Unreval XL and its variants

http://www.firstlight.cn 2010-11-23

Systems of non-linear multivariate equations are at the heart of many cryptographic algorithms, in particular in the public key settin g. This paper investigates some algorithms to solve such systems. Usually, computing the Gr\"obner basis of the corresponding ideal is the b est choice in this context. The best known and also most efficient algorithms for this task are F$_4$ and F$_5$. Another strategy to solve su ch systems is called \emph{eXtended Linearization (XL)} from Eurocrypt 2000. For two reasons this is not as popular as Gr\"obner bases. F irst it is believed that its running time is worse than F$_4$ and second it is not as well understood as Gr\"obner bases. This contribution chall enges both.

存档文本