Curriculum Vitae

Julio Hernandez-Castro

Office address: ETSISI
Universidad Politecnica de Madrid
Despacho 1208
Madrid
Email: jc.hernandez.castro@upm.es

Contents

1 Education

2013–2014	Postgraduate Certificate in Higher Education (PGCHE) Unit for the Enhancement of Learning and Teaching University of Kent, Canterbury, UK
1999–2003	Ph.D. in Computer Science Carlos III University, Madrid, Spain
1998–1999	M.Sc. in Coding Theory and Cryptography University of Valladolid, Spain
1990–1995	B.Sc. in Mathematics Complutense University, Madrid, Spain

2 Research Interests

My research interests are wide, but all within the area of Computer Security. I have ample experience in computer and network security, including computer forensics, which can be considered as my main research area. I have also strong interests in 'Internet of Things' security, offering low-cost, embedded solutions for, between others, RFID security. I have a large experience in the conception and analysis of lightweight primitives and protocols for very constrained devices. Finally, I am an expert in steganography and steganalysis, and have published multiple papers on both areas and in the related one of Data Loss Prevention. I have develop an interest in studying randomness, both on its generation and analysis, and I've published some papers on the topic, which fits nicely with my interest in IoT as randomness generation is particularly challenging in these constraints devices. I am very interested in blockchain technology, particularly on its security aspects. I am a fan and early adopter of both Bitcoin and Ethereum, and have done research on these topics, some funded by the Ethereum Foundation. I try to put all this past research experience to work in devising new tools and techniques in Cybersecurity, particularly through interdisciplinary work with colleagues from Economics, Anthropology, Electronics, Physical Sciences, etc. I also like Recreational Mathematics and chess (peak ELO rating was 1912). I am a native Spanish speaker, and fluent in both English and French. I have extensive programming experience in C and Python.

3 Research and Academic Positions

06/2023–Present	Associate Professor ETSISI Universidad Politecnica Madrid
10/2017–06/2023	Professor School of Computing University of Kent, UK
10/2015–09/2017	Senior Lecturer School of Computing University of Kent, UK
09/2012–09/2015	Lecturer School of Computing University of Kent, UK
02/2009–09/2012	Senior Lecturer School of Computing Portsmouth University, UK
10/2004–02/2009	Associate Professor (Tenure track, Prof. Titular Interino + Visitante) Department of Computer Science Carlos III University of Madrid, Spain
02/2003–10/2004	Lecturer (Ayudante Doctor) Department of Computer Science Carlos III University of Madrid, Spain
10/1999–02/2003	Research Assistant (Ayudante de Universidad) Department of Computer Science Carlos III University of Madrid, Spain

4 Research Visits

06/2000–09/2000	Cryptography and Computer Communications Security Group Bradford University, UK.
02/2002–05/2002	Basic Research In Computer Science (BRICS) Department of Computer Science University of Aarhus, Denmark. ***(Marie Curie EU Fellow)***
09/2003–03/2004	CAPS Team INRIA-IRISA Rennes, Rennes, France. ***(INRIA PostDoc Fellowship)***
10/2004–03/2005	LIFL, INRIA North Europe Universite de Lille, Lille, France.
10/2007–02/2008	Crypto Group University of Louvain, Louvain-la-Neuve, Belgium.
11/2008–12/2008	DOLPHIN Team CNRS-INRIA Nord-Europe, Lille, France
14/06/2013–21/06/2013	Information Security Group University of Louvain, Louvain-la-Neuve, Belgium.
15/07/2013–19/07/2013	University of York, UK. ***(LMS Grant)***

5 Selected Publications

5.1 Books

1. **Security of Ubiquitous Computing Systems**
   Gildas Avoine, J. Hernandez-Castro (Editors)
   Springer-Verlag
   ISBN 978-3-030-10591-4
   2019

2. **Security and Trends in Wireless Identification and Sensing Platform Tags: Advancements in RFID**
   Pedro Peris, J. Hernandez-Castro, T. Li (Editors)
   IGI Global, August, 2012. DOI: 10.4018/978-1-4666-1990-6, ISBN13: 9781466619906

3. **Security in Information Systems, Proceedings of the 3rd International Workshop on Security in Information Systems, WOSIS 2005**
   Eduardo Fernández-Medina, J. Hernandez-Castro, Luis García Villalba (Editors)
   Miami, USA, May 2005. INSTICC Press 2005. ISBN: 972-8865-25-2.

4. **Security In Information Systems, Proceedings of the 2nd International Workshop on Security In Information Systems, WOSIS 2004**
   Eduardo Fernández-Medina, J. Hernandez-Castro, Luis Javier García Villalba (Editors)
   Porto, Portugal, April 2004 INSTICC Press 2004. ISBN: 972-8865-07-4.

5.2 Book Chapters

1. **RFID Specification Revisited.**
   P. Peris, J. Hernandez-Castro, J.M.E. Tapiador, A. Ribagorda.
   In *The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems*, chapter 6, pp. 127–156, 2008
   Auerbach Publications (CRC Press, Taylor & Francis Group)

2. **Cooperation-based Security in P2P and Mobile Ad Hoc Networks.**
   E. Palomar, J.M.E. Tapiador, J. Hernandez-Castro, A. Ribagorda.
   In *Cooperative Wireless Communication*. Chapter 17, pp. 393–410, 2009. ISBN: 978-1-4200-6469-8
   Auerbach Publications (CRC Press, Taylor & Francis Group)

3. **Game Theory and Cooperation Analysis.**
   A. Alcaide, J.M.E. Tapiador, J. Hernandez-Castro, A. Ribagorda.
   In *Cooperative Wireless Communication*, Chapter 9, pp. 193–208, 2009. ISBN: 978-1-4200-6469-8
   Auerbach Publications (CRC Press, Taylor & Francis Group)

4. **Secure Content Distribution in Pure Peer-to-Peer and Ad Hoc Networks.**
   E. Palomar, J.M.E. Tapiador, J. Hernandez-Castro, A. Ribagorda.
   In *Handbook of Research on Secure Multimedia Distribution.* Chapter 20, pp. 384–402, 2009
   IGI Global (formerly Idea Group, Inc.)

