Daniel Escudero

Curriculum Vitae

Current Position

Sep. 2021 – Present **Research Scientist**, *JP Morgan AI Research*, New York, USA.

Education

May. 2017 – Aug. 2021 **PhD in Computer Science**, *Aarhus University*, Aarhus, Denmark.

May. 2017 – Apr. 2019 **Master in Mathematics**, *Aarhus University*, Aarhus, Denmark.

Jan. 2017 – Dec. 2018 **Master in Mathematics**, *Universidad Nacional de Colombia*, Medellín, Colombia.

Aug. 2012 – Dec. 2016 **Bachelor in Mathematics**, *Universidad Nacional de Colombia*, Medellín, Colombia.

Short Duration Courses

Jun. 2019 **2nd Summer School on Cryptology Crypto-CO**, *Medellín*, Colombia.

Feb. 2019 **Winter School on Zero Knowledge**, *Bar Ilan University*, Israel.

Jul. 2017 **Summer School on Post-Quantum Cryptography**, *Eindhoven*, The Netherlands.

Sep. 2016 **Cryptography**, *Online course offered by University of Maryland, College Park*, Coursera.

Jul. 2016 **1st Summer School on Cryptology Crypto-CO**, *Bogotá*, Colombia.

May 2016 **Usable security**, *Online course offered by University of Maryland, College Park*, Coursera.

Oct. 2015 **Summer School on Mathematical and Practical Aspects of Fully Homomorphic Encryption and Multi-Linear Maps**, *Paris*, France.

May 2015 **Encuentro Colombiano de Computación Cuántica**, *Bogotá*, Colombia.

Sep. 2014 **Cryptography 1**, *Online course offered by Stanford university*, Coursera.

Theses

PhD Thesis (Aarhus University, Aug. 2021)

Title *Secure Multiparty Computation over* $Z/2^kZ$

Supervisors Ivan Damgård and Peter Scholl

Master Thesis (UNAL, Feb. 2019)

Title *Cubic Multivariate Cryptosystems Based on the Big-Field Idea and Their Vulnerability to a Min-Rank Attack*

Supervisor Daniel Cabarcas Jaramillo

Bachelor Thesis (UNAL, Dec. 2016)

Title *Groebner Bases and Applications to the Security of Multivariate Public Key Cryptosystems*

Supervisor Daniel Cabarcas Jaramillo

Previous Experience

Teaching

Aug. 2020 – Present **Teaching assistant**, *Aarhus University*, Aarhus, Denmark.
Teaching assistant in Machine Learning

Jul. 2020 **Invited lecturer**, *Shanghai Jiao Tong University*, Shanghai, China.
Crash Course on Secure Multiparty Computation

Jan. 2020 – May 2020 **Teaching assistant**, *Aarhus University*, Aarhus, Denmark.
Teaching assistant in Computer Architecture, Operating Systems and Networks

Jan. 2019 – May 2019 **Teaching assistant**, *Aarhus University*, Aarhus, Denmark.
Teaching assistant in Computer Architecture, Operating Systems and Networks

Aug. 2018 – Dec. 2018 **Teaching assistant**, *Aarhus University*, Aarhus, Denmark.
Teaching assistant in Distributed Systems and Security

Feb. 2018 – Jun. 2018 **Teaching assistant**, *Aarhus University*, Aarhus, Denmark.
Teaching assistant in Computability and Logic

Feb. 2016 – May. 2019 **Virtual tutor**, *Tutor.com*, USA.
Virtual tutor in Calculus, Linear Algebra, Finite Mathematics and Discrete Mathematics

Aug. 2017 – Dec. 2017 **Teaching assistant**, *Aarhus University*, Aarhus, Denmark.
Teaching assistant in Machine Learning

Aug. 2016 – Dec. 2016 **Teaching assistant**, *Universidad Nacional de Colombia*, Medellín, Colombia.
Teaching assistant in Vector and Analytic Geometry

Aug. 2014 – Jul. 2015 **Virtual tutor Ticademia**, *Universidad Nacional de Colombia*, Medellín, Colombia.
Virtual tutor in Basic Mathematics, Ticademia virtual platform

Jan. 2014 – Jul. 2014 **Teaching assistant**, *Universidad Nacional de Colombia*, Medellín.
Teaching assistant in Linear Algebra

Visits and Internships

Aug. 2019 – Sep. 2019 **CWI**, Amsterdam, The Netherlands.
Research visit

Jun. 2019 **Visa Research**, Palo Alto, USA.
Short Research Visit

Feb. 2019 **Bar Ilan University**, Ramat Gan, Israel.
Short Research Visit

Jun. 2018 – Jul. 2018 **Bar Ilan University**, Ramat Gan, Israel.
Internship on implementation of Multiparty Computation

