Francisco Rodríguez-Henríquez

Associate Professor CINVESTAV 3-C
CINVESTAV-IPN
Av. Instituto Politécnico Nacional No. 2508, 07360,
México City, México
Tel: (52) (55) 5061 3800 Ext. 6570
fax: (52) (55) 5061 3757
francisco@cs.cinvestav.mx
http://delta.cs.cinvestav.mx/~francisco/

11 de marzo de 2015

Personal information

Nationality:	Salvadoran and Mexican
Date and Place of Birth:	March 5, 1968, San Salvador, El Salvador
Civil State:	Married.

Education

1996-2000:	**Doctor of Philosophy,** Computer and Electrical Engineering Department, Oregon State University, thesis title: "New Algorithms and Architectures for Arithmetic in GF(2^m) Suitable for Elliptic Curve Cryptography" Advisor: Çetin K. Koç.
1989-1992:	**Master in Science,** Electronic Engineering, National Institute of Astrophysics, Optics and Electronics, Puebla, México.
1984-1989:	**Bachelors in Electronics,** Faculty of Science, University of Puebla, México

Research interests

Applied cryptography. My main area of interest is on efficient hardware and software implementations of cryptographic algorithms with especial emphasis on elliptic curve cryptography, bilinear pairings and pairing-based protocols.

Professional experience

03/2007-Present:	**Associate Professor,** Center for Advanced Research CINVESTAV, México
05/2002-02/2007:	**Assistant Professor,** Center for Advanced Research CINVESTAV, México
02/2001-04/2002:	**Cryptographic Designer Architect,** rTrust Technologies, Inc, Oregon, EUA
07/2000-01/2001:	**Security Architect,** CV Cryptovision GmbH, Germany

Publications

Books

1. Francisco Rodríguez-Henríquez, N.A. Saqib, Arturo Díaz Pérez and Cetin Kaya Koc, "Cryptographic Algorithms on Reconfigurable Hardware", Springer First Edition, November 2006, 362 pages, ISBN: 0387338837.

Book chapters

1. Debrup Chakraborty and Francisco Rodríguez-Henríquez, "Block Cipher Modes of Operation from a Hardware Implementation Perspective", in Çetin Kaya Koç (editor), Cryptographic Engineering, Springer, 2008 ISBN 978-0-387-71817-0.

Journal papers

1. Eric Zavattoni, Luis J. Dominguez Perez, Shigeo Mitsunari, Ana H. Sánchez-Ramrez, Tadanori Teruya, Francisco Rodríguez-Henríquez: Software implementation of an Attribute-Based Encryption scheme (to appear in IEEE Transactions on Computers)

2. Gora Adj, Alfred Menezes, Thomaz Oliveira, Francisco Rodríguez-Henríquez: Weakness of $\mathbb{F}_{3^{6*1429}}$ and $\mathbb{F}_{2^{4*3041}}$ for Discrete Logarithm Cryptography Finite Fields and Their Applications 32: 148-170 (2015)

3. María de Lourdes López-García, Luis J Domínguez Pérez and Francisco Rodríguez-Henríquez: A pairing-based blind signature e-voting scheme. The Computer Journal 57(10): 1460-1471 (2014)

4. Gora Adj and Francisco Rodríguez-Henríquez: Square root computation over even extension fields. IEEE Trans. Computers 63(11): 2829-2841 (2014)

5. Juan E. Guzmán-Trampe, Nareli Cruz Cortés, Luis J. Dominguez Perez, Daniel Ortiz Arroyo, Francisco Rodríguez-Henríquez: Low-cost addition-subtraction sequences for the final exponentiation in pairings. Finite Fields and Their Applications 29: 1-17 (2014)

6. Thomaz Oliveira, Julio López, Diego F. Aranha, Francisco Rodríguez-Henríquez: Two is the fastest prime: lambda coordinates for binary elliptic curves. J. Cryptographic Engineering 4(1): 3-17 (2014)

7. Debrup Chakraborty, Cuauhtemoc Mancillas-López, Francisco Rodríguez-Henríquez and Palash Sarkar: Efficient Hardware Implementations of BRW Polynomials and Tweakable Enciphering Schemes. IEEE Transactions on Computers, Vol. 62, Issue 2: 279-294, January 2013.

