ATELIER « LA SÉCURITÉ INFORMATIQUE ET LA CRYPTOGRAPHIE »
12–16 AVRIL 2010

WORKSHOP ON COMPUTER SECURITY AND CRYPTOGRAPHY
APRIL 12–16, 2010

(Hyper-)elliptic curve cryptography

Renate Scheidler

Department of Mathematics & Statistics
University of Calgary
2500 University Drive NW
Calgary, AB T2N 1N4
CANADA

rscheidl@ucalgary.ca

This talk provides an overview of elliptic and hyperelliptic curves in the context of their use in discrete logarithm based cryptography. We begin with a brief review of elliptic curves and their group law. Next, we move on to hyperelliptic curves and their associated group (the Jacobian), describing a representation of group elements as well as the group operation. We summarize methods for determining the group order as well as extracting discrete logarithms on both elliptic and hyperelliptic curves. If time permits, alternative curve models will be discussed.