Francisco Rodríguez-Henríquez

Technical Director
Cryptography Research Center
Technology Innovation Institute
Abu Dhabi, UAE

francisco.rodriguez-henriquez@tii.ae

franciscorh.org | DBLP | Google Scholar | IACR | ORCID

Personal Information

0. **Full Name:** Francisco José Rambó Rodríguez-Henríquez.
1. **Nationality:** Salvadoran, Mexican.
2. **Civil state:** Married, two children.

Degrees

- **1996–2000:** Doctorate, Electrical and Computer Engineering, Oregon State University. Thesis: *New Algorithms and Architectures for Arithmetic in GF(2^m) Suitable for Elliptic Curve Cryptography.* Supervisor: Çetin K. Koç.
- **1989–1992:** Master of Science, Electronic Engineering, National Institute of Astrophysics, Optics and Electronics, Puebla, México.
- **1984–1989:** Bachelor's in Electronics, Faculty of Science, University of Puebla, México.

Employment

- **2021/05 – Present:** Technical Director, Cryptography Research Center, Technology Innovation Institute, Abu Dhabi, UAE.
- **2014/09 – 2022/05:** Professor, Computer Science Department, CINVESTAV. Full-time tenured professor.
- **2006/09 – 2014/08:** Associate Professor, Computer Science Department, CINVESTAV.
- **2002/05 – 2006/08:** Assistant Professor, Computer Science Section, CINVESTAV.

Research specialization

Applied cryptography. My research focuses on efficient implementations of cryptographic algorithms, with particular emphasis on elliptic-curve, pairing-based and isogeny-based cryptography, post-quantum cryptography, computer arithmetic, cryptanalysis, and cryptography in real systems.

Selected distinctions

- Best Paper Award, EUROCRYPT 2025, for "Polynomial Time Cryptanalytic Extraction of Deep Neural Networks in the Hard-Label Setting."
- Best Paper Award, CHES 2013, for "Lambda Coordinates for Binary Elliptic Curves."
- Best Paper Award, CHES 2009, for "Hardware Accelerator for the Tate Pairing in Characteristic Three Based on Karatsuba–Ofman Multipliers."
- Runner-up for Best Paper Award, ASIACRYPT 2022, for "SwiftEC: Shallue–van de Woestijne Indifferentiable Function to Elliptic Curves."
- Runner-up for Best Paper Award, CHES 2016, for "Software Implementation of Koblitz Curves over Quadratic Fields."

Community building and real-world impact

- Co-founder of LATINCRYPT and ASCrypto, which established recurring conference and advanced-school venues for cryptology in Latin America.
- Co-developed FIDELIS, an electronic voting system used in official academic elections at CINVESTAV, combining voter privacy, authentication, verifiability, and homomorphic tallying.
- Co-led Applacovid, a decentralized privacy-preserving contact-tracing project developed during the COVID-19 pandemic for Android and iOS devices.

Monographic books

0. F. Rodríguez-Henríquez, N. A. Saqib, A. Díaz Pérez, and Ç. K. Koç, *Cryptographic Algorithms on Reconfigurable Hardware*. Springer, 2007, 362 pages. ISBN 0-387-33883-7.

Edited books

0. N. El Mrabet, L. Ghammam, F. Rodríguez-Henríquez (editors): Progress in Cryptology - AFRICACRYPT 2026 - 17th International Conference on Cryptology in Africa, Hammamet, Tunisia, July 8–10, 2026, Proceedings. Lecture Notes in Computer Science 16832, Springer 2026, ISBN 978-3-032-31129-0.
1. F. Rodríguez-Henríquez and B.-Y. Yang (Chief Editors): IACR Transactions on Cryptographic Hardware and Embedded Systems Vol 2024 No. 1-4.
2. A. Castañeda, F. Rodríguez-Henríquez: LATIN 2022: Theoretical Informatics - 15th Latin American Symposium, Guanajuato, Mexico, November 7–11, 2022, Proceedings. Lecture Notes in Computer Science 13568, Springer 2022, ISBN 978-3-031-20623-8.
3. L. Budaghyan, F. Rodríguez-Henríquez: Arithmetic of Finite Fields - 7th International Workshop, WAIFI 2018, Bergen, Norway, June 14-16, 2018, Proceedings. Lecture Notes in Computer Science 11321, Springer 2018, ISBN 978-3-030-05152-5.
4. K. E. Lauter, F. Rodríguez-Henríquez: Progress in Cryptology -LATINCRYPT 2015 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, August 23-26, 2015, Proceedings. Lecture Notes in Computer Science 9230, Springer 2015, ISBN 978-3-319-22173-1.
5. F. Özbudak, F. Rodríguez-Henríquez: Arithmetic of Finite Fields - 4th International Workshop, WAIFI 2012, Bochum, Germany, July 16-19, 2012. Proceedings. Lecture Notes in Computer Science 7369, Springer 2012, ISBN 978-3-642-31661-6.

Book chapters

0. M. J. Kannwischer, R. Niederhagen, F. Rodriguez-Henriquez, and P. Schwabe: "Post-Quantum Implementations". Chapter in Embedded Cryptography 2. Emmanuel Prouff, Guénaël Renault, Matthieu Rivain and Colin O'Flynn (editors), Wiley-ISTE (2025), pp. 249–286.
1. M-A León-Chávez, L. Pandolfo Perin, and F. Rodríguez-Henríquez: "Post-Quantum Digital Signatures for Bitcoin" Chapter 11 in K. Daimi, I. Dionysiou, N. El Madhoun (editors) "Principles and Practice of Blockchains", Springer 2023, ISBN 978-3-031-10506-7.
2. J.-L. Beuchat, N. El Mrabet, L. Fuentes-Castañeda, and F. Rodríguez-Henríquez: "Mathematical Background", Chapter 2 in Nadia El Mrabet and Marc Joye (editor), Guide to Pairing-based Cryptography, CRC Press, Taylor and Francis Group (Chapman & Hall), 2016 ISBN 978-1-4987-2950-5.

3. J. L. Beuchat, L. J. Dominguez Perez, S. Duquesne, N. El Mrabet, L. Fuentes-Castañeda, and F. Rodríguez-Henríquez: "Arithmetic of Finite Fields", Chapter 5 in Nadia El Mrabet and Marc Joye (editor), Guide to Pairing-based Cryptography, CRC Press, Taylor and Francis Group (Chapman & Hall), 2016 ISBN 978-1-4987-2950-5.

4. J.-L. Beuchat, L. J. Dominguez Perez, L. Fuentes-Castañeda, and F. Rodríguez-Henríquez: "Final Exponentiation", Chapter 7 in Nadia El Mrabet and Marc Joye (editor), Guide to Pairing-based Cryptography, CRC Press, Taylor and Francis Group (Chapman & Hall), 2016 ISBN 978-1-4987-2950-5.

