

IQ-CRYPTOGRAPHY: IEEE P1363 STANDARDIZATION PROPOSAL

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

Centre for Information Security and Cryptography
University of Calgary

April 18, 2005

IQ-Cryptography — Overview

Alternative mathematical setting for public key cryptography

Class group (finite, abelian) of an imaginary quadratic order

$$O_{\Delta} = \mathbb{Z} + \mathbb{Z} \frac{\Delta + \sqrt{\Delta}}{2}, \Delta < 0$$

Efficient arithmetic, representation of group elements

Security based on intractable computational problems in the class group

- seem independent of factoring, finite field DLP
- believed to be harder

Arithmetic and Efficiency

Unique representatives of group elements (reduced ideal)

- (a, b) with $a, b \in \mathbb{Z}$, $4a \mid b^2 - \Delta$, $a, b < \sqrt{|\Delta|}$

Group operation: ideal multiplication and reduction (Gauß)

- $O(\log^2 |\Delta|)$, practical version NUCOMP (Shanks)
- fast inversion: $b \Leftarrow -b$

Slower than RSA for current security levels, improves as security requirements increase

Hard Problems and Security

IQ-DLP (discrete log), IQ-RP (root problem), IQ-OP (order problem)

- known reductions: $\text{IQ-RP} \leq_P \text{IQ-OP} \leq_P \text{IQ-DLP}$
- also $\text{IFP} \leq_P \text{IQ-OP}$ — computing order of class group intractable

Random class group is cryptographically suitable with high probability

Best known algorithm: MPQS analogue, conjectured complexity $O(\exp(\{1 + o(1)\}\sqrt{\log \Delta \log \log \Delta}))$

- no known NFS analogue (smaller parameters for equivalent security)

Proposed Protocols

IQ-DH — Diffie-Hellman key exchange in the class group

IQ-Schnorr (signature w/appendix, security: IQ-DLP)

- based on Poupard/Stern formulation of Schnorr's signature scheme
- can't compute order of class group (larger parameters required)

IQ-GQ (signature w/appendix, security: IQ-RP)

- straightforward adaptation of Guillou/Quisquater scheme

Generic exponentiation/multiexponentiation improvements apply to all

Summary

IQ-Cryptography — secure and efficient alternative setting for PKC

Stronger security than RSA, finite field DLP

- believed to be independent of other settings

Efficiency continues to be improved

- IQ-Schnorr signature generation faster than RSA, everything else slower

Worthy of standardization as a backup to other widely-used settings