Zachary Espiritu

MongoDB Research, New York, NY, USA

`me@zacharyespiritu.com` `https://zacharyespiritu.com`

Research Interests

Applied cryptography, algorithms and data structures, formal methods and optimization, systems security, usable security.

Education

Sep 2017 – Dec 2021 **Brown University, Sc.M. (Concurrent Masters)** in Computer Science

Sep 2017 – Dec 2021 **Brown University, Sc.B. with Honors** in Computer Science
Honors Thesis: "Time- and Space-Efficient Aggregate Range Queries over Encrypted Databases" (Advisor: Roberto Tamassia; Reader: Vasileios Kemerlis)

Current Position

Feb 2023 – current **MongoDB Research**, New York, NY
Senior Research Engineer
Conducting research on cryptographic techniques for securing real-world databases. Serves as primary contact for all engineering teams in the company for advising on and reviewing any cryptographic deployments within the company.

Publications

⁂ *denotes papers where authors are listed alphabetically.*

1. **Z. Espiritu** ⁂, S. Kamara, T. Moataz, V. Ogier. "Leafblower: a Leakage Attack Against TEE-Based Encrypted Databases". To appear in *Proceedings of the 47th IEEE Symposium on Security and Privacy* (San Francisco, CA, USA). 2026.

2. M. George, S. Kamara, T. Moataz, **Z. Espiritu**. "Structured Encryption and Distribution-aware Leakage Suppression". To appear at *Asiacrypt 2025* (Melbourne, Australia). 2025.

3. **Z. Espiritu** ⁂, S. Kamara, T. Moataz, A. Park. "PolySys: an Algebraic Leakage Attack Engine". In *Proceedings of the 34th USENIX Security Symposium* (Seattle, WA, USA). 2025.

4. A. Agarwal, **Z. Espiritu** ⁂. "Sequentially Consistent Concurrent Encrypted Multimaps". In *Proceedings of the 10th IEEE European Symposium on Security and Privacy* (Venice, Italy). 2025.

5. **Z. Espiritu** ⁂, S. Kamara, T. Moataz. "Bayesian Leakage Analysis: A Framework for Analyzing Leakage in Cryptography". In *IACR Communications in Cryptology*, Vol. 2, Iss. 1. 2025.

6. **Z. Espiritu** ⁂, M. George, S. Kamara, L. Qin. "Synq: Public Policy Analytics Over Encrypted Data". In *Proceedings of the 45th IEEE Symposium on Security and Privacy* (San Francisco, California, USA). 2024.

7. F. Falzon, E. A. Markatou, **Z. Espiritu**, R. Tamassia. "Range Search over Encrypted Multi-Attribute Data". In *Proceedings of the VLDB Endowment*, Vol. 16, Iss. 4. (Vancouver, Canada). 2023.

8. E. A. Markatou, F. Falzon, **Z. Espiritu**, R. Tamassia. "Attacks on Encrypted Response-Hiding Range Search Schemes in Multiple Dimensions". In *Proceedings of Privacy Enhancing Technologies*, Vol. 2023, Iss. 2. (Lausanne, Switzerland). 2023.

9. **Z. Espiritu**, E. A. Markatou, R. Tamassia. "Time- and Space-Efficient Aggregate Range Queries on Encrypted Databases". In *Proceedings of Privacy Enhancing Technologies*, Vol. 2022, Iss. 4. (Sydney, Australia). 2022.

Previous Employment

Feb 2022 – Feb 2023 **D.E. Shaw & Co.**, New York, NY
Systems Security Engineer

Summer 2021 **Cloud Security Group at Brown University**, Providence, RI
Undergraduate Researcher

Summer 2020 **Google**, Remote
Software Engineering Intern, Cloud EKM (External Key Manager) and KMS (Key Management Service)

Summer 2018 **Brown PLT at Brown University**, Providence, RI
Undergraduate Researcher

Summer 2017 **Order.co (formerly Negotiatus)**, New York, NY
Software Engineering Intern

Summer 2016 **Order.co (formerly Negotiatus)**, New York, NY
Software Engineering Intern

Teaching Assistant Experience

All listed courses were taught at Brown University.

Fall 2021	CSCI 1650: Software Security and Exploitation (Head TA)
Spring 2021	CSCI 1660: Computer Systems Security (Head TA)
Fall 2020	CSCI 1730: Design and Implementation of Programming Languages (Head TA)
Spring 2020	CSCI 1660: Computer Systems Security (Head TA)

Fall 2019	CSCI 1730: Design and Implementation of Programming Languages
Spring 2019	CSCI 1660: Computer Systems Security (Head TA)
Fall 2018	CSCI 0190: Accelerated Introduction to Computer Science (Head TA)
Spring 2018	CSCI 0040: Introduction to Scientific Computing and Problem-Solving
Fall 2017	CSCI 0050: A Data-Centric Introduction to Programming

Academic Service

2026	Artifact Evaluation Committee for IEEE S&P 2026
	Artifact Evaluation Committee for PETS 2026
2025	External Reviewer for VLDB 2025
	External Reviewer for CRYPTO 2025
2024	External Reviewer for CRYPTO 2024
	External Reviewer for SRDS 2024
	External Reviewer for ACM TOPS 2024
2023	External Reviewer for ACM CCS 2023
	External Reviewer for CRYPTO 2023

Department Service

Department of Computer Science, Brown University, Providence, RI

Oct 2019 – Dec 2021 *Meta Teaching Assistant*

Coordinated hiring and training of 600+ teaching assistants each year across 50 CS courses in collaboration with department faculty and staff.

Apr 2019 – Dec 2021 *SPOC (Systems Programmer, Operator, Consultant) / Sunlab Consultant*

On-call technical staff supporting all Linux infrastructure in the department.

Awards and Funding

2022 *Brown CS Norman K. Meyrowitz '81 Award*

Awarded for "exceptionally meritorious service to Brown CS". (2nd-ever student in award history to receive; one of 4 students to receive this award since it was created in 2020.)

Brown CS Senior Prize

Awarded for academic work and service to Brown CS (6.8% of graduating undergraduates in Computer Science).

2021 *Crowdstrike NextGen Scholarship* ($10,000)

Brown CS Randy Pausch Undergraduate Research Fellowship ($10,000)

(ISC)^2 Undergraduate Cybersecurity Scholarship ($3,000)

Mentoring / Supervision

2024 Supervisor for Valentin Ogier (intern) at MongoDB Research, *now at NetApp*

Supervisor for John Wilkinson (intern) at MongoDB Research, *now at Saronic*