5. E. Ochoa-Jiménez, F. Rodríguez-Henríquez, and M. Tibouchi: "Hashing into Elliptic Curves", Chapter 8 in Nadia El Mrabet and Marc Joye (editor), Guide to Pairing-based Cryptography, CRC Press, Taylor and Francis Group (Chapman & Hall), 2016 ISBN 9781-4987-2950-5.

6. D. Chakraborty and F. Rodríguez-Henríquez, "Block Cipher Modes of Operation from a Hardware Implementation Perspective", in Çetin Kaya Koç (editor), Cryptographic Engineering, Springer, 2009, XXII, 522 p. 70 illus., ISBN: 978-0-387-71816-3.

Journal papers

0. N. Carlini, J. Chávez-Saab, A. Hambitzer, F. Rodríguez-Henríquez, A. Shamir: "Polynomial Time Cryptanalytic Extraction of Deep Neural Networks in the Hard-Label Setting". *Journal of Cryptology*, accepted for publication, to appear. Extended version of the EUROCRYPT 2025 Best Paper. IACR Cryptology ePrint Archive, Report 2024/1580.

1. D. Santos, J. C. López Hernández, F. Rodríguez-Henríquez: "Efficient Vectorized Implementation of MQOM". *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2027(1), accepted, to appear.

2. D. L. Gazzoni Filho, G. Adj, S. Bettaieb, A. Budroni, J. Chávez-Saab, F. Rodríguez-Henríquez: "Sota Voce: Low-Noise Sampling of Sparse Fixed-Weight Vectors". IACR Trans. Cryptogr. Hardw. Embed. Syst. 2026(1): 353–375 (2026).

3. F. C. Rodrigues, D. L. Gazzoni Filho, G. Adj, I. A. Canales-Martínez, J. Chávez-Saab, J. López, M. Scott, F. Rodríguez-Henríquez: "Generation of Fast Finite Field Arithmetic for Cortex-M4 with ECDH and SQIsign Applications". IACR Trans. Cryptogr. Hardw. Embed. Syst. 2025(4): 588–620 (2025).

4. J. Chávez-Saab, F. Rodríguez-Henríquez, M. Tibouchi: "SwiftEC: Shallue-van de Woestijne Indifferentiable Function to Elliptic Curves". J. Cryptol. 38(1): 3 (2025)

5. M. A. Aardal, G. Adj, A. Alblooshi, D. F. Aranha, I. A. Canales Martinez, J. Chávez-Saab, D. Luiz Gazzoni Filho, K. Reijnders, F. Rodríguez-Henríquez: "Optimized One-Dimensional SQIsign Verification on Intel and Cortex-M4". IACR Trans. Cryptogr. Hardw. Embed. Syst. 2025(1): 497–522 (2025)

6. F. Campos, J. Chávez-Saab, J.-J. Chi-Domínguez, M. Meyer, K. Reijnders, F. Rodríguez-Henríquez, P. Schwabe, T. Wiggers: "Optimizations and Practicality of High-Security CSIDH". IACR Commun. Cryptol. 1(1): 5 (2024)

7. M. Corte-Real Santos, J. Komada Eriksen, M. Meyer, F. Rodríguez-Henríquez: "Finding Practical Parameters for Isogeny-based Cryptography". IACR Commun. Cryptol. 1(3): 39 (2024)

8. A. Augusto Giron, R. Custódio, F. Rodríguez-Henríquez: "Post-quantum hybrid key exchange: a systematic mapping study". J. Cryptogr. Eng. 13(1): 71–88 (2023)

9. G. Adj, J.-J. Chi-Domínguez, F. Rodríguez-Henríquez: "Karatsuba-based square-root Vélu's formulas applied to two isogeny-based protocols". J. Cryptogr. Eng. 13(1): 89–106 (2023)

10. K. Phalakarn, V. Suppakitpaisarn, F. Rodríguez-Henríquez, M. Anwar Hasan: "Vectorized and Parallel Computation of Large Smooth-Degree Isogenies using Precedence-Constrained Scheduling". IACR Trans. Cryptogr. Hardw. Embed. Syst. 2023(3): 246–269 (2023)

11. J.-J. Chi-Domínguez and F. Rodríguez-Henríquez: "Optimal strategies for CSIDH". Adv. Math. Commun. 16(2): 383–411 (2022)

12. L. Rivera-Zamarripa, G. Adj, N. Cruz Cortés, C. Aguilar Ibáñez, F. Rodríguez-Henríquez: "A Parallel Strategy for Solving Sparse Linear Systems Over Finite Fields". Computación y Sistemas 26(1) (2022)

13. J. Chávez-Saab, J.-J. Chi-Domínguez, S. Jaques, F. Rodríguez-Henríquez: "The SQALE of CSIDH: sublinear Vélu quantum-resistant isogeny action with low exponents". J. Cryptogr. Eng. 12(3): 349–368 (2022)

14. D. Cervantes-Vázquez, E. Ochoa-Jiménez, F. Rodríguez-Henríquez: "Parallel Strategies for SIDH: Toward Computing SIDH Twice as Fast". IEEE Trans. Computers 71(6): 1249–1260 (2022)

15. M. Á. León-Chávez, F. Rodríguez-Henríquez: "Post-Quantum Digital Signature for the Mexican Digital Invoices by Internet". Computación y Sistemas 25(4) (2021)

16. J.-J. Chi-Domínguez, F. Rodríguez-Henríquez, B. Smith: "Extending the GLS endomorphism to speed up GHS Weil descent using Magma". Finite Fields Their Appl. 75: 101891 (2021)

17. D. Cervantes-Vázquez, E. Ochoa-Jiménez, F. Rodríguez-Henríquez: "Extended supersingular isogeny Diffie-Hellman key exchange protocol: Revenge of the SIDH". IET Inf. Secur. 15(5): 364–374 (2021)

18. E. Ochoa-Jiménez, L. Rivera-Zamarripa, N. Cruz Cortés, F. Rodríguez-Henríquez: "Implementation of RSA Signatures on GPU and CPU Architectures". IEEE Access 8: 9928–9941 (2020)

19. M. Kiwi, Y. Kohayakawa, S. Rajsbaum, F. Rodríguez-Henríquez, J. L. Szwarcfiter, A. Viola: "A perspective on theoretical computer science in Latin America". Commun. ACM 63(11): 102–107 (2020).

20. L. Rivera-Zamarripa, L. M. Rodríguez, M. A. León-Chávez, N. Cruz-Cortés, F. Rodríguez-Henríquez: "Security Analysis of the Mexican Fiscal Digital Certificate System". Computación y Sistemas 23(2): 477–490 (2019)

21. T. Oliveira, J. López, D. Cervantes-Vázquez, F. Rodríguez-Henríquez: "Koblitz Curves over Quadratic Fields". J. Cryptol. 32(3): 867–894 (2019).

22. G. Adj, I. Canales-Martínez, N. Cruz-Cortés, A. Menezes, T. Oliveira, L. Rivera-Zamarripa, F. Rodríguez-Henríquez: "Computing discrete logarithms in cryptographically-interesting characteristic-three finite fields". Adv. Math. Commun. 12(4): 741–759 (2018).

