CURRICULUM VITAE

NAME	Carmela González Troncoso	TELEPHONE	+41 21 69 37180
ADDRESS	EPFL IC IINFCOM SPRING BC 258 (Batiment BC) Station 14, CH-1015 Lausanne Switzerland	E-MAIL	carmela.troncoso@epfl.ch

ACADEMIC POSITIONS AND EMPLOYMENT

École Polytechnique Féderale de Lausanne, Switzerland

Nov 2017 – ongoing *Tenure Track Assistant Professor*

IMDEA Software Institute, *Spain*

Oct 2015 – September 2017 Senior Researcher (Faculty member)

Galician Research and Development Center in Advanced Telecomunications (Gradiant), Spain

Dec 2014 – Sep 2015 *Security and Privacy Technical Lead (leading a group of 5 people)*

Sep 2012 – Nov 2014 *Post-doctoral Researcher*

COSIC Group, ESAT, Katholieke Universiteit Leuven , Belgium

Apr 2011 – Sep 2012 *Post-doctoral Researcher*

Oct 2006 – Apr 2011 *PhD Candidate*

Microsoft Research Cambridge, UK

Sept 2008 – Nov 2008 *Intern (Supervisor: George Danezis)*

Education

Oct 2006 – Apr 2011 **PhD** *COSIC Group, ESAT, Katholieke Universiteit Leuven , Belgium*

PhD Thesis: “Design and analysis methods for privacy technologies”. Advisors: Prof. Bart Preneel and Prof. Claudia Diaz.

- awarded summa cum laude with the congratulations of the board of examiners (only awarded in exceptional circumstances, at most 5% of the doctorates in engineering at K.U.Leuven)

- winner of the ERCIM STM WG 2012 Award for the Best Ph.D. Thesis on Security and Trust Management.

Sep 2005 – May 2006 **MSc Thesis (Hons)** *University of Vigo, Spain / Université Henri Poncaré, France*

MSc Thesis: "Development of a web application to the conversion of learning agreements in the ERASMUS program." (Honor Mention) Advisors: Prof. Juan Carlos Burguillo and Prof. Christophe Simon.

Sep 2000 – Sep 2005 **Bsc in Telecommunication Engineering** *University of Vigo, Spain*

Two specializations: Telematics and Electronics

Sep 1996 – Sep 2000 **High School Diploma (Hons)** *University of Vigo, Spain*

POSITIONS OF RESPONSIBILITY

- **Co-Editor-in-Chief (and Program Chair) of Proceedings on Privacy Enhancing Technologies** (2018,2019)
- **PET Award Chair** (2016, 2017)
- **Poster and Demo Chair** ACM Computers and Communications Security (2013)
- **Program Chair** Hot Topics in Privacy Enhancing Technologies Workshop (2010,2011)

- **General Chair** Privacy Enhancing Technologies Symposium (2012), IEEE International Workshop on Information Forensics and Security (2017)
- **Publicity Chair** Privacy Enhancing Technologies Symposium (2014)
- **Member of the Board** of the Privacy Enhancing Technologies Symposium (2011-)

- **Selected Program Committee Membership:**
  IEEE Security and Privacy Symposium (2016-2018)
  ACM Asia Conference on Computers and Communications Security (2017)
  ACM Conference on Computers and Communications Security (2013, 2014, 2017)
  Privacy Enhancing Technologies Symposium (2010, 2011, 2013, 2014, 2017)
  International Conference on Financial Cryptography and Data Security (2012, 2015, 2016)
  European Symposium on Research in Computer Security (2011, 2012, 2013)
  Workshop on Privacy in the Electronic Society (2012, 2013)
  Selected Areas in Cryptography (2015)
- **Selected Journal reviews:**
  Elsevier Computers & Security
  IEEE Transactions on Mobile Computing
  IEEE Transactions on Dependable and Secure Computing
  IEEE Security & Privacy Magazine
  ACM Transactions on Information and System Security

- **Evaluator H2020 Project Proposals** (2015: H2020 CAPS ICT10)
- **Scientific Committee Member** of the Summer school on real-world crypto and privacy (2016-)
- **Expert** for the European Union Agency for Network and Information Security (ENISA) (2015-)
- **ERCIM STM 2016 PhD Thesis Award Committee** (2016)
- **Doctoral thesis examiner:** Anna Krasnova (RU Nijmegen), Alvaro Garcia (INRIA), Michael Herrmann (KU Leuven), Federico Olmedo (Polytechnica University Madrid), Juan Elices (University New Mexico)

