دوره مهندسی معکوس نرم افزار

- Site: OnHexGroup.ir
- Youtube: @onhexgroup
- Telegram: onhex_ir
- Twitter: @onhexgroup
- Github: onhexgroup

نسخه ی ۳۲ و ۶۴ بیتی

پلتفرم: ویندوز

ارائه دهنده : **OnhexGroup**

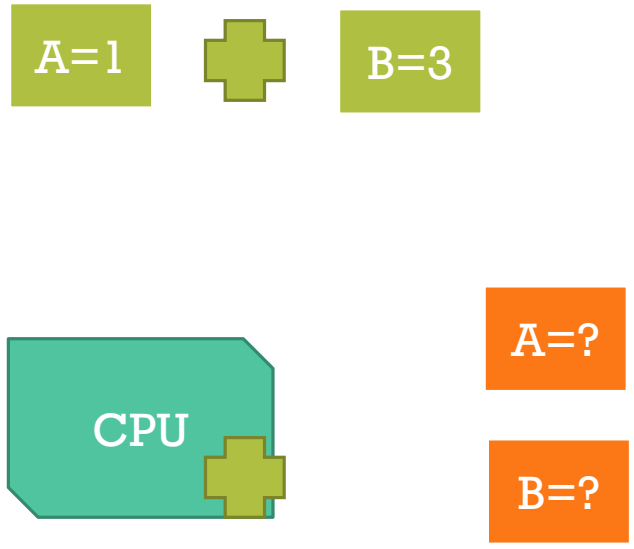
Onhexgroup.ir

مفهوم رجیسترها

- رجیسترها حافظه های سریعی هستن و مانند یک متغیر عمل میکنن

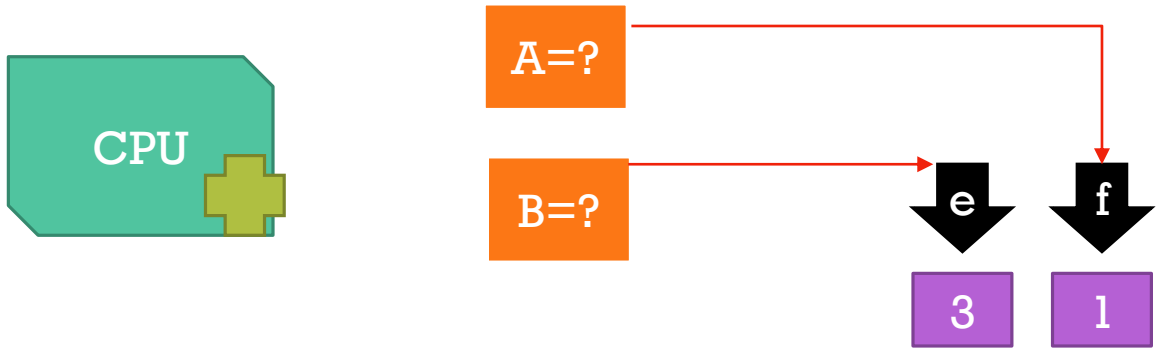
Twitter:Onhexgroup

مفهوم رجیسترها



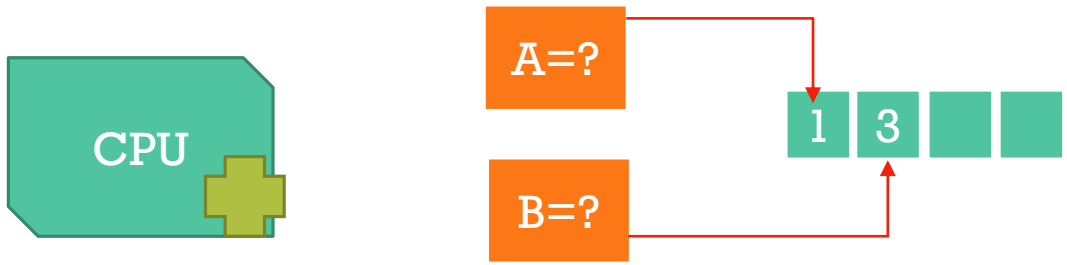
Twitter:Onhexgroup

مفهوم رجیسترها



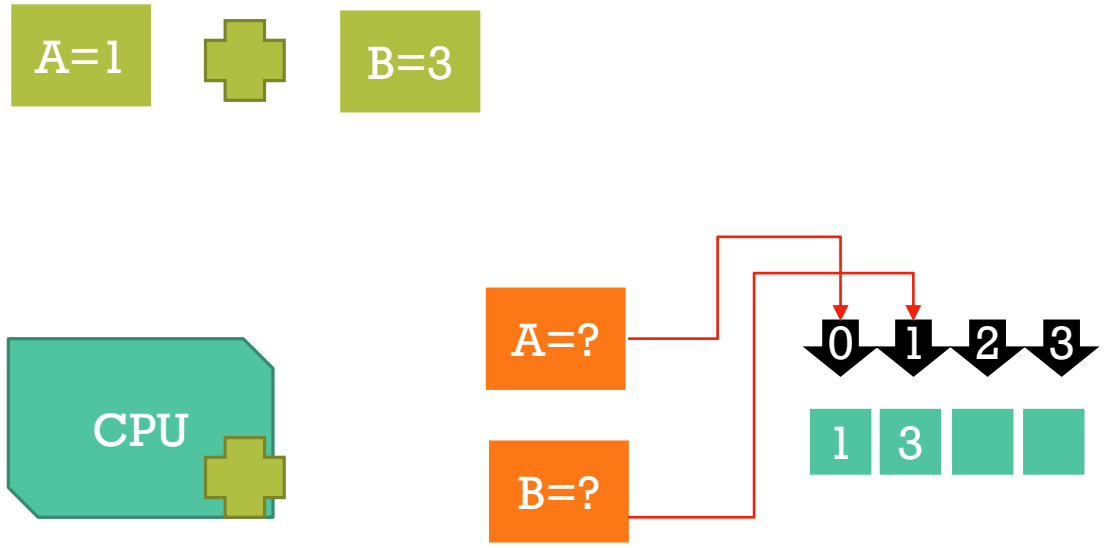
Twitter:Onhexgroup

مفهوم رجیسترها



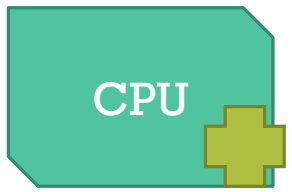
Twitter:Onhexgroup

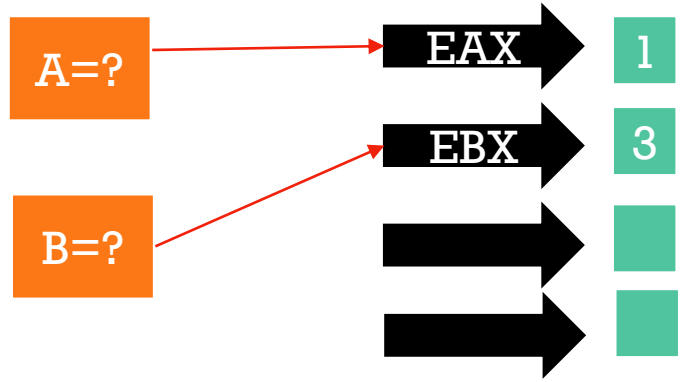
مفهوم رجیسترها



Twitter:Onhexgroup

مفهوم رجیسترها





انواع رجیسترهای پایه

- رجیسترهای همه منظوره
- رجیسترهای سگمنت
- رجیسترهای وضعیت و کنترلی
- رجیستر اشاره گر دستور

