

Índex de termes

- λ -descomposició, 8,40
- algorisme
 - de Berlekamp-Massey, 56
 - distribuïdor, 16
 - euclidà equivalent, 56
 - recuperador, 16
- anònims, esquemes per a compartir secrets, 59
- aplicació cumulativa, 32
- apropiació indeguda, 6,53
- arrel cúbica , 141
- autodual, estructura, 31,75
- base, 18
- Berlekamp-Massey, algorisme de, 56
- bipartit complet, graf, 69
- bipartita de quasi llinar, estructura d'accés, 81
- bipartita, estructura d'accés, 9,80
- boicotejador, 53
- cúbica , arrel, 141
- caixa negra, 16
- centrals, vèrtexs, 64
- centre d'un graf, 64
- cicle generalitzat, 113
 - de rang 3 i llargada n , 117
- circuit en un matroide, 38
- circuital, esquema, 8,22
- clausura, 18
- coloracions d'arestes de grafs bipartits, 44
- computació amb tolerància a fallides,
 - 16
 - computacionalment segurs, 59
 - condicionada, entropia, 46
 - condicionada, informació mútua, 47
 - conjugat, 147
 - conjunt de diferències planar, 58
 - connectada, estructura, 18
 - connectat, matroide, 38
 - construcció d'espai vectorial, 28
 - construcció per descomposició, 40, 102
 - criptografia visual, 5,59
 - criptosistema
 - de Fiat- Shamir, 151
 - de Rabin, 151
 - cumulativa, aplicació, 32
 - descomposició, λ 8,40
 - descomposició, construcció per, 40, 102
 - diferències planar, conjunt de, 58
 - dinàmic,
 - esquema, 59
 - esquema totalment, 59
 - distància del taxista, 98
 - distribuïdor
 - mentider, 59
 - algorisme, 16
 - distribució de claus, 16
 - dual, estructura, 31
 - enganyar
 - un participant amb uns fragments,

- 128
- probabilitat d', 128
- entropia 46
 - condicionada, 46
- espai vectorial,
 - construcció d', 28
 - esquema d', 29
 - estructura d'accés d', 28,29
- esquema
 - (Γ, δ) -segur, 128
 - (Γ, ϵ) -robust, 129
 - (r, n, δ) -segur, 129
 - (r, n, ϵ) -robust, 129
 - circuital, 8,22
 - de Karnin, Greene i Hellman, 19
 - de les regles de distribució, 34
 - de llindar (t, n) , 18
 - de llindar robust (t, n, ϵ) , 55
 - de Salomaa, 25
 - d'espai vectorial, 29
 - dinàmic, 59
 - geomètric Blakley, 7
 - geomètric segur enfront mentiders, 57
 - ideal, 27
 - per a compartir secrets, 5
 - polinomial de Shamir, 7,20,29
 - totalment dinàmic, 59
- esquemes
 - amb capacitat de vet, 60
 - multi secret, 59
 - no perfectes, 17
 - per a compartir diversos secrets no independents, 59
 - per a compartir secrets amb capacitat de desenrolament, 60
 - per a compartir secrets anònims, 59
 - preposicionats, 59
 - segurs enfront de mentiders, 53,127
- estafadors, 53
- estrella
 - des de un subconjunt, 102
 - generalitzada, 102
 - graf, 41
- estructura d'accés, 6,17
 - autodual, 31,75
 - connectada, 18
 - bipartita (N_1, N_2) , 80
 - bipartita de quasi llindar (X, Y) , 81
 - definida per pesos i llindar, 62
 - d'espai vectorial, 28
 - multipartita (X_1, \dots, X_ℓ) , 94
 - universalment ideal, 39
 - de llindar (n, n) , 19
 - de llindar (t, n) , 15,18
 - dual, 31
 - homogènia, 8,18
 - ideal, 28,37
 - uniforme, 8,18
- estructures d'accés
 - bipartites, 9
 - basades en codis lineals correctors d'errors, 19
 - determinades per un graf, 8,19
 - de llindar amb pesos, 7,19,22
 - intrínseques, 19
- fórmula booleana per una estructura, 22,31
- Fermat, petit teorema de, 146
- Fiat- Shamir, criptosistema de, 151
- fragment d'informació, 5,16
- geomètric de Blakley, esquema 7, 30
- gestió de claus, 16
- graf
 - amb pesos, 67
 - bipartit complet, 69

