Zachary Espiritu

Website: zacharyespiritu.com • **Email**: zachary_espiritu@brown.edu
GitHub: ZacharyEspiritu • **LinkedIn**: zacharyespiritu

Education

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

- **Relevant courses:** Algorithms, Cryptography, Distributed Systems, Formal Methods, Human-Computer Interaction, Operations Research, Operating Systems, Probabilistic Methods for CS, Software Security.

Experience

Aug 2020 – Present **Encrypted Systems Lab** • **Researcher, Applied Cryptography**

- Wrote novel crypto protocol and Node.js prototype for **MA Dept. of Public Health** to securely conduct epidemic research over DBs of ~30 distributed MA institutions, eliminating costly, vulnerable, manual anonymization step.

Sep 2020 – Present **Cryptography, Anonymity, Privacy, Security (CAPS) Group** • **Researcher, Encrypted Databases**

- Designed 7 novel, O(1)-time, provably secure aggregate query schemes for encrypted databases, reducing state-of-the-art runtime and storage overhead by 90% in practice, and eliminating all-known reconstruction attacks.
- Devised dynamic programming algorithm to reduce Python experiment setup times by 99%, allowing larger benchmarks (which would have taken 8.75 years to run) to complete in < 1 hour and appear in final publication.
- Developed novel algorithms to attack and fully reconstruct plaintext of higher-dimensional, encrypted DBs.

May 2020 – Aug 2020 **Google** • **Software Engineering Intern**

- Architected, coded, and released open-source OpenSSL engine allowing web servers to use Google Cloud HSM keys for cryptographic signatures without any source code changes. In C++ with gRPC and Bazel components.

Jun 2018 – Aug 2018 **Brown PLT (Programming Languages Team)** • **Research Programmer**

- Wrote machine learning package, used yearly in 90-student course, for Pyret, a functional programming language.

Jun 2016 – Aug 2017 **Negotiatus** • **Software Engineering Intern** (Jun 2017 – Aug 2017 and Jun 2016 – Aug 2016)

- Led full-stack development in HTML, JavaScript, and Ruby on Rails of still-existing, core value propositions such as Scheduled Orders, which converted ~20% of non-recurring revenue into monthly recurring revenue by 2017.
- Optimized SQL queries via PostgreSQL materialized view caching layer for up to 100x faster product searches.

Research Publications

Aug 2021 **Z. Espiritu**, E. A. Markatou, R. Tamassia. **Efficient Aggregate Range Queries on Encrypted Databases.** (Under Review)

Aug 2021 F. Falzon, E. A. Markatou, **Z. Espiritu**, R. Tamassia. **Encrypted Range Search in Multiple Dimensions.** (Under Review)

Computer Science Department Teaching Experience

Sep 2018 – Present **Head Teaching Assistant (for 6 Computer Science Courses)**

- Hired, trained, and directly managed 54 TAs as HTA for multiple courses, including Software / Binary Exploitation (2021) and Computer Systems Security (2021, 2020, 2019), a generalist course covering defenses and pen-testing in Linux systems security, web application security, and cloud storage security.
- Designed new security course project for 92 students on cryptographic authentication/authorization and using untrusted servers for secure file storage and sharing. Project scored average student evaluations of 4.61 / 5.00.
- Automated 3 courses' grading and project setup via Bash scripts integrated with Linux VMs and Docker containers in Google Compute Engine, saving 250 staff hours over 3 courses and $4k/year in dept. budget.

Oct 2019 – Present **Meta Teaching Assistant (TA Program Coordinator)**

- Headed hiring and training of 781 TAs in 56 courses by managing 112 HTAs in 14 time zones as dotted-line reports.
- Created Python / shell scripts and new organizational processes to save 300 staff hours of manual tasks ($5k/year).
- Wrote **GrblGrader**, an open-source, modular feedback delivery system in JavaScript; seen by 1k students/year.

Selected Projects

- **Vehicle Routing Optimization:** Programmed top-performing local search solver out of 21 teams for NP-hard vehicle transportation problem in grad-level competition. In Python, with earlier prototypes in IBM CPLEX and Java.
- **Weenix:** Wrote OS kernel in C. Based on Unix, with process management, file interfaces, and virtual memory.

Awards and Scholarships

Jul 2021 **CrowdStrike NextGen Cybersecurity Scholarship**
(6 selected nationwide; $7,500 scholarship)

Mar 2021 **Randy Pausch Undergraduate Research Grant**

May 2021 **(ISC)² Undergraduate Security Scholarship**
(20 selected nationwide; $1,000 scholarship)

Nov 2020 **1st Place out of 100 at Hack@Home CTF**