CRISES - Security & Privacy

Características generales | Características del Equipo de Investigación | Características de la Investigación

IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR

NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	CRISES - Security & Privacy
UNIDAD/DEPARTAMENTO DE PERTENENCIA	Departament d'Enginyeria Informàtica i Matemàtiques
CENTRO/INSTITUTO/UNIVERSIDAD/ORGANISMO DE PERTENENCIA	Universitat Rovira i Virgili

DATOS DE CONTACTO

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	Josep Domingo-Ferrer	TELÉFONO	977 558109
ROL EN EL EQUIPO	Investigador Principal	MAIL	josep.domingo@urv.cat
WEB DEL EQUIPO	https://crises-deim.urv.cat		

DIRECCIÓN POSTAL DEL EQUIPO

EDIFICIO	Campus Sescelades	CENTRO	
TIPO DE VÍA	Avda.	NOMBRE DE LA VÍA	Països Catalans
NÚMERO	26	CIUDAD	Tarragona
PROVINCIA	Tarragona	CÓDIGO POSTAL	43007

DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE

PERSONA DE CONTACTO	Francisco Díaz González
MAIL	vr.recerca@urv.cat
TELÉFONO	977 55 8001
WEB	https://www.urv.cat/

DIRECCIÓN POSTAL DEL ORGANISMO

EDIFICIO	Rectorado	CENTRO	
TIPO DE VÍA	Carrer	NOMBRE DE LA VÍA	de l'Escorxador
NÚMERO	s/n	CIUDAD	Tarragona
PROVINCIA	Tarragona	CÓDIGO POSTAL	43003

INVESTIGADOR PRINCIPAL

NOMBRE	TITULACIÓN
Josep Domingo-Ferrer	Catedrático Universitario

TRAYECTORIA PROFESIONAL

Josep Domingo-Ferrer is a Distinguished Professor of Computer Science and an ICREA-Acadèmia Researcher at Universitat Rovira i Virgili, Tarragona, Catalonia, where he holds the UNESCO Chair in Data Privacy and is the founding director of CYBERCAT-Center for Cybersecurity Research of Catalonia. He received his B.Sc.-M.Sc. and Ph.D. degrees in Computer Science from the Autonomous University of Barcelona in 1988 and 1991, respectively (Outstanding Graduation Award). He also holds a B.Sc.-M.Sc. in Mathematics. His research interests are in data privacy, data security, statistical disclosure control and cryptographic protocols, with a focus on the conciliation of privacy, security and functionality.

He has won three consecutive times (2008, 2013 and 2018) the ICREA-Acadèmia Prize, awarded for a 5-year period by the Government of Catalonia to the research leaders among faculty members in Catalan universities (13% success rate). In 2016 he was made an ACM Distinguished Scientist and a Fellow of Institut d'Estudis Catalans, the Catalan national academy. He received a Google Faculty Research Award (2014, 16% success rate). He was decorated by the Government of Catalonia with the "Narcís Monturiol" Medal for merit in science and technology (2012). He was made an Elected Member of Academia Europaea and of the International Statistical Institute in 2012. He was elevated to Fellow of IEEE (Institute of Electrical and Electronics Engineers) in 2012. Between 2007 and 2008, he was a co-recipient of four entrepreneurship prizes. In 2004, he got the TOYPS'2004 Award from the Junior Chambers of Catalonia. In 2003, he was a co-recipient of a research prize from the Association of Telecom Engineers of Catalonia. He has authored 5 patents and over 450 publications (H-index=61, Nov. 17, 2020), and as of Aug. 2015 he has ranked among the world's top 1% cited computer scientists (Essential Science Indicators). He has co-ordinated the H2020 project "CLARUS", the CONSOLIDER "ARES" team on security and privacy (one of Spain's strongest research teams), the EU FP5 project CO-ORTHOGONAL, the "CO-UTILITY" project (Templeton World Charity Foundation), and several Spanish funded and U.S. funded research projects. He has chaired 21 international conferences and has served in the program committee of over 360 conferences on privacy and security. He is a co-Editor-in-Chief of "Transactions on Data Privacy", an Associate Editor of the "Journal of Official Statistics", "KAIS-Knowledge and Information Systems", and a past Associate Editor of "IEEE Transactions on Dependable and Secure Computing" and "Computer Communications". He has been an Invited Professor at Beihang University (2015), National University of Ireland (2015) and Università di Roma 3 (2011); a Visiting Researcher at Katholieke Universiteit Leuven (2005) and a Visiting Fellow at Princeton University (2004). He was a Visiting Ph.D. Student at the Siemens Central R+D Department, München (1990) and at the University of Wisconsin-Milwaukee (1990).

WEB Y REDES SOCIALES

https://crises-deim.urv.cat/jdomingo/

MIEMBROS DEL EQUIPO

Castella Roca, Jordi	Sanchez, David	Bras Amoròs, Maria
Viejo, Alexandre	Farras, Oriol	Batet, Montserrat
Martínez, Sergio	Blanco, Alberto	Ribes, Jordi
Anglés, Carles	Rebollo, David	Manjón, Jesús A.

CRISES - Security & Privacy		
Características generales	Características del Equipo de Investigación	Características de la Investigación

LÍNEAS Y ÁREAS DE INVESTIGACIÓN	
ÁREAS DE INVESTIGACIÓN	**PRINCIPALES LÍNEAS DE INVESTIGACIÓN**
PRIVACIDAD	Análisis Big Data enfocado al respeto de la privacidad Protocolos criptográficos de preservación de la privacidad Privacidad en las consultas Aplicaciones móviles de preservación de la privacidad Sanitización y anonimización de datos Privacidad en IoT Sistemas de autenticación anónimos Private Information Retrieval (PIR) Tecnologías de seguridad respetuosas con la privacidad Herramientas de monitorización de la preservación de la privacidad
MÉTRICAS	Evaluación y métricas de privacidad
ÁREAS DE INTERÉS	Criptografía Criptografía post-cuántica Fog Computing Cloud Computing Data mining Seguridad en Big Data

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES AÑO 2021

J. Domingo-Ferrer, K. Muralidhar and M. Bras-Amoròs, "General confidentiality and utility metrics for privacy-preserving data publishing based on the permutation model'", IEEE Transactions on Dependable and Secure Computing. To Appear.

M. Bamiloshin, A. Ben-Efraim and C. Padró, "Common Information, Matroid Representation, and Secret Sharing for Matroid Ports", Designs, Codes and Cryptography. To Appear.

O. Farràs, "Secret Sharing Schemes for Ports of Matroids of Rank 3", Kybernetika, Vol. , Feb 2021, ISSN: 0023-5954.

J. Domingo-Ferrer, D. Sánchez and A. Blanco-Justicia, "The limits of differential privacy (and its misuse in data release and machine learning)", Communications of the ACM. To Appear.

PUBLICACIONES AÑO 2020

J. Domingo-Ferrer and A. Blanco-Justicia, "Ethical Value-Centric Cybersecurity: A Methodology Based on a Value Graph", Science and Engineering Ethics, Vol. 11713, no. 11, pp. 1267-1285, Jun 2020, ISSN: 1353-3452.

O. Farràs, T. Kaced, S. Martín Molleví and C. Padró, "Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing", IEEE Transactions on Information Theory, Vol. 66, no. 11, pp. 7088-7100, Jun 2020, ISSN: 0018-9448.

D. Pàmies-Estrems, J. Castellà-Roca and J. Garcia-Alfaro, "A Real-Time Query Log Protection Method for Web Search Engines", IEEE Access, Vol. 8, pp. 87393-87413, May 2020, ISSN: 2169-3536.

A. Blanco-Justicia, J. Domingo-Ferrer, S. Martínez and D. Sánchez, "Machine learning explainability via microaggregation and shallow decision trees", Knowledge-Based Systems, Vol. 194, no. 105532, Apr 2020, ISSN: 0950-7051

M. Batet and D. Sánchez, "Leveraging synonymy and polysemy to improve semantic similarity assessments based on intrinsic information content", Artificial Intelligence Review, Vol. 53, pp. 2023-2041, Mar 2020, ISSN: 0269-2821.

D. Sánchez, S. Martínez, J. Domingo-Ferrer, J. Soria-Comas and M. Batet, "μ-ANT: semantic microaggregation-based anonymization tool", Bioinformatics, Vol. 36, no. 5, pp. 1652-1653, Mar 2020, ISSN: 1367-4803.

J. Domingo-Ferrer, D. Sánchez, S. Ricci and M. Muñoz-Batista, "Outsourcing Analyses on Privacy-Protected Multivariate Categorical Data Stored in Untrusted Clouds", Knowledge and Information Systems, Vol. 62, pp. 2301-2326, Feb 2020, ISSN: 0219-1377.

A. Viejo and D. Sánchez, "Secure monitoring in IoT-based services via fog orchestration", Future Generation Computer Systems, Vol. 107, pp. 443-457, Feb 2020, ISSN: 0167-739X.

J. Parra-Arnau, J. Domingo-Ferrer and J. Soria-Comas, "Differentially Private Data Publishing via Cross-Moment Microaggregation", Information Fusion, Vol. 53, pp. 269-288, Jan 2020, ISSN: 1566-2535.

A. Beimel and O. Farràs, "The Share Size of Secret-Sharing Schemes for Almost All Access Structures and Graphs", Theory of Cryptography Conference - TCC2020, Nov 2020.

J. Domingo-Ferrer, A. Blanco-Justicia, D. Sánchez and N. Jebreel, "Co-utile peer-to-peer decentralized computing", CCGRID2020, Melbourne, Australia, In Proceedings of 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing - CCGrid 2020, pp. 31-40, ISBN: 978-1-7281-6095-5, Jun 2020.

PUBLICACIONES AÑO 2019

O. Farràs and J. Ribes-González, "Provably secure public-key encryption with conjunctive and subset keyword search", International Journal of Information Security, Vol. 18, no. 5, pp. 533-548, Oct 2019, ISSN: 1615-5262.

J. Domingo-Ferrer, J. Soria-Comas and R. Mulero-Vellido, "Steered microaggregation as a unified primitive to anonymize data sets and data streams", IEEE Transactions on Information Forensics and Security, Vol. 14, no. 12, pp. 3298-3311, Oct 2019, ISSN: 1556-6013.

J. Domingo-Ferrer, O. Farràs, J. Ribes-González and D. Sánchez, "Privacy-preserving cloud computing on sensitive data: a survey of methods, products and challenges'", Computer Communications, Vol. 140, pp. 38-60, May 2019, ISSN: 0140-3664.

A. Viejo and D. Sánchez, "Secure and privacy-preserving orchestration and delivery of fog-enabled IoT services", Ad Hoc Networks, Vol. 82, pp. 113-125, Jan 2019, ISSN: 1570-8705.

M. Rodriguez-Garcia, M. Batet and D. Sánchez, "Utility-preserving privacy protection of nominal data sets via semantic rank swapping", Information Fusion, Vol. 45, pp. 282-295, Jan 2019, ISSN: 1566-2535.

J. Soria-Comas, J. Domingo-Ferrer and R. Mulero, "Efficient near-optimal variable-size microaggregation", Modeling Decisions for Artificial Intelligence-MDAI 2019, Milan, Italy, In Lecture Notes in Computer Science vol. 11676, pp. 333-345, ISBN: 0302-9743, Sep 2019.

J. Soria-Comas and J. Domingo-Ferrer, "Mitigating the curse of dimensionality in data anonymization", Modeling Decisions for Artificial Intelligence-MDAI 2019, Milan, Italy, In Lecture Notes in Computer Science vol. 11676, pp. 346-355, ISBN: 0302-9743, Sep 2019.

A. Blanco-Justicia and J. Domingo-Ferrer, "Machine learning explainability through comprehensible decision trees", CD-MAKE 2019, Canterbury, England, In Lecture Notes in Computer Science vol. 11713, pp. 15-26, ISBN: 0302-9743, Aug 2019.

F. Hassan, D. Sánchez, J. Soria-Comas and J. Domingo-Ferrer, "Automatic Anonymization of Textual Documents: Detecting Sensitive Information via Word Embeddings", 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom2019), Roturoa, New Zealand, Aug 2019.

J. Domingo-Ferrer, "Personal big data, GDPR and anonymization", Flexible Query Answering Systems-FQAS 2019, Amantea, Italy, In Lecture Notes in Computer Science vol. 11529, pp. 7-10, ISBN: 0302-9743, Jul 2019.

C. Anglès-Tafalla, S. Ricci, P. Dzurenda, J. Hajny, J. Castellà-Roca, and A. Viejo, "Decentralized privacy-preserving access for low emission zones", SECRYPT 2019, Prague, Czech Republic, In Proceedings of the 16th International Joint Conference on e-Business and Telecommunications - Volume 2: SECRYPT, pp. 485-491, ISBN: 978-989-758-378-0, Jul 2019.

J. Domingo-Ferrer, C. Pérez-Solà and A. Blanco-Justicia, "Collaborative explanation of deep models with limited interaction for trade secret and privacy preservation", 1st Workshop on Fairness, Accountability, Transparency, Ethics and Society on the Web-FATES 2019, San Francisco, USA, In Companion Proceedings of The 2019 World Wide Web Conference - WWW2019, ACM, pp. 501-507, ISBN: 978-1-4503-6675-5, May 2019.

C. Angles-Tafalla. J. Castellà-Roca and A. Viejo, "Privacy-Preserving and Secure Decentralized Access Control System for Low Emission Zones", IEEE INFOCOM 2019, Paris, France, In IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), ISBN: 978-1-7281-1879-6, May 2019.

B. Applebaum, A. Beimel, O. Farràs, O. Nir and N. Peter, "Secret-Sharing Schemes for General and Uniform Access Structures", Advances in Cryptology – EUROCRYPT 2019, Darmstad, (Germany, In Lecture Notes in Computer Science vol. 11478, pp. 441-471, ISBN: 0302-9743, Apr 2019.

PUBLICACIONES AÑO 2018

M. Bras-Amorós and J. Fernández-González, "Computation of Numerical Semigroups by Means of Seeds", Mathematics of Computation, Vol. 87, pp. 2539-2550, Dec 2018, ISSN: 0025-5718.

J. Castellà-Roca, M. Mut-Puigserver, M. M. Payeras-Capella, A. Viejo, and C. Anglès-Tafalla, "Secure and privacy-preserving lightweight access control system for low emission zones", Computer Networks, Vol. 145, pp. 13-26, Nov 2018, ISSN: 1389-1286.

D. Sánchez and A. Viejo, "Privacy-preserving and advertising-friendly web surfing", Computer Communications, Vol. 130, pp. 113-123, Oct 2018, ISSN: 0140-3664.

D. Sánchez, M. Batet, A. Viejo, M. Rodriguez-Garcia and J. Castellà-Roca, "A semantic-preserving differentially private method for releasing query logs", Information Sciences, Vol. 460, pp. 223-237, Sep 2018, ISSN: 0020-0255.

M. Batet and D. Sánchez, "Semantic disclosure control: semantics meets data privacy", Online Information Review, Vol. 42, no. 3, pp. 290-303, Jun 2018, ISSN: 1468-4527.

J. Domingo-Ferrer, A. Blanco-Justicia and C. Ràfols, "Dynamic group size accreditation and group discounts preserving anonymity", International Journal of Information Security, Vol. 17, no. 3, pp. 243-260, May 2018, ISSN: 1615-5262.

D. Sánchez, J. Domingo-Ferrer and S. Martínez, "Co-utile disclosure of private data in social networks", Information Sciences, Vol. 441, pp. 50-60, May 2018, ISSN: 0020-0255.

A. Blanco-Justicia and J.Domingo-Ferrer, "Efficient privacy-preserving implicit authentication", Computer Communications, Vol. 125, pp. 13-23, May 2018, ISSN: 0140-3664.

J. Domingo-Ferrer, S. Ricci and C. Domingo-Enrich, "Outsourcing scalar products and matrix products on privacy-protected unencrypted data stored in untrusted clouds", Information Sciences, Vol. 436, pp. 320-342, Apr 2018, ISSN: 0020-0255.

PUBLICACIONES RELACIONADAS DESTACADAS

J. Soria-Comas and J.Domingo-Ferrer, "Differentially Private Data Publishing via Optimal Univariate Microaggregation and Record Perturbation", Knowledge-Based Systems, Vol. 153, pp. 78-90, Apr 2018, ISSN: 0950-7051.

R. Jardí-Cedó, M. Mut-Puigserver, M. Magdalena Payeras-Capellà, J. Castellà-Roca, A. Viejo, "Time-based Low Emission Zones Preserving Drivers' Privacy", Future Generation Computer Systems, Vol. 80, pp. 558-571, Mar 2018, ISSN: 0167-739X.

M. Bras-Amorós, "A Decoding Approach to Reed-Solomon Codes from Their Definition", American Mathematical Monthly, Vol. 125, no. 4, pp. 320-338, Mar 2018, ISSN: 0002-9890.