Youtube: @onhexgroup

رجیسترهای همه منظوره

- رجیسترهای همه منظوره یا رجیسترهای عمومی یا General Purpose register یا GPR
- امکان استفاده در همه جا و قابلیت ذخیره داده و آدرس دارن
- البته کاربردهای خاصی رو هم دارن

Github: @onhexgroup

رجیسترهای همه منظوره

- در سیستم های ۳۲ بیتی :
  - اندازه رجیسترها حداکثر ۳۲ بیت
  - ۸ رجیستر همه منظوره داریم:
    - **EAX , EBX , ECX , EDX , ESI , EDI , EBP , ESP**

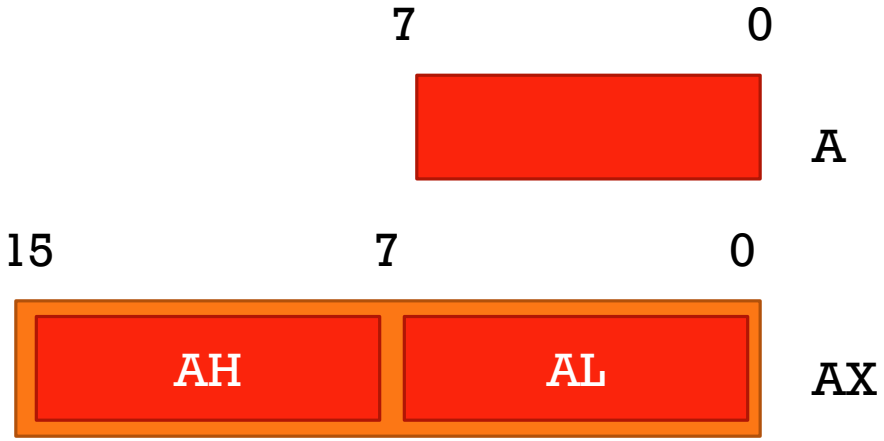
- در سیستم های ۶۴ بیتی :
  - اندازه رجیسترها حداکثر ۶۴ بیت
  - ۱۶ رجیستر همه منظوره داریم :
    - **RAX,RBX,RCX,RDX,RSI,RDI,RBP,RSP,R8...R15**
    - **R0...R15**