23. F. Rodríguez-Henríquez, E. Savaş (editors): Special issue in honor of Peter Lawrence Montgomery. J. Cryptographic Engineering 8(3): 185–187 (2018)

24. T. Oliveira, J. López, F. Rodríguez-Henríquez: "The Montgomery Ladder on Binary Elliptic Curves". J. Cryptogr. Eng. 8(3): 241–258 (2018).

25. A. U. Ay, C. Mancillas-López, E. Öztürk, F. Rodríguez-Henríquez, E. Savaş: "Constant-time hardware computation of elliptic curve scalar multiplication around the 128 bit security level". Microprocessors and Microsystems - Embedded Hardware Design 62: 79–90 (2018)

26. G. Adj, I. Canales-Martínez, L. Rivera-Zamarripa, F. Rodríguez-Henríquez: "Smoothness Test for Polynomials Defined Over Small Characteristic Finite Fields". Mathematics in Computer Science 12(3): 319–337 (2018)

27. A. Faz-Hernández, J. López Hernández, E. Ochoa-Jiménez, F. Rodríguez-Henríquez: "A Faster Software Implementation of the Supersingular Isogeny Diffie-Hellman Key Exchange Protocol". IEEE Trans. Computers 67(11): 1622–1636 (2018).

28. S. Chatterjee, A. Menezes, F. Rodríguez-Henríquez: "On Instantiating Pairing-Based Protocols with Elliptic Curves of Embedding Degree One". IEEE Trans. Computers 66(6): 1061–1070 (2017).

29. J. E. Ochoa-Jiménez, F. Rodríguez-Henríquez: "Protected Implementation of Pairing Based Two Factor Authentication Protocol". IEEE Latin America Transactions 14(9): 4173–4180 (2016).

30. G. Adj, A. Menezes, T. Oliveira, F. Rodríguez-Henríquez: "Weakness of $\mathbb{F}_{3^{6\cdot 1429}}$ and $\mathbb{F}_{2^{4\cdot 3041}}$ for Discrete Logarithm Cryptography". Finite Fields Appl. 32: 148–170 (2015).

31. E. Zavattoni, L. J. Dominguez Perez, S. Mitsunari, A. H. Sánchez-Ramírez, T. Teruya, F. Rodríguez-Henríquez: "Software Implementation of an Attribute-Based Encryption Scheme". IEEE Trans. Computers 64(5): 1429–1441 (2015)

32. L. López-García, L. J. Dominguez Perez, F. Rodríguez-Henríquez: "A Pairing-Based Blind Signature E-Voting Scheme". Comput. J. 57(10): 1460–1471 (2014)

33. J. E. Guzmán-Trampe, N. Cruz-Cortés, L. J. Dominguez Perez, D. Ortiz-Arroyo, F. Rodríguez-Henríquez: "Low-cost addition-subtraction sequences for the final exponentiation in pairings". Finite Fields and Their Applications 29: 1–17 (2014)

34. G. Adj, F. Rodríguez-Henríquez: "Square Root Computation over Even Extension Fields". IEEE Trans. Computers 63(11): 2829–2841 (2014)

35. T. Oliveira, J. López, D. F. Aranha, F. Rodríguez-Henríquez: "Two is the fastest prime: lambda coordinates for binary elliptic curves". J. Cryptographic Engineering 4(1): 3–17 (2014)

36. D. Chakraborty, C. Mancillas-López, F. Rodríguez-Henríquez and P. Sarkar: "Efficient Hardware Implementations of BRW Polynomials and Tweakable Enciphering Schemes". IEEE Transactions on Computers, Vol. 62, Issue 2: 279–294, January 2013.

37. J. Taverne, A. Faz-Hernández, D. F. Aranha, F. Rodríguez-Henríquez, D. Hankerson, J. López: "Speeding scalar multiplication over binary elliptic curves using the new carry-less multiplication instruction". J. Cryptographic Engineering 1(3): 187–199 (2011)

38. L. Martínez-Ramos, L. López-García, F. Rodríguez-Henríquez: "Achieving Identity-Based Cryptography in a Personal Digital Assistant Device". J. Appl. Res. Technol. 9(3): 324–334 (2011).

39. J.-L. Beuchat, J. Detrey, N. Estibals, E. Okamoto, F. Rodríguez-Henríquez: "Fast Architectures for the η_T Pairing over Small-Characteristic Supersingular Elliptic Curves". IEEE Trans. Computers 60(2): 266–281 (2011).

40. C. Mancillas-López, D. Chakraborty, F. Rodríguez-Henríquez: "Reconfigurable Hardware Implementations of Tweakable Enciphering Schemes". IEEE Trans. Computers 59(11): 1547–1561 (2010).

41. O. Ahmadi, F. Rodríguez-Henríquez: "Low Complexity Cubing and Cube Root Computation over $\mathbb{F}_{3^m}$ in Polynomial Basis". IEEE Trans. Computers 59(10): 1297–1308 (2010).

42. D. Ortiz-Arroyo, F. Rodríguez-Henríquez, C. Coello Coello: "The Turing-850 Project: Developing a Personal Computer in the Early 1980s in Mexico". IEEE Annals Hist. Comput. 32(4): 60–71 (2010).

43. O. Ahmadi, D. Hankerson and F. Rodríguez-Henríquez, "Parallel Formulations of Scalar Multiplication on Koblitz Curves", Special Issue on Cryptography in Computer System Security, Journal of Universal Computer Science (JUCS), volume 14, No. 3, pp. 481–504, 2008.

44. V. González-García, F. Rodríguez-Henríquez and N. Cruz-Cortés, "On the Security of Mexican Digital Fiscal Documents", In: Special Issue on the 50 years of Computing in Mexico. Journal Computación y Sistemas, vol. 12, número 1, pp. 25–39, July-September 2008.

45. F. Rodríguez-Henríquez, G. Morales-Luna, J. López-Hernández: "Low-Complexity Bit-Parallel Square Root Computation over GF(2^m) for All Trinomials". IEEE Trans. Computers 57(4): 472–480 (2008).

46. N. Cruz-Cortés, F. Rodríguez-Henríquez, C. A. Coello Coello: "An Artificial Immune System Heuristic for Generating Short Addition Chains". IEEE Trans. Evol. Comput. 12(1): 1–24 (2008).

47. Y. Rangel-Romero, R. Vega-García, A. Menchaca-Méndez, D. Acoltzi-Cervantes, L. Martínez-Ramos, M. Mecate-Zambrano, F. Montalvo-Lezama, J. Barrón-Vidales, N. Cortez-Duarte, F. Rodríguez-Henríquez: "Comments on: 'How to Repair the Hill Cipher'". J. Zhejiang Univ. Sci. A 9(2): 211–214 (2008).

48. F. Rodríguez-Henríquez, G. Morales-Luna, Nazar A. Saqib, N. Cruz-Cortés. "Parallel Itoh-Tsujii multiplicative inversion algorithm for a special class of trinomials" Design, Codes and Cryptography 45(1): 19–37 (2007).

