1020-94-134 **Hu Lei*** (hu@is.ac.cn), Yuquan Road,19A, Graduate School of the Chineses Academy of Sc, Beijing, 100049, Peoples Rep of China, and **Jintai Ding**, **Xuyun Nie**, **John Wagner** and **Jianyu Li**. *Cryptanalysis on the New Instance of Tractable Rational Map Cryptosystems.*

Tractable rational map cryptosystem (TRMC) is a new family of multivariate public key cryptosystems. It uses tractable rational map defined over a finite field as its central nonlinear map, and the latter is composed with two linear maps from the inner and outer respectively to get the encryption cipher.

A previous version of TRMC, TRMC-2, is designed such that its decryption involves solving a sub-system of equations. Joux etc. found the existence of the sub-system turned out to be a weakness, and they introduced a variant of the XL algorithm to built an equivalent private key to find the corresponding plaintext. To avoid this attack, the inventor of TRMC proposed a new instance, TRMC-4, recently. But unfortunately, we find is vulnerable to a linearization attack. The attack is an application of Patarin's linarization method, and we do two phases of linear equation system solving so that the finding of plaintext is only to solve a polynomial system on at most 11 variables, which can be easily done by Gröbner base methods.

In this talk, we will first review multivariate public key cryptography and the idea and schemes of the TRMC design. Then we will present how our attack works in details. We will also report our confirmed computer experimental results. (Received August 24, 2006)