6th BIU Winter School: Cryptography in the Cloud – Verifiable Computation and Special Encryption

Monday, January 4, 2016 – Verifiable Computation	
8:30 am to 9:00 am	***Registration***
9:00 am to 9:05 am	Opening remarks
9:05 am to 10:00 am	Michael Walfish: Introduction and Overview of Verifiable Computation
10:00 am to 10:15 am	*Coffee break*
10:15 am to 11:15 am	Yael Kalai: Short Proofs of Delegated Computation: Foundations and Feasibility 1
11:15 am to 11:30 am	*Coffee break*
11:30 am to 12:30 pm	Yael Kalai: Short Proofs of Delegated Computation: Foundations and Feasibility 2
12:30 pm to 2:00 pm	*Lunch*
2:00 pm to 3:00 pm	Yael Kalai: Short Proofs of Delegated Computation: Foundations and Feasibility 3
3:00 pm to 3:15 pm	*Coffee break*
3:15 pm to 4:15 pm	Michael Walfish: Interactive Arguments with Preprocessing
4:15 pm to 4:30 pm	*Coffee break*
4:30 pm to 5:30 pm	Eran Tromer: SNARKs with Preprocessing
6:30 pm	*Bus to Tel Aviv*
Tuesday, January 5, 2016 – Verifiable Computation	
9:00 am to 10:30 am	Michael Walfish: Interactive Proofs and Program Representations 1
10:30 am to 10:45 am	*Coffee break*
10:45 am to 11:45 am	Eran Tromer: Program Representations 2
11:45 am to 12:00 pm	*Coffee break*
12:00 pm to 1:30 pm	Eran Tromer: SNARKs (Without Preprocessing) and Their Applications
1:30 pm	*Excursion*

Wednesday January 6, 2016 – Verifiable Computation and Special Encryption	
9:00 am to 10:00 am	Michael Walfish: Additional Applications and Summary of Verifiable Computation
10:00 am to 10:15 am	*Coffee break*
10:15 am to 10:45 am	Alexandra Boldyreva: Introduction to Searchable Encryption (models and motivation)
10:45 am to 11:45 am	Mor Weiss: Format-Preserving Encryption 1
11:45 am to 12:00 pm	*Coffee break*
12:00 pm to 1:00 pm	Mor Weiss: Format-Preserving Encryption 2
1:00 pm to 2:30 pm	*Lunch*
2:30 pm to 3:30 pm	Mor Weiss: Format-Preserving Encryption 3
3:30 pm to 3:45 pm	*Coffee break*
3:45 pm to 4:45 pm	Alexandra Boldyreva: Order-Preserving Encryption 1
4:45 pm to 5:00 pm	*Coffee break*
5:00 pm to 6:00 pm	Alexandra Boldyreva: Order-Preserving Encryption 2
6:30 pm	*Bus to Tel Aviv*

Thursday, January 7, 2016 – Special Encryption	
9:00 am to 10:00 am	Alexandra Boldyreva: Statistical Attacks on Deterministic and Order-Preserving Encryption
10:00 am to 10:15 am	*Coffee break*
10:15 am to 11:15 am	Hugo Krawczyk: Probabilistic Searchable Symmetric Encryption
11:15 am to 11:30 am	*Coffee break*
11:30 am to 12:30 pm	Hugo Krawczyk: Practical Searchable Encryption on Large Datasets 1
12:30 pm to 2:00 pm	*Lunch*
2:00 pm to 3:00 pm	Benny Pinkas: Searchable Encryption Using ORAM
3:00 pm to 3:15 pm	*Coffee Break*
3:15 pm to 4:15 pm	Hugo Krawczyk: Practical Searchable Encryption on Large Datasets 2
4:15 pm to 4:30 pm	*Coffee Break*
4:30 pm to 5:30 pm	Hugo Krawczyk: Practical Searchable Encryption on Large Datasets 3
5:30pm	*Farewell*