Elliptic Curves for Applications

Tanja Lange

Technische Universiteit Eindhoven, The Netherlands
`tanja@hyperelliptic.org`

Abstract. More than 25 years ago, elliptic curves over finite fields were suggested as a group in which the Discrete Logarithm Problem (DLP) can be hard. Since then many researchers have scrutinized the security of the DLP on elliptic curves with the result that for suitably chosen curves only exponential attacks are known. For comparison, the RSA cryptosystem is broken if large numbers can be factored; factoring is possible in subexponential time. As a consequence the parameters for elliptic-curve cryptography (ECC) can be chosen significantly smaller than for RSA at the same level of security and arithmetic becomes faster, too.

The NaCl library (Networking and Cryptography library) uses ECC as the public-key component for authenticated encryption (using symmetric-key cryptography for the authenticator and for generating the bulk of the ciphertext) and for signatures. On all levels the algorithms are chosen to simplify implementation without leaking information through software side channels. All implementations in NaCl are timing-invariant and do not have data-dependent branches.

This tutorial explains how to compute on elliptic curves over fields of odd characteristic; how to make the arithmetic efficient; how to avoid data-dependent branches in single-scalar multiplication in the variable-base-point and in the fixed-base-point scenario; how the algorithms in NaCl are designed; and how to use NaCl.

NaCl is joint work with Daniel J. Bernstein and Peter Schwabe. Software and documentation are available at <http://nacl.cr.yp.to>.