
FCS 文章精要 信息工程大学任炯炯等：HALFLOOP 的两个较大版本的相关密钥飞去来器攻击

作者：writer 来源：科学网

本文原地址：<https://www.iikx.com/news/progress/38435.html>

本文仅供学习交流之用，版权归原作者所有，请勿用于商业用途！

FCS 文章精要

信息工程大学任

炯炯等：HALFLOOP 的两个较大版本的相关密钥飞去来器攻击。论文标题：Related-key boomerang attacks on two larger variants of HALFLOOP

期刊：Frontiers of Computer Science

作者：Kangkang SHI, Jiongjiong REN, Shaozhen CHEN

发表时间：21 Feb 2025

DOI：10.1007/s11704-025-40755-0

微信链接：[点击此处阅读微信文章](#)

RESEARCH ARTICLE

Related-key boomerang attacks on two larger variants of HALFLOOP

Kangkang SHI, Jiongjiong REN✉, Shaozhen CHEN

School of Cyber Science and Technology, Information Engineering University, Zhengzhou 450001, China

Received July 25, 2024; accepted February 19, 2025

E-mail: jiongjiong_fun@163.com

© Higher Education Press 2026

引用格式：

Kangkang SHI, Jiongjiong REN, Shaozhen CHEN. Related-key boomerang attacks on two larger variants of HALFLOOP. Front. Comput. Sci., 2026, 20(4): 2004801

阅读原文：



文章精要

自动链路建立(Automatic link establishment, ALE)技术为简化高频无线电系统通讯而生。HALFLOOP算法是一个可调分组密码，它已由美国国防部标准化以保护ALE传输信息。根据HALFLOOP现有攻击的分析显示，针对该密码结构本身的更强的非通用性攻击方法有待探索。

本文发现，HALFLOOP密码内部状态规模小于主密钥的特性导致其密钥调度算法的扩散性较弱。为此，针对HALFLOOP的两个大型变体，本文提出了相关密钥飞去来器攻击。这一成果不仅揭示了该标准密码的潜在设计缺陷，更为密钥扩展算法的安全性改进敲响警钟。

在研究过程中，本文融合理论分析与自动化工具，改进了针对非线性密钥扩展密码的三明治区分器的创新搜索模型。一方面突破传统简单线性关系约束，通过推导内部线性层更多约束条件提升搜索效率；另一方面克服非线性密钥扩展带来的障碍，有效规避弱密钥攻击甚至无效的区分器。

将该模型应用于HALFLOOP两个大型变体后，成功获取适用于密钥恢复攻击的三明治区分器，并通过实验验证了区分器的正确性。

HALFLOOP-48上密钥差分和相应的概率为的三明治区分器

本文最终在HALFLOOP 实施了近乎全轮的相关密钥飞去来器攻击。对于HALFLOOP-48，与之前的非通用方法相比，全轮攻击的时间复杂度有较大的提高。此外，本文还在HALFLOOP-96 上取得了突破，即9轮的非弱密钥攻击。未来工作可聚焦于探究具有类似结构的其他密码算法，并针对密钥扩展算法暴露的设计缺陷进行改进。

期刊简介

Frontiers of Computer Science (FCS) 是由教育部主管、高等教育出版社和北京航空航天大学共同主办，南京大学支持，SpringerNature 公司海外发行的英文学术期刊。本刊于 2007 年创刊，月刊，全球发行。主要刊登计算机科学领域具有创新性的综述论文、研究论文等。本刊主编为周志华院士，共同主编为熊璋教授。编委会及青年 AE

团队由国内外知名学者及优秀青年学者组成。本刊被 SCI、Ei、DBLP、INSPEC、SCOPUS 和中国科学引文数据库（CSCD）核心库等收录，为 CCF 推荐B类期刊；两次入选中国科技期刊国际影响力提升计划；入选第4届中国国际化精品科技期刊；两次入选中国科技期刊卓越行动计划（一期梯队、二期领军）。

Frontiers of Computer Science
2024 IF = 4.6

Fast and high quality peer review
Rapid publication upon acceptance
Fast Track of Revised Top Conference Submission

SCI (E), Ei
CCF B
Scopus, DBLP, INSPEC

Paper types

- Perspective/News/Highlights
- Review/Verspectives
- Research Article
- Letter/Obit

Subject areas (not limited to)

- Architecture
- Subarea
- Artificial intelligence
- Theoretical computer science
- Networks and communication
- Information systems
- Image and graphics
- Information security
- Interdisciplinary

Editorial Board

主编	副主编	副主编	执行编辑
周志华 南京大学	陈维良 北京航空航天大学	许可 北京航空航天大学	周磊 浙江大学
			陈为 浙江大学
			高磊 复旦大学
			廖小飞 华中科技大学
			廖峰 北京航空航天大学
			张健 中科院软件所
			张毅英 东南大学
			傅盛 复旦大学

在线投稿网址:
<https://mc.manuscriptcentral.com/fwpcfs>
Tel: +86(10) 8233 8176
E-mail: FCS@pub.hep.cn

Higher Education Press, Beihang University, Nanjing University, Springer

中国学术前沿期刊网

<http://journal.hep.com.cn>

来源：Frontiers of Computer Science

更多 科学进展 请访问 <https://www.iikx.com/news/progress/>

本文版权归原作者所有，请勿用于商业用途，[爱科学iikx.com](https://www.iikx.com)转发