FUNDING

- **Individual Grants**

2008-2011	**PhD Fellowship**	*Flemish Research Foundation (FWO), Belgium*
2007-2008	**Postgraduate Grant**	*Fundación Barrie de la Maza, Spain*

- **Principal investigator** of three European Projects (2013-2016)
  PRIPARE – Preparing Industry to Privacy-by-design by sypporting its Application in Research (FP7 GA number 610613) BUDGET: 78.324,00 €
  WITDOM - empoWering prIvacy and securiTy in non-trusteD envirOnMents (H2020 GA number 644371) BUDGET: 219.487,50 €.
  NEXTLEAP - NEXt Generation Technosocial and Legal Encryption Access and Privacy (H2020 GA number TBA) BUDGET: 298.856,25 €

- **Principal investigator** of three Spanish National Projects (2013-2015)
  EMRISCO – Respuesta a emergencias en comunidades inteligentes: Credibilidad de la información y seguridad (I+D+i Orientada a los Retos de la Sociedad TEC2013-47665-C4-2-R) BUDGET: 30.000,00 €.
  INRISCO – Monitorización de incidentes en comunidades inteligentes: Seguridad, Privacidad y diseño de arquitectura Big Data (I+D+i Orientada a los Retos de la Sociedad TEC2014-54335-C4-4-R) BUDGET: 30.000,00 €.
  DataMantium – Computación y comunicaciones seguras en la nube para entornos hostiles (RETOS-COLABORACIÓN 2016) BUDGET: 321.594,00 €.

Invited talks

- **Keynote:** *Bayesian inference to evaluate information leakage in complex scenarios.* ACM Information Hiding and Multimedia Security Workshop (2013)
- **Keynote:** *Design and analysis methods for privacy technologies.* International Workshop on Security and Trust Management (2012).

Awards

- Best Reviewer Award at the 38th IEEE Security and Privacy Symposium (2017)
- Best Reviewer Award at the 37th IEEE Security and Privacy Symposium (2016)
- ERCIM STM WG 2012 Award for the Best Ph.D. Thesis on Security and Trust Management (2012)
- Best Student Paper Award at IEEE Intl. Workshop on Information Forensics and Security (2011)
- University of Vigo Enrolment Award for High School outstanding students (2000)

TEACHING & STUDENT SUPERVISION

- **PhD Co-advisor** of one student University of Vigo (2013-) working on the application of signal processing techniques to privacy problems, and advisor of one student at IMDEA Software Institute (2016-) working on privacy aspects of decentralization.
- **Supervised eight undergraduate final year projects**: privacy implications of Open Data (2016), study of CryptDB performance (2013), privacy-preserving social networks (2010), implementation of an anonymous credential server (2009), modeling of privacy technologies in vehicular environments (2009), implementation of the NTRU cryptosystem on a smart card (2009), implementation of credentials on a smart card (2008), long-term archival of files (2008), and Thunderbird extension to collect users' profiles (2008).
- **Teaching Assistant** Problem Solving and Development: Embedded Systems and Multimedia (KULeuven, 2007-2009).
- **Summer-school lecturer**:
  - "*Introduction to Traffic Analysis*" at Summer school on real-world crypto and privacy (2016)
  - "*Introduction to Traffic Analysis*" at EPFL Summer Research Institute (2016)
  - "*Introduction to Privacy*" at Intensive Programme on Information and Communication Systems Security (2016).

PATENTS

- METHOD AND SYSTEM FOR AUTHENTICATION BY MEANS OF TOKENS. S. Patureau Mirand, C. Troncoso, D. Chaves Dieguez. WO2015193578. December 2015.

OTHER

- NATIONALITY: Spanish
- LANGUAGES (ILR SCALE): Spanish (Native), English (Full professional proficiency), French (Limited working proficiency), Dutch (Elementary proficiency).
- Member of the Association for Computing Machinery (ACM).

PEER-REVIEWED PUBLICATIONS

The computer security community publishes in international high-impact peer-reviewed conferences with acceptance rates often lower than 15%-20%. The most prestigious venues in the field are the IEEE Symposium on Security and Privacy, ACM Computer and Communications Security (CCS), USENIX Security Symposium and the ISOC Conference on Network and Distributed Systems Security (NDSS). Top publications comprise papers published in these selected venues, as well as publications with more than 50 citations (according to Google Scholar in November 2016).