5. **Lightweight Cryptography for RFID Systems.**
   P. Peris, J. Hernandez-Castro, J.M.E. Tapiador, A. Ribagorda.
   In *Security in RFID and Sensor Networks.* pp. 121–150, 2009
   Auerbach Publications (CRC Press, Taylor & Francis Group)

6. **Attacking RFID Systems.**
   P. Peris, J. Hernandez-Castro, J.M.E. Tapiador, A. Ribagorda.
   In *Security in RFID and Sensor Networks.* pp.29–48
   Auerbach Publications (CRC Press, Taylor & Francis Group), 2009.

7. **Seguridad Informatica y PKI.** (in Spanish)
   L. J. Garcia-Villalba, J. Hernandez-Castro.
   In *Tecnologias Biometricas Aplicadas a la Seguridad.*
   Editorial RA-MA. pp. 375–436. M. Tapiador, J.A. Siguenza (Ed.)
   ISBN: 84-7897-636-1.

8. **Autenticacion LDAP.** (in Spanish)
   J.M. Sierra, J. Hernandez-Castro.
   In *Seguridad en Bases de Datos.*
   Editorial DINTEL. pp. 301–322. Fernandez, E; Piattini, M; Serrano, M.A (Ed.) ISBN: 84-931933-9-9.

5.3 Articles in Refereed Journals

1. **A methodology for studying untrusted software.**
   J. Hernandez-Castro, J Sierra, A. Ribagorda, B. Ramos.
   USENIX Login **25**(3):30–33 (2000)

2. **Genetic algorithms can be used to obtain good linear congruential generators.**
   J. Hernandez-Castro, A. Ribagorda, P. Isasi, J. Sierra.
   Cryptologia **25**(3):213–230 (2001)

3. **Search Engines as a security threat.**
   J. Hernandez-Castro, J. Sierra, A. Ribagorda, B. Ramos.
   IEEE Computer **34**(1):25–30 (2001)

4. **Beware of the security software.**
   J. Hernandez-Castro, J. Sierra, A. Ribagorda.
   Information Systems Security Journal **12**(6):39–46 (2004)

5. **Filtering Spam at E-Mail Server Level with Improved CRM114.**
   V. Mendez, J. Hernandez-Castro, J. Carretero, F. Garcia.
   Information Systems Security Journal **13**(3):21–39 (2004)

6. **Low computational cost integrity for block ciphers.**
   J. Sierra, J. Hernandez-Castro, N. Jayaram, A. Ribagorda.
   Future Generation Computer Systems **20**(5):857–863 (2004)

7. **Finding Efficient Distinguishers for Cryptographic Mappings, with an Application to the Block Cipher TEA.**
   J. Hernandez-Castro, P. Isasi.
   Computational Intelligence Journal **20**(3):517–525 (2004)

8. **Hiding Data in Games.**
J. Hernandez-Castro, I. Blasco, J. Garcia-Villalba.
International Computer Game Association Journal (ICGA) **27**(2):96–101 (2004)

9. **Reference Chromosome to Overcome User Fatigue in IEC.**
Y. Saez, P. Isasi, J. Segovia, J. Hernandez-Castro.
New Generation Computing **23**(2):129–142 (2005)

10. **New Results on the Genetic Cryptanalysis of TEA and Reduced round Versions of XTEA.**
J. Hernandez-Castro, P. Isasi.
New Generation Computing **23**(3):233–243 (2005)

11. **The strict avalanche criterion randomness test.**
J. Hernandez-Castro, J. Sierra, A. Seznec, A.Izquierdo, A. Ribagorda.
Mathematics and Computers in Simulation **68**(1):1–7 (2005)

12. **Steganography in Games: A General Methodology with Application to the Game of Go.**
J. Hernandez-Castro, I. Blasco, J. Tapiador, A. Ribagorda.
Computers & Security **25**(1):64–71 (2006)

13. **Bayesian Rational Exchange.**
J. Tapiador, A. Alcaide, J. Hernandez-Castro, A. Ribagorda.
Int. J. of Information Security **7**(1):85–100 (2008)

14. **Secure Content Access and Replication in Pure P2P Networks.**
E. Palomar, J. Tapiador, J. Hernandez-Castro, A. Ribagorda.
Computer Communications **31**(2):266–279 (2008)

15. **Automated Design of Cryptographic Hash Schemes by Evolving Highly Non-Linear Functions.**
J. Tapiador, J. Hernandez-Castro, P. Peris, A. Ribagorda.
Journal of Information Science and Engineering **24**(4) (2008)

16. **Cryptanalysis of Syverson's Rational Exchange Protocol.**
A. Alcaide, J. Tapiador, J. Hernandez-Castro, A. Ribagorda.
International Journal of Network Security **7**(2):190–195 (2008)

17. **On the Distinguishability of Distance-bounded Permutations in Ordered Channels.**
J. Tapiador, J. Hernandez-Castro, A. Alcaide, A. Ribagorda.
IEEE Transactions on Information Security and Forensics **3**(2):166–172 (2008)

18. **Automated Design of a Lightweight Block Cipher with Genetic Programming.**
J. Polimon, J. Hernandez-Castro, J. Tapiador, A. Ribagorda.
Int. J. of Knowledge-Based and Intelligent Engineering Systems **12**(1):3–14 (2008)

19. **LAMED – A PRNG for EPC Class-1 Generation-2 RFID Specification.**
P. Peris, J. Hernandez-Castro, J. Tapiador, A. Ribagorda.
Computer Standards & Interfaces. **31**(1):88–97 (2009)