8. Jonathan Taverne, Armando Faz-Hernández, Diego F. Aranha, Francisco Rodríguez-Henríquez, Darrel Hankerson and Julio López: Speeding scalar multiplication over binary elliptic curves using the new carry-less multiplication instruction. Springer Journal of Cryptographic Engineering, Vol. 1, Issue 3: 187-199, April 2011.

9. Luis Martínez-Ramos, Lourdes López-García and Francisco Rodríguez-Henríquez: Achieving Identity-Based Cryptography in a Personal Digital Assistant Device. The Journal Of Applied Research And Technology, Vol.9, Issue 3: 324-334, December 2011.

10. Jean-Luc Beuchat, Jérémie Detrey, Nicolas Estibals, Eiji Okamoto and Francisco Rodríguez-Henríquez: Fast Architectures for the η_T Pairing over Small-Characteristic Supersingular Elliptic Curves. IEEE Transactions on Computers, Vol. 60, Issue 2: 266-281, February 2011.

11. Cuauhtemoc Mancillas-López, Debrup Chakraborty and Francisco Rodríguez-Henríquez: Reconfigurable Hardware Implementations of Tweakable Enciphering Schemes. IEEE Transactions on Computers Vol. 59, Issue 11: 1547-1561, November 2010.

12. Omran Ahmadi and Francisco Rodríguez-Henríquez: Low Complexity Cubing and Cube Root Computation over $\mathbb{F}_{3m}$ in Standard Basis. IEEE Transactions on Computers, Vol. 59, Issue 10: 1297-1308, October 2010.

13. Daniel Ortiz-Arroyo, Francisco Rodríguez-Henríquez and Carlos Coello Coello: The Turing-850 Project: Developing a Personal Computer in the Early 1980s in Mexico, IEEE Annals of the History of Computing, Vol 32, Issue 4: 60-71, October-December 2010.

14. Vladimir González García, Francisco Rodríguez-Henríquez and Nareli Cruz Cortés: On the Security of Mexican Digital Fiscal Documents. Computación y Sistemas, Vol 12, Issue 1: 25-39, January 2008.

15. Omran Ahmadi, Darrel Hankerson and Francisco 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, Issue 3: 481-504, 2008.

16. Francisco Rodríguez-Henríquez, Guillermo Morales-Luna and Julio López-Hernández: Low Complexity Bit-Parallel Square Root Computation over GF(2^m) for all Trinomials. IEEE Transactions on Computers, Vol. 57, Issue 4: 472–480, April 2008.

17. Nareli Cruz-Cortés, Francisco Rodríguez-Henríquez and Carlos A. Coello Coello: An Artificial Immune System Heuristic for Generating Short Addition Chains. IEEE Transactions on Evolutionary Computation, Vol. 12, Issue 1: 1-24, February 2008.

18. Yahir Rangel-Romero, Rodrigo Vega-Garca, Adriana Menchaca-Méndez, Daniel Acoltzi-Cervantes, Luis Martínez-Ramos, Miriam Mecate-Zambrano, Fernando Montalvo-Lezama, Jesús Barrón-Vidales, Nidia Cortez-Duarte and Francisco Rodríguez-Henríquez: Comments on: How to repair the Hill cipher, Journal of Zhejiang University - Science A, Volume 9, Issue 2: 211-214, February 2008, Springer.

19. Francisco Rodríguez-Henríquez, Guillermo Morales-Luna, Nazar A. Saqib and Nareli Cruz Cortés: Parallel Itoh-Tsujii multiplicative inversion algorithm for a special class of trinomials. Design, Codes and Cryptography Vol. 45, Issue 1: 19-37, January 2007.