Onhexgroup.ir

اندازه رجیسترهای همه منظوره

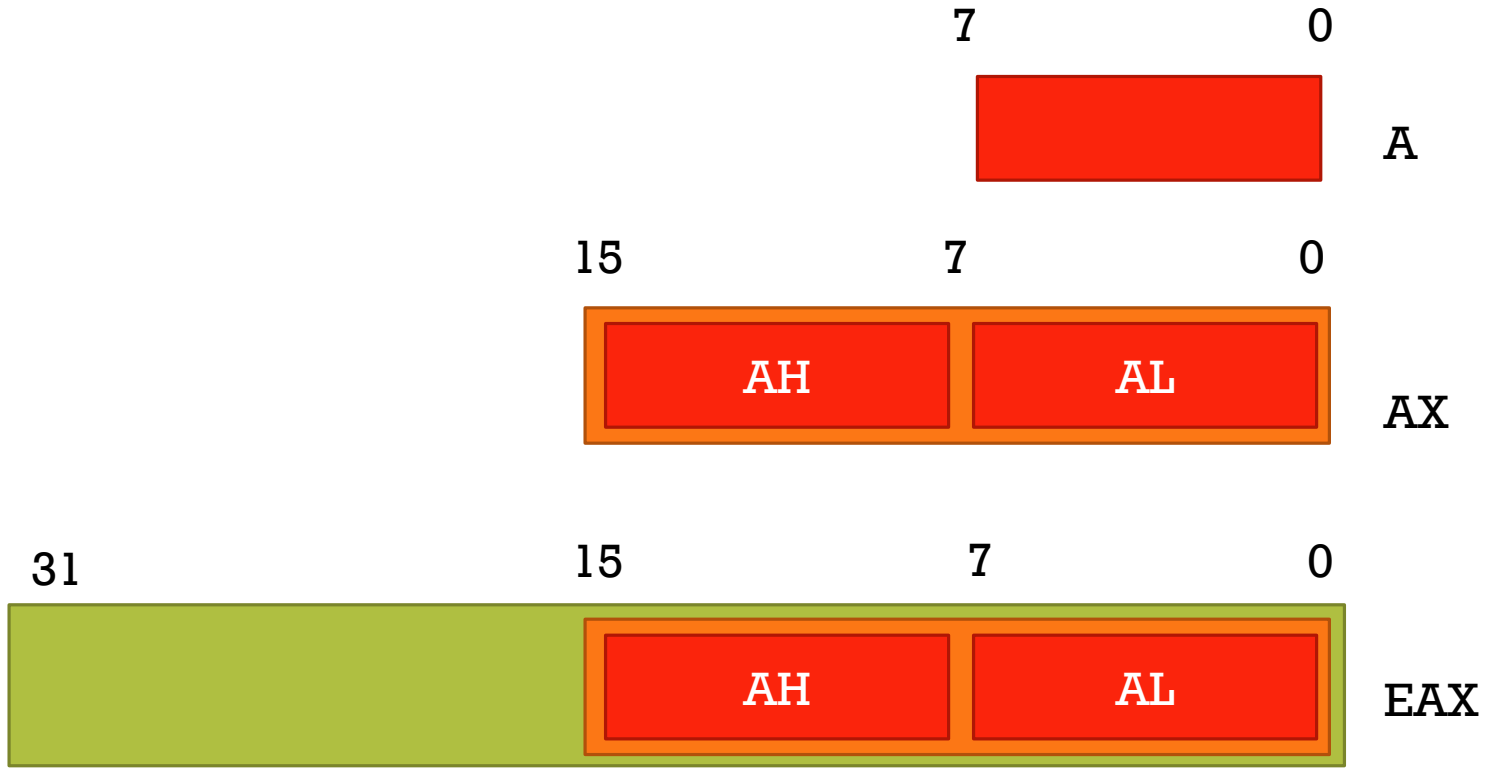
Telegram: onhex_ir

اندازه رجیسترهای همه منظوره



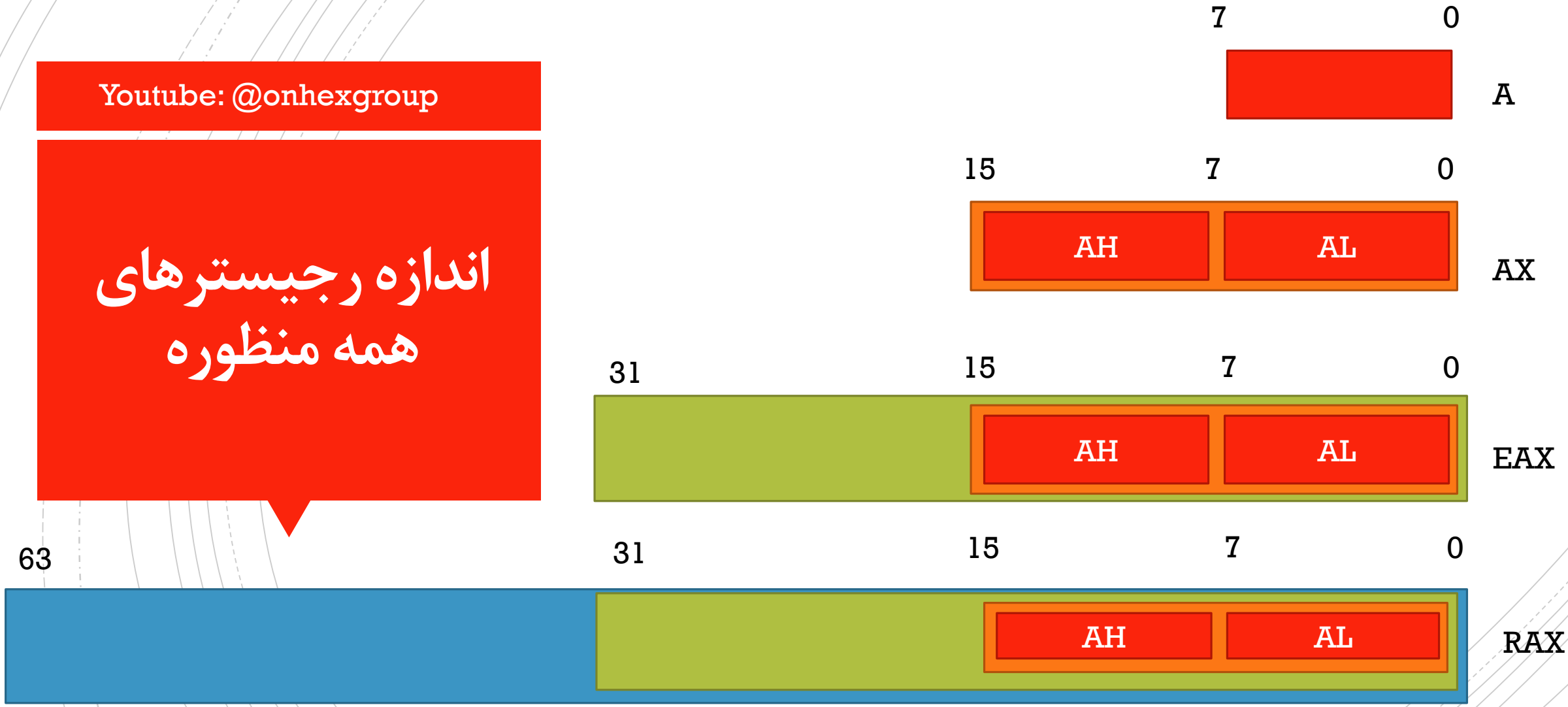
Youtube: @onhexgroup

اندازه رجیسترهای همه منظوره



Youtube: @onhexgroup

اندازه رجیسترهای همه منظوره



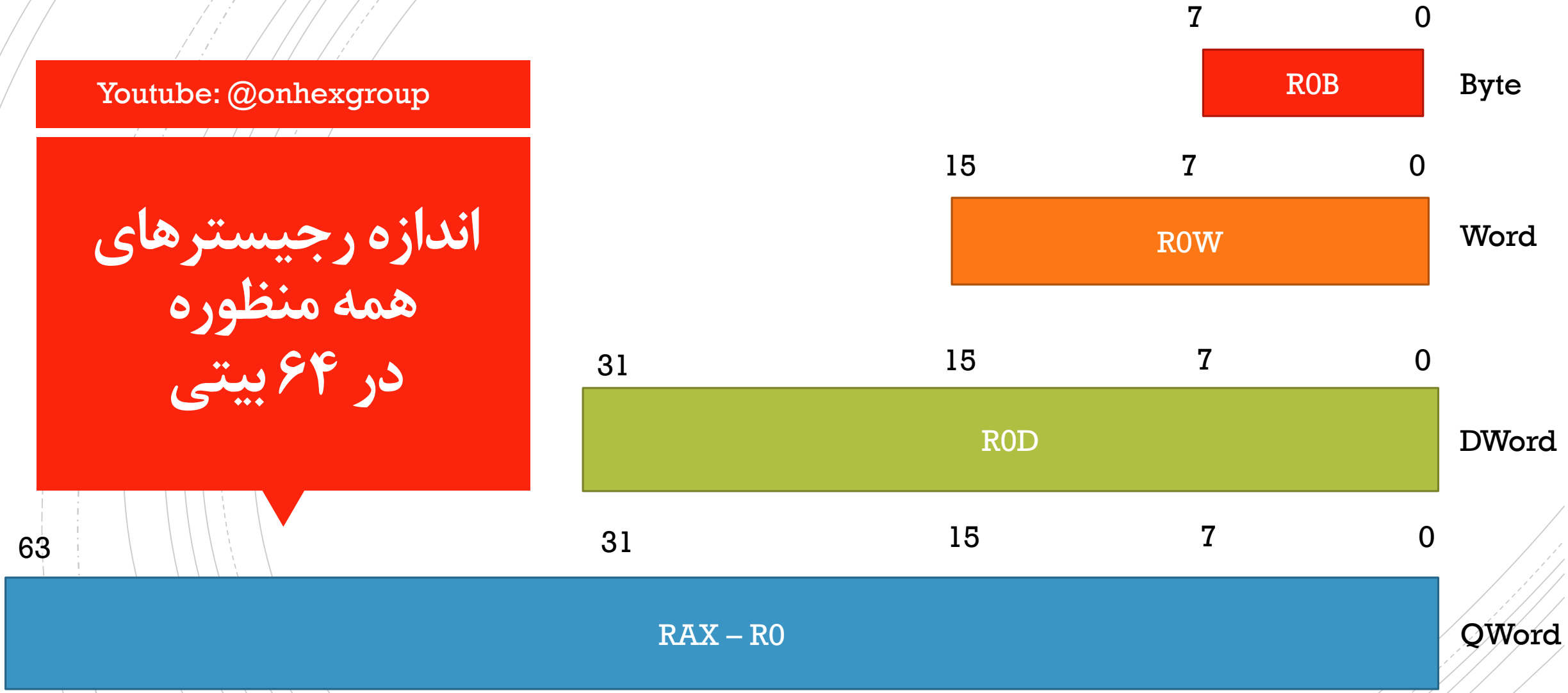
Github: @onhexgroup

نوع داده رجیسترهای همه منظوره

- رجیستر **AL** و **AH** = ۸ بیت = ۱ بایت
- رجیستر **AX** = ۱۶ بیت = ۲ بایت = ۱ کلمه
- رجیستر **EAX** = ۳۲ بیت = ۴ بایت = ۲ کلمه = ۱ **Dword**
