Carmela Troncoso

EPFL IC IINFCOM SPRING
Station 14, CH-1015 Lausanne
Switzerland

+41 21 69 37180
carmela.troncoso@epfl.ch
@carmelatroncoso

EDUCATION

KU Leuven, Belgium
Ph.D. in Engineering — **April 2011**
Advisors: Prof. Bart Preneel and Prof. Claudia Diaz
Dissertation: Design and analysis methods for privacy technologies

University of Vigo, Spain
MSc in Telecommunications Engineering — **May 2006**

ACADEMIC POSITIONS

École Polytechnique Féderale de Lausanne, Switzerland
Associate professor — **May 2022-ongoing**
Head of the SPRING Lab

École Polytechnique Féderale de Lausanne, Switzerland
Assistant professor — **November 2017-May 2022**
Head of the SPRING Lab

IMDEA Software Institute, Spain
Senior Researcher (equivalent to faculty member) — **October 2015-September 2017**

COSIC Group, KU Leuven, Belgium
Post-doctoral researcher — **May 2011-September 2012**

OTHER POSITIONS

Galician Research and Development Center in Advanced Telecomunications (Gradiant), Spain
Security and Privacy Technical Lead — **September 2012 – September 2015**

AWARDS

- Distinguished Paper Award IEEE Security and Privacy Symposium (2022)
- EPFL Latsis University Prize (2022)
- Best Teacher award in Computer Science at EPFL (2022)
- Distinguished Paper Award Usenix Security Symposium (2022)
- Future 50 (2021)
- Spanish Data Protection Agency Premio Emilio Aced Protección de Datos (2020)
- 40 under 40 Emerging Leaders by Fortune Magazine (2020)
- Best Paper Award Networks and Distributed Systems Symposium (2018)
- CNIL-INRIA Privacy Protection Award 2017
- 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 Paper Award -IEEE Intl. Workshop on Information Forensics and Security (2011)

SERVICE

Program Committee chair

- IEEE Conference on Secure and Trustworthy Machine Learning (co-chair with Nicolas Papernot 2024)
- USENIX Security Symposium (co-chair with Joseph Calandrino 2023)
- IEEE European Symposium on Security and Privacy (co-chair with Lujo Bauer 2021, co-chair with David Evans 2022)
- USENIX Security and AI Networking Conference (co-chair with Richard Harang 2020)
- Editor-in-Chief (and Program Chair) of Proceedings on Privacy Enhancing Technologies (co-chair with Damon McCoy and Rachel Greenstadt 2018, co-chair with Kostas Chatzikokolakis 2019)
- Hot Topics in Privacy Enhancing Technologies Workshop (co-chair with Andrei Serjantov 2010, co-chair with Julien Freudiger 2011)

General Chair

- IEEE International Workshop on Information Forensics and Security (co-chair with Teddy Furon, 2017)
- Privacy Enhancing Technologies Symposium (2012 Vigo ES, 2023 Lausanne CH)

Other organizational committees

- Co-organizer Privacy-Preserving Machine Learning (CCS Workshop) (2019,2021)
- Co-organizer Towards Trustworthy ML: Rethinking Security and Privacy for ML (ICLR Workshop) (2020)
- PET Award Chair (co-chair with Nicholas Hopper 2016, co-chair with Bryan Ford 2017)
- Publicity Chair Privacy Enhancing Technologies Symposium (2014)
- Poster/Demo Chair ACM Computers and Communications Security (co-chair with Thomas Schneider 2013)

Steering committees

- IEEE Symposium on Security and Privacy (2020-)
- Applied Machine Learning Days Academic Committee (2020-)
- Computer Security Foundations Symposium (2019-)
- Privacy Enhancing Technologies Symposium (2011-)
- Scientific Committee Member of the Summer school on real-world crypto and privacy (2016-)

