1056-13-1203 **Bo-Yin Yang*** (by@crypto.tw), 128 Sec 2 Academia Rd, Inst. of Information Science, Taipei, 11529, Taiwan. *Multivariate Public Key Cryptography.*

A multivariate public key cryptosystem (MPKCs for short) have a set of (usually) quadratic polynomials over a finite field as its public map. Its security rests on the hardness of solving a system of nonlinear equations over a finite field, and that of finding an isomorphism between two quadratic maps. This family is considered to be one of the major families of PKCs that could resist potentially even the powerful quantum computers of the future. There has been fast and intensive research in Multivariate Public Key Cryptography in the last two decades. Some constructions are not as secure as was claimed initially, but others are still viable. We give an overview of multivariate public key cryptography and discusse the current status of the research in this area, including designs, attacks, and implementations. (Received September 21, 2009)