通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

董乐,杜皎,吴文玲.基于高阶差分的type-1广义Feistel-SP结构与Feistel-SPSP结构比较研究[J].通信学报,2014,(7):1~9

基于高阶差分的type-1广义Feistel-SP结构与Feistel-SPSP结构比较研究

Higher-order differences based research on comparison betweentype-1 generalized Feistel-SP network and Feistel-SPSP network

投稿时间： 2014-06-01

DOI：10.3969/j.issn.1000-436x.2014.7.001

中文关键词：type-1广义Feistel结构 单SP函数 双SP函数 高阶差分 伪随机性

英文关键词:type-1 Feistel structure single SP-function double SP-function higher-order difference pseudo- randomness

基金项目:河南师范大学博士启动基金资助项目（01016500148）；国家自然科学基金资助项目（61272476, 61202422）

作者	单位
董乐，杜皎，吴文玲	1. 河南师范大学数学与信息科学学院，河南 新乡 453007；2. 中国科学院软件研究所可信计算与信息保障实验室，北京 100190；3. 河南师范大学数学与科学计算实验室，河南 新乡 453007

中文摘要：

通过对代数次数增加情况的分析，研究了type-1广义Feistel结构下，单SP(substitution-permutation)模型与双SP模型抵抗高阶差分分析的能力。结合高阶积分与高阶差分思想，开发了四路type-1广义Feistel-SP与Feistel-SPSP结构代数次数上界估计的新方法。利用这一方法，分别构造了这2种结构在2种常用参数下的区分器。结果显示，四路type-1广义Feistel结构下，双SP模型抵抗高阶差分攻击的能力不如单SP模型。

英文摘要：

The powers against the higher-order differential cryptanalysis of the single-SP(substitution-permutation) model and the double-SP model are studied in the type-1 Feistel network by analyzing the growths of algebraic degrees. Combining the higher-order integral and the higher-order difference, a new method is exploited to estimate the upper bounds of algebraic degrees for the 4-line type-1 Feistel-SP scheme and the 4-line type-1 Feistel-SPSP scheme. Applying the new method, distinguishers of the two schemes are constructed with four common parameters. As a result, the double-SP model is weaker than the single-SP model against the higher-order differential attack under the 4-line type-1 Feistel structure.

查看全文 查看/发表评论 下载PDF阅读器

关闭

地址：北京市丰台区成寿寺路11号邮电出版大厦8层 电话：010-81055478，81055479
81055480，81055482 电子邮件：xuebao@ptpress.com.cn
技术支持：北京勤云科技发展有限公司