PANEL SESSION

Cryptographic Policy Guidelines

Scott Charney (USA)
Stephanie Perrin (Canada)
Steve Orlowski (Australia)
Norman Reaburn (Australia)
Nigel Hickson (UK)
Philippe Dejean (France)
Using Cyclotomic Polynomials to Construct
Efficient Discrete Logarithm Cryptosystems over Finite Fields

Arjen K. Lenstra

Citibank, N.A., 4 Sylvan Way, Parsippany, NJ 07054, U.S.A.
Email: arjen.lenstra@citicorp.com

Abstract. We show how to use cyclotomic polynomials to construct subgroups of
multiplicative groups of finite fields that allow very efficient implementation of
discrete logarithm based public key cryptosystems. Depending on the type of
application and implementation, the resulting schemes may be up to three times
faster than the fastest known schemes of comparable security that use more
conventional choices of subgroups or finite fields.

1 Introduction

In this paper we consider public key cryptosystems that are based, for their security,
on the difficulty of the discrete logarithm problem in the multiplicative group of a
finite field. Several such cryptosystems have been proposed. Examples are the
signature and encryption algorithms due to Taher ElGamal (cf. [3]) and variations
thereof. We propose a new variation that has distinct computational advantages over
previously proposed schemes.

The most time consuming operation in the ElGamal schemes is exponentiation in
the finite field. Therefore variants have been proposed that make the exponentiation
faster without affecting the security. Claus Schnorr proposed to work in a small
subgroup of the multiplicative group of a prime field of large characteristic (cf. [13]).
Such subgroups not only make the signature considerably shorter, but they also make
the exponentiation considerably faster by using short exponents. Supposedly, using
subgroups does not affect the security of the scheme if the subgroup order is prime
and sufficiently large (though small compared to the characteristic). A variant of
Schnorr's proposal was adopted in the U.S. Government’s Digital Signature
Standard (cf. [6]). All these variants allow efficient software implementations.

Gordon Agnew et al. proposed to work in a large extension of the field of two
elements (cf. [2]). With a so-called 'optimal normal basis' representation of the
extension field multiplication becomes very fast and squaring reduces to a circular
shift, so that exponentiation can be done very efficiently. Although this
representation does not affect the security of the scheme, fields of characteristic two
are generally considered to be more vulnerable to attacks than other fields of
comparable sizes. The security of Agnew's variant can be boosted by working in a
quadratic extension, an idea that is similar to Schnorr's. To take full advantage of
this variant a hardware implementation is strongly recommended.