Program Committee Membership

2023 EuroS&P'24

2022 **PoPETS'22, SEC'22**

2021 **PoPETS'21, Oakland'21, OSDI'21**

2020 **SEC'20, NDSS'20, NSDI'20,** EuroSys'20, EuroS&P'20

2019 WPES ’19, CSET’19, EdgeSys19, PiMLAI’19, PPML’19
2018 **Oakland’18, CCS’18,** PiMLAI’18, PPML’18
2017 AsiaCCS’17, **PETS’17**, **Oakland’17, CCS’17**
2016 **Oakland’16, FC’16**
2015 **FC’15**
2014 **CCS’14**, **PETS’14**
2013 **CCS’13 ,**WPES’13, **PETS’13**
2012 **PETS’12,** WPES’12

GRANTS

- **Swiss National Science Foundation – Research project**
  MinWeb – Web Privacy through Data Minimization (499’980 CHF, Sole PI , 2024-2028)
- **Fondation Botnar – Research project**
  EPFL Real-Time Epidemiology I-DAIR Pathfinder (5M CHF, Main PI of 11 researchers, 2020-2023)
- **Swiss National Science Foundation – Research project**
  VaultML – Preventing privacy leaks in machine learning (355'836 CHF, Sole PI , 2020-2023)
- **Google Security and Privacy Research Award** (75,000 USD, sole PI, 2018)
- **Principal investigator** European Projects (2013-2016)
  PRIPARE – Preparing Industry to Privacy-by-design by supporting its Application in Research (FP7 GA number 610613) MY SHARE: 78.324,00 €
  WITDOM - empoWering prIvacy and securiTy in non-trusteD envirOnMents (H2020 GA number 644371) MY SHARE: 219.487,50 €.
  NEXTLEAP - NEXt Generation Technosocial and Legal Encryption Access and Privacy (H2020 GA number TBA) MY SHARE: 298.856,25 €
- **Principal investigator** 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)
  MY SHARE: 30.000,00 €.
  INRISCO – Monitorización de incidentes en comunidades inteligentes: Seguridad, Privacidad y diseño de arquitectura Big Data (I+D+i Orientada a Retos de la Sociedad TEC2014-54335-C4-4-R)
  MY SHARE: 30.000,00 €.
  DataMantium – Computación y comunicaciones seguras en la nube para entornos hostiles (RETOS-COLABORACIÓN 2016)
  MY SHARE: 321.594,00 €.

- PhD Fellowship *Flemish Research Foundation (FWO), Belgium (30.000 €, personal grant,* 2008).

- Graduate Grant *Fundación Barrie de la Maza, Spain (25000€, personal grant, 2007)*

INVITED TALKS & KEYNOTES

- *Engineering Privacy Beyond the Paper.* European Symposium on Research in Computer Security. ESORICS (2023)
- *Digital Identities and the Role of Privacy Engineering.* Swiss Cyber Storm (2022)
- *Hardware for privacy engineering.* Conference on Cryptographic Hardware and Embedded Systems (2021)
- *Cryptographer’s panel.* RSA conference (2021)
- *Designing Technology in Pandemic times.* Computer Security Foundations Symposium (2021)
- *Designing Technology in Pandemic times.* CyLab series at CMU (2021)
- *Contact Tracing Apps: Engineering Privacy in Quicksand.* MOBILESoft (2021)
- *Contact Tracing Apps: Engineering Privacy in Quicksand.* USENIX Enigma (2021)
- *Privacy by Design -- From Theory to Practice in the Context of COVID-19 Contact Tracing.* Real World Cryptography (2021)
- *Is synthetic data private?* Privacy-preserving Machine Learning- PriML and PPML Joint edition (2020).

- *Engineering Privacy in Contact Tracing Apps.* International Conference on Cryptology in India (Indocrypt) (2020)
- *PETs, POTs, and pitfalls: rethinking the protection of users against machine learning*. CISPA Distinguished lecture Series (2019)
- *PETs, POTs, and pitfalls: rethinking the protection of users against machine learning*. Keynote at Usenix Security and AI Networking Conference (ScAINet) (2019)
- *Privacy technologies need to go to the gym: on the challenges of privacy engineering in an Agile world*. Keynote at IEEE International Workshop on Privacy Engineering (2019)
- *Bayesian inference to evaluate information leakage in complex scenarios.* Keynote at ACM Information Hiding and Multimedia Security Workshop (2013)
- *Design and analysis methods for privacy technologies.* Keynote at International Workshop on Security and Trust Management (2012).

