



南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异

汇编与逆向技术基础

第2章 IA-32处理器体系结构

王志

zwang@nankai.edu.cn

南开大学 网络空间安全学院

2021/2022



本章知识点

允公允能 日新月异

- 计算机体系结构
- IA-32处理器体系结构
- IA-32的内存管理





南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异

计算机体系结构



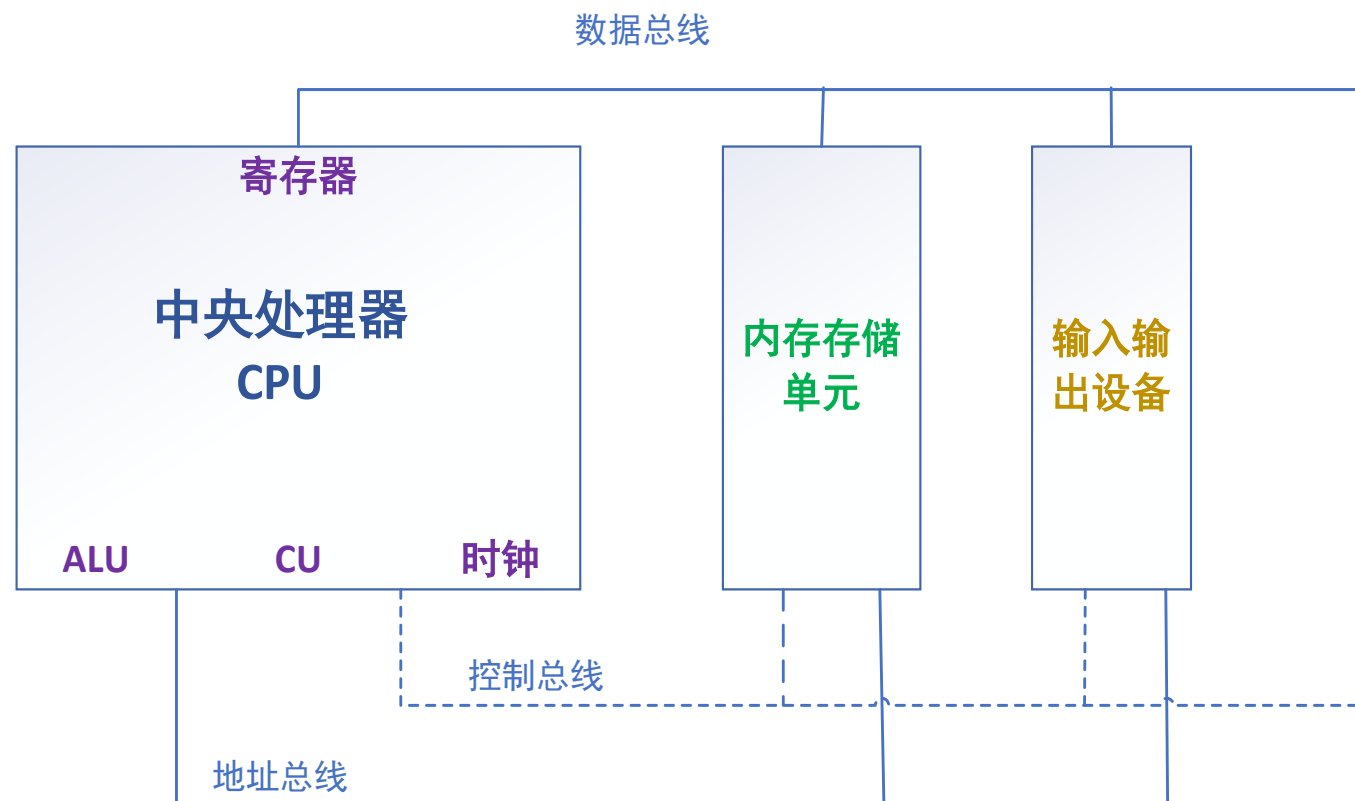
计算机基本概念

允允允允 日新月异

- 计算机基本结构
- 指令执行周期
- 内存的读取
- 程序是如何运行的



计算机基本结构





计算机基本结构

允允允允 日新月异

- 中央处理器（CPU，Central Processor Unit)进行计算和逻辑操作的地方
 - 寄存器（Register）
 - 时钟（clock）
 - 控制单元（CU，Control Unit）
 - 算数逻辑单元（ALU，Arithmetic Logic Unit）