20. **An Ultra Light Authentication Protocol Resistant to Passive Attacks under the Gen-2 Specification.**
P. Peris-Lopez, J. Hernandez-Castro, J. Tapiador and A. Ribagorda.
Journal of Information Science and Engineering, Vol. 25 No. 1, pp. 33-57 (2009)

21. **Cryptanalysis of a Novel Authentication Protocol Conforming EPC-C1G2 Standard.**
P. Peris, J. Hernandez-Castro, J. Tapiador, A. Ribagorda.
Computer Standards & Interfaces **31**(2):372–380, (2009)

22. **Blind Steganalysis of MP3Stego.**
J. Hernandez-Castro, J. Tapiador, E. Palomar, A. Romero.
Journal of Information Science and Engineering, v. 26, pp. 1787–1799, 2010

23. **Practical attacks on a mutual authentication scheme under the EPC Class-1 Generation-2 standard.**
P. Peris-Lopez, Tieyan Li, J. Hernandez-Castro, J. Tapiador.
Comp. Communications, v.32, Issues 7-10, pp. 1185-1193, 2009.

24. **Highly Entangled Multiqubit States, with very Simple Algebraic Structure**
J. Tapiador, J. Hernandez-Castro, J. Clark, S. Stepney.
J. Phys. A: Math. Theor. 42 (2009)

25. **Vulnerability analysis of RFID protocols for tag ownership transfer**
P. Peris, J. Hernandez-Castro, J. Tapiador, T. Li, Y. Li.
Computer Networks. Volume 54, Issue 9, pp. 1502–1508, 2010

26. **Lightweight Props on the Weak Security of EPC Class-1 Generation-2 Standard**
P. Peris-Lopez, Tieyan Li and J. Hernandez-Castro.
IEICE Transactions on Information and Systems, Vol. E93-D, No.3, pp. 518–527, 2010

27. **Reid et al.'s Distance Bounding Protocol and Mafia Fraud Attacks over Noisy Channels**
A. Mitrokotsa, C. Dimitrakakis, P. Peris-Lopez, J. Hernandez-Castro.
IEEE Communications Letters, Volume 14, Issue 2, pp. 121-123, 2010

28. **Flaws on RFID grouping-proofs. Guidelines for future sound protocols**
P. Peris-Lopez, A. Orfila, J. Hernandez-Castro, J. van der Lubbe
Journal of Network and Computer Applications 34(3): 833-845, 2011

29. **A Secure Distance-based RFID Identification Protocol with an Off-line Back–end Database**
P. Peris-Lopez, A. Orfila, E. Palomar, J. Hernandez-Castro
Journal of Personal and Ubiquitous Computing, pp. 1-15. Springer, 2011

30. **A framework for avoiding steganography usage over HTTP**
J. Blasco, J.Hernandez-Castro, J.M. Fuentes, B. Ramos
J. Network and Computer Applications 35(1): 491-501 (2012)

31. **Online Randomization Strategies to Obfuscate User Behavioral Patterns**
J. Tapiador, J. Hernandez-Castro, P. Peris-Lopez
J. Network Syst. Manage. 20(4): 561-578 (2012)

32. **Metaheuristic Traceability Attack against SLMAP, an RFID Lightweight Authentication Protocol.**
J. Hernandez-Castro, J. Tapiador, P. Lopez, J. Clark, El-Ghazali Talbi
Int. J. Found. Comput. Sci. 23(2): 543-553 (2012)

33. **A genetic tango attack against the David-Prasad RFID ultra-lightweight authentication protocol**
D. Barrero, J. Hernandez-Castro, P. Peris, D. Camacho
Expert Systems (2012)

34. **Bypassing information leakage protection with trusted applications**
J. Blasco, J. Hernandez-Castro, J. Tapiador, A. Ribagorda
Computers & Security 31(4): 557-568 (2012)

35. **A study on the false positive rate of Stegdetect**
O. Khalind, J. Hernandez-Castro, B. Aziz
Digital Investigation v.9, Issue 3: 235-245 (2013)

36. **Cryptanalysis of the RNTS system**
P. Picazo, L. Ortiz, P. Peris-Lopez, J. Hernandez-Castro
The Journal of Supercomputing v. 65, Issue 2: 949-960 (2013)

37. **Cybercrime prevalence and impact in the UK**
Julio Hernandez-Castro, Eerke Boiten
Computer Fraud & Security, v. 2014, Issue 2, pp. 5-8 (2014)

38. **Cryptanalysis of Cho et al.: A hash-based RFID tag mutual authentication protocol**
M Safkhani, P Peris-Lopez, J. Hernandez-Castro, N Bagheri
Journal of Computational and Applied Mathematics, v. 259, pp. 571-577 (2014)

39. **Source identification for mobile devices, based on wavelet transforms combined with sensor imperfections**
A. Sandoval, D Arenas, J Rosales, L García, J Hernandez-Castro
Computing Journal, v. 96, issue 9, pp. 829-841 (2014)

40. **On the limits of engine analysis for cheating detection in chess**
D. Barnes, J. Hernandez-Castro
Computers & Security Journal, v. 48, pp. 58-73 (2015)

41. **Automatic detection of potentially illegal online sales of elephant ivory via data mining**
J. Hernandez-Castro, and David Roberts
PeerJ Computer Science 1.e10 (2015): 1-11

42. **Steganalysis of Openpuff through atomic concatenation of mp4 flags**
T Sloan, J. Hernandez-Castro
Digital Investigation v. 13, pp. 15–21 (2015)

43. **Forensic analysis of video steganography tools**
T Sloan, J. Hernandez-Castro
PeerJ Computer Science. May 2015

44. **Detecting discussion communities on vaccination in twitter**
G. Bello-Orgaz, J. Hernandez-Castro, D. Camacho
Future Generation Computer Systems, v.66 pp.125–136, 2016

