MICHAEL JACOBSON, University of Calgary, Calgary, Alberta
Security Estimates for Quadratic Field Based Cryptosystems

The security of public-key cryptosystems using quadratic fields is based on two types of discrete logarithm problem. In the imaginary quadratic case, the discrete logarithm problem in the ideal class group is used, whereas in the real quadratic case the principal ideal problem (also known as the infrastructure discrete logarithm problem) is used instead. In this talk, we describe recent improvements to the best known algorithms for solving these two problems. Our numerical results are presented, as well as extrapolations leading to recommendations for parameter sizes providing approximately the same level of security as block ciphers with 80, 112, 128, 192, and 256-bit symmetric keys.