Zachary Espiritu

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

Education

Brown University **Concurrent Sc.B and Sc.M in Computer Science** • GPA: 4.0 / 4.0 Jan 2021 – Present

- **Relevant courses**: Algorithms, Cryptography, Distributed Systems, Formal Methods, Graphics, Human-Computer Interaction, Operations Research, Operating Systems, Probability, Software Security and Exploitation, Systems Security.
- Recipient of the **CrowdStrike NextGen Scholarship** and **(ISC)² Information Security Scholarship** for cybersecurity work.

Experience

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

- Created novel crypto protocol for *MA Dept. of Public Health* to securely conduct epidemic research over obliviously-linked databases of 22 distributed MA institutions; using technologies such as *multiparty computation, homomorphic encryption, and oblivious PRFs*.
- Developed complementary Java / Node.js / AWS prototype, *eliminating costly and risky manual anonymization* process.

Crypto & Privacy Group **Researcher, Defenses and Attacks on Encrypted Databases** Sep 2020 – Present

- Designed 7 novel, constant-time, provably secure aggregate range query schemes for encrypted DBs, *lowering state-of-the-art runtime and storage overhead by up to 83%* in practice.
- Devised dynamic programming algorithm to *reduce experiment setup times by 99%*, allowing inclusion of larger Python benchmarks (by 3 orders of magnitude) in final publication.
- Developed 2 novel algorithmic attacks that *fully reconstruct plaintext of multidimensional encrypted databases* by exploiting geometric patterns in the database index structure.

Google **Software Engineering Intern, Google Cloud HSM and KMS** May 2020 – Aug 2020

- Architected and developed open-source OpenSSL engine allowing web servers (such as Apache and Nginx) to use Google Cloud HSM keys for cryptographic signatures *without source code changes*. C++ with gRPC and Bazel components.

Brown PLT **Research Intern, Programming Languages** Jun 2018 – Aug 2018

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

Selected Projects

- **Private Set Intersection**: Developed 2 novel variants and protocols for *authenticated private set intersection* problem designed to be privacy preserving to the certificate authority. Using bilinear maps; research in graduate-level research seminar.
- **Raft / Zookeeper**: Created Go / Golang implementations of distributed, fault-tolerant key-value stores such as Raft and Zookeeper.
- **Vehicle Routing Optimization Solver**: Designed top-performing local search solver out of 21 teams for NP-hard vehicle routing problem in graduate-level competition, requiring movement of delivery cars according to resource limits. Python and Java.

Department Service

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

- Hired, trained, and managed 54 TAs as HTA for 6 courses, including **Computer Systems Security** (2021, 2020, 2019), a generalist course covering defenses and pen-testing in network security (TLS, etc.), cloud security architecture and design, etc.
- Authored new project for 92 students in security course on applied cryptography fundamentals, security design review, and using untrusted servers for secure, efficient file storage and sharing. Project scored average student evaluations of 4.51 / 5.00.
- Automated 3 courses' grading and project setup via Bash scripts integrated with Linux VMs and Docker containers in GCP, saving 250 staff hours over 3 courses and $4k/year in dept. budget.

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

- Led hiring / training of 781 TAs over 56 courses by managing 112 HTAs over 14 time zones; authored Bash and Python scripts and new organizational processes to reduce management workload by 300 hours, yielding department savings of $5k/year.
- Released GrblGrader, a modular grading management system. JavaScript; 1000 student impressions/year across 8 CS courses.

Publications

Z. Espiritu, E. A. Markatou, R. Tamassia. ***Time- and Space-Efficient Aggregate Range Queries on Encrypted Databases***. *Under Review.*

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