- رجیستر **RAX** = ۶۴ بیت = ۸ بایت = ۴ کلمه = ۲ **DWORD** = ۱ **QWORD**

Youtube: @onhexgroup

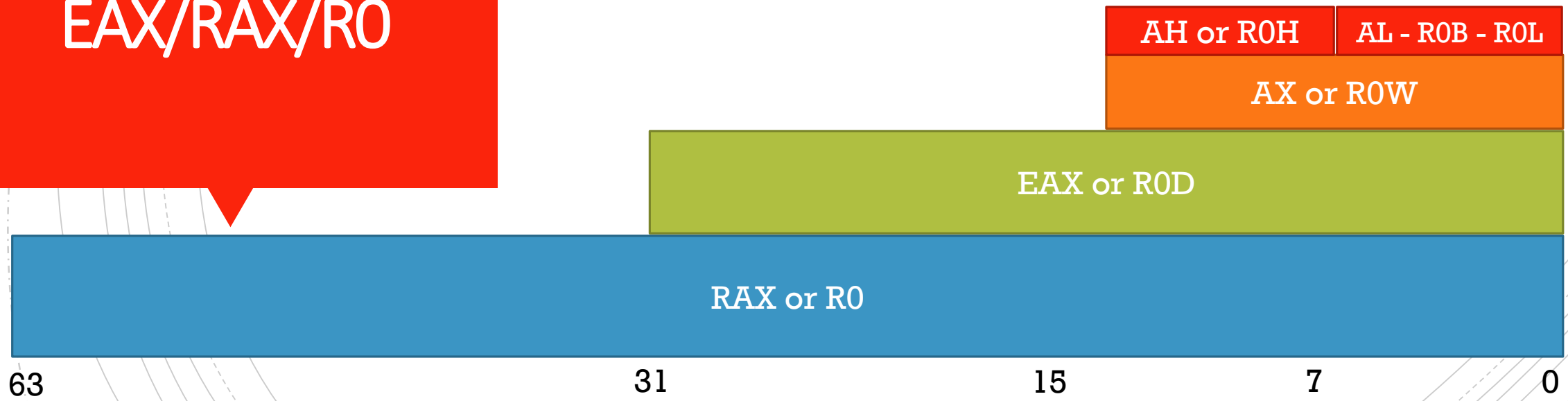
اندازه رجیسترهای همه منظوره در ۶۴ بیتی



Twitter: @onhexgroup

رجیستر EAX/RAX/R0

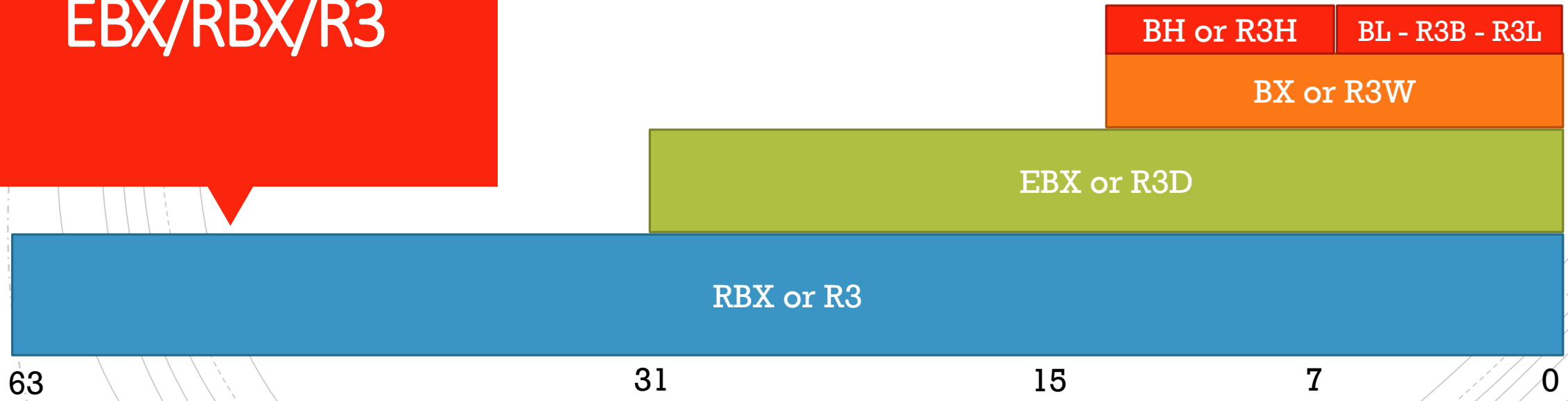
- رجیستر همه منظوره هستش.
- در ۳۲ بیتی : EAX
- در ۶۴ بیتی : RAX یا R0
- انباره یا Accumulator



- رجیستر همه منظوره هستش.
- در ۳۲ بیتی : EBX
- در ۶۴ بیتی : RBX یا R3
- Base Register : آدرس Base برنامه رو ذخیره میکنه.