D. Sánchez, L. Martínez-Sanahuja, M. Batet, "Survey and evaluation of Web search engine hit counts as research tools in computational linguistics", Information Systems, Vol. 73, pp. 50-60, Mar 2018, ISSN: 0306-4379.

O. Farràs, T. Kaced, S. Martín and C. Padró, "Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing", 37th Annual Eurocrypt Conference - EUROCRYPT 2018, Tel Aviv, Israel, In Lecture Notes in Computer Science vol. 10820, pp. 597-621, ISBN: 0302-9743, May 2018.

J. Domingo-Ferrer, "Big data anonymization requirements vs privacy models", ICETE2018, Porto, Portugal, In 15th International Joint Conference on e-Business and Telecommunications-ICETE 2018-Volume 2: SECRYPT 2018, pp. 471-478, ISBN: 978-989-758-319-3, Jul 2018.

F. Hassan, J. Domingo-Ferrer and J.Soria-Comas, "Anonymization of Unstructured Data via Named-Entity Recognition", Modeling Decisions for Artificial Intelligence - 2018, Mallorca (Spain), In Lecture Notes in Computer Science vol. 11144, pp. 296-305, ISBN: 0302-9743, Oct 2018.

J. Domingo-Ferrer, R. Mulero-Vellido and J.Soria-Comas, "Multiparty Computation with Statistical Input Confidentiality via Randomized Response", Privacy in Statistical Databases - PSD 2018, Valencia (Spain), In Lecture Notes in Computer Science vol. 11126, pp. 175-186, ISBN: 0302-9743, Sep 2018.

N. Ruiz, K. Muralidhar and J. Domingo-Ferrer, "On the privacy Guarantees of Synthetic Data: A Reassessment from the Maximum-knowledge Attacker Perspective", Privacy in Statistical Databases - PSD 2018, Valencia (Spain), In Lecture Notes in Computer Science vol. 11126, pp. 59-74, ISBN: 0302-9743, Sep 2018.

PUBLICACIONES AÑO 2017

O. Farràs, T. Hansen, T. Kaced and C. Padró, "On the Information Ratio of Non-Perfect Secret Sharing Schemes", Algorithmica, Vol. 79, no. 4, pp. 987-103, Dec 2017, ISSN: 0178-4617.

M. M. Payeras-Capellà, M. Mut-Puigserver, J. Castellà-Roca and J. Bondia-Barceló, "Design and Performance Evaluation of Two Approaches to Obtain Anonymity in Transferable Electronic Ticketing Schemes", Mobile Networks and Applications, Vol. 22, no. 6, pp. 1137-1156, Dec 2017, ISSN: 1383-469X.

D.Sánchez and M. Batet, "Privacy-preserving data outsourcing in the cloud via semantic data splitting", Computer Communications, Vol. 110, pp. 187-201, Sep 2017, ISSN: 0140-3664.

J. Soria-Comas, J. Domingo-Ferrer, D. Sánchez and D. Megías, "Individual differential privacy: a utility-preserving formulation of differential privacy guarantees", IEEE Transactions on Information Forensics and Security, Vol. 12, no. 6, pp. 1418-1429, Jun 2017, ISSN: 1556-6013.

D. Sánchez and A. Viejo, "Personalized privacy in open data sharing scenarios", Online Information Review, Vol. 41, no. 3, pp. 298-310, Apr 2017, ISSN: 1468-4527.

M. Rodríguez-García, M. Batet and D. Sánchez, "A semantic framework for noise addition with nominal data", Knowledge-Based Systems, Vol. 122, pp. 103-118, Apr 2017, ISSN: 0950-7051.

A. Ngusi-Turi, J. Domingo-Ferrer, D. Sánchez and D. Osmani, "A co-utility approach to the mesh economy: the crowd-based business model", Review of Managerial Science, Vol. 11, no. 2, pp. 411-442, Mar 2017, ISSN: 1863-6683.

J. Domingo-Ferrer, S. Martínez, D. Sánchez and J. Soria-Comas, "Co-utility: self-enforcing protocols for the mutual benefit of participants", Engineering Applications of Artificial Intelligence, Vol. 59, pp. 148-158, Mar 2017, ISSN: 0952-1976.

D. Sánchez and M. Batet, "Toward sensitive document release with privacy guarantees", Engineering Applications of Artificial Intelligence, Vol. 59, pp. 23-34, Mar 2017, ISSN: 0952-1976.

J. Domingo-Ferrer and J. Soria-Comas, "Steered Microaggregation: A Unified Primitive for Anonymization of Data Sets and Data Streams", 10th International Workshop on Privacy and Anonymity in the Information Society-PAIS 2017, New Orleans (USA), In IEEE ICDM 2017 Workshops Proceedings, pp. 995-1002, ISBN: 978-1-5386-3800-2, Nov 2017.

J. Alderman, B. R. Curtis, O. Farràs, K. M. Martin, and J. Ribes-González, "Private Outsourced Kriging Interpolation", Financial Cryptography and Data Security - FC 2017, Sliema (Malta), In Lecture Notes in Computer Science vol. 10323, pp. 75-90, ISBN: 0302-9743, Nov 2017

I. Cascudo, I. Damgärd, O. Farràs and S. Ranellucci, "Resource-efficient OT combiners with active security", Theory of Cryptography - TCC 2017, Baltimore, USA, In Lecture Notes in Computer Science vol. 10678, pp. 461-486, ISBN: 0302-9743, Nov 2017.

A. Beimel, O. Farràs, Y. Mintz and N. Peter, "Linear Secret-Sharing Schemes for Forbidden Graph Access Structures", Theory of Cryptography - TCC 2017, Baltimore, USA, In Lecture Notes in Computer Science vol. 10678, pp. 394-423, ISBN: 0302-9743, Nov 2017.

J. Domingo-Ferrer, S. Ricci and J. Soria-Comas, "A methodology to compare anonymization methods regarding their risk-utility trade-off", Modeling Decisions for Artificial Intelligence-MDAI 2017, Kitakyushu, Japan, In Lecture Notes in Computer Science vol. 10571, pp. 132-143, ISBN: 0302-9743, Oct 2017.

J. Castellà-Roca, M. Mut-Puigserver, M. M. Payeras-Capellà, A. Viejo and C.Anglès-Tafalla, "Secure and Anonymous Vehicle Access Control System to Traffic-Restricted Urban Areas", 3rd International Workshop on Vehicular Networking and Intelligent Transportation Systems - VENITS2017, Vancouver (Canada), Aug 2017.

J. Domingo-Ferrer, "Privacy-preserving and co-utile distributed social credit", IWOCA 2017- 28th International Workshop on Combinatorial Algorithms, Newcastle, Australia, In Lecture Notes in Computer Science vol. 10765, pp. 371-382, ISBN: 0302-9743, Jul 2017.

J. Soria-Comas and J. Domingo-Ferrer, "Differentially private data sets based on microaggregation and record perturbation", Modeling Decisions for Arti cial Intelligence-MDAI 2017, Kitakyushu, Japan, In Lecture Notes in Computer Science vol. 10571, pp. 119-131, ISBN: 0302-9743, Oct 2017.

J. Soria-Comas and J. Domingo-Ferrer, "A non-parametric model for accurate and provably private synthetic data sets", International Conference on Availability, Reliability and Security - ARES 2017, Reggio Calabria, Italy, Aug 2017. Best paper award.

PUBLICACIONES AÑO 2016

D. Pàmies-Estrems, J. Castellà-Roca and A. Viejo, "Working at the Web Search Engine Side to Generate Privacy-Preserving User Profiles", Expert Systems with Applications, Vol. 64, pp. 523-535, Dec 2016, ISSN: 0957-4174.

. Domingo-Ferrer, O. Farràs, S. Martínez, D. Sánchez and J. Soria-Comas, "Self-enforcing protocols via co-utile reputation management", Information Sciences, Vol. 367, pp. 159-175, Nov 2016, ISSN: 0020-0255.

D. Sánchez, S. Martínez and J. Domingo-Ferrer , "Co-utile P2P ridesharing via decentralization and reputation management", Transportation research part C - Emerging technologies, Vol. 73, pp. 147-166, Nov 2016, ISSN: 0968-090X.

R. Jardí-Cedó, J. Castellà-Roca and A. Viejo, "Privacy-Preserving Electronic Road Pricing System for Low Emission Zones with Dynamic Pricing", Security and Communication Networks, Vol. 9, pp. 3197-3218, Nov 2016, ISSN: 1939-0114.

A. Blanco-Justicia and J. Domingo-Ferrer, "Privacy-aware loyalty programs", Computer Communications, Vol. 82, pp. 83-94, May 2016, ISSN: 0140-3664.

A. Beimel, O. Farràs and Y. Mintz, "Secret-Sharing Schemes for Very Dense Graphs", Journal of Cryptology, Vol. 29, no. 2, pp. 336-362, Apr 2016, ISSN: 0933-2790.

J. Domingo-Ferrer and K. Muralidhar, "New directions in anonymization: permutation paradigm, verifiability by subjects and intruders, transparency to users", Information Sciences, Vol. 337, pp. 11-24, Apr 2016, ISSN: 0020-0255.

D. Sánchez, S. Martínez and J. Domingo-Ferrer, "Comment on 'Unique in the shopping mall: On the reidentifiability of credit card metadata'", Science, Vol. 351, Special issue, pp. 1274-1274, Mar 2016, ISSN: 0036-8075.

M.Imran-Daud, D. Sánchez, A. Viejo, "Privacy-driven access control in social networks by means of automatic semantic annotation", Computer Communications, Vol. 76, pp. 12-25, Feb 2016, ISSN: 0140-3664.

Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farràs and J. Manjón, "Contributory broadcast encryption with efficient encryption and short ciphertexts", IEEE Transactions on Computers, Vol. 65, no. 2, pp. 466-479, Jan 2016, ISSN: 0018-9340 .

A. Viejo and D. Sánchez, "Enforcing Transparent Access to Private Content in Social Networks by Means of Automatic Sanitization", Expert Systems with Applications, Vol. 62, pp. 148-160, Jan 2016, ISSN: 0957-4174.

D. Sánchez and M. Batet, "C-sanitized: A privacy model for document redaction and sanitization", Journal of the Association for Information Science and Technology, Vol. 67, no. 1, pp. 148-163, Jan 2016, ISSN: 1532-2882.

D. Sánchez, J. Domingo-Ferrer, S. Martínez, and J. Soria-Comas, "Utility-Preserving Differentially Private Data Releases Via Individual Ranking Microaggregation", Information Fusion, Vol. 30, pp. 1-14, Jan 2016, ISSN: 1566-2535.

PUBLICACIONES RELACIONADAS DESTACADAS

A. Nigussie Turi, J. Domingo-Ferrer and D. Sánchez, "Filtering P2P loans based on co-utile reputation", 13th International Conference on Applied Computing - AC 2016, Mannheim, Germany, In IADIS Press, pp. 139-146, ISBN: 978-989-8533-56, Oct 2016.

K. Muralidhar and J. Domingo-Ferrer, "Rank-Based Record Linkage for Re-Identification Risk Assessment", Provacy in Statistical Databases - PSD2016, Dubrovnik, Croatia, In Lecture Notes in Computer Science vol. 9867, pp. 225-236, ISBN: 0302-9743, Sep 2016.

J. Domingo-Ferrer and J. Soria-Comas, "Anonymization in the Time of Big Data", Privacy in Statistical Databases - PSD2016, Dubrovnik, Croatia, In Lecture Notes in Computer Science vol. 9867, pp. 57-68, ISBN: 0302-9743, Sep 2016.

M. Rodriguez-Garcia, D. Sánchez and M. Batet, "Perturbative data protection of multivariate nominal datasets", Privacy in Statistical Databases - PSD2016, Dubrovnik, Croatia, In Lecture Notes in Computer Science vol. 9867, pp. 94-106, ISBN: 0302-9743, Sep 2016.

M. Batet and D. Sánchez, "Improving Semantic Relatedness Assessments: Ontologies Meet Textual Corpora", International Conference on Knowledge-Based and Intelligent Information & Engineering Systems - KES 2016, York, UK, In Procedia Computer Science 96, pp. 365-374, ISBN: , Sep 2016.

L. Martínez-Sanahuja and D. Sánchez, "Evaluating the Suitability of Web Search Engines as Proxies for Knowledge Discovery from the Web", International Conference on Knowledge-Based and Intelligent Information & Engineering Systems - KES 2016, York (UK), Sep 2016.

J. Bondia-Barceló, J. Castellà-Roca and A. Viejo, "Building Privacy-Preserving Search Engine Query Logs for Data Monetization", 13th IEEE International Conference on Advanced and Trusted Computing - ATC'16, Toulouse, France, Jul 2016.

J. Domingo-Ferrer and D. Megías, "Co-utility for digital content protection and digital forgetting", MedHocNet 2016-15th Annual Mediterranean Ad Hoc Networking Workshop, Vilanova i la Geltrú, Jun 2016.

O. Farràs, "Recent Advances in Non-perfect Secret Sharing Schemes", CiE 2016: Pursuit of the Universal, Paris, France, In Lecture Notes in Computer Science vol. 9709, pp. 89-98, ISBN: 0302-9743, Jun 2016.

J. Soria-Comas, J. Domingo-Ferrer, D. Sánchez and S. Martínez, "t-Closeness through microaggregation: strict privacy with enhanced utility preservation (extended abstract)", 32nd IEEE International Conference on Data Engineering-ICDE 2016, Helsinki, Finland, In IEEE Computer Society, pp. 1464-1465, ISBN: 978-1-5090-2020, May 2016.

M. Imran-Daud, D. Sánchez and A. Viejo , "Ontology-based Access Control Management: Two Use Cases", ICAART 2016, Rome (Italy), In Proceedings of the 8th International Conference on Agents and Artificial Intelligence, pp. 244-249, ISBN: 978-989-758-172, Feb 2016.

A. Beimel, O. Farràs and N. Peter, "Secret Sharing Schemes for Dense Forbidden Graphs", SCN 2016: Security and Cryptography for Networks, Amalfi, Italy, In Lecture Notes in Computer Science vol. 9841, pp. 509-528, ISBN: 0302-9743, Aug 2016.

S. Ricci, J. Domingo-Ferrer and D. Sánchez, "Privacy-preserving cloud-based statistical analyses on sensitive categorical data", Modeling Decisions for Artificial Intelligence-MDAI 2016, Andorra, In Lecture Notes in Computer Science vol. 9880, pp. 227-238, ISBN: 0302-9743, Sep 2016.

PUBLICACIONES 2015

G. Karopoulos, G. Portokalidis, J. Domingo-Ferrer, Y. Lin, D. Geneiatakis and G. Kambourakis, "Security and privacy in unified communications: challenges and solutions", Computer Communications, Vol. 68, pp. 1-3, Dec 2015, ISSN: 0140-3664.

J. Soria-Comas, J. Domingo-Ferrer, D. Sánchez and S. Martínez, "t-Closeness through microaggregation: strict privacy with enhanced utility preservation", IEEE Transactions on Knowledge and Data Engineering, Vol. 27, no. 11, pp. 3098-3110, Oct 2015, ISSN: 1041-4347.

S. Hajian, J. Domingo-Ferrer, A. Monreale, D. Pedreschi and F. Giannotti, "Discrimination- and privacy-aware patterns", Data Mining and Knowledge Discovery, Vol. 29, no. 6, pp. 1733-1782, Sep 2015, ISSN: 1384-5810.

L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin and Z. Dong, "Round-efficient and sender-unrestricted dynamic group key agreement protocol for secure group communications", IEEE Transactions on Information Forensics and Security, Vol. 10, no. 11, pp. 2352-2364, Sep 2015, ISSN: 1556-6013.

L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer and B. Liu, "Practical secure and privacy-preserving scheme for value-added applications in VANETs", Computer Communications, Vol. 71, pp. 50-60, Dec 2015, ISSN: 0140-3664.

M. Bras-Amorós and M. Pujol, "Side Lengths of Equiangular Polygons (as seen by a coding theorist)", American Mathematical Monthly, Vol. 122, no. 5, pp. 476-478, May 2015, ISSN: 0002-9890.

L. Malina, A. Vives-Guasch, J. Castellà-Roca, A. Viejo, J. Hajny, "Efficient Group Signatures for Privacy-Preserving Vehicular Networks", Telecommunication Systems, Vol. 58, no. 4, pp. 293-311, Apr 2015, ISSN: 1018-4864.

F. Casino, J. Domingo-Ferrer, C. Patsakis, D. Puig and A. Solanas, "A k-anonymous approach to privacy preserving collaborative filtering", Journal of Computer and System Sciences, Vol. 81, no. 6, pp. 1000-1011, Apr 2015, ISSN: 0022-0000.

