文章编号：0258-2724(2010)02-0302-06 DOI：10.3969/j.issn.0258-2724.2010.02.024

AES加密算法的密钥搜索量子线路设计

叶 峰， 袁家斌
（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
中图分类号：TP309.7 **文献标识码**：A

Key Search Quantum Circuit Design of AES Cipher

YE Feng， *YUAN Jiabin*
(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.

Key words: quantum circuit design; key search; AES cipher; reversible computation

物理学家Feynman于1982年首次提出的量子计算是一种依照量子力学理论进行的新型计算[1-4]. 量子计算机可以接受代表所有可能输入值的叠加态作为输入状态，然后同时对它们进行一系列么正变换以得到输出值的叠加态，这使得量子计算机可以同时计算函数$f(x)$在许多不同x处的值，这就是量子并行性[5]. 量子计算机能比经典计算机更有效地解决某些问题，例如分解大整数的量子算法[6]和量子搜索算法[7-10]，这两种量子算法分别对目前广泛使用的RSA[11]公钥密码算法和大多数私钥密码算法（如AES[12]算法）提出了严重挑战. 针对具体密码算法的量子密钥搜索线路设计的研究将使这种挑战更加接近现实.

量子计算机可以用量子线路或称量子计算网

收稿日期：2008-06-02
作者简介：叶峰(1974－)，男，博士研究生，研究方向为智能信息系统、信息安全，电话：13813828003，E-mail：yefeng_nuaa@china.com.cn
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

络来描述. 量子线路包含一组量子逻辑门和连接量子门的连线,每个量子门执行一个基本么正运算. 由于么正运算都是可逆运算,所以量子线路必须是可逆线路[13-16]. 量子线路可以执行经典计算并具有量子并行性,目前已经设计了量子加法器和量子乘法器等量子线路[17]. 另一方面,量子搜索算法是一个黑箱算法,针对密码算法的量子密钥搜索问题需要在权衡时间、空间效率的基础上实现相应的量子搜索线路. 这是因为在设计量子线路时,为了保持量子计算的可逆性并节约量子线路所必须的辅助比特,往往需要增加计算步骤.

本文研究量子搜索算法用于 AES (advanced encryption standard)加密算法的穷举密钥搜索,首先简要介绍 AES 加密算法流程及需要实现的计算部件,然后给出 AES 算法的密钥搜索量子线路设计.

1　AES 算法简介

高级加密标准(AES)是美国国家标准和技术研究所(NIST)于 2001 年 11 月发布的新一代密码标准,用来取代旧的数据加密标准(DES)和三重 DES 而成为美国联邦信息处理标准(FIPS PUB 197). 由于 AES 是 DES 的继承者,它自从被接纳为标准之日起就已经被银行业、行政部门和工业界作为事实上的密码标准[12].

AES 是一种迭代型分组密码,有着固定的轮函数和固定的分组长度(128 比特),但密钥长度可变. 本文为简便起见,采用常用的密钥长度(128 比特). 128 比特的明文分组和密文分组以字节为单位,可以看作是 16 个单元的一维字节数组,分别记为 $p[16]$ 和 $c'[16]$. 128 比特密钥也被看作为字节数组 $k[16]$,通过密钥扩展算法 KeyExpansion,扩展为 44 个字的扩展密钥字数组 $w[44]$.

AES 加密算法输入 $p[16]$ 和 $w[44]$,输出 $c'[16]$. 加密过程包含一次初始的轮密钥加 AddRoundKey,然后接着 9 轮完全相同的轮函数 Round,最后再进行一次结束轮函数 FinalRound 运算. AES 的轮数随着密钥长度变化,本文为简便起见只讨论密钥长度为 128 比特的情况. 轮函数 Round 包含 4 个步骤:字节代换 SubBytes、行移位 ShiftRows、列混淆 MixColumns 和轮密钥加 AddRoundKey. 结束轮函数 FinalRound 与轮函数 Round 的区别在于省去了列混淆 MixColumns. 由此可见,加密需要实现的计算部件只有 4 种:AddRoundKey、SubBytes、ShiftRows 和 MixColumns. 怎样在节约时、空资源的基础上,在量子计算机上实现这些部件并把它们有效组合在一起是本文研究的重点.