45. **Assessing the extent and nature of wildlife trade on the dark web**
J. Harrison., D. Roberts, and J. Hernandez-Castro
Conservation Biology (2016)

46. **Theia: a tool for the forensic analysis of mobile devices**
A. Orozco, J. Rosales, D. Arenas, J. Villalba and J. Hernandez-Castro
Computing (2016): 1-36

47. **A Survey of Security and Privacy Issues in ePassport Protocols**
G. Avoine, A. Beaujeant, J. Hernandez-Castro, L. Demay and P. Teuwen.
ACM Computing Surveys (CSUR) 48, no. 3 (2016)

48. **Assessing the extent and nature of wildlife trade on the dark web**
J. Harrison, D. Roberts, J. Hernandez-Castro
Conservation Biology 30 (4), 900–904 (2016)

49. **Pitfalls in ultralightweight authentication protocol designs**
G. Avoine, X. Carpent, J. Hernandez-Castro
IEEE Transactions on Mobile Computing 15 (9), 2317–2332 (2016)

50. **Detecting discussion communities on vaccination in twitter**
G. Bello-Orgaz, J. Hernandez-Castro, D. Camacho
Future Generation Computer Systems 66, 125–136 (2017)

51. **No Bot Expects the DeepCAPTCHA! Introducing Immutable Adversarial Examples, With Applications to CAPTCHA Generation**
M Osadchy, J Hernandez-Castro, S Gibson, O Dunkelman, D Perez
IEEE Transactions on Information Forensics and Security 12 (11), pp.2640–2653, 2017

52. **Certifiably biased: an in-depth analysis of a common criteria EAL4+ certified TRNG.**
Hurley-Smith, Darren, and Julio Hernandez-Castro.
IEEE Transactions on Information Forensics and Security 13, no. 4 (2018): pp. 1031–1041, 2018

53. **To pay or not: game theoretic models of ransomware.**
E Cartwright, J Hernandez Castro, A Cartwright.
Journal of Cybersecurity 5 (1), 2019

54. **On the unbearable lightness of FIPS 140-2 randomness tests.**
D Hurley-Smith, C Patsakis, J Hernandez-Castro.
IEEE Transactions on Information Forensics and Security, 2020

55. **On the Effectiveness of Ransomware Decryption Tools.**
B Filiz, B Arief, O Cetin, J Hernandez-Castro.
Computers & Security 111, 2021

56. **PoPL: Proof-of-Presence and Locality, or How to Secure Financial Transactions on Your Smartphone.**
Yonas Leguesse, C. Colombo, M. Vella M, J. Hernandez-Castro J.
IEEE Access. 2021 Dec 21;9:168600-12

57. **An investigation of individual willingness to pay ransomware.**
Cartwright, A., Cartwright, E., Xue, L., Hernandez-Castro, J.
Journal of Financial Crime, 2022

58. **Sensitivity and uniformity in statistical randomness tests.**
Luengo EA, Cerna ML, Villalba LJ, Hurley-Smith D, Hernandez-Castro J.
Journal of Information Security and Applications. 2022 Nov 1;70:103322.

5.4 Articles in Refereed Conference Proceedings

1. **Why current statistical approaches to ransomware detection fail.**
J Pont, B Arief, J Hernandez-Castro.
International Conference on Information Security, p. 199-216, 2020

2. **An Analysis of Bitcoin Laundry Services**
   T de Balthasar, J Hernandez-Castro
   In Proceedings of the 2017 Nordic Conference on Secure IT Systems, pp. 297–312, to be published by LNCS

3. **Bias in the TRNG of the Mifare EV1 Card**
   Darren Hurley-Smith, J Hernandez-Castro
   In Proceedings of the RFIDSec'16 Conference, to be published by LNCS

4. **A Survey of Social Web Mining Applications for Disease Outbreak Detection**
   G Bello-Orgaz, J Hernandez-Castro, D Camacho
   In Proceedings of the Intelligent Distributed Computing VIII, pp. 345-356, 2015

5. **Techniques for Source Camera Identification**
   A. Sandoval, D. Gonzalez, J. Rosales, LJ Garcıa and J. Hernandez-Castro.
   In Proceedings of the 6th International Conference on Information Technology, pp. 1-9, 2013

6. **On the security of Tan et al. serverless RFID authentication and search protocols**
   M. Safkhani, P. Peris-Lopez, N. Bagheri, M. Naderi and J. Hernandez-Castro.
   In Radio Frequency Identification. Security and Privacy Issues, pp. 1-19. Springer Berlin, 2013

7. **Another Fallen Hash-Based RFID Authentication Protocol**
   J. Hernandez-Castro, P. Peris, M Safkhani, N Bagheri, M Naderi
   In Proceedings of Information Security Theory and Practice - 6th IFIP WG 11.2 International Workshop, WISTP 2012, Egham, UK, June 20-22, 2012

8. **AKARI-X: a Pseudorandom Number Generator for Secure Lightweight Systems**
   H. Martin, E. Millan, L. Entrena, P. Peris, J. Hernandez-Castro
   In Proceedings of The 17th IEEE International On-Line Testing Symposium. IEEE Computer Society Press, Athens, Greece, 2011

9. **Studying the pseudo random number generator of a low-cost RFID tag**
   M. Merhi, J. Hernandez-Castro, Pedro Peris
   In Proceedings of IEEE RFID-TA, pp. 381–385, 2011

10. **On the Strength of Egglue and Other Logic CAPTCHAs**
    Carlos Javier, Arturo Ribagorda, J. Hernandez-Castro
    SECRYPT pp. 157-167, 2011

11. **Quasi-Linear Cryptanalysis of a Secure RFID Ultralightweight Authentication Protocol**
    Pedro Peris, J. Hernandez-Castro, Raphael C.-W. Phan, Juan Estevez, Tieyan Li.
    In Proceedings of Inscrypt, pp. 427–442, 2010

