Hiding Secrets in Software

Amit Sahai

Professor, Computer Science Director, Center for Encrypted Functionalities Professor, Computer Science

CURRENT RESEARCH

Using mathematics to revolutionize cybersecurity

Mathematical encryption methods, like RSA, have withstood the test of time and remain unbroken decades after their inception, thus proving that sophisticated mathematical tools are an effective way to protect sensitive information. With this truth in mind, Dr. Amit Sahai, of the University of California, Los Angeles, uses mathematics to improve cybersecurity. The problem is, hackers routinely infiltrate servers and steal important data and currently, our response to such attacks are only reactionary. Dr. Sahai's research is working to prevent the attack from ever occurring. He is building new mathematical foundations to address cybersecurity threats that were traditionally seen as outside the scope of mathematical approaches. He hopes that like other transformative revolutions in the past, mathematics will provide the basis for revolutionary advancements in cybersecurity for the future.

Recently, Dr. Sahai and his team made major progress on such problems, in work that has been hailed as a "watershed moment for cryptography." For the first time, Dr. Sahai developed mathematical methods for hiding secrets within software. With his incredibly intelligent team of Ph.D. students and postdoctoral research associates in addition to his many collaborations including some of his past Ph.D. students that have gone on to faculty positions at excellent universities like University of California, Berkeley and Johns Hopkins, Dr. Sahai's work is advancing at an incredible rate. Thus, the combination of mathematical depth and the potential for long-term impact places Dr. Sahai's work at the beginning of a cybersecurity paradigm shift.

Current research includes:

- Functional Encryption and...

Read More at benefunder.com/

AFFILIATION

University of California, Los Angeles

EDUCATION

- Ph.D., in Computer Science, 2000 , MIT
- M.S., in Computer Science, 1998 , MIT
- B.A. summa cum laude, in Mathematics, 1996 , University of California, Berkeley

AWARDS

- Okawa Research Grant Award
- Google Faculty Research Award
- Pazy Memorial Award
- National Science Foundation Frontier Award (Lead PI)
- Alfred P. Sloan Foundation Research Fellow

RESEARCH AREAS

Technology, Computational Sciences / Mathematics, Cybersecurity, Informational Sciences / Internet

FUNDING REQUEST

Your contributions will support the continued research of Dr. Amit Sahai, of the University of California, Los Angeles, as he uses mathematics to transform cybersecurity. Donations will fund the necessary costs required for training the brightest minds to work to find solutions. In choosing to donate, you will play a role in developing new mathematical foundations for our future!