Youtube: @onhexgroup

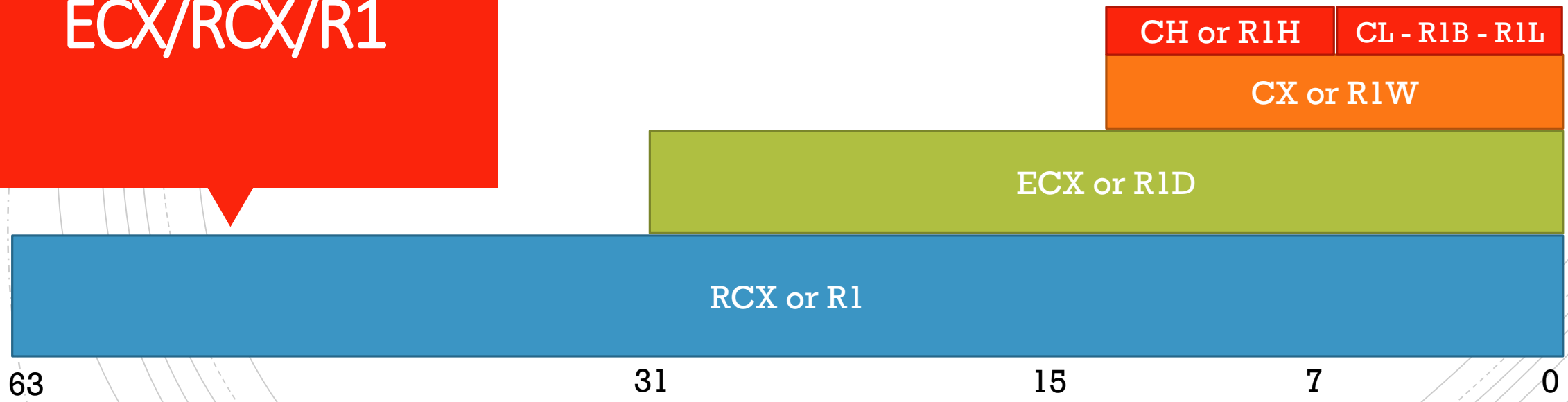
رجیستر EBX/RBX/R3



Github: @onhexgroup

رجیستر ECX/RCX/R1

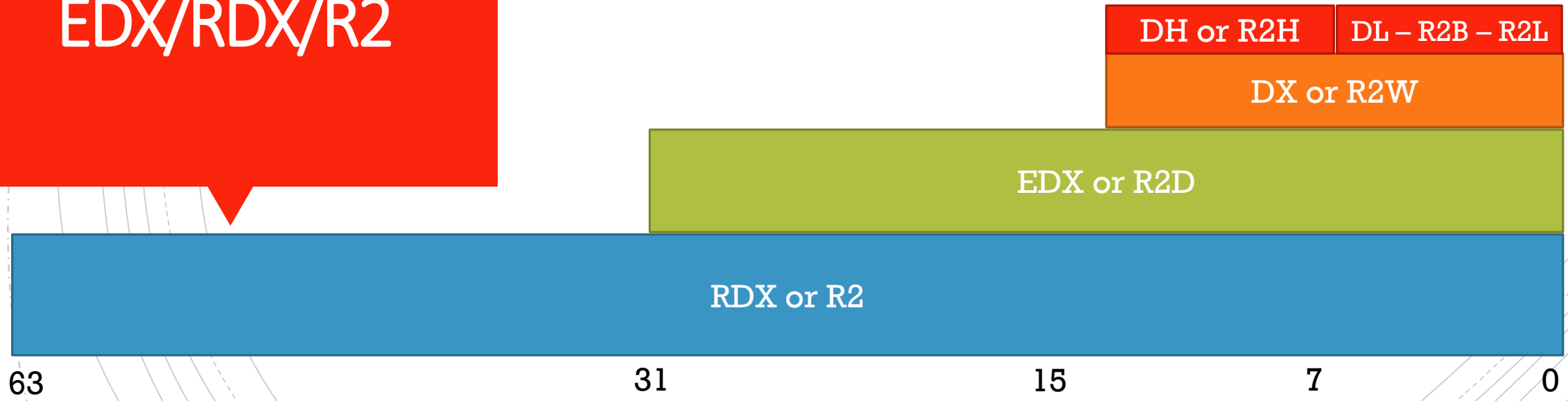
- رجیستر همه منظوره هستش.
- در ۳۲ بیتی : ECX
- در ۶۴ بیتی : RCX یا R1
- شمارنده (Counter) برای رشته ها و حلقه ها



OnHexGroup.ir

رجیستر EDX/RDX/R2

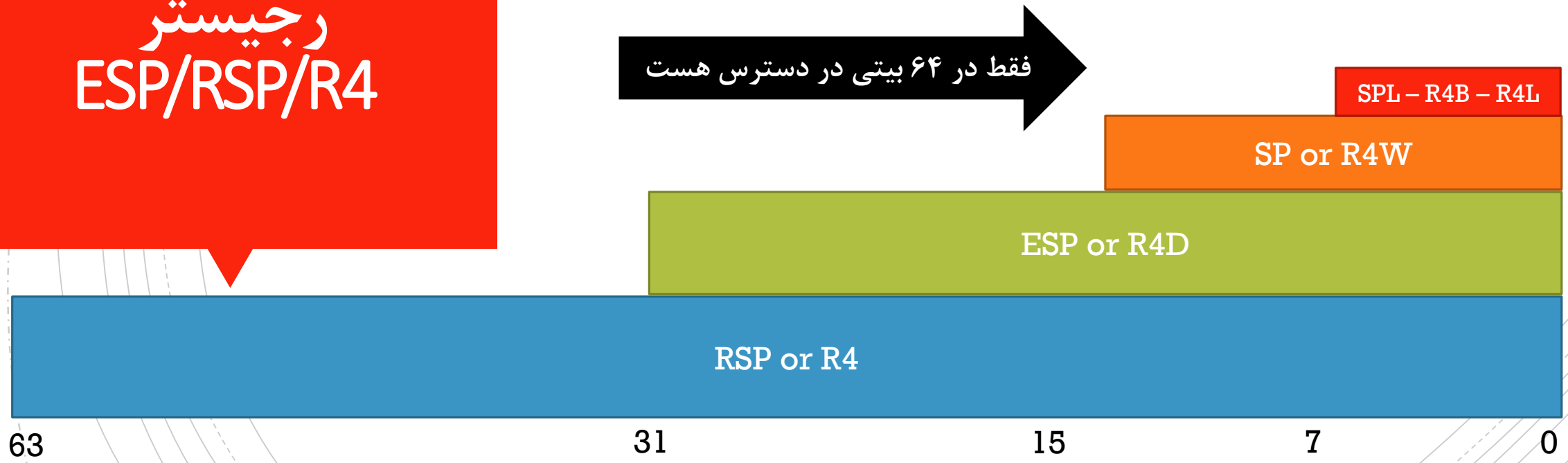
- رجیستر همه منظوره هستش.
- در ۳۲ بیتی : EDX
- در ۶۴ بیتی : RDX یا R2
- Data register و در عملیات I/O استفاده میشه.