49. F. Rodríguez-Henríquez, D. Ortiz-Arroyo and C. García-Zamora, "Yet another improvement over the Mu–Varadharajan e-voting protocol", Computer Standards & Interfaces Volume 29, Issue 4, Pages 471–480, May 2007.

50. N. A. Saqib, F. Rodríguez-Henríquez, A. Díaz-Pérez, "A Reconfigurable Processor for High Speed Point Multiplication in Elliptic Curves", International Journal of Embedded Systems, pp. 237–249, Vol. 1, Issue 3–4, 2005.

51. F. Rodríguez-Henríquez, N. A. Saqib, A. Díaz-Pérez: "A Fast Parallel Implementation of Elliptic Curve Point Multiplication over GF(2^m)". Microprocessors and Microsystems 28(5–6): 329–339 (2004).

52. F. Rodríguez-Henríquez, Ç. K. Koç: "Parallel Multipliers Based on Special Irreducible Pentanomials". IEEE Trans. Computers 52(12): 1535–1542 (2003).

53. F. Rodríguez-Henríquez, N. A. Saqib, A. Díaz-Pérez: "4.2 Gbit/s Single-Chip FPGA Implementation of AES Algorithm". Electronics Letters 39(15): 1115–1116 (2003).

Preprint papers

0. G. Adj, J.-J. Chi-Domínguez, V. Mateu, F. Rodríguez-Henríquez: "Faulty isogenies: a new kind of leakage". IACR Cryptol. ePrint Arch. 2022: 153 (2022)

Selected conference papers

0. A. Perez Keilty, D. F. Aranha, E. Pagnin, F. Rodríguez-Henríquez: "That's AmorE: Amortized Efficiency for Pairing Delegation". CRYPTO (8) 2025: 211–246.

1. N. Carlini, J. Chávez-Saab, A. Hambitzer, F. Rodríguez-Henríquez, A. Shamir: "Polynomial Time Cryptanalytic Extraction of Deep Neural Networks in the Hard-Label Setting". EUROCRYPT (1) 2025: 364–396 [Best paper award].

2. I. A. Canales Martínez, J. Chávez-Saab, A. Hambitzer, F. Rodríguez-Henríquez, N. Satpute, A. Shamir: "Polynomial Time Cryptanalytic Extraction of Neural Network Models". EUROCRYPT (3) 2024: 3–33.

3. J. Chávez-Saab, F. Rodríguez-Henríquez, M. Tibouchi: "SwiftEC: Shallue-van de Woestijne Indifferentiable Function to Elliptic Curves - Faster Indifferentiable Hashing to Elliptic Curves". ASIACRYPT (1) 2022: 63–92 [Runner-up paper award]

4. E. Bellini, J. Chávez-Saab, J.-J. Chi-Domínguez, A. Esser, S. Ionica, L. Rivera-Zamarripa, F. Rodríguez-Henríquez, M. Trimoska, F. Zweydinger: "Parallel Isogeny Path Finding with Limited Memory". INDOCRYPT 2022: 294–316
5. D. F. Aranha, E. Pagnin, F. Rodríguez-Henríquez: "LOVE a Pairing". LATINCRYPT 2021: 320–340
6. J. Chávez-Saab, F. Rodríguez-Henríquez, M. Tibouchi: "Verifiable Isogeny Walks: Towards an Isogeny-Based Postquantum VDF". SAC 2021: 441–460
7. D. Cervantes-Vázquez, M. Chenu, J.-J. Chi-Domínguez, L. De Feo, F. Rodríguez-Henríquez, B. Smith: "Stronger and Faster Side-Channel Protections for CSIDH". LATINCRYPT 2019: 173–193.
8. G. Adj, D. Cervantes-Vázquez, J.-J. Chi-Domínguez, A. Menezes, F. Rodríguez-Henríquez: "On the Cost of Computing Isogenies Between Supersingular Elliptic Curves". SAC 2018: 322–343
9. T. Oliveira, J. López, H. Hisil, A. Faz-Hernández, F. Rodríguez-Henríquez: "How to (Pre-)Compute a Ladder - Improving the Performance of X25519 and X448". SAC 2017: 172–191.
10. N. Cruz-Cortés, E. Ochoa-Jiménez, L. Rivera-Zamarripa, F. Rodríguez-Henríquez: "A GPU Parallel Implementation of the RSA Private Operation". CARLA 2016: 188–203
11. T. Oliveira, J. López, F. Rodríguez-Henríquez: "Software Implementation of Koblitz Curves over Quadratic Fields". CHES 2016: 259–279 [Runner-up paper award]
12. A. U. Ay, E. Öztürk, F. Rodríguez-Henríquez, E. Savaş: "Design and Implementation of a Constant-Time FPGA Accelerator for Fast Elliptic Curve Cryptography". ReConFig 2016: 1–8.
13. G. Adj, A. Menezes, T. Oliveira, F. Rodríguez-Henríquez: "Computing Discrete Logarithms in $\mathbb{F}_{3^{6\cdot 137}}$ and $\mathbb{F}_{3^{6\cdot 163}}$ Using Magma". WAIFI 2014: 3–22.
14. T. Oliveira, D. F. Aranha, J. López Hernández, F. Rodríguez-Henríquez: "Fast Point Multiplication Algorithms for Binary Elliptic Curves with and without Precomputation". SAC 2014: 324–344.
15. G. Adj, A. Menezes, T. Oliveira, F. Rodríguez-Henríquez: "Weakness of $\mathbb{F}_{3^{6\cdot 509}}$ for Discrete Logarithm Cryptography". Pairing 2013: 20–44.
16. T. Oliveira, J. López, D. F. Aranha, F. Rodríguez-Henríquez: "Lambda Coordinates for Binary Elliptic Curves". CHES 2013: 311–330 [Best paper award].
17. A. H. Sánchez, F. Rodríguez-Henríquez: "NEON Implementation of an Attribute-Based Encryption Scheme". ACNS 2013: 322–338.
18. D. F. Aranha, L. Fuentes-Castañeda, E. Knapp, A. Menezes, F. Rodríguez-Henríquez: "Implementing Pairings at the 192-Bit Security Level". Pairing 2012: 177–195.
19. D. F. Aranha, A. Faz-Hernández, J. López, F. Rodríguez-Henríquez: "Faster Implementation of Scalar Multiplication on Koblitz Curves". LATINCRYPT 2012: 177–193.
20. L. Fuentes-Castañeda, E. Knapp, F. Rodríguez-Henríquez: "Faster Hashing to $\mathbb{G}_2$". SAC 2011: 412–430.
21. D. F. Aranha, E. Knapp, A. Menezes, F. Rodríguez-Henríquez: "Parallelizing the Weil and Tate Pairings". IMACC 2011: 275–295.
22. C. Chávez-Corona, E. Ferrer Moreno, F. Rodríguez-Henríquez: "Hardware Design of a 256-Bit Prime Field Multiplier Suitable for Computing Bilinear Pairings". ReConFig 2011: 229–234.