Apr. 2018 **CWI**, Amsterdam, The Netherlands.
Research visit

Nov. 2016 **Aarhus University**, Aarhus, Denmark.
Research visit

Oct. 2015 **Pierre and Marie Curie University**, Paris, France.
Research visit

Industry

Oct. 2019 – Dec. 2019 **External consulting**, *Alpha, Telefonica*, Barcelona, Spain.
Consultancy services on Privacy Preserving Machine Learning, Multi-Party Computation and related technologies

Jun. 2018 – Feb. 2019 **External consulting**, *OFF-THE-GRID*, New York, USA.
Consultancy services on Multi-Party Computation and related technologies

Jul. 2017 – Aug. 2017 **External consulting**, *DNI Developers*, Bogotá, Colombia.
Analysis and C# Implementation of digital signatures to provide authenticity in the project MiCertific@doDigital

Community Service

Nov. 2021 **External Reviewer**, *EC'22*.
External Reviewer for the conference Eurocrypt 2022

Aug. 2021 **Reviewer**, *TDS*.
Reviewer for the Transactions on Data Science 2021

Aug. 2021 **Reviewer**, *TCS*.
Reviewer for Theoretical Computer Science 2021

Jun. 2021 **External Reviewer**, *CCS'21*.
External Reviewer for the conference CCS 2021

Mar. 2021 **External Reviewer**, *CRYPTO'21*.
External Reviewer for the conference CRYPTO 2021

Feb. 2021 **External Reviewer**, *FC'21*.
External Reviewer for the conference Financial Cryptography 2021

Jul. 2020 **External Reviewer**, *TCC'20*.
External Reviewer for the Theory of Cryptography Conference 2020

Jun. 2020 **External Reviewer**, *AC'20*.
External Reviewer for the conference Asiacrypt 2020

Feb. 2020 **External Reviewer**, *CRYPTO'20*.
External Reviewer for the conference CRYPTO 2020

Feb. 2020 **External Reviewer**, *CCS'20*.
External Reviewer for the ACM Conference on Computer and Communications Security 2020

Feb. 2020 **External Reviewer**, *TDSC'20*.
External Reviewer for the Transactions on Dependable and Secure Computing 2020

Apr. 2019 **External Reviewer**, *IWSEC'19*.
External Reviewer for the International Workshop on Security 2019

March. 2019 **External Reviewer**, *CRYPTO'19*.
External Reviewer for the conference CRYPTO 2019

Dec. 2018 **External Reviewer**, *PQC'19*.
External Reviewer for the conference Post-Quantum Crypto 2019

Nov. 2018 **External Reviewer**, *EC'18*.
External Reviewer for the conference Eurocrypt 2018

Jun. 2018 **External Reviewer**, *BCS'18*.
External Reviewer for the conference BalkanCryptSec 2018

Nov. 2017 **External Reviewer**, *PKC'18*.
External Reviewer for the conference Public Key Cryptography 2018

Others

Aug. 2015 – Dec. 2016 **Research assistant**, *Colciencias*, Medellín, Colombia.
Research project on Multivariate Public Key Cryptography

Languages

Spanish	Native
English	Fluent
Danish	Beginner

Computer Skills

OS	Linux, Windows, MacOX	Typography	LaTeX
Scientific	Magma, SageMath	Programming	Python, C++, Java, Go

Software

corrOT **Correlated Oblivious Transfer**.
`https://github.com/deescuderoo/corrOT`

Awards

Apr. 2019 **Tesis de Maestria Laureada**, *Universidad Nacional de Colombia*, Medellín.

Apr. 2017 **Best Bachelor Thesis in Mathematics**, *Universidad Nacional de Colombia*, Medellín.

Aug. 2012 - Aug. 2016 **Best Grade Average**, *Universidad Nacional de Colombia*, Medellín.

Talks

Dec. 2021 **Improved single-round secure multiplication using regenerating codes**, *ASIACRYPT*, Virtual Conference 2021.

Nov. 2021 **Information-theoretically secure MPC against mixed dynamic adversaries**, *TCC*, Raleigh, U.S.A. (Hybrid Conference) 2021.

Oct. 2021 **Honest majority MPC with abort with minimal online communication**, *Latincrypt*, Virtual Conference 2021.

Aug. 2021 **Fantastic Four: Honest-Majority Four-Party Secure Computation With Malicious Security**, *USENIX*, Virtual Conference 2021.

Sep. 2020 **PRIMAL: A Framework for Secure Evaluation of Neural Networks**, *OpenMined Privacy Conference*, Virtual Conference 2020.

Sep. 2020 **Efficient Protocols for Oblivious Linear Function Evaluation from Ring-LWE**, *SCN 2020: 12th Conference on Security and Cryptography for Networks*, Virtual Conference.

