How to Encrypt Software

Amit Sahai
Professor, Computer Science, UCLA

Abstract
The goal of secure program obfuscation is to make a program “unintelligible” while preserving its functionality. For decades, program obfuscation for general programs has remained an art, with all public general-purpose obfuscation methods known to be broken.

In this talk, we will describe new developments this year that for the first time provide a mathematical approach to the problem of general-purpose program obfuscation, where extracting secrets from the obfuscated program requires solving mathematical problems that currently take hundreds of years to solve on the world's fastest computing systems. We will also discuss the implications of these developments.

This talk is based on joint works with Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, and Brent Waters.

Biography
Professor Amit Sahai received his Ph.D. in Computer Science from MIT in 2000. From 2000 to 2004, he was on the faculty at Princeton University; in 2004 he joined UCLA, where he currently holds the position of Professor of Computer Science. His research interests are in security and cryptography, and theoretical computer science more broadly. He has published more than 100 original technical research papers at venues such as the ACM Symposium on Theory of Computing (STOC), CRYPTO, and the Journal of the ACM. He has given a number of invited talks at institutions such as MIT, Stanford, and Berkeley, including the 2004 Distinguished Cryptographer Lecture Series at NTT Labs, Japan. Professor Sahai is the recipient of numerous honors; he was named an Alfred P. Sloan Foundation Research Fellow in 2002, received an Okawa Research Grant Award in 2007, a Xerox Foundation Faculty Award in 2010, a Google Faculty Research Award in 2010, and the 2013 Pazy Memorial Award.