23. J. Taverne, A. Faz-Hernández, D. F. Aranha, F. Rodríguez-Henríquez, D. Hankerson, J. López: "Software Implementation of Binary Elliptic Curves: Impact of the Carry-Less Multiplier on Scalar Multiplication". CHES 2011: 108–123.

24. J.-L. Beuchat, J. E. González-Díaz, S. Mitsunari, E. Okamoto, F. Rodríguez-Henríquez, T. Teruya: "High-Speed Software Implementation of the Optimal Ate Pairing over Barreto-Naehrig Curves". Pairing 2010: 21–39.

25. C. Mancillas-López, D. Chakraborty, F. Rodríguez-Henríquez: "On Some Weaknesses in the Disk Encryption Schemes EME and EME2". ICISS 2009: 265–279.

26. J.-L. Beuchat, E. López-Trejo, L. Martínez-Ramos, S. Mitsunari, F. Rodríguez-Henríquez: "Multi-core Implementation of the Tate Pairing over Supersingular Elliptic Curves". CANS 2009: 413–432.

27. J.-L. Beuchat, J. Detrey, N. Estibals, E. Okamoto, F. Rodríguez-Henríquez: "Hardware Accelerator for the Tate Pairing in Characteristic Three Based on Karatsuba-Ofman Multipliers". CHES 2009: 225–239 [Best paper award].

28. J.-L. Beuchat, N. Brisebarre, J. Detrey, E. Okamoto, F. Rodríguez-Henríquez: "A Comparison Between Hardware Accelerators for the Modified Tate Pairing over $\mathbb{F}_{2^m}$ and $\mathbb{F}_{3^m}$". Pairing 2008: 297–315.

29. L. López-García, F. Rodríguez-Henríquez, M. A. León-Chávez: "An e-Voting Protocol Based on Pairing Blind Signatures". SECRYPT 2008: 214–217.

30. C. Mancillas-López, D. Chakraborty, F. Rodríguez-Henríquez: "Efficient Implementations of Some Tweakable Enciphering Schemes in Reconfigurable Hardware". INDOCRYPT 2007: 414–424.

31. F. Rodríguez-Henríquez, G. Morales-Luna, N. A. Saqib, N. Cruz-Cortés: "A Parallel Version of the Itoh-Tsujii Multiplicative Inversion Algorithm". ARC 2007: 226–237.

32. E. López-Trejo, F. Rodríguez-Henríquez, A. Díaz-Pérez: "An Efficient FPGA Implementation of CCM Mode Using AES". ICISC 2005: 208–215.

33. N. Cruz-Cortés, F. Rodríguez-Henríquez, R. Juárez Morales, C. A. Coello Coello: "Finding Optimal Addition Chains Using a Genetic Algorithm Approach". CIS 2005: 208–215.

34. M. Heinze, D. Ortiz-Arroyo, H. Legind Larsen, F. Rodríguez-Henríquez: "Fuzzeval: A Fuzzy Controller-Based Approach in Adaptive Learning for Backgammon Game". MICAI 2005: 224–233.

35. F. Rodríguez-Henríquez, N. A. Saqib, N. Cruz-Cortés: "A Fast Implementation of Multiplicative Inversion over GF(2^m)". ITCC (1) 2005: 574–579.

36. N. Cruz-Cortés, F. Rodríguez-Henríquez, C. A. Coello Coello: "On the Optimal Computation of Finite Field Exponentiation". IBERAMIA 2004: 747–756.

37. N. A. Saqib, F. Rodríguez-Henríquez, A. Díaz-Pérez: "A Parallel Architecture for Computing Scalar Multiplication on Hessian Elliptic Curves". ITCC (2) 2004: 493–497.

38. N. A. Saqib, F. Rodríguez-Henríquez, A. Díaz-Pérez: "A Parallel Architecture for Fast Computation of Elliptic Curve Scalar Multiplication over GF(2^m)". IPDPS/RAW 2004: 144–151.

39. N. A. Saqib, F. Rodríguez-Henríquez, A. Díaz-Pérez: "Two Approaches for a Single-Chip FPGA Implementation of an Encryptor/Decryptor AES Core". FPL 2003: 303–312.

40. F. Rodríguez-Henríquez, Ç. K. Koç: "On Fully Parallel Karatsuba Multipliers for GF(2^m)". CST 2003: 405–410.

41. F. Rodríguez-Henríquez, J. M. Rocha-Pérez, J. Silva-Martínez, "Performance of a Decision Feedback Demodulator In A Time-Dispersive Channel For ISI Cancellation And Its Implementation In Switched-Capacitor Technique", The 10th International Symposium on Personal, Indoor and Mobile Radio Communications Osaka, JAPAN September 15, 1999.

Student and post-doctoral supervision

Ph.D. students supervised

0. Dr. Nazar Abbas Saqib, "Efficient Implementation of Cryptographic Algorithms on Reconfigurable Hardware Devices", CINVESTAV, Sep 2004. Supervisors: Dr. Arturo Díaz-Pérez y Dr. Francisco Rodríguez-Henríquez.
1. Dr. María de Lourdes López García, "Diseño de un protocolo para votaciones electrónicas basado en firmas a ciegas definidas sobre emparejamientos bilineales", June 16, 2011, Supervisor: Dr. Francisco Rodríguez Henríquez.
2. Dr. Thomaz Eduardo de Figueiredo Oliveira, "Cryptography in Small-Characteristic Finite Fields", February 26, 2016. Supervisor: Dr. Francisco Rodríguez Henríquez and Dr. Julio López.
3. Dr. Gora Adj, "Discrete logarithms in small characteristic finite fields: attacking Type 1 pairing-based cryptography", July 27, 2016. Supervisors: Prof. Alfred Menezes and Dr. Francisco Rodríguez Henríquez.
4. Dr. José Eduardo Ochoa Jiménez "Analysis and efficient implementation of public key cryptographic protocols", February 28, 2019. Supervisor: Dr. Francisco Rodríguez Henríquez.
5. Dr. Jesús-Javier Chi Domínguez, "Elliptic curves in classical and post-quantum cryptography" December 6, 2019. Supervisor: Dr. Francisco Rodríguez-Henríquez.
6. Dr. Daniel Ildelfonso Cervantes Vázquez, "Isogenies on public-key cryptography", February 26, 2021, Supervisor: Dr. Francisco Rodríguez Henríquez.
7. Dr. José Abraham Bernal Gutiérrez, "Quantum Security Estimates for Isogeny-based Cryptography and New Isogeny-based Cryptographic Primitives", April 28, Supervisors: Dr. Cuauhtemoc Mancillas López and Dr. Francisco Rodríguez Henríquez.
8. Dr. Jorge Emmanuel Chávez Saab, "Estimados de Seguridad Cuántica para Criptografía Basada en Isogenias y Nuevas Primitivas Criptográficas Basadas en Isogenias". July 28, 2023.Supervisors: Dr. Francisco Rodríguez Henríquez and Dr. Cuauhtemoc Mancillas López.

