

IEEE 1363.4 PAR

Paul Dickinson, Safuat Hamdy, Michael J. Jacobson, Jr.

Centre for Information Security and Cryptography
University of Calgary

August 18, 2005

Title

Standard Specification for Public Key Cryptography based on Class Groups Of Imaginary Quadratic Number Fields (IQ Cryptography)

Scope

Specification of a suite of primitives for performing IQ Cryptography. Specified are techniques for encryption, decryption, signatures and system setup. We also give pseudocode for the implementation of the necessary mathematical operations in imaginary quadratic class groups.

Purpose

The IEEE 1363 and 1363a standards provide a comprehensive framework for the implementation of various forms of public key cryptographic protocols. The computational problems upon which these protocols are based are the discrete logarithm, integer factorization and elliptic curve families. Using imaginary quadratic class fields, we find analogous problems that are at least as hard as their regular counterparts, and appear to be harder in some cases. More importantly, the hardness of the IQ problems appears to be independent of the hardness of other variants of the same problems. As there are no rigorous proofs of the difficulty of any of these problems, and progress is continually being made in finding more efficient solutions, having an independent set of problems upon which to base cryptographic systems is desirable.

Reason

Cryptography based on class groups of imaginary quadratic number fields has been a subject of attention among cryptographers in recent years. We wish to expose the idea to the public, and provide an alternative framework for public key cryptography that is efficient and as secure as existing systems based on discrete logarithms and integer factorization. As the security is independent of these problems, our cryptosystems provide a secure alternative in the event that existing cryptosystems are found to be insecure. By including it in an IEEE standard, we wish to provide a complete and concise reference for those wishing to implement IQ based methods securely.