|  |  |
| --- | --- |
| 弯道和树的图片  991CN X  高级教程 | 摘要  [通过迷人的摘要吸引您的读者。它通常是文件的简短摘要。当您准备好添加内容时，只需单击此处并开始键入。]  fx-es(ms)编写组  [课程标题] |

# 前言

目录

[前言 1](#_Toc166018705)

[第一章 汇编语言 4](#_Toc166018706)

[1.1 汇编语言简介 4](#_Toc166018707)

[1.2 常用指令（nX-U16指令集） 4](#_Toc166018708)

[第二章 硬件与系统架构 4](#_Toc166018709)

[2.1 nX-U16处理器 4](#_Toc166018710)

[2.2 内存与寄存器 4](#_Toc166018711)

[2.3 自检与计算器版本号 4](#_Toc166018712)

[2.4 ROM概述 4](#_Toc166018713)

[2.5 矩阵键盘 4](#_Toc166018714)

[第三章 字符与表达式 4](#_Toc166018715)

[3.1 单字节与双字节字符 4](#_Toc166018716)

[3.2 数学显示字符 4](#_Toc166018717)

[3.3 映射字符 4](#_Toc166018718)

[第四章 内存分区 4](#_Toc166018719)

[4.1 输入区，撤销区与回放区 4](#_Toc166018720)

[4.2 变量区与变量存储格式 4](#_Toc166018721)

[4.3 历史记录区 5](#_Toc166018722)

[4.4 设置区 5](#_Toc166018723)

[4.5 即时状态区 5](#_Toc166018724)

[4.6 堆栈区 5](#_Toc166018725)

[4.7 随机数种子 5](#_Toc166018726)

[4.8 显示缓存区 5](#_Toc166018727)

[4.9 空闲区 5](#_Toc166018728)

[4.10 杂项 5](#_Toc166018729)

[第五章 输入的显示与编辑 5](#_Toc166018730)

[5.1 输入的显示 5](#_Toc166018731)

[5.2 输入的编辑 5](#_Toc166018732)

[5.2.1 光标移动 5](#_Toc166018733)

[5.2.2 增删字符 5](#_Toc166018734)

[5.2.3 撤销 5](#_Toc166018735)

[5.2.4 插入 5](#_Toc166018736)

[5.2.5 编辑数学表达式 5](#_Toc166018737)

[第六章 特殊字符 5](#_Toc166018738)

[6.1 字符转换器 6](#_Toc166018739)

[6.1.1 字符转换器原理 6](#_Toc166018740)

[6.1.2 连续刷字符 6](#_Toc166018741)

[6.1.3 根号法复制字符 6](#_Toc166018742)

[6.2 溢出 6](#_Toc166018743)

[6.2.1 达成溢出的方法 6](#_Toc166018744)

[6.2.2 溢出法刷字符 6](#_Toc166018745)

[6.2.3 溢出法复制字符 6](#_Toc166018746)

[6.2.4 定向填充法 6](#_Toc166018747)

[6.3 @法刷字符 6](#_Toc166018748)

[6.3.1 @法刷字符原理 6](#_Toc166018749)

[6.3.2 @法的优化 6](#_Toc166018750)

[6.3.3 在x an模式下@法的变化 6](#_Toc166018751)

[6.4 字符的特殊性质 6](#_Toc166018752)

[第七章 返回导向编程 6](#_Toc166018753)

[7.1 an / @的异常性质 7](#_Toc166018754)

[7.2 ROP进入方法 7](#_Toc166018755)

[7.2.1 x an /@ 模式 7](#_Toc166018756)

[7.2.2 an+12char法与@+2char法 7](#_Toc166018757)

[7.3 简单ROP 7](#_Toc166018758)

[7.3.1 内存修改器 7](#_Toc166018759)

[7.3.2 显示字符 7](#_Toc166018760)

[7.3.3 读取按键 7](#_Toc166018761)

[7.3.4 循环结构 7](#_Toc166018762)

[7.3.5 分支结构 7](#_Toc166018763)

[7.4 ROP进阶 7](#_Toc166018764)

[7.4.1 编辑内存 7](#_Toc166018765)

[7.4.2 计时 7](#_Toc166018766)

[7.4.3 ROM提取 7](#_Toc166018767)

[7.4.4 绘制屏幕 7](#_Toc166018768)

[7.4.5 调用其他函数 7](#_Toc166018769)

[7.4.6 quickcpy——快速注入内存 7](#_Toc166018770)

[7.5 ROP实战 7](#_Toc166018771)

[7.5.1 内存注入可视化 7](#_Toc166018772)

[7.5.2 像素编辑器 8](#_Toc166018773)

[7.5.3 贪吃蛇 8](#_Toc166018774)

[7.5.4 俄罗斯方块 8](#_Toc166018775)

[7.5.5 1024 8](#_Toc166018776)

[7.5.6 函数绘图 8](#_Toc166018777)

[附录一 字符表 8](#_Toc166018778)

[附录二 常用汇编指令 8](#_Toc166018779)

[附录三 按键内码对应表 8](#_Toc166018780)

[附录四 模拟器的配置与使用 8](#_Toc166018781)

[附录五 ROM函数地址索引 8](#_Toc166018782)

[附录六 用Ghidra反编译ROM 8](#_Toc166018783)

[附录七 Github上的数字资源仓库 8](#_Toc166018784)

[结语 8](#_Toc166018785)

# 汇编语言

## 汇编语言简介

## 常用指令（nX-U16指令集）

# 硬件与系统架构

## nX-U16处理器

## 内存与寄存器

## 自检与计算器版本号

## ROM概述

## 矩阵键盘

# 字符与表达式

## 单字节与双字节字符

## 数学显示字符

## 映射字符

# 内存分区

## 输入区，撤销区与回放区

## 变量区与变量存储格式

## 历史记录区

## 设置区

## 即时状态区

## 堆栈区

## 随机数种子

## 显示缓存区

## 空闲区

## 杂项

# 输入的显示与编辑

## 输入的显示

## 输入的编辑

### 光标移动

### 增删字符

### 撤销

### 插入

### 编辑数学表达式

# 特殊字符

## 字符转换器

### 字符转换器原理

### 连续刷字符

### 根号法复制字符

## 溢出

### 达成溢出的方法

#### 方程溢出

#### 线性求和溢出

#### 双字节溢出

#### 框溢出

### 溢出法刷字符

### 溢出法复制字符

### 定向填充法

## @法刷字符

### @法刷字符原理

### @法的优化

### 在x an模式下@法的变化

## 字符的特殊性质

# 返回导向编程

## an / @的异常性质

## ROP进入方法

### x an /@ 模式

### an+12char法与@+2char法

## 简单ROP

### 内存修改器

### 显示字符

### 读取按键

### 循环结构

### 分支结构

## ROP进阶

### 编辑内存

### 计时

### ROM提取

### 绘制屏幕

### 调用其他函数

### quickcpy——快速注入内存

## ROP实战

### 内存注入可视化

### 像素编辑器

### 贪吃蛇

### 俄罗斯方块

### 1024

### 函数绘图

# 附录一 字符表

# 附录二 常用汇编指令

# 附录三 按键内码对应表

# 附录四 模拟器的配置与使用

# 附录五 ROM函数地址索引

# 附录六 用Ghidra反编译ROM

# 附录七 Github上的数字资源仓库

# 结语