BIBLIOMETRICS (Google Scholar September 2017)

h-index: 19 (17 since 2011); citations: 1429 (1147 since 2011); peak rate: 238 citations/year in 2015.

TOP PUBLICATIONS

1. Apostolos Pyrgelis, Carmela Troncoso, and Emiliano De Cristofaro. Knock Knock, Who's There? Membership Inference on Aggregate Location Data. NDSS 2018.
2. S. Oya, C. Troncoso, and F. Pérez-González: “Back to the Drawing Board: Revisiting the Design of Optimal Location Privacy-preserving Mechanisms”. In ACM Conference on Computer and Communications Security (CCS 2017), 2017.
3. S. Matic, C. Troncoso, J. Caballero: “Dissecting Tor Bridges: a Security Evaluation of their Private and Public Infrastructures”. In Network and Distributed System Security Symposium (NDSS 2017), 2017.
4. R. Shokri, G. Theodorakopoulos, C. Troncoso, J. Hubaux, and J. Le Boudec, "Protecting Location Privacy: Optimal Strategy against Localization Attacks" In 19th ACM Conference on Computer and Communications Security (CCS 2012), ACM, 617-627, 2012. (144 citations)
5. E. Balsa, C. Troncoso, and C. Diaz, "OB-PWS: Obfuscation-Based Private Web Search," In IEEE Symposium on Security and Privacy 2012, IEEE, 491-505, 2012. (39 citations).
6. P. Mittal, F. Olumofin, C. Troncoso, N. Borisov, and I. Goldberg, "PIR-Tor: Scalable Anonymous Communication Using Private Information Retrieval," In 20th USENIX Security Symposium 2011, Usenix, 17 pages, 2011. (41 citations)
7. S. F. Gürses, C. Troncoso, and C. Diaz, "Engineering Privacy by Design," In Computers, Privacy & Data Protection, 25 pages, 2011. (96 citations)
8. J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede, "PrETP: Privacy-Preserving Electronic Toll Pricing," In 19th USENIX Security Symposium 2010, Usenix, pp. 63-78, 2010. (105 citations)
9. R. Shokri, C. Troncoso, C. Diaz, J. Freudiger, and J. Hubaux, "Unraveling an Old Cloak: k-anonymity for Location Privacy," In Proceedings of the 9th ACM workshop on Privacy in the electronic society (WPES 2010), K. Frikken (ed.), ACM, pp. 115-118, 2010. (86 citations)
10. C. Troncoso, and G. Danezis, "The Bayesian Analysis of Mix Networks," In Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS 2009), E. Al-Shaer, S. Jha, and A. D. Keromytis (eds.), ACM, pp. 369-379, 2009. (45 citations)
11. C. Troncoso, B. Gierlichs, B. Preneel, and I. Verbauwhede, "Perfect Matching Disclosure Attacks," In Privacy Enhancing Technologies Symposium, PETS 2008, Lecture Notes in Computer Science 5134, N. Borisov, and I. Goldberg (eds.), Springer-Verlag, pp. 2-23, 2008. (66 citations)
12. G. Danezis, C. Diaz, and C. Troncoso, "Two-Sided Statistical Disclosure Attack," In Proceedings of Privacy Enhancing Technologies Workshop, PET 2007, Lecture Notes in Computer Science 4776, N. Borisov, and P. Golle (eds.), Springer-Verlag, pp. 30-44, 2007. (59 citations)
13. G. Danezis, C. Diaz, C. Troncoso, and B. Laurie, "Drac: An Architecture for Anonymous Low-Volume Communications," In Privacy Enhancing Technologies - 10th International Symposium, PETS 2010, Lecture Notes in Computer Science 6205, M. J. Atallah, and N. J. Hopper (eds.), Springer-Verlag, pp. 202-219, 2010. (52 citations)
14. C. Troncoso, G. Danezis, E. Kosta, and B. Preneel, "PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance," In ACM workshop on Privacy in the electronic society (WPES 2007), T. Yu (ed.), ACM, pp. 99-107, 2007. (104 citations)

