



January 8
2019

Greater Tel Aviv Area
Cryptography Symposium

Ziskind Building, Room 155
Weizmann Institute of Science

Program:

- | | |
|---------------|---|
| 09:40 - 10:00 | Gathering and Coffee [Ziskind Lobby] |
| 10:00 - 11:00 | Alon Rosen [IDC]
Finding a Nash Equilibrium is No Easier than Breaking Fiat-Shamir |
| 11:00 - 11:20 | Coffee Break [Ziskind Lobby] |
| 11:20 - 12:20 | Venkata Koppula [Weizmann]
CPA to CCA Transformation via Hinting PRGs |
| 12:20 - 13:40 | Lunch Break [Ziskind Lobby] |
| 13:40 - 14:40 | Yuval Ishai [Technion]
Compressing Vector OLE: Secure Computation with Silent Preprocessing |
| 14:40 - 15:00 | Coffee Break [Ziskind Lobby] |
| 15:00 - 16:00 | Omer Paneth [Northeastern University and MIT]
How to Delegate Computations Publicly |

Website & Registration: <http://tiny.cc/gtacswwis>