20. Francisco Rodríguez-Henríquez, Daniel Ortiz-Arroyo and Claudia García-Zamora: Yet another improvement over the Mu-Varadharajan e-voting protocol, Computer Standards & Interfaces Volume 29, Issue 4: 471-480, May 2007.

21. Nazar A. Saqib, Francisco Rodríguez-Henríquez and Arturo Díaz-Pérez: A Reconfigurable Processor for High Speed Point Multiplication in Elliptic Curves, International Journal of Embedded Systems, Vol. 1, Issue 3-4: 237-249, 2005.

22. Francisco Rodríguez-Henríquez, Nazar A. Saqib and Arturo Díaz-Pérez: A Fast Parallel Implementation of Elliptic Curve Point Multiplication over GF(2^m). Journal of Microprocessor and Microsystems Vol. 28, Issue 5-6: 329-339, August 2004.

23. Francisco Rodríguez-Henríquez and Çetin K. Koç: Parallel Multipliers based on Special Irreducible Pentanomials. IEEE Transactions on Computers, Vol. 52, Issue 12: 1535-1542, December 2003.

24. Francisco Rodríguez-Henríquez, Nazar A. Saqib, and Arturo Díaz-Pérez: 4.2 Gbit/s single-chip FPGA implementation of AES algorithm. Electronics Letters, Vol.39, Issue 15: 1115-1116, July 24, 2003.

Selected international conference papers

1. Gora Adj, Alfred Menezes, Thomaz Oliveira, Francisco Rodríguez-Henríquez: Computing Discrete Logarithms in $\mathbb{F}_{3^{6*137}}$ and $\mathbb{F}_{3^{6*163}}$ Using Magma. WAIFI 2014: Vol. 9061 in Lecture Notes in Computer Science, pp 3-22

2. Thomaz Oliveira, Diego F. Aranha, Julio López Hernández, Francisco Rodríguez-Henríquez: Fast Point Multiplication Algorithms for Binary Elliptic Curves with and without Precomputation. Selected Areas in Cryptography 2014: Vol. 8781 in Lecture Notes in Computer Science, 324-344

3. Gora Adj, Alfred Menezes, Thomaz Oliveira and Francisco Rodríguez-Henríquez: Weakness of $\mathbb{F}_{3^{6*509}}$ for Discrete Logarithm Cryptography. Pairing 2013: Vol. 8365 in Lecture Notes in Computer Science, pp 311-330

4. Thomaz Oliveira, Julio López, Diego F. Aranha and Francisco Rodríguez-Henríquez: Lambda coordinates for binary elliptic curves. CHES 2013: Vol. 8086 in Lecture Notes in Computer Science, pp 311-330 [**Best paper award**].

5. Ana Helena Sánchez and Francisco Rodríguez-Henríquez: NEON implementation of an attribute-based encryption scheme. ACNS 2013: Vol. 7954 in Lecture Notes in Computer Science, pp 322-338

6. Diego F. Aranha, Laura Fuentes-Castañeda, Edward Knapp, Alfred Menezes and Francisco Rodríguez-Henríquez: Implementing Pairings at the 192-Bit Security Level. Pairing 2012: Vol. 7708 in Lecture Notes in Computer Science, pp 177-195

7. Diego F. Aranha, Armando Faz-Hernández, Julio López and Francisco Rodríguez-Henríquez: Faster Implementation of Scalar Multiplication on Koblitz Curves. LATINCRYPT 2012: Vol. 7533 in Lecture Notes in Computer Science, pp 177-193.

8. Laura Fuentes-Castañeda, Edward Knapp and Francisco Rodríguez-Henríquez: Faster Hashing to $\mathbb{G}_2$, SAC 2011: Vol. 7118 in Lecture Notes in Computer Science, pp 412-430.