Jun. 2020 **Efficient Protocols for Oblivious Linear Function Evaluation from Ring-LWE**, *TPMPC 2020: Theory and Practice of Multi-Party Computation Workshops*, Virtual Conference.

Jun. 2019 **New Primitives for Actively-Secure MPC over Rings with Applications to Private Machine Learning**, *TPMPC 2019: Theory and Practice of Multi-Party Computation Workshops*, Ramat Gan, Israel.

May. 2019 **New Primitives for Actively-Secure MPC over Rings with Applications to Private Machine Learning**, *IEEE Security & Privacy 2019*, San Francisco, United States.

Aug. 2018 **SPDZ2k: Efficient MPC mod 2ˆk for Dishonest Majority**, *CRYPTO 2018*, Santa Barbara, United States.

May. 2018 **SPDZ2k: Efficient MPC mod 2ˆk for Dishonest Majority**, *TPMPC 2018: Theory and Practice of Multi-Party Computation Workshops*, Aarhus, Denmark.

Apr. 2018 **Rank Analysis of Multivariate Cryptosystems**, *PQC 2018: Post-Quantum Cryptography*, Fort Lauderdale, USA.

Nov. 2017 **Secure Multiparty Computation**, *ICAMI 2017: International Conference on Applied Mathematics and Informatics*, San Andrés, Colombia.

Jul. 2016 **Algebraic attacks on MPK cryptosystems**, *Crypto-CO: Summer school on Cryptography*, Bogotá, Colombia.

Publications

Mark Abspoel, Ronald Cramer, Daniel Escudero, Ivan Damgård, and Chaoping Xing. Improved single-round secure multiplication using regenerating codes. Asiacrypt, 2021.

Ivan Damgård, Daniel Escudero, and Divya Ravi. Iinformation-theoretically secure mpc against mixed dynamic adversaries. TCC, 2021.

Diego F. Aranha, Anders Dalskov, Daniel Escudero, and Claudio Orlandi. Improved threshold signatures, proactive secret sharing, and input certification from LSS isomorphisms. Latincrypt, 2021.

Anders Dalskov and Daniel Escudero. Honest majority MPC with abort with minimal online communication. Latincrypt, 2021.

Anders Dalskov, Daniel Escudero, and Marcel Keller. Fantastic four: Honest-majority four-party secure computation with malicious security. USENIX, 2021.

Mark Abspoel, Daniel Escudero, and Nikolaj Volgushev. Secure training of decision trees with continuous attributes. PoPETs, 2021.

Mark Abspoel, Anders Dalskov, Daniel Escudero, and Ariel Nof. An efficient passive-to-active compiler for honest-majority mpc over rings. ACNS, 2021.

Carsten Baum, Daniel Escudero, Alberto Perouzo-Ulloa, Peter Scholl, and Juan Ramón Troncoso-Pastoriza. Efficient protocols for oblivious linear function evaluation from ring-lwe. SCN, 2020.

Mark Abspoel, Ronald Cramer, Ivan Damgård, Daniel Escudero, Matthieu Rambaud, Chaoping Xing, and Chen Yuan. Asymptotically good multiplicative lsss over galois rings and applications to mpc over $\mathbb{Z}/p^k\mathbb{Z}$. Asiacrypt, 2020.

Daniel Escudero, Satrajit Ghosh, Marcel Keller, Rahul Rachuri, and Peter Scholl. Improved primitives for mpc over mixed arithmetic-binary circuits. CRYPTO, 2020.

Anders P. K. Dalskov, Daniel Escudero, and Marcel Keller. Secure evaluation of quantized neural networks. PoPETs, 2020.

Mark Abspoel, Ronald Cramer, Ivan Damgård, Daniel Escudero, and Chen Yuan. Efficient information-theoretic secure multiparty computation over $\mathbb{Z}/p^k\mathbb{Z}$ via galois rings. Theory of Cryptography Conference, TCC, 2019.

I. Damgård, D. Escudero, T. Frederiksen, M. Keller, P. Scholl, and N. Volgushev. New primitives for actively-secure mpc over rings with applications to private machine learning. IEEE Symposium on Security and Privacy (SP), 2019.

Ronald Cramer, Ivan Damgård, Daniel Escudero, Peter Scholl, and Chaoping Xing. Spdz2k: Efficient MPC mod 2^k for dishonest majority. CRYPTO, 2018.

John Baena, Daniel Cabarcas, Daniel E. Escudero, Karan Khathuria, and Javier A. Verbel. Rank analysis of cubic multivariate cryptosystems. PQCrypto, 2019.

John B. Baena, Daniel Cabarcas, Daniel E. Escudero, Jaiberth Porras-Barrera, and Javier A. Verbel. Efficient zhfe key generation. PQCrypto, 2018.