



# Jesús Javier Chi Domínguez

Ph.D. degree

- 26 January 1992
- Tampere, Finland
- +52 1 55 3576 1747
- jjchidguez.github.io
- chidoys@gmail.com

## About me

I feel comfortable learning about another computer science (and mathematical) topics different from mine. I display great curiosity and attempts to fit my diverse experiences into a clear understanding of the world.

## Skills

Cryptanalysis



Analysis and design of algorithms



C-code programming



Python-code programming



Magma-code programming



Shell script-code programming



C-code programming★5.0  
Analysis and design of algorithms★4.5

(\*)[The skill scale is from 0 (Fundamental Awareness) to 6 (Expert).]

## Interests

Public-key and post-quantum cryptography, cryptanalysis, elliptic-curve, and isogeny-based cryptography; C and Python -code software development

## Education

- 2016-2019 Computer Science Department, Center for Research and Advanced Studies of the National Polytechnic Institute of Mexico (Cinvestav - IPN)  
Ph.D. degree on Computer Science.  
Thesis: Elliptic curves in classical and post-quantum cryptography.  
Advisor: Dr. Francisco José Rambó Rodríguez Henríquez.
- 2013-2015 Computer Science Department, Center for Research and Advanced Studies of the National Polytechnic Institute of Mexico (Cinvestav - IPN)  
Master's degree on Computer Science.  
Thesis: The gGHS attack applied on Galbraith-Lin-Scott curves.  
Advisor: Dr. Francisco José Rambó Rodríguez Henríquez.
- 2009-2013 Faculty of Mathematics, Autonomous University of Yucatán (FMAT - UADY)  
Bachelor's degree on Mathematics  
Degree obtained by general grade point average modality

## Publications

- 2020 D. Belyavsky, B. Brumley, J.-J. Chi-Domínguez, L. Rivera-Zamarripa, I. Ustinov,  
*Set It and Forget It! Turnkey ECC for Instant Integration*, Annual Computer Security Applications Conference - ACSAC 2020, ACM (2020), 760-771
- 2020 J.-J. Chi-Domínguez, F. Rodríguez-Henríquez,  
*Optimal strategies for CSIDH*, Advances in Mathematics of Communications, 2020, doi: 10.3934/amc.2020116
- 2020 S. ul Hassan, I. Gridin, I. Delgado-Lozano, C. Pereida García, J.-J. Chi-Domínguez, A. Cabrera Aldaya, and B. Brumley,  
*Déjà Vu: Side-Channel Analysis of Mozilla’s NSS*, Conference on Computer and Communications Security - CCS 2020, ACM (2020), 1887-1902.
- 2019 D. Cervantes-Vázquez, M. Chenu, J.-J. Chi-Domínguez, L. De Feo, F. Rodríguez-Henríquez, and B. Smith,  
*Stronger and Faster Side-Channel Protections for CSIDH*, Progress in Cryptology - LATINCRYPT 2019, LNCS 11774 (2019), 173-193.
- 2018 G. Adj, D. Cervantes-Vázquez, J.-J. Chi-Domínguez, A. Menezes, and F. Rodríguez-Henríquez,  
*On the cost of computing isogenies between supersingular elliptic curves*, Selected Areas in Cryptography - SAC 2018. LNCS 11349 (2018), 322-343.
- 2015 J.-J. Chi and T. Oliveira,  
*Attacking a Binary GLS Elliptic Curve with Magma*, Progress in Cryptology - LATINCRYPT 2015. LNCS 9230 (2015), 308-326.

## Experience

- 2020 Postdoctoral Research Fellow at the Faculty of Information Technology and Communication Sciences of Tampere University, Finland. Under the guidance of Prof. Billy Bob Brumley. Since February 12.
- 2015 Research stay at the Department of Computer Science and Engineering of Sabancı University, Turkey. Advised by Prof. Dr. Erkay Savas and Dr. Osmanbey Uzunkol (April 27 to July 13)