Twitter: @onhexgroup

رجیستر ESP/RSP/R4

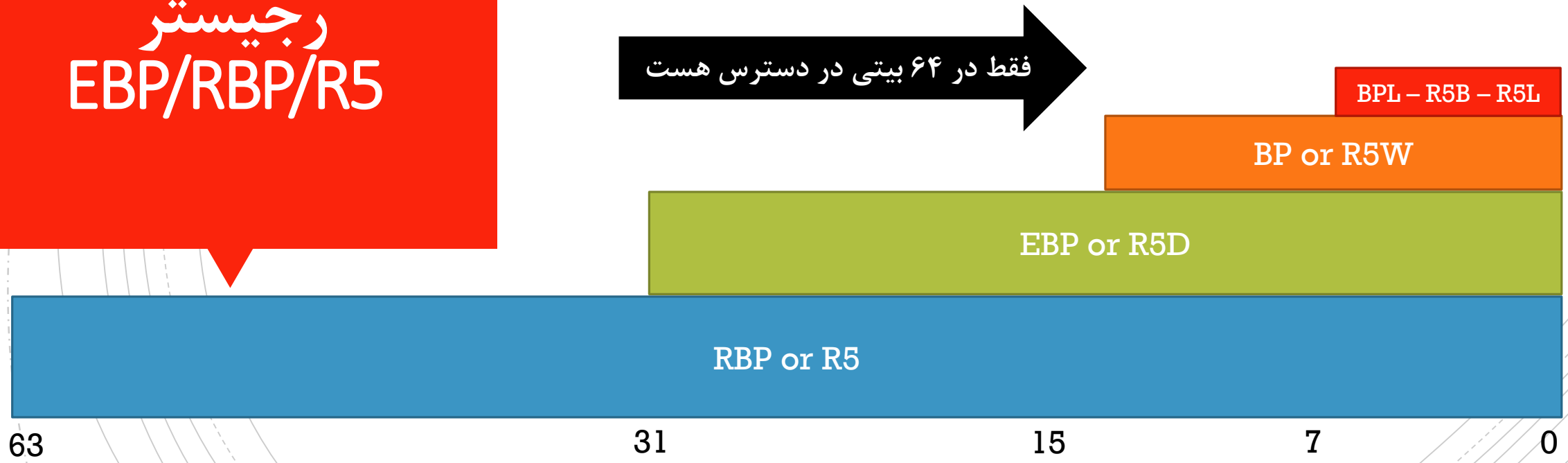
- رجیستر همه منظوره هستش.
- در ۳۲ بیتی : ESP
- در ۶۴ بیتی : RSP یا R4
- اشاره گر پشته یا Stack pointer



Twitter: @onhexgroup

رجیستر EBP/RBP/R5

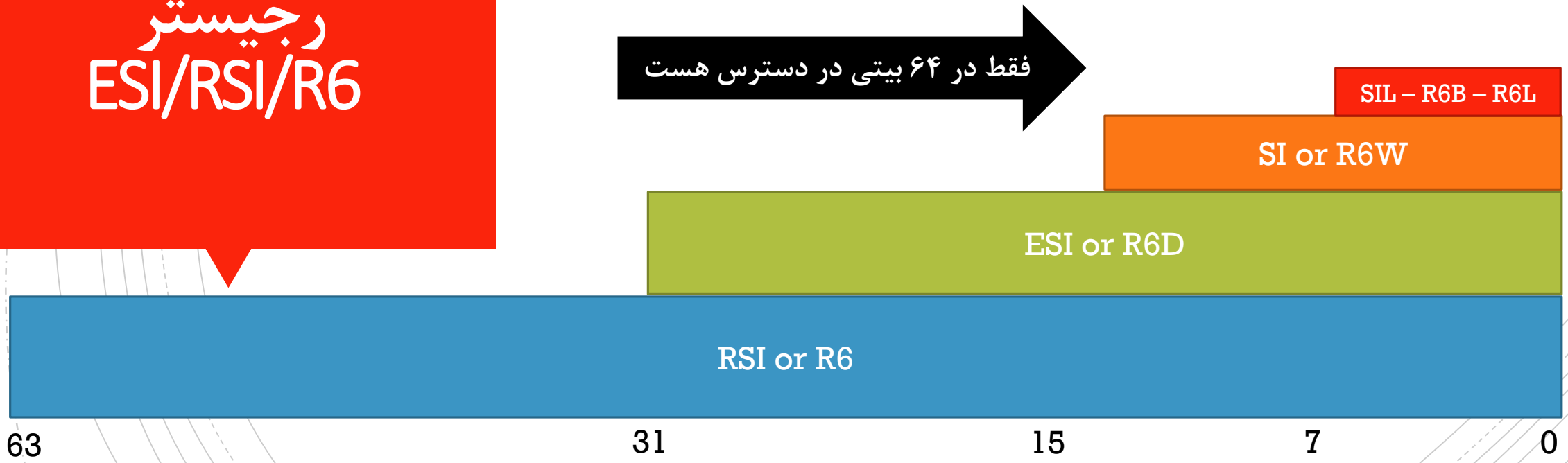
- رجیستر همه منظوره هستش.
- در ۳۲ بیتی : EBP
- در ۶۴ بیتی : RBP یا R5
- اشاره گر به داده در پشته یا Base pointer – به انتهای فریم پشته اشاره میکنه



- رجیستر همه منظوره هستش.
- در ۳۲ بیتی : ESI
- در ۶۴ بیتی : RSI یا R6
- اشاره گر به داده و در عملیات رشته معروف Source Index

