Logarithmic Lattices.

Leo Ducas, CWI

In this talk, I wish to give an overview of 3 lattices constructed as via logarithmic maps, making connections between geometry of numbers and index-calculus techniques.

The first two played a crucial role in recent algorithm for finding mildly short vector in cyclotomic ideals. The third one is extracted from a deprecated cryptosystem (Chor-Rivest), and turns out to offers a decoding radius near Minkowsky's bound.