2　回退计算

由于量子计算是可逆计算,为了计算不可逆函数 $f(x)$,量子计算模块 U_f 需要引入辅助比特并产生后续计算不需要的垃圾比特[5]:

$$U_f(|x,a\rangle) = |f(x), g(x)\rangle. \tag{1}$$

U_f 把输入量子比特 $|x\rangle$ 和辅助量子比特 $|a\rangle$ 变换为输出量子比特 $|f(x)\rangle$ 和与输入值 x 相关的额外输出量子比特 $|g(x)\rangle$,辅助比特成为被污染的所谓“垃圾比特”. 开始时 $|x\rangle$ 和 $|a\rangle$ 处于非纠缠态,经过量子计算后,所有量子比特纠缠在一起,所以必须使用被称为“回退计算[18]”的技术把辅助比特置回它的初始值. 回退计算的方法是,在 U_f 完成计算任务后,把 $|f(x)\rangle$ 异或出来加以保存,然后再利用 U_f 的逆线路(记作 U_f^{-1})完全回退所有的计算过程. 其计算框图如图 1 所示,图中的短斜线表示一组量子比特.

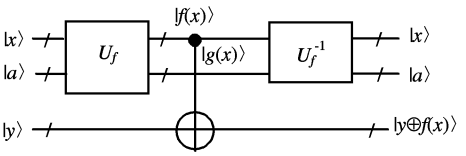

图 1　回退计算

Fig. 1　Reversing computation

在计算的前后,$|a\rangle$ 没有发生变化,且与其它量子比特不纠缠,在后续的计算中仍然可以被重复使用. 图 1 所示的量子线路的么正变换如式(2)所示,记为 U_f'.

$$U_f'(|x,y\rangle) = |x, y\oplus f(x)\rangle, \tag{2}$$

式中,省略了没有改变的 $|a\rangle$. U_f' 以可逆且没有垃圾比特的方式实现了 $f(x)$,量子比特 $|y\rangle$ 用来保存输出结果($f(x)$的值),其长度等于 $f(x)$ 的长度. 如果 $f(x)$ 本身是可逆的(隐含着输出比特数等于输入比特数),且后续计算不需要用到 x 的值,可以用 $|x\rangle$ 自身来存储 $|f(x)\rangle$,如式(3)所示.

$$U_f''(|x\rangle) = |f(x)\rangle. \tag{3}$$

3　AES 算法的密钥搜索量子线路设计

文献[5]给出了量子搜索算法的线路框图,要实现加密算法的密钥搜索量子线路,主要需设计实

现量子黑箱 Oracle 线路. 图 2 给出了密钥搜索量子线路的量子黑箱 Oracle. 图 2 中 $|x\rangle$ 是待搜索密钥空间所有元素的叠加态,$f(x)$ 是判断 x 是不是正确密钥的判定函数,其定义如式(4)所示.

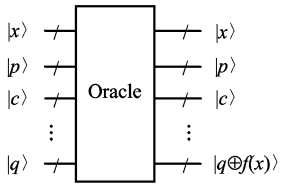

图 2 密钥搜索的量子黑箱 Oracle
Fig. 2 Quantum oracle of the key search

$$f(x)=\begin{cases}1, & e(p,x)=c'=c;\\ 0, & e(p,x)=c'\neq c.\end{cases} \tag{4}$$

式(4)中:x 为待搜索的密钥;p 为已知明文;c' 为加密密文;c 为已知密文;e 为加密函数;$|q\rangle$ 为单量子比特,起标记解的作用,它的初始值置为 $(|0\rangle-|1\rangle)/\sqrt{2}$. 明文量子比特 $|p\rangle$、密文量子比特 $|c\rangle$、一些辅助量子比特以及 $|q\rangle$ 在 Oracle 作用的前后都保持不变,且与 $|x\rangle$ 不纠缠. 于是总的效果是,如果 $f(x)=0$,则 $|x\rangle$ 保持不变;如果 $f(x)=1$,则 $|x\rangle$ 变成 $-|x\rangle$. 量子黑箱 Oracle 的么正变换(记为 O)为:

$$O(|x\rangle|p\rangle|c\rangle\cdots|q\rangle=(-1)^{f(x)}|x\rangle|p\rangle|c\rangle\cdots|q\rangle. \tag{5}$$

采用自顶向下、逐步求精的 AES 算法密钥搜索量子黑箱 Oracle 线路的详细设计如下.

图 3 是 AES 密钥搜索算法的量子黑箱 Oracle 线路框图,它实现图 2 的功能. 线路的输入包括:128 量子比特的 $|x\rangle$、$|p\rangle$、$|c\rangle$、用于存储扩展密钥 w 的辅助比特(长度为 44 个字,初始值为 $|0\rangle$)和初始化为 $(|0\rangle-|1\rangle)/\sqrt{2}$ 的 $|q\rangle$.