Master's students supervised

0. M.Sc. Laura Itzelt Reyes Montiel, "Estudio, Diseño y Evaluación de Protocolos de Autenticación para Redes Inalámbricas", CINVESTAV, January 2004. Supervisor: Dr. Francisco Rodríguez-Henríquez.
1. M.Sc. Carlos Eduardo López Peza, "Sistema de Seguridad para Intercambio de Datos en Dispositivos Móviles" CINVESTAV, April 2005 Supervisor: Dr. Francisco Rodríguez-Henríquez.
2. M.Sc. Guillermo Martínez Silva, "Diseño e Implementación de una Autoridad Certificadora en Plataformas Móviles" Tec de Monterrey campus Ciudad. de México, July Supervisor: Dr. Francisco Rodríguez-Henríquez.
3. M.Sc. Emmanuel López Trejo, "Implementación Eficiente en FPGA del Modo CCM usando AES" CINVESTAV, September 2005. Supervisor: Dr. Francisco Rodríguez-Henríquez.
4. M.Sc. Claudia Patricia García Zamora: "Diseño y Desarrollo de un Sistema para Elecciones Electrónicas Seguras (SELES)" CINVESTAV, September 2005. Supervisor: Dr. Francisco Rodríguez-Henríquez.

5. M.Sc. Juan Manuel Cruz Alcaraz: "Multiplicación Escalar en Curvas de Koblitz: Arquitectura en Hardware Reconfigurable" CINVESTAV, November 2005. Supervisor: Dr. Francisco Rodríguez-Henríquez.

6. M.Sc. Efrén Clemente Cuervo: "Implementación de un Monedero Digital Móvil" CINVESTAV, November 2005. Supervisor: Dr. Francisco Rodríguez-Henríquez.

7. M.Sc. Sabel Mercurio Hernández Rodríguez: "Multiplicación Escalar en Curvas Elípticas empleando Bisección de Punto: una Arquitectura en Hardware Reconfigurable" CINVESTAV, February 2006. Supervisor: Dr. Francisco Rodríguez-Henríquez.

8. M.Sc. Óscar Irineo Fuentes: "Jugador Inteligente de Backgammon" Departamento de Computación, CINVESTAV, December 2006. Supervisors: Dr. Francisco Rodríguez-Henríquez. Co-supervisor: Dra. Nareli Cruz Cortés.

9. M.Sc. Verónica Edith Bautista López: "Sistema electrónico de compra y venta de servicios utilizando dispositivos móviles ligeros" Facultad de Ciencias de la Computación, Benemérita Universidad Autónoma de Puebla, February 2007. Supervisors: Dr. Francisco Rodríguez-Henríquez. Co-supervisor: Dr. Miguel Ángel León Chávez.

10. M. Sc. María de Lourdes López García: "Sistema electrónico de votación" Facultad de Ciencias de la Computación, Benemérita Universidad Autónoma de Puebla, february Supervisors: Dr. Miguel Ángel León Chávez. Co-supervisor: Dr. Francisco Rodríguez-Henríquez.

11. M.Sc. Vladimir González García: "Diseño y Desarrollo de un Prototipo de Notaría Digital" Laboratorio Nacional de Informática Avanzada, Centro de Enseñanza LA-NIA, August 2007. Supervisors: Dr. Francisco Rodríguez-Henríquez. Co-supervisor: Dra. Nareli Cruz Cortés.

12. M.Sc. Luis Martínez Ramos: "Diseño e implementación eficiente del emparejamiento etaT en dispositivos móviles y arquitecturas multinúcleo". Departamento de Computación, CINVESTAV, December 2008. Supervisor: Dr. Francisco Rodríguez-Henríquez.

13. M.Sc. Nidia Asunción Cortez Duarte: "Implementación de Emparejamientos bilineales en característica dos y tres en Hardware Reconfigurable". Departamento de Computación, CINVESTAV, August 2009. Supervisor: Dr. Francisco Rodríguez-Henríquez.

14. M.Sc. Gabriel Labrada Hernández, "Paralelización de la Multiplicación escalar en curvas elípticas en una arquitectura multinúcleo de Intel". Departamento de Computación, CINVESTAV, 26.02.2010. Supervisor: Dr. Francisco Rodríguez-Henríquez.

15. M.Sc. Jesús Francisco Quintanar Villareal, "Sistema de monitorización ambiental con redes inalámbricas de sensores para el insectario del CINVESTAV-IPN Zacatenco". Departamento de Computación, CINVESTAV, 12.08.2010. Supervisor: Dr. Francisco Rodríguez-Henríquez.

16. M.Sc. Jonathan Taverne, "Implentation Efficiente de la Multiplication Scalaire utilisant la Parallisation Cryptographie sur les Courbes Elliptiques". Departamento de Computación, CINVESTAV, September 24, 2010. Supervisor: Dr. Francisco Rodríguez-Henríquez (In collaboration with Université Lyon 1, France).

17. M.Sc. Jorge Enrique González Díaz, "Diseño e implementación eficiente del emparejamiento óptimo". Departamento de Computación, CINVESTAV, 29.09.2010. Supervisor: Dr. Francisco Rodríguez-Henríquez.

18. M.Sc. Iván Cabrera Altamirano, "Mecanismo seguro de recolección de datos utilizando nodos móviles en redes inalámbricas de sensores", 14.12.2010, Supervisor: Dr. Francisco Rodríguez-Henríquez.

19. M.Sc. Eric Zavattoni, "Implementation en C/C++ du protocole D'attribute based encryption en utilizant les couplages asymetriques", 16.09.2011, Supervisor: Dr. Francisco Rodríguez-Henríquez (In collaboration with Université Lyon 1, France).

20. M.Sc. Laura Fuentes Castañeda, “Estudio y Análisis de emparejamientos bilineales definidos sobre curvas ordinarias con alto nivel de seguridad”, 09.12.2011, Supervisor: Francisco Rodríguez Henríquez.

21. M.Sc. Armando Faz Hernández, “Implementación multinúcleo de la multiplicación escalar en curvas de Roblitz”, 17.02.2012, Supervisors: Dr. Francisco Rodríguez Henríquez y Dr. Debrup Chakraborty.

22. M. Sc. Gora Adj, “Racines Carrées dans les Extensions Quadratiques de Corps Finis”, 10/07/2012, Director de Tesis: Dr. Francisco Rodríguez Henríquez (In collaboration with Université Lyon 1, France).

23. M.Sc. Cuauhtémoc Chávez Corona, “Implementación en hardware de multiplicadores modulares orientados a emparejamientos bilineales”, 13.07.2012, Supervisors: Dr. Francisco Rodríguez Henríquez y Dr. Debrup Chakraborty.

24. M.Sc. Ana Helena Sánchez Ramírez, “Implementación de la criptografía basada en atributos en un dispositivo móvil”, 23.10.2012, Supervisor: Dr. Francisco Rodríguez Henríquez.