D. Sánchez, M. Batet, S. Martínez and J. Domingo-Ferrer, "Semantic variance: An intuitive measure for ontology accuracy evaluation", Engineering Applications of Artificial Intelligence, Vol. 39, pp. 89-99, Mar 2015, ISSN: 0952-1976.

O. Farràs and C. Padró, "Extending Brickell-Davenport Theorem to Non-Perfect Secret Sharing Schemes", Designs, Codes and Cryptography, Vol. 74, no. 2, pp. 495-510, Feb 2015, ISSN: 0925-1022.

C. Romero-Tris, D. Castellà, A. Viejo, J. Castellà-Roca, F. Solsona, J. M. Mateo-Sanz, "Design of a P2P network that protects users' privacy in front of Web Search Engines", Computer Communications, Vol. 57, pp. 37-49, Feb 2015, ISSN: 0140-3664.

J. Domingo-Ferrer and J. Soria-Comas, "From t-closeness to differential privacy and vice versa in data anonymization", Knowledge-Based Systems, Vol. 74, pp. 151-158, Jan 2015, ISSN: 0950-7051.

M. Rodriguez-Garcia, M. Batet and D. Sánchez, "Semantic Noise: Privacy-protection of Nominal Microdata through Uncorrelated Noise Addition", 27th International Conference on Tools with Artificial Intelligence - ICTAI 2015, Vietri Sul Mare, Italy, Nov 2015.

A. Turi, J. Domingo-Ferrer, D. Sánchez and D. Osmani, "Co-Utility: Conciliating Individual Freedom and Common Good for the Crowd-based Business Model", 2015 IEEE Intl. Conf. on e-Business Engineering (ICEBE 2015), Beijing, China, Nov 2015.

J. Domingo-Ferrer, S. Ricci and J. Soria-Comas, "Disclosure risk assessment via record linkage by a maximum-knowledge attacker", 13th Annual International Conference on Privacy, Security and Trust-PST 2015, Izmir, Turkey, Sep 2015.

J. Soria-Comas and J. Domingo-Ferrer, "Co-utile collaborative anonymization of microdata", Modeling Decisions for Artificial Intelligence-MDAI 2015, Skövde, Sweden, In Lecture Notes in Computer Science vol. 9321, pp. 192-206, ISBN: 0302-9743, Sep 2015

A. Calviño, S. Ricci and J. Domingo-Ferrer, "Privacy-preserving distributed statistical computation to a semi-honest multi-cloud", 1st IEEE Workshop on Security and Privacy in the Cloud-SPC 2015, Florence, Italy, Sep 2015.

M.I. Daud, D. Sánchez, A. Viejo, "Ontology-Based Delegation of Access Control: An Enhancement to the XACML Delegation Profile", Trust, Privacy and Security in Digital Business - 12th International Conference, TrustBus 2015, Valencia, Spain, In Lecture Notes in Computer Science vol. 9264, pp. 18-29, ISBN: 0302-9743, Aug 2015.

J. Domingo-Ferrer and J. Soria-Comas, "Data anonymization", Risks and Security of Internet and Systems - CRISIS 2014, Trento, Italy, In Lecture Notes in Computer Science vol. 8924, pp. 267-271, ISBN: 0302-9743, Jun 2015.

J. Domingo-Ferrer, Q. Wu and A. Blanco, "Flexible and robust privacy-preserving implicit authentication", IFIP SEC 2015-Intl. Information Security and Privacy Conference, Hamburg, Germany, In IFIP AICT 455, Springer, pp. 18-34, ISBN: 978-3-319-18466, May 2015.

J. Domingo-Ferrer, J. Soria-Comas and O. Ciobotaru, "Co-utility: self-enforcing protocols without coordination mechanisms", IEOM 2015, Dubai, United Arab Emirates, In Proceedings of the 2015 International Conference on Industrial Engineering and Operations Management, IEEE, pp. 1-17, ISBN: 978-1-4799-6064, Mar 2015.

M. Batet and D. Sánchez, "Ontology Selection for Semantic Similarity Assessment", International Conference on Agents and Artificial Intelligence - ICAART'15, Lisbon, Portugal, Jan 2015.

D. Sánchez, A. Viejo, "Privacy Risk Assessment of Textual Publications in Social Networks", International Conference on Agents and Artificial Intelligence - ICAART'15, Lisboa, Portugal, Jan 2015.

R. Jardí-Cedó, J. Castellà-Roca, A. Viejo, "Privacy-Preserving Electronic Toll System with Dynamic Pricing for Low Emission Zones", DPM/SETOP/QASA 2014, Wroclaw, Poland, In Lecture Notes in Computer Science vol. 8872, pp. 327-334, ISBN: 0302-9743, Feb 2015.

PUBLICACIONES AÑO 2014

D. Sánchez, M. Batet, A. Viejo, "Utility-Preserving Privacy Protection of Textual Healthcare Documents", Journal of Biomedical Informatics, Vol. 52, pp. 189-198, Dec 2014, ISSN: 1532-0464.

M. Bras-Amorós, K. Lee and A. Vico-Oton, "New Lower Bounds on the Generalized Hamming Weights of AG Codes", IEEE Transactions on Information Theory, Vol. 60, no. 10, pp. 5930-5937, Oct 2014, ISSN: 0018-9448.

J. Soria-Comas, J. Domingo-Ferrer, D. Sánchez and S. Martínez, "Enhancing data utility in differential privacy via microaggregation-based k-anonymity", The VLDB Journal, Vol. 23, no. 5, pp. 771-794, Sep 2014, ISSN: 1066-8888.

PUBLICACIONES RELACIONADAS DESTACADAS

D. Sánchez, M. Batet, A. Viejo, "Utility-Preserving Sanitization of Semantically Correlated Terms in Textual Documents", Information Sciences, Vol. 279, pp. 77-93, Sep 2014, ISSN: 0020-0255.

S. Hajian, J. Domingo-Ferrer and O. Farràs, "Generalization-based privacy preservation and discrimination prevention in data publishing and mining", Data Mining and Knowledge Discovery, Vol. 28, no. 5, pp. 1158-1188, Aug 2014, ISSN: 1384-5810.

H. Wang, Q. Wu, B. Qin, J. Domingo-Ferrer, "FRR: Fair Remote Retrieval of Outsourced Private Medical Records in Electronic Health Networks", Journal of Biomedical Informatics, Vol. 50, pp. 226-233, Aug 2014, ISSN: 1532-0464.

R. Di Pietro, S. Guarino, N. V. Verde and J. Domingo-Ferrer, "Security in wireless ad-hoc networks - A survey", Computer Communications, Vol. 51, pp. 1-20, Jul 2014, ISSN: 0140-3664.

C. Romero-Tris, J. Castellà-Roca, A. Viejo, "Distributed System for Private Web Search with Untrusted Partners", Computer Networks, Vol. 67, pp. 26-42, Jul 2014, ISSN: 1389-1286.

K.Stokes and O.Farràs, "Linear spaces and transversal designs: k-anonymous combinatorial configurations for anonymous database search", Designs, Codes and Cryptography, Vol. 71, no. 3, pp. 503-524, Jun 2014, ISSN: 0925-1022.

A. Viejo and D. Sánchez, "Profiling Social Networks to Provide Useful and Privacy-Preserving Web Search", Journal of the Association for Information Science and Technology, Vol. 65, no. 12, pp. 2444-2458, May 2014, ISSN: 1532-2882.

L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin and P. Zheng, "Signatures in hierarchical certificateless cryptography: efficient constructions and provable security", Information Sciences, Vol. 272, pp. 223-237, May 2014, ISSN: 0020-0255.

K. Lee, M. Bras-Amorós, M. E. O'Sullivan, "Unique Decoding of General AG Codes ", IEEE Transactions on Information Theory, Vol. 60, no. 4, pp. 2038-2053, Apr 2014, ISSN: 0018-9448.

O. Farràs, C. Padró, C. Xing and A. Yang, "Natural Generalizations of Threshold Secret Sharing", IEEE Transactions on Information Theory, Vol. 60, no. 3, pp. 1652-1664, Mar 2014, ISSN: 0018-9448.

D. Megías and J. Domingo-Ferrer, "Privacy-Aware Peer-to-Peer Content Distribution Using Automatically Recombined Fingerprints", Multimedia Systems, Vol. 20, no. 2, pp. 105-125, Feb 2014, ISSN: 0942-4962.

K. Stokes, M. Bras-Amorós, "Linear, non-homogeneous, symmetric patterns and prime power generators in numerical semigroups associated to combinatorial configurations", Semigroup Forum, Vol. 88, no. 1, pp. 11-20, Feb 2014, ISSN: 0037-1912.

M. Bras-Amorós and A. Vico-Oton, "On the Geil-Matsumoto Bound and the Length of AG codes", Designs, Codes and Cryptography, Vol. 70, no. 1, pp. 117-125, Jan 2014, ISSN: 0925-1022.

M. Batet and D. Sánchez, "A Semantic Approach for Ontology Evaluation", IEEE International Conference on Tools with Artificial Intelligence - ICTAI 2014, Limassol, Cyprus, Nov 2014.

R. Jardí-Cedó, M. Mut-Puigserver, M. M. Payeras-Capella, J. Castellà-Roca, A. Viejo, "Electronic Road Pricing System for Low Emission Zones to Preserve Driver Privacy", 11th Internacional Conference on Modeling Decisions for Artificial Intelligence - MDAI'14, Tokyo, Japan, In Lecture Notes in Computer Science vol. 8825, pp. 1-13, ISBN: 0302-9743, Oct 2014.

D. Sánchez, J. Domingo-Ferrer and S. Martínez, "Improving the Utility of Differential Privacy via Univariate Microaggregation", Privacy in Statistical Databases - PSD2014, Eivissa, Spain, In Lecture Notes in Computer Science vol. 8744, pp. 130-142, ISBN: 0302-9743, Sep 2014.

K. Muralidhar, R. Sarathy and J. Domingo-Ferrer, "Reverse mapping to preserve the marginal distributions of attributes in masked microdata", Privacy in Statistical Databases - PSD 2014, Eivissa, Spain, In Lecture Notes in Computer Science vol. 8744, pp. 105-116, ISBN: 0302-9743, Sep 2014.

J. Domingo-Ferrer and A. Blanco-Justicia, "Group discounts compatible with buyer privacy", DPM/SETOP/QASA 2014, Wroclaw, Poland, In Lecture Notes in Computer Science vol. 8872, pp. 47-57, ISBN: 0302-9743, Sep 2014.

A. Blanco-Justicia and J. Domingo-Ferrer, "Privacy-preserving loyalty programs", DPM/SETOP/QASA 2014, Wroclaw, Poland, In Lecture Notes in Computer Science vol. 8872, pp. 133-146, ISBN: 0302-9743, Sep 2014.

O. Farràs, T. Hansen, T. Kaced and C. Padró, "Optimal Non-Perfect Uniform Secret Sharing Schemes", Advances in Cryptology - Crypto 2014, Santa Barbara, USA, In Lecture Notes in Computer Science vol. 8617, pp. 217-234, ISBN: 0302-9743, Aug 2014.

A. Vives-Guasch, M. M. Payeras-Capellà, M. Mut-Puigserver, J. Castellà-Roca and J.L. Ferrer-Gomila, "Anonymous and Transferable Electronic Ticketing Scheme", DPM 2013 and SETOP 2013, Egham, UK, In Lecture Notes in Computer Science vol. 8247, pp. 100-113, ISBN: 0302-9743, Jun 2014.

A. Erola and J.Castellà-Roca, "Using search results to microaggregate query logs semantically", DPM2013 - SETOP 2013, Egham, UK, In Lecture Notes in Computer Science vol. 9847, pp. 148-161, ISBN: 0302-9743, Jun 2014.

A. Blanco, J. Domingo-Ferrer, O. Farràs and D. Sánchez, "Distance computation between two private preference functions", IFIP International Information Security and Privacy Conference - SEC 2014, Marrakech, Morocco, In IFIP AICT 428, pp. 460-470, ISBN: 978-3-642-55414, Jun 2014.

M. Batet and D. Sánchez, "Privacy protection of textual medical documents", Network Operations and Management Symposium - NOMS 2014, Krakow, Poland, In Network Operations and Management Symposium (NOMS), 2014 IEEE, pp. 1-6, ISBN: , May 2014.

A. Zigomitros, A. Solanas and C. Patsakis, "The role of inference in the anonymization of medical records", 27th International Symposium on Computer-based Medical Systems (IEEE CBMS 2014), New York, USA, May 2014.

M. Batet, A. Erola, D. Sánchez and J. Castellà-Roca, "Semantic Anonymisation of Set-valued Data", 6th International Conference on Agents and Artificial Intelligence - ICAART 2014, Angers, France, Mar 2014.

B. Liu, L. Zhang and J. Domingo-Ferrer, "On the security of a privacy-preserving key management scheme for location based services in VANETs", Foundations and Practice of Security - FPS 2013, La Rochelle (France), In Lecture Notes in Computer Science vol. 8352, pp. 323-335, ISBN: 0302-9743, Mar 2014.

O. Farràs, J. Domingo-Ferrer and A. Blanco-Justicia, "Privacy-Preserving Trust Management Mechanisms from Private Matching Schemes", 8th DPM International Workshop on Data Privacy Management - DPM2013, Egham, UK, In Lecture Notes in Computer Science vol. 8247, pp. 390-398, ISBN: 0302-9743, Mar 2014.

S. Hajian, A. Monreale, D. Pedreschi, J. Domingo-Ferrer and F. Giannotti, "Fair pattern discovery", 29th Symposium on Applied Computing - ACM SAC 2014, Gyeongju, Korea, Mar 2014.

PUBLICACIONES AÑO 2013

C. Patsakis and A. Solanas, "Privacy-Aware Event Data Recorders: Cryptography Meets the Automotive Industry Again", IEEE Communications Magazine, Vol. 51, no. 12, pp. 122-128, Dec 2013, ISSN: 0163-6804.

B. Qin, H. Wang, Q. Wu, J. Liu and J. Domingo-Ferrer, "Simultaneous authentication and secrecy in identity-based data upload to cloud", Cluster Computing, Vol. 16, no. 4, pp. 845-859, Nov 2013, ISSN: 1386-7857.

D. Sánchez, M.Batet and A. Viejo, "Minimizing the Disclosure Risk of Semantic Correlations in Document Sanitization", Information Sciences, Vol. 249, pp. 110-123, Nov 2013, ISSN: 0020-0255.

A. Pere Isern-Deyà, A. Vives-Guasch, M. Mut-Puigserver, M Payeras-Capellà and J. Castellà-Roca, "A Secure Automatic Fare Collection System for Time-based or Distance-based Services with Revocable Anonymity for Users", Computer Journal, Vol. 56, no. 10, pp. 1198-1215, Oct 2013, ISSN: 0010-4620

A. Solanas, A. Martínez-Ballesté, Pablo A. Pérez-Martínez, A. Fernandez, and J. Ramos, "m-carer: Privacy-aware monitoring for people with mild cognitive impairment and dementia", IEEE Journal on Selected Areas in Communications, Vol. 31, no. 9, pp. 19-27, Sep 2013, ISSN: 0733-8716.

L. Zhang, Q. Wu and B. Qin, "Identity-Based Optimistic Fair Exchange in the Standard Model", Security and Communication Networks, Vol. 6, no. 8, pp. 1010-1020, Aug 2013, ISSN: 1939-0114.

J. Soria-Comas and J. Domingo-Ferrer, "Optimal data-independent noise for differential privacy", Information Sciences, Vol. 250, pp. 200-214, Aug 2013, ISSN: 0020-0255.

S. Hajian and J. Domingo-Ferrer, "A methodology for direct and indirect discrimination prevention in data mining", IEEE Transactions on Knowledge and Data Engineering, Vol. 25, no. 7, pp. 1445-1459, Jun 2013, ISSN: 1041-4347.

M. Batet, A. Erola, D. Sánchez and J. Castellà-Roca, "Utility preserving query log anonymization via semantic microaggregation", Information Sciences, Vol. 242, pp. 49-63, Jun 2013, ISSN: 0020-0255.

A. Martínez-Ballesté, P. Pérez and A. Solanas, "The Pursuit of Citizens Privacy: A Privacy-Aware Smart City is Possible", IEEE Communications Magazine, Vol. 51, no. 6, pp. 136-141, Jun 2013, ISSN: 0163-6804.

J. Domingo-Ferrer, D. Sánchez and G. Rufian-Torrell, "Anonymization of nominal data based on semantic marginality", Information Sciences, Vol. 242, pp. 35-48, May 2013, ISSN: 0020-0255.

PUBLICACIONES RELACIONADAS DESTACADAS

Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer and J. Manjón, "Fast Transmission to Remote Cooperative Groups: A New Key Management Paradigm", IEEE-ACM Transactions on Networking, Vol. 21, no. 2, pp. 621-633, Apr 2013, ISSN: 1063-6692.

