

CS559 Curve Based Cryptography - Prof. Ming-Deh Huang
Scribe: Iftikhar A Burhanuddin
burhanud@usc.edu
Class #1 - January 08, 2002

Administrivia: Class timings changed to Tuesday 3:30-6

Course contents: What, How and Why of Curve-based cryptography

Grading: Final project (could be purely theoretical, a combination of theory and implementation but not implementation based alone) and class participation

Textbook: Algebraic Aspects of Cryptography (Algorithms and Computation in Mathematics, Vol 3) by Neal I. Koblitz, Springer. July 1998. Price: \$64.95

Supplementary reading (Recommended but not required):

1. Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, CRC Press. October 1996. Price: \$94.95 Entire book available online <http://cacr.math.uwaterloo.ca/hac/>
2. A Course in Number Theory and Cryptography (Graduate Texts in Mathematics, No 114) by Neal I. Koblitz, Springer. September 1994. Price: \$49.95
3. Handouts

For deeper treatment on the subject of elliptic curves:

1. J.S. Milne's notes on Elliptic Curves and other course notes, pre-prints available at <http://www.jmilne.org/math/index.html>
2. J. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, GTM 106.

Overview of textbook:

Chapter 1 - good write-up about PKC

Chapter 2 - Basic complexity theory

Chapter 3 - Algebra - finite fields and polynomial rings

Chapter 6 - Elliptic and Hyperelliptic curves.

There is also an appendix with an introduction to hyperelliptic curves.

History of Cryptography: Earliest encryption scheme? First known cipher - the Caesar cipher, which was a simple shift of the alphabet. #Theory has been involved since Day 1 - Caesar cipher := $x + 3 \pmod{26}$

PKC has a much shorter history and it started with W. Diffie and M.E. Hellman's paper [1] in 1976. Koblitz's notes in the first chapter that Needham in '68 came up with what we now call one-way functions. With PKC came substantial applications of # Theory.

RSA := 2 primes (p,q), 1 composite # (n)

The world's most famous and widely used PKCsystem had it's origins in a paper by R. Rivest, A. Shamir and L. Adleman [2] published in 1978. Check pictures of the three young scientists during the 'crypto years' available at <http://www.usc.edu/dept/molecular-science/RSApics.htm>

Theoretic issues in the RSA algorithm: primality & factorization

Was Gauss speaking complexity theoretically when he said:

"The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and prolix that even for numbers that do not exceed the limits of tables constructed by estimated men, i.e. for numbers that do not yield to artificial methods, they try the patience of even the practiced calculator... The dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated." – Karl Friedrich Gauss, *Disquisitiones Arithmeticae* (translation: A. A. Clarke)

Mid 70s to the mid 80s baby # theory was used for PKC and then V. Miller [3] and N. Koblitz [4] independently proposed using Elliptic curves to do cryptography.

Victor Miller's inspiration for ECC lay in Don Coppersmith's recent results in computing Discrete Logarithms over finite fields [5] which lowered the bound from $L[\frac{1}{2}]$ to $L[\frac{1}{3}]$.

Meanwhile people were using Elliptic curves for factoring [6] and primality testing too [7]. With the flurry of results in early 90s came the companies ... pushing ECC.

Questions which could be explored during the semester:

1. Is ECC a better bet to RSA in wireless and other resource constrained environments?
2. Should no known sub-exponential attacks for Elliptic curve analogue of Discrete Logarithm problem translate to using 160 bits keys instead of 1024 bit keys?
3. What are the implications of efficient Quantum algorithms for factoring and discrete log?

Bibliography:

1. New directions in cryptography from IEEE transactions on Information Theory, IT 22:644-654, 1976.
2. R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, 21(2):120-126, February 1978.
3. Victor Miller, Use of elliptic curves in cryptography. In Advances in Cryptology: Proceedings of Crypto '85, volume 218 of Lecture Notes in Computer Science, pages 417-426, Berlin, 1986. Springer-Verlag.
4. Neal Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, Vol. 48, No. 177, 1987, 203-209.
5. Don Coppersmith, Fast evaluation of logarithms in fields of characteristic two, IEEE Transactions on Information Theory 30 (1984), 587-594.
6. Hendrik W. Lenstra, Jr., Factoring integers with elliptic curves, Annals of Mathematics (2) 126 (1987), 649-673.
7. Leonard M. Adleman and Ming-Deh Huang, Recognizing primes in random polynomial time. In Alfred Aho, editor, Proceedings of the 19th Annual ACM Symposium on Theory of Computing, pages 462-469, New York City, NY, May 1987.