CT Advanced Computing Center (CACC) Security Seminar Series 2024

Speaker: Hemi Leibowitz from UConn
Date: October 9, 2024
Time: 11- 12:30pm
Location: ITE 336
Meeting Link : https://uconn-cmr.webex.com/uconn-cmr/j.php?MTID=m4d36ddf4d36edd727aa04331cdb7d7f6
Meeting number (access code): 2633 368 4613
Meeting password: MqmJMizs533

Security Seminar: Hemi Leibowitz-CMoSS: Composable Modular Security Specifications Framework

We present CMoSS, a framework that enables modular specifications, design and reduction-based proofs of security for practical cryptographic protocols.
CMoSS, building on MoSS, supports complex and practical requirements and models, including various types of delays and failures.
In particular, CMoSS extends MoSS by supporting composition of protocols, facilitating modular, top-down specifications, design and analysis.
Composition of protocols in CMoSS is simple, and we show that it preserves the properties (requirements) of the composite protocols, under certain conditions.
We define satisfaction of requirements assuming a model and a black box, and show that this definition enables natural forms of protocol composition