1056-14-982 **Raymond A. Heindl*** (rheindl@gmail.com). *Multivariate Public Key Cryptosystems from Diophantine Equations.*

Most public key cryptosystems used in practice are based on integer factorization or discrete logarithms (in finite fields or elliptic curves). However, if large enough quantum computers can be built, Shor's algorithm will render them completely insecure. Multivariate public key cryptosystems (MPKC) are one possible alternative. MPKC makes use of the fact that solving multivariate polynomial systems over a finite field is an NP-complete problem, for which it is not known whether there is a polynomial algorithm on quantum computers. In this talk, we give a brief introduction to the area, and we propose a new multivariate public key encryption scheme that is based on Diophantine equations. (Received September 19, 2009)