CPU

允公允能 日新月异

- 寄存器：数据存储，数量有限
- 时钟：同步CPU的内部操作
- 控制单元：控制机器指令的执行步骤
- 算数逻辑单元：算术运算、逻辑运算



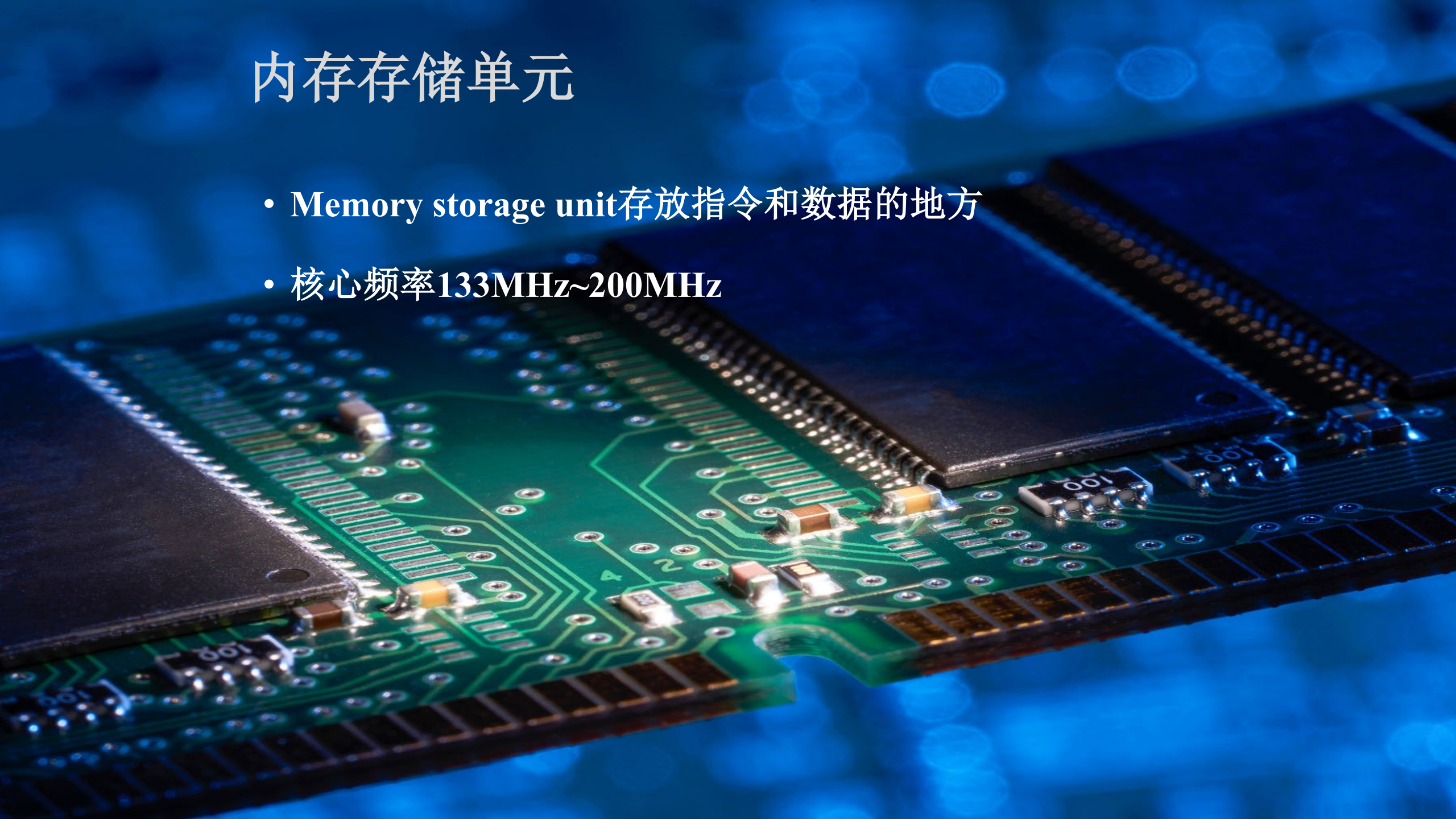
CPU时钟

- 每个时钟周期CPU完成一步操作
- 时钟频率=1/时钟周期
- 时钟频率反映了CPU速度的快慢
- 软件优化



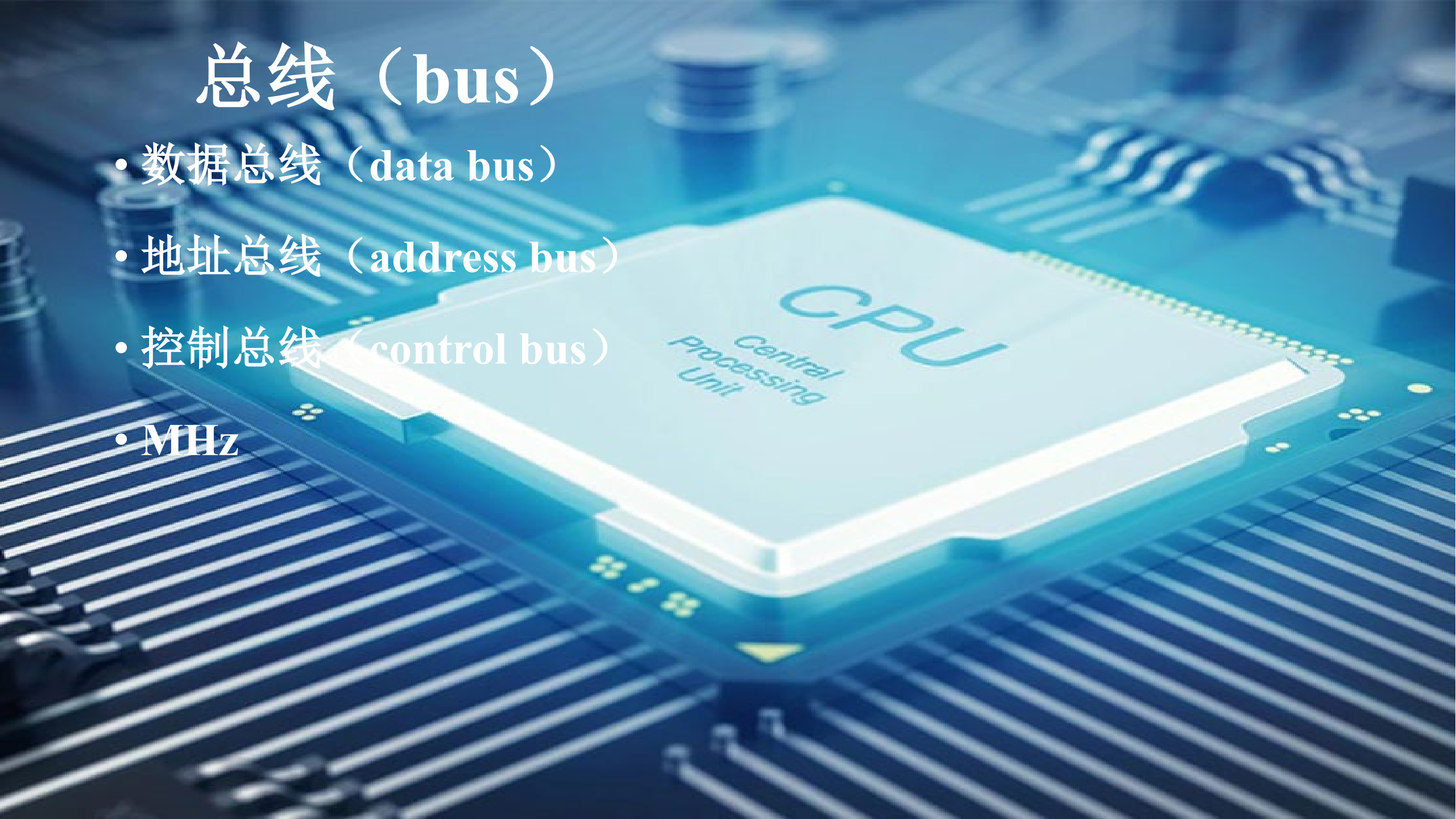
内存存储单元

- Memory storage unit存放指令和数据的地方
- 核心频率133MHz~200MHz



总线 (bus)

- 数据总线 (data bus)
- 地址总线 (address bus)
- 控制总线 (control bus)
- MHz



指令执行周期

允能日新月异

- 单条机器指令的执行包括一系列操作
 - 取指令：指令指针IP
 - 解码：控制单元CU确定执行什么操作
 - 取操作数：从内存读操作数
 - 执行：算术逻辑单元ALU
 - 存储输出操作数：向内存写入





