Random walks on Arakelov class groups

Boer, K. de

Stellingen

behorende bij het proefschrift
"Random Walks on Arakelov Class Groups"
van Koen de Boer

(i) By jumping and crawling on the Arakelov class group one gets everywhere, but nowhere in particular.

(ii) In all ideal lattices of a fixed number field it is about equally hard to find short vectors.

(iii) Carefully picking random elements in a random ideal of a cyclotomic field results often in a relative near-prime ideal.

(iv) The power residue symbol can be computed efficiently, assuming the Generalized Riemann Hypothesis.

(v) The Hilbert symbol can also be computed efficiently, assuming the Generalized Riemann Hypothesis.

(vi) The quantum complexity of the continuous hidden subgroup problem depends, next to on the fourth power of the lattice dimension, only linearly on the logarithm of the Lipschitz constant of the oracle function, the logarithm of the inverse first minimum of the hidden lattice's dual and the logarithm of the inverse allowed probability error.

(vii) Breaking lattice-based cryptography is not known to be NP-hard. In fact, neither is breaking any other cryptography.

(viii) Mandating 'backdoors' in cryptographic software for general public use opening doors for mass surveillance should absolutely be avoided.

(ix) Changing sex on legal documents should be made easier and a third sex 'X' should be included as a valid option.

(x) Scientists should not only present their results truthfully, but also strive for simplicity and avoid unnecessary complexities.

(xi) Self-consciousness can hinder creativity.