TEACHING & STUDENT SUPERVISION

PhD Advisor: Simon Oya (University of Vigo, 2013-2019), Sandra Siby (EPFL 2017-2022), Sinem Sav* (2022-2023), , Christian Mouchet* (2022-2023), Sylvain Chatel* (2022-2023), Bogdan Kulynych (EPFL 2016-2023), Kasra Edalatnejadkhamene (EPFL 2017-2023), Theresa Stadler (EPFL 2020-), Klim Kireev (EPFL 2021-), Mathilde Raynal (EPFL 2021-), Boya Wang (2022-), Saiid El Hajj Chehade (2023-), Christian Knabenhans (2023-), Eric Jolles (2024-)

*Students co-advised with J.P. Hubaux

Teaching:

Information Security and Privacy, COM-402, 6 ECTS, 200+ students *(redesigned, co-instructor JP Hubaux, P. Oechslin)*	Spring 2019, Fall 2018
Advanced Topics in Privacy Technologies, CS-523, 7 ECTS, 100+ students	Fall 2018, Spring 2019, Spring 2021, Spring 2023
Computer Security, COM-310, 4 ECTS, 200+ students *(redesigned)*	Fall 2018, Fall 2019, Fall 2020, Fall 2021, Fall 2023

PATENTS

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

BIBLIOMETRICS (Google Scholar March 2023)

h-index: 36 (28 since 2019); citations: 5136 (3146 since 2019)

JOURNAL PUBLICATIONS

1. H. Abelson, R. J. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, J. Callas, W. Diffie, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, V. Teague, C. Troncoso: Bugs in our pockets: the risks of client-side scanning. J. Cybersecur. 10(1) (2024)
2. S. Siby, L. Barman, C. A. Wood, M. Fayed, N. Sullivan, C. Troncoso. Evaluating practical QUIC website fingerprinting defenses for the masses. Proceedings on Privacy Enhancing Technologies 2023(4)
3. Kasra EdalatNejad, Mathilde Raynal, Wouter Lueks, Carmela Troncoso. Private Collection Matching Protocols. Proceedings on Privacy Enhancing Technologies 2023(3).
4. C. Troncoso, D. Bogdanov, E. Bugnion, S. Chatel, C. Cremers, S. F. Gürses, J-P Hubaux, D. Jackson, J. R. Larus, W. Lueks, R. Oliveira, M. Payer, B. Preneel, A. Pyrgelis, M. Salathé, T. Stadler, M. Veale: Deploying decentralized, privacy-preserving proximity tracing. Commun. ACM 2022.
5. B. Kulynych, M. Yaghini, G. Cherubin, M. Veale, C. Troncoso. “Disparate Vulnerability to Membership Inference Attacks”. Proceedings on Privacy Enhancing Technologies, PoPETs 2022.
6. W. Lueks, S. Gürses, M. Veale, E. Bugnion, M. Salathé, K. G. Paterson, and C. Troncoso. “CrowdNotifier: Decentralized Privacy-Preserving Presence Tracing”. Proceedings on Privacy Enhancing Technologies, PoPETs 2021(4)
7. Salathé M, Althaus C, Anderegg N, Antonioli D, Ballouz T, Bugnon E, Čapkun S, Jackson D, Kim SI, Larus J, Low N, Lueks W, Menges D, Moullet C, Payer M, Riou J, Stadler T, Troncoso C, Vayena E, von Wyl V. “Early evidence of effectiveness of digital contact tracing for SARS-CoV-2 in Switzerland”. Swiss Med Weekly. 2020.
8. V. von Wyl, S. Bonhoeffer, E. Bugnion, A. Puhan Milo, M. Salathé, T. Stadler, C. Troncoso, E. Vayena, N. Low. “A research agenda for digital proximity tracing apps”. Swiss Medical Weekly 2020.
9. W. Lueks, B. Hampiholi, G. Alpar, and C. Troncoso, “Tandem: Securing Keys by Using a Central Server While Preserving Privacy” Proceedings on Privacy Enhancing Technologies, PoPETs 2020(2), 2020.
10. Á. Feal, P. Calciati, N. Vallina-Rodriguez, C. Troncoso, and A. Gorla, “Angel or Devil? A Privacy Study of Mobile Parental Control Apps” Proceedings on Privacy Enhancing Technologies, PoPETs 2020(2), 2020.
11. 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.

