JESÚS JAVIER CHI DOMÍNGUEZ

Ph.D. degree

jesus.dominguez@tii.ae | Abu Dhabi, UAE | jjchidguez.github.io | 0000-0002-9753-7263
pqc-ryde.org/ | pqc-mirath.org/

EXPERIENCE

Senior Cryptographer Post Quantum

Cryptography Research Center, Technology Innovation Institute

May 2021 – Ongoing | Abu Dhabi, UAE

- My research centers on the cryptanalysis and constant-time C-code implementations of elliptic-curve and isogeny-based cryptographic protocols, where constant-time means its running-time is independent (or it does depend on randomness non-correlated) from its input. My current research also includes code-based and lattice-based cryptography. Additionally, I am participating in the NIST competition for "Post-Quantum Cryptography: Digital Signature Schemes (Round 2 Additional Signatures)" as a collaborator of the Mirath and RYDE submissions.

Postdoctoral Research Fellow

Faculty of Information Technology and Communication Sciences of Tampere University

February 2020 – April 2021 | Tampere, Finland

- Advised by Prof. Dr. Billy Bob Brumley
- Focused on the (mathematical and probabilistic) study of side-channel analysis applied to both existing and emerging cryptosystems

Research stay

Department of Computer Science and Engineering of Sabanci Univerisity

May 2015 – July 2015 | Istanbul, Turkey

- Under the guidance of Prof. Dr. Erkay Savas and Dr. Osmanbey Uzunkol
- Centered on the cryptanalysis of binary elliptic curves: gGHS Weil descent attack

PUBLICATIONS

Journal Articles

- Bidoux, L., Chi-Domínguez, J., Feneuil, T., Gaborit, P., Joux, A., Rivain, M., & Vinçotte, A. (2025). RYDE: a digital signature scheme based on rank syndrome decoding problem with mpc-in-the-head paradigm. *Des. Codes Cryptogr.*, *93*(5), 1451–1486. doi:10.1007/S10623-024-01544-1
- Budroni, A., Chi-Domínguez, J., & Franch, E. (2025). Don't use it twice: Reloaded! on the lattice isomorphism group action. *IACR Commun. Cryptol.*, *2*(2), 9. doi:10.62056/AY76CHDJ
- Chi-Domínguez, J., Ochoa-Jimenez, E., & Pontaza-Rodas, R.-N. (2025). Let us walk on the 3-isogeny graph: Efficient, fast, and simple. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, *2025*(4), 644–666. doi:10.46586/tches.v2025.i4.644-666
- Campos, F., Chávez-Saab, J., Chi-Domínguez, J., Meyer, M., Reijnders, K., Rodríguez-Henríquez, F., … Wiggers, T. (2024). Optimizations and practicality of high-security CSIDH. *IACR Commun. Cryptol.*, *1*(1), 5. doi:10.62056/ANJBKSDJA

ABOUT ME

"I am a mathematician cryptographer who loves programming and learning new topics related to my research lines"

INTERESTS

Public-key cryptography | Cryptanalysis | Post-quantum cryptography | Isogenies | Rank-metric | Elliptic curves

SKILLS

Cryptanalysis | C-code programming | Git | Python-code programming | Magma-code programming | LaTeX

LANGUAGES

Spanish
English

EDUCATION

Ph.D. in Computer Science

Computer Science Department, Cinvestav - IPN

2016 – 2019 | Mexico City, Mexico

- Advisor: Dr. Francisco Rodríguez-Henríquez
- Thesis: Elliptic curves in classical and post-quantum cryptography

M.S. in Computer Science

Computer Science Department, Cinvestav - IPN

2013 – 2015 | Mexico City, Mexico

- Advisor: Dr. Francisco Rodríguez-Henríquez
- Thesis: The gGHS attack applied on Galbraith-Lin-Scott curves

B.S. in Mathematics

Faculty of Mathematics, Autonomous University of Yucatán

2009 – 2013 | Yucatán, Mexico

- Degree obtained by general grade point average modality

- Adj, G., Chi-Domínguez, J., & Rodríguez-Henríquez, F. (2023). Karatsuba-based square-root Vélu's formulas applied to two isogeny-based protocols. *J. Cryptogr. Eng.*, *13*(1), 89–106. doi:10.1007/s13389-022-00293-y
- Chávez-Saab, J., Chi-Domínguez, J., Jaques, S., & Rodríguez-Henríquez, F. (2022). The SQALE of CSIDH: sublinear Vélu quantum-resistant isogeny action with low exponents. *J. Cryptogr. Eng.*, *12*(3), 349–368. doi:10.1007/s13389-021-00271-w
- Chi-Domínguez, J., & Rodríguez-Henríquez, F. (2022). Optimal strategies for CSIDH. *Adv. Math. Commun.*, *16*(2), 383–411. doi:10.3934/amc.2020116
- Chi-Domínguez, J., Rodríguez-Henríquez, F., & Smith, B. (2021). Extending the GLS endomorphism to speed up GHS Weil descent using Magma. *Finite Fields Their Appl.*, *75*, 101891. doi:10.1016/j.ffa.2021.101891

