Zachary Espiritu

New York, NY, USA

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

Research Interests

Algorithms and data structures, cryptography, databases, formal methods and optimization, systems security, usable security.

Education

Sep 2017 – Dec 2021 **Brown University, Sc.M. (Concurrent Masters)** in Computer Science (GPA: 4.0 / 4.0)

Sep 2017 – Dec 2021 **Brown University, Sc.B. with Honors** in Computer Science (GPA: 4.0 / 4.0)

Honors Thesis: "Time- and Space-Efficient Aggregate Range Queries over Encrypted Databases" (Advisor: Roberto Tamassia)

Current Position

Feb 2023 – current **MongoDB Research**, New York, NY

Senior Research Engineer

Conducting research on encrypted search and database security. Serves as primary contact for engineering teams for advising and reviewing cryptographic deployments within MongoDB.

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". In *Proceedings of the 47th IEEE Symposium on Security and Privacy* (San Francisco, CA, USA). 2026.

2. L. N. Rosenbloom, S. Kamara, **Z. Espiritu**, T. Moataz, A. Bahi, J. Wilkinson. "tigro: Trust Infrastructure for Grassroots Organizing via Grounded Digital Annotations". In *Proceedings of Privacy Enhancing Technologies*, Vol. 2026, Iss. 2 (Calgary, Canada). 2026. *To appear*.

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

4. **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.

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

6.   **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.

7.   **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.

8.   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.

9.   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.

10.   **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.

Manuscripts

11.   **Z. Espiritu** ⁂, M. George. "tEX: (Practical and Near-Optimal) $_{tiny}$ Encrypted indeXes". *Under submission.*

Patents / Applications

12.   A. Agarwal, **Z. Espiritu** ⁂, M. George, S. Kamara, T. Moataz, A. Park, inventors; MongoDB, Inc., assignee. "Systems and Methods for Multi-Party Private Database Implementation". 2025. *Patent pending.* [US-20250358112-A1]

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, EKM (External Key Manager) / KMS (Key Management Service)*

Summer 2018	**Brown PLT at Brown University**, Providence, RI *Undergraduate Researcher*
Summer 2017 and Summer 2016	**Order.co (formerly Negotiatus)**, New York, NY *Software Engineering Intern*

Awards and Funding

2022	*Brown CS Norman K. Meyrowitz '81 Award* Awarded for "exceptionally meritorious service to Brown CS". (2nd student to receive in award history; 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 CS undergraduates).
2021	*Crowdstrike NextGen Scholarship* ($10,000) *Brown CS Randy Pausch Undergraduate Research Fellowship* ($10,000) *(ISC)² Undergraduate Cybersecurity Scholarship* ($3,000)

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

Research Mentoring / Supervision

2024	Masters intern Valentin Ogier at MongoDB Research, *now at NetApp*. Collaboration led to *Leafblower* [1] at IEEE S&P 2026. Undergraduate intern John Wilkinson at MongoDB Research, *now at Saronic*. Collaboration led to *Tigro* [2] at PETS 2026.

Professional Service

Artifact Evaluation	IEEE S&P (2026), PETS (2026), USENIX Security (2026)
External Reviewer	CRYPTO (2023, 2024, 2025), ACM CCS (2023), SRDS (2024), VLDB (2025)
Journal Reviewer	ACM TOPS (2024)

Organization Service

MongoDB Research, New York, NY

Aug 2024 – current — *MongoDB PhD Fellowship Committee*

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.

Interests and Hobbies

Marathon (and ultramarathon) running

Pottery on the wheel

Theatrical lighting design

Security CTF competitions (solo winner of Brown's 2021 CTF and MongoDB's 2024 CTF)

Dance Dance Revolution