Nicholas Genise

Personal

Email: nicholasgenise@gmail.com
Website: https://ngenise.github.io

Education

Ph.D. in Electrical and Computer Engineering, UCSD (Sept. 2019)
Advisor: Professor Daniele Micciancio
Dissertation: *Gadgets and Gaussians in Lattice-Based Cryptography.*

M.S. in Electrical and Computer Engineering, UCSD (Sept. 2016).

B.S.E. in Electrical Engineering, University of Michigan, Ann Arbor (May 2013).

UM-SJTU Joint Institute, Shanghai Jiao Tong University, Shanghai (June-August 2011).

Selected Work Experience

Duality Technologies, Hoboken, NJ (January 2022-present)
Scientist.

SRI International, Menlo Park, CA (July 2020- January 2022)
Advanced Computer Scientist.

Rutgers University, New Brunswick, NJ (Sept. 2019-June 2020)
Postdoctoral Researcher in Mathematics.
Supervisor: Professor Stephen D. Miller.

Visa Research, Palo Alto, CA (June-August 2018)
Intern in Advanced Cryptography.
Supervisors: Dr. Yilei Chen and Dr. Pratyay Mukherjee.

Publications

13. "Collaborative Privacy-Preserving Analysis of Oncological Data using Multiparty Homomorphic Encryption," (with Ravit Geva, Alexander Gusev, Yuriy Polyakov, Lior Liram, Oded Rosolio, Andreea Alexandru, Marcelo Blatt, Zohar Duchin, Barliz Waissengrin, Dan Mirelman, Felix Bukstein, Deborah T. Blumenthal, Ido Wolf, Sharon Pelles, Tali Schaffer, Lee A. Lavi, Daniele Micciancio, Vinod Vaikuntanathan, Ahmad Al Badawi, and Shafi Goldwasser). *(To Appear) Proceedings of the National Academy of Sciences.*

12. "On the Hardness of Scheme-Switching Between SIMD FHE Schemes," (with Karim Eldefrawy and Nathan Manohar). *(To Appear) PQCrypto 2023.*

11. "OpenFHE: Open-Source Fully Homomorphic Encryption Library," (with Ahmad Al Badawi, Jack Bates, Flvio Bergamaschi, David Bruce Cousins, Saroja Erabelli, Shai Halevi, Hamish Hunt, Andrey Kim, Yongwoo Lee, Zeyu Liu, Daniele Micciancio, Ian Quah, Yuriy Polyakov, R. V. Saraswathy, Kurt Rohloff, Jonathan Saylor, Dmitriy Suponitsky, Matthew Triplett, Vinod Vaikuntanathan, Vincent Zucca). *WAHC 2022* eprint: https://ia.cr/2022/915

10. “CraterLake: A Hardware Accelerator for Efficient Unbounded Computation on Encrypted Data” (with Nikola Samardzic, Axel Feldman, Aleksandar Krastev, Nathan Manohar, Srinivas Devadas, Karim Eldefrawy, Chris Peikert, and Daniel Sanchez). *ISCA 2022.*
9. “On Regenerating Codes and Proactive Secret Sharing: Relationships and Implications,” (with Karim Eldefrawy, Rutuja Kshirsagar, and Moti Yung). *SSS 2021.* eprint: `https://ia.cr/2022/096`
8. “Quantum Optimization Heuristics with an Application to Knapsack Problems” (with Wim van Dam, Karim Eldefrawy, and Natalie Parham), *IEEE Quantum Week 2021.* arxiv: `https://arxiv.org/abs/2108.08805`
7. “Gadget-Based iNTRU Lattice Trapdoors” (with Baiyu Li), *Indocrypt 2020.* ePrint: `https://ia.cr/2020/1354`
6. “Improved Discrete Gaussian and Subgaussian Analysis for Lattice Cryptography” (with Daniele Micciancio, Chris Peikert, and Michael Walter), *PKC 2020.* eprint: `https://ia.cr/2020/337`
5. “Implementing Token-Based Obfuscation Under (Ring) LWE” (with Cheng Chen, Daniele Micciancio, Yuriy Polyakov, and Kurt Rohloff), *WAHC 2020.* ePrint: `https://ia.cr/2018/1222`
4. “Approximate Trapdoors for Lattices and Smaller Hash-and-Sign Signatures” (with Yilei Chen and Pratyay Mukherjee), *Asiacrypt 2019.* ePrint: `https://ia.cr/2019/1029`
3. “Homomorphic Encryption for Finite Automata” (with Craig Gentry, Shai Halevi, Baiyu Li, and Daniele Micciancio), *Asiacrypt 2019.* ePrint: `https://ia.cr/2019/176`
2. “Building an Efficient Lattice Gadget Toolkit: Subgaussian Sampling and More” (with Daniele Micciancio and Yuriy Polyakov), *Eurocrypt 2019.* ePrint: `https://ia.cr/2018/946`
1. “Faster Gaussian Sampling for Trapdoor Lattices with Arbitrary Modulus” (with Daniele Micciancio), *Eurocrypt 2018.* ePrint: `https://ia.cr/2017/308`

