

1046-12-284

Crystal Clough* (ccloughc1@email.uc.edu), Dept of Mathematics, ML 0025, 839 Old
Chemistry, Cincinnati, OH 45221. *Square-Vinegar Signature Scheme*.

We propose a digital signature scheme based on multivariate polynomials. The Square-Vinegar system can be much faster than similar schemes by utilizing odd characteristic and a simpler core map. These changes are possible due to the interaction of Gröbner basis algorithms and field equations. Our claims are supported by extensive experiments, which reveal that the relationship between algebraic attacks and the degree of the core map is more intricate than previously thought. (Received August 25, 2008)