AES-128 中 S 盒变换的量子线路优化

刘建美[1,2]，王 洪[1,2*]，马 智[1,2]，段乾恒[1,2]，费洋扬[1,2]，孟祥栋[1,2]

（1. 数学工程与先进计算国家重点实验室，郑州 450001；2. 河南省网络密码技术重点实验室，郑州 450001）

摘要 使用空间资源优化的量子 Karatsuba 乘法来优化实现 AES-128 中的8×8 S 盒变换，同时引入了衡量时间资源代价和空间资源代价折衷的指标——量子比特数目与 T 门深度之积。对实现8×8 S 盒变换的分析表明，利用空间资源优化的量子 Karatsuba 乘法的求乘法逆线路具有更优性能，其 Toffoli 门数目、量子比特数目、量子比特数目与 T 门深度之积更优。此外，使用加窗量子查表方法，进一步优化了求乘法逆以及实现 S 盒所需的量子资源。在此基础上，基于 Qiskit 分析验证了所需的量子资源。

关键词 乘法逆；优化实现；量子线路；S 盒

中图分类号 TP301 **文献标志码** A DOI 10.12178/1001-0548.2022346

Quantum Circuit Optimization for the S-Box of AES-128

LIU Jianmei[1,2], WANG Hong[1,2*], MA Zhi[1,2], DUAN Qianheng[1,2], FEI Yangyang[1,2], and MENG Xiangdong[1,2]

(1. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China;
2. Henan Key Laboratory of Network Cryptography Technology, Zhengzhou 450001, China)

Abstract With the help of the space-efficient quantum Karatsuba algorithm for multiplication, the quantum implementation for the 8×8 S-box of AES-128 has been optimized. At the same time, the product of the number of qubits and the depth of T gates has been introduced to measure the tradeoff between time resource cost and space resource cost. It has been shown in the analysis of the implementation of the 8×8 S-box transformation that the circuit using the space-efficient quantum Karatsuba multiplication to find the multiplication inverse has better performance, and all of the number of Toffoli gates, the number of qubits, and the product of the number of qubits and the depth of T gates are all better. Furthermore, the method of windowed quantum lookups has been used in this paper to optimize the resource cost for implementing the multiplication inverse and the S-box. Based on them, the resource needed has been analyzed and verified in Qiskit.

Key words multiplication inverse; optimization; quantum circuit; S-box

AES 是一种分组加密的标准算法，它有 3 种最常见的方案，分别是 AES-128、AES-192 和 AES-256，区别在于密钥长度不同。AES 加密算法分为轮函数和密钥扩展函数两部分。轮函数中的字节代换和密钥扩展函数中的字代换涉及非线性变换，在 AES-128 算法中字节代换和字循环左移操作分别由 16 个和 4 个 8 比特输入/输出的 S 盒构成。

利用量子的特性来有效地解决密码学领域中的计算难题，是计算机科学和密码学研究的新方向。与量子图灵机模型等价的量子线路模型能够清晰、直观地模拟量子信息处理的过程，对设计量子计算装置和新的量子算法都有很好的指导作用。针对量子算法对应的量子线路进行资源优化设计，有助于进一步降低量子算法对量子计算资源的需求，实现量子资源与量子算法复杂度的折衷。

Grover 算法可用于对称密码的密钥搜索攻击，与经典搜索相比有平方加速的效果。因此，对 Grover 算法攻击 AES 时所需的量子资源进行更准确的估计，有利于评估 AES 算法在量子设备上的安全性能，为抗量子密码的设计提供参考。

在 AES 算法的量子实现过程中，S 盒占据了

收稿日期：2022−10−13；修回日期：2022−12−05
基金项目：国家自然科学基金（61972413, 61901525, 62002385）
作者简介：刘建美，博士生，主要从事量子算法与线路优化方面的研究。
*通信作者 E-mail: redwang@meac-skl.cn

大部分的计算资源，因此研究 S 盒的有效量子线路实现是当前热点。经典的 AES 算法通常使用查表法，采用经典线路实现 S 盒变换，需要消耗大量的存储资源，而且延时较长。利用量子线路模型，借助量子门线路优化实现 S 盒，是值得研究的方向。