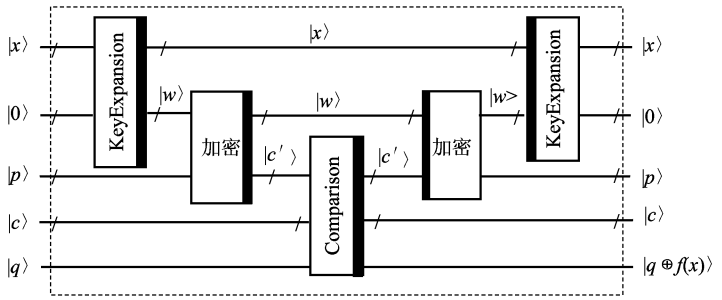

图 3 AES 的量子密钥搜索算法的量子黑箱 Oracle 线路框图
Fig. 3 Quantum oracle of the key search algorithm of AES

AES 算法包含一个密钥扩展函数 KeyExpansion,输入 $|x\rangle$,输出 $|w\rangle$(长度为 44 个字). $|w\rangle$ 和 $|p\rangle$ 作为输入一起送入 AES 的量子加密模块,加密模块将 $|p\rangle$ 变换成 $|c'\rangle$,并保持 $|w\rangle$ 不变. 接着,$|c\rangle$ 和 $|c'\rangle$ 被送入比较器 Comparison,经过比较形成判定函数 $f(x)$ 的值,并与 $|q\rangle$ 进行异或运算. 至此已经完成了预定的逻辑功能,但是作为辅助比特 $|0\rangle$ 和 $|p\rangle$ 已经被改变,并与 $|x\rangle$ 纠缠在一起. Oracle 线路依次回退计算加密模块和 KeyExpansion 模块,将辅助比特置回初始值. 注意图 3 中左边带黑色边条的模块是右边带黑色边条模块的逆模块,是把原模块中的所有基本量子逻辑门逆序排列而构造成的.

3.1 量子比较模块

量子比较模块 Comparison 的线路如图 4 所示. 图中 c 和 c' 的下标为比特序号;$|0\rangle$ 为辅助量子比特. 这里是以 3 量子比特为例, 128 量子比特可依此类推. 量子比较器用量子受控非门和量子非门

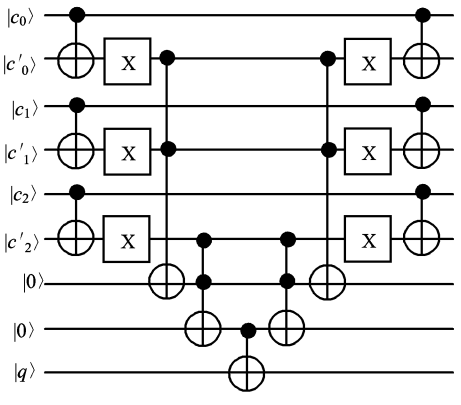

图 4 比较模块的量子线路
Fig. 4 Quantum comparison module

实现 $|c\rangle$ 与 $|c'\rangle$ 的逐位比较,再将位比较结果用 Toffoli 门逐位“与”在一起作为控制比特,$|q\rangle$ 作为目标比特,执行量子受控非运算. 接着进行回退计算,把输入量子比特 $|c'\rangle$ 和辅助量子比特 $|0\rangle$ 置回原值.

3.2　量子加密模块

图 5 是量子加密模块的线路框图. 量子加密模块对$|w\rangle$和$|p\rangle$进行运算,保持$|w\rangle$的值不变,并把$|p\rangle$的内容变换成$|c'\rangle$. 在量子加密模块中,只有轮密钥加 AddRoundKey 需要$|p\rangle$和$|w\rangle$参加计算,其它步骤都只针对$|p\rangle$. 限于篇幅,下面简要给出 4 个计算部件 AddRoundKey、SubBytes、ShiftRows 和 MixColumns 的量子线路设计.

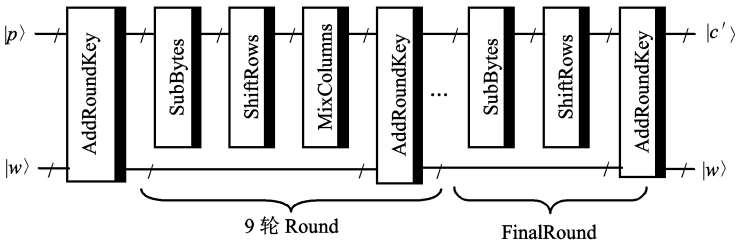

图 5　量子加密模块的线路框图
Fig. 5　Quantum encryption module

3.2.1　量子轮密钥加 AddRoundKey

AddRoundKey 运算把 128 量子比特$|p\rangle$与$|w\rangle$中对应该轮的 128 量子比特轮密钥位(占$|w\rangle$数组中的 4 个字)进行逐位异或(XOR)运算,这可以用 128 个量子受控非门并行排列来实现.

