The Weizmann Institute of Science
Faculty of Mathematics and Computer Science

Foundations of Computer Science Seminar

Room 1, Ziskind Building
on Monday, Dec 16, 2024
at 11:15

Lior Rotem
Stanford

will speak on

Accountability in Threshold Cryptography

Abstract:
Threshold cryptography has been fundamental to secure distributed protocols for over three decades. However, it often comes at the expense of accountability: when secret information is shared among multiple parties, it can be difficult to determine who is at fault if this information is leaked or misused.
In this talk, I will present a recent line of works that demonstrate that this trade-off is not inherent—we can indeed build accountable threshold cryptosystems. Most of the talk will focus on accountability in secret sharing. Suppose Alice uses a t-out-of-n secret sharing scheme to store her secret key on n servers. This guarantees that the servers learn nothing about her secret key, even if t-1 of them collude. But what happens if some servers decide to sell their shares? In this case, Alice should be able to hold them accountable; otherwise, they have a risk-free incentive to sell her shares. A secret sharing scheme that allows Alice to trace the leak back to the corrupted servers is called a traceable secret sharing scheme. I will present new definitions and practical constructions for traceable secret sharing, based on the natural and widely-used schemes of Shamir and Blakley.