Elliptic Curve DiffieHellman RSA

Seongjin Cho (Josh)

May 23, 2013

Contents

1 Introduction

The development of Elliptic curve both strengthened the security and increased the performance of RSA public key cryptosystem as it enabled us to use smaller key size in approximately same degree of security. However, one may naturally ask how this seemingly unrelated object *elliptic curve* plays active role in public key cryptosystem. To answer this question, this paper will investigate what properties of the elliptic curve enabled such strong security. Also, this paper will further discuss and implement specific example key agreement protocol called *Elliptic curve DiffieHellman* (ECDH). Much of our the work in this paper is based on Professor Neal Koblitz's *A Course in Number Theory and Cryptography* [**?**].

We will first introduce some terminologies and background information about basic Diffie-Hellman cryptosystem. We then briefly define and enumerate several properties of elliptic curve to emphasize what aspect of elliptic curve improved the previous RSA cryptosystem. Next, we will analyze the key establishment procedure using analogue between Alice and Bob. Then we will finish our paper with pseudocode and further possible application.

2 Some Background Knowledge

1. I will assume as little as possible.
2. I am adding this just because it is
3. This list will be deleted in final draft!

2.1 Diffie-Hellman

2.2 Elliptic curve

In our paper, we define elliptic curve to be slightly more restrictive because other kind of elliptic curves are unnecessarily.

Definition 1. *Let $f(x)$ be a cubic polynomial without terms in characteristic 2 and have distinct roots. Then the solutions to the equation*

$$y^2 = f(x) \tag{1}$$

are called the points of the elliptic curve defined by 1, and we will usually use $F(x,y) = y^2 - f(x) = 0$ instead of the form 1.

3 Elliptic Curve DiffieHellman

3.1 elliptic curve Diffie-Hellman

4 Algorithm

4.1 Pseudocode