Twitter: @onhexgroup

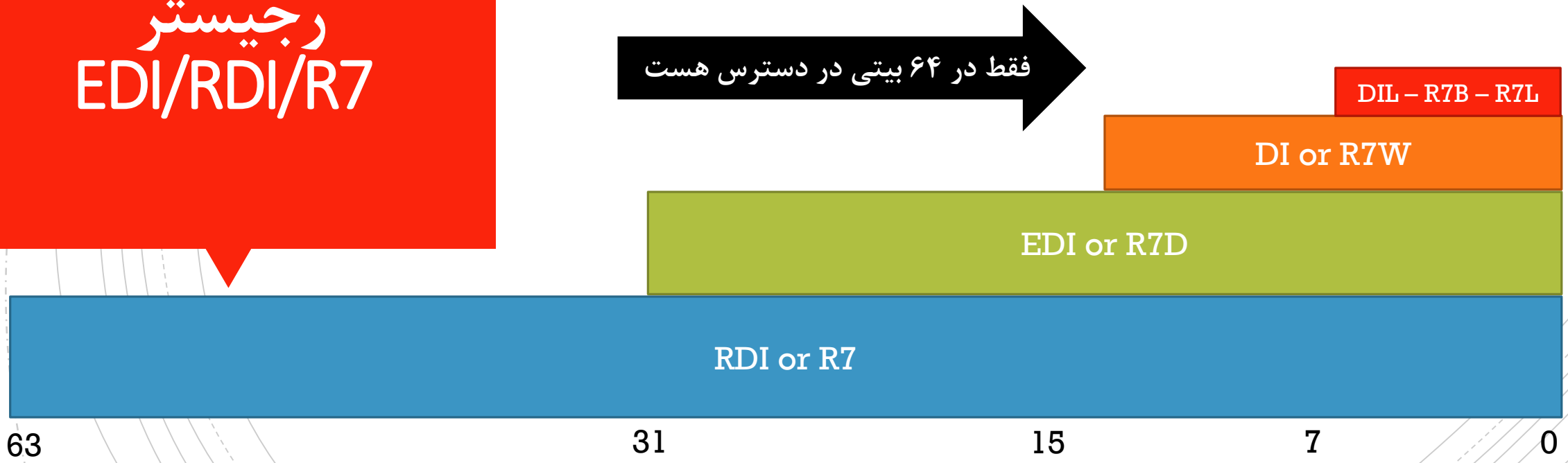
رجیستر ESI/RSI/R6



- رجیستر همه منظوره هستش.
- در ۳۲ بیتی : EDI
- در ۶۴ بیتی : RDI یا R7
- اشاره گر به داده و در عملیات رشته معروف به Destination Index

Twitter: @onhexgroup

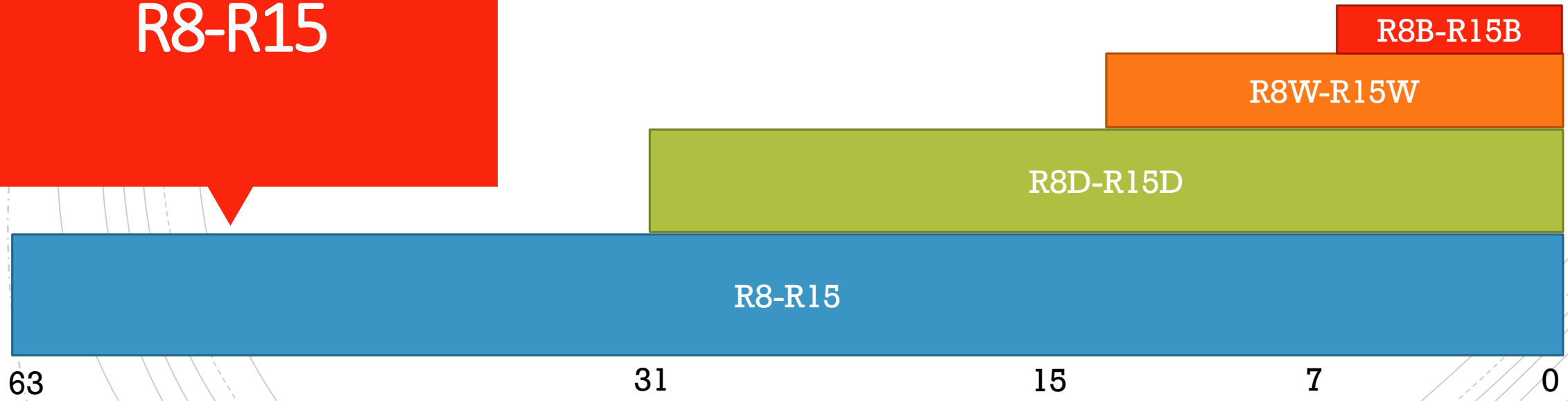
رجیستر EDI/RDI/R7



Twitter: @onhexgroup

رجیسترهای R8-R15

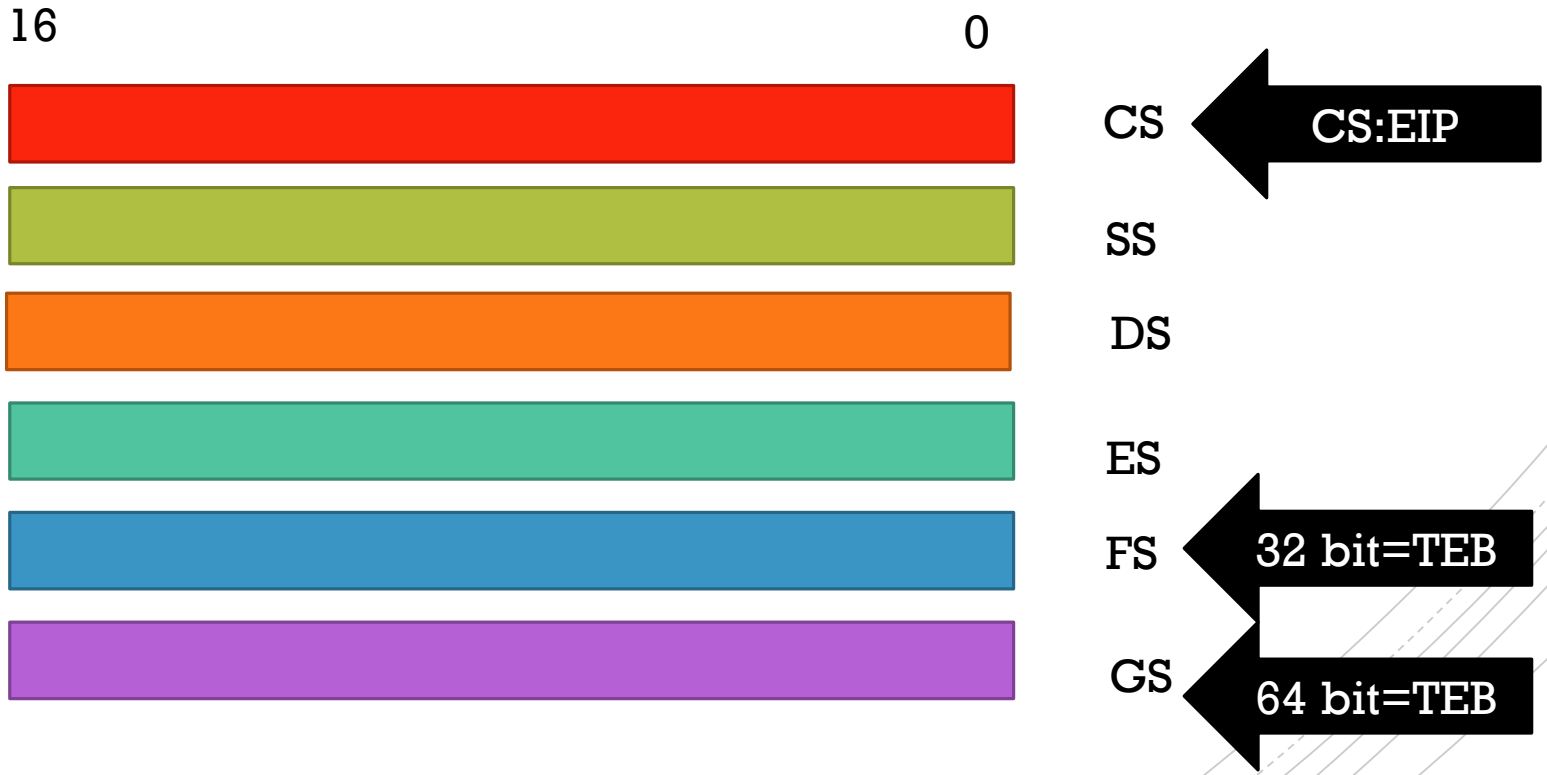
- رجیستر همه منظوره ی جدید که مختص نسخه ی ۶۴ بیتی هستش.
- از R8 تا R15 در دسترس هستن.



