Abstract:
In 1996, Coppersmith introduced lattice-based methods for finding small roots of modular polynomials. By using the method, a number of vulnerability of RSA have been reported so far. In this talk, I explain the basic approach of the method. Then, I introduce our attack on small CRT-exponent RSA. The attacks improve previous ones proposed by Bleichenbacher-May (PKC'06) and Jochemsz-May (Crypto'07). In general, to recover as large root as possible, we should design appropriate lattices that relate to algebraic structures of the target polynomials. We obtain the results by exploiting additional algebraic structures in a clever way.