计算机工程与应用 2007 43 (16): 152-155 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

对Py的一种改进的区分攻击

胡学先，那 键，刘文芬

信息工程大学 信息工程学院，郑州 450002

收稿日期 修回日期 网络版发布日期 2007-5-19 接受日期

摘要 提出了对流密码算法的一种改进的区分攻击方法。首先利用隐Markov模型给出了有效计算的输出序列在一个特定的事件发生的情况下的条件分布的公式，并由此构造了一个“最优”区分器，在区分优势和目前最有效的区分攻击相同的情况下，所需密钥流长度缩短为原来的1/3.2。

关键词 流密码 区分攻击 隐Markov模型

分类号

Improved distinguishing attack on Py

HU Xue-xian，NA Jian，LIU Wen-fen

Institute of Information Engineering，Information Engineering University，Zhengzhou 450002，China

Abstract

A method for efficiently computing the conditional probability of the output sequence of Py is given， which is based on the theory of hidden Markov model， and from this a distinguisher optimal for this model is built. For the same advantage as that of the best known distinguisher，this attack results in a reduction in the samples needed by a factor of approximately 3.2.

Key words stream cipher distinguishing attack Hidden Markov Model

DOI:

通讯作者 胡学先 E-mail：xuexian_hu@yahoo.com.cn