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 $Z/2^k Z$*
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

Feb. 2023 – Jun. 2023 **Lecturer**, *Universidad Nacional de Colombia*, Medellín, Colombia.
Master-level course on "Advanced Topics on Cryptography". Main topics: MPC, FHE and ZKPs.

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

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

Aug. 2020 – Jan. 2021 **Teaching assistant**, *Aarhus University*, Aarhus, Denmark.
Teaching assistant in Machine Learning

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

Event Organization

Jul. 2025 **Program Co-Chair**, *LATINCRYPT 2025*, Medellín, Colombia.
9th International Conference on Cryptology and Information Security in Latin America

Oct. 2023 **Support Member**, *LATINCRYPT 2023*, Quito, Ecuador.
8th International Conference on Cryptology and Information Security in Latin America

Nov. 2022 **Co-Organizer**, *Workshop on Secure and Private Computing in AI and Finance*, New York City, USA.
Affiliated event with the 3rd ACM International Conference on AI in Finance, ICAIF'22

Community Service

Feb. 2025 **External Reviewer**, *CRYPTO'25*.
External reviewer for the conference CRYPTO 2024

Oct. 2024 **Program Committee**, *ICLR'25*.
Program committee member for the International Conference on Learning Representations 2025

Oct. 2024 **Program Committee**, *Eurocrypt'25*.
Program committee member for the conference Eurocrypt 2025

May. 2024	**Program Committee**, *Asiacrypt'24*. Program committee member for the conference Asiacrypt 2024
Mar. 2024	**Reviewer**, *ICML'24*. External reviewer for the conference ICML 2024
Feb. 2024	**External Reviewer**, *CRYPTO'24*. External reviewer for the conference CRYPTO 2024
Jan. 2024	**Program committee**, *CCS'24*. Program committee member for the conference CCS 2024
Jan. 2024	**External Reviewer**, *PKC'24*. External reviewer for the conference PKC 2024
Jan. 2024	**External Reviewer**, *S&P'24*. External reviewer for the conference S&P 2024
Oct. 2023	**Program committee**, *AsiaCCS'24*. Program committee member for the conference AsiaCCS 2024
Oct. 2023	**Program committee**, *Eurocrypt'24*. Program committee member for the conference Eurocrypt 2024 (*distinguished PC member*)
Sep. 2023	**Reviewer**, *JCS*. Reviewer for the Journal of Computer Security 2023
Sep. 2023	**Reviewer**, *TDSC*. Reviewer for the Transactions on Dependable and Secure Computing 2023
Jun. 2023	**Program committee**, *Latincrypt'23*. Program committee member for the conference Latincrypt 2023
May. 2023	**Program committee**, *CCS'23*. Program committee member for the ACM Conference on Computer and Communications Security (CCS) 2023
Mar. 2023	**Reviewer**, *JoC*. Reviewer for the Journal of Cryptology 2023
Jan. 2023	**External Reviewer**, *CRYPTO'23*. External Reviewer for the conference CRYPTO 2023
Jan. 2023	**External reviewer**, *PKC'23*. Reviewer for the conference on Public Key Cryptography (PKC) 2023
Oct. 2022	**Reviewer**, *JoC*. Reviewer for the Journal of Cryptology 2022
Oct. 2022	**External reviewer**, *PKC'22*. External reviewer for the conference on Public Key Cryptography (PKC) 2022
Jun. 2022	**Reviewer**, *TIFS*. Reviewer for the IEEE Transactions on Information Forensics & Security 2022
Jun. 2022	**External Reviewer**, *Asiacrypt*. Reviewer for the conference Asiacrypt 2022

Apr. 2022	**Program committee**, *CFAIL*. Program committee member for The Fourth Conference for Failed Approaches and Insightful Losses in Cryptology 2022
Mar. 2022	**External Reviewer**, *CRYPTO'22*. External Reviewer for the conference CRYPTO 2022
Feb. 2022	**Reviewer**, *TDSC*. Reviewer for the IEEE Transactions on Dependable and Secure Computing 2022
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

Software

TurboPack	**TurboPack: Honest Majority MPC with Constant Online Communication**. https://github.com/deescuderoo/turbopack
corrOT	**Correlated Oblivious Transfer**. https://github.com/deescuderoo/corrOT

Partial Contribution

FRN	**Fast Fully Secure Multi-Party Computation Over Any Ring with Two-Thirds Honest Majority (CCS'22)**. https://github.com/anderspkd/ccs-DEN22

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

Jan. 2024	L **for the Price of One: On the Benefits of Using more than** $t+1$ **Parties in Threshold Signing**, *JPMC AlgoCRYPT Seminars*, New York, USA.
Dec. 2024	L **for the Price of One: On the Benefits of Using more than** $t+1$ **Parties in Threshold Signing**, *Kolkata Cryptoday*, Kolkata, India.
Aug. 2024	**Sublinear Distributed Product Checks on Replicated Secret-Shared Data over Z2k without Ring Extensions**, *PPML workshop (affiliated event at CRYPTO 2024)*, Santa Barbara, USA.
Aug. 2024	**Fully Secure MPC and zk-FLIOP Over Rings: New Constructions, Improvements and Extensions**, *CRYPTO 2024*, Santa Barbara, USA.

