

AES 密钥扩展新方法

杨小东, 王 毅

(哈尔滨工业大学 深圳研究生院, 广东 深圳 518055)

摘 要: 在分析原有的 AES 算法密钥生成改进方法所存在的不足的基础上, 根据单向性思想提出了几种新的 AES 密钥扩展算法, 从加密强度和运行速度两方面对原有方法进行了改善. 通过分析以及实验数据表明, 该方法既保证了密钥扩展算法的安全性, 又提高了其运行的效率.

关键词: 密钥扩展, 单向性, AES 算法, 随机函数

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2012)01-0102-03

New Methods of AES Key Expansion

YANG Xiao-dong, WANG Yi

(Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen 518055, China)

Abstract: In this paper, based on the analysis of the shortcomings of the original key expansion method, some new methods for the key expansion algorithm of AES encryption algorithm are proposed according to the one-way property, which improved the original method in two aspects-encryption strength and running speed. Analysis and experimental data illustrated that the proposed methods not only guaranteed the security of the original algorithm but also improved its efficiency.

Key words: key expansion; one-way property; AES algorithm; random function

1 引言

AES 作为新一代数据加密标准, 其算法本身所具有的模块性、对称性等特点使设计者可以在修改其中的某一部分结构的同时不至于影响其他部分的正常运行. AES 采用了扩充初始密钥生成子密钥的方法, 通过对其密钥扩展算法的分析, 可知 AES 密码扩展具有直接高效并且快速的优点, 但是也有通过其中任何一轮子密钥即可破解全部密钥的缺陷, 可以通过分析的其中的某一轮子密钥得到前几轮的全部密钥, 也可通过得到的某一轮子密钥用固定算法推导出后一轮以致后面几轮所有的密钥^[1]. 逆向思维是进行密钥破解分析时需要有的思路, 如能够找到一种新方法, 使得算法运行中既可以保持在从前向后生成密钥时所具有的快速性^[2], 又能够使逆向推导密钥困难异常, 就可以防止各种攻击方法针

对 AES 密钥扩展的弱点, 仅通过截获其中任意一轮子密钥即可破解初始密钥的威胁. 这种使得密钥扩展过程不可逆的思想即称为单向性思路. 文献[1]利用单向性策略提出了一种 AES 密钥扩展改进方法, 本文对该算法进行了分析, 针对标准算法的不足之处^[3]提出了几种新的改进方法, 在保证安全性进一步提高的同时, 也加快了密钥扩展的效率.

2 对原有改进算法的分析

文献^[1]根据单向性策略提出了一种 AES 密钥扩展改进方法. 对该算法进行分析: 假设某一轮的密钥已经被攻击者获取, 推算攻击者已知 W_{i+4} , W_{i+5} , W_{i+6} , W_{i+7} , 推算出 W_i , W_{i+1} , W_{i+2} , W_{i+3} 所需付出的代价. 由于 W_{i+4} 与 W_i , W_{i+2} 相关, 可通过穷举法进行暴力攻击. W_i 的长度为 32 位, 可以通过 2^{32} 次穷举来确定 W_i 和 W_{i+2} . 确定 W_i 和 W_{i+2} 之

收稿日期: 2011-05-10; 修回日期: 2011-06-12

基金项目: 中央高校基本科研业务费专项资金项目(HIT. NSRIF. 2009134)

后,即可利用 W_i 和 W_{i+2} 推出 W_{i+1} , 利用 W_{i+2} 和 W_{i+1} 推出 W_{i+3} , 因此可以全部推出上一轮的密钥。这是由第三轮以及其以后轮数的密钥推断前边几轮密钥的情况,需要经过 2^{32} 次穷举。如果已知第二轮密钥,情况则有所不同, W_0, W_1, W_2, W_3 是初始密钥, 四行数组没有任何关系, 因此用 W_4 推出 W_0 和 W_2 之后, 还需用 W_5 推出 W_1 和 W_3 , 方可推出初始密钥, 因此, 已知第二轮密钥, 推断初始密钥需要 2^{64} 次穷举。如果攻击者得到了第三轮的子密钥, 需要用 2^{96} 次穷举来破解初始密钥, 如果攻击者得到了第四轮的子密钥, 则需要用 2^{128} 次穷举来破解初始密钥, 这已经同对密码的暴力攻击没有区别, 因此, 该方法对防止第四轮及其以后的子密钥攻击具有强力抗攻击作用, 对第三轮及其之前的子密钥攻击防御较弱。