12. 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.
13. R. Shokri, G. Theodorakopoulos, C. Troncoso: “Privacy Games along Location Traces”. In ACM Transactions on Privacy and Security 11:(1): 11-31, 2017.
14. 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.
15. 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)
16. 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.
17. 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.
18. 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.

CONFERENCE PUBLICATIONS

1. T. Stadler, B. Kulynych, N. Papernot, M. Gastpar, C. Troncoso. The Fundamental Limits of Least-Privilege Learning. ICML 24.
2. C. Mouchet, S. Chatel, A. Pyrgelis, C. Troncoso. Helium: Scalable MPC among Lightweight Participants and under Churn. CCS 2024.
3. S. Chatel, C. Knabenhans, A. Pyrgelis, C. Troncoso, J-P. Hubaux. Verifiable Encodings for Secure Homomorphic Analytics. CCS 2024.
4. S. El Hajj Chehade, S. Siby, C. Troncoso. SINBAD: Saliency-informed detection of breakage caused by ad blocking. IEEE Security and Privacy Symposium, 2024.
5. K. EdalatNejad, W. Lueks, J. Sukaitis, V. Graf Narbel, M. Marelli, C. Troncoso. Janus: Safe Biometric Deduplication for Humanitarian Aid Distribution. IEEE Security and Privacy Symposium, 2024.
6. D. Pasquini, G. Ateniese, C. Troncoso. Universal Neural-Cracking-Machines: Self-Configurable Password Models from Auxiliary Data. IEEE Security and Privacy Symposium, 2024.
7. K. Kireev, M. Andriushchenko, C. Troncoso, N. Flammarion. Transferable Adversarial Robustness for Categorical Data via Universal Robust Embeddings. NeurIPS 2023
8. B. Kulynych, H. Hsu, C. Troncoso, F. P. Calmon. Arbitrary Decisions are a Hidden Cost of Differentially Private Training. Fairness, Accountability and Transparency. FAccT 2023.
9. B. Wang, W. Lueks, J. Sukaitis, V. Graf Narbel, C. Troncoso. Not Yet Another Digital ID: Privacy-Preserving Humanitarian Aid Distribution. IEEE Security and Privacy Symposium, 2023.
10. S. Chatel, C. Mouchet, A. Utkan Sahin, A. Pyrgelis, C. Troncoso, J-P Hubaux. PELTA - Shielding Multiparty-FHE against Malicious Adversaries. CCS 2023.
11. S. Munir, S. Siby, U. Iqbal, S. Englehardt, Z. Shafiq, C. Troncoso. CookieGraph: Understanding and Detecting First-Party Tracking Cookies. CCS 2023.
12. D. Pasquini, M. Raynal, C. Troncoso: On the (In)security of Peer-to-Peer Decentralized Machine Learning. IEEE Security and Privacy Symposium, 2023.
13. K. Chatzikokolakis, G. Cherubin, C. Palamidessi, and C. Troncoso, “The Bayes Security Measure” Computer Security Foundations Symposium, 2023.
14. S. Munir, S. Siby, U. Iqbal, S. Englehardt, Z. Shafiq, C. Troncoso. CookieGraph: Understanding and Detecting First-Party Tracking Cookies. CCS 2023.
15. K. Kireev, B. Kulynych, and C. Troncoso, “Adversarial Robustness for Tabular Data through Cost and Utility Awareness”, NDSS 2023.
16. T. Stadler, B. Oprisanu, C. Troncoso. “Synthetic Data: Anonymisation Groundhog Day”. USENIX Security Symposium, 2022.
17. S. Siby, U. Iqbal, S. Englehardt, Z. Shafiq, C. Troncoso. “WebGraph: Capturing Advertising and Tracking Information Flows for Robust Blocking”. USENIX Security Symposium 2022.
18. G. Cherubin, R. Jansen, C. Troncoso. “Online Website Fingerprinting: Evaluating Website Fingerprinting Attacks on Tor in the Real World”. USENIX Security 2022.