12. **Cryptanalysis of the David-Prasad RFID ultralightweight authentication protocol**
    Hernandez-Castro, J. and Peris-Lopez, P. and Phan, R. and Tapiador, J.
    In Proceedings of the RFIDSec2010, pp. 22–34, 2010

13. **Fine-Grained Timing using Genetic Programming.**
    David R. White, Juan M. E. Tapiador, J. Hernandez-Castro and John A. Clark.
    In Proceedings of EuroGP, pp. 325–336, 2010

14. **Cryptographic Puzzles and Distance-bounding Protocols: Practical Tools for RFID Security.**
    P. Peris, J. Hernandez-Castro, J. Tapiador, E. Palomar and Jan C. A. van der Lubbe.
    In Proceedings of the IEEE International Conference on RFID, pp. 45–52, 2010

15. **Security Flaws in a Recent Ultralightweight RFID Protocol.**
    Galan E, J. Hernandez-Castro, Alcaide A, and Ribagorda, A.
    In 2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT), pp. 682–685, 2010

16. **A Strong Authentication Protocol Based on Portable One-Time Dynamic URLs.**
    P. Peris, J. Hernandez-Castro, J. Tapiador and Jan C. A. van der Lubbe.
    In RFIDSec 10 Asia, Singapore, February 22-23, 2010

17. **Weaknesses in Two Recent Lightweight RFID Authentication Protocols.**
Pedro Peris-Lopez, J. Hernandez-Castro, J. M. E. Tapiador, Tieyan Li and Jan C. A. van der Lubbe.
In the 5th China International Conference on Information Security and Cryptology (In Cooperation with IACR), Beijing, December, 2009. Note: An extended version of this work was presented at the 5th Workshop on RFID Security (RFIDSec09). Leuven, July, 2009.

18. **Security Flaws in an Efficient Pseudo-Random Number Generator for Low-Power Environment.**
Pedro Peris, J. Hernandez-Castro, Juan Tapiador, Enrique Millan, Jan C.A. van der Lubbe.
In The First ICST International Workshop on Security in Emerging Wireless Communication and Networking Systems (in conjunction with SecureComm 2009), Volume 42 of LNICST, pages 25-35. Springer-Verlag. Athens, September, 2009.

19. **Cryptanalysis of the SASI Ultralightweight RFID Authentication Protocol with Modular Rotations.**
J. Hernandez-Castro, J. Tapiador, P. Peris, Tieyan Li and Jean-Jacques Quisquater.
In International Workshop on Coding and Cryptography, Lofthus, Norway, May 10-15, 2009.

20. **Effects of Cooperation-based Peer-to-Peer Authentication on System Performance**
E. Palomar, A. Ribagorda, J. Tapiador, J. Hernandez-Castro
Workshop on Secure Multimedia Communication and Services (SECMCS'09)

21. **Metaheuristic Traceability Attack against SLMAP, an RFID Lightweight Authentication Protocol.**
J. Hernandez-Castro, J. Tapiador, P. Peris, John A Clark and El Ghazali Talbi.
Proceedings of the 12th International Workshop on Nature Inspired Distributed Computing (NIDISC09). IEEE Press.

22. **Steganalysis of Hydan**
J. Blasco, J. Hernandez-Castro, J. Estevez, A. Ribagorda, Miguel Orellana
Proceedings of the 24th IFIP International Information Security Conference (SEC-2009).

23. **Non-standard Attacks against Cryptographic Protocols, with an Example over a Simplified Mutual Authentication Protocol.**
J.Hernandez-Castro, J. Tapiador, A. Ribagorda.
Model. Comp. and Optim. in Inform. Syst., MCO 2008: CCIS **14**: 589–596. Springer-Verlag

24. **Nature Inspired Synthesis of Rational Protocols.**
A. Alcaide, J. Tapiador, J.Hernandez-Castro, A. Ribagorda
Parallel Problem Solving from Nature PPSN X, 2008. LNCS **5199**:981–990. Springer-Verlag.

25. **Csteg: Talking in C code.**
J. Blasco, J. Hernandez-Castro, J. Tapiador, A. Ribagorda.
SECRYPT 2008, pp. 399–406. INSTICC Press

26. **On the Salsa20 Core Function.**
J. Hernandez-Castro, J. Tapiador, J.-J. Quisquater.
*Fast Software Encryption 2008.*LNCS **5086**:462–469. Springer-Verlag.

27. **Non-Linear Cryptanalysis Revisited: Heuristic Search for Approximations to S-boxes.**
J. Tapiador, J.A. Clark, J. Hernandez-Castro.
IMA Conf. Crypto and Coding 2007. LNCS **4887**:99–117. Springer-Verlag.

28. **Bayesian Analysis of Secure P2P Sharing Protocols.**
E. Palomar, A. Alcaide, J.M.E. Tapiador, J.Hernandez-Castro.
IS 2007(OTM Conferences). LNCS **4804**:1701–1717. Springer-Verlag.

29. **A Multi-party Rational Exchange Protocol.**
A. Alcaide, J. Tapiador, J. Hernandez-Castro, A. Ribagorda.
IS 2007(OTM Workshops). LNCS **4805**:42–43. Springer-Verlag.

30. **An Efficient Authentication Protocol for RFID Systems Resistant to Active Attacks.**
P. Peris, J. Hernandez-Castro, J. Tapiador, A. Ribagorda.
SECUBIQ 2007 (EUC Workshops). LNCS **4809**:781–794. Springer-Verlag.

31. **Towards Automated Design of Multi-party Rational Exchange.**
A. Alcaide, J. Tapiador, J. Hernandez-Castro, A. Ribagorda.
RRS 2007, pp. 387–390. IEEE Press.

32. **A P2P File-Sharing Protocol based on Cryptographic Puzzles.**
E. Palomar, J. Tapiador, J. Hernandez-Castro, A. Ribagorda.
DBISP2P 2007. LNCS Springer-Verlag.

