



# Rosa Ana Tomàs Cuñat

## Dades personals-contacte / Datos personales-contacto / Personal information-contact



Descarregar imatge

**nom:** Rosa Ana Tomàs Cuñat

**Titularitat:** Professor associat / Profesor asociado / Partial Time Lecturer

**Àrea:** Matemàtica Aplicada / Matemática Aplicada / Applied Mathematics

**Departament:** Matemàtica / Matemática / Mathematics

**Escola Politècnica Superior / Escuela Politécnica Superior / Polytechnic Superior School:** Escola Politècnica Superior / Escuela Politécnica Superior / Polytechnic Superior School

**Campus de Cappedon. Edifici EPS. Despach 1.22 / Campus de Cappedon. Edificio EPS. Despacho 1.22 / Campus of Cappedon. EPS Building. Office 1.22**

**Correu electrònic:** [rosana.tomas@udl.cat](mailto:rosana.tomas@udl.cat)  
mailto:rosana.tomas@udl.cat

**Despach/Despacho/Office:**



+34 973 70 27 74

**Code ORCID:**

<https://orcid.org/0000-0002-1995-3974>  
<https://orcid.org/0000-0002-1995>



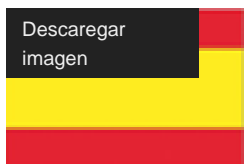
**TORNAR AL LLISTAT / VOLVER AL LISTADO / BACK TO LIST** [  
[/sites/Eps/ca/lescola/organitzacio/personal-docent-i-investigador/](#)]

## Formació acadèmica / Formación académica / Academic training



Descarregar imatge

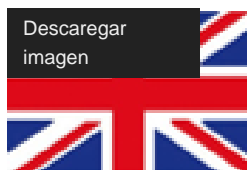
Doctora per la Universitat de Lleida (2011)



Descarregar imatge

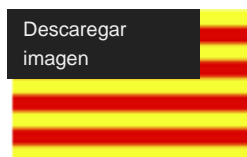
Doctora por la Universidad de Lleida (2011)

PhD (2011 – Universitat de Lleida)



**TORNAR AL LLISTAT / VOLVER AL LISTADO / BACK TO LIST** [  
/sites/Eps/ca/lescola/organitzacio/personal-docent-i-investigador/ ]

## Experiència professional / Experiencia profesional / Professional experience



- 2006-2007 (EPS)
- Llenguatges, autòmats i gramàtiques (501110)
  - Models abstractes de càlcul (501111)

2007-2008 (EPS)

- Llenguatges, autòmats i gramàtiques (501110)
- Models abstractes de càlcul (501111)

2013-2014 (FCE)

- Numeració, càlcul i mesura (100811)
- Aprenentatge de les matemàtiques (100717)
- Pràctiques escolars II (100741)
- Pràctiques escolars III (100742)
- Practicum (generalista) (100845)

2018-2019 (FDET)

- Matemàtiques d'empresarials (101303)
- Docència repetida de matemàtiques d'empresarials.

2018-2019 (EPS)

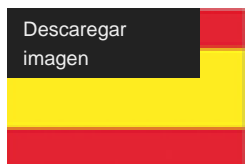
- Estructura de Computadors I (102002)
- Estructura de Computadors II (102003)

2019-2020 (FDET)

- Matemàtiques d'empresarials (101303)
- Docència repetida de matemàtiques d'empresarials.

2019-2020 (EPS)

- Estructura de Computadors I (102002)
- Estructura de Computadors II (102003)
- Ciberseguretat (1000173)



- 2006-2007 (EPS)
- Llenguatges, autòmats i gramàtiques (501110)
  - Models abstractes de càlcul (501111)

2007-2008 (EPS)



- Llenguatges, autòmats i gramàtiques (501110)
- Models abstractes de càlcul (501111)

2013-2014 (FCE)

- Numeració, càlcul i mesura (100811)
- Aprenentatge de les matemàtiques (100717)
- Pràctiques escolars II (100741)
- Pràctiques escolars III (100742)
- Practicum (generalista) (100845)

2018-2019 (FDET)

- Matemàtiques d'empresarials (101303)
- Docència repetida de matemàtiques d'empresarials.

2018-2019 (EPS)

- Estructura de Computadors I (102002)
- Estructura de Computadors II (102003)

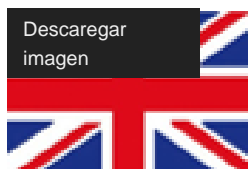
2019-2020 (FDET)

- Matemàtiques d'empresarials (101303)
- Docència repetida de matemàtiques d'empresarials.

2019-2020 (EPS)

- Estructura de Computadors I (102002)
- Estructura de Computadors II (102003)

Ciberseguretat (1000173)



2006-2007 (EPS)

- Llenguatges, autòmats i gramàtiques (501110)
- Models abstractes de càlcul (501111)

2007-2008 (EPS)

- Llenguatges, autòmats i gramàtiques (501110)
- Models abstractes de càlcul (501111)

2013-2014 (FCE)

- Numeració, càlcul i mesura (100811)
- Aprenentatge de les matemàtiques (100717)
- Pràctiques escolars II (100741)
- Pràctiques escolars III (100742)
- Practicum (generalista) (100845)

2018-2019 (FDET)

- Matemàtiques d'empresarials (101303)



- Docència repetida de matemàtiques d'empresarials.

2018-2019 (EPS)

- Estructura de Computadors I (102002)
- Estructura de Computadors II (102003)

2019-2020 (FDET)

- Matemàtiques d'empresarials (101303)
- Docència repetida de matemàtiques d'empresarials.

