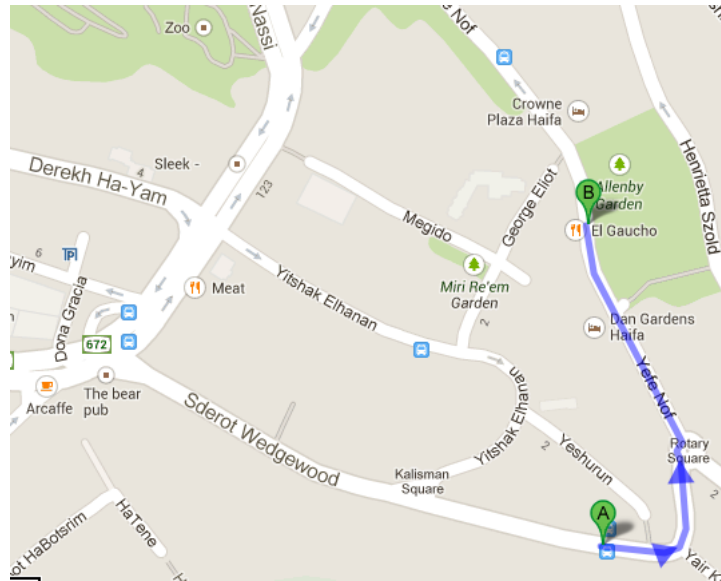


Lightweight Crypto Day 2014

- 9:00 – 9:30 Registration & Coffee
- 9:30 – 9:35 Welcome and Opening Remarks
- 9:35 – 10:25 **Roberto Avanzi** — Lightweight crypto and the industry
- 10:25 – 11:15 **Nathan Keller** — The lightweight block ciphers zoo
- 11:15 – 11:35 Coffee Break
- 11:35 – 12:25 **Christian Rechberger** — Symmetric-crypto research meets practice:
Low latency ciphers
- 12:25 – 14:00 Lunch Break
- 14:00 – 14:50 **Itai Dinur** — The lightweight block cipher LED as an inspiration
for cryptanalysis
- 14:50 – 15:20 **Riaal Domingues** — Standardisation efforts in lightweight cryptography
- 15:20 – 15:40 Coffee Break
- 15:40 – 16:30 **Rump session**
- 16:30 – 17:15 **Discussion** — What are the research goals in lightweight cryptography?
- 19:30 Dinner at the El-Gaicho restaurant (120 Yefe Nof st.)

El-Gaicho — 120 Yefe Nof st.:



Buses 30, 37, 37N, or 237 from the university to Carmel center. Get off one stop **after** Carmel center (unless you take 237, get off at Carmel center). Schedule: 18:00, 18:14, 18:30, 18:44, 18:55, 19:00, . . . The ride takes about 20–25 minutes.

You can also arrive early, and walk down the Louis promenade (continue on Yefe-Nof for another 400 meters).