- estrella, 41
- multipartit complet, 39,41
 - centre d'un, 64
 - estructures d'accés determinades per un, 8,19
- grau, 11,102
- homogènia, estructura, 8,18
- illegals, secrets 57
- ideal, estructura, 28,37
- identificació humana, 60
- indeguda, apropiació, 6,53
- informació mútua, 47
 - condicionada, 47
- interpolació polinòmica, 21
- Karnin, Greene i Hellman, esquema de, 19
- Lema de les mans encaixades, 102
- llindar, 15
 - amb pesos, estructures de, 7,19,22
 - robust, (t, n, ϵ) -esquema de, 55
 - (n, n) -estructura de, 19
 - (t, n) -esquema de, 18
 - estructura d'accés bipartita de quasi, 81
 - estructura d'accés definida per pesos i, 62
 - estructura de, 15
- mètode
 - de la força bruta, 39
 - de Peralta, 146
 - de Tonelli-Shanks, 149
- matroide, 7,37
 - connectat, 38
 - de Vamos, 39
 - representable, 38
 - circuit en un, 38
 - punts d'un, 38
 - subconjunts dependents d'un, 38
 - subconjunts independents d'un, 38
- mentider, 6,53,127
 - distribuidor, 59
- mentiders, esquemes segurs enfront de, 53,127
- minimals, subconjunts, 18
- monòtona, 6,18
- multi secret, esquemes, 59
- multi-estat, 59
- multipartit complet, graf, 39,41
- multipartita, (X_1, \dots, X_ℓ) -estructura d'accés, 94
- no perfectes, esquemes, 17
- norma, 147
- Peralta, mètode de, 146
- perfecte, 5,17,35,48
- pesos i llindar, estructura d'accés definida per, 62
- pesos
 - k -graf amb, 67
 - estructures de llindar amb, 7,19,22
- petit teorema de Fermat, 146
- probabilitat d'enganyar, 128
- problema
 - de la renovació de fragments, 59
 - de la reutilització de fragments, 59
- protocols segurs multipart, 16
- prova de coneixement zero, 57
- punts
 - consecutius de Π_0 , 81
 - d'un matroide, 38
 - minimals (e. multipartita), 94
 - minimals, 81
- quasi-llindar, 9
 - estructura d'accés bipartita de (X, Y) , 81
- Rabin, criptosistema de, 151
- rang

- d'un matroide, 38
- d'una estructura, 18
- realitzar, 17
- recobriment multipartit complet, 43,69
- recuperador, algorisme, 16
- regla de distribució, 34
- renovació de fragments, problema de la, 59
- representable, matroide, 38
- reutilització de fragments, problema de la, 59
- robust
 - (t, n, ϵ) -esquema de llindar, 55
 - esquema (r, n, ϵ) , 129
- secrets il·legals, 57
- segur, esquema (r, n, δ) , 129
- seguretat
 - computacional, 17
 - condicional contra mentiders, 55
 - incondicional contra mentiders, 55
 - no computacional, 17
- segurs, computacionalment 59
- Shamir, esquema polinomial de, 7,20,29
- sistemes de Steiner, 45
- subconjunt autoritzat, 5
- subconjunts
 - dependents d'un matroide, 38
 - independents d'un matroide, 38
 - minimals, 18
- subestructura, 17
- subgrup de Sylow, 150
- subordinats, vèrtexs, 64
- successió independent
 - de participants, 52
 - de subconjunts, 49
- Sylow, 150
- taxa d'informació, 48
 - òptima, 28
 - de l'esquema, 26
 - del participant, 26
- taxa mitjana
 - d'informació òptima, 28
 - d'informació, 27,49
- taxista, distància del, 98
- Teoria de la Informació, 45
- Tonelli-Shanks, mètode de, 149
- uniforme, estructura, 8,18
- vèrtexs
 - centrals, 64
 - subordinats, 64
- Vamos, matroide de, 39
- vector de contribució, 27
- visual, criptografia, 5,59