33. **Cryptanalysis of a Novel Authentication Protocol Conforming EPC-C1G2 Standard.**
P. Peris, J. Hernandez-Castro, J.Tapiador, A. Ribagorda.
RFIDSec 2007.

34. **Heuristic Search for Non-Linear Cryptanalytic Approximations.**
J. Tapiador, J. Hernandez-Castro, J.A. Clark.
CEC 2007, pp. 3561–3568. IEEE Press.

35. **Dealing with Sporadic Strangers, or the (Un)Suitability of Trust for Mobile P2P Security.**
E. Palomar, J. Tapiador, J.Hernandez-Castro, A. Ribagorda.
PDMST 2007 (DEXA), pp. 779–783. IEEE Press.

36. **Solving the Simultaneously Scanning Problem Anonymously: Clumbing Proofs for RFID Tags.**
P. Peris, J. Hernandez-Castro, J.Tapiador, A. Ribagorda.
SecPerU 2007, pp. 55–60. IEEE Press.

37. **EMAP: An Efficient Mutual Authentication Protocol for Low-cost RFID Tags.**
P. Peris, J. Hernandez-Castro, J. Tapiador, A. Ribagorda.
IS 2006 (OTM Workshops). LNCS **4277**:352–361. Springer-Verlag.

38. **LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID Tags.**
P. Peris, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A. Ribagorda.
RFIDSec 2006.

39. **Certificate-based Access Control in Pure P2P Networks.**
E. Palomar, J. Tapiador, J. Hernandez-Castro, A. Ribagorda.
P2P 2006, pp. 177–184. IEEE Press.

40. **A Protocol for Secure Content Distribution in Pure P2P Networks.**
E. Palomar, J. Tapiador, J. Hernandez-Castro, A. Ribagorda.
PDMST 2006 (DEXA), pp. 712–716. IEEE Press.

41. **Lamar: A New Pseudorandom Number Generator Evolved by means of Genetic Programming.**
C. Lamenca, J. Hernandez-Castro, J. Tapiador, A. Ribagorda.
PPSN 2006. LNCS **4193**:850–859. Springer-Verlag.

42. **Finding State-of-the-Art Noncryptographic Hashes with Genetic Programming.**
C. Estebanez, J. Hernandez-Castro, A. Ribagorda, P. Isasi.
PPSN 2006. LNCS **4193**:818–827. Springer-Verlag.

43. **M2AP: A Minimalist Mutual Authentication Protocol for Low-cost RFID Tags.**
P. Peris, J. Hernandez-Castro, J. Tapiador, A. Ribagorda.
UIC 2006. LNCS **4159**:912–923. Springer-Verlag.

44. **Security in P2P Networks: Survey and Research Directions.**
E. Palomar, J. Tapiador, J. Hernandez-Castro, A. Ribagorda.
EUC 2006. LNCS **4097**:183–192. Springer-Verlag.

45. **RFID Systems: A Survey on Security Threats and Proposed Solutions.**
P. Peris, J. Hernandez-Castro, J. Tapiador, A. Ribagorda.
PWC 2006. LNCS **4217**:159–170. Springer-Verlag.

46. **A P2P Content Authentication Protocol based on Byzantine Agreement.**
E. Palomar, J. Tapiador, J. Hernandez-Castro, A. Ribagorda.
ETRICS 2006. LNCS **3995**:60–72. Springer-Verlag.

47. **An Extended Model of Rational Exchange based on Dynamic Games of Imperfect Information.**
A. Alcaide, J. Tapiador, J. Hernandez-Castro, A. Ribagorda.
ETRICS 2006. LNCS **3995**:396–408. Springer-Verlag.

48. **Wheedham: An Automatically Designed Block Cipher by means of Genetic Programming.**
J. Hernandez-Castro, J. Tapiador, A. Ribagorda, B. Ramos.
CEC 2006, pp. 192–199. IEEE Press.

49. **Attacks on Port-Knocking Authentication Mechanism.**
A. Izquierdo, J. Torres, J.Tapiador, J. Hernandez-Castro
ICCSA 2005. LNCS **3483**:1292–1300. Springer-Verlag.

50. **Security Issues in Network File Systems.**
A. Izquierdo, J. Sierra, J. Hernandez-Castro, A. Ribagorda
ICCSA 2004. LNCS **3043**:812–820. Springer-Verlag.

51. **Forecasting Time Series by means of Evolutionary Algorithms.**
C. Luque, P. Isasi, J. Hernandez-Castro
PPSN 2004. LNCS **342**:1061–1070. Springer-Verlag.

52. **New results on the genetic cryptanalysis of TEA and reduced round versions of XTEA .**
J. Hernandez-Castro, P. Isasi.
CEC 2004, pp. 2124–2129. IEEE Press.

53. **Improving CRM114 Speed and Accuracy to Allow Filtering Spam at the Email Server.**
V. Mendez, J. Hernandez-Castro, J. Carretero, F. Garcia.
2004 MIT Spam Conference

54. **Finding efficient distinguishers for cryptographic mappings, with an application to the block cipher TEA.**
J. Hernandez-Castro, P. Isasi.
CEC 2003, pp. 2189–2193. IEEE Press

55. **On MARS sboxes strength against linear cryptanalysis.**
C. Hernandez, L. Garcia-Villalba, J. Hernandez-Castro, J. Sierra.
ICCSA 2003. LNCS **2668**:79–83. Springer-Verlag.

56. **Cryptanalysis with classifiers of some models of pseudorandom number generators.**
J. Hernandez-Castro, J. Sierra, P. Isasi, A. Ribagorda.
RASC 2002, pp. 423–429. The Nottingham Trent University Press.