S 盒实现中求乘法逆的操作耗费了大量的计算资源，因此可以利用量子计算的优势设计量子线路使得求逆操作更加高效。其中，一个比较理想的方案是基于伊藤−辻井（Itoh-Tsujii）算法[1] 来进行求逆操作。Itoh-Tsujii 算法利用了这样一条性质：在正规基表示中，“平方对应系数的一个置换”。因为映射$\xi \mapsto \xi^{2^i}$是F_2上的双射，所以可用一个合适的非奇异$n\times n$矩阵进行矩阵与向量的乘法来实现该映射。其中，矩阵中的元素是属于F_2的。然后，借助该矩阵的 LUP 分解和若干次乘法操作来实现需要的求逆。文献 [2] 提出了用 Grover 算法攻击 AES 算法的量子线路并给出了其整体耗费的量子资源，并指出：执行求逆操作时用文献 [3] 的乘法能比文献 [4] 的乘法节省 60% 的量子比特数目，代价是增加了门数目和门深度。

当前，在基于量子计算的密码分析领域中，设计或优化量子线路时主要关注的是量子线路深度，特别是 T 门深度，原因如下：在含噪声中等规模量子（NISQ）时代，通过增加适当规模量子比特但能优化量子线路深度的方案比那些为降低量子比特数目而增加过多量子门和线路深度的方案[2, 5-6] 更有利；支配容错量子计算所需时间的是 T 门深度，而非量子门数目、线路深度或测量深度[7]。

美国国家标准技术研究所（NIST）用关于 AES 的量子线路的复杂性（线路深度的界，被称为 MAXDEPTH）作为基准将后量子密码方案分成不同的安全等级，呼吁后量子密码标准化。为了进一步实现量子线路中空间资源代价和时间资源代价的更好折衷，文献 [8-9] 用量子比特数目与 T 门深度之积（Qubits-Depth）作为时间资源花费和空间资源消耗的权衡指标来衡量量子线路的优劣。文献 [10] 提出了在 Karatsuba 乘法的基础上用亚平方深度规模 ($O(n^{\log_2 3})$) 的 Toffoli 门实现乘法线路，同时所用的量子比特数目最优（$3n$个）。

本文引入指标 Qubits-Depth 对文献 [10]、文献 [3] 和文献 [4] 的乘法线路作了全面的量子资源代价比较，发现：在 S 盒中求乘法逆的量子线路的时间资源代价和空间代价折衷方面，本文的求乘法逆线路更优。此外，本文用加窗查表方法进一步减少了求乘法逆以及 S 盒实现所需要的量子乘法次数。

1　三种乘法量子线路实现的资源对比

平方深度的乘法线路[3] 通过定义一个上三角矩阵 $\boldsymbol{U}$、一个下三角矩阵 $\boldsymbol{L}$ 和一个矩阵 $\boldsymbol{Q}$ 来实现 $\boldsymbol{c}\equiv\boldsymbol{a}\cdot\boldsymbol{b} \bmod m(x)$。其中：

$$\boldsymbol{U}=\begin{pmatrix} 0 & a_{n-1} & a_{n-2} & \cdots & a_2 & a_1 \\ 0 & 0 & a_{n-1} & \cdots & a_3 & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{n-1} & a_{n-2} \\ 0 & 0 & 0 & \cdots & 0 & a_{n-1} \end{pmatrix}$$

$$\boldsymbol{L}=\begin{pmatrix} a_0 & 0 & 0 & \cdots & 0 & 0 \\ a_1 & a_0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-2} & a_{m-3} & a_{m-4} & \cdots & a_0 & 0 \\ a_{n-1} & a_{m-2} & a_{m-3} & \cdots & a_1 & a_0 \end{pmatrix}$$

$$\left(x^n, x^{n+1}, \cdots, x^{2n-2}\right)^{\mathrm{T}} = \boldsymbol{Q}\cdot\boldsymbol{x}$$

$$\boldsymbol{x} = \left(1, x^1, \cdots, x^{n-1}\right)^{\mathrm{T}}$$

$$\boldsymbol{d} = \boldsymbol{L}\cdot\boldsymbol{b} \quad \boldsymbol{b} = (b_0, b_1, \cdots, b_{n-1})^{\mathrm{T}}$$

$$\boldsymbol{e} = \boldsymbol{U}\cdot\boldsymbol{b} \quad \boldsymbol{c} = \boldsymbol{d} + \boldsymbol{Q}^{\mathrm{T}}\boldsymbol{e}$$

