Dirichlet L-series and transforming generators of principal ideals in lattice-based cryptography
M.B. Blom

Abstract

This thesis discusses an algorithm to transform an arbitrary generator of a principal fractional ideal to a short generator. This algorithm contributes to a key-recovery attack on Soliloquy.

Both Soliloquy and the key-recovery attack are discussed in this thesis.

Lattices in cryptography and algebraic number theory are connected using the log-unit lattice by embedding number fields in $\mathbb{R}^n$. Furthermore, Dirichlet L-series are explored, including its analytical continuation and the special values $L(1,\chi)$.

Finally, Dirichlet L-series are linked to the class number of a number field.