19. K. EdalatNejad, W. Lueks, J.-P. Martin, S Ledésert, A. L'Hôte, B. Thomas, L. Girod, C. Troncoso, “Datashare Network: A Decentralized Privacy-Preserving Search Engine for Investigative Journalists”. USENIX Security Symposium, 2020.
20. W. Lueks, I Querejeta-Azurmendi, C. Troncoso, “VoteAgain: A scalable coercion-resistant voting system”. USENIX Security Symposium, 2020.
21. B. Kulynych, R. Overdorf, C. Troncoso, S. Gürses. “POTs: Protective Optimization Technologies”. Fairness, Accountability and Transparency (FAT*), 2020.
22. A. Pyrgelis, C. Troncoso, and E. De Cristofaro: ‘‘Measuring Membership Privacy on Aggregate Location Time-Series” Measurement and Analysis of Computing Systems (SIGMETRICS), 2020.
23. S. Siby, M. Juarez, C. Diaz, N. Vallina-Rodriguez, C. Troncoso, " Encrypted DNS--> Privacy? A Traffic Analysis Perspective". Networks and Distributed Systems Symposium, 2020.
24. Jean Louis Raisaro, Juan Ramón Troncoso-Pastoriza, Yamane El-Zein, Mathias Humbert, Carmela Troncoso, Jacques Fellay, Jean-Pierre Hubaux. ”GenoShare: Supporting Privacy-Informed Decisions for Sharing Individual-Level Genetic Data.” Medical Informatics Europe, 2020.
25. S. Boukoros, M. Humbert, S. Katzenbeisser, and C. Troncoso: “On (The Lack Of) Location Privacy in Crowdsourcing Applications”. Usenix Security 2019.
26. S. Oya, C. Troncoso, and F. Pérez-González. Rethinking Location Privacy for Unpredictable Mobility Behaviors. IEEE EuroS&P 2019.
27. C. Chen , D. E. Asoni, A. Perrig, D. Barrera, G. Danezis, and C. Troncoso. TARANET: Traffic-Analysis Resistant Anonymity at the NETwork layer. IEEE EuroS&P 2018.
28. A. Pyrgelis, C. Troncoso, and E. De Cristofaro. “Knock Knock, Who's There? Membership Inference on Aggregate Location Data”. Networks and Distributed Systems Symposium 2018.
29. 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.
30. S. Matic, C. Troncoso, J. Caballero: “Dissecting Tor Bridges: a Security Evaluation of their Private and Public Infrastructures”. Network and Distributed System Security Symposium, NDSS, 2017.
31. 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, 2017.
32. 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, 2017.
33. 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.
34. 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.
35. 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.
36. F. Perez-Gonzalez, and C. Troncoso: “Understanding Statistical Disclosure: A Least Squares approach“, In Privacy Enhancing Technologies Symposium, PETS, 2012.
37. 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.
38. 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.
39. 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.
40. 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.

41. 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.
42. G. Danezis, and C. Troncoso, "Vida: How to use Bayesian inference to de-anonymize persistent communications," In Privacy Enhancing Technologies Symposium, PETS, 2009.
43. 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.
44. 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.
45. C. Diaz, C. Troncoso, and A. Serjantov, "On the Impact of Social Network Profiling on Anonymity," In Privacy Enhancing Technologies Symposium, PETS, 2008.
46. 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.
47. 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.
48. 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.
49. 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.