JOURNAL PUBLICATIONS

1. A. Pyrgelis, C. Troncoso, and E. De Cristofaro: “What Does The Crowd Say About You? Evaluating Aggregation-based Location Privacy“. Proceedings on Privacy Enhancing Technologies, PoPETs 2017(4), 2017.
2. C. Troncoso, M. Isaakidis, G. Danezis, and H. Halpin: “Systematizing Decentralization and Privacy: Lessons from 15 years of research and deployments“. Proceedings on Privacy Enhancing Technologies, PoPETs 2017(4), 2017.
3. R. Shokri, G. Theodorakopoulos, C. Troncoso: “Privacy Games along Location Traces”. In ACM Transactions on Privacy and Security 11:(1): 11-31, 2017.
4. S. Oya, F. Pérez-González, C. Troncoso: “Design of pool mixes against profiling attacks in real conditions”. In IEEE/ACM Transactions on Networking 24(6): 3662-3675, 2016.
5. F. Pérez-González, C. Troncoso, S. Oya: “A Least Squares Approach to the Static Traffic Analysis of High-Latency Anonymous Communication Systems“. IEEE Transactions on Information Forensics and Security 9(9): 1341-1355 (2014)
6. E. Balsa, C. Troncoso, and C. Diaz: “A Metric to Evaluate Interaction Obfuscation in Online Social Networks“. In International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 20(6): 877-892, 2012.
7. C. Troncoso, G. Danezis, E. Kosta, J. Balasch, and B. Preneel, "PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance (Journal version)," IEEE Transactions on Dependable and Secure Computing 8(5), pp. 742-755, 2011.
8. C. Troncoso, E. Costa-Montenegro, C. Diaz, and S. Schiffner, "On the difficulty of achieving anonymity for Vehicle-2-X communication," Computer Networks 55(14), pp. 3199-3210, 2011.

PUBLICATIONS IN SPECIALIZED VENUES

1. Chen Chen , Daniele E. Asoni, Adrian Perrig, David Barrera, George Danezis, and Carmela Troncoso. TARANET: Traffic-Analysis Resistant Anonymity at the NETwork layer. IEEE EuroS&P 2018.
2. J. Hayes, C. Troncoso, and G. Danezis: “TASP: Towards Anonymity Sets that Persist“. ACM Workshop on Privacy in the Electronic Society, ACM, pp 177-180, 2016.
3. S. Oya, C. Troncoso, and F. Pérez-González: “Do Dummies Pay Off? Limits of Dummy Traffic Protection in Anonymous Communications“. Privacy Enhancing Technologies Symposium 2014: 204-223.
4. G. Theodorakopoulos, R. Shokri, C. Troncoso, J-P. Hubaux, and J-Y Le Boudec: “Prolonging the Hide-and-Seek Game: Optimal Trajectory Privacy for Location-Based Services“ ACM Workshop on Privacy in the Electronic Society 2014: 73-82.
5. G. Danezis,and C. Troncoso: “You cannot hide for long: de-anonymization of real-world dynamic behaviour“. ACM Workshop on Privacy in the Electronic Society 2013: 49-60
6. M. Herrmann,C. Troncoso,C. Diaz, and B. Preneel: “Optimal sporadic location privacy preserving systems in presence of bandwidth constraints“. ACM Workshop on Privacy in the Electronic Society 2013: 167-178
7. F. Perez-Gonzalez, and C. Troncoso: “Understanding Statistical Disclosure: A Least Squares approach“, In Privacy Enhancing Technologies Symposium, PETS 2012, Lecture Notes in Computer Science 7384, S. Fischer-Huebner, and M. Wright (eds.), Springer-Verlag, pp. 38-57, 2012.
8. C. Diaz, S. Murdoch, and C. Troncoso, "Impact of Network Topology on Anonymity and Overhead in Low-Latency Anonymity Networks," In Privacy Enhancing Technologies Symposium, PETS 2010, Lecture Notes in Computer Science 6205, M. J. Atallah, and N. J. Hopper (eds.), Springer-Verlag, pp. 184-201, 2010.
9. G. Danezis, and C. Troncoso, "Vida: How to use Bayesian inference to de-anonymize persistent communications," In Privacy Enhancing Technologies Symposium, PETS 2009, Lecture Notes in Computer Science 5672, M. J. Atallah, and I. Goldberg (eds.), Springer-Verlag, pp. 406-423, 2009.

