International Conference on Security of Information and Networks

SIN 2007

May 8-10, 2007

TUTORIAL PROPOSAL

1. **Tutorial title.**

ELLİPTIC CURVE CRYPTOGRAPHY

2. **Proponent(s) information.**

Prof. Dr. Ersan Akyıldız

Director , The Institute of Applied Mathematics
Middle East Technical University
06531, Ankara Turkey

Ph: (312) 210 2987
Fax: (312) 210 2985

3. **Email contact.**

ersan@metu.edu.tr

4. **Instructor(s) bio-sketch.**

B.Sc: Mathematics, Middle East Technical University, Turkey, 1973
Ph.D.: Mathematics, University of British Columbia, Canada, 1977
EMPLOYMENT HISTORY
Professor 2/1990- Present Middle East Tech.Univ. Dept. of Math., Turkey
9/2002- 8/2005 Chairman, Inst. of App. Math.Cryptography Dept. METU.
8/2005- Present Director, Institute of Applied Math.
Area Of Specialization:

Cryptography and Algebraic Geometry

5. **Tutorial abstract.**

In this tutorial we shall introduce the elliptic curve cryptography, which is believed to be one of the most promising candidates for the next generation cryptographic tool. The following issues will be discussed :

1. Finite field arithmetic and basic properties of elliptic curves over finite fields.
2. Elliptic Curve Discrete Logarithm Problem .
3. Attacks on Elliptic Curve Cryptosystems.
4. Minimum Requirement for Secure Elliptic Curve Cryptosystems
5. Standardization of Elliptic Curve Cryptosystems
6. Construction of Elliptic Curves

6. **Tutorial outline.**

1. **Basic Discrete Mathematics (60 minutes)**
   (a) Discrete Mathematics : Groups and Fields
   (b) Finite Fields: F_p and F_{2^m} and Their Arithmetic
   (c) Receommended Finite Fields
   (d) Applications: Prime Generation, Irreducible Polynomial Selection, and Algorithms to do Finite Field Arithmetic

2. **Elliptic Curves (100 minutes)**
   (a) Elliptic Curves $E(F)$ over a field F.
   (b) The Group Law of Eliptic Curves
   (c) Elliptic Curves Over F_p and F_{2^m}
   (d) Addition Operation on $E(F_p)$ and $E(F_{2^m})$
   (e) Some Basic Concepts and Facts:
      - Elliptic Curve Arithmetic
      - Hasse-Weil Theorem

3. **Elliptic Curve Cryptography (ECC) (100 minutes)**

   (a) Discrete Logarithm Problem on Elliptic Curves

   (b) Security:

      ∗ Polard's Rho Algorithm
      ∗ Pohling-Hellman Attack
      ∗ Anomalous, MOV and Weil Descent Test

   (c) Selecting an Appropriate Elliptic Curve:

      ∗ Using Hasse's Theorem
      ∗ Choosing a Curve at Random
      ∗ The Complex Multiplication Method

   (d) Recommended Curves

   (e) Applications Using MIRACL

4. **Elliptic Curve Cryptography in Practice (100 minutes)**

   (a) ECC Domain Parameters

   (b) ECC System Setup

   (c) Key Pairs

   (d) Public Key Validation

   (e) ECDH Key Agreement Protocol

   (f) EC ElGamal Cryptosystem

   (g) ECDSA

   (h) Applications Using MIRACL

7. **Tutorial goals.**

The arena for applying mathematics to cryptography expanded dramatically when Diffie and Hellman invented an entirely new type of cryptography, called public key. At the heart of this concept is the idea of using a one-way function for encryption. The functions used for encryption belong to a special class of one-way functions that remain one-way only if some information (the decryption key) is kept secret. Again using informal terminology, we can define a public-key encryption function (also called a "trapdoor" function) as a map from plaintext message units to ciphertext message units that can be feasibly computed by anyone having the public key but whose inverse function (which deciphers the ciphertext message units) cannot be computed in a reasonable amount of time without some additional information, called the private key.

In 1985 Koblitz and Miller independently proposed using the group of points on an elliptic curve $E(F)$ defined over a finite field F in cryptography. Their point was the map $f : \{1, 2, ...n\} \rightarrow E(F)$, $f(k) = kP$,is a one- way function for the suitable elliptic curves $E(F)$ over the finite field F. Here P is a fixed point on $E(F)$ of order n.This idea has brought the Discrete Logarithm Problem on Elliptic Curves and and thus the whole theory of Public Key Elliptic Curve Cryptography. The reasons why Elliptic Curve Cryptography are important for cryptographic applications can be summarized as :

- They have the potential to provide faster public-key cryptosystems with smaller key sizes in comparison with RSA systems.
- Many public-key algorithms, like Diffie-Hellman, ElGamal, and Schnorr, can be easily implemented in elliptic curves over finite fields.

For the complexity of elliptic curve theory, it is not easy to fully understand the theorems while reading the papers or books about Elliptic Curve Cryptography. But with the development of Elliptic Curve Cryptography and for its advantage over other cryptosystems on finite fields, more and more people express their interests in this field. This tutorial is just for those who want to quickly refer to the basic knowledge, especially the available cryptography schemes used in this filed.