电子与信息学报 2003 25 (10): 1398-1402 ISSN: 1009-5896 CN: 11-4494/TN

论文

密码学控选逻辑控制序列与输出序列的互信息

刘传东, 吕述望, 范修斌

中国科技大学,研究生院信息安全国家重点实验室,北京,100039

收稿日期 2002-5-29 修回日期 2002-11-14 网络版发布日期 2008-6-16 接受日期

摘要
给出了密码学控选逻辑的概率模型，得到了密码学控选逻辑控制序列与输出序列互信息为零的充要条件，同时利用控制序列在输出序列上的信息泄漏，给出了分析密码学控选逻辑的一种方法。

关键词 密码学控选逻辑 互信息 “停走”型钟控序列

分类号 TN918

The mutual information between control and output sequences of the control-choice cryptographic logic

Liu Chuandong, Lǚ Shuwang, Fan Xiubin

State Key Lab. of Info. Security, Graduate School of USTC, Beijing 100039, China

Abstract
This paper presents the probability model of the control-choice cryptographic logic. A necessery and sufficient condition is gained which satisfies that the mutual information is zero between control and output sequences of the control-choice cryptographic logic. By using the information leak between control and output sequences, a method of analysing the control-choice cryptographic logic is given.

Key words Control-choice cryptographic logic Mutual information Stop-and-go clock-control- led sequence

DOI:

通讯作者

作者个人主页 刘传东; 吕述望; 范修斌