南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异



IA-32处理器体系结构



IA-32处理器体系结构

- IA-32（Intel Architecture 32-bit）英特尔32位体系结构
 - 1985年 80386 CPU首先使用
 - 32位内存地址
 - 32位数据操作数





允公允能 日新月异

工作模式

- 实地址模式（Real-Address Mode）
 - 16位，8086程序设计环境
- 保护模式（Protected Mode）
 - 32位，IA-32程序设计环境
 - 虚拟8086模式：执行8086程序



南开大学
Nankai University



实地址模式

允公允能 日新月异

- 16位的8086程序设计环境
 - 20条地址线
 - 存储空间**1MB**（2的20次方）





允公允能 日新月异

保护模式

- IA-32 CPU的存储管理和保护机制
 - 多任务操作系统
 - 程序有独立的4GB内存存储空间（ 2^{32} 次方）



南开大学
Nankai University



地址空间

允公允能 日新月异

- IA-32 CPU 4GB 地址空间
 - 32位的寻址上限
- 8086只有1MB地址空间

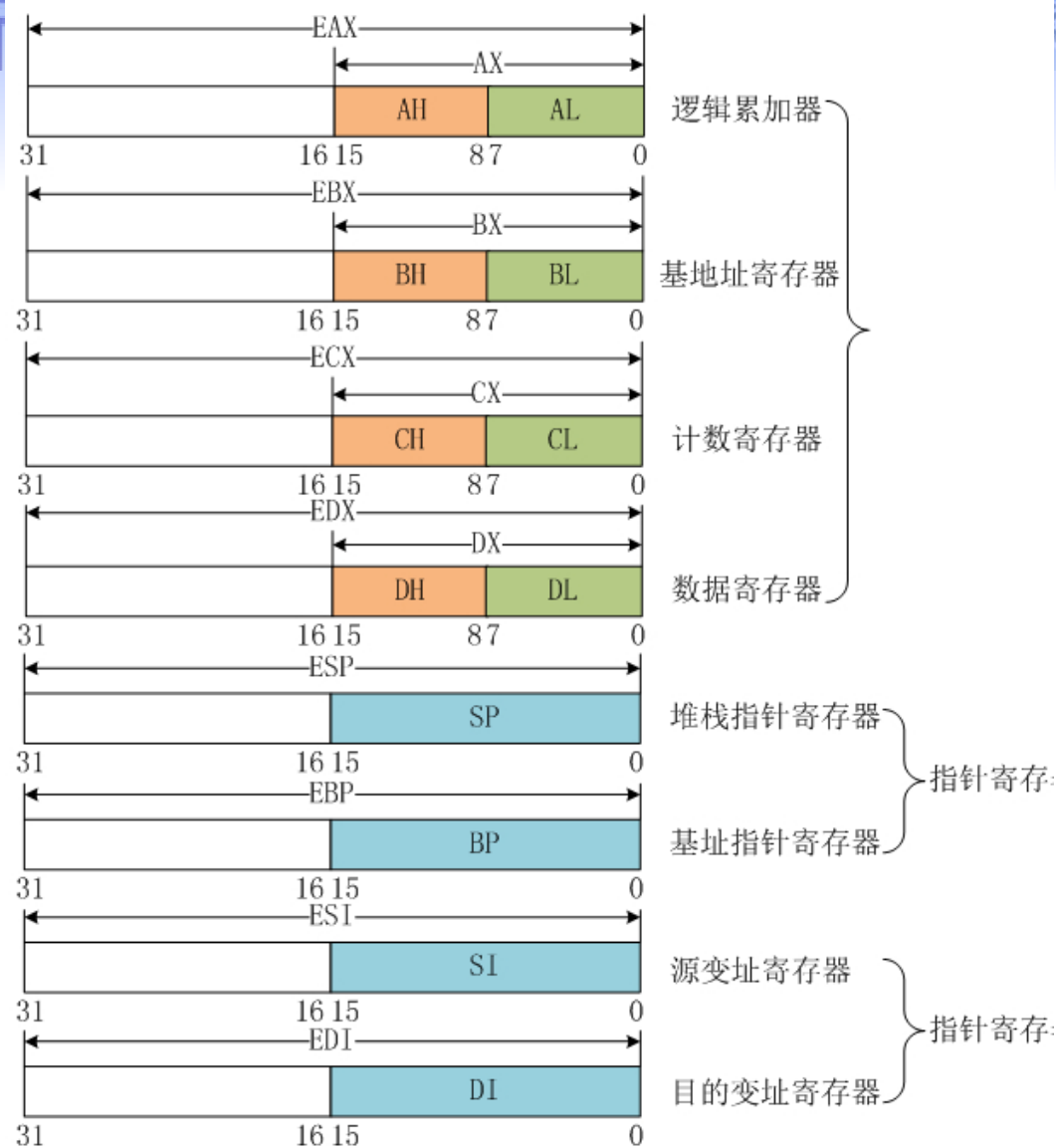


寄存器 (Register)

- 寄存器是CPU内部的**高速存储单元**
 - 比内存的访问速度快很多
 - 优化循环结构执行速度，把循环计数变量放到寄存器中。



日新月异



通用寄存器

8个32位通用寄存器

EAX

EBX

ECX

EDX

ESP

EBP

ESI

EDI



南开大学
Nankai University



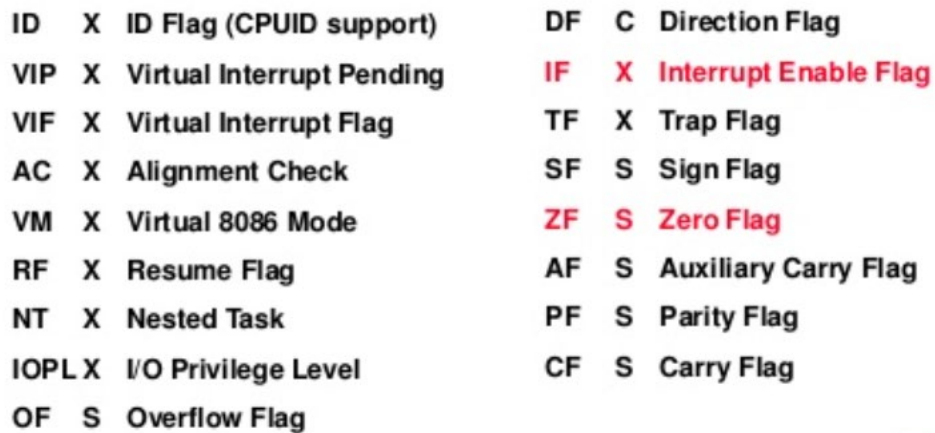
段寄存器

- CS: Code Segment, 代码段寄存器
- SS: Stack Segment, 栈段寄存器
- DS: Data Segment, 数据段寄存器
