Time: Monday May 2nd, 2011 5:00pm
Location: Buchanan A203

Pairing based Cryptography

Monireh Rezai Rad , University of Calgary

The world of cryptography went through a big revolution by the introduction of public-key cryptography (PKC). PKC enable unknown sender to send encrypted information to a receiver such that nobody, but the receiver is able to decrypt it. Recently there has been a gradual shift towards curve-based cryptography. Elliptic curves are a popular choice in PKC. Moreover, these curves allow for more protocols to be implemented, this is achieved by using a bilinear map called pairing, which can be efficiently computed in many cases. Parings have recently been exploited in several cryptographic applications such as identity based cryptography (where your e-mail address is your public key) and tripartite key exchange (where three parties can agree on a secret across insecure communication channels). A highly ! useful generalization of elliptic curve cryptography is cryptosystems based on hyperelliptic curves which also carry the pairing construction.