2019-2020 (EPS)




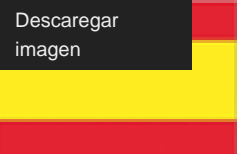





- Estructura de Computadors I (102002)
- Estructura de Computadors II (102003)

Ciberseguretat (1000173)



**TORNAR AL LLISTAT / VOLVER AL LISTADO / BACK TO LIST** [ </sites/Eps/ca/lescola/organitzacio/personal-docent-i-investigador/> ]

## Docència / Docencia / Teaching

-  Descaregar imagen  
▪ Grau en informàtica
-  ▪ Doble titulació: Grau en Enginyeria Informàtica i Grau en Administració i Direcció d'Empreses
-  ▪ Grau en Administració i Direcció d'Empreses
-  Descaregar imagen  
▪ Grado de informática
-  ▪ Doble grado: Grado de informática y Grado de Administración y Dirección de Empresas
-  ▪ Grado de Administración y Dirección de Empresas
-  Descaregar imagen  
▪ Bachelor's Degree in Computer Engineering
-  ▪ Double Bachelor's Degree: in Computer Engineering + in Business Administration and Management
-  ▪ Degree Business Administration and Management



**TORNAR AL LLISTAT / VOLVER AL LISTADO / BACK TO LIST** [ </sites/Eps/ca/lescola/organitzacio/personal-docent-i-investigador/> ]

## Gestió / Gestión / Management



[TORNAR AL LLISTAT](#) / [VOLVER AL LISTADO](#) / [BACK TO LIST](#) [ [/sites/Eps/ca/lescola/organitzacio/personal-docent-i-investigador/](#) ]

## Recerca / Investigación / Research

### Àmbit de recerca / Ambito de investigación / Research area



Criptografia

Criptografía

Cryptography

### Activitats de recerca / Actividades de investigación / Research activities



Volcanoes of  $l$ -isogenies of elliptic curves over finite fields: the case  $l=3$ . 912357 - Publicacions Matemàtiques. 1, pp. 165 - 180. (Espanya): 2007. ISSN 0214-1493

Non-reducible Meyer-Müller's like elliptic curve cryptosystem. 916846 – IEEE Latin America Transactions. 10 - 3, pp. 1730 - 1733. (Estats Units d'Amèrica): 2012. ISSN 1548-0992

- On Edwards curves and ZVP-attacks. 908839 – Applicable Algebra in Engineering Communication and Computing. 24 - 6, pp. 507 - 517. (Alemanya): 2013. ISSN 0938-1279
- Security analysis of order preserving symmetric cryptography. 915450 -Applied Mathematics & Information Sciences. 7 - 4, pp. 1285 - 1295. (Estats Units d'Amèrica): 2013. ISSN 1935-0090



- Securing databases by using diagonal-based order preserving symmetric encryption. 917843 - Applied Mathematics & Information Sciences. 8 - 5, pp. 2085 - 2094. (Bahrain): 2014. ISSN 2325-0399

Descargar imagen

- Volcanoes of  $l$ -isogenies of elliptic curves over finite fields: the case  $l=3$ . 912357 - Publicacions Matemàtiques. 1, pp. 165 - 180. (Espanya): 2007. ISSN 0214-1493
- Non-reducible Meyer-Müller's like elliptic curve cryptosystem. 916846 – IEEE Latin America Transactions. 10 - 3, pp. 1730 - 1733. (Estats Units d'Amèrica): 2012. ISSN 1548-0992

- On Edwards curves and ZVP-attacks. 908839 – Applicable Algebra in Engineering Communication and Computing. 24 - 6, pp. 507 - 517. (Alemanya): 2013. ISSN 0938-1279
- Security analysis of order preserving symmetric cryptography. 915450 -Applied Mathematics & Information Sciences. 7 - 4, pp. 1285 - 1295. (Estats Units d'Amèrica): 2013. ISSN 1935-0090
- Securing databases by using diagonal-based order preserving symmetric encryption. 917843 - Applied Mathematics & Information Sciences. 8 - 5, pp. 2085 - 2094. (Bahrain): 2014. ISSN 2325-0399

Descargar imagen

- Volcanoes of  $l$ -isogenies of elliptic curves over finite fields: the case  $l=3$ . 912357 - Publicacions Matemàtiques. 1, pp. 165 - 180. (Espanya): 2007. ISSN 0214-1493
- Non-reducible Meyer-Müller's like elliptic curve cryptosystem. 916846 – IEEE Latin America Transactions. 10 - 3, pp. 1730 - 1733. (Estats Units d'Amèrica): 2012. ISSN 1548-0992

- On Edwards curves and ZVP-attacks. 908839 – Applicable Algebra in Engineering Communication and Computing. 24 - 6, pp. 507 - 517. (Alemanya): 2013. ISSN 0938-1279
- Security analysis of order preserving symmetric cryptography. 915450 -Applied Mathematics & Information Sciences. 7 - 4, pp. 1285 - 1295. (Estats Units d'Amèrica): 2013. ISSN 1935-0090
- Securing databases by using diagonal-based order preserving symmetric encryption. 917843 - Applied Mathematics & Information Sciences. 8 - 5, pp. 2085 - 2094. (Bahrain): 2014. ISSN 2325-0399



**TORNAR AL LLISTAT / VOLVER AL LISTADO / BACK TO LIST [**  
</sites/Eps/ca/lescola/organitzacio/personal-docent-i-investigador/> ]