German-Israeli Minerva Summer School 2008

Arithmetic Geometry and Public Key Cryptography

Tel Aviv University, 27 July — 4 August, 2008.

Organizers: Gerhard Frey (Essen) and Moshe Jarden (Tel Aviv).

Program

Sunday, 27 July

10:00 – 11:00 Registration by Meira Hillel, Schrieber Building, room 130, Tel: (792)-3-640-8043. Please bring your tickets.

11:10 – 12:00 Moshe Jarden: Curves, Jacobian and zeta functions over finite fields.

12:10 – 13:00 Uzi Vishne: Principles of public key cryptography, RSA, discrete logarithms, protocols based on pairings.

13:00 – 15:00 Lunch break.

15:10 – 17:00 Eduardo Ocampo: Introduction to SAGE

17:30 – 19:00 Eduardo Ocamp: Practise of SAGE

Monday, 28 July

10:10 – 11:00 Moshe Jarden: Curves, Jacobian and zeta functions over finite fields.

11:10 – 12:00 Uzi Vishne: Principles of public key cryptography, RSA, discrete logarithms, protocols based on pairings.

12:10 – 13:00 Claus Diem: Index calculus for curves of small genus

13:00 – 15:00 Lunch break.

15:10 – 16:00 Frank Müller: Applications in the world of communications

16:30 – 17:15 Discussion

Tuesday, 29 July

10:10 – 11:00 Moshe Jarden: Curves, Jacobian and zeta functions over finite fields.

11:10 – 12:00 Uzi Vishne: Principles of public key cryptography, RSA, discrete logarithms, protocols based on pairings.

12:10 – 13:00 Wulf-Dieter Geyer: Arithmetic of elliptic and hyperelliptic curves.

13:00 – 15:00 Lunch break.

15:10 – 16:00 Geyer: Exercises on CM methods (class polynomials).

16:30 – 17:30 Geyer: Implementation carried out by the participants.

18:00 – 19:00 Questions and discussion

Wednesday, 30 July

10:10 – 11:00 Wulf-Dieter Geyer: Arithmetic of elliptic and hyperelliptic curves.

11:10 – 12:00 Frederik Vercauteren: Point counting: p-adic and l-adic methods.

Thursday, 31 July

10:10 – 11:00 Gerhard Frey: Duality theorems and Brauer groups.

11:10 – 12:00 Frederik Vercauteren: Point counting: p-adic and l-adic methods.

12:10 – 13:00 Gerhard Frey: Duality theorems and Brauer groups.

13:00 – 15:00 Lunch break.

15:10 – 16:00 Geyer: CM Methods (Construction of good elliptic curves).

16:30 – 17:30 Implementation carried out by the participants.

17:30 – 19:00 Geyer: Questions and discussion.

Friday, 1 August

08:30 – 09:30 A bus will pick you up at your hotel and bring you to Jerusalem.

09:30 – 17:00 Moshe Jarden: Tour in Jerusalem with a professional guide.

17:00 – 18:30 Moshe Jarden: Travel to Masada. Sleeping in a Hotel by Masada

Saturday, 2 August

07:30 – 12:00 Moshe Jarden: Climbing the Masada, a tour on the hill, visiting a museum.

12:00 – 14:00 Lunch break

14:00 – 17:00 Moshe Jarden: Visiting Nahal David.

17:00 – 19:30 Return to Tel Aviv with the bus.

Sunday, 3 August

10:10 – 11:00 Wulf-Dieter Geyer: Arithmetic of elliptic and hyperelliptic curves.

11:10 – 12:00 Claus Diem: Index calculus for curves of small genus

12:10 – 13:00 Gerhard Frey: Duality theorems and Brauer groups.

13:00 – 15:00 Lunch break.

15:10 – 16:00 Jan Tuitman: Point counting.

16:10 – 17:00 Jan Tuitman: Exercises on point counting.

Monday, 4 August

10:10 – 11:00 Wulf-Dieter Geyer: Arithmetic of elliptic and hyperelliptic curves

11:10 – 12:00 Gerhard Frey: Duality theorems and Brauer groups.

12:10 – 13:00 Claus Diem: Index calculus algorithms

13:00 – 15:00 Lunch break.

15:15 – 16:00 Claus Diem: Arithmetic on curves and discrete logarithmus.

16:15 – 17:00 Claus Diem: Arithmetic on curves and discrete logarithmus.

17:10 – 18:00 Moshe Jarden: Concluding discussion.

Tuesday, 5 August

Travelling home.