Twitter: @onhexgroup

رجیسترهای سگمنت

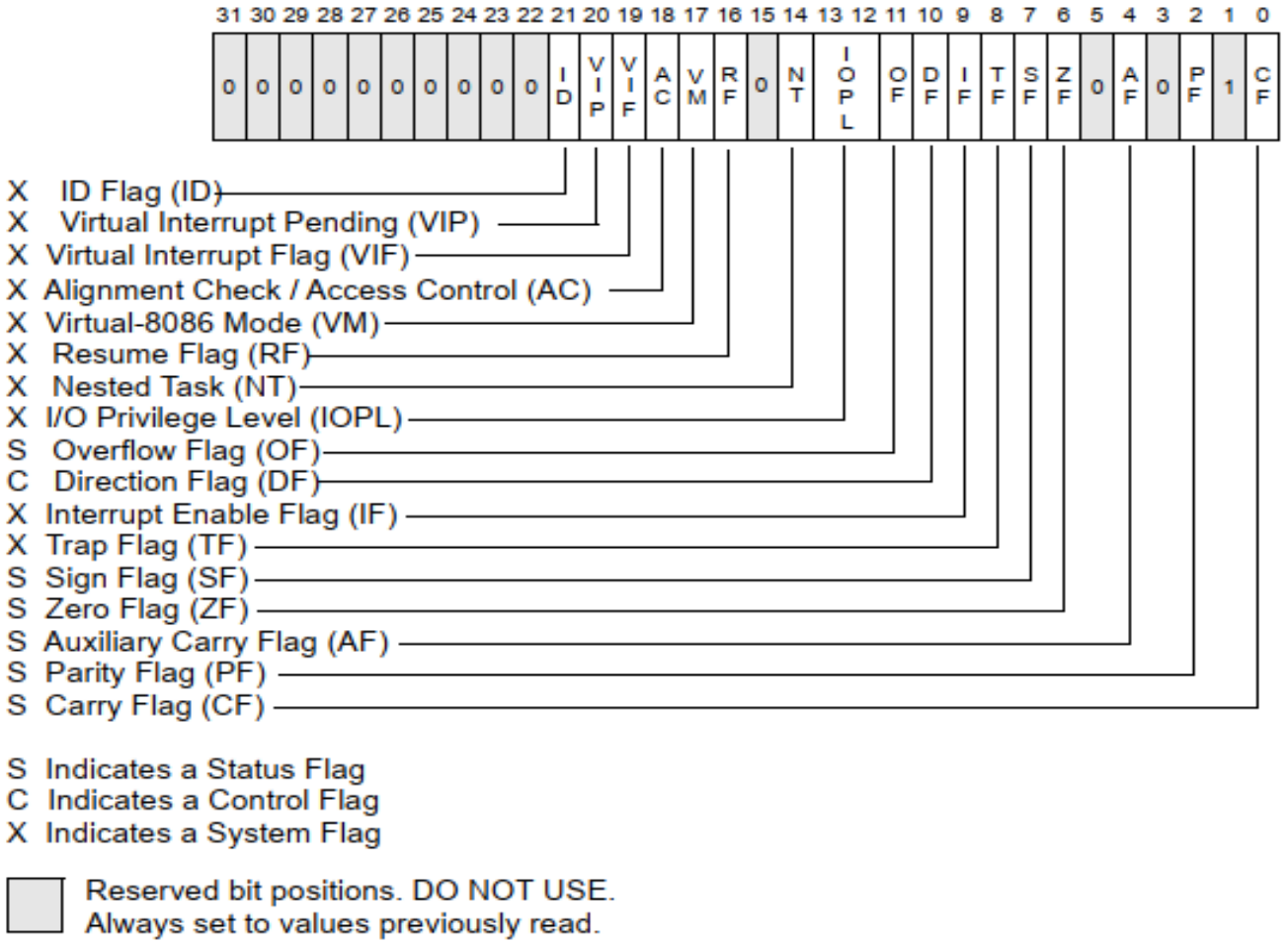
- سگمنت ناحیه ی پیوسته ای از مموری هستش که با آدرس شروع (Base) و محدوده تعریف میشه.
  - هدف : تقسیم حافظه برای حفاظت و کنترل ساده بود.
  - رجیسترهای سگمنت به این ناحیه ها اشاره میکنن.
- این رجیسترها در سیستم های مدرن زیاد استفاده نمیشن. (مدل Flat)
- در کل ۶ تا رجیستر سگمنت داریم که هر کدوم به یه بخشی از حافظه اشاره میکنن (محل شروع) :



Twitter: @onhexgroup

رجیسترهای وضعیت و کنترلی EFLAGS/RFLAGS

- هر بیتش یه نامی داره که بهش فلگ میگن.
  - در ۳۲ بیتی اندازه اش ۳۲ بیت
  - در ۶۴ بیتی اندازه اش ۶۴ بیت
- فلگ های سیستمی ، کنترلی و وضعیتی



Twitter: @onhexgroup

رجیستر اشاره گر آدرس EIP/RIP

- Instruction Pointer Register
- نشون دهنده آدرس بعدی که میخواد اجرا بشه
- برنامه مستقیما نمیتونه تغییرش بده
- در ۳۲ بیتی ، ۳۲ بیت و در ۶۴ بیتی ، ۶۴ بیت اندازه داره

Twitter: @onhexgroup

منابع

- https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/x86-architecture
- https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/x64-architecture
- https://en.wikibooks.org/wiki/X86_Assembly/X86_Architecture