SAVETHEDATE

UC/EasyUC Summer School

August 11-14, 2025
Boston University

Since its first draft formulation 25 years ago, the Universally Composable (UC) security framework has been used to specify and analyze the security of cryptographic protocols in multiple scenarios, quickly becoming the gold standard for cryptographic security, while also being used for specifying and analyzing non-cryptographic computing systems. The framework eventually matured with a definitive exposition in the Journal of the ACM.

In the last decade and a half, there has been a great deal of interest in mechanizing proofs of cryptographic security using proof assistants, such as EasyCrypt. Even more recently, researchers have turned their attention to mechanizing proofs of UC Security. One such effort is EasyUC, which provides a domain specific language (DSL) for UC. The implementation of the UC DSL provides a typechecker that catches many errors that may lurk in paper-and-pencil UC models, an interpreter that lets UC designers experiment with their models, and a translator into EasyCrypt, where sequence of games security proofs can be carried out. There is also a graphical user interface for generating skeleton UC DSL code.

In summer 2025, the originator of UC, Ran Canetti, and the designers and developers of EasyUC including Alley Stoughton are joining forces to hold a summer school at Boston University. The summer school will feature both lectures on UC and EasyUC, as well as tutorial sessions in which participants can learn to use the EasyUC tools and/or create paper-and-pencil UC models and analyses. There will be breakout sessions on more advanced topics, including advances in the theory and application of UC, using the UC DSL for modeling system security, and carrying out sequence of games proofs in EasyUC. The school welcomes a broad range of participants who will benefit from exposure to a variety of aspects of UC and its mechanization via EasyUC, as we bring these two research areas together for four days of learning, collaboration and hands-on practice.

If you might be interested in participating in the summer school, we hope you will put yourself on our mailing list and give us feedback that will help us fine tune our plans for the school. You can also email the organizers at uc-easyuc-summer-school+owners@googlegroups.com.

The organizers of this summer school would like to thank DARPA for their support on our work under the HARDEN program.

BOSTON UNIVERSITY

RIVERSIDE RESEARCH