WORKSHOP PUBLICATIONS

1. B. Kulynych, H. Hsu, C. Troncoso, F. P. Calmon: Arbitrary Decisions Are a Hidden Cost of Differentially Private Training. EWAF 2023
2. W. Lueks, B. Kulynych, J. Fasquelle, S. Le Bail-Collet, and C. Troncoso.”zksk: A Library for Composable Zero-Knowledge Proofs”. ACM Workshop on Privacy in the Electronic Society. 2019.
3. M. Yaghini, B. Kulynych, G. Cherubin, C. Troncoso. Disparate Vulnerability: on the Unfairness of Privacy Attacks Against Machine Learning. ACM CCS Workshop on Privacy-preserving Machine Learning. 2019
4. W. Lueks, M. Daumas, C. Troncoso. “Lightnion: seamless anonymous communication from any web browser”. Workshop on Measurements, Attacks and Defenses for the Web, 2019.
5. B. Kulynych, J. Hayes, N. Samarin, C. Troncoso. Evading classifiers in discrete domains with provable optimality guarantees. NeurIPS Workshop on Security in Machine Learning, 2018.
6. R. Overdorf, B. Kulynych, E. Balsa, C. Troncoso, S. Gürses. Questioning the assumptions behind fairness solutions. Critiquing and Correcting Trends in Machine Learning (NeurIPS 2018 Workshop).
7. B. Kulynych, W. Lueks, M. Isaakidis, G. Danezis, and C. Troncoso. ClaimChain: Improving the Security and Privacy of In-band Key Distribution for Messaging. Workshop on Privacy in the Electronic Society, ACM Workshop on Privacy in the Electronic Society 2018.
8. S. Siby, M. Juarez, N. Vallina, and C. Troncoso: “DNS Privacy not so private: the traffic analysis perspective.” HotPETS 2018.
9. S. Oya, C. Troncoso, and F. Pérez-González: “Is Geo-indistinguishability what you are looking for?”. In ACM Workshop on Privacy in the Electronic Society, ACM Workshop on Privacy in the Electronic Society 2017.
10. B. Kulynych and C. Troncoso. Feature importance scores and lossless feature pruning using Banzhaf power indices. NIPS Symposium on Interpretable Machine Learning, 2017.
11. J. Hayes, C. Troncoso, and G. Danezis: “TASP: Towards Anonymity Sets that Persist“. ACM Workshop on Privacy in the Electronic Society, 2016.
12. 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.

13. 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.
14. 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.
15. C. Troncoso: "Bayesian inference to evaluate information leakage in complex scenarios". IH&MMSec 2013
16. 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, 2013.
17. 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.
18. 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, 2011.
19. 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, 2010.
20. 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, 2008. *(71 citations)*
21. 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), 2008.
22. 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.
23. C. Troncoso, C. Diaz, O. Dunkelman, and B. Preneel, "Traffic Analysis Attacks on a Continuously-Observable Steganographic File," In Information Hiding Workshop, IH, 2007.
24. 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.

OTHER PEER-REVIEWED PUBLICATIONS

1. B. Pirelli, S. Gurses, C. Troncoso. “On the challenges of engineering/deploying Privacy By Design”. Privacy Law Scholars Conference (PLSC Europe) 2019.
2. B. Kulynych, M. Isaakidis, C. Troncoso, and G. Danezis. “Modern key distribution with ClaimChain”. 34c3: 34th Chaos Communication Congress. 2017
3. S. Gurses, C. Troncoso, C. Diaz. "Engineering Privacy by Design Reloaded". Amsterdam Privacy Conference. 2015.
4. S. F. Gürses, C. Troncoso, and C. Diaz, "Engineering Privacy by Design," In Computers, Privacy & Data Protection, 25 pages, 2011.

NON PEER-REVIEWED PUBLICATIONS AND PRE-PRINTS

1. T. Stadler, W. Lueks, K. Kohls, C. Troncoso:Preliminary Analysis of Potential Harms in the Luca Tracing System. arXiv preprint, arXiv:2103.11958 (2021)
2. J. Benzler, D. Bogdanov, G. Kirchner, W. Lueks, R. Lucas, R. Oliveira, B. Preneel, M. Salathe, C. Troncoso, V. von Wyl “Towards a common performance and effectiveness terminology for digital proximity tracing applications” arXiv preprint arXiv:2012.12927 (2021)
3. “Privacy Engineering Meets Software Engineering. On the Challenges of Engineering Privacy By Design” arXiv preprint arXiv:2007.08613 (2020)
4. C. Troncoso, M. Payer, J.-P. Hubaux, M. Salathé, J. Larus, E. Bugnion, W. Lueks et al. "Decentralized privacy-preserving proximity tracing." arXiv preprint arXiv:2005.12273 (2020).
5. Evading classifiers in discrete domains with provable optimality guarantees (long version). Bogdan Kulynych, Jamie Hayes, Nikita Samarin, Carmela Troncoso. 2019.