57. **Easing collision finding in cryptographic primitives with genetic algorithms.**
J. Hernandez-Castro, P. Isasi. A. Ribagorda.
CEC 2002, pp. 535–539. IEEE Press

58. **Distinguishing TEA from a random permutation.**
J. Hernandez-Castro, J. Sierra, A. Ribagorda, B. Ramos, C. Mex-Perera.
IMA Conf. Crypto and Coding 2001. LNCS **2260**:374–377. Springer-Verlag.

59. **Robust New Method in Frequency Domain Watermarking.**
D. Sanchez, A. Orfila, J. Hernandez-Castro, J. Sierra.
ISC 2001. LNCS **2200**:166–182. Springer-Verlag.

6 Research Projects and Grants

1. **London Mathematical Society (LMS) Small Computer Science Grant**. July 2013. £500

2. **ChessWitan: Detecting cheating in Chess. Microsoft Azure Scientific Research Grant**. MSR - Microsoft Research. Period: 2013 – 2014. $\$40K$

3. **Detecting Wildlife Crime in eBay**. Chester Zoo. Period: 2014 – 2015. £4k

4. **Cryptanalysis of ubiquitous computing systems (CRYPTACUS)**. EU COST (European Cooperation in Science and Technology) Action IC 1403 - European Union. Period: 2014 – 2018. Vice-Chair. Project total of €423K.

5. **Improving cyber security using realistic synthetic face generation**. EPSRC Project in cooperation with MOST. co-PI. Period: 01/03/15–01/04/17. Value of £155K

6. **aS – Authenticated Self**. TSB/InnovateUK Project. Period: 01/04/15–01/06/17. co-PI for Kent, for £283K

7. **EPSRC SeeK Project**. EPSRC. Period: 01/04/16–01/10/19. I am the PI for Kent, which received £273K

8. **HORIZON 2020 Project RAMES**. EU Commission. Period: 01/09/16–01/09/19. I am the PI for Kent, which received €471K out of a project total of €3.8m

9. **GCHQ Summer Internships**. GCHQ. IP & co-IP. Period: 01/06/15–01/09/15 and 01/06/16-01/09/16. £18K

10. **IoT Lab**. GCHQ. Co-IP. Period: 01/06/15–01/09/15. £10K

11. **Kent Digital Media Archive**. GCHQ. Period: 01/06/15–01/09/16. PI. £26K

12. **Red-Blue Team for the Contiki IoT OS**. GCHQ. Period: 01/01/17–31/03/17. co-PI. £37K

13. **EPSRC - EMPHASIS**. Period: 01/07/17–31/06/19. Kent PI. £443K for Kent from a £1.2m project.

14. **EPSRC - RISE**. Period: 01/11/18–01/04/19. PI. £36K

15. **Huawei - Video Watermarking**. Period: 01/06/19–01/06/20. PI. £230K

16. **EPSRC - Quantum Communications Hub 2**. Period: 01/12/19–31/12/24. PI. £576K

17. **Horizon 2020 - HEROES**. Period: 01/12/21–31/12/24. PI. £436K

18. **Horizon 2020 - ALUNA**. Period: 01/05/23–31/04/25. PI. £225K

19. **EPSRC - CharIoT**. Period: 01/09/23–31/08/25. co-PI. £468K

7 Organization of Scientific Events

1. VIII RECSI (Reunion Espanola de Criptologia y Seguridad de la Informacion) (Spanish Conference on Cryptology and Information Security), September 2004.

2. Second International Workshop on Security in Information Systems, (WOSIS 2004) Porto, Portugal, April 2004.

3. Third International Workshop on Security in Information Systems, (WOSIS 2005) Miami, USA, May 2005.

4. Journees C2 – Cryptographie et Codage. 30 January to 4 February, 2005. Aussois, France

5. International Conference on Information Theoretic Security (ICITS 07) Madrid, Spain, May 25-28, 2007.

6. Co-Chair of the Organising Committee of ARES 2019, the International Conference on Availability, Reliability and Security
   University of Kent, Canterbury, UK
   August 26 — 29, 2019

8 Supervision Activity

8.1 Ph.D. Students

1. **Ultralightweight cryptography for Low-Cost RFID Systems**
   Pedro Peris-Lopez
   Carlos III University of Madrid – 4^{th} November, 2008.
   Sobresaliente Cum Laude por unanimidad
   (Accepted/Passed with no corrections)

2. **Steganography and Data Leakage Prevention**
   Jorge Blasco Alis
   Carlos III University of Madrid – 15^{th} June, 2012
   (Accepted/Passed with no corrections)

3. **Video Steganography and Steganalysis**
   Tom Sloan
   School of Computing, Kent University – 11^{th} December 2018
   (Accepted/Passed with minor corrections)

4. **Identifying Ransomware Through Statistical and Behavioural Analysis**
   Jaime Pont
   School of Computing, Kent University – 14^{th} October 2022
   (Accepted/Passed with minor corrections)

8.2 M.Sc. and B.Sc Students

More than 80 M.Sc. and final year project supervisions so far. Can provide further details upon request.

9 Professional Services

9.1 Affiliations

- Association of Computing Machinery (ACM)
- International Association for Cryptologic Research (IACR)
- British Computer Society (BCS)
- London Mathematical Society
- Electronic Frontier Foundation
- Member of the IFIP Working Group 11.2 on Pervasive Systems Security
- Fellow of the Higher Education Academy since 17/09/2014

9.2 Other

- Guest Editor in the Journal of Research and Practice in Information Technology (JRPIT) 38(1): (2006)

- Member of the Advisory & Editorial Board of the International Journal of Future Generation Communication and Networking

- Member of the Editorial Board of the International Journal of Digital Crime and Forensics (IJDCF)

Ph.D. Examiner for:

- Alejandro Martin, Universidad Autonoma de Madrid, Madrid, Spain, March 2019
- Murtadha Hassan Alyasiri, The University of York, December 2018
- Mohamad Tayara, Newcastle University, UK, 2016
- Sarah Abu Ghazalah, Royal Holloway, UK, 2016
- Zeeshan Bilal, Royal Holloway, UK, 2014
- Gerhard de Koning, Radboud University, The Netherlands, 11 April, 2013
- James McLaughlin, The University of York, UK. 19 November 2012
- Cesar Estebanez Tascon, Carlos III University of Madrid, Spain (2011)
- Ahmad Salah El Ahmad, Newcastle University, UK (2011)
- Xun Don – University of York, UK (2010)
- Jesus Sanchez Rodrigo – University of Castilla la Mancha, Spain (2009)
- Almudena Alcaide Raya – Carlos III University, Madrid, Spain (2009)
- Esther Palomar – Carlos III University, Madrid, Spain (2008)
- Antonio Izquierdo – Carlos III University, Madrid, Spain (2006)
- Ana Isabel Gonzalez-Tablas – Carlos III University, Madrid, Spain (2005)
- Rodolfo Villaroel – University of Castilla la Mancha, Spain (2005)

9.3 Invited Talks & Seminars

- *My Journey through Steganography and Steganalysis, with lessons from 15 years of practice*
  Invited Speaker at CUING'2019 in Canterbury, August 29, 2019
- *On the difficulty of certifying randomness*
  Invited Speaker at JNIC'2019 in Caceres, Spain, June 6, 2019
- *Ransomware in Healthcare*
  Invited Speaker at the Healthcare Security Group, Universitat Rovira i Virgil, Tarragona, Spain, May 22, 2019
- *The Quest for Randomness*
  Invited Speaker at the A Coruna Master in CyberSecurity Security Seminar Series. A Coruna, Spain, May 15, 2019
- *An Economic Analysis of Ransomware: To Pay or not to Pay*
  Invited Speaker at the TUDelft Security Seminar Series. Delft, July 11, 2018
- *Certifying the uncertifiable*
  Invited Speaker at the Birmingham Security Seminar Series. Birmingham, May 18, 2017
- *Ransomware and its Influence on IoT devices, Critical Infrastructure and Elections*
  Invited Speaker at the CSPCI1 Conference (Cybersecurity: Protecting Critical Infrastructure). London, May 16, 2017
- *Cryptanalysis of ubiquitous computing systems*
  Invited Speaker at the 18th MELECON Conference. Cyprus, April 18, 2016

- *Adversarial Examples: The limits of Deep Learning and their applications to new CAPTCHAs*
  Essex University, June 6, 2016

- *Video Steganalysis: State of the Art*
  Complutense University, May 4, 2015

- *Recent Developments in Video Steganalysis*
  City University, April 8, 2015

- *Video Steganalysis*
  Complutense University, September 2014

- *Computer Forensics Analysis of Images & Digital Cameras*
  Complutense University, June 2013

- *Challenges in RFID Security*
  Heriot-Watt University, October 2012

- *Steganography & Steganalysis: A Primer*
  Complutense University. Madrid, 2008.

- *Security Engineering*
  Spanish National Institute of Public Administration, May 2008.

- Lab. of Algorithmics, Cryptology and Security (LACS) Seminar
  On the security of the Salsa20 hash function. University of Luxembourg
  November, 2007

- *Steganography & Steganalysis: History, Practical Cases & Internet Applications*
  Juan de Velasco Institute for Studies in Security and Defence, 2007.

- *Security Engineering*
  Spanish National Institute of Public Administration, May 2007.

- *Steganography & Steganalysis*
  Master Degree in Computer Science.
  Complutense University. Madrid, 2007.

- *Computer Forensics*
  Spanish National Institute of Public Administration, June 2007.

- *Security Engineering*
  Spanish National Institute of Public Administration, May 2006

- *Steganography & Steganalysis*
  Master Degree in Computer Science.
  Complutense University. Madrid, 2006.

10 Other

- My Erdös number is 3:
  J.C. Hernandez-Castro → J.-J. Quisquater → A. Odlyzko → P. Erdös.

- **My Google Scholar Author Profile, on the** $20th$ **April 2023 shows 5641 citations from 150+ articles, a h-index of 32, and 118 publications with 10 citations or more (i10–index=118).**
- **Member of the Home Office** Costs of Cyber Security **group**
- **Member of the Europol Expert Platform in Criminal Use of Information Hiding (Steganography) and of the Europol Virtual Currencies Taskforce**
- **Vice-Chair and member of the Management Committee of the European COST Action CRYPTACUS (Cryptanalysis of ubiquitous computing systems) involving 75 researchers from 28 Countries.**
- **I am one of the 7 named researchers in a successful application for the Academic Centre of Excellence for Cyber Security Research (ACE-CSR) scheme. This is a very prestigious label, only awarded by GCHQ to 17 Universities in the UK.**
- **I have been an External Examiner for the University of Wales (Newport)**
- **I am currently, or have recently been, a reviewer for the following foreign Research Funding Agencies: Fonds National de la Recherche Scientifique (FNRS - Belgium), L'Agence Nationale de la Recherche (ANR-France), FNR (Fonds National de la Recherche, Luxembourg), the Science Foundation Ireland (SFI) and CONICYT (Chile)**
- **I have a quite active media profile. I have been interviewed a number of times for national and local radio and TV, and I also write regular pieces at TheConversation.com, greatly contributing to University of Kent's prestige and visibility. For example, articles of or about my work have been published in major UK newspapers, including The Times, Guardian, Independent, etc. raising our media profile, but also in USA Today, 20 minutes, etc.**
- **I am also one of the two cofounders of Kent's Cybersecurity Survey, a series of surveys on Cybersecurity in the UK that last year produced a media impact equivalent of £255K with a cost of £2K**
- **Newton Fund reviewer for the British Council**
- **EPSRC Peer Review Associate College member**
- Recently appointed **Member of the European Union Agency for Network and Information Security (ENISA) IOTsec Expert Group**