UC San Diego
UC San Diego News Center

January 13, 2018 | By Doug Ramsey

Computer Science Major Honored for Undergraduate Research in Applied Cryptography

Computer Science and Engineering undergraduate Julia Len recently got word that she is a runner-up for a prestigious award honoring outstanding undergraduate researchers. The awards are given annually by the Computing Research Association (CRA) to undergrads at North American universities who show "outstanding research potential in an area of computing research."

Watch streaming video of Julia Len's presentation to the 2017 ACM Computer and Communications Security Conference in Dallas, TX.

Len is currently doing a fifth year of undergraduate work at the University of California San Diego after changing her major from Bioengineering to Computer Science mid-way through her undergraduate studies. The student was honored for research she carried out last spring in a CSE 191 course (Projects in Cryptography) taught by CSE professor Mihir Bellare. Doing a project in applied cryptography, Len helped develop cryptographic hash functions that provide provable security guarantees.

"Hash functions are some of the most vital cryptographic tools," noted Len. "For example, the TLS protocol underlying HTTPS—which we rely on for everyday interactions with popular websites—uses hash functions to create digital certificates that authenticate servers. If an adversary were to find a collision for such a hash function, certificates could be forged and allow servers to be impersonated, putting personal information at risk of theft."

"Our project improved the design of hash functions after analyzing hash functions constructed using the Merkle-Damgard transform," she added. "The most commonly utilized hash functions are constructed using the Merkle-Damgard transform, which iterates a compression function to produce a hash function. Our work proved that weakening the condition on the compression function would still result in a collision-resistant hash function."

According to professor Bellare, Len contributed to a method for designing hash functions that are less likely to fail in the future. “Her work provides new design paradigms that yield hash functions with improved provable-security guarantees, decreasing the likelihood of failure and moving us towards greater security in future Internet communications,” observed Bellare. “Julia obtains this as part of a general framework that also explains the weaknesses of the current design paradigm and unifies different approaches and results in the area.”

The project was so successful that it became the subject of a joint academic paper by Len with Bellare and CSE Ph.D. student Joseph Jaeger. On behalf of her coauthors, Len flew to Dallas last November and presented their joint paper* on collision-resistant hashing at the 2017 ACM Computer and Communications Security Conference (CCS). The meeting brings together information security researchers, practitioners, developers and users from all over the world to explore cutting-edge ideas and results. (Also attending CCS 2017—to accept the CCS Test of Time Award—was CSE professor and security researcher Hovav Shacham.)

“Julia has done innovative, timely, real world-relevant research in cryptography leading to a paper she co-authored at CCS 2017, considered to be a first-tier conference in security and cryptography,” Bellare noted in a letter nominating Len for the CRA award. “She also presented the paper in Dallas, and it’s very rare for an undergraduate to present at a first-tier conference, and much of the work was done while she was a junior!”

Len is a former president of the UC San Diego Scholars Society and is active in the UC San Diego chapter of Women in Computing. She became a CSE Tutor in Spring 2016, and since then has tutored for courses including Introduction to Modern Cryptography (CSE 107), Theory of Computability (CSE 105), Discrete Mathematics (CSE 20), and Computer Organization and Systems Programming (CSE 30). Len was also head tutor for the popular lower-division course, Introduction to Computer Science and Object-Oriented Programming: Java (CSE 11).

A Regents Scholar, Len is looking forward to graduating this June, and she has already applied to multiple Ph.D. programs in Computer Science. She plans to pursue cryptography research for her doctorate, and isn't wasting any time: she wants to start grad school this fall.

The very competitive CRA program selects four winners and four runners-up each year. Julia Len is one of four students nominated from UC San Diego this year, and she is the first student from UC San Diego to get this far in the CRA competition.

The CRA awards were sponsored this year by Mitsubishi Electric Research Labs, which alternates as sponsor every other year with Microsoft Research.

---

*Bellare, M., Jaeger, J., & Len, J. (2017, October). "Better Than Advertised: Improved Collision-Resistance Guarantees for MD-Based Hash Functions." In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 891-906). ACM. https://doi.org/10.1145/3133956.3134087

MEDIA CONTACT

Doug Ramsey, , dramsey@ucsd.edu