A. Solanas, A. Martínez-Ballesté and J.M. Mateo-Sanz, "Distributed Architecture with Double-Phase Microaggregation for the Private Sharing of Biomedical Data in Mobile Health", IEEE Transactions on Information Forensics and Security, Vol. 8, no. 6, pp. 901-910, Apr 2013, ISSN: 1556-6013.

J. Domingo-Ferrer and D. Megías, "Distributed multicast of fingerprinted content based on a rational peer-to-peer community", Computer Communications, Vol. 36, no. 5, pp. 542-550, Mar 2013, ISSN: 0140-3664.

S. Martínez, D. Sánchez and A. Valls, "A semantic framework to protect the privacy of electronic health records with non-numerical attributes", Journal of Biomedical Informatics, Vol. 46, no. 2, pp. 294-303, Feb 2013, ISSN: 1532-0464.

D. Sánchez, M. Batet and A. Viejo, "Automatic general-purpose sanitization of textual documents", IEEE Transactions on Information Forensics and Security, Vol. 8, no. 6, pp. 853-862, Feb 2013, ISSN: 1556-6013.

D. Sánchez, J. Castellà-Roca, A. Viejo, "Knowledge-Based Scheme to Create Privacy-Preserving but Semantically-Related Queries for Web Search Engines", Information Sciences, Vol. 218, no. 1, pp. 17-30, Jan 2013, ISSN: 0020-0255.

D. Sánchez and M. Batet, "A semantic similarity method based on information content exploiting multiple ontologies", Expert Systems with Applications, Vol. 40, no. 4, pp. 1393-1399, Jan 2013, ISSN: 0957-4174.

R. Trujillo and J. Domingo-Ferrer, "On the privacy offered by k-d-anonymity", Information Systems, Vol. 38, no. 4, pp. 491-494, Jan 2013, ISSN: 0306-4379.

J. Domingo-Ferrer, "Facility location and social choice via microaggregation", Modeling Decisions for Artificial Intelligence-MDAI 2013, Barcelona, Spain, In Lecture Notes in Computer Science vol. 8234, pp. 49-57, ISBN: 0302-9743, Nov 2013.

C. Patsakis and A.Solanas, "Privacy as a Product: A case study in the m-Health", Fourth International Conference on Information, Intelligence, Systems and Applications - IISA 2013, Piraeus, Greece, Oct 2013.

A. Vives-Guasch, M. M. Payeras-Capellà, M. Mut-Puigserver, J. Castellà-Roca and J.L. Ferrer-Gomila, "Anonymous and Transferable Electronic Ticketing Scheme", 8th DPM International Workshop on Data Privacy Management - DPM2013, Egham, UK, Sep 2013.

A. Erola and J.Castellà-Roca, "Using search results to microaggregate query logs semantically", 8th DPM International Workshop on Data Privacy Management - DPM2013, Egham, UK, Sep 2013.

F. Casino, J. Domingo-Ferrer, C. Patsakis, D. Puig and A. Solanas, "Privacy Preserving Collaborative Filtering with k-Anonymity through Microaggregation", 10th IEEE International Conference on e-Business Engineering (ICEBE 2013), Coventry, United Kingdom, Sep 2013.

C. Patsakis and A. Solanas, "Trading Privacy in the Cloud: A Fairer Way to Share Private Information", 10th IEEE International Conference on e-Business Engineering (ICEBE 2013), Coventry, United Kingdom, Sep 2013.

F. Casino, C. Patsakis, D. Puig and A. Solanas, "On Privacy Preserving Collaborative Filtering: Current Trends, Open Problems, and New Issues", 10th IEEE International Conference on e-Business Engineering (ICEBE 2013), Coventry, United Kingdom, Sep 2013.

A. Viejo, J. Castellà-Roca and G. Rufián, "Preserving the User's Privacy in Social Networking Sites", 10th International Conference on Trust, Privacy and Security in Digital Business - TrustBus 2013, Prague, Czech Republic , Aug 2013.

D. Sánchez, M. Batet, A. Viejo, "Detecting Term Relationships to Improve Textual Document Sanitization", Pacific Asia Conference on Information Systems- PACIS 2013, Jeju Island, Korea, Aug 2013.

J. Soria-Comas and J. Domingo-Ferrer, "Differential privacy via t-closeness in data publishing", 11th Annual Conference on Privacy, Security and Trust-PST 2013, Tarragona, Catalonia, In IEEE Computer Society, pp. 27-35, ISBN: 978-1-4673-5839, Jul 2013.

J. Domingo-Ferrer, "On the connection between t-closeness and differential privacy for data releases", 10th International Conference on Security and Cryptography-SECRYPT 2013, Reykjavik, Iceland, Jul 2013.

J. Soria-Comas, J. Domingo-Ferrer, David Sánchez and Sergio Martínez, "Improving the utility of differentially private data releases via k-anonymity", 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications -IEEE TrustCom 2013, Melbourne, Australia, Jul 2013.

A. Viejo and D. Sánchez, "Providing Useful and Private Web Search by Means of Social Network Profiling", Eleventh Annual Conference on Privacy, Security and Trust - PST2013, Tarragona, Catalonia, Jul 2013.

D. Megías and J. Domingo-Ferrer, "DNA-inspired anonymous fingerprinting for efficient peer-to-peer content distribution", IEEE Congress on Evolutionary Computation, Cancun, Mexico, In IEEE Computer Society, pp. 2376-2383, ISBN: 978-1-4799-0452, Jun 2013.

L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer and P. Zeng, "A Generic Construction of Proxy Signatures from Certificateless Signatures", IEEE AINA 2013, Barcelona, Spain, In IEEE Computer Society, pp. 259-266, ISBN: 978-1-4673-5550, Mar 2013.

P. A. Pérez-Martínez, A. Martínez-Ballesté and A. Solanas, "Privacy in smart cities: A case study of smart public parking", Third International Conference on Pervasive and Embeded Computing and Communications Systems - PECCS 2013, Barcelona, Spain, Mar 2013.

A. Martínez-Ballesté, H. Rashwan, J. Castellà-Roca and D. Puig, "A Trustworthy Database for Privacy-Preserving Video Surveillance", Privacy and Anonymity in the Information Society - PAIS 2013, Genoa (Italy), Mar 2013.

PUBLICACIONES AÑO 2012

R. Jardí, J.Pujol, J. Castellà-Roca and A. Viejo, "Study on Poll-Site Voting and Verification Systems", Computers & Security, Vol. 31, no. 8, pp. 989-1010, Dec 2012, ISSN: 0167-4048.

A. Viejo, D. Sánchez, J. Castellà-Roca, "Preventing Automatic User Profiling in Web 2.0 Applications", Knowledge-Based Systems, Vol. 36, pp. 191-205, Dec 2012, ISSN: 0950-7051.

J. Soria-Comas and J. Domingo-Ferrer, "Sensitivity-Independent Differential Privacy via Prior Knowledge Refinement", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 20, no. 6, pp. 855-876, Dec 2012, ISSN: 0218-4885.

J. Domingo-Ferrer and R. Trujillo-Rasua, "Microaggregation- and permutation-based anonymization of movement data", Information Sciences, Vol. 208, pp. 55-80, Nov 2012, ISSN: 0020-0255.

S. Martínez, A. Valls and D. Sánchez, "Semantically-grounded construction of centroids for datasets with textual attributes", Knowledge-Based Systems, Vol. 35, pp. 160-172, Nov 2012, ISSN: 0950-7051.

M. Mut-Puigserver, M.M. Payeras-Capellà, J.L. Ferrer-Gomila, A. Vives-Guasch and J. Castellà-Roca, "A survey of electronic ticketing applied to transport", Computers & Security, Vol. 31, no. 8, pp. 925-939, Nov 2012, ISSN: 0167-4048.

B. Qin, Q. Wu, L.Zhang, J. Domingo-Ferrer and O.Farras, "Provably Secure Threshold Public-Key Encryption with Adaptive Security and Short Ciphertexts", Information Sciences, Vol. 210, pp. 67-80, Nov 2012, ISSN: 0020-0255.

M. Bras-Amorós, "The Ordinarization Transform of a Numerical Semigroup and Semigroups with a Large Number of Intervals", Journal of Pure and Applied Algebra, Vol. 216, no. 11, pp. 2507-2518, Nov 2012, ISSN: 0022-4049.

J. van den Hoven, D. Helbing, D. Pedreschi, J. Domingo-Ferrer, F. Giannotti and M. Christen, "FuturICT - The road towards ethical ICT", European Physical Journal-Special Topics, Vol. 214, pp. 143-181, Nov 2012, ISSN: 1951-6355.

S. Martínez, D. Sánchez, A. Valls, M. Batet, "Privacy protection of textual attributes through a semantic-based masking method", Information Fusion, Vol. 13, no. 4, pp. 304-314, Oct 2012, ISSN: 1566-2535.

J. Domingo-Ferrer and U. González-Nicolás, "Rational behavior in peer-to-peer profile obfuscation for anonymous keyword search: the multi-hop scenario", Information Sciences, Vol. 200, pp. 123-134, Oct 2012, ISSN: 0020-0255.

D. Sánchez and M. Batet, "A New Model to Compute the Information Content of Concepts from Taxonomic Knowledge ", International Journal on Semantic Web and Information Systems, Vol. 8, no. 2, pp. 38-50, Oct 2012, ISSN: 1552-6283.

O. Farràs, I. Gracia, S. Martín Mollevi and C. Padró, "Linear Threshold Multisecret Sharing Schemes", Information Processing Letters, Vol. 112, no. 17, pp. 667-673, Sep 2012, ISSN: 0020-0190.

D. Sánchez, M. Batet, D. Isern and A. Valls, "Ontology-based semantic similarity: a new feature-based approach", Expert Systems with Applications, Vol. 39, no. 9, pp. 7718-7728, Jul 2012, ISSN: 0957-4174.

A. Viejo, Q. Wu and J. Domingo-Ferrer, "Asymmetric Homomorphisms for Secure Aggregation in Heterogeneous Scenarios", Information Fusion, Vol. 13, no. 4, pp. 285-295, Jun 2012, ISSN: 1566-2535.

PUBLICACIONES RELACIONADAS DESTACADAS

O. Farràs, J. Ruth Metcalf-Burton, C. Padró and L. Vázquez, "On the Optimization of Bipartite Secret Sharing Schemes", Designs, Codes and Cryptography, Vol. 63, no. 2, pp. 255-271, Jun 2012, ISSN: 0925-1022.

R. Trujillo-Rasúa, A. Solanas, P. A. Pérez-Martínez and J. Domingo-Ferrer, "Predictive protocol for the scalable identification of RFID tags through collaborative readers", Computers in Industry, Vol. 63, no. 6, pp. 557-573, Jun 2012, ISSN: 0166-3615.

K. Lee, M. Bras-Amorós, M. E. O'Sullivan, "Unique Decoding of Plane AG Codes via Interpolation", IEEE Transactions on Information Theory, Vol. 58, no. 6, pp. 3941-3950, Jun 2012, ISSN: 0018-9448.

G. Navarro-Arribas, V. Torra, A. Erola and J. Castellà-Roca, "User k-anonymity for privacy preserving data mining of query logs", Information Processing and Management, Vol. 48, no. 3, pp. 476-487, May 2012, ISSN: 0306-4573.

O. Farràs and C. Padró, "Ideal Hierarchical Secret Sharing Schemes", IEEE Transactions on Information Theory, Vol. 58, no. 5, pp. 3273-3286, May 2012, ISSN: 0018-9448.

O. Farràs, J. Martí-Farré and C. Padró, "Ideal Multipartite Secret Sharing Schemes", Journal of Cryptology, Vol. 25, no. 3, pp. 434-463, Apr 2012, ISSN: 0933-2790.

S. Martínez, D. Sánchez and A. Valls, "Semantic Adaptive Microaggregation of Categorical Microdata", Computers & Security, Vol. 31, no. 5, pp. 653-672, Apr 2012, ISSN: 0167-4048.

D. Rebollo-Monedero, J. Forné and J. Domingo-Ferrer, "Query profile obfuscation by means of optimal query exchange between users", IEEE Transactions on Dependable and Secure Computing, Vol. 9, no. 5, pp. 641-655, Mar 2012, ISSN: 1545-5971.

D. Sánchez, A. Solé-Ribalta, M. Batet and F. Serratosa, "Enabling semantic similarity estimation across multiple ontologies: an evaluation in the biomedical domain", Journal of Biomedical Informatics, Vol. 45, no. 1, pp. 141-145, Feb 2012, ISSN: 1532-0464.

J. Domingo-Ferrer and U. González-Nicolás, "Rational behavior in peer-to-peer profile obfuscation for anonymous keyword search", Information Sciences, Vol. 185, no. 1, pp. 191-204, Jan 2012, ISSN: 0020-0255.

M. Bras-Amorós and K.Stokes, "The semigroup of combinatorial configurations", Semigroup Forum, Vol. 84, no. 1, pp. 91-96, Jan 2012, ISSN: 0037-1912.

A. Vives-Guasch, M. Payeras-Capellà, M. M. Puigserver, J. Castellà-Roca, J.L. Ferrer-Gomila, "A secure e-ticketing scheme for mobile devices with Near Field Communication (NFC) that includes exculpability and reusability", IEICE Transactions on Information Systems , Vol. 95, no. 1, pp. 78-93, Jan 2012, ISSN: 0916-8532.

S. Hajian and J. Domingo-Ferrer, "A study on the impact of data anonymization on anti-discrimination", IEEE 12th International Conference on Data Mining, Brussels, Belgium, Dec 2012.

D. Sánchez, M. Batet, A. Viejo, "Detecting sensitive information from textual documents: an information-theoretic approach", Modeling Decisions for Artificial Intelligence-MDAI 2012, Girona, Catalunya, In Lecture Notes in Computer Science vol. 7647, pp. 173-184, ISBN: 0302-9743, Nov 2012.

A. Viejo, D. Sánchez, J. Castellà-Roca, "Using Profiling Techniques to Protect the User's Privacy in Twitter", Modeling Decisions for Artificial Intelligence-MDAI 2012, Girona, Catalunya, In Lecture Notes in Computer Science vol. 7647, pp. 161-172, ISBN: 0302-9743, Nov 2012.

L. Zhang, Q. Wu, B. Qin and J. Domingo-Ferrer, "Practical privacy for value-added applications in vehicular ad hoc networks", The 6th International Conference on Network and System Security - NSS 2012, Wu Yi Shan, Fujian, China, Nov 2012.

J. Domingo-Ferrer, "Marginality: a numerical mapping for enhanced exploitation of taxonomic attributes", Modeling Decisions for Artificial Intelligence-MDAI 2012, Girona, Catalunya, In Lecture Notes in Computer Science vol. 7647, pp. 367-381, ISBN: 0302-9743, Nov 2012.

L. Zhang, Q. Wu, B. Qin and J. Domingo-Ferrer, "Practical privacy for value-added applications in vehicular ad hoc networks", Internet and Distributed Computing Systems - 5th International Conference, IDCS 2012, Wuyishan, Fujian, China, In Lecture Notes in Computer Science vol. 7646, pp. 43-56, ISBN: 0302-9743, Nov 2012.

L. Malina, J. Castellà-Roca, A. Vives-Guasch and J. Hajny, "Short-term Linkable Group Signatures with Categorized Batch Verification", 5th International Symposium on Foundations and Practice of Security - FPS 2012, Montreal, Canada, Oct 2012

A. Viejo, J. Castellà-Roca O.Bernado and J.M. Mateo-Sanz, "Single-party private web search", 10th Privacy, Security and Trust - PST2012, Paris, France, Oct 2012.

A. Oganian and J. Domingo-Ferrer, "Hybrid microdata via modelbased clustering", Privacy in Statistical Databases-PSD 2012, Palermo, Italy, In Lecture Notes in Computer Science vol. 7556, pp. 103-115, ISBN: 0302-9743, Sep 2012.

J. Domingo-Ferrer, K. Muralidhar and G. Rufian-Torrell, "Anonymization methods for taxonomic microdata", Privacy in Statistical Databases-PSD 2012, Palermo, Italy, In Lecture Notes in Computer Science vol. 7556, pp. 90-102, ISBN: 0302-9743, Sep 2012.

J. Soria-Comas and J. Domingo-Ferrer, "Differential privacy through knowledge refinement", PASSAT 2012, Amsterdam, The Netherlands. In Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Conference on Social Computing (SocialCom), pp. 702-707, ISBN: 978-1-4673-5638, Sep 2012.

B. Qin, H. Wang, Q. Wu, J. Liu and J. Domingo-Ferrer, "An Identity based Signcryption Scheme in the Standard Model", 4-th International Conference on Intelligent Networking and Collaborative Systems - INCOS 2012, Bucharest, Romania, Sep 2012.

H. Wang, B. Qin and J. Domingo-Ferrer, "An Improved Binary Authentication Tree Algorithm for Vehicular Networks", 4-th International Conference on Intelligent Networking and Collaborative Systems - INCOS 2012, Bucharest, Romania, Sep 2012.

