



# JESÚS JAVIER CHI DOMÍNGUEZ

Ph.D. degree

@ jesus.dominguez@tii.ae  
ID 0000-0002-9753-7263

📍 Abu Dhabi, UAE

🌐 jjchidguez.github.io

🐦 @jjchidguez

## EXPERIENCE

- Senior Cryptographer Post Quantum  
**Cryptography Research Centre, 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.

- 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 Sabancı University**  
📅 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

- 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

- Chi-Domínguez, J., & Reijnders, K. (2022). Fully projective radical isogenies in constant-time. In S. D. Galbraith (Ed.), *Topics in cryptography - 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

## 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

- 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
- 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

## GIVEN TALKS

---

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