- ES: Extra(Data) Segment, 数据段寄存器
- FS: Data Segment, 数据段寄存器
- GS: Data Segment, 数据段寄存器

00261DD7	8B55 E0	mov edx,dword ptr ss:[ebp-0x20]
00261DDA	8B02	mov eax,dword ptr ds:[edx]
00261DDC	8945 D8	mov dword ptr ss:[ebp-0x28],eax



允允能日新月异



Bit Positions shown as "0" or "1" are Intel reserved.

S = Status Flag
C = Control Flag
X = System Flag



零标志

允公允能 日新月异

- 零标志（ZF）：若算数或者逻辑运算结果为0则将其置1，反之清零

- xor eax, eax
- jz



进位标志

允公允能 日新月异

- 进位标志（CF）：在无符号算术运算的结果最高有效位(most-significant bit)发生进位或借位则将其置1，反之清零。
 - add eax, 0xffffffff
 - jc



溢出标志

允公允能 日新月异

- **溢出标志（OF）**：在有符号算术运算的结果是较大的正数或较小的负数，并且目的操作数无法容纳时，将该位置1，反之清零。
- 这个标志为带符号整型运算指示溢出状态。



符号标志

允公允能 日新月异

- 符号标志（SF）：该标志被设置为有符号整型的最高有效位。
- 0表示算术或者逻辑运算结果为正
- 1表示算数或者逻辑运算结果为负



奇偶标志

允公允能 日新月异

- 奇偶标志（PF）：如果结果的最低有效字节(least-significant byte)包含偶数个1位则该位置1，否则清零。
- 数据校验





辅助进位标志

允公允能 日新月异

- **辅助进位标志（AC）**：如果算术操作在结果的第3位发生进位或借位则将该标志置1，否则清零。
- 这个标志在BCD(binary-code decimal)算术运算中被使用。



