

Rump Session Schedule

6:30 Daniel Brown - *Multi-Dimensional Montgomery Ladders*

Montgomery's ladder enables elliptic curve scalar multiplication using only x-coordinates. It has the side benefit that the number of steps generally does not depend on the scalar multiplier. Bernstein generalized Montgomery's ladder to combinations of two points. This presentation generalizes further, to three or more points.

6:37 Daniel Brown - *The Unprovable Security of RSA-OAEP in the Standard Model*

Bellare and Rogaway proposed Optimal Asymmetric Encryption Padding (OAEP) as a method for RSA encryption that was provably secure in the random oracle model (ROM). Real world hash functions are not random oracles, however, so proofs in the standard model do not permit such random oracles. This presentation shows that it is impossible to prove in the standard model that breaking RSA-OAEP is as hard as the RSA problem.

6:50 Stefan Erickson - *Explicit Arithmetic Formulas for Hyperelliptic Curves of Genus 2*

Hyperelliptic curves of low genus have the advantage of using smaller field sizes than elliptic curves. The effectiveness of hyperelliptic cryptosystems depends on efficient algorithms for arithmetic. We present the addition and doubling formulas for real curves of genus 2, as well as an improvement for imaginary curves of genus 2.

6:57 Ali Miri and Patrick Longa - *Accelerating Point Arithmetic over Binary and Prime Fields on Elliptic Curve Cryptosystems*

In this talk, we describe how simple algebraic techniques can be used to accelerate the basic formulae for point operations on Elliptic Curve Cryptosystems (ECC). First, we present improved formulae in affine and inversion-free coordinates for composite DA (Doubling/Addition), AD (Addition/Doubling) and DD (Doubling/Doubling or Quadrupling) operations that are faster than previous methods and the traditional approach of executing the basic point operations consecutively. These new operations are part of what we call Composite Point Arithmetic, which has received increased attention in the last few years. It has several applications in the cryptographic arena, for instance, to develop faster ECC scalar multiplication algorithms, to improve scalar multiplication algorithms based on double-base chains or mixed binary/ternary bases, and to accelerate applications that take advantage of simultaneous point multiplications techniques. Second, we have boosted the traditional point operations by exploiting key redundancies in the formulae and replacing cheaper field squaring for field multiplications. The improvement is shown to be considerable, especially in binary fields, where it is possible to build complete multiplication-free formulae. The latter would mean reduced area costs and notably faster implementations. Furthermore, we apply this technique to composite operations and show that the improvement in this case is even greater given the high operation redundancy found in its formulae.

7:10 Claus Diem - *Some comments on the ECDLP and multivariate cryptosystems.*

7:30 Tanja Lange - *eBATS*

eBATS (ECRYPT Benchmarking of Asymmetric Systems) is a new project to measure the time and space consumed by public-key systems.

7:37 Nigel Smart - *Reviving the Dead*

Cryptographers of the world unite!

7:45 Kenny Paterson - *City of the Random Oracle*

In this talk, we will take a photographic tour of Toronto and investigate its connections with the origins of the Random Oracle.