AES 密钥扩展算法的研究

何　丰，王耀灯

（重庆邮电大学 光电工程学院，重庆 400065）

摘　要：高级加密标准(AES)的传统密钥扩展算法在已知某一轮密钥的情况下，包括初始密钥在内的所有轮密钥较容易破解.通过对加解密算法的实现方法与过程进行研究，针对原密钥扩展算法存在的缺点，利用采用单向性策略与随机数产生函数相结合的方法，对传统扩展算法进行改进.通过 Keil 软件模拟在 24 MHz 的工作环境下，对算法进行仿真测试，结果表明该方法能在保证密钥扩展算法安全性的同时保证算法高效运行.

关键词：高级加密标准；密钥扩展算法；随机数产生函数

Research on AES Key Expansion Algorithm

HE Feng，WANG Yao-deng

(School of Optoelectronic Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract：The traditional key expansion algorithm of the Advanced Encryption Standard(AES) is easy to be cracked under the condition that a certain round key is known. Through the research on the implementation method and the process of encryption and decryption algorithm, aiming at shortcomings of the key expansion algorithm are relatively easy to crack round key, by the methods of combine one-way strategy and random function , the key expansion algorithm is improved. And then simulation the algorithm through the Keil software in 24Mhz , The results show that this method is effective in ensuring the safety of the key expansion algorithm and can guarantee the efficient operation at the same time.

Key words：advanced encryption standard； key expansion algorithm；random function

作者简介：

何　丰　男，(1962 -)，教授，硕士生导师. 研究方向为电子电路、电工理论与新技术.

王耀灯(通讯作者)　男，(1988-)，硕士研究生.研究方向为电工理论与通信网技术.

E-mail：179923937@qq.com.