控制标志

允公允能 日新月异

- 方向标志 (DF)
 - 控制串指令(MOVS, CMPS, SCAS, LODS以及STOS)
 - 设置DF标志使得串指令自动递减（从高地址向低地址方向处理字符串），清除该标志则使得串指令自动递增
 - STD以及CLD指令分别用于设置以及清除DF标志。



系统标志

允公允能 日新月异

- TF：将该位设置为1以允许单步调试模式，清零则禁用该模式。
- 调试器的单步调试功能





指令指针

允公允能 日新月异

- 指令指针寄存器（EIP）存放下一条机器指令的内存地址。
- 跳转指令可以修改指令指针寄存器





南開大學

NANKAI UNIVERSITY, P.R.CHINA 1919

允公允能 日新月異



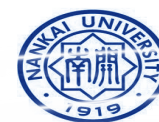
IA-32内存管理



IA-32内存管理

允允允允 日新月异

- IA-32保护模式的内存管理比实地址模式要复杂
 - 多任务
 - 多用户
 - 段模式、页模式
 - 页模式也是基于段模式的，通常称为段页式



平坦模式 (FLAT)

- 每个程序有独立的4GB虚拟地址空间
 - 数据
 - 指令
 - 数据 \longleftrightarrow 指令
- 虚拟地址到物理地址的转换是透明的



允公允能 日新月异

段管理

- 一般保护模式的程序有3个段
 - 代码段, CS
 - 数据段, DS
 - 堆栈段, SS
- 段是一块内存空间





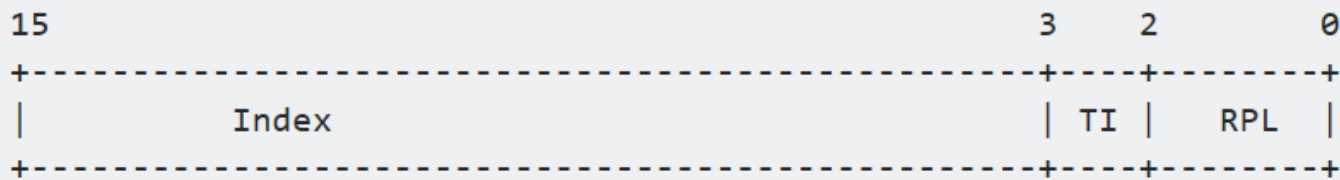
段管理

- GDT (Global Descriptor Table) 全局描述符表
 - 整个系统只有一个GDT (64bit)
 - Intel提供了一个寄存器**GDTR**用来存放GDT的入口地址
- LDT (Local Descriptor Table) 局部描述符表
 - 每个程序都有自己的LDT
 - IA-32为LDT的入口地址也提供了一个寄存器**LDTR**
 - 因为在任何时刻只能有一个任务在运行, 所以LDTR也只需要有一个