A. Beimel, O. Farràs and Y. Mintz, "Secret Sharing Schemes for Very Dense Graphs", Advances in Cryptology - CRYPTO 2012, Santa Barbara, CA, USA, In Lecture Notes in Computer Science vol. 7417, pp. 144-161, ISBN: 0302-9743, Aug 2012.

S. Martínez, D. Sánchez and A. Valls, "Towards k-anonymous non-numerical data via Semantic Resampling", Information Processing and Management of Uncertainty in Knowledge-Based Systems - IPMU 2012, Catania, Italy, In Proceedings of IPMU 2012, Part IV, CCIS 300, pp. 519-528, ISBN: 1865-0929, Jul 2012.

J. Domingo-Ferrer and J. Soria-Comas, "Differential privacy: optimal noise and data quality in SDC", EURO 2012: XXV European Conference on Operations Research, Vilnius, Lithuania, Jul 2012.

M. Bras-Amorós and A. Vico-Oton, "On the Maximal Gap of an Ideal and the Feng-Rao Numbers", Iberian Meeting on Numerical Semigroups, Vila-Real, Portugal, Jul 2012.

M. Bras-Amorós and A. Vico-Oton, "Non-homogeneous Patterns on Numerical Semigroups", Iberian Meeting on Numerical Semigroups, Vila-Real, Portugal, Jul 2012

J. Soria-Comas and J. Domingo-Ferrer, "Probabilistic k-anonymity through microaggregation and data swapping", FUZZ-IEEE 2012, IEEE International Conference on Fuzzy Systems, Brisbane, Australia, Jun 2012.

K. Stokes and V. Torra, "n-Confusion: a generalization of k-anonymity", PAIS 2012, Berlin, Germany, Mar 2012.

PUBLICACIONES AÑO 2011

M. Bras-Amorós, J. Domingo-Ferrer, A. Vico-Oton, "Co-citations and Relevance of Authors and Author Groups", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 19, Special issue, pp. 127-139, Dec 2011, ISSN: 0218-4885.

S. Hajian and M. Abdollahi Azgomi, "A Privacy Preserving Clustering Technique for Horizontally and Vertically Distributed Datasets", Intelligent Data Analysis, Vol. 15, no. 4, pp. 503-532, Nov 2011, ISSN: 1088-467X.

A. Erola, J. Castellà-Roca, A. Viejo and J.M. Mateo-Sanz, "Exploting Social Networks to Provide Privacy in Personalized Web Search", Journal of Systems and Software, Vol. 84, no. 10, pp. 1734-17445, Oct 2011, ISSN: 0164-1212.

R. Trujillo-Rasúa and A. Solanas, "Efficient probabilistic communication protocol for the private identification of RFID tags by means of collaborative readers", Computer Networks, Vol. 55, no. 15, pp. 3211-3223, Oct 2011, ISSN: 1389-1286.

L. Zhang, Q. Wu, B. Qin and J. Domingo-Ferrer, "Provably secure one-round identity-based authenticated asymmetric group key agreement protocol", Information Sciences, Vol. 181, no. 19, pp. 4318-4349, Oct 2011, ISSN: 0020-0255.

L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer and Ú. González-Nicolás, "Asymmetric group key agreement protocol for open networks and its application to broadcast encryption", Computer Networks, Vol. 55, no. 15, pp. 3246-3255, Oct 2011, ISSN: 1389-1286.

J. Domingo-Ferrer, "Coprivacy: an introduction to the theory and applications of co-operative privacy", SORT-Statistics and Operations Research Transactions, Vol. 35, Special issue, pp. 25-40, Sep 2011, ISSN: 1696-2281.

A. Erola, J. Castellà-Roca, G. Navarro-Arribas and V. Torra, "Semantic microaggregation for the anonymization of query logs using the open directory project", SORT-Statistics and Operations Research Transactions, Vol. 0, Special issue, pp. 41-58, Sep 2011, ISSN: 1696-2281.

PUBLICACIONES RELACIONADAS DESTACADAS

J. Domingo-Ferrer, "Risk-Utility Paradigms for Statistical Disclosure Limitation: How to Think, But Not How to Act - Discussion: A Science of Statistical Disclosure Limitation?", International Statistical Review, Vol. 79, no. 2, pp. 184-186, May 2011, ISSN: 0306-7734 .

K. Stokes and M. Bras-Amorós, "Associating a numerical semigroup to the triangle-free configurations", Advances in Mathemathics of Communication, Vol. 5, no. 2, pp. 351-371, May 2011, ISSN: 1930-5346.

R. Di Pietro and A. Viejo, "Location Privacy and Resilience in Wireless Sensor Networks Querying", Computer Communications, Vol. 34, no. 3, pp. 515-523, Mar 2011, ISSN: 0140-3664.

M. Bras-Amorós, J. Domingo-Ferrer and V. Torra, "A bibliometric index based on collabotarion distance between cited and citing authors", Journal of Informetrics, Vol. 5, no. 2, pp. 248-264, Mar 2011, ISSN: 1751-1577.

J. Domingo-Ferrer and U. Gonzalez-Nicolas, "Decapitation of networks with and without weights and direction: the economics of iterated attack and defense", Computer Networks, Vol. 55, no. 1, pp. 119-130, Jan 2011, ISSN: 1389-1286.

A. Fernandez-Mir, R. Trujillo-Rasua, J. Castellà-Roca and J. Domingo-Ferrer, "A scalable RFID authentication protocol supporting ownership transfer and controlled delegation", Radio Frequency Identification: Security and Privacy Issues-RFIDsec 2011, Northampton (USA), In Lecture Notes in Computer Science vol. 7055, pp. 147-162, ISBN: 0302-9743, Dec 2011.

Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer and O. Farras, "Bridging Broadcast Encryption and Group Key Agreement", Intnl. Conf. on the Theory and Application of Cryptology and Information Security - ASIACRYPT 2011, Seoul, Korea, In Lecture Notes in Computer Science vol. 7073, pp. 143-160, ISBN: 0302-9743, Nov 2011.

O. Farràs, C. Padró, C. Xing and A. Yang, "Natural Generalizations of Threshold Secret Sharing", Intnl. Conf. on the Theory and Application of Cryptology and Information Security - ASIACRYPT 2011, Seoul, Korea, In Lecture Notes in Computer Science vol. 7073, pp. 610-627, ISBN: 0302-9743, Nov 2011.

B. Qin, Q. Wu, J. Domingo-Ferrer and L. Zhang, "Preserving Security and Privacy in Large-Scale VANETs", Thirteenth International Conference on Information and Communications Security - ICICS 2011, Beijing, China, In Lecture Notes in Computer Science vol. 7043, pp. 121-135, ISBN: 0302-9743, Nov 2011.

B. Qin, Q. Wu, J. Domingo-Ferrer and W. Susilo, "Distributed Privacy-Preserving Secure Aggregation in Vehicular Communication", Third International Conf. on Intelligent Networking and Collaborative Systems - IEEE INCoS 2011, Fukuoka, Japan, Nov 2011.

R. Trujillo-Rasua, A. Martínez-Ballesté and A. Solanas, "Revisión de protocolos para la identificación escalable, segura y privada en sistemas RFID", 5as Jornadas Científicas sobre RFID, Tarragona, Spain, Nov 2011.

C. Romero-Tris, A. Viejo and J. Castellà-Roca, "Improving query delay in private web search", International Workshop on Securing Information in Distributed Environments and Ubiquitous Systems - SIDEUS 2011, Barcelona, Spain, Oct 2011.

J. Domingo-Ferrer and R. Trujillo-Rasua, "Anonymization of Trajectory Data", 7th Joint UNECE/Eurostat Work Session on SDC, Tarragona, Catalonia, Oct 2011.

R. Trujillo-Rasua and A. Solanas, "Scalable Trajectory-based Protocol for RFID Tags Identification", IEEE International Conference on RFID-Technology and Applications - RFID-TA 2011, Sitges (Spain), Sep 2011.

C. Romero-Tris, J. Castellà-Roca and A. Viejo, "Multi-party private web search with untrusted partners", 7th International Conference on Security and Privacy in Communication Networks - SecureComm\'11, London, UK, In Lecture Notes of the Institute for Computer Sciences, Vol 96, pp. 261-280, ISBN: 1867-8211, Sep 2011.

M. Bras-Amorós and A. Vico-Oton, "On the Geil-Matsumoto Bound", Third International Castle Meeting on Coding Theory and Applications, Cardona, Spain, Sep 2011.

M. Bras-Amorós, "Ordinarization Transform of a Numerical Semigroup", European Conference on Combinatorics, Graph Theory and Applications - EuroComb 2011, Budapest, Hungary, Sep 2011.

S. Hajian, J. Domingo-Ferrer and A. Martínez-Ballesté, "Rule protection for indirect discrimination prevention in data mining", Modeling Decisions for Artificial Intelligence-MDAI 2011, Changsha, China, In Lecture Notes in Computer Science vol. 6820, pp. 211-222, ISBN: 0302-9743, Jul 2011.

K. Stokes and V. Torra, "On some clustering approaches for graphs", IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Taipei, Taiwan, Jun 2011.

O.Farràs and C. Padró, "Ideal Secret Sharing Schemes for Useful Multipartite Access Structures", International Workshop on Coding and Cryptology - IWCC2011 , Qingdao, China, In Lecture Notes in Computer Science vol. 6639, pp. 99-108, ISBN: 0302-9743, May 2011.

J. Pujol-Ahullo, R. Jardi-Cedo, J. Castella-Roca, O. Farràs , "TTP SmartCard - based ElGamal Cryptosystem using Threshold Scheme for Electronic Elections ", Foundations & Practice of Security 2011 - FPS 2011, Paris, France, May 2011.

P. A. Pérez-Martinez and A. Solanas, "W3-privacy: the three dimensions of user privacy in LBS", Twelfth ACM International Symposium on Mobile Ad Hoc Networking and Computing - MOBIHOC 2011, Paris, France, May 2011.

S. Hajian, J. Domingo-Ferrer and A. Martínez-Ballesté, "Discrimination prevention in data mining for intrusion and crime detection", IEEE Symposium Series in Computational Intelligence in Cyber Security - CICS 2011, Paris, France, Apr 2011.

K. Stokes and M. Bras-Amorós, "On query self-submission in peer-to-peer user-private information retrieval", PAIS 2011 collocate with EDBT/ICDT, Uppsala, Sweden, In Proceedings of the 4th International Workshop on Privacy and Anonymity in the Information Society, ISBN: 978-1-4503-0528, Mar 2011.

A. Vives-Guasch, M. Payeras-Capella, M. Mut and J. Castellà-Roca, "E-Ticketing scheme for mobile devices with exculpability", Data Privacy Management and Autonomous Spontaneous Security - SETOP 2010 & DPM 2010, In Lecture Notes in Computer Science vol. 6514, pp. 79-92, ISBN: 0302-9743, Jan 2011.

J. Domingo-Ferrer, "Rational Enforcement of Digital Oblivion", PAIS 2011 collocate with EDBT/ICDT, Uppsala, Sweden, In Proceedings of the 4th International Workshop on Privacy and Anonymity in the Information Society, ISBN: 978-1-4503-0528, Mar 2011.

A. Fernàndez-Mir, J. Castellà-Roca and A. Viejo, "Secure and Scalable RFID Authentication Protocol", Data Privacy Management and Autonomous Spontaneous Security - SETOP 2010 & DPM 2010, In Lecture Notes in Computer Science vol. 6514, pp. 231-243, ISBN: 0302-9743, Jan 2011

PUBLICACIONES AÑO 2010

D. Rebollo-Monedero, J. Forné and J. Domingo-Ferrer, "From t-closeness-like privacy to postrandomization via information theory", IEEE Transactions on Knowledge and Data Engineering, Vol. 22, no. 11, pp. 1623-1636, Nov 2010, ISSN: 1041-4347.

A. Viejo, J. Castellà-Roca, "Using Social Networks to Distort Users\' Profiles Generated by Web Search Engines", Computer Networks, Vol. 54, no. 9, pp. 1343-1357, Oct 2010, ISSN: 1389-1286.

V. Daza, J. Herranz, P. Morillo and C. Ràfols, "Extensions of access structures and their cryptographic applications", Applicable Algebra in Engineering, Communication and Computing, Vol. 21, no. 4, pp. 257-284, Jul 2010, ISSN: 0938-1279

L. Zhang, Q. Wu, A. Solanas, J. Domingo-Ferrer, "A Scalable Robust Authentication Protocol For Secure Vehicular Communications", IEEE Transactions on Vehicular Technology, Vol. 59, no. 4, pp. 1606-1617, Jun 2010, ISSN: 0018-9545.

J. Domingo-Ferrer, U. González-Nicolás, "Hybrid Microdata Using Microaggregation", Information Sciences, Vol. 180, no. 15, pp. 2834-2844, Jun 2010, ISSN: 0020-0255.

D. Rebollo, J. Forné, A. Solanas and A. Martínez-Ballesté, "Private Location-Based Information Retrieval through User Collaboration", Computer Communications, Vol. 33, no. 6, pp. 762-774, Apr 2010, ISSN: 0140-3664.

Q. Wu, J. Domingo-Ferrer and Ú. González-Nicolás, "Balanced Trustworthiness, Safety and Privacy in Vehicle-to-Vehicle Communications", IEEE Transactions on Vehicular Technology, Vol. 59, no. 2, pp. 559-573, Mar 2010, ISSN: 0018-9545.

L.Zhang, F.Zhang, Q. Wu and J. Domingo-Ferrer, "Simulatable certificateless two-party authenticated key agreement protocol", Information Sciences, Vol. 180, no. 6, pp. 1020-1030, Mar 2010, ISSN: 0020-0255.

K. Stokes and M. Bras-Amorós, "Optimal Configurations for Peer-to-Peer User-Private Information Retrieval", Computers & Mathematics with Applications, Vol. 59, no. 4, pp. 1568-1577, Feb 2010, ISSN: 0898-1221.

B. Qin, Q. Wu, L. Zhang and J. Domingo-Ferrer, "Threshold public-key encryption with adaptive security and short ciphertexts", Information and Communications Security - ICICS 2010, Barcelona, Spain, In Lecture Notes in Computer Science vol. 6476, pp. 62-76, ISBN: 0302-9743, Dec 2010.

B. Qin, L. Zhang, Q. Wu and J. Domingo-Ferrer, "Secure compression of privacy-preserving witnesses in vehicular ad hoc networks", 1st International Workshop on Vehicular Communications and Networking - VECON 2010, Nov 2010.

J. Domingo-Ferrer, M. Sramka and R. Trujillo, "Privacy preserving Publication of Trajectories Using Microaggregation", SPRINGL 2010-3rd ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS, San José (USA), Nov 2010.

L. Zhang, Q. Wu, J. Domingo-Ferrer and B. Qin, "Hierarchical Certificateless Signatures", TrustCom 2010, Kowloon, Hong Kong, In Proceedings of TRUSTCOM 2010-IEEE/IFIP 8th Intl. Conference on Embedded and Ubiquitous Computing-EUC 2010, IEEE Computer Society Press, pp. 572-577, ISBN: 978-0-7695-4322, Nov 2010.

PUBLICACIONES RELACIONADAS DESTACADAS

J. Domingo-Ferrer, "Rational privacy disclosure in social networks", Modeling Decisions for Artificial Intelligence, In Lecture Notes in Computer Science vol. 6408, pp. 255-265, ISBN: 0302-9743, Nov 2010.

M. Bras-Amorós, J. Domingo-Ferrer, V. Torra, "A Bibliometric Index Based On Collaboration Distances", Modeling Decisions for Arti, In Lecture Notes in Computer Science vol. 6408, pp. 5-6, ISBN: 0302-9743, Nov 2010.

A. Vives-Guasch, J. Castellà-Roca, M. Payeras-Capellà and M. M. Puigserver, "An Electronic and secure automatic fare Collection system with revocable anonymity for users", 8th International conference on advances on Mobile computing and multimedia - MoMM 2010, Paris, France, Nov 2010.

Q. Wu, B. Qin, L. Zhang and J. Domingo-Ferrer, "Ad hoc broadcast encryption", 17th ACM Conference on Computer and Communications Security - CCS 2010, Chicago (USA), Oct 2010.

J. Domingo-Ferrer, "Coprivacy: towards a theory of sustainable privacy", Privacy in Statistical Databases-PSD 2010, In Lecture Notes in Computer Science vol. 6344, pp. 258-268, ISBN: 0302-9743, Sep 2010.

A. Erola, J. Castellà-Roca, G. Navarro-Arribas and V. Torra, "Semantic Microaggregation for the Anonymization of Query Logs", Privacy in Statistical Databases-PSD 2010, Corfu, Greece, In Lecture Notes in Computer Science vol. 6344, pp. 127-137, ISBN: 0302-9743, Sep 2010.