Manuscripts

1. “F1: A Fast and Programmable Accelerator for Fully Homomorphic Encryption” (with Axel Feldmann, Nikola Samardzic, Aleksandar Krastev, Srini Devadas, Karim Eldefrawy, Ron Dreslinski, Chris Peikert, and Daniel Sanchez).
arxiv: `https://arxiv.org/abs/2109.05371`.

Talks

- “Gadget-Based iNTRU Lattice Trapdoors” *INDOCRYPT, December 2020.*
- “Implementing Token-Based Obfuscation under (Ring)LWE” *WAHC, December 2020.*
- “Improved Discrete Gaussian and Subgaussian Analysis for Lattice Cryptography” *PKC, June 2020.*

- "Improved Discrete Gaussian and Subgaussian Analysis for Lattice Cryptography" *Simons Lattice Online Seminar, April 2020.*
- "Approximate Trapdoors for Lattices and Smaller Hash-and-Sign Signatures" *ASIACRYPT, December 2019.*
- "Building an Efficient Lattice Gadget Toolkit: Subgaussian Sampling and More" *EUROCRYPT, May 2019.*
- "Approximate Trapdoors for Lattices" *Visa Research, August 2018.*
- "Faster Gaussian Sampling for Trapdoor Lattices with Arbitrary Modulus" *Visa Research, July 2018.*
- "Faster Gaussian Sampling for Trapdoor Lattices with Arbitrary Modulus" *EUROCRYPT, May 2018.*

Professional Activities

Program committees: Inscrypt 2022

External reviewer for JoC, Designs Codes and Cryptography, TCC, Asiacrypt, Eurocrypt, PKC, CCS, CRYPTO, and PQCrypto.

Organizer, NY CryptoDay seminar, Fall 2019-Present (`https://nycryptoday.wordpress.com/`).

Mentorship

- Nathan Manohar, *Summer Intern, SRI 2021*
- Rutuja Kshirsagar, *Summer Intern, SRI 2020*

Teaching

Math 354: Linear Optimization (Fall 2020), Guest Lecturer, Rutgers University, New Brunswick.

CSE 105: Theory of Computation (Fall 2017), Teaching Assistant, UCSD.

CSE 20: Discrete Mathematics (Spring 2017, Winter 2017, Winter 2015), Teaching Assistant, UCSD.

CSE 21: Mathematics for Algorithms and Systems Analysis (Summer 2017), Teaching Assistant, UCSD.

ECE 15: Intro. Programming (Fall 2014), Teaching Assistant, UCSD.

EECS 215: Intro Circuits (Fall 2012, Winter 2013), Lab Instructor, University of Michigan, Ann Arbor.

Awards

Jacobs Fellowship, Jacobs School of Engineering, UCSD (September 2013-August 2016).

References

Daniele Micciancio. Email: `daniele@cs.ucsd.edu`

Yilei Chen. Email: `chenyilei.ra@gmail.com`

Shai Halevi. Email: `shaih@alum.mit.edu`

Stephen D. Miller. Email: `sdmiller@math.rutgers.edu`