1026-11-196 **Alexander May*** (may@informatik.tu-darmstadt.de), Alexander May, Hochschulstr. 10, 64289 Darmstadt, Germany. *Solving RSA Problems with Lattice Reduction.*

Our talk addresses the problem of inverting the RSA function and the problem of factorizing integers. We relax these problems in several ways and show that the relaxations lead to polynomial time solvable problems. In our approach, we model the relaxed problems as polynomial equations which have roots of small size. The roots are then found by a method originally introduced by D. Coppersmith in 1996, which in turn is based on the famous LLL lattice reduction algorithm.

We also present a novel application for RSA with so-called small CRT exponents. Namely, we show that the factorization of an RSA modulus $N = pq$ can be found in polynomial time provided that RSA is used with a secret exponent $d$ such that both $d \bmod p-1$ and $d \bmod q-1$ are smaller than $N^{0.073}$. The existence of such a polynomial time attack answers a long-standing open problem by Wiener. (Received February 27, 2007)