25. M.Sc. José Eduardo Ochoa Jiménez, “Función picadillo determinista al grupo G2 y su aplicación en autenticación para dispositivos móviles” 04.12.2013, Supervisors: Dr. Francisco Rodríguez Henríquez y Dra. María de Lourdes López García.

26. M.Sc. Rogelio Vargas Márquez, “Diseño de un compilador para protocolos criptográficos” 13.12.2013, Supervisor: Dr. Francisco Rodríguez Henríquez.

27. M.Sc. Jesús Javier Chi Domínguez, “El ataque gGHS aplicado a curvas de Galbraith-Lin-Scott” 02.12.2015, Supervisor: Dr. Francisco Rodríguez Henríquez.

28. M.Sc. Isaac Andrés Canales Martínez, “Implementación eficiente de prueba de suavidad para polinomios” 02.12.2015, Supervisor: Dr. Francisco Rodríguez Henríquez.

29. M.Sc. Abraham Jesús Basurto Becerra, “Aspectos de seguridad de Bitcoin y su aplicación en una alternativa de infraestructura de llave pública”, 17.12.2015, Supervisor: Dr. Francisco Rodríguez Henríquez.

30. M.Sc. Daniel Idelfonso Cervantes Vázquez, “De la búsqueda de endomorfismos eficientes en curvas elípticas binarias”. 05.08.2016, Supervisor: Dr. Francisco Rodríguez Henríquez.

31. M.Sc. Laiphel Marco Gómez Trujillo, “Análisis de la seguridad y privacidad ofrecida por dispositivos Android”, 11/10/2017. Director de Tesis: Dr. Francisco José Rambó Rodríguez Henríquez.

32. M.Sc. Mathilde Chenu - de La Morinerie, “Isogeny-based quantum-resistant signatures”. September 25, 2018. Advisors: Francisco Rodríguez Henríquez and Benjamin Smith (In collaboration with Université Paris Saclay).

Post-doctoral fellows supervised

0. Dr. Luis J Dominguez Perez (Completed), CINVESTAV. Project title: “Applications of pairing-based cryptography”. 2014/01-2014/12.

1. Dr. Thomas Oliveira (Completed), CINVESTAV. Project title: “Applications of elliptic-curve-based cryptography”. 2016/03-2016/09.

2. Dr. Gora Adj (Completed), CINVESTAV. Project title: “Studies on discrete logarithms for small characteristic fields” 2016/08-2016/12.

Event Organization

0. General co-chair: CHES 2027 (Cancún, Mexico), 2027.
1. Program co-chair: SAC 2027 (University of Victoria, Canada), September 2027.
2. Program co-chair: AFRICACRYPT 2026 (Hammamet, Tunisia), July 8–10, 2026.
3. Artifact Chair: EUROCRYPT 2026.
4. General chair: CRYPTO 2025 (Santa Barbara, USA), August 2025.
5. Main organizer: Glowing Hot Topics in Cryptography (GHTC), CRYPTO-affiliated event, 2022–2025.
6. Program co-chair: CHES 2024 (Halifax, Canada), September 2024.
7. Program co-chair: LATIN 2022 (Guanajuato, México), November 2022.
8. Program co-chair: WAIFI 2018 (Bergen, Norway), June 2018.
9. Program co-chair: The IACR Cryptology School on Advanced School of Cryptography, La Habana, Cuba, September 15–19, 2017.
10. General chair and program co-chair: LATINCRYPT 2015 (Guadalajara, México), August 2015.
11. General co-chair: ECC 2012 (Querétaro, México), October 2012.
12. Program co-chair: WAIFI 2012 (Bochum, Germany), July 2012.
13. General chair and co-founder: LATINCRYPT 2010 (Puebla, México), August 2010.

Editorial service

0. Member, IACR Board of Directors, 2024–2026.
1. Member, ASIACRYPT Steering Committee, 2024–present.
2. Member, CHES Steering Committee, 2023–2028.
3. Co-Editor-in-Chief, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2024.
4. Associate editor of Journal of Universal Computer Science (JUCS), 2009–2021.
5. Associate editor of IEEE Transactions on Computers, 2011–2016.
6. Associate editor of Journal of Cryptographic Engineering, Springer, 2011–2025.
7. Associate editor of Elsevier's Journal of VLSI, 2017–2020.
8. Guest editor, Special Issue in honor of Peter Lawrence Montgomery, Journal of Cryptographic Engineering, Springer, Volume 8, Issue 3, October 2018.
9. Associate editor of IEEE Transactions on Emerging Topics in Computing, 2019–2022.
10. Program committee membership includes EuroISI 2008; ENC 2009; CHES 2009, 2019–2023, 2026–2027; WAIFI 2010, 2012, 2014, 2018; LATINCRYPT 2010, 2012, 2014–2015, 2017, 2019, 2021, 2023, 2025; Pairing 2010, 2012–2013; LightSec 2011, 2013–2015, 2017–2018, 2025; ARC 2012–2013; ACNS 2013, 2017, 2019, 2024; SAC 2013; ARITH22–ARITH26; WITCOM 2015; INDOCRYPT 2015; ASIACRYPT 2021; LATIN 2022; EUROCRYPT 2026–2027; and CRYPTO 2027.

11. IACR program chair: CHES 2024.

Selected invited talks

0. “Introduction to Isogeny-based cryptography”, Talk given in the Coloquio Nacional de Códigos y Criptografía, June 26, 2025.
1. “The quest for reliable post-quantum cryptography”, Talk given in Ciberseguridad 2024, INAOE, October 15, 2024.
2. “A state-of-the-art review of key-exchange isogeny-based protocols”, talk given in the Technology Innovation Institute (TII), Abu Dhabi, United Arab Emirates - March 11, 2021.
3. “Pre-quantum and post-quantum variants of the Diffie-Hellman protocol”, talk given at the 7th International Conference on Mathematics and Computing (ICMC 2021)Shibpur, India - March 5, 2021
4. “How long can we safely use pre-quantum ECC? [a.k.a. The end of ECC]”, Opening remarks for the ECC 2020 third discussion panel. October 29, 2020.
5. “On Vélu’s new formulae and their applications to CSIDH and B-SIDH constant-time implementations”, talk given at the Rump Session of CHES 2020. September 16, 2020.
6. “Parallel strategies for SIDH: Towards computing SIDH twice as fast”, talk given in the Tutte Colloquium, Combinatorics & Optimization Department, Faculty of Mathematics, University of Waterloo. Waterloo, Ontario, Canada - February 28, 2020.
7. “A brief introduction to quantum hardware”, talk given in the Electrical Engineering Department, University of Waterloo. Waterloo, Ontario, Canada - November 20, 2019.
8. “Side-Channel Protections for CSIDH ”, talk given in the Crypto reading group of the Combinatorics & Optimization Department, Faculty of Mathematics, University of Waterloo. Waterloo, Ontario, Canada -October 9, 2019.
9. “Isogenous Alice”, talk given in the The Advanced School on Cryptology and Information Security in Latin America (ASCrypto) 2019, Santiago, Chile - October First, 2019.
10. “Some cryptographic aspects of electronic voting”. Talk given at the Summer School on Cryptography Crypto-CO, Medellín Colombia June 14 2019
11. “Isogenous Alice”. Talk given at the Summer School on Cryptography Crypto-CO, Medellín Colombia June 14 2019
12. “Modern Alice’s Adventures in Cryptoland”. Talk given at the Summer School on Cryptography Crypto-CO, Medellín Colombia June 10 2019
13. “A [magical] parallel variant of SIDH ”, talk given in the CHES 2018 rump session, Amsterdam, September 2018.
14. “Bitcoin: An unexpected journey”, and its short animation video, at slide 46. Talk given at the ”Coloquio CINVESTAV”, Auditorio Rosenblueth, CDMX, México - February 7, 2018.
15. “Hardware implementation of cryptographic algorithms”, Latincrypt 2017, Havana, Cuba, September 18, 2017.
16. “Discrete Logarithm Problem in characteristic-three pairing-based cryptography”, talk given in Crypto 2016 rump session, Santa Barbara, California - August 18, 2016
17. “Crowdsourcing discrete logs to humans”, talk given in the CHES 2016 rump session, Santa Barbara, California - August 18, 2016

