Submittee: Renate Scheidler
Date Submitted: 2011-02-24 17:20
Title: Workshop on Elliptic Curves and Computation
Event Type: Conference-Workshop

Location:
Microsoft Research, Redmond, Washington, USA

Dates:
Oct 18-22, 2010

Topic:
The connection between elliptic curves, cryptology and the theory of computation.

Methodology:
30 one-hour invited lectures, plus a rump session for 5-10 minute impromptu presentations on recent results, work in progress, or announcements of interest to attendees.

Objectives Achieved:
The year 1985 marks the invention of elliptic curve cryptography, and thus the beginning of a 25 year period in which a number of influential papers initiated a fundamental connection between elliptic curves, cryptology and the theory of computation. Since 1997 there has been an annual 2.5 day workshop on this topic. This year (2010), a full week meeting was held to celebrate the 25th anniversary of this seminal invention. The meeting showcased some of the fundamental results of the aforementioned papers and featured as speakers the most influential researchers in the field of elliptic curves. The program included talks on applications of elliptic curves in cryptography and other fundamental results concerning elliptic curves and computation.

Scientific Highlights:
Lectures by Neal Koblitz and Victor Miller (the co-inventors of elliptic curve cryptography), Bryan Birch (who co-formulated the celebrated Birch/Swinnerton-Dyer conjecture), and Gerhard Frey (whose groundbreaking work on elliptic curves and modular forms played a major role in paving the way toward the celebrated Wiles-Taylor proof of Fermat's Theorem).

Organizers:
Koblitz, Neal, Mathematics, University of Washington (Seattle, WA, USA) Lauter, Kristin, Cryptography Research Group, Microsoft Research (Redmond, WA, USA) Miller, Victor, Institute for Defense Analyses, (Alexandria, VA, USA) Stein, William, Mathematics, University of Washington (Seattle, WA, USA

Speakers:
# Daniel J. Bernstein (University of Illinois at Chicago, USA) Algorithms for primes This talk will consist of a series of light mini-talks inspired by Atkin's papers on recognizing primes (1982, "On a primality test of Solovay and Strassen"; 1995, "Intelligent primality test offer"), proving primes to be prime (1993, "Elliptic curves and primality proving"), factoring integers into primes (1993, "Finding suitable curves for the elliptic curve method of factorization"), and enumerating primes (2004, "Prime sieves using binary quadratic forms"). # Bryan Birch (Oxford, UK) A Tribute to Oliver Atkin As a tribute to Oliver Atkin, I will be surveying his work; I will also be including some biographical details. As that would be far too much to talk about, I will be forced to be selective, and will mainly concentrate on work he did in his earlier years, including a bit about what may have influenced him to do that work, and what his work led to. # Wouter Castryck (K.U.Leuven, Belgium) The probability of primality of the order of a genus 2 curve Jacobian In 2000, Galbraith and McKee conjectured a formula estimating the probability of primality of the number of rational points on an elliptic curve over a finite field. Their heuristic derivation was based on an analytic class number formula counting bivariate quadratic forms up to equivalence. We will give alternative heuristics in favor of the conjecture, based on a random matrix model. This approach seems better-suited for generalizing the conjecture to curves of higher genus. We will then elaborate this in genus 2. This is joint work with Hendrik Hubrechts and Alessandra Rigato. # Melissa Chase (Microsoft Research, USA) Pairing-based proof systems and applications to anonymous credentials Pairing based cryptography has resulted in a number of breakthrough results, including some major developments in the area of zero knowledge proof systems. A zero knowledge proof system allows a party to prove that a statement is true without revealing any other information. Zero knowledge proofs are used in everything from identification protocols (allowing a party to prove that he is who he claims to be) and encryption schemes with stronger security properties, to securing protocols against malicious adversaries, and constructing privacy preserving systems. It has been shown that zero knowledge proofs can be constructed from a variety of number theoretic assumptions (or, more generally from any trapdoor permutation); however most of these constructions are complex and inefficient. In '06 Groth, Ostrovsky, an Sahai showed how to construct proof systems based on pairings which have much more structure than traditional constructions; this structure in turn has since been shown to result in proof systems with greater efficiency, stronger security, and more functionality. This talk will describe at a high level how pairings allows us to construct zero knowledge proofs with more structure than traditional tools, and then discuss some of the applications that take advantage of this structure, focusing on applications to privacy and anonymity. # Andreas Enge (INRIA Bordeaux - Sud-Ouest and IMB, France) Class polynomials by Chinese remaindering Polynomials generating ring class fields of imaginary-quadratic number fields are the main ingredient for obtaining elliptic curves with prescribed complex multiplication. In recent years, algorithms computing such class polynomials by Chinese remaindering have been found which are faster (both in theory and practice) than the classical complex analytic approach. I will give an overview of the algorithms and concentrate on how the last stumbling block could be overcome, the use of alternative class invariants that lead to smaller polynomials. # Junfeng Fan (K.U.Leuven, Belgium) ECC on constrained devices The embedded security community has been looking at the ECC ever since it was introduced. Hardware designers are now challenged by limited area (3) can be given in terms of composition laws on trilinear forms. For example, one can compute Jacobians of trigonal curves via composition on certain trilinear forms.

Links:
http://2010.eccworkshop.org/