Jesús Javier Chi Domínguez

Ph.D. degree

26 January 1992

Abu Dhabi, UAE

+971 58 900 7196,
+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. In summary, I am a mathematician cryptographer whom loves programming.

Skills

Cryptanalysis

Analysis and design of algorithms

C-code programming

Python-code programming

Magma-code programming

Bash & Shell-script programming

Git

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

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

Current work

Working at the Cryptography Research Centre (CRC) of the Technology Innovation Institute (TII), Abu Dhabi, UAE. I'm currently focusing on the (math- ematical and probabilistic) study of side-channel analysis applied to both existing and emerging cryptosystems. Additionally, I am also collaborating in the crypt- analysis and secure C-code implementations of elliptic-curve and isogeny-based cryptographic protocols.

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

Conferences

2022 J.-J. Chi-Domínguez, K. Reijnders,
Fully Projective Radical Isogenies in Constant-Time, Topics in Cryptology – CT-RSA 2022, LNCS 13161 (2022), 73–95.

2021 V. Sedlacek, J.-J. Chi-Domínguez, J. Jancar, B. B. Brumley,
A Formula for Disaster: A Unified Approach to Elliptic Curve Special-Point-Based Attack, Advances in Cryptology - ASIACRYPT 2021, LNCS 13090 (2021), 130–159.

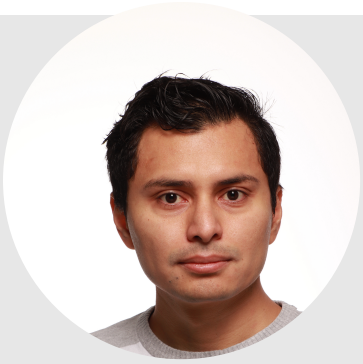
2020 D. Belyavsky, B. B. Brumley, J.-J. Chi-Domínguez, L. Rivera-Zamarripa, I. Ustinov,
Set It and Forget It! Turnkey ECC for Instant Integration, Annual Computer Security Applications Conference - ACSAC 2020, ACM (2020), 760-771.

2020 S. ul Hassan, I. Gridin, I. Delgado-Lozano, C. Pereida García, J.-J. Chi-Domínguez, A. Cabrera Aldaya, and B. 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.



Jesús Javier Chi Domínguez

Ph.D. degree

26 January 1992

Abu Dhabi, UAE

+971 58 900 7196,
+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. In summary, I am a mathematician cryptographer whom loves programming.

Skills

- Cryptanalysis
- Analysis and design of algorithms
- C-code programming
- Python-code programming
- Magma-code programming
- Bash & Shell-script programming
- Git

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

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

Journals

2021 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, Journal of Cryptographic Engineering, (2021), doi: https://doi.org/10.1007/s13389-021-00271-w

2021 J.-J. Chi-Domínguez, F. Rodriíguez-Henriquez, B. Smith
Extending the GLS endomorphism to speed up GHS Weil descent using Magma, Finite Fields and Their Applications, 75 (2021), doi: https://doi.org/10.1016/j.ffa.2021.101891

2020 J.-J. Chi-Domínguez, F. Rodríguez-Henríquez,
Optimal strategies for CSIDH, Advances in Mathematics of Communications, 2020, doi: 10.3934/amc.2020116

Given talks

2021 Summer School name: ASCRYPTO 2021. Talk given: *A quick journey on what SI[DH/KE] is*

2019 Conference name: LATINCRYPT 2019. Paper presented: *Stronger and Faster Side-Channel Protections for CSIDH*

2018 Conference name: SAC 2018. Paper presented: *On the cost of computing isogenies between supersingular elliptic curves*

2015 Conference name: LATINCRYPT 2015. Paper presented: *Attacking a Binary GLS Elliptic Curve with Magma*

Experience

2020-2021 Postdoctoral Research Fellow at the Faculty of Information Technology and Communication Sciences of Tampere University, Finland. Advised by Prof. Dr. Billy Bob Brumley. From 13/02/2020 to 30/04/2021.

2015 Research stay at the Department of Computer Science and Engineering of Sabanci Univerisity, Turkey. Under the guidance of Prof. Dr. Erkay Savas and Dr. Osmanbey Uzunkol. From April to July.

Other information

I was part of the PC members in the 7th International Conference on Cryptology and Information Security in Latin America – LATINCRYPT 2021, Bogota, Colombia.