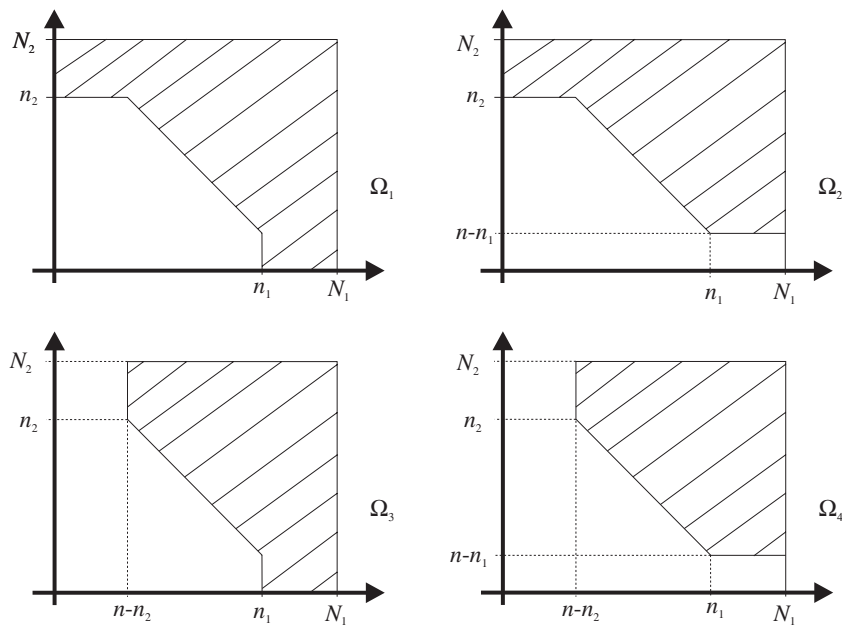


Esquemes per a compartir secrets



Tesi Doctoral presentada per
Germán Sáez i Moreno
a la Universitat Politècnica de Catalunya
Director de la Tesi:
Carles Padró Laimon

Índex

1	Introducció	5
2	Esquemes per a compartir secrets	15
2.1	Esquema per a compartir secrets perfecte	16
2.2	Exemples d'esquemes per a compartir secrets	19
2.3	Taxa d'informació	26
2.4	Esquema d'espai vectorial	28
2.5	Model general de les regles de distribució	34
2.6	Caracterització dels esquemes ideals	37
2.7	Fites inferiors de la taxa d'informació òptima	40
2.8	Fites superiors de la taxa d'informació òptima	45
2.9	Esquemes segurs enfront de mentiders	53
3	Taxa d'informació	61
3.1	Estructures definides per pesos i llindar	62
3.1.1	Caracterització de les estructures d'accés definides per pesos i llindar de rang dos	63
3.1.2	Fites en la taxa d'informació òptima	68
3.1.3	Estructura dual d'una estructura definida per pesos i llindar	71
3.2	Estructures d'accés bipartites	79
3.2.1	Estructures d'accés bipartites ideals	81
3.2.2	Fites de la taxa d'informació òptima	87
3.2.3	Generalització per estructures d'accés multipartites	94
3.3	Fites per les estructures de llindar amb dos pesos	96
3.3.1	Fites inferiors de la taxa d'informació òptima per dos pesos i llindar	96
3.3.2	Fites superiors de la taxa d'informació òptima per esquemes per dos pesos i llindar	98

3.3.3	Generalització per fites de la taxa d'informació òptima per més de dos pesos	99
3.4	Fites inferiors per les estructures homogènies	101
3.4.1	Primera construcció	102
3.4.2	Segona construcció	104
3.4.3	Comparació entre les dues construccions	108
3.4.4	Comparació amb les fites per estructures homogènies de rang r	111
3.4.5	Comparació amb les fites per estructures homogènies de rang 3	114
3.5	Fites superiors per les estructures homogènies de rang 3	117
4	Esquemes segurs enfront de mentiders	127
4.1	Esquemes (Γ, δ) -segurs i (Γ, ϵ) -robustos	128
4.2	Un esquema vectorial (Γ, δ) -segur	130
4.3	Un esquema de llindar (r, n, ϵ) -robust	134
4.4	Esquema (Γ, δ) -segur per estructures qualssevol	138
5	Arrels cúbiques a \mathbb{Z}_m	141
5.1	Existència i nombre de solucions	142
5.2	Modificació del mètode de Peralta	146
5.3	Modificació del mètode de Tonelli-Shanks	149
5.4	Algunes aplicacions criptogràfiques	151
6	Conclusions	153

Llista de Figures

2.1	Algorisme distribuïdor i recuperador en un esquema per a compartir secrets	17
2.2	Tots els secrets són possibles a l'esquema polinomial de Shamir per $t = 3$	21
2.3	Circuit associat a la forma normal conjuntiva per l'estructura $\Gamma_0 = \{\{p_1, p_2\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}\}$	23
2.4	Circuit associat a la forma normal disjuntiva per l'estructura $\Gamma_0 = \{\{p_1, p_2\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}\}$	24
2.5	Acció d'un boicotejador	53
2.6	Apropiació indeguda	54
3.1	Estructura d'accés homogènia de rang 2 definida per pesos i llindar.	65
3.2	El 1-graf és un graf multipartit complet.	69
3.3	Graf multipartit complet $H_{q,0}$	70
3.4	Minimals del dual d'una estructura de rang 2 homogènia amb $ A_k \geq 2$	76
3.5	Minimals del dual d'una estructura de rang 2 homogènia amb $A_k = \emptyset$ i amb $ C_k \geq 2$	77
3.6	Minimals del dual d'una estructura de rang 2 no homogènia amb $ A_k \geq 2$	79
3.7	Minimals del dual d'una estructura de rang 2 no homogènia amb $A_k = \emptyset$ i $ C_k \geq 2$	80
3.8	(X, Y) -estructures d'accés bipartites de quasi llindar $\Omega_j(n, n_1, n_2)$	82
3.9	Estructura d'accés Γ definida per pesos 4 i 5 i per llindar $t = 40$ amb $ \omega^{-1}(4) > 10$ i $ \omega^{-1}(5) > 8$	87
3.10	Estructures d'accés $\Gamma, \Gamma', \Gamma_1$ i Γ_2	90
3.11	Successió $\{B_{ij}\}_{i,j}$ per $i \neq s$	91
3.12	Cas de dos minimal en una estructura bipartita.	93

- 3.13 Exemple de construcció de Γ' a partir d'un cicle generalitzat de
 $n = 9$ elements amb $q = 6$ còpies. 118
- 3.14 $S_0^a S_1^a S_2^a$ fa independent la successió B_1, \dots, B_9 per $n = 9, k = 1$
i $q = 6$ 124