Conference Proceedings

- Bencina, B., Budroni, A., Chi-Domínguez, J., & Kulkarni, M. (2024). Properties of lattice isomorphism as a cryptographic group action. In M. O. Saarinen & D. Smith-Tone (Eds.), *Post-quantum cryptography - 15th international workshop, pqcrypto 2024, oxford, uk, june 12-14, 2024, proceedings, part I* (Vol. 14771, pp. 170–201). doi:10.1007/978-3-031-62743-9_6
- Budroni, A., Chi-Domínguez, J., D'Alconzo, G., Scala, A. J. D., & Kulkarni, M. (2024). Don't Use it Twice! Solving Relaxed Linear Equivalence Problems. In K.-M. Chung & Y. Sasaki (Eds.), *Advances in cryptology - ASIACRYPT 2025 - 30th international conference on the theory and application of cryptology and information security, singapore, december 9-13, 2024, proceedings, part I* (Vol. 15491, pp. 35–65). Springer. Retrieved from https://doi.org/10.1007/978-981-96-0944-4_2
- Chi-Domínguez, J., Esser, A., Kunzweiler, S., & May, A. (2023). Low memory attacks on small key CSIDH. In M. Tibouchi & X. Wang (Eds.), *Applied cryptography and network security - 21st international conference, ACNS 2023, kyoto, japan, june 19-22, 2023, proceedings, part II* (Vol. 13906, pp. 276–304). doi:10.1007/978-3-031-33491-7_11
- Bellini, E., Chávez-Saab, J., Chi-Domínguez, J., Esser, A., Ionica, S., Rivera-Zamarripa, L., … Zweydinger, F. (2022). Parallel Isogeny Path Finding with Limited Memory. In T. Isobe & S. Sarkar (Eds.), *Progress in cryptology – indocrypt 2022* (Vol. 13774, pp. 294–316). doi:10.1007/978-3-031-22912-1_13
- Chi-Domínguez, J., & Reijnders, K. (2022). Fully Projective Radical Isogenies in Constant-Time. In S. D. Galbraith (Ed.), *Topics in cryptology - CT-RSA 2022 - cryptographers' track at the RSA conference 2022, virtual event, march 1-2, 2022, proceedings* (Vol. 13161, pp. 73–95). doi:10.1007/978-3-030-95312-6_4
- Sedlacek, V., Chi-Domínguez, J., Jancar, J., & Brumley, B. B. (2021). A Formula for Disaster: A Unified Approach to Elliptic Curve Special-Point-Based Attacks. In M. Tibouchi & H. Wang (Eds.), *Advances in cryptology - ASIACRYPT 2021 - 27th international conference on the theory and application of cryptology and information security, singapore, december 6-10, 2021, proceedings, part I* (Vol. 13090, pp. 130–159). doi:10.1007/978-3-030-92062-3_5
- Belyavsky, D., Brumley, B. B., Chi-Domínguez, J., Rivera-Zamarripa, L., & Ustinov, I. (2020). Set It and Forget It! Turnkey ECC for Instant Integration. In *ACSAC '20: Annual computer security applications conference, virtual event / austin, tx, usa, 7-11 december, 2020* (pp. 760–771). doi:10.1145/3427228.3427291

GIVEN TALKS

Let us walk on the 3-isogeny graph: efficient, fast, and simple

CHES 2025

2025 — Kuala Lumpur, Malaysia

Don't Use it Twice! Solving Relaxed Linear Equivalence Problems

ASIACRYPT 2024

2024 — Kolkata, India

Low Memory Attacks on Small Key CSIDH

ACNS 2023

2023 — Kyoto, Japan

A quick journey on what SI[DH/KE] is

ASCRYPTO 2021

2021 — Virtual

Stronger and Faster Side-Channel Protections for CSIDH

LATINCRYPT 2019

2019 — Santiago de Chile

On the cost of computing isogenies between supersingular elliptic curves

SAC 2018

2018 — Calgary, Canada

Attacking a Binary GLS Elliptic Curve with Magma

LATINCRYPT 2015

2015 — Guadalajara, Mexico

- ul Hassan, S., Gridin, I., Delgado-Lozano, I. M., García, C. P., Chi-Domínguez, J., Aldaya, A. C., & Brumley, B. B. (2020). Déjà Vu: Side-Channel Analysis of Mozilla's NSS. In J. Ligatti, X. Ou, J. Katz, & G. Vigna (Eds.), *CCS '20: 2020 ACM SIGSAC conference on computer and communications security, virtual event, usa, november 9-13, 2020* (pp. 1887–1902). doi:10.1145/3372297.3421761
- Cervantes-Vázquez, D., Chenu, M., Chi-Domínguez, J., Feo, L. D., Rodríguez-Henríquez, F., & Smith, B. (2019). Stronger and Faster Side-Channel Protections for CSIDH. In P. Schwabe & N. Thériault (Eds.), *Progress in cryptology - LATINCRYPT 2019 - 6th international conference on cryptology and information security in latin america, santiago de chile, chile, october 2-4, 2019, proceedings* (Vol. 11774, pp. 173–193). doi:10.1007/978-3-030-30530-7_9
- Adj, G., Cervantes-Vázquez, D., Chi-Domínguez, J., Menezes, A., & Rodríguez-Henríquez, F. (2018). On the Cost of Computing Isogenies Between Supersingular Elliptic Curves. In C. Cid & M. J. J. Jr. (Eds.), *Selected areas in cryptography - SAC 2018 - 25th international conference, calgary, ab, canada, august 15-17, 2018, revised selected papers* (Vol. 11349, pp. 322–343). doi:10.1007/978-3-030-10970-7_15
- Chi, J., & Oliveira, T. (2015). Attacking a Binary GLS Elliptic Curve with Magma. In K. E. Lauter & F. Rodríguez-Henríquez (Eds.), *Progress in cryptology - LATINCRYPT 2015 - 4th international conference on cryptology and information security in latin america, guadalajara, mexico, august 23-26, 2015, proceedings* (Vol. 9230, pp. 308–326). doi:10.1007/978-3-319-22174-8_17