9. Diego F. Aranha, Edward Knapp, Alfred Menezes and Francisco Rodríguez-Henríquez: Parallelizing the Weil and Tate Pairings. IMA Int. Conf. 2011: Vol. 7089 in Lecture Notes in Computer Science, pp 275-295.

10. Cuauhtémoc Chávez-Corona, Edgar Ferrer Moreno and Francisco Rodríguez Henríquez: Hardware design of a 256-bit prime field multiplier suitable for computing bilinear pairings, 2011 International Conference on ReConFigurable Computing and FPGAs (ReConFig 2011), pp 229-234.

11. Jonathan Taverne, Armando Faz-Hernández, Diego F. Aranha, Francisco Rodríguez-Henríquez, Darrel Hankerson and Julio López: Software Implementation of Binary Elliptic Curves: Impact of the Carry-Less Multiplier on Scalar Multiplication. CHES 2011, Vol. 6917 in Lecture Notes in Computer Science, pp 108-123.

12. Jean-Luc Beuchat, Jorge Enrique González Díaz, Shigeo Mitsunari, Eiji Okamoto, Francisco Rodríguez-Henríquez and Tadanori Teruya: High-Speed Software Implementation of the Optimal Ate Pairing over Barreto-Naehrig Curves. Pairing 2010, Vol. 6487 in Lecture Notes in Computer Science, pp 21-39.

13. Iván Cabrera Altamirano and Francisco Rodríguez-Henríquez: A Scalable Intelligent Room Based on Wireless Sensor Networks and RFIDs, IEEE CCE 2010, pp 434-439.

14. Cuauhtemoc Mancillas-López, Debrup Chakraborty and Francisco Rodríguez-Henríquez: On Some Weaknesses in the Disc Encryption Schemes EME and EME2. ICISS 2009: Volume 5905 in Lecture Notes in Computer Science, pp 265-279.

15. Jean-Luc Beuchat, Emmanuel López-Trejo, Luis Martínez-Ramos, Shigeo Mitsunari and Francisco Rodríguez-Henríquez: Multi-core Implementation of the Tate Pairing over Supersingular Elliptic Curves. CANS 2009: Volume 5888 in Lecture Notes in Computer Science, pp 413-432.

16. Jean-Luc Beuchat, Jérémie Detrey, Nicolas Estibals, Eiji Okamoto and Francisco Rodríguez-Henríquez: Hardware Accelerator for the Tate Pairing in Characteristic Three Based on Karatsuba-Ofman Multipliers. CHES 2009: Volume 5747 in Lecture Notes in Computer Science, pp 225-239 [**Best paper award**].

17. Jean-Luc Beuchat, Nicolas Brisebarre, Jérémie Detrey, Eiji Okamoto and Francisco Rodríguez-Henríquez: A Comparison Between Hardware Accelerators for the Modified Tate Pairing over $\mathbb{F}_{2^m}$ and $\mathbb{F}_{3^m}$, Pairing 2008: Volume 5209 in Lecture Notes in Computer Science, pp 297-315.

18. Cuauhtemoc Mancillas-López, Debrup Chakraborty and Francisco Rodríguez-Henríquez: Efficient Implementations of Some Tweakable Enciphering Schemes in Reconfigurable Hardware. INDOCRYPT 2007: Volume 4859 in Lecture Notes in Computer Science 4859, pp. 414-424.

19. Francisco Rodríguez-Henríquez, Guillermo Morales-Luna, Nazar A. Saqib and Nareli Cruz-Cortés: A Parallel Version of the Itoh-Tsujii Multiplicative Inversion Algorithm. ARC 2007: Volume 4419 in Lecture Notes in Computer Science 4419, pp 226-237.

20. Emmanuel López-Trejo, Francisco Rodríguez-Henríquez and Arturo Díaz- Pérez: An Efficient FPGA implementation of CCM Using AES, ICISC 2005: Volume 3935 Lecture Notes in Computer Science, pp. 322-334

21. Sabel Mercurio Hernández Rodríguez and Francisco Rodríguez-Henríquez: An FPGA Arithmetic Logic Unit for Computing Scalar Multiplication using the Half-and-Add Method. IEEE ReConFig05: 7 pages.

