1016-14-19 **Jintai Ding*** (ding@math.uc.edu), Dept. Math Sci. MO 0025, U. of Cincinnati, Cincinnati, OH 45221, **Dieter Schmidt** (dschmidt@ececs.uc.edu), Dept of Electrical & Computer Engineering and, Computer Scienecs, U. of Cincinnati, Cincinnati, OH 45221, and **Jason Gower** (gowerj@math.uc.edu), Dept. Math.Sci., ML 0025, U. of Cincinnati, Cincinnati, OH 45221.
Zhuang-zi: A New Algorithm for Solving Multivariable Polynomial Equations over a Finite Field. Preliminary report.

We propose a new idea for solving systems of multivariate polynomial equations over a finite field, a difficult problem known to be NP-hard. Our motivation comes from recent development of so-called multivariate public key cryptosystems (MPKCs), where the public key is a set of multivariate polynomials over some finite field and surprising algebraic attacks on symmetric cryptosystems such as AES and other steam ciphers. The key idea is to utilize fact that any vector space on a finite field can be identified as a bigger finite field, which allows us to lift the problem from multivariable case to a singe variable situation and solve it with a special algorithm we have developed in combination with Berlekamp's algorithm. In essence, we seek to replace the classical approach where we treat each variable individually with the global approach where we deal with all the variables simultaneously. Our approach is inspired by the works of Goubin, Kipnis, Patarin, Shamir et al. related to the design and attack of HFE MPKCs. We show examples that our algorithm works much faster than any other exiting algorithms including the new Groebner algorithm (F4, F5) by Faugere. This algorithm is named after an ancient Chinese philosopher Zhuan-zhi also known as Chuan-Tsu. (Received December 20, 2005)