3.2.2　量子字节代换 SubBytes

SubBytes(记为 S)是字节查表操作,对$|p\rangle$的每个字节$|p[i]\rangle$($0\leqslant i<16$)分别进行 S 盒查表运算. AES 定义了一个 S_{RD}表,为 16×16 字节的矩阵. 通过量子寻址方案[5],量子查表可以对经典内存中的 S_{RD}表进行叠加态查表操作,把以$|p[i]\rangle$为地址的内存单元的值$|S_{\mathrm{RD}}(p[i])\rangle$按位异或到数据比特$|0\rangle$. 为了用$|p\rangle$本身保存查表值,对查表结果先交换$|p[i]\rangle$和数据比特的值,量子交换门 Swap(记为 W)用 3 个量子受控非门实现,然后再进行量子逆 S 盒查表 InvSubBytes(记为 I)操作,逆 S 盒 S_{RD}^{-1}的表值根据 S_{RD}表预先计算好,由于 $S_{\mathrm{RD}}^{-1}(S_{\mathrm{RD}}(x))=x$,所以:

$$\begin{aligned}&I(W(S(|p[i],0\rangle)))=\\&\quad I(W(|p[i],0\oplus S_{\mathrm{RD}}(p[i])\rangle))=\\&\quad I(|S_{\mathrm{RD}}(p[i]),p[i]\rangle)=\\&\quad |S_{\mathrm{RD}}(p[i]),p[i]\oplus S_{\mathrm{RD}}^{-1}(S_{\mathrm{RD}}(p[i]))\rangle=\\&\quad |S_{\mathrm{RD}}(p[i]),0\rangle.\end{aligned}$$

从上式可知,数据比特$|0\rangle$在计算前后没有改变,可视为内部辅助比特.

3.2.3　量子行移位 ShiftRows

行移位 ShiftRows 是字节换位操作,如图 6 所示,输入和输出都是 16 个字节的一维字节数组 p.

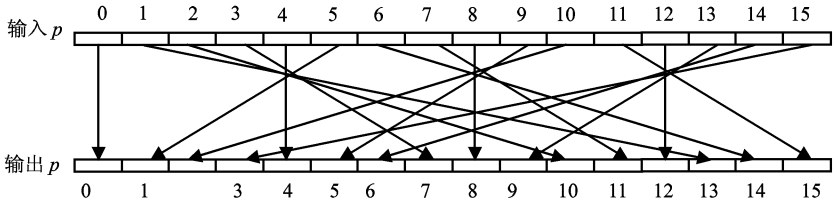

图 6　行移位变换
Fig. 6　ShiftRows transform

由此可以看出一些循环拷贝链: 0→0; 1→13→9→5→1; 2→10→2; 3→7→11→15→3; 4→4; 6→14→6; 8→8; 12→12. 根据循环拷贝链可以构造出如图 7 所示的行移位 ShiftRows 的量子线路,图中每条线代表一个字节,字节与字节之间的交叉连线是量子交换门,由 8 个量子比特交换门组合而成. 图 7 的量子线路没有用辅助比特,并且用$|p\rangle$本身保存结果.

3.2.4　量子列混淆 MixColumns

列混淆 MixColumns(记为 M)对明文数组通过 4 个不同的线性变换得到输出值. 为了用$|p\rangle$本身保存列混淆的结果,先用辅助比特(初始化为$|0\rangle$,长度为 128 量子比特)保存列混淆的输出,然后交换$|p\rangle$和辅助比特的值,再进行逆向逆列混淆,如图 8 所示.