文献 [3] 中的乘法所用量子比特数目为$3n$，Toffoli 门数目为n^2。

文献 [4] 提出亚平方深度规模 ($O(n^{\log_2 3})$) 的乘法线路，代价是增加了量子比特的数目：其所用量子比特数目为$O(n^{\log_2 3})$，Toffoli 门数目为$n^{\log_2 3}$。

文献 [10] 的乘法对应的量子线路需要的 Toffoli 门数目和 Toffoli 门深度规模为$O(n^{\log_2 3})$，量子比特数目规模为$O(n)$，图 1 为$n=4$时$F_2[x]/(1+x+x^4)$中两个多项式$f(x)=f_0+f_1x+f_2x^2+f_3x^3$和$g(x)=g_0+g_1x+g_2x^2+g_3x^3$相乘的量子线路，将$f(x)\cdot g(x) \bmod m(x)$的结果存到$h(x)$所在的寄存器中，图 1 中$m(x)=1+x+x^4$。

文献 [2] 用的是文献 [3] 提出的乘法，该乘法比文献 [4] 的乘法需要的量子比特数目少，但增加了对量子门数目和量子门深度的需求。

为了进一步实现空间资源代价和时间资源代价之间的折衷，本文引入量子比特数目与 T 门深度之积这个指标对文献 [10]、文献 [3] 和文献 [4] 的乘法线路作了全面的量子资源代价比较。对比结果如表 1 所示。

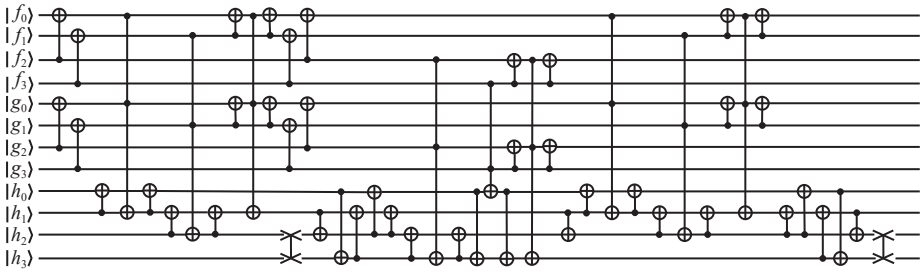

图 1 $f(x)\cdot g(x) \mod (x^4+x+1)$的量子线路

表 1 乘法量子线路资源消耗对比

量子资源	文献	Field size 2^n			复杂度
		n=4	n=8	n=16	
Toffoli Gates	[10]	9	27	81	$O(n^{\log_2 3})$
	[3]	16	64	256	$O(n^2)$
	[4]	9	27	81	$O(n^{\log_2 3})$
Qubits	[10]	12	24	48	$O(n)$
	[3]	12	24	48	$O(n)$
	[4]	17	30	113	$O(n^{\log_2 3})$
Qubits-Depth	[10]	432	2 592	15 552	$O(n^{1+\log_2 3})$
	[3]	768	6 144	49 152	$O(n^3)$
	[4]	612	3 240	36 612	$O(n^{2\log_2 3})$

从表 1 可以看出，随着n规模的增大，文献 [10] 的乘法线路在时空资源折衷方面比文献 [3] 和文献 [4] 更优。

2 求乘法逆的量子线路优化

AES 算法中唯一的非线性变换由 S 盒构成，实现 S 盒变换中的求乘法逆操作耗费了大量的计算资源。因此，可以借助量子计算的优势设计基于伊藤−辻井（Itoh-Tsujii）算法的量子线路，从而使得求逆操作更加高效。将一个字节看作有限域 GF(2^8) 上的元素，映射到其乘法逆元（令“00”的乘法逆元映射到它本身）。其中，有限域 GF(2^8) 的不可约多项式为 $m(x)=1+x+x^3+x^4+x^8$。假设一个字节的状态为：

$$\alpha \in \mathrm{F}_2[x]/(1+x+x^3+x^4+x^8)$$

借鉴文献 [11] 的思想，计算：

$$\alpha^{-1}=\alpha^{254}=((\alpha\cdot\alpha^2)\cdot(\alpha\cdot\alpha^2)^4\cdot(\alpha\cdot\alpha^2)^{16}\cdot\alpha^{64})^2$$

