. Medidas de desempeño	15
2.3.1. Aceleramiento, eficiencia y redundancia	15
2.4. Clase de complejidad paralela	17
2.4.1. La clase NC	17
3. Multiprocesadores y multicomputadoras	19
3.1. Introducción	19
3.2. Multicomputadora de hipercubo	20
3.2.1. Estructura recursiva del hipercubo	20
3.2.2. Propiedades topológicas de un cubo (N, b, k)	23
3.2.3. Incrustamiento de topologías simples	26
3.3. Multiprocesadores de memoria compartida	35
3.3.1. Conceptos básicos	35
3.3.2. Análisis de redes bloqueantes	38
3.3.3. Análisis de redes no bloqueantes	41
3.4. Multicomputadora de componentes comunes	43
3.4.1. Arquitectura	43
3.4.2. Interfaz de paso de mensajes MPI	44
4. Operaciones aritméticas básicas	45
4.1. Introducción	45

4.2.	Adición paralela	45
4.2.1.	Algoritmo de Brent	45
4.3.	Multiplicación paralela	49
4.3.1.	Multiplicación de primaria en paralelo	49
4.3.2.	Algoritmo de Karatsuba-Ofman	49
4.3.3.	Multiplicación mediante convolución	50
4.4.	Transformada rápida de Fourier modular	51
4.4.1.	Raíces de la unidad en aritmética modular	51
4.4.2.	Transformada rápida de Fourier	54
4.4.3.	Convolución de vectores	60
4.4.4.	Producto de polinomios	61
4.4.5.	Algoritmo de Schonhage-Strassen	65
5.	Campos finitos	71
5.1.	Introducción	71
5.2.	El campo finito $GF(p)$	72
5.3.	El campo finito $GF(2^m)$	73
5.3.1.	Representación en bases polinomiales	73
5.3.2.	Representación en bases normales	76
6.	Curvas elípticas	83
6.1.	Introducción	83
6.2.	Ecuaciones de Weierstrass	83
6.3.	Estructura de grupo de una curva elíptica	86
6.4.	Cálculo de operaciones de grupo	88
6.5.	Curvas elípticas sobre $GF(p)$	89
6.6.	Curvas elípticas sobre $GF(2^m)$	91
6.7.	Interpretación gráfica de la aritmética de puntos sobre curvas elípticas	93
6.8.	Propiedades fundamentales	93
6.9.	Logaritmo discreto sobre curvas elípticas	95
6.10.	Curvas de Koblitz	98
6.10.1.	Propiedades básicas	99
7.	Criptosistemas de curvas elípticas (CCE)	103
7.1.	Introducción	103
7.2.	Elección de una curva apropiada	103
7.2.1.	Método 1 - Selección de una curva aleatoria	104
7.2.2.	Método 2 - Seleccionando primero el orden de la curva	104
7.2.3.	Método 3 - Usando el teorema de Weil	105

7.3.	Generación de claves	106
7.4.	Representación del campo	107
7.4.1.	El campo finito $GF(p)$	107
7.4.2.	El campo finito $GF(2^m)$	107
7.5.	Representación de puntos sobre la curva.	107
7.5.1.	Compresión de puntos (Curvas elípticas sobre $GF(p)$)	108
7.5.2.	Compresión de puntos (Curvas elípticas sobre $GF(2^m)$)	108
7.6.	Esquema de cifrado (ECES)	109
7.6.1.	Cifrado	109
7.6.2.	Descifrado	111
7.6.3.	Ejemplo de cifrado con ECES	113
7.6.4.	Cifrado ECES sobre la curva K-163	114
7.7.	Firma digital (ECSS y ECDSA)	116
7.7.1.	Esquema de firma digital de curvas elípticas ECSS . .	117
7.7.2.	Verificación de firma ECSS	118
7.7.3.	Ejemplo de firma digital ECSS	119
7.7.4.	Algoritmo de firma digital ECDSA	121
7.7.5.	Verificación de firma digital ECDSA	122
7.7.6.	Ejemplo de firma digital ECDSA	124
7.7.7.	Firma digital ECDSA sobre K-163	125
7.8.	Protocolo de acuerdo de clave (ECKEP)	127
8.	Algoritmos para CCE	129
8.1.	Introducción	129
8.2.	Algoritmos del campo subyacente.	129
8.3.	Algoritmos de multiplicación escalar	130
8.3.1.	Algoritmo binario	130
8.3.2.	Algoritmo m -ario	131
8.3.3.	Cadenas aditivas	132
8.3.4.	Método de adición y substracción	133
8.3.5.	Método de ventana	135
9.	Algoritmo paralelo de multiplicación escalar	139
9.1.	Introducción	139
9.2.	Multiplicación escalar	139
9.3.	Método binario	140
9.4.	Método binario de orden p	142
9.5.	El método τ -ario de orden p	145

10.Implementación y resultados experimentales	149
10.1. Introducción	149
10.2. Implementación del campo subyacente	149
10.3. Implementación de curvas elípticas	150
10.4. Desempeño de las operaciones de puntos	151
10.5. Implementación del algoritmo paralelo	152
10.6. Desempeño del algoritmo paralelo	153
10.6.1. Curvas binarias aleatorias	153
10.6.2. Curvas de Koblitz	154
10.7. Conclusiones	156
A. Código de la aritmética de puntos	157
A.1. Definición de clase	157
A.2. Implementación de clase	159
A.3. Programa de prueba	161
A.4. Salida de una ejecución	164
B. Código del esquema de cifrado ECES	167
B.1. Generación de claves	167
B.2. Cifrado	169
B.3. Descifrado	171
C. Código de firma digital ECDSA	173
C.1. Generación de claves	173
C.2. Generación de firma	175
C.3. Verificación de firmas	177
D. Código del algoritmo paralelo	179
D.1. Algoritmo binario de orden p	179
E. Especificación de curvas elípticas	187
E.1. Curva B-163	187
E.2. Curva B-233	188
E.3. Curva B-283	188
E.4. Curva B-409	189
E.5. Curva B-571	189
E.6. Curva K-163	190
E.7. Curva K-233	190
E.8. Curva K-283	191
E.9. Curva K-409	191

E.10. Curva K-571	192
-----------------------------	-----

