Algorithms for multiquadratic number fields

Daniel J. Bernstein
University of Illinois at Chicago

Abstract :

Gentry's breakthrough ideal-lattice-based homomorphic encryption system at STOC 2009 was shown several years later to be breakable by a fast quantum algorithm if the underlying number field is chosen as a cyclotomic field (with small h-plus, a condition very frequently satisfied). The same attack also breaks followup cryptosystems by Smart and Vercauteren at PKC 2010 and by Gentry and Halevi at Eurocrypt 2011.

This quantum algorithm has two stages: first, a quantum algorithm by Biasse and Song to find a generator of a principal ideal, building on a unit-group algorithm by Eisentraeger, Hallgren, Kitaev, and Song; second, a simple trick pointed out by Campbell, Groves, and Shepherd to reduce the generator to a short generator.

Can one avoid this attack by replacing cyclotomic fields with other number fields? Some parts of the cryptographic literature suggest that Galois number fields are good for security. Textbooks on algebraic number theory describe another family of high-degree Galois number fields, namely multiquadratics. What happens if cyclotomics are replaced with multiquadratics?

The answer is an even worse security disaster: there is, even without quantum computers, a fast attack against the resulting cryptosystems.

This is joint work with Jens Bauch, Henry de Valence, Tanja Lange, and Christine van Vredendaal.