段寄存器

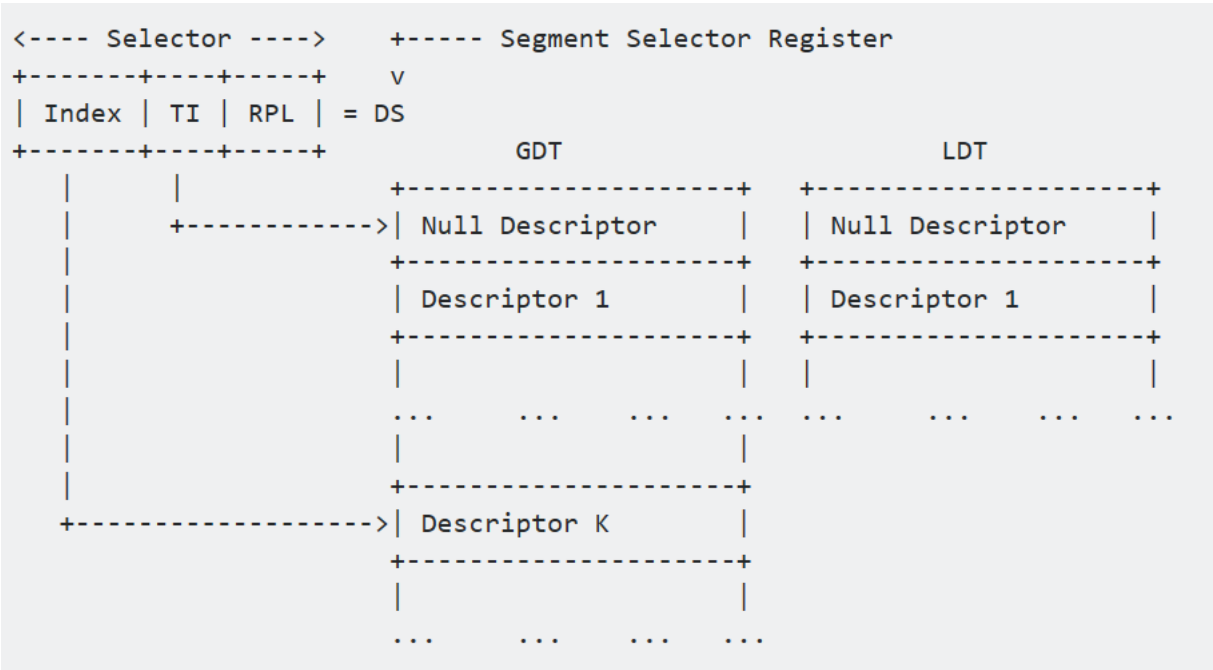
- index (13bits) , 段描述符在表中的索引
- TI (1bit) , 0是GDT, 1是LDT
- RPL (2bits) , Request Privilege Level, 权限
 - Ring 0, Kernel Mode
 - Ring 3, User Mode