18. "Efficient implementation of pairing-based and elliptic-curve based protocols and their applications to modern security" In: Centre International de Mathématiques Pures et Appliquées (CIMPA), Modelos matemáticos para las aplicaciones de seguridad en La Habana Cuba, 29 de agosto a 9 de septiembre.

19. "Aplicaciones de muy alto impacto y muy alto volumen de la seguridad informática en México [versión actualizada]", talk given at the CSMX 2016, Taller de Seguridad Informática Puebla, Mexico Friday April 29 2016.

20. "A Little Day Music of Four Cryptographic Problems and their Solutions", talk given in the Semana de Ciberseguridad at CIC-IPN Mexico City, Thursday December 4 2014.

21. "Computing Discrete Logarithms in F36
ast137 and F36
ast163 using Magma", International Workshop on the Arithmetic of Finite Fields WAIFI 2014 Gebze, Turkey. September 26-28, 2014.

22. "Implementing pairing-based protocols", keynote speaker at the 6th International Conference on Pairing-Based Cryptography (Pairing 2013), Beijing, China, November 22-24 2013.

23. "On the complexity of computing discrete logarithms in the field GF(36
ast509)", Worcester Polytechnic Institute (WPI),Worcester, EUA, September 17 2013.

24. "Hardware design of cryptographic algorithms". The 13th International Conference on Cryptology (Indocrypt 2012), 9 December 2012 Kolkata, India.

25. "Introduction to Elliptic Curve Cryptography (Part II) Aspectos de Implementación— Implementation Aspects", Workshop on Elliptic curve cryptography ECC 2012, Querétaro, México, October 2012.

26. "Hardware Implementation of Pairings", Invited Speaker In The São Paulo Advanced School of Cryptography — SP-ASCrypto 2011, Oct 20-26, 2011, at the University of Campinas, Brazil.

27. "Multicore Implementation of two public-key cryptographic algorithms". Universidad de Puerto Rico, San Juan, February 2011.

28. "Faster Implementation of Pairings", Invited Speaker In Workshop on Elliptic Curves and Computation, ECC 2010, Oct 18-22, 2010 at Microsoft Research in Redmond, Washington, USA

29. "Aplicaciones de muy alto impacto y muy alto volumen de la seguridad informática en México". Primera Escuela Nacional en Seguridad de la Información y los Servicios, Mexico City, November 28 2010.

30. "Leakage-resilient cryptographers in the Latincrypt-model", talk given in Crypto 2010 rump session, Santa Barbara, California - August 18, 2010

31. "Software and Hardware Implementations of the Tate pairing over Supersingular Elliptic Curves". Universidad de Puerto Rico, San Juan, February 5 2010.

32. "Information Security Management". Universidad del Turabo, Puerto Rico, February 1-5, 2010.

33. "Alice's Adventures in Cryptoland", Keynote speech at 19th Internacional Conference on Electronics Communications and Computers (Conielecomp 2009), 27 de febrero de 2009.

34. "Extendiendo nuestros sentidos y nuestros destinos con redes inalámbricas de sensores (in Spanish)". Grand Challenges in Computer Science Research in Latin America Workshop (CharLA'08), Buenos Aires Argentina, September 5 2008.

Research funding

0. CONACyT project 313572: “Sistema descentralizado para detectar zonas de riesgo y contacto con personas confirmadas con COVID-19 protegiendo la privacidad de los participantes”, $80,000 USD, May 2020.
1. México-Uruguay Binational project: “Rastreo de recorridos integrado a datos de diagnóstico”, $8,000 USD, 2020-2021.
2. México-Uruguay Binational project: “Sistema digital descentralizado para contactos con personas confirmas con COVID-19”, $15,000 USD, 2020-2021.
3. Microsoft Research Donative of $5,000 USD to organize Latincrypt 2017, the Fifth International Conference on Cryptology and Information Security in Latin America, September 2017, La Habana, Cuba.
4. IACR donative of $5,000 USD to organize ASCrypto 2017, The Advanced School on Cryptology and Information Security in Latin America, September 2017, La Habana, Cuba.
5. Oracle México Donative of $5,000 USD to organize Latincrypt 2015, Latincrypt 2015, the Fourth International Conference on Cryptology and Information Security in Latin America, August 2015, Guadalajara, México.
6. Microsoft Research Donative of $5,000 USD to organize Latincrypt 2015, the Fourth International Conference on Cryptology and Information Security in Latin America,. August 2015, Guadalajara, México.
7. SEP-CONACyT, Basic Science project“Análisis, estudio y desarrollo de criptografiia post-cuántica”, $110,000 USD, 2013-2016.
8. Microsoft Research Donative of $5,000 USD to organize the ECC 2012, the 16th in a series of annual workshops dedicated to the study of elliptic curve cryptography and related areas. October 2012, Querétaro, México.
9. University of California and CONACyT, proyect UCMEXUS 2010: “Pairing-based cryptography with applications to information security”, $25,000 USD.
10. CONACyT, Basic Science project: “Análisis y estudio de algoritmos de alto desempeño para emparejamientos bilineales y criptografía basada en la identidad y su implementación en software y Hardware”, $10,000 USD, 2008-2011.
11. SEP-CONACyT, Basic Science project 2006-2009: “Diseño e Implementación de Algoritmos Criptográficos en Hardware Reconfigurable Usando Heuriisticas Evolutivas”, $45,000 USD, 2006-2009.
12. CONACyT-NSF project: “Secure Information Sharing for Distance Collaboration”, $68,000 USD, 2003-2006 [Participant Researcher].
13. SEP-CONACyT, Basic Science project: “Estudio, Análisis y Desarrollo de Algoritmos de Muy Alto Desempeño para Arquitecturas Hardware/Software”, $120,000 USD, 2003-2006 [Participant Researcher].

Abu Dhabi, UAE. October 23, 2026.