因此，有限域 GF(2^8) 中的求乘法逆操作可以转化成 6 次乘法操作和 14 次平方操作。

文献 [3] 提出的乘法线路所需要的 Toffoli 门数目和 Toffoli 门深度均为$O(n^2)$，量子比特数目为$O(n)$；文献 [4] 提出的乘法线路所需要的 Toffoli 门数目和 Toffoli 门深度均为$O(n^{\log_2 3})$，量子比特数目为$O(n^{\log_2 3})$。本文采用文献 [10] 的乘法，并给出了其对应的量子线路（见图 1）。

因为映射$\xi\mapsto\xi^2(\xi\in\mathrm{GF}(2^8))$是 GF($2^8$) 上的双射，所以可原位存放平方后的结果（用$g(x)$平方模$m(x)$后所得多项式的系数信息替代$g(x)$的系数信息）。利用 GF($2^8$) 上的平方运算是线性映射这一事实，可将平方对应的映射写成一个8×8矩阵。使用 LUP 矩阵分解方法对该矩阵进行分解，得到一个下三角矩阵、一个上三角矩阵和一个置换矩阵，从而可以转化成一个包含若干个交换门和至多$8^2-8=56$个 CNOT 门的线路。

在真正的物理实现中，实现量子线路所需的 T 门数目是值得特别关注的：对大多数容错量子计算方案而言 T 门的实现是通过所谓的魔幻态提纯（该过程花费大量物理资源，比较昂贵）来完成的，在表层编码中认为一个 T 门的花费大约是 CNOT 门的 100 倍[12]，因此 T 门数目越少越好。因此，考虑容错量子计算的实现方案，乘法线路耗费的物理资源比平方线路昂贵得多。

本文用加窗查表方法来减少求乘法逆过程中乘法操作的次数：用“查表法”将多个操作合并在一起，通过增加一定的预计算量、减少乘法操作的次数来提高求逆操作的运算速度。在量子计算中，许多情况下可以把多个操作合并成一个操作，索引由 QROM（量子只读存储器）查表产生的值。量子只读存储器（QROM）的目的是：读取被量子寄存器索引的经典值。查表加法是这样一种加法：需要加到寄存器中的值是在一个表中查询所得的结果，由量子寄存器从一个经典表格里进行数据寻址。其中，表中的值要无条件地加到目标比特上。

3 优化后实现 S 盒所需的资源估计

使用优化后的量子乘法线路，对乘法求逆操作以及 S 盒量子线路实现中需要的量子比特数目、

Toffoli 门数目、Toffoli 门深度以及量子比特数目与 T 门深度之积（Qubits-Depth）进行资源估计。可以将费马小定理用到特征为 2 的有限域的求逆操作中，借助平方操作通过n次乘法和$n-1$次平方达到求逆的目的。1988 年 Itoh 和 Tsujii 对求逆操作中所需的乘法次数进行优化，使其降到$2\log_2 n$以下（具体地，需要$\lfloor\log_2(n-1)\rfloor+t-1$次乘法。其中，$t$为$n-1$的汉明重量，$t\leqslant\lfloor\log_2(n-1)\rfloor+1$）。

以不可约多项式$m(x)=x^4+x+1$构造的有限域 GF(2^4) 中多项式$f(x)$的求逆操作的量子线路如图 2 所示。

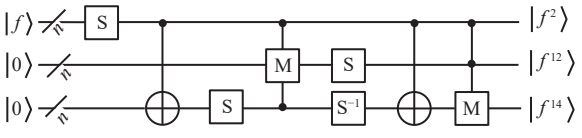

图 2　计算$f^{-1}\ \mathrm{mod}\ (x^4+x+1)$的量子线路

图 2 中 S 表示平方操作（squaring），S^{-1} 表示撤销平方操作的逆运算（the uncomputation of the squaring），M 表示乘法操作（multiplication）。