3 算法的改进

针对 AES 密钥扩展算法的不足之处, 本文从抗攻击强度并兼顾程序执行时间方面做了改进, 提出几种新方法。

3.1 方法 1

为减小计算量, 取消 RootByte, SubWord 与 Rcon 算法, 令 W_i 每一位元素左移 a 位异或 W_{i+1} 每一位元素右移 c 位, 生成 W_{i+4} 对应元素, 令 W_{i+2} 左移 e 位异或 W_{i+3} 右移 g 位生成 W_{i+5} , 令 W_i 每一位元素右移 b 位异或 W_{i+1} 每一位元素左移 d 位, 生成 W_{i+6} 对应元素, 令 W_{i+2} 每一位元素右移 f 位异或 W_{i+3} 每一位元素左移 h 位, 生成 W_{i+7} 对应元素, 以此类推, 得到需要加密的所有轮次的子密钥。在算法具体实施过程中, 每一位数左移还是右移, 移动多少位, 均可随机选择, 并不局限于方法中所指出的具体位数。其算法原理图如图 1 所示。

算法分析: 根据原来的方法进行研究, W_{i+6} , W_{i+4} 只与 W_i 和 W_{i+1} 有关, W_{i+7} , W_{i+5} 只与 W_{i+2} 和 W_{i+3} 有关, 每一轮子密钥内部相关性不大。用 2^{32} 次穷举可通过 W_{i+4} 推断出 W_i 和 W_{i+1} , 用 2^{32} 次穷举可通过 W_{i+5} 推断出 W_{i+2} 和 W_{i+3} , 推断前一轮密钥共需要 2^{64} 次穷举。此种推断在任何一轮均相同, 任何一轮推断前一轮均需要 2^{64} 次穷举, 通过分析, 此种改进算法使得算法运行到第二轮时强度即可与暴力破解相同。

3.2 方法 2

方法 1 在改进效果上明显好于原有的方法, 但是仍未达到经过一轮变换即可使其自身抗攻击强度与对密钥直接进行暴力攻击的强度相同的目的。借

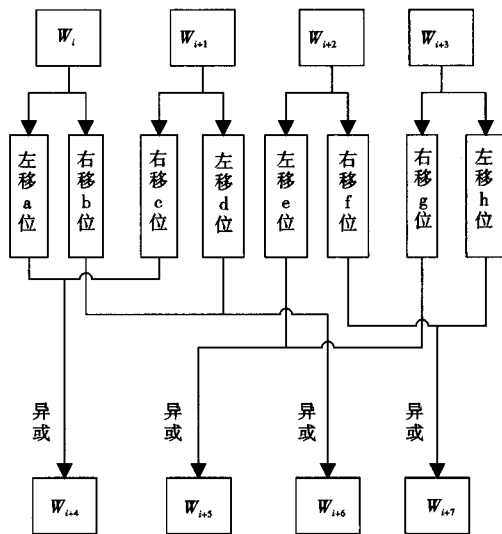


图 1 方法 1 原理图

助具有单向性或随机性的函数或能提高密钥扩展的强度。但凡有规律的单向函数, 或多或少具有倒推的方法与可能性, 而随机函数生成的值无法倒推^[4]。对此, 本方案引入随机函数, 本方法主要思想是对初始密钥各数值进行移位后相加, 生成的数值作为随机函数的种子, 生成下一轮的各个密钥。以此类推, 生成下面各轮密钥。在算法的具体应用中, 各轮各个数值移位的方向, 移位的位数均不同, 对生成的随机数也采用不同的密钥分配方法, 打乱原有的顺序, 加大生成子密钥的混乱程度, 使得攻击者没有分析的头绪, 该方法自身也没有逆向推导的策略, 因为其本身就成为随机函数。其原理图如图 2 所示。