10. B. Gierlichs, C. Troncoso, C. Diaz, B. Preneel, and I. Verbauwhede, "Revisiting A Combinatorial Approach Toward Measuring Anonymity," In ACM workshop on Privacy in the electronic society (WPES 2008), V. Atluri , and M. Winslett (eds.), ACM, pp. 111-116, 2008.
11. C. Diaz, C. Troncoso, and A. Serjantov, "On the Impact of Social Network Profiling on Anonymity," In Privacy Enhancing Technologies Symposium, PETS 2008, Lecture Notes in Computer Science 5134, N. Borisov, and I. Goldberg (eds.), Springer-Verlag, pp. 44-62, 2008.
12. C. Diaz, C. Troncoso, and G. Danezis, "Does additional information always reduce anonymity?," In ACM workshop on Privacy in the electronic society (WPES 2007), T. Yu (ed.), ACM, pp. 72-75, 2007.

OTHER PEER-REVIEWED PUBLICATIONS

1. Bogdan Kulynych and Carmela Troncoso. Feature importance scores and lossless feature pruning using Banzhaf power indices. NIPS 2017 Symposium on Interpretable Machine Learnin.g
2. Bogdan Kulynych, Marios Isaakidis, Carmela Troncoso, and Geore Danezis. Modern key distribution with ClaimChain. 34c3: 34th Chaos Communication Congress. 2017
3. O. Kennedy, D. R. Hipp, S. Idreos, A. Marian, A. Nandi, and C. Troncoso, E. Wu, “Small Data”, In 33rd IEEE International Conference on Data Engineering (ICDE 2017), IEEE, pp. 1475-1476, 2017.
4. S. Oya, F. Pérez-González, and C. Troncoso, “Filter design for delay-based anonymous communications”, in IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), IEEE, pp. 2107-2111, 2017.
5. S. Gurses, C. Troncoso, C. Diaz. "Engineering Privacy by Design Reloaded". Amsterdam Privacy Conference. 2015
6. C. Troncoso: "Bayesian inference to evaluate information leakage in complex scenarios". IH&MMSec 2013: 1-2
7. M. Fontani,E. Argones-Rúa,C. Troncoso, and M. Barni: "The watchful forensic analyst: Multi-clue information fusion with background knowledge" In IEEE International Workshop on Information Forensics and Security (WIFS 2013): 120-125, 2013.
8. F. Perez-Gonzalez, and C. Troncoso, "A Least Squares Approach to User Profiling in Pool Mix-based Anonymous Communication Systems," In IEEE International Workshop on Information Forensics and Security (WIFS 2012), IEEE, 115-120, 2012
9. J. A. Elices, F. Perez-Gonzalez, and C. Troncoso, "Fingerprinting Tor's Hidden Service Log Files Using a Timing Channel," In IEEE International Workshop on Information Forensics and Security (WIFS 2011), IEEE, 6 pages, 2011.
10. P. Mittal, N. Borisov, A. Rial, and C. Troncoso, "Scalable Anonymous Communication with Provable Security," In USENIX Workshop on Hot Topics in Security 2010, USENIX, 7 pages, 2010.
11. G. Danezis, C. Diaz, E. Käsper, and C. Troncoso, "The wisdom of Crowds: attacks and optimal constructions," In European Symposium on Research in Computer Security (ESORICS 2009), Lecture Notes in Computer Science 5789, M. Backes, and P. Ning (eds.), Springer-Verlag, pp. 406-423, 2009.
12. C. Diaz, C. Troncoso, and B. Preneel, "A Framework for the Analysis of Mix-Based Steganographic File Systems," In European Symposium on Research in Computer Security (ESORICS 2008), Lecture Notes in Computer Science 5283, S. Jajodia, and J. Lopez (eds.), Springer-Verlag, pp. 428-445, 2008.
13. C. Troncoso, D. De Cock, and B. Preneel, "Improving Secure Long-Term Archival of Digitally Signed Documents," In International Workshop on Storage Security and Survivability (StorageSS 2008), Y. Kim, and B. Yurcik (eds.), pp. 27-36, 2008.
14. G. Danezis, C. Diaz, S. Faust, E. Käsper, C. Troncoso, and B. Preneel, "Efficient Negative Databases from Cryptographic Hash Functions," In Information Security Conference, ISC 2007, Lecture Notes in Computer Science 4779, J. A. Garay, A. K. Lenstra, M. Mambo, and R. Peralta (eds.), Springer-Verlag, pp. 423-436, 2007.
15. C. Troncoso, C. Diaz, O. Dunkelman, and B. Preneel, "Traffic Analysis Attacks on a Continuously-Observable Steganographic File," In Information Hiding Workshop, IH 2007, Lecture Notes in Computer Science 4567, F. Cayre, G. J. Doërr, and T. Furon (eds.), Springer-Verlag, pp. 220-236, 2007