3.1　未使用加窗查表时实现 S 盒所需量子资源

在量子线路情形下，求逆需要的 Toffoli 门数目和 Toffoli 门深度均为：

$$n^{\log_2 3}(\lfloor\log_2(n-1)\rfloor+t-1)$$

需要的辅助量子比特数目为：

$$n\cdot\max(\lfloor\log_2(n-1)\rfloor+t-1,\lfloor\log_2(n-1)\rfloor+1)$$

总共需要的逻辑量子比特数目为：

$$n+n\cdot\max(\lfloor\log_2(n-1)\rfloor+t-1,\lfloor\log_2(n-1)\rfloor+1)$$

量子比特数目与 T 门深度之积为：

$$4n^{1+\log_2 3}(\lfloor\log_2(n-1)\rfloor+t-1)\cdot[1+\max(\lfloor\log_2(n-1)\rfloor+t-1,\lfloor\log_2(n-1)\rfloor+1)]$$

AES-128 算法中 S 盒变换为一个 8 比特输入、8 比特输出的变换，本文实现一个8×8 S 盒变换需要的量子比特数目为 40、Toffoli 门数目为 108、量子比特数目与 T 门深度之积为 17 280；采用文献 [2] 的量子线路进行一次 S 盒变换需要的量子比特数目为 40、Toffoli 门数目为 256、其量子比特数目与 T 门深度之积为 81 920。可以看出，本文所用的乘法线路实现 S 盒变换时在时空资源折衷方面比文献 [2] 更优。

3.2　使用加窗查表后实现 S 盒所需量子资源

使用加窗查表后，执行求乘法逆操作时需要的乘法操作由之前的$\lfloor\log_2(n-1)\rfloor+t-1$次变为$(\lfloor\log_2(n-1)\rfloor+t-1)/c_{\mathrm{mul}}$次，该优化所需要的代价是：要查找一个大小为$c_{\mathrm{mul}}$的表。其中，每次查表需要的 T 门数目和测量深度[13] 都为$2^{c_{\mathrm{mul}}}\cdot4$。求乘法逆的量子线路所需 T 门数目和 T 门深度分别为：

$$(7n^{\log_2 3}+4\cdot2^{c_{\mathrm{mul}}})(\lfloor\log_2(n-1)\rfloor+t-1)/c_{\mathrm{mul}}$$

$$(4n^{\log_2 3}+4\cdot2^{c_{\mathrm{mul}}})(\lfloor\log_2(n-1)\rfloor+t-1)/c_{\mathrm{mul}}$$

可以看出，使用加窗后比不使用加窗操作时 T 门数目和 T 门深度要小。

在 AES-128 中实现 S 盒时可令$c_{\mathrm{mul}}=2$，则得 T 门数目和 T 门深度分别为 410 和 248。量子比特数目为 42，量子比特数目与 T 门深度之积为 10 416。通过增加一定的预计算量，进一步实现了空间资源代价和时间资源代价之间的折衷。

4　实验仿真结果

本文使用 Qiskit 量子计算模拟平台，对提出的 S 盒量子线路实现中需要的量子比特数目、Toffoli 门数目、T 门深度以及量子比特数目与 T 门深度之积（Qubits-Depth）进行资源估计的数值模拟，并与文献 [2] 中 S 盒量子线路实现所消耗的量子资源做了对比。

两种 S 盒实现方式的量子线路资源消耗的实验仿真对比结果如表 2 所示。

表 2　8×8 S 盒量子线路资源消耗对比

量子资源	本文	文献[2]
Toffoli gates	108	256
qubits	41	41
qubits-depth	17 712	41 984

从表 2 可以看出，本文乘法线路实现 S 盒时的量子资源消耗的模拟仿真结果与理论值符合。

使用加窗查表操作后，在 AES-128 中实现 S 盒时令$c_{\mathrm{mul}}=2$，数值模拟得：本文方案所需的 T 门数目和 T 门深度分别为 410 和 248，量子比特数目为 43，量子比特数目与 T 门深度之积为 10 664；文献 [2] 方案所需的 T 门数目和 T 门深度分别为 928 和 272，量子比特数目为 43，量子比特数目与 T 门深度之积为 23 392。如表 3 所示。