M. Bras-Amorós, K. Stokes, M. Greferath, "Problems Related to Combinatorial Con figurations with Applications to P2P-User Private Information Retrieval", 19th International Symposium on Mathematical Theory of Networks and Systems - MTNS 2010, Budapest, Hungary, Jul 2010.

J. Pujol-Ahulló, R. Jardí-Cedó, J. Castellà-Roca, "Verification Systems for Electronic Voting: A Survey", 4th International Conference on Electronic Voting - EVOTE2010, Bregenz, Austria, Jul 2010.

A. Solanas, U. Gonzáles-Nicolás and A. Martínez-Ballesté, "A variable-MDAV-based partitioning strategy to continuous multivariate microaggregation with genetic algorithms", The 2010 International Joint Conference on Neural Networks (IJCNN 2010) , Barcelona, Spain, Jul 2010.

L. Zhang, Q. Wu, B. Qin and J. Domingo-Ferrer, "Identity-based authenticated asymmetric group key agreement", The 16th Annual International Computing and Combinatorics Conference - COCOON 2010, Vietnam, In Lecture Notes in Computer Science vol. 6169, pp. 510-519, ISBN: 0302-9743, Jul 2010.

J. Domingo-Ferrer and K.Stokes, "The zeta function and data mining", Second workshop on zeta functions in algebra and geometry, Palma de Mallorca, Spain, May 2010.

K. Stokes and M. Bras-Amorós, "The semigroup of combinatorial configurations", Iberian meeting on numerical semigroups, Granada (Spain), Feb 2010.

M. Bras-Amorós and K. Stokes, "On the existence of combinatorial configurations", 3rd International Workshop on Optimal Network Topologies (IWONT), Barcelona, Spain, Jun 2010.

PUBLICACIONES AÑO 2009

J. Domingo-Ferrer, M. Bras-Amorós, Q. Wu, J. Manjón, "User-Private Information Retrieval Based on a Peer-to-Peer Community", Data & Knowledge Engineering, Vol. 68, no. 11, pp. 1237-1252, Nov 2009, ISSN: 0169-023X.

M. Bras-Amorós, "On Numerical Semigroups and the Redundancy of Improved Codes Correcting Generic Errors", Designs, Codes and Cryptography, Vol. 53, no. 2, pp. 111-118, Nov 2009, ISSN: 0925-1022.

J. Domingo-Ferrer and Y. Saygin, "Recent progress in database privacy", Data & Knowledge Engineering, Vol. 68, no. 11, pp. 1157-1159, Nov 2009, ISSN: 0169-023X.

J. Alberto Rodríguez, A. Kamisalic and J. Domingo-Ferrer, "On reliability indices of communication networks", Computers & Mathematics with Applications, Vol. 58, no. 7, pp. 1433-1440, Oct 2009, ISSN: 0898-1221.

J. Domingo-Ferrer, A. Solanas and Jordi Castellà-Roca, "h(k)-Private Information Retrieval from Privacy-Uncooperative Queryable Databases", Online Information Review, Vol. 33, pp. 720-744, Aug 2009, ISSN: 1468-4527.

J. Castellà-Roca, A. Viejo, J. Herrera-Joancomartí, "Preserving user\'s privacy in web search engines", Computer Communications, Vol. 32, no. 13, pp. 1541-1551, Aug 2009, ISSN: 0140-3664.

M. Bras-Amorós, "Bounds on the Number of Numerical Semigroups of a Given Genus", Journal of Pure and Applied Algebra, Vol. 213, no. 6, pp. 997-1001, Jun 2009, ISSN: 0022-4049.

A. Viejo, J. Domingo-Ferrer, F. Sebé and J. Castellà, "Secure Many-to-One Communications in Wireless Sensor Networks", Sensors, Vol. 9, no. 7, pp. 5324-5338, Jun 2009, ISSN: 1424-8220.

V. Daza, J. Domingo-Ferrer, F. Sebé and A. Viejo, "Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks", IEEE Transactions on Vehicular Technology, Vol. 58, no. 4, pp. 1876-1886, Jan 2009, ISSN: 0018-9545.

J.Domingo-Ferrer, "Weighted Network Decapitation: The Economics of Iterated Attack and Defense", ACM First International Workshop on Privacy and Anonymity for Very Large Datasets (PAVLAD 2009) with, Hong Khon, China, Nov 2009.

J. Domingo-Ferrer, "The functionality-security-privacy game", Modeling Decisions for Artificial Intelligence - MDAI 2009, In Lecture Notes in Computer Science vol. 5861, pp. 92-101, ISBN: 0302-9743, Nov 2009.

P. A. Pérez-Martínez and A. Solanas, "Location Privacy Through Users? Collaboration: A Distributed Pseudonymizer", Third International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies - , Sliema, Malta, Oct 2009.

J. Domingo-Ferrer, Q. Wu, "Safety and Privacy in Vehicular Communications", Privacy in Location-Based Applications - PILBA 2008, In Lecture Notes in Computer Science vol. 5599, pp. 173-189, ISBN: 0302-9743, Jul 2009.

M. Bras-Amorós, M. E. O'Sullivan, "From the Euclidean Algorithm for Solving a Key Equation for Dual Reed-Solomon Codes to the Berlekamp-Massey Algorithm", Applied Algebra, Algebraic Algorithms and Error Correcting Codes - AAECC-18, In Lecture Notes in Computer Science vol. 5527, pp. 32-42, ISBN: 0302-9743, Jun 2009.

A. Viejo, F. Sebé and J. Domingo-Ferrer, "Aggregation of trustworthy announcement messages in vehicular ad hoc networks", 2009 IEEE 69th Vehicular Technology Conference VTC2009-Spring, Barcelona (Spain), Apr 2009.

Q. Wu, Yi Mu, W. Susilo, B. Qin and J. Domingo-Ferrer, "Asymmetric group key agreement", Advances in Cryptology-EUROCRYPT 2009, In Lecture Notes in Computer Science vol. 5479, pp. 153-170, ISBN: 0302-9743, Apr 2009.

J. Domingo-Ferrer and D. Rebollo-Monedero, "Measuring risk and utility of anonymized data using information theory", 2nd International Workshop on Privacy and Anonymity in the Information Society (PAIS 2009) collocate with EDBT/ICDT, Saint-Petersburg (Russia), Mar 2009.

D. Rebollo-Monedero, J. Forné, L. Subirats, A. Solanas and A. Martínez-Ballesté, "A collaborative protocol for private retrieval of location-based information", IADIS International Conference e-Society 2009, Barcelona (Spain), Feb 2009.

PUBLICACIONES AÑO 2008

J. Domingo-Ferrer and A. Solanas, "A measure of variance for hierarchical nominal attributes", Information Sciences, Vol. 178, no. 24, pp. 4644-4655, Dec 2008, ISSN: 0020-0255.

J. Domingo-Ferrer, A. Viejo, F. Sebé and Ú. González-Nicolás, "Privacy homomorphisms for social networks with private relationships", Computer Networks, Vol. 52, no. 15, pp. 3007-3016, Oct 2008, ISSN: 1389-1286.

F. Sebé, J. Domingo-Ferrer, A. Martí-nez-Ballesté, Y. Deswarte and J.J. Quisquater, "Efficient remote data possession checking in critical information infrastructures", IEEE Transactions on Knowledge and Data Engineering, Vol. 20, no. 8, pp. 1034-1038, Aug 2008, ISSN: 1041-4347.

V. Daza, J. Herranz and G. Sáez, "On the computational security of a distributed key distribution scheme", IEEE Transactions on Computers, Vol. 57, pp. 1087-1097, Aug 2008, ISSN: 0018-9340 .

A. Viejo, F. Sebé and J. Domingo-Ferrer, "Secure and Scalable Many-to-One Symbol Transmission for Sensor Networks", Computer Communications, Vol. 31, pp. 2408-2413, Jun 2008, ISSN: 0140-3664.

A. Solanas and A. Martí-nez-Ballesté, "A TTP-Free Protocol for Location Privacy in Location-Based Services", Computer Communications, Vol. 31, pp. 1181-1191, Apr 2008, ISSN: 0140-3664.

M. Bras-Amorós, "Fibonacci-Like Behavior of the Number of Numerical Semigroups of a Given Genus", Semigroup Forum, Vol. 76, pp. 379-384, Mar 2008, ISSN: 0037-1912.

J. Domingo-Ferrer, F. Sebé and A. Solanas, "A polynomial-time approximation to optimal multivariate microaggregation", Computers & Mathematics with Applications, Vol. 55, pp. 714-732, Feb 2008, ISSN: 0898-1221.

M. Bras-Amorós, M.E. O'Sullivan, "Redundancies of Correction-Capability-Optimized Reed-Muller Codes", Discrete Applied Mathematics, Vol. 156, no. 166, pp. 3005-3010, Feb 2008, ISSN: 0166-218X.

PUBLICACIONES RELACIONADAS DESTACADAS

M. Bras-Amorós, M.E. O'Sullivan, "Duality for some families of correction capability optimized evaluation codes", Advances in Mathemathics of Communication, Vol. 2, no. 1, pp. 15-22, Feb 2008, ISSN: 1930-5346.

A. Solanas, J. Domingo-Ferrer and A. Martínez-Ballesté, "Location Privacy in Location-Based Services: Beyond TTP-based Schemes", 1st International Workshop on Privacy in Location-Based Applications (PILBA 2008) within 13th Europe, Málaga (Spain), Oct 2008.

A. Solanas and R. Di Pietro, "A Linear-Time Multivariate Microaggregation for Privacy Protection in Uniform Very Large Data Sets", Modeling Decisions for Artificial Intelligence - MDAI 2008, In Lecture Notes in Computer Science vol. 5285, pp. 203-214, ISBN: 0302-9743, Oct 2008.

J. Domingo-Ferrer and M. Bras-Amorós, "A shared steganographic file system with error correction", Modeling Decisions for Artificial Intelligence-MDAI 2008, In Lecture Notes in Computer Science vol. 5285, pp. 227-238, ISBN: 0302-9743, Oct 2008.

J. Domingo-Ferrer and M. Bras-Amorós, "Peer-to-peer private information retrieval", Privacy in Statistical Databases- PSD 2008, In Lecture Notes in Computer Science vol. 5262, pp. 315-323, ISBN: 0302-9743, Sep 2008.

David Rebollo, Jordi Forné and Josep Domingo-Ferrer, "From t-closeness to PRAM and noise addition via information theory", Privacy in Statistical Databases - PSD 2008, In Lecture Notes in Computer Science vol. 5262, pp. 100-112, ISBN: 0302-9743, Sep 2008.

Josep Domingo-Ferrer, Francesc Sebé and Agusti Solanas, "An anonimity model achievable via microaggregation", 5th VLDB Workshop on Secure Data Management-SDM 2008, In Lecture Notes in Computer Science vol. 5159, pp. 209-218, ISBN: 0302-9743, Aug 2008.

Vicenç Torra, Sadaaki Miyamoto, Yasunori Endo and Josep Domingo-Ferrer, "On Intuitionistic fuzzy clustering for its application to privacy", International Conference on Fuzzy Systems (FUZZ 2008), Jul 2008.

M. Gheorghita, A. Solanas and J.Forne, "Location Privacy in Chain-Based Protocols for Location-Based Services", The Third International Conference on Digital Telecommunications (ICDT08), Bucharest (Romania), Jul 2008.

Agusti Solanas, Glòria Pujol, Antoni Martí-nez Ballesté and Josep M. Mateo-Sanz, "A Post-processing Method to Lessen k-Anonymity Dissimilarities", 1st International Workshop on Privacy and Security by means of Artificial Intelligence (PSAI), Mar 2008.

Agusti Solanas, Francesc Sebé and Josep Domingo-Ferrer, "Micro-aggregation-Based Heuristics for p-sensitive k-anonymity: One Step Beyond", 1st International Workshop on Privacy and Anonymity in the Information Society (PAIS) collocated with EDBT/ICDT, Mar 2008.

Josep Domingo-Ferrer and Vicenç Torra, "A critique of k-anonimity and some of its enhacements", Proceedings of ARES/PSAI 2008, Mar 2008.

M. Bras-Amorós, "Results on Numerical Semigroups with Applications to Algebraic Geometry Codes", Iberian Meeting on Numerical Semigroups, Mar 2008.

M. Bras-Amorós, "Optimized Evaluation Codes Guaranteeing Correction of Generic Errors", 4th Workshop on Coding and Systems, Mar 2008.

PUBLICACIONES AÑO 2007

V. Daza, J. Herranz, P. Morillo and C. Ràfols, "Cryptographic techniques for mobile ad-hoc networks", Computer Networks, Vol. 51, pp. 4938-4950, Dec 2007, ISSN: 1389-1286.

M. Bras-Amorós, A. de Mier, "Representation of Numerical Semigroups by Dyck Paths", Semigroup Forum, Vol. 75, pp. 677-682, Nov 2007, ISSN: 0037-1912.

Maria Bras-Amorós, M.E. O'Sullivan, "The Order Bound on the Minimum Distance of the One-Point Codes Associated to the Garcia-Stichtenoth Tower of Function Fields", IEEE Transactions on Information Theory, Vol. 53, no. 18, pp. 4241-4245, Nov 2007, ISSN: 0018-9448.

Josep Domingo-Ferrer, Joachim Posegga, Francesc Sebé and Vicenç Torra, "Advances in smart cards", Computer Networks, Vol. 51, pp. 2219-2222, Aug 2007, ISSN: 1389-1286.

Agusti Solanas, Josep Domingo-Ferrer, Antoni Martí-nez-Ballesté, Vanesa Daza, "A Distributed Architecture for Scalable Private RFID Tag Identification", Computer Networks, Vol. 51, pp. 2268-2279, Aug 2007, ISSN: 1389-1286.

Maria Bras-Amorós, M.E. O'Sullivan, "On Semigroups Generated by Two Consecutive Integers and Improved Hermitian Codes", IEEE Transactions on Information Theory, Vol. 53, no. 18, pp. 2560-2566, Jul 2007, ISSN: 0018-9448.

F. Sebé, A. Viejo and J. Domingo-Ferrer, "Secure Many-to-One Symbol transmission for Implementation on Smart Cards", Computer Networks, Vol. 51, pp. 2299-2307, Jan 2007, ISSN: 1389-1286.

Francesc Sebé and Josep Domingo-Ferrer, "Scalability and security in biased many-to-one communication", Computer Networks, Vol. 51, pp. 1-13, Jan 2007, ISSN: 1389-1286.

M. Bras-Amorós, M. E. O'Sullivan, "Extended Norm-Trace Codes with Optimized Correction Capability", Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, In Lecture Notes in Computer Science vol. 4851, pp. 337-346, ISBN: 0302-9743, Dec 2007.

Antoni Martinez-Balleste and Agusti Solanas, "Privacy in the Information and Communication Technologies", IEEE Intl. Conf. on Granular Computing, Nov 2007.

V. Daza, J. Herranz, P. Morillo and C. Ràfols, "CCA2-secure threshold broadcast encryption with shorter ciphertexts", Proceedings of the 1st International Conference on Provable Security - ProvSec 2007, In Lecture Notes in Computer Science vol. 4784, pp. 35-50, ISBN: 0302-9743, Nov 2007.

Alexandre Viejo, Francesc Sebé and Josep Domingo-Ferrer, "Secure and private incentive-based advertisement dissemination in mobile ad hoc networks", IWSEC 2007, In Lecture Notes in Computer Science vol. 4752, pp. 185-198, ISBN: 0302-9743, Oct 2007.

Agusti Solanas, "A Study of Convex Hull Intersection in Clustering with Cardinality Constraints", XXX Congreso Nacional de Estadí-stica e Investigación Operativa, Sep 2007.

Josep Domingo-Ferrer, "A three-dimensional conceptual framework for database privacy", 4th VLDB Workshop on Secure Data Management - SDM 2007, In Lecture Notes in Computer Science vol. 4721, pp. 193-202, ISBN: 0302-9743, Sep 2007.

Josep Domingo-Ferrer, "A public-key protocol for social networks with private relationships", Modeling Decisions for Artificial Intelligence - MDAI 2007, In Lecture Notes in Computer Science vol. 4617, pp. 373-379, ISBN: 0302-9743, Aug 2007.

Jordi Castellà-Roca, Vanesa Daza, Josep Domingo-Ferrer, Jesús Manjón, Francesc Sebé and Alexandre Viejo, "An incentive-based system for information providers over peer-to-peer mobile ad-hoc networks", Modeling Decisions for Artificial Intelligence-MDAI 2007, In Lecture Notes in Computer Science vol. 4617, pp. 380-392, ISBN: 0302-9743, Aug 2007.

Jordi Aragones, Antoni Martinez-Ballesté and Agusti Solanas, "A Brief Survey on RFID Privacy and Security", World Congress on Engineering WCE-07, Jul 2007.