图 8 中有两点需要说明:(1) 定义号右边的 MixColumns 与定义号左边的 MixColumns 是不同的,右边是单输入输出,左边是双输入输出;(2) 逆列混淆 InvMixColumns(记为 C)是列混淆 MixColumns 的逆变换,而逆向逆列混淆(左边带黑

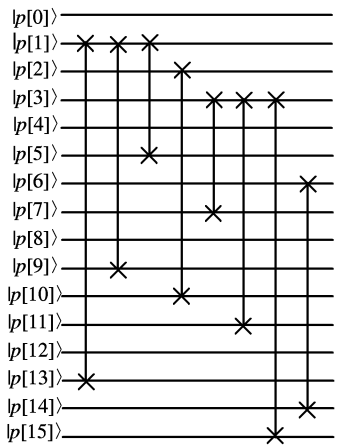

图 7 量子行移位
Fig. 7 Quantum ShiftRows

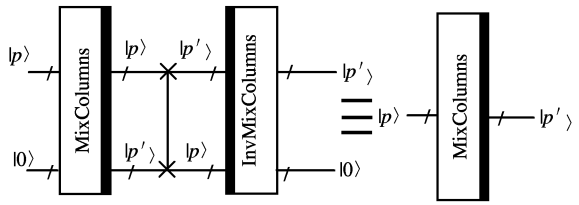

图 8 列混淆模块框图
Fig. 8 Quantum MixColumns

色边条表示逆向)是逆列混淆的基本逻辑门逆向排列. 式(6)是图 8 的么正变换式, C 的上标 -1 表示么正逆变换.

$$C^{-1}(W(M(|p,0\rangle))) = C^{-1}(W|p,p'\rangle)) = C^{-1}(|p',p)\rangle = |p',0\rangle. \quad (6)$$

限于篇幅 MixColumns 的详细量子线路将在后续文章中给出.

4 结束语

本文研究 Grover 量子搜索算法用于经典密码算法 AES 的密钥搜索问题,给出量子搜索线路中最重要的量子黑箱 Oracle 线路设计. AES 的量子黑箱线路主要包括 3 个模块:KeyExpansion 模块、加密模块和比较模块 Comparison,而量子加密模块又包含 4 个子模块:量子 AddRoundKey、量子 SubBytes、量子 ShiftRows 和量子 MixColumns,限于篇幅,本文只给出加密模块和比较模块的量子线路设计.

在各个模块的量子线路设计过程中,主要考虑如何将经典计算转换成可逆量子计算,并平衡空间资源(辅助量子比特)和时间资源(额外计算步骤). 因为在量子计算过程中,纠缠效应会使辅助比特被污染,需要用回退计算的方法去纠缠,而回退计算需要额外的计算步骤,应该根据不同的计算任务采取合理的回退计算策略.

针对同一个计算任务,可以有许多不同的计算方法和线路设计策略,总的目标是尽可能节省辅助比特和计算步骤. 本文是经典密码密钥搜索量子线路设计的初次研究,文中线路不一定是最优的,今后将在此基础上给出更加节省时空资源的量子线路设计. 后续文章也将给出 KeyExpansion 模块线路设计.

参考文献:

[1] FEYNMAN R. Simulating physics with computers[J]. Int. J. Theor. Phys., 1982, 21(6): 467-488.

[2] 吴楠,宋方敏. 量子计算与量子计算机[J]. 计算机科学与探索,2007,1(1): 1-16.
WU Nan, SONG Fangmin. Quantum computing and quantum computers[J]. Journal of Frontiers of Computer Science and Technology, 2007, 1(1): 1-16.

[3] OKSIN M, CHONG F, CHUANG I. A practical architecture for reliable quantum computers[J]. IEEE Computer, 2002, 35(1): 79-87.

[4] 吴楠,宋方敏. 一种高效、容错的通用量子计算机体系结构[J]. 计算机学报,2009,32(1): 161-168.
WU Nan, SONG Fangmin. A novel kind of architecture with high-efficiency and error-tolerance of universal quantum computer[J]. Chinese Journal of Computers, 2009, 32(1): 161-168.

[5] NIELSEN M A, CHUANG I L. 量子计算和量子信息(一)——量子计算部分[M]. 赵千川译. 北京:清华大学出版社,2004: 29-247.

[6] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM J. Comp., 1997, 26(5): 1484-1509.

[7] GROVER L K. Quantum mechanics helps in searching for a needle in a haystack[J]. Phys. Rev. Lett., 1997, 79(2): 325-329.

[8] GROVER L K. Quantum computers can search rapidly by using almost any transformation[J]. Phys. Rev. Lett., 1998, 80(29): 4329-4332.

[9] BIHAM O, SHAPIRA D, SHIMONI Y. Analysis of Grover's quantum search algorithm as a dynamical system[J]. Phys. Rev. A, 2003, 68(2): 2326-2333.

[10] 李盼池,李士勇. 一种 Grover 量子搜索算法的改进策略[J]. 智能系统学报,2007,2(1): 35-39.
LI Panchi, LI Shiyong. An improved measure in

(下转第 316 页)