加窗查表后实现 S 盒时量子资源消耗的模拟仿真结果与理论值符合。

表 1、表 2、表 3 中 Qubits-Depth 指的是量子

比特数目与 T 门深度之积，而本文中的 Toffoli 门实现时采用文献 [14] 中 T 门深度为 4 的方案。

表 3 加窗后实现 8×8 S 盒量子资源消耗对比

量子资源	本文	文献[2]
Toffoli gates	59	133
qubits	43	43
qubits-depth	10 664	23 392

5 结束语

本文使用空间资源优化的量子 Karatsuba 乘法来优化实现 AES-128 中的8×8 S 盒变换，同时引入量子比特数目与 T 门深度之积来衡量时间资源代价和空间资源代价的折衷；对比发现，基于空间资源优化的量子 Karatsuba 乘法在实现8×8 S 盒变换中的求乘法逆操作时，Toffoli 门数目、量子比特数目、量子比特数目与 T 门深度之积更优。此外，本文使用加窗查表方法使得求乘法逆以及实现 S 盒所需的量子资源更加优化。

下一步的研究方向是考虑 AES 算法中列混合的优化实现以及考虑含噪声条件下 AES 算法各部件面向现实量子设备的量子线路优化、结合 Grover 算法和实际芯片拓扑结构对现实量子计算设备上 AES 整体算法的性能做出评估。

参 考 文 献

[1] ITOH T, TSUJII S. A fast algorithm for computing multiplicative inverses in GF(2^m) using normal bases[J]. Information and Computation, 1988, 78(3): 171-177.

[2] GRASSL M, LANGENBERG B, ROETTELER M, et al. Applying grover ’s algorithm to AES: Quantum resource estimates[C]//2016 7th International Conference on Post-Quantum Cryptography (PQCrypto 2016). Cham: Springer, 2016: 29-43.

[3] MASLOV D, MATHEW J, CHEUNG D, et al. An O(m^2)-depth quantum algorithm for the elliptic curve discrete logarithm problem over GF(2^m)^a[J]. Quantum Information & Computation, 2009, 9(7): 610-621.

[4] KEPLEY S, STEINWANDT R. Quantum circuits for F_{2^n}-multiplication with subquadratic gate count[J]. Quantum Information Processing, 2015, 14(7): 2373-2386.

[5] ALMAZROOIE M, SAMSUDIN A, ABDULLAH R, et al. Quantum reversible circuit of AES-128[J]. Quantum Information Processing, 2018, 17(5): 1-30.

[6] LANGENBERG B, PHAM H, STEINWANDT R. Reducing the cost of implementing the advanced encryption standard as a quantum circuit[J]. IEEE Transactions on Quantum Engineering, 2020, 1(2500112): 1-12.

[7] FOWLER A G. Time-optimal quantum computation [EB/OL]. [2022-7-29]. https://api.semanticscholar.org/CorpusID:116647042.

[8] HUANG Z, SUN S. Synthesizing quantum circuits of AES with lower T-depth and less qubits[C]//2022 28th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2022). Cham: Springer, 2023: 614-644.

[9] JANG K, BAKSI A, SONG G, et al. Quantum analysis of AES[EB/OL]. [2022-7-29]. https://eprint.iacr.org/2022/683.

[10] HOOF I. Space-efficient quantum multiplication of polynomials for binary finite fields with sub-quadratic Toffoli gate count[J]. Quantum Information & Computation, 2020, 20(9&10): 721-735.

[11] AMENTO B, ROTTELER M, STEINWANDT R. Efficient quantum circuits for binary elliptic curve arithmetic: Reducing T-gate complexity[J]. Quantum Information & Computation, 2013, 13(7): 631-644.

[12] FOWLER A G, STEPHENS A M, GROSZKOWSKI P. High threshold universal quantum computation on the surface code[J]. Physical Review A, 2009, 80(5): 052312.

[13] BABBUSH R, GIDNEY C, BERRY D W, et al. Encoding electronic spectra in quantum circuits with linear T complexity[J]. Physical Review X, 2018, 8(4): 041015.

[14] AMY M, MASLOV D, MOSCA M, et al. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2013, 32(6): 818-830.

编 辑 叶 芳