

FRANCESCA FALZON

ffalzon@ethz.ch

[My Website](#)

EDUCATION

University of Chicago

Ph.D. Computer Science

Chicago, IL, USA

Oct 2018 – Jun 2023

- Thesis: "A Combinatorial Approach to Leakage Abuse Attacks and Their Mitigation"
- Advisors: Roberto Tamassia and Ben Zhao

University of Chicago

M.S. Computer Science, GPA: 3.921 / 4.0

Chicago, IL, USA

Oct 2018 – Aug 2020

- Thesis: "Full Database Reconstruction in Two Dimensions"
- Advisor: David Cash

Rutgers University

B.A. Mathematics, GPA: 3.903 / 4.0

New Brunswick, NJ, USA

Sept 2013 – May 2017

- Summa Cum Laude, Phi Beta Kappa.

RESEARCH AND PROFESSIONAL EXPERIENCE

ETH Zürich

Postdoc

Zürich, Switzerland

Jul 2023 – Present

- Conducting research relating to encrypted databases in the Applied Cryptography Group. I am hosted by Prof. Kenneth Paterson.
- Organizing cryptography-related events such as Swiss Crypto Day.
- Funded by the Swiss CYD Distinguished Postdoctoral Fellowship.

IBM Zürich

Research Intern

Zürich, Switzerland

Jul 2022 – Dec 2022

- Conducted research on Proofs of Liability in the Blockchain group under the supervision of Dr. Kaoutar Elkhiyaoui, Dr. Elli Androulaki, and Dr. Angelo De Caro.

Brown University

Visiting Ph.D. Student

Providence, RI, USA

Oct 2021 – June 2022, Jan 2023 – Jun 2023

- Worked on encrypted databases under the guidance of Prof. Roberto Tamassia.
- Designing schemes that support multi-dimensional range queries with a sliding scale of trade-offs with respect to security, storage overhead, and bandwidth.

ETH Zürich

Visiting Ph.D. Student

Zürich, Switzerland

Jun 2021 – Sept 2021

- Designed and analyzed leakage-abuse attacks on encrypted graph database schemes that support shortest path queries under the guidance of Prof. Kenneth Paterson.

University of Chicago

Graduate Research Assistant

Chicago, IL, USA

Oct 2018 – May 2021

- Designed and deployed a number of database reconstruction attacks from the leakage of range queries over multi-attribute encrypted data. These attacks include both full and approximate database reconstruction; the results can be found [here](#) and [here](#).
- Developed new dynamic encrypted multi-map (EMM) schemes that hide the number of records returned upon each query.

Rutgers University

Undergraduate Research Assistant

New Brunswick, NJ, USA

Sept 2017 – Oct 2018

- Studied collections of sets and their graph representations utilizing tools from combinatorics.
- Formalized the notion of a region graph with the goal of developing scalable, interactive graph-exploration tools.

Lehman College CUNY

REU Participant

New York, NY, USA

Sept 2016 to Oct 2017

- Sought an efficient algorithm for finding the closure of a given set of rooted triples.
- Chosen through a competitive selection process and awarded a stipend of \$5000. Supported by the NSF.

PUBLICATIONS

- **Francesca Falzon**, Kaoutar Elkhiyaoui, Yacov Manevich, Angelo De Caro. Short Privacy-Preserving Proofs of Liabilities. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*. Copenhagen, Denmark, November 2023. (To Appear)
- Evangelia Anna Markatou^{*}, **Francesca Falzon**^{*}, Zachary Espiritu, Roberto Tamassia. Attacks on Encrypted Response-Hiding Range Search Schemes in Multiple Dimensions. In *Proceedings of the 23rd Privacy Enhancing Technologies Symposium (PoPETS)*. Lausanne, Switzerland. July 2023. [[PDF](#)]

- **Francesca Falzon**^{*}, Evangelia Anna Markatou^{*}, Zachary Espiritu, Roberto Tamassia. Encrypted Range Search in Multiple Dimensions. In *Proceedings of the 49th International Conference on Very Large Data Bases (VLDB)*. Vancouver, Canada, August 2023. [PDF]
- **Francesca Falzon**, Kenneth G. Paterson. An Efficient Query Recovery Attack Against a Graph Encryption Scheme. In *European Symposium on Research in Computer Security (ESORICS)*. Copenhagen, Denmark, September 2022. [PDF]
Won the ESORICS best student paper award.
- Evangelia Anna Markatou^{*}, **Francesca Falzon**^{*}, William Schor, Roberto Tamassia. Reconstructing with Less: Leakage Abuse Attacks in Two-Dimensions. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*. Virtual, South Korea, November 2021. [PDF]
- **Francesca Falzon**^{*}, Evangelia Anna Markatou^{*}, Akshima, David Cash, Adam Rivkin, Jesse Stern, Roberto Tamassia. Full Database Reconstruction Attack in Two-Dimensions. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*. Virtual, USA, November 2020. [PDF]