Apr. 2024	**Multi-Verifier Zero-Knowledge Proofs for Any Constant Fraction of Corrupted Verifiers**, *Security seminar, University of Pennsylvania*, Philadelphia, USA.
Jan. 2024	**TurboPack: Honest Majority MPC with Constant Online Communication**, *TII seminar*, Abu Dhabi, UAE.
Dec. 2023	**TurboPack: Honest Majority MPC with Constant Online Communication**, *Microsoft Research*, Bangalore, India.
Oct. 2023	**On Fully-Secure Honest Majority MPC without n^2 Round Overhead**, *Latincrypt 2023*, Quito, Ecuador.
Sep. 2023	**On Fully-Secure Honest Majority MPC without n^2 Round Overhead (Invited Talk)**, *International Conference on Coding and Cryptography (ICCC) 2023*, Virtual Conference 2023.
Aug. 2023	**Panelist at Crypto meets AI - GHTC**, *Affiliated event at CRYPTO'23*, Santa Barbara (CA), United States.
Jun. 2023	**Phoenix: Secure Computation in an Unstable Network with Dropouts and Comebacks**, *ITC 2023*, Aarhus, Denmark.
Nov. 2022	**TurboPack: Honest Majority MPC with Constant Online Communication**, *NYU Crypto seminar*, New York City, United States.
Nov. 2022	**TurboPack: Honest Majority MPC with Constant Online Communication**, *CCS 2022*, Los Angeles (CA), United States.
Aug. 2022	**More Efficient Dishonest Majority Secure Computation over $\mathbb{Z}_{2^k}$ via Galois Rings**, *CRYPTO 2022*, Santa Barbara (CA), United States.
May 2022	**Fast Fully Secure Multi-Party Computation over Any Ring with Two-Thirds Honest Majority (Invited Talk)**, *International Conference on Coding and Cryptography (ICCC) 2022*, Virtual Conference 2022.
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 2^k for Dishonest Majority**, *CRYPTO 2018*, Santa Barbara, United States.
May. 2018	**SPDZ2k: Efficient MPC mod 2^k 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

1. Sofia Celi, Daniel Escudero, and Guilhem Niot. Share the mayo: thresholdizing mayo. PQ Crypto, 2025.

2. Alexander Bienstock, Daniel Escudero, and Antigoni Polychroniadou. Perfectly secure fluid mpc with abort and linear communication complexity. Communications in Cryptology, 2025.

3. Leo de Castro, Antigoni Polychroniadou, and Daniel Escudero. Privacy-preserving large language model inference via gpu-accelerated fully homomorphic encryption. Neurips Safe Generative AI Workshop, 2024.

4. Amit Agarwal, Alexander Bienstock, Ivan Damgård, and Daniel Escudero. Honest majority god mpc with $o(\text{depth}(c))$ rounds and low online communication. Asiacrypt, 2024.

5. Daniel Escudero, Yifan Song, and Wenhao Wang. Perfectly-secure multiparty computation with linear communication complexity over any modulus. Asiacrypt, 2024.

6. Yun Li, Daniel Escudero, Yufei Duan, Zhicong Huang, Cheng Hong, Chao Zhang, and Yifan Song. Sublinear distributed product checks on replicated secret-shared data over z_2^k without ring extensions. CCS, 2024.

7. Ivan Tjuawinata Daniel Escudero and Chaoping Xing. On information-theoretic secure multiparty computation with local repairability. PKC, 2024.

8. Daniel Escudero Anders Dalskov and Ariel Nof. Fully secure mpc and zk-fliop over rings: New constructions, improvements and extensions. CRYPTO, 2024.

9. Yifan Song Daniel Escudero, Antigoni Polychroniadou and Chenkai Weng. Multi-verifier zero-knowledge proofs for any constant fraction of corrupted verifiers. CCS, 2024.

10. Daniel Escudero, Hongqing Liu, Chaoping Xing, and Chen Yuan. Degree-d reverse multiplication-friendly embeddings: Constructions and applications. Asiacrypt, 2023.

11. Daniel Escudero and Serge Fehr. On fully-secure honest majority mpc without n^2 round overhead. Latincrypt, 2023.

12. Daniel Escudero, Vipul Goyal, Antigoni Polychroniadou, Yifan Song, and Chenkai Weng. SuperPack: Dishonest majority MPC with constant online communication. Eurocrypt, 2023.

13. Ivan Damgård, Daniel Escudero, and Antigoni Polychroniadou. Phoenix: Secure computation in an unstable network with dropouts and comebacks. Information Theoretic Cryptography, 2023.

14. Daniel Escudero Alexander Bienstock and Antigoni Polychroniadou. On linear communication complexity for (maximally) fluid mpc. CRYPTO, 2023.

15. Thomas Attema, Ignacio Cascudo, Ronald Cramer, Ivan Damgård, and Daniel Escudero. Vector commitments over rings and compressed sigma-protocols. TCC, 2022.

16. Daniel Escudero, Chaoping Xing, and Chen Yuan. More efficient dishonest majority secure computation over $\mathbb{Z}_{2^k}$ via galois rings. CRYPTO, 2022.

17. Anders Dalskov, Daniel Escudero, and Ariel Nof. Fast fully secure multi-party computation over any ring with two-thirds honest majority. CCS, 2022.

18. Daniel Escudero, Vipul Goyal, Antigoni Polychroniadou, and Yifan Song. TurboPack: Honest majority MPC with constant online communication. CCS, 2022.

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

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

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

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

23. Daniel Escudero and Eduardo Soria-Vazquez. Efficient information-theoretic multi-party computation over non-commutative rings. CRYPTO, 2021.

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

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

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

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

28. Carsten Baum, Daniel Escudero, Alberto Perouzo-Ulloa, Peter Scholl, and Juan Ramón Troncoso-Pastoriza. Efficient protocols for oblivious linear function evaluation from ring-lwe. Journal of Computer Security, Volume 30, 2020.

29. 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.

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

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

32. 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.

33. 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.

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

35. John Baena, Daniel Cabarcas, Daniel E. Escudero, Karan Khathuria, and Javier A. Verbel. Rank analysis of cubic multivariate cryptosystems. PQCrypto, 2018.

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