22. Mario Alberto García-Martínez, Rubén Posada-Gámez, Guillermo Morales-Luna and Francisco Rodríguez-Henríquez: FPGA Implementation of an Efficient Multiplier over Finite Fields GF(2^m). IEEE ReConFig05, 5 pages.

23. Nareli Cruz-Cortés, Francisco Rodríguez-Henríquez, Carlos A. Coello Coello: On the Optimal Computation of Finite Field Exponentiation, IBERAMIA 2004: Volume 3315 Lecture Notes in Computer Science, pp. 747-756.

24. Francisco Rodríguez-Henríquez, Carlos E. López-Peza and Miguel Ángel León-Chávez: Comparative Performance Analysis of Public-Key Cryptographic Operations in the WTLS Handshake Protocol. IEEE CIE 2004: pp 124-129.

25. Nazar A. Saqib, Francisco Rodríguez-Henríquez and Arturo Díaz-Pérez: A Parallel Architecture for Fast Computation of Elliptic Curve Scalar Multiplication over GF(2^m). IEEE RAW 2004: pp. 144-154.

26. Nazar A. Saqib, Francisco Rodríguez-Henríquez and Arturo Díaz-Pérez: Two Approaches for a Single-Chip FPGA Implementation of an Encryptor/Decryptor AES Core. FPL 2003: Volume 2778 in Lecture Notes in Computer Science 2778, pp. 303-312.

27. Francisco Rodríguez-Henríquez and Çetin K. Koç: On fully parallel Karatsuba Multipliers for GF(2^m). CST 2003, pp. 405-410.

Selected invited talks and seminars

1. Francisco Rodríguez-Henríquez: Computing Discrete Logarithms in $\mathbb{F}_{3^{6*137}}$ and $\mathbb{F}_{3^{6*163}}$ Using Magma, keynote speaker at the Arithmetic of Finite Fields - 5th International Workshop, WAIFI 2014, Gebze, Turkey, September 27, 2014.

2. Francisco Rodríguez-Henríquez: Implementing pairing-based protocols, keynote speaker at the 6th International Conference on Pairing-Based Cryptography (Pairing 2013), Beijing, China, November 23 2013.

3. Francisco Rodríguez-Henríquez: On the complexity of computing discrete logarithms in the field GF($3^{6\cdot 509}$), Worcester Polytechnic Institute (WPI), Worcester, EUA, September 17 2013.

4. Francisco Rodríguez-Henríquez: Weakness of GF($3^{6\cdot 509}$) for Discrete Logarithm Cryptography, Crypto 2013 rump session, Santa Barbara, EUA, August 20 2013.

5. Francisco Rodríguez-Henríquez: Hardware design of cryptographic algorithms. The 13th International Conference on Cryptology (Indocrypt 2012), 9 December 2012 Kolkata, India.

6. Francisco Rodríguez-Henríquez: Introduction to Elliptic Curve Cryptography (Part II) Aspectos de Implementación — Implementation Aspects, Workshop on Elliptic curve cryptography ECC 2012, Querétaro, México, October 2013.

7. Francisco Rodríguez-Henríquez: Hardware Implementation of Pairings. Invited Speaker In The Säo Paulo Advanced School of Cryptography SP-ASCrypto 2011, University of Campinas, Brazil, October 20-26, 2011.

8. Francisco Rodríguez-Henríquez: Multicore Implementation of two public-key cryptographic algorithms. Universidad de Puerto Rico, San Juan, February 2011.

9. Francisco Rodríguez-Henríquez: Faster Implementation of Pairings. Invited Speaker In Workshop on Elliptic Curves and Computation ECC 2010, Microsoft Research in Redmond, Washington, USA Oct 18, 2010.

