电子科技大学学报
Journal of University of Electronic Science and Technology of China

线性化方程方法破解TTM公钥加密体制

作者：刘梦娟，聂旭云，胡 磊 ，吴 劲

关键词：代数攻击; 线性化方程; 公钥密码学; 三角形体制; TTM

摘要

TTM是一类三角形多变量公钥密码体制。该文经过分析2004年的TTM实例发现，该实例中存在大量的一阶线性化方程，而且对于给定的公钥，这些线性化方程都可以通过预计算得到。对于给定的合法密文，可以利用一阶线性化方程攻击方法在2^{19}个2^8域上的运算内找到了其相应的明文。该方法与二阶线性化方程攻击方法相比，恢复明文的复杂度降低了2^{12}倍。计算机实验证实了上述结果。

请点击下载（右键另存为）或浏览:UESTC20100230.pdf