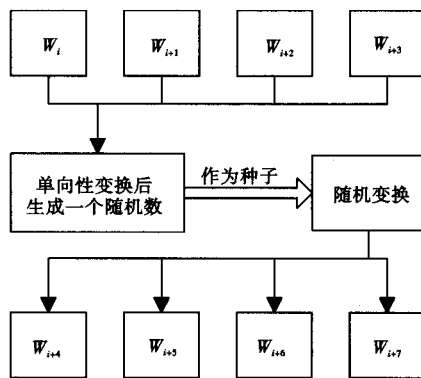


图 2 方法 2 原理图

算法分析: 每个元素与前边对应的元素均无关, 因此, 如欲推出前面的一轮的密钥, 只能对各值均进行 2^{32} 次穷举, 推出一轮密钥, 需要经过 2^{128} 次穷举。随机性是本方法最大的特点, 其特点使得攻击者无从下手, 正如 HIV 病毒在人体内复制一样, 具有强大的变异能力, 使任何一种单一的方法均无从下手,

唯有穷举法能成为对付此方法的鸡尾酒疗法. 本方法改进了策略 2 中提出的方法, 使得算法运行一轮时便需要 2^{128} 次穷举方可推出前一轮密钥, 其强度与暴力破解无异.

3.3 方法 3

方法 2 虽然在加强密钥强度方面做了大量工作, 但是其忽视了程序运行的效率问题. 随机数生成相对于其它程序而言运行时间很长, 攻击密钥的强度逐轮增大, 但经过一轮加密后, 其强度就已经达到要求, 所以没有必要付出效率的降低的代价来换取更高攻击强度的子密钥. 如能找到一种方法, 在提高密钥强度的基础上又能减少程序运行时间, 是本文所追求的最终目标. 在综合各方法的基础上, 本文提出第三种改进方法, 对密钥矩阵的初始 4 行赋予初始密钥, 这一步不变, 在第 5 到第 8 行用另一套与初始密钥无关的新密钥填充, 两套密钥不存在任何关系, 在新的密钥的基础上, 用 AES 固有的设计方法, 进行密钥扩展. 该方法原理图如图 3 所示.

算法分析: 攻击者可以按照文献[1]提出的方法进行攻击, 并且会很快推出经第一轮扩展生成的密钥, 但是由算法知, 第一轮扩展生成的密钥与初始密钥无任何关系, 由第一轮密钥推出子密钥仍需要 2^{128} 次穷举, 其强度仍与暴力攻击相同, 而且该方法极大节省了时间, 提高了效率, 对固有的 AES 算法亦仅做了一小部分改动, 避免了其它问题的发生, 该方法为一种兼顾安全与效率的好方法.

4 各改进方法综合分析

通过对各方法的分析, 可以做出各方法需要攻击强度与扩展轮数的关系, 如表 1 所示. 表中所列程

序运行时间为在 keil 环境中模拟 8MHz 下各方法所运行的时间. 从表中可以看出, 方法 2 美中不足之处在于其运行时间明显高于前边几种方法, 对程序运行的效率产生了一定影响. 方法 1 虽然有较快的运行速度, 但是其加密强度效果稍差. 如果对方方法 2 算法的步骤做一定简化, 亦可减少程序运行时间, 提高效率, 但强度与速度之间的矛盾是固有的, 加快速度就会使得安全性降低, 做简化处理, 需要对其安全度需重新评估. 方法 3 在 AES 固有的密钥扩展方法上进行改进, 不仅加快了程序运行速度, 也达到了 AES 密钥生成算法的安全性指标, 是一种较好的改进方法.

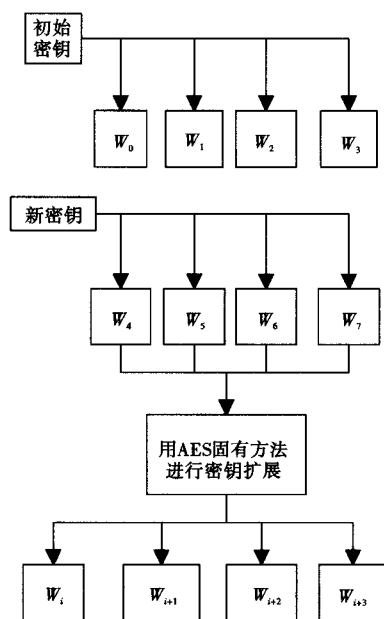


图 3 方法 3 原理图

表 1 改进方法对比表

方法	第一轮扩展后需要 穷举攻击次数	第二轮扩展后需要 穷举攻击次数	第三轮扩展后 需要穷举攻击次数	程序运行 所需时间(秒)
标准算法	0	0	0	0.05602956
方法 1	2^{64}	2^{128}	2^{128}	0.05359805
方法 2	2^{128}	2^{128}	2^{128}	0.14636865
方法 3	2^{128}	2^{128}	2^{128}	0.05293355

5 结束语

本文在原有的对密钥扩展改进算法的分析的基础上, 利用单向性策略, 提出了几种新的密钥扩展算法. 实验表明, 如只欲加强密钥生成的抗攻击强度,

对时间没有太多要求, 方法 2 是一种好方法; 如希望在不影响 AES 整体算法效率的同时, 也使得生成的子密钥具有高强度的抗攻击性, 方法 3 是一种较好的密钥扩展改进办法.