10. Jorge González-Díaz and Francisco Rodríguez-Henríquez: Leakage-resilient cryptographers in the Latincrypt-model. Rump Session of Crypto2010, Santa Brbara California, August 2010.

11. Francisco Rodríguez-Henríquez: 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.

12. Francisco Rodríguez-Henríquez: Software and Hardware Implementations of the Tate pairing over Supersingular Elliptic Curves. Universidad de Puerto Rico, San Juan, February 5 2010.

13. Francisco Rodríguez-Henríquez: Information Security Managment. Universidad del Turabo, Puerto Rico, February 1-5 2010.

14. Francisco Rodríguez-Henríquez: Alice's Adventures in Cryptoland. Keynote speech at 19th Internacional Conference on Electronics Communications and Computers (Conielecomp 2009), Cholula, México, February 27 2009.

15. Francisco Rodríguez-Henríquez: 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.

16. Francisco Rodríguez-Henríquez: Inverse Frobenius and Frobenius Operador Computation over GF(p^m). Laboratoire de l'Informatique du Parallélisme at the École Normale Supérieure de Lyon, November 26 2008.

17. Francisco Rodríguez-Henríquez: Security Applications. Jiangsu University, Zhenjiang, China, December 13 2007.

18. Francisco Rodríguez-Henríquez: Research and Development of Digital Identity Technology. Southeast University, Nanjing, China, December 9 2007.

19. Francisco Rodríguez-Henríquez: Design of Subquadratic field multipliers over fields of characteristic 3. University of Tsukuba, Tsukuba, Japan, October 3 2007.

20. Francisco Rodríguez-Henríquez: Parallel Formulations of Scalar Multiplication on Koblitz Curves, Universidade Estadual de Campinas - UNICAMP, Instituto de Computacao - IC. Campinas, Säo Paulo, Brazil, March 2007.

21. Francisco Rodríguez-Henríquez: Low complexity bit-parallel square root computation over GF(2^m) for all trinomials and its applications to cryptography, Centre for Applied Cryptographic Research (CACR), University of Waterloo, Canada, July 2006.

22. Francisco Rodríguez-Henríquez: Some Comments on Efficient Hardware/software Implementations of Rijndael: the New Advanced Encryption Standard (AES). University of Puebla, Puebla, October 2002.

23. Francisco Rodríguez-Henríquez: Invited talk in Information Security Lab (ISL) at Oregon State University, Corvallis, Oregon, September 2002.

24. Francisco Rodríguez-Henríquez: Modern Cryptography and its applications: An Introduction, X International Conference On Electronics, Communications & Computers (CONIELECOMP), UDLAP, Puebla, February 2000.

Editorial work

1. Co-editor of the Volume: Ferruh Özbudak and Francisco Rodríguez-Henríquez (Eds.): 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.

2. Associate Editor of the following Journals: IEEE Transactions on Computers, Journal of Universal Computer Science, Journal of Cryptographic Engineering.

3. Committee Member in the following International Conferences: SAC'2103, CANS'2013, LightSec'2013, ECC'2013, ARC'2103, ECC'2012, Pairing'2012, LatinCrypt'2012, ARC'2012, WAIFI 2010, CHES'2011, LightSec'2011, ECC'2011, WAIFI 2010, EUROISI'2008, ISCIS'2007, ISCIS'2006.

Graduate student supervision

Current graduate students under supervision

1. Thomaz Oliveira. PhD student January 2012-present
2. Gora Adj. PhD student September 2012-present
3. Armando Faz-Hernández. PhD student January 2013-present

Ph.D students supervised

1. Dr. Nazar Abbas Saqib. Thesis title: Efficient Implementation of Cryptographic Algorithms on Reconfigurable Hardware Devices, Computer Science Department CINVESTAV-IPN, September 2004. Supervisors: Arturo Díaz-Pérez and Francisco Rodríguez-Henríquez.
2. Dr. María de Lourdes López-García. Thesis title: Diseño de un protocolo para votaciones electrónicas basado en firmas a ciegas definidas sobre emparejamientos bilineales, Computer Science Department CINVESTAV-IPN, June 2011. Supervisor: Francisco Rodríguez-Henríquez.