Vanesa Daza and Josep Domingo-Ferrer, "On partial anonymity in secret sharing", EuroPKI 2007, In Lecture Notes in Computer Science vol. 4582, pp. 193-202, ISBN: 0302-9743, Jun 2007.

gusti Solanas and Antoni Martí-nez-Ballesté, "Privacy Protection in location-based services through a public-key homomorphism", EuroPKI 2007, In Lecture Notes in Computer Science vol. 4582, pp. 362-368, ISBN: 0302-9743, Jun 2007.

Antoni Martí-nez-Ballesté, Agusti Solanas, Josep Domingo-Ferrer and Josep M. Mateo-Sanz, "A genetic approach to multivariate microaggregation for database privacy", 23rd International Conference on Data Engineering. Workshop on Privacy Data Management, Apr 2007.

PUBLICACIONES AÑO 2006

Francesc Sebé, Josep Domingo-Ferrer, Jordi Castellà -Roca, "Watermarking numerical data in presence of noise", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 14, pp. 495-508, Aug 2006, ISSN: 0218-4885.

Josep Domingo-Ferrer, Antoni Martí-nez-Ballesté, Josep M. Mateo-Sanz and Francesc Sebé, "Efficient multivariate data-oriented microaggregation", The VLDB Journal, Vol. 15, pp. 355-369, Aug 2006, ISSN: 1066-8888.

Vicenç Torra, Josep Domingo-Ferrer, Josep M. Mateo-Sanz, Michael Ng, "Regression for ordinal variables without underlying continuous variables", Information Sciences, Vol. 11, pp. 465-474, Feb 2006, ISSN: 0020-0255.

Josep Domingo-Ferrer and Francesc Sebé, "Optimal multivariate 2-microaggregation for microdata protection: a 2-approximation", Privacy in Statistical Databases - PSD 2006, In Lecture Notes in Computer Science vol. 4302, pp. 129-138, ISBN: 0302-9743, Dec 2006.

Vicenç Torra, John Abowd and Josep Domingo-Ferrer, "Using Mahalanobis distance-based record linkage for disclosure risk assessment", Privacy in Statistical Databases - PSD 2006, In Lecture Notes in Computer Science vol. 4302, pp. 233-242, ISBN: 0302-9743, Dec 2006.

Agusti Solanas, Antoni Martí-nez-Ballesté, Josep M. Mateo-Sanz and Josep Domingo-Ferrer, "Multivariate microaggregation based on genetic algorithms", IEEE IS 2006, Varna (Bulgaria), In Proceedings of the 3rd IEEE Conference on Intelligent Systems , ISBN: 1-4244-0196-8, Sep 2006.

PUBLICACIONES RELACIONADAS DESTACADAS

Agusti Solanas, Antoni Martí-nez-Ballesté, Josep Domingo-Ferrer, "V-MDAV: A multivariate microaggregation with variable group size", COMPSTAT2006, Rome (Italy), In Proceedings of COMPSTAT2006, ISBN: 3-7908-1708-2, Aug 2006.

Vicenç Torra and Josep Domingo-Ferrer, "Establishing a benchmark for re-identification methods and its validation using fuzzy clustering", 2006 IEEE World Congress on Computational Intelligence, Jul 2006.

Josep Domingo-Ferrer, "Microaggregation for database and location privacy", Next Generation Information Technologies and Systems - NGITS 2006, In Lecture Notes in Computer Science vol. 4032, pp. 106-116, ISBN: 0302-9743, Jul 2006.

Josep Domingo-Ferrer, Vicenç Torra, Josep M. Mateo-Sanz and Francesc Sebé, "Re-identification and synthetic data generators: a case study", Information Processing and Management of Uncertainty in Knowledge-Based Systems-IPMU2006, Paris (France), Jul 2006.

Jordi Castellà-Roca, Josep Domingo-Ferrer, Francesc Sebé, "A smart card-based mental poker system", Proceedings of IFIP CARDIS 2006, In Lecture Notes in Computer Science vol. 3928, pp. 48-61, ISBN: 0302-9743, Apr 2006.

Agusti- Solanas, Josep Domingo-Ferrer, "Watermarking non-numerical databases", Modeling Decisions for Artificial Intelligence - MDAI 2006, In Lecture Notes in Computer Science vol. 3885, pp. 239-250, ISBN: 0302-9743, Apr 2006.

Jordi Castellà-Roca, Josep Domingo-Ferrer and Francesc Sebé, "On the security of a repaired mental poker protocol", 3rd Intl. Conf. on Information Technology: New Generations-ITNG2006, Las Vegas (USA), Apr 2006

Josep Domingo-Ferrer, Agusti- Solanas and Antoni Martí-nez-Ballesté, "Privacy in statistical databases: k-anonymity through microaggregation", Proceedings of IEEE Granular Computing 2006, Jan 2006

Jordi Castellà-Roca, Vanesa Daza, Josep Domingo-Ferrer and Francesc Sebé, "Privacy homomorphisms for e-gambling and mental poker", IEEE Granular Computing 2006, In Proceedings of IEEE Granular Computing 2006, pp. 788-791, ISBN: 1-4244-0133-X, Jan 2006.

Agusti Solanas, Antoni Martinez-Ballesté, Josep M. Mateo-Sanz and Josep Domingo-Ferrer, "A 2d-tree-based blocking method for microaggregating very large data sets", ARES/DAWAM2006, Vienna (Austria), In Proceedings of ARES/DAWAM2006, pp. 922-928, ISBN: 0-7695-2567-9, Jan 2006.

PUBLICACIONES AÑO 2005

Josep Domingo-Ferrer and Vicenç Torra, "Privacy in Data Mining", Data Mining and Knowledge Discovery, Vol. 11, pp. 117-119, Sep 2005, ISSN: 1384-5810.

Josep M. Mateo-Sanz, Josep Domingo-Ferrer and Francesc Sebé, "Probabilistic information loss measures in confidentiality protection of continuous microdata", Data Mining and Knowledge Discovery, Vol. 11, pp. 181-193, Sep 2005, ISSN: 1384-5810.

Josep Domingo-Ferrer and Vicenç Torra, "Ordinal, continuous and heterogeneous k-anonymity through microaggregation", Data Mining and Knowledge Discovery, Vol. 11, pp. 195-212, Sep 2005, ISSN: 1384-5810.

Josep Domingo-Ferrer, Francesc Sebé and Antoni Martí-nez-Ballesté, "On multicast fingerprinting and collusion security", 1st International Conference on Automated Production of Cross Media Content for Multi-channel Distri, Nov 2005.

Jordi Castellà-Roca, Francesc Sebé and Josep Domingo-Ferrer, "Dropout-tolerant TTP-free mental poker", Trust and Privacy in Digital Business-TrustBus 2005, In Lecture Notes in Computer Science vol. 3592, pp. 30-40, ISBN: 0302-9743, Aug 2005.

Francesc Sebé, Josep Domingo-Ferrer and Agusti Solanas, "Noise-robust watermarking for numerical datasets", Modeling Decisions for Artificial Intelligence - MDAI 2005, In Lecture Notes in Computer Science vol. 3558, pp. 134-143, ISBN: 0302-9743, Jul 2005.

Joaquin Garcia, Fréderic Cuppens, Fabien Autrel, Jordi Castellà-Roca, Joan Borrell, Guillermo Navarro, and Jose A. Ortega-Ruiz, "Protecting on-line casinos against fraudulent player drop-out", EEE Intl. Conf. on Information Technology: Coding and Computing-ITCC2005, Jan 2005.

Jordi Castellà-Roca, Guillermo Navarro, Jose A. Ortega-Ruiz and Joaquin Garcí-a, "Digital chips for an on-line casino", IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC2005, Jan 2005.

PUBLICACIONES AÑO 2004

Francesc Sebé and Josep Domingo-Ferrer, "A critique to the Burmester and Le attack to Sebé and Domingo-Ferrer fingerprinting scheme", Electronics Letters, Vol. 40, no. 13, pp. 1261-1262, Sep 2004, ISSN: 0013-5194.

Josep Domingo-Ferrer and Vicenç Torra, "Selecting potentially relevant records using re-identification methods", New Generation Computing, Vol. 22, no. 3, pp. 239-252, May 2004, ISSN: 0288-3635.

Josep Domingo-Ferrer and Vicenç Torra, "Disclosure risk assessment in statistical data protection", Journal of Computational and Applied Mathematics, Vol. 164, pp. 285-293, Mar 2004, ISSN: 0377-0427.

Antoni Martí-nez-Ballesté, Francesc Sebé and Josep Domingo-Ferrer, "Secure many-to-one transmission of q-ary symbols", Intelligence in Communication Systems - IFIP Intellcomm 2004, In Lecture Notes in Computer Science vol. 3283, pp. 85-91, ISBN: 0302-9743, Nov 2004.

Antoni Martí-nez-Ballesté, Josep Domingo-Ferrer and Francesc Sebé, "Large-Scale Pay-As-You-Watch for Unicast and Multicast Communications", Trust and Privacy in Digital Business - TrustBus 2004, In Lecture Notes in Computer Science vol. 3184, pp. 261-268, ISBN: 0302-9743, Sep 2004.

Josep M. Mateo-Sanz, Josep Domingo-Ferrer and Vicenç Torra, "Object positioning based on partial preferences", Modeling Decisions for Artificial Intelligence 2004, In Lecture Notes in Computer Science vol. 3131, pp. 252-259, ISBN: 0302-9743, Aug 2004.

Josep Domingo-Ferrer, "On the synergy between certificate verification trees and PayTree-like micropayments", EuroPKI 2004, In Lecture Notes in Computer Science vol. 3093, pp. 180-190, ISBN: 0302-9743, Jun 2004.

Josep Domingo-Ferrer, Francesc Sebé and Jordi Castellà, "On the security of noise addition for privacy in statistical databases", Privacy in Statistical Databases - PSD 2004, In Lecture Notes in Computer Science vol. 3050, pp. 149-161, ISBN: 0302-9743, Jun 2004.

Josep M. Mateo-Sanz, Francesc Sebé and Josep Domingo-Ferrer, "Outlier protection in continuous microdata masking", Privacy in Statistical Databases - PSD 2004, In Lecture Notes in Computer Science vol. 3050, pp. 201-215, ISBN: 0302-9743, Jun 2004.

Josep M. Mateo-Sanz, Antoni Martí-nez-Ballesté and Josep Domingo-Ferrer, "Fast generation of accurate synthetic microdata", Privacy in Statistical Databases - PSD 2004, In Lecture Notes in Computer Science vol. 3050, pp. 298-306, ISBN: 0302-9743, Jun 2004.

Josep Domingo-Ferrer, Antoni Martí-nez-Ballesté and Francesc Sebé, "Secure reverse communication in a multicast tree", Networking 2004, In Lecture Notes in Computer Science vol. 3042, pp. 807-816, ISBN: 0302-9743, May 2004.

Anna Oganian, Josep Domingo-Ferrer and Vicenç Torra, "Internal intrusion scenarios in inference control of tabular databases", Information Processing and Management of Uncertainty in Knowledge-Based Systems-IPMU2004, Jan 2004.

Antoni Martí-nez-Ballesté, Francesc Sebé and Josep Domingo-Ferrer, "Secure large-scale bingo", IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC2004, Jan 2004.

J. Herrera-Joancomarti, J. Prieto-Blàzquez and J. Castellà-Roca, "A secure electronic examination protocol using wireless networks", IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC 2004, Jan 2004.

Antoni Martí-nez-Ballesté, Francesc Sebé and Josep Domingo-Ferrer, "Computer skills training to (mililed-aged) adults: problems and program", IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC2004, Jan 2004.

Jordi Castellà-Roca and Josep Domingo-Ferrer, "A non-repudiable bitstring commitment scheme based on a public-key cryptosystem", IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC2004, Jan 2004.

Jordi Castellà-Roca and Josep Domingo-Ferrer, "On the security of an efficient TTP-free mental poker protocol", IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC2004, Jan 2004.

PUBLICACIONES AÑOS 2003-1994

Josep Domingo-Ferrer and Vicenç Torra, "Disclosure risk assessment in statistical disclosure control of microdata via advanced record linkage", Statistics and Computing, Vol. 13, pp. 343-354, Oct 2003, ISSN: 0960-3174.

Aïda Valls, Vicenç Torra and Josep Domingo-Ferrer, "Semantic based aggregation for statistical disclosure control", International Journal of Intelligent Systems, Vol. 18, pp. 393-951, Sep 2003, ISSN: 0884-8173.

Francesc Sebé and Josep Domingo-Ferrer, "Collusion-secure and cost-effective detection of unlawful multimedia redistribution", IEEE Transactions on Systems, Man and Cybernetics, Part C, Vol. 33, pp. 382-389, Aug 2003, ISSN: 1094-6977.

Josep Domingo-Ferrer and Vicenç Torra, "Median-based aggregation operators for prototype construction in ordinal scales", International Journal of Intelligent Systems, Vol. 18, pp. 633-655, Jun 2003, ISSN: 0884-8173.

PUBLICACIONES RELACIONADAS DESTACADAS

Josep Domingo-Ferrer and Vicenç Torra, "On the connections between statistical disclosure control for microdata and some artificial intelligence tools", Information Sciences, Vol. 151, pp. 153-170, May 2003, ISSN: 0020-0255.

Jordi Castellà-Roca, Josep Domingo-Ferrer, Andreu Riera and Joan Borrell, "Practical mental poker without a TTP based on homomorphic encryption", Progress in Cryptology - Indocrypt 2003, In Lecture Notes in Computer Science vol. 2904, pp. 280-294, ISBN: 0302-9743, Dec 2003.

Josep Domingo-Ferrer, Antoni Martí-nez-Ballesté and Francesc Sebé, "MINPAY: a Multi-device INternet PAY-as-you-watch system", IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC2003, Jan 2003.

Josep Domingo-Ferrer, "Networking in the new ICT curricula", IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC2003, Jan 2003.

Josep Domingo-Ferrer and Vicenç Torra, "Trends in aggregation and security assessment for inference control in statistical databases", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 10, pp. 453-458, Oct 2002, ISSN: 0218-4885.

Francesc Sebé and Josep Domingo-Ferrer, "Scattering codes to implement short 3-secure fingerprinting for copyright protection", Electronics Letters, Vol. 38, pp. 958-959, Aug 2002, ISSN: 0013-5194.

Josep Domingo-Ferrer and Vicenç Torra, "A critique of the sensitivity rules usually employed for statistical table protection", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 10, pp. 545-556, May 2002, ISSN: 0218-4885.

Josep Domingo-Ferrer and Josep M. Mateo-Sanz, "Practical data-oriented microaggregation for statistical disclosure control", IEEE Transactions on Knowledge and Data Engineering, Vol. 14, no. 1, pp. 189-201, Feb 2002, ISSN: 1041-4347.

Josep Domingo-Ferrer, Josep M. Mateo-Sanz, Anna Oganian and Àngel Torres, "On the security of microaggregation with individual ranking: analytical attacks", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 10, pp. 477-492, Jan 2002, ISSN: 0218-4885.

Josep Domingo-Ferrer, "A provably secure additive and multiplicative privacy homomorphism", Information Security, In Lecture Notes in Computer Science vol. 2433, pp. 471-483, ISBN: 0302-9743, Sep 2002.

Josep Domingo-Ferrer and Vicenç Torra, "Validating distance-based record linkage with probabilistic record linkage", Topics in Artificial Intelligence, In Lecture Notes in Computer Science vol. 2504, pp. 207-215, ISBN: 0302-9743, Sep 2002.

Francesc Sebé and Josep Domingo-Ferrer, "Short 3-secure fingerprinting codes for copyright protection", Information Security, In Lecture Notes in Computer Science vol. 2384, pp. 316-327, ISBN: 0302-9743, Jun 2002.

Ramesh A. Dandekar, Josep Domingo-Ferrer and Francesc Sebé, "LHS-based hybrid microdata vs rank swapping and microaggregation for numeric microdata protection", Inference Control in Statistical Databases, In Lecture Notes in Computer Science vol. 2316, pp. 153-162, ISBN: 0302-9743, Apr 2002.

Francesc Sebé, Josep Domingo-Ferrer, Josep M. Mateo-Sanz and Vicenç Torra, "Post-masking optimization of the tradeoff between information loss and disclosure risk in masked microdata sets", Inference Control in Statistical Databases, In Lecture Notes in Computer Science vol. 2316, pp. 163-171, ISBN: 0302-9743, Apr 2002.

Josep Domingo-Ferrer, Anna Oganian and Vicenç Torra, "Information-theoretic disclosure risk measures in statistical disclosure control of tabular data", Proceedings of the 14th Intl. Conf. on Scientific and Statistical DataBase Management, Jan 2002.

Josep Domingo-Ferrer, Antoni Martí-nez-Ballesté and Francesc Sebé, "MICROCAST: Smart card based (micro)pay-per-view for multicast services", Proceedings of IFIP/USENIX 5th Smart Card Research and Advanced Application Conference-CARDIS2002, Jan 2002.