(下转第 108 页)

表 3 不同方法的准确率与耗时的对比

	耗时(ms)	准确率
基于元数据的判定方法	14857	45.6%
基于网页内容的语义判定方法	1876553	97.3%
本文方法	43449	95.4%

另外,使用文中提出的方法,分别对相关度高的、相关度低的以及不相关的网页进行了实验,实验结果如表 4 所示. 可以分析出:主题相关度越高的网页其相关度判定的准确率也越高,由于用户一般不会关注排名 50 之后的信息,因此,网页主题相关度低影响到判定准确率的问题几乎不会对用户造成影响.

表 4 本文方法针对不同类型数据的准确率

	主题相关度高的 Web 数据	主题相关度低的 Web 数据	不相关的 Web 数据
准确率	98.8%	81.5%	45.7%

5 结束语

高准确率和低耗时是相互矛盾的,本文提出的基于动态匹配的主题相关度算法在很大程度上减少了这种矛盾. 实验结果表明:从准确率和耗时相统一的角度,本文提出的方法达到了较好的效果.

参考文献:

[1] 中国互联网络信息中心. 第二十六次中国互联网络发

展状况统计报告[EB/OL]. [2011-05-28]. Retp://re-search. cnnce. cn/html.

[2] 王继成,萧嵘,孙正兴,等. Web 信息检索研究发展[J]. 计算机研究与发展, 2001,38(2): 187-193.

[3] F Menczer, G Pant, P Srinivasan, et al. evaluating Topic-Driven Web Crawlers [C]// Proceedings of the 24 Annual International ACM/SIGIR conference, New Orleans, USA; ACM, 2007.

[4] Cutler M, Shih Yung-ming, Meng Wei-yi. Using the structure of HTML documents to improve retrieval [C] // Proceedings of the 11st IEEE Conference on Tools with AI, CA, USA; IEEE, 2009;406-409.

[5] 韩先培. 基于布局特征与语言特征的网页主要内容块发现 [J]. 中文信息学报. 2008(1):15-21.

[6] 张天广. 基于 Internet 的银行竞争情报收集系统的研究与实现 [D]. 西安: 西北大学, 2009.

[7] Yi J, Sundaresan N. Metadata based web mining for relevance [C]// Proceedings of the In IEEE 2000 International Database Engineering and Applications Symposium (IDEAS'00) Yokohama; IEEE, 2010: 113-121.

[8] Bing Liu, Chee Wee Chin, Hwee Tou Ng. Mining topic-specific concepts and definitions on the web [C]// Proceedings of the 12th international conference on World Wide Web, NY, USA; ACM, 2003: 251-260.

[9] Sergey Brin. Extracting patterns and relations [J] Computer Science Department Stanford University, 2009: 172-183.

作者简介:

郑敏女, (1982—), 博士研究生, 讲师. 研究方向为搜索引擎复杂系统建模研究.

(上接第 104 页)

参考文献:

[1] 胡亮, 袁巍, 于孟涛, 等. 单向性策略与 AES 密钥生成算法的改进 [J]. 吉林大学学报:工学版, 2009, 39(1): 138-141.

[2] 景为平, 徐晨, 陈海进. AES 密码算法的结构优化与实现 [J]. 微电子学与计算机, 2007, 24(2): 36-38.

[3] 吴文玲, 冯登国. 分组密码工作模式的研究现状 [J]. 计算机学报, 2006, 29(1): 22-25.

[4] 闫茂德, 纪志强, 贺显曜, 等. AES 与 ECC 混合加密算法的无线数据通信系统设计 [J]. 微电子学与计算机, 2007, 24(7): 135-138.

作者简介:

杨小东 男, (1985—), 硕士. 研究方向为加密技术与无线通信.

王毅 男, (1966—), 博士, 博士生导师. 研究方向为电力电子及电气传动.