1056-14-477 **Johannes Buchmann**, **Jintai Ding** and **Mohamed Saied Emam Mohamed*** (mohamed@cdc.informatik.tu-darmstadt.de), Technische Universitaet Darmstadt,Fachbereich, Informatik, Kryptographie und Computer Algebr, Hochschulstrasse 10, Darmstadt, Hessen 64289, and **Wael Said Abd Elmageed Mohamed** and **Daniel Cabarcas**. *MutantXL: An Efficient Algorithm for Solving Multivariate Polynomial Equations.*

MutantXL is an algorithm for solving systems of polynomial equations that was proposed at SCC 2008 and improved in PQC 2008. This talk shows how the concept of mutants can be used to speed up the XL algorithm. The MutantXL algorithm is a new and very efficient alternative to solve multivariate polynomial equations on the function ring over $\mathbb{F}_2$. This talk also introduces a new efficient algorithm for computing Gröbner bases of zero-dimensional ideals called MXL_3. The MXL_3 is based on MutantXL algorithm, MXL_2 improvements, and a new sufficient condition for a set of polynomials to be a Gröbner basis. The experiments showed that both in classical cryptographic challenges and random systems, MXL_3 algorithm performs substantially better than the F_4 algorithm implemented in Magma, currently the best publicly available implementation of F_4. (Received September 12, 2009)