西南交通大学学报 2010, 45(2) 302-307 DOI: 10. 3969/ j. issn. 0258-2724. ISSN: 0258-2724 CN: 51-1277/U

论文

AES 加密算法的密钥搜索量子线路设计

南京航空航天大学信息科学与技术学院, 江苏南京210016

摘要:

为验证量子搜索应用于分组密码密钥搜索的可行性,在分析AES 算法计算流程和需要实现的计算模块的基础上,设计了一种AES 算法密钥搜索的量子线路,包括密钥扩展KeyExpansion 模块、量子加密模块和量子比较模块. 其中,量子加密模块包含量子轮密钥加AddRoundKey、量子字节代换SubBytes、量子行移位ShiftRows 和量子列混淆MixColumns. 为了使辅助比特能被后续计算重用,采用回退计算方法去除量子纠缠,在实现量子加密模块时根据4 个子模块的不同计算任务采取相应的回退计算策略,以节省计算时间和量子存储空间. 研究结果表明:将量子搜索算法应用于分组密码的密钥穷举搜索攻击以达到二次方加速是可行的.

关键词: 量子线路设计 密钥搜索 AES 加密算法 回退计算

Key Search Quantum Circuit Design of AES Cipher

College of Information Science and Technology, Nanjing University of Aeronautics & Astronautics, Nanjing 210016,
China

Abstract:

In order to verify the feasibility of applying the quantum search to the key search of block ciphers, a key search quantum circuit of AES (advanced encryption standard) cipher was designed, including KeyExpansion module, encryption module and comparison module, based on the analyses of its computation processes and computation modules needed to be achieved. The encryption module includes four sub-modules, i. e. , quantum AddRoundKey, SubBytes, ShiftRows and MixColumns. In order to reuse the working quantum bits, the reversible computation is used to eliminate the quantum entanglement effect, and different methods of the reversible computation are adopted to different tasks of the 4 sub-modules in the realization of the quantum encryption module so as to save computation time and quantum memory. The research shows that applying the quantum search scheme to the key search of block ciphers to save square root time is feasible

Keywords: quantum circuit design key search AES cipher reversible computation

收稿日期 2008-06-02 修回日期 网络版发布日期

DOI: 10. 3969/ j. issn. 0258-2724.

基金项目:

通讯作者: 袁家斌(1968-),男,教授,主要研究方向为信息安全,电话:025-84893924,E-mail:jbyuan@ nuaa. edu. cn

作者简介:

参考文献:

本刊中的类似文章

文章评论 (请注意:本站实行文责自负, 请不要发表与学术无关的内容!评论内容不代表本站观点.)

反馈人		邮箱地址	
反馈标题		验证码	5453