Winter School on Bilinear Pairings in Cryptography

Location: Wohl Center, Bar-Ilan University

School organizer: Yehuda Lindell

Monday, February 4, 2013 – Background to Elliptic Curves	
9:00 am to 9:30 am	***Registration***
9:30 am to 9:35 am	Opening remarks – Yehuda Lindell
9:35 am to 10:00 am	School overview – Dan Boneh
10:00 am to 11:30 am	The basics of elliptic curves – Nigel Smart
11:30 am to 12:00 pm	*Coffee break*
12:00 pm to 1:30 pm	The discrete log problem on elliptic curves – Nigel Smart
1:30 pm to 3:00 pm	*Lunch*
3:00 pm to 4:30 pm	Applications of elliptic curves to cryptography – Nigel Smart
4:30 pm to 5:00 pm	*Coffee break*
5:00 pm to 5:45 pm	Tutorial (QA session in small groups)
6:00 pm	*Bus to hotel and Tel Aviv*
Tuesday, February 5, 2013 – Pairings and Applications	
9:30 am to 10:30 am	The basics of pairings – Dan Boneh
10:30 am to 11:00 am	Identity-based encryption and variants – Dan Boneh
11:00 am to 11:30 am	*Coffee break*
11:30 am to 1:00 pm	Identity-based encryption and variants (continued) – Dan Boneh
1:00 pm to 2:30 pm	*Lunch*
2:30 pm to 4:30 pm	Attribute-based encryption – Allison Bishop Lewko
4:30 pm	*Tour in the old city of Jaffa (including refreshments)*
8:00 pm	*Dinner at Meatos Restaurant, Tel Aviv*

Wednesday, February 6, 2013 - Applications	
9:30 am to 10:30 am	Broadcast encryption and traitor tracing – Dan Boneh
10:30 am to 10:45 am	*Short break*
10:45 am to 11:45 am	Functional encryption – Allison Bishop Lewko
11:45 am to 12:15 pm	*Coffee break*
12:15 pm to 1:15 pm	Non-interactive zero knowledge – Jens Groth
1:15 pm to 3:00 pm	*Lunch*
3:00 pm to 4:00 pm	Non-interactive zero knowledge from pairings – Jens Groth
4:00 pm to 4:30 pm	*Coffee break*
4:30 pm to 5:30 pm	Non-interactive zero knowledge from pairings (continued) – Jens Groth
5:45 pm	*Bus to hotel and Tel Aviv*
Thursday, February 7, 2013 – Applications and How Pairings Work	
9:30 am to 10:30 am	Anonymous credentials and eCash – Anna Lysyanskaya
10:30 am to 10:45 am	*Short break*
10:45 am to 11:45 am	Anonymous credentials and eCash (continued) – Anna Lysyanskaya
11:45 am to 12:00 pm	*Short coffee break*
12:00 pm to 1:00 pm	How pairings work – Florian Hess
1:00 pm to 2:30 pm	*Lunch*
2:30 pm to 4:00 pm	How pairings work and how to compute them efficiently – Florian Hess
4:00 pm to 4:30 pm	*Coffee break*
4:30 pm to 6:00 pm	How pairings work and how to compute them efficiently (cont.) – Florian Hess
6:00 pm	*Farewell and bus to hotel*

We thank the European Research Council and Bar-Ilan University for their financial support.

Department of Computer Science, Faculty of Exact Sciences, Bar-Ilan University