1020-94-135 **Jintai Ding*** (ding@math.uc.edu), Dept. Math. Sci., U. of Cincinnati, Cincinnati, OH 45221, and **Dieter Schmidt**. *Multivariate Public Key Cryptography.*

For the last three decades, public key cryptosystems (PKC) become a indispensable part of our modern communication system. The security of traditional PKC, such as RSA, depends on hard number theory problems such as factoring or discrete logarithms. However, due to the quantum computer attack by Shor, and demand for more efficient cryptosystems for small devices, there is a need to search for alternatives.

Multivariate public key cryptosystem (MPKC) is a promising alternative. Different from traditional PKC, the public key of MPKC is usually a set of quadratic polynomials. The security of MPKC relies on the difficulty of solving systems of nonlinear polynomial equations with many variables, and the latter is a NP-complete problem in general. Compared with RSA public key cryptosystems, the computation in MPKC can be very fast because it is operated on a small finite field.

In this talk, we will give a general survey about the research and the critical mathematical problems in this area. (Received August 24, 2006)