Josep Domingo-Ferrer and Antoni Martí-nez-Ballesté, "STREAMOBILE: Pay-per-view video streaming to mobile devices over the Internet", Proceedings of the 13th International Workshop on Database and Expert Systems Applications DEXA2, Jan 2002.

Josep Domingo-Ferrer and Vicenç Torra, "Extending microaggregation procedures using defuzzification methods for categorical variables", Proceedings of the First International Symposium on Intelligent Systems (IS2002), Jan 2002.

Josep Domingo-Ferrer and Vicenç Torra, "Approximating fuzzy measures by hierarchically decomposable ones", Proceedings of the Fifth International Conference on Information Fusion. FUSION2002, Jan 2002.

Josep Domingo-Ferrer and Francesc Sebé, "Invertible spread-spectrum watermarking for image authentication and multilevel access to precision-critical watermarked images", IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC2002, Jan 2002.

Josep Domingo-Ferrer and Francesc Sebé, "Enhancing watermark robustness through mixture of watermarked digital objects", IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC2002, Jan 2002.

Josep Domingo-Ferrer and Pieter H. Hartel, "Current directions in smart cards", Computer Networks, Vol. 36, pp. 377-379, Jul 2001, ISSN: 1389-1286.

Josep Domingo-Ferrer, "Advances in inference control in statistical databases: an overview", Inference Control in Statistical Databases, In Lecture Notes in Computer Science vol. 2316, pp. 1-8, ISBN: 0302-9743, Apr 2002

Josep Domingo-Ferrer, "Mobile agent route protection through hash-based mechanisms", Progress in Cryptology - Indocrypt 2001, In Lecture Notes in Computer Science vol. 2247, pp. 17-29, ISBN: 0302-9743, Dec 2001.

Francesc Sebé and Josep Domingo-Ferrer, "Oblivious image watermarking robust against scaling and geometric distortions", Proceedings of the 4th International Conference on Information Security - ISC 01, In Lecture Notes in Computer Science vol. 2200, pp. 420-432, ISBN: 0302-9743, Oct 2001.

Josep Domingo-Ferrer, Josep M. Mateo-Sanz and Vicenç Torra, "Comparing SDC methods for microdata on the basis of information loss and disclosure risk", Pre-proceedings of ETK-NTTS2001, Jan 2001.

Josep Domingo-Ferrer, Josep M. Mateo-Sanz and Francesc Sebé, "Watermarking for multilevel access to statistical databases", IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC2001, Jan 2001.

Josep Domingo-Ferrer and J. Herrera-Joancomartí-, "Short collusion-secure fingerprints based on dual binary Hamming codes", Electronics Letters, Vol. 36, pp. 1997-1699, Sep 2000, ISSN: 0013-5194.

Francesc Sebé, Josep Domingo-Ferrer and Jordi Herrera-Joancomartí-, "Spatial-Domain Image Watermarking Robust Against Compression, Filtering, Cropping and Scaling", Information Security, In Lecture Notes in Computer Science vol. 1975, pp. 44-53, ISBN: 0302-9743, Dec 2000.

Josep Domingo-Ferrer and Jordi Herrera-Joancomartí-, "Efficient smart-card based anonymous fingerprinting", Proceedings of the The International Conference on Smart Card Research and Applications - CARDIS 98 , In Lecture Notes in Computer Science vol. 1820, pp. 231-238, ISBN: 0302-9743, Oct 2000.

Josep Domingo-Ferrer, Josep M. Mateo-Sanz and R. X. Sánchez del Castillo, "Cryptographic techniques in statistical data protection", Proceedings of the Joint UN/ECE-Eurostat Work Session on Statistical Data Confidentiality, Jan 2000.

Jordi Castellà, Josep Domingo-Ferrer, Jordi Herrera-Joancomartí- and Jordi Planes, "A performance comparison of Java Cards for micropayment implementation", Smart Card Research and Advanced Application-Proc. of IFIP CARDIS2000, Jan 2000.

Josep Domingo-Ferrer and Jordi Herrera-Joancomartí, "Simple collusion-secure fingerprinting schemes for images", IEEE Intl. Conf. on Information Technology: Coding and Computing-ITCC2000, Jan 2000.

Josep Domingo-Ferrer and Josep M. Mateo-Sanz, "On resampling for statistical confidentiality in contingency tables", Computers & Mathematics with Applications, Vol. 0, pp. 13-32, Dec 1999, ISSN: 0898-1221.

Josep Domingo-Ferrer, Jordi Herrera-Joancomartí-, "Spending programs: A tool for flexible micropayments", Information Security, In Lecture Notes in Computer Science vol. 1729, pp. 1-13, ISBN: 0302-9743, Nov 1999.

Josep Domingo-Ferrer, "Anonymous fingerprinting based on committed oblivious transfer", Public Key Cryptography, In Lecture Notes in Computer Science vol. 1560, pp. 43-52, ISBN: 0302-9743, Mar 1999

Josep Domingo-Ferrer, "Anonymous fingerprinting of electronic information with automatic identification of redistributors", Electronics Letters, Vol. 34, pp. 1303-1304, Jun 1998, ISSN: 0013-5194.

Josep M. Mateo-Sanz and Josep Domingo-Ferrer, "A method for data-oriented multivariate microaggregation", Statistical data protection - SDP 1998, Lisbon, In Statistical data protection. Proceedings of the conference, pp. 89-99, ISBN: 92-828-1712-1, Mar 1998.

J. Castilla, J. Domingo-Ferrer and R. X. Sánchez del Castillo, "Dike: A Prototype for Secure Delegation of Statistical Data", Statistical data protection - SDP 1998, Lisbon (Portugal), In Statistical data protection. Proceedings of the conference, pp. 177-186, ISBN: 92-828-1712-1, Mar 1998.

Josep Domingo-Ferrer, "Multi-application smart cards and encrypted data processing", Future Generation Computer Systems, Vol. 13, pp. 65-74, Jun 1997, ISSN: 0167-739X.

Josep Domingo-Ferrer and Ricardo X. Sánchez del Castillo, "An implementable scheme for secure delegation of statistical data", Information Security, In Lecture Notes in Computer Science vol. 1334, pp. 445-451, ISBN: 0302-9743, Nov 1997.

CRISES - Security & Privacy		
Características generales	Características del Equipo de Investigación	Características de la Investigación

PUBLICACIONES RELACIONADAS DESTACADAS
Josep Domingo-Ferrer, "A new privacy homomorphism and applications", Information Processing Letters, Vol. 60, pp. 277-282, Dec 1996, ISSN: 0020-0190
Josep Domingo-Ferrer, "Achieving rights untransferability with client-independent servers", Designs, Codes and Cryptography, Vol. 8, pp. 263-272, Dec 1996, ISSN: 0925-1022.
Josep Domingo-Ferrer and Josep M. Mateo-Sanz, "On the security of cell suppression in contingency tables with quantitative factors", Proceedings of the 3rd International Seminar on Statistical Confidentiality, Jan 1996.
Josep Domingo-Ferrer, "Privacy homomorphisms for subcontracting statistical computation", Proceedings of the 3rd International Seminar on Statistical Confidentiality, Jan 1996.
Josep Domingo-Ferrer, "Multi-application smart cards and encrypted data processing", Smart Card Research and Advanced Application - CARDIS1996, Jan 1996.
Josep Domingo-Ferrer, "Untransferable rights in a client-independent server environment", Advances in Cryptology - EUROCRYPT 93, In Lecture Notes in Computer Science vol. 765, pp. 260-266, ISBN: 0302-9743, May 1994.

PROYECTOS RELEVANTES

MobidataLab: Labs for prototyping future Mobility Data sharing cloud solutions (EC Horizon 2020, MG-4-7-2020, GA: 101006879). Duration: 2021-2024. IP: Josep Domingo-Ferrer

SoBigData++: European Integrated Infrastructure for Social Mining and Big Data Analytics (EC Horizon 2020, INFRAIA-2018-2020, GA: 871042). Duration 2020-2023. IP: Josep Domingo-Ferrer

CLEANUP: Machine Learning for the Anonymisation of Unstructured Personal Data (Norwegian Research Council). Duration 2020-2023. IP: David Sánchez

DRAC: Designing RISC-V-based Accelerators for next generation Computers (FEDER-Generalitat de Catalunya, Associacions d'agrupacions emergents, ref. 001-P-001723). Duration: 2020-2022. IP: Oriol Farràs

FEM IoT: Fostering the Emerging Market of Internet of Things (FEDER-Generalitat de Catalunya, Associacions d'agrupacions emergents, ref. 001-P-001662). Duration: 2020-2022. IP: Jordi Castellà

BANDIT: Advanced Blockchain Attacks and Defense Techniques (EC Horizon 2020, MSCA-ITN-2018, GA: 814284). Duration: 2019-2023. IP: Josep Domingo-Ferrer

CONSENT: GDPR-compliant CONSumer oriENTed IOT (Spanish Ministerio de Ciencia, Innovación y Universidades, ref. RTI2018-095094-B-C21). Duration: 2019-2021. IP: Josep Domingo-Ferrer and Jordi Castellà

Sec-MCloud: Manejo de datos privado y seguro en entornos multicloud sin criptografia (Spanish Ministerio de Ciencia, Innovación y Universidades, ref. RTI2018-095094-B-C21). Duration: 2017-2020. IP: Maria Bras and David Sánchez

CANVAS: Constructing an Alliance for Value-driven Cybersecurity (EC Horizon 2020, DS-2015-1, GA: 700540). Duration: 2016-2019. IP: Josep Domingo-Ferrer

CLARUS: a framework for user centred privacy and security in the cloud (EC Horizon 2020, ICT-2014-, GA: 644024). Duration: 2015-2017. IP: Josep Domingo-Ferrer

Inter-Trust: Interoperable Trust Assurance Infrastructure (EC FP7, ICT, GA: 317731). Duration: 2012-2015. IP: Josep Domingo-Ferrer

DwB: Data without Boundaries (EC FP7, INFRA-2010, GA: 262608). Duration: 2011-2015. IP: Josep Domingo-Ferrer

ESSNet-SDC: A Network of Excellence in the European Statistical System in the field of Statistical Disclosure Control (European Comission, Ref: 5200.2005.003-2007.670). Duration: 2008-2009. IP: Josep Domingo-Ferrer

CENEX-SDC: Centre of Excellence on Statistical Disclosure Control (European Comission, ref. 25200.2005.001-2005.619). Duration: 2006.

RESET: Roadmaps for European research on Smartcard Technologies (European Comission, FP5, ref. IST-2001-37936). Duration: 2002-2003

AMRADS: Accompanying Measure for R&D in Statistics (European Comission, FP5, ref. IST-2000-26125). Duration: 2001-2003

CO-ORTHOGONAL: Co-Orthogonal Codes in Cryptography, Data Security, Watermarking and Entity Authentication (European Comission, FP5, ref. IST-2001-32012). Duration: 2001-2002. IP: Josep Domingo-Ferrer

PROYECTOS RELEVANTES

CASC: Computational Aspects of Statistical Confidentiality (European Comission, FP5, ref. IST-2000-25069). Duration: 2001-2003. IP: Josep Domingo-Ferrer

CO-UTILITY: Conciliating individual freedom and common good in the information society (Templeton World Charity Foundation, ref. TWCF0095/AB60). Duration: 2014-2017. IP: Josep Domingo-Ferrer

PRIVATEDISCOUNT: Privacy-preserving loyalty and group discounts (Google Faculty Award). Duration: 2014-2015. IP: Josep Domingo-Ferrer

Research Data Center-based Confidentiality (U. S. Census Bureau & National Science Foundation, ref. 47632-10043. Duration: 2004-2006. IP: Josep Domingo-Ferrer

OTTILIE-R: Optimizing the Tradeoff beTween Information Loss and dIsclosurE risk for continuous microdata (U. S. Bureau of the Census, ref. OBLIG-2000-29158-0-0). Duration: 2000-2001. IP: Josep Domingo-Ferrer

SECURITAS: Red de investigación en ciberseguridad y privacidad, (Ministerio de Ciencia, Innovación y Universidades, ref. RED2018-102321-T). Duration: 2020-2021. IP: Josep Domingo-Ferrer

ISSUM: Integrated System for Smart Urban Mobility (Dirección General de Tráfico, ref. SPIP2017-02250). Duration: 2017-2018. IP: Alexandre Viejo.

SPARK & GO (Dirección General de Tráfico, ref. SPIP2015-01783). Duration: 2057-2016. IP: Jordi Castellà

Red de excelencia Consolider ARES (Ministerio de Econonomia y Competitividad, ref. TIN2015-70054-REDC). Duration: 2015-2017. IP: Josep Domingo-Ferrer

SmartGlacis: Tecnologías de seguridad y privacidad para ciudades inteligentes (Ministerio de Economía y Competitividad, ref. TIN2014-57364-C2-1-R). Duration: 2015-2018. IPs: Josep Domingo-Ferrer y Jordi Castellà

MobileKey: Desarrollo de un mecanismo de aprovisionamiento de certificados digitales para entornos móviles (Ministerio de Economía y Competitividad, ref. RTC-2014-2552-7). Duration: 2014-2016. IP: Jordi Castellà

BallotNext: Diseño y desarrollo de un sistema de votación avanzado basado en papel (Ministerio de Industria, Turismo y Comercio, INNPACTO, ref. IPT-2012-0603-430000). Duration: 2013-2015. IP: Jordi Castellà

ICWT: In cloud we trust? improving trust in the cloud via security, privacy, reli- ability, and integrity (Ministerio de Economía y Competitividad, ref. TIN2012-32757). Duration: 2013-2015. IP: Maria Bras.

CO-PRIVACY: Privacidad sostenible para una sociedad de la información sostenible (Ministerio de Ciencia e Innovación, ref. TIN2011-27076-C03-01). Duration: 2012-2016. IP: Josep Domingo-Ferrer

eVerification/2: Verificación electrónica para sistemas de votación electrónica presencial (Ministerio de Industria, Turismo y Comercio, AVANZA I+D, ref. TSI-020100-2011-39). Duration: 2011-2013. IP: Jordi Castellà

SECloud: Investigación y desarrollo de una plataforma SEgura para aplicaciones Cloud computing (Ministerio de Industria, Turismo y Comercio, AVANZA I+D, ref. TSI-020302-2010-153). Duration: 2010-2013. IP: Jordi Castellà

Audit Transparency Voting Process (Ministerio de Industria, Turismo y Comercio, INNPACTO, ref. IPT-430000- 2010-31). Duration: 2010-2012. IP: Jordi Castellà

PROYECTOS RELEVANTES

RIPUP: Peer-to-peer User-Private Information Retrieval (Ministerio de Ciencia e Innovación, ref. TIN2009-11689). Duration: 2010-2012. IP: Maria Bras

eVerification: Verificación electrónica para sistemas de votación electrónica presencial (Ministerio de Industria, Turismo y Comercio, AVANZA I+D, ref. TSI-020100-2009-720). Duration: 2009-2010. IP: Jordi Castellà

ARES: team for Advanced REsearch on Information Security and privacy (Ministerio de Educación y Ciencia, CONSOLIDER INGENIO 2010, ref. CSD2007-00004). Duration: 2007-2014. IP: Josep Domingo-Ferrer

E-AEGIS: Escudo electrónico para conciliar la privacidad de los consumidores la seguridad de las transacciones en la sociedad de la información (Ministerio de Educación y Ciencia, ref. TSI2007-65406-C03-01). Duration: 2007-2012. IP: Josep Domingo-Ferrer

PROPRIETAS: Protección de la propiedad intelectual y privacidad en multicast sobre redes móviles ad-hoc (Ministerio de Educación, Cultura y Deporte, ref. SEG2004-04352-C04-01). Duration: 2004-2007. IP: Josep Domingo-Ferrer

STREAMOBILE: Streaming de contenidos multimedia hacia dispositivos móviles con retribución por micropago (Ministerio de Ciencia y Tecnología, ref. TIC2001-0633-C03). Duration: 2001-2003. IP: Josep Domingo-Ferrer

Comercio electrónico seguro basado en la información (Ministerio de Ciencia y Tecnología, ref. TEL98-0699-C02-02). Duration: 1998-2001. IP: Josep Domingo-Ferrer

Intercambio electrónico seguro de datos y documentos multimedia (Ministerio de Ciencia y Tecnología, ref. TIC95-0903-C02-02). Duration: 1995-1997. IP: Josep Domingo-Ferrer

Criptografía y seguridad de acceso en la red de banda ancha (Ministerio de Ciencia y Tecnología, ref. TIC92-1323-E). Duration: 1992-1994. IP: Josep Domingo-Ferrer

Security and privacy of individual data used to extract public information (Australian Research Council, ref. DP160100913). Duration: 2015-2016. IP: Josep Domingo-Ferrer