PREPRINTS

- Micah Altman, Aloni Cohen, **Francesca Falzon**, Evangelia Anna Markatou, Kobbi Nissim, Michel Jose Reymond, Sidhant Saraogi, Alexandra Wood. A Principled Approach to Defining Anonymization As Applied to EU Data Protection Law. 2022. [PDF]
- Emily Wenger, **Francesca Falzon**, Josephine Passananti, Haitao Zheng, Ben Y. Zhao. Assessing Privacy Risks from Feature Vector Reconstruction Attacks. 2022. [PDF]

INVITED TALKS AND PRESENTATIONS

- *An Efficient Query Recovery Attack Against a Graph Encryption Scheme (Invited talk)*. Zürich Information Security and Privacy Center (ZISC) Seminar. Zürich, Switzerland. 30 June 2022.
- *Full Database Reconstruction in Two-Dimensions (Invited talk)*. Microsoft Research Redmond Cryptography Colloquium. Virtual, USA. 24 November 2020.
- *Multi-dimensional database reconstruction (Poster talk)*. 7th Midwest Security Workshop. Chicago, IL. April 2019.
- *On the Complexity of the Rooted Triples Problem (Oral talk)*. Special Session on Mathematical Phylogenetics, American Mathematical Society Sectional Meeting. New York, NY. May 2017.

TA EXPERIENCE

- Masters Program in Computer Science (MPCS) Algorithms, University of Chicago. Spring 2021.
- MPCS Foundations of Computational Data Analysis, University of Chicago. Winter 2021.
- MPCS Discrete Math, University of Chicago. Autumn 2020.
- MPCS Algorithms, University of Chicago. Spring 2020.
- Cryptography, University of Chicago. Autumn 2019.
- MPCS Mathematics for Computer Science and Data Analysis, University of Chicago. Winter 2019.
- Cryptography, University of Chicago. Autumn 2018.
- Discrete Mathematics High School Summer Camp, Rutgers University. Summer 2018.
- Learning Strategies & GRE Prep Academic Coach, Rutgers University. Spring 2018.
- Introduction to Proofs, Rutgers University. Spring 2017.
- Calculus II, Rutgers University. Spring 2016.

AWARDS

- Armasuisse CYD Distinguished Postdoctoral Fellowship (CHF 250,000). 2022.
- ESORICS 2022 Best Student Paper Award (EUR 500). 2022.
- Think Swiss Research Scholarship (CHF 4800). 2020.
- Armed Forces Communications and Electronics Association Ralph W. Shrader Diversity Scholarship (USD 3000). 2019.
- Rutgers University School of Arts and Sciences Excellence Scholarship (USD 1000). 2016.

VOLUNTEER AND OUTREACH

- Second Swiss Crypto Day, (*Co-Organizer*). September 2023.
- UChicago CS Ph.D. Student Socia
- ETH Zurich CS PhD Paint Night Social, (*Organizer*). November 2021.
- UChicago CS Ph.D. Student Social Events, (*Student Minister*). 2019 to 2020.
- UChicago CS Ph.D. Student Tea-time, (*Co-founder, Student Minister*). 2018 to 2019.
- CompilerHer @ UChicago: Middle School Student Outreach, (*Teacher for Computer Security Course*). April 2019.
- New Jersey Office of Homeland Security, (*Cybersecurity Analysis Intern*). January 2019 to April 2018.
- Princeton Splash: High School Student Outreach, (*Teacher for Cryptography, Intro to Mathematical Logic*). April 2018, April 2017.
- Rutgers Women in the Mathematical Sciences Club, (*Co-founder, President*). 2016 to 2017.
- Rutgers International Student Orientation, (*Volunteer Organizer*). 2015 to 2016.
- Trim Magazine: Rutgers' Student-run Fashion and Lifestyle Magazine, (*Creative Director, Editor*). 2015 to 2016.
- Permanent Mission of Malta to the United Nations, (*Advisory Intern*). 2015.

^{*} Indicates that authors contributed equally and are listed in alphabetical or reverse-alphabetical order, respectively.

SKILLS

Technical Skills Python (Libraries: NetworkX, Matplotlib)

Survey Skills Qualtrics

Spoken Languages English (Native), Maltese (Native), Italian (B1)