TI = Table Indicator: 0 = GDT, 1 = LDT

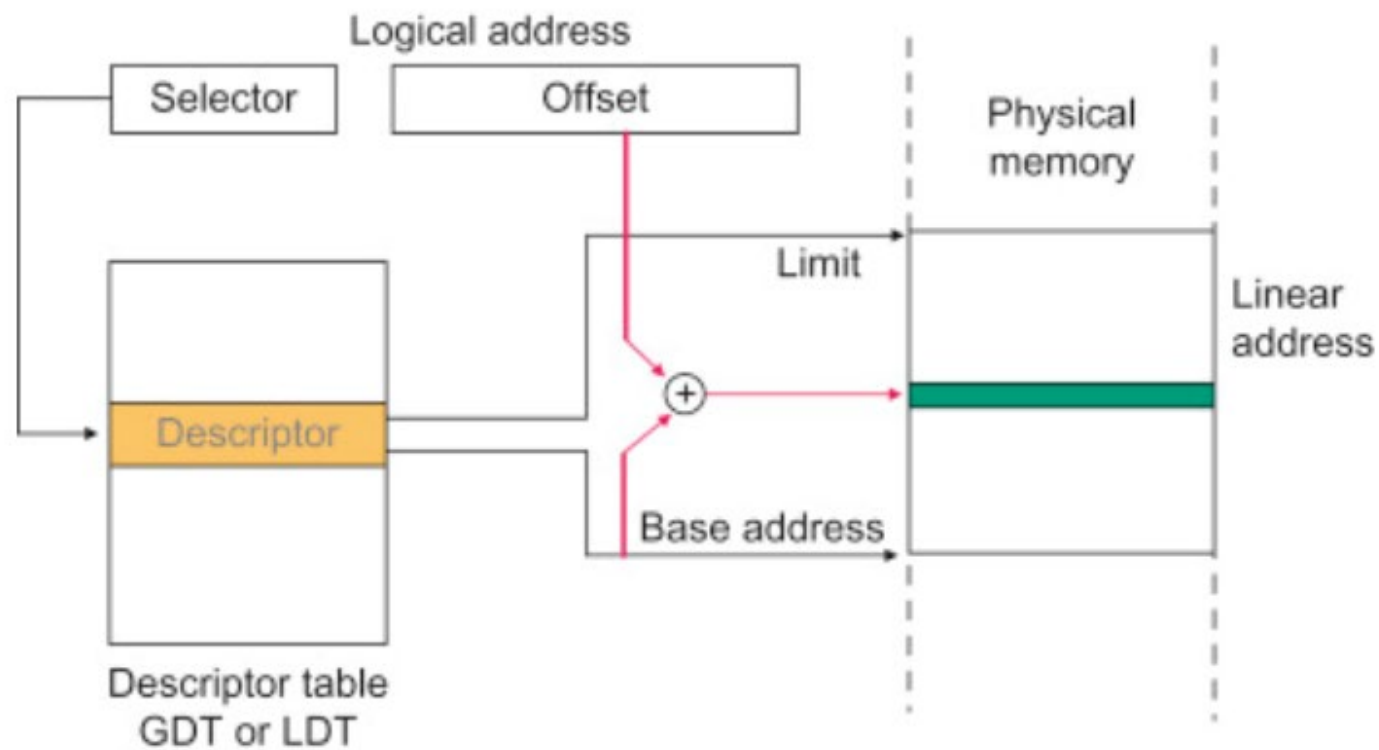


段描述符





段模式

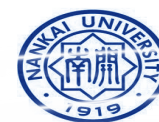




允公允能 日新月异

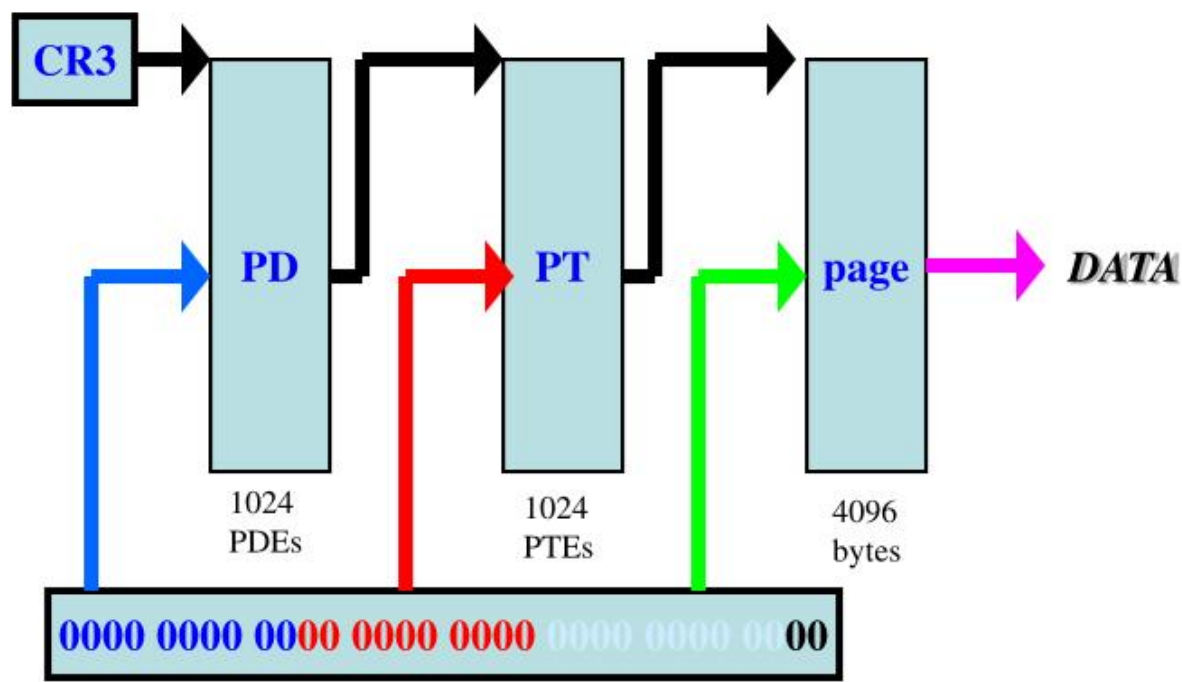
分页机制

- 段又被分割成内存页（page）
- 内存页统一为4096字节的内存块
- 提高内存的利用率，减少内存碎片
- 页交换，不使用的内存页被交换到硬盘上
 - 虚拟内存空间大于实际的物理内存空间
 - 页交换降低程序执行速度



分页机制

Virtual Address Translation



© Microsoft Corporation 2004

页目录表 (PDT) 的每一项元素称为页目录表项 (PDE)

每个页目录表项指向一个页表 (PTT)

每个页表的大小为**4KB**，即一个页表可以存储**1024**个页表项 (PTE)

页表 (PTT) 的每一个元素称为页表项 (PTE)

页表项 (PTE) 所指向的才是真正的物理页



南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异



汇编与逆向技术基础

第2章 IA-32处理器体系结构