Post-doctoral fellows

1. Luis Julián Domínguez Pérez, February 2012-August 2012

Master students supervised

1. M. Sc. Rogelio Vargas-Márquez, CINVESTAV-IPN, December 2013.
2. M. Sc. José Eduardo Ochoa-Jiménez CINVESTAV-IPN, December 2013.
3. M. Sc. Ana Helena Sánchez Ramírez, CINVESTAV-IPN, October 2012.
4. M. Sc. Gora Adj, Université de Lyon-1, July 2012.
5. M. Sc. Cuauhtémoc Chávez Corona, CINVESTAV-IPN, July 2012 [co-supervisor: Dr. Debrup Chakraborty].
6. M. Sc. Armando Faz Hernández, CINVESTAV-IPN, February 2012 [co-supervisor: Dr. Debrup Chakraborty].
7. M. Sc. Eric Zavattoni, Université de Lyon-1, February 2012.
8. M. Sc. Laura Fuentes Castañeda, CINVESTAV-IPN, December 2011.
9. M. Sc. Jonathan Taverne, Université de Lyon-1, September 2011.
10. M. Sc. Iván Cabrera Altamirano, CINVESTAV-IPN, December 2010.
11. M. Sc. Jorge Enrique González Díaz, CINVESTAV-IPN, September 2010.
12. M. Sc. Jesús Francisco Quintanar Villareal, CINVESTAV-IPN, August 2010.
13. M. Sc. Gabriel Labrada Hernández, CINVESTAV-IPN, February 2010.
14. M. Sc. Nidia Asunción Cortez Duarte, CINVESTAV-IPN, August 2009.
15. M. Sc. Luis Martínez Ramos, CINVESTAV-IPN, December 2008.
16. M. Sc. Vladimir González García, LANIA, August 2007 [Co-supervisor: Dr. Nareli Cruz Cortés].
17. M. Sc. María de Lourdes López García, BUAP, February 2007 [Co-supervisor: Dr. Miguel Ángel León Chávez].
18. M. Sc. Verónica Edith Bautista López, BUAP, February 2007 [Co-supervisor: Dr. Miguel Ángel León Chávez].

19. M. Sc. Óscar Irineo Fuentes, CINVESTAV-IPN, December 2006 [Co-supervisor: Dr. Nareli Cruz Cortés].
20. M. Sc. Sabel Mercurio Hernández Rodríguez, CINVESTAV-IPN, February 2006.
21. M. Sc. Efrén Clemente Cuervo, CINVESTAV-IPN, November 2005.
22. M. Sc. Juan Manuel Cruz Alcaraz, CINVESTAV-IPN, November 2005.
23. M. Sc. Claudia Patricia García Zamora, CINVESTAV-IPN, September 2005.
24. M. Sc. Emmanuel López Trejo, CINVESTAV-IPN, September 2005.
25. M. Sc. Guillermo Martínez Silva, ITESM, July 2005.
26. M. Sc. Carlos Eduardo López Peza, CINVESTAV-IPN, Abril 2005.
27. M. Sc. Laura Itzelt Reyes Montiel, CINVESTAV-IPN, January 2004.

Research grants

1. SEP-CONACyT, Basic Science project 2013-2016: Análisis, estudio y desarrollo de criptografía post-cuántica, $110,000 USD.
2. University of California and CONACyT, proyect UCMEXUS 2010: Pairing-based cryptography with applications to information security, $25,000 USD.
3. CONACyT, Basic Science project 2008: 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.
4. SEP-CONACyT, Basic Science project 2006-2009: Diseño e Implementación de Algoritmos Criptográficos en Hardware Reconfigurable Usando Heurísticas Evolutivas, $45,000 USD.