Visão geral da ISA x86-64

Alan Kleiman

Instituto de Computação
Universidade Estadual de Campinas

3 de Novembro de 2005

Roteiro

Introdução

- Foco na ISA x86-64 (também conhecido como EMT64, x64, AMD64)
- Extensão da ISA IA32 (x86-32, ou x86)
  - Espaço de endereçamento de 64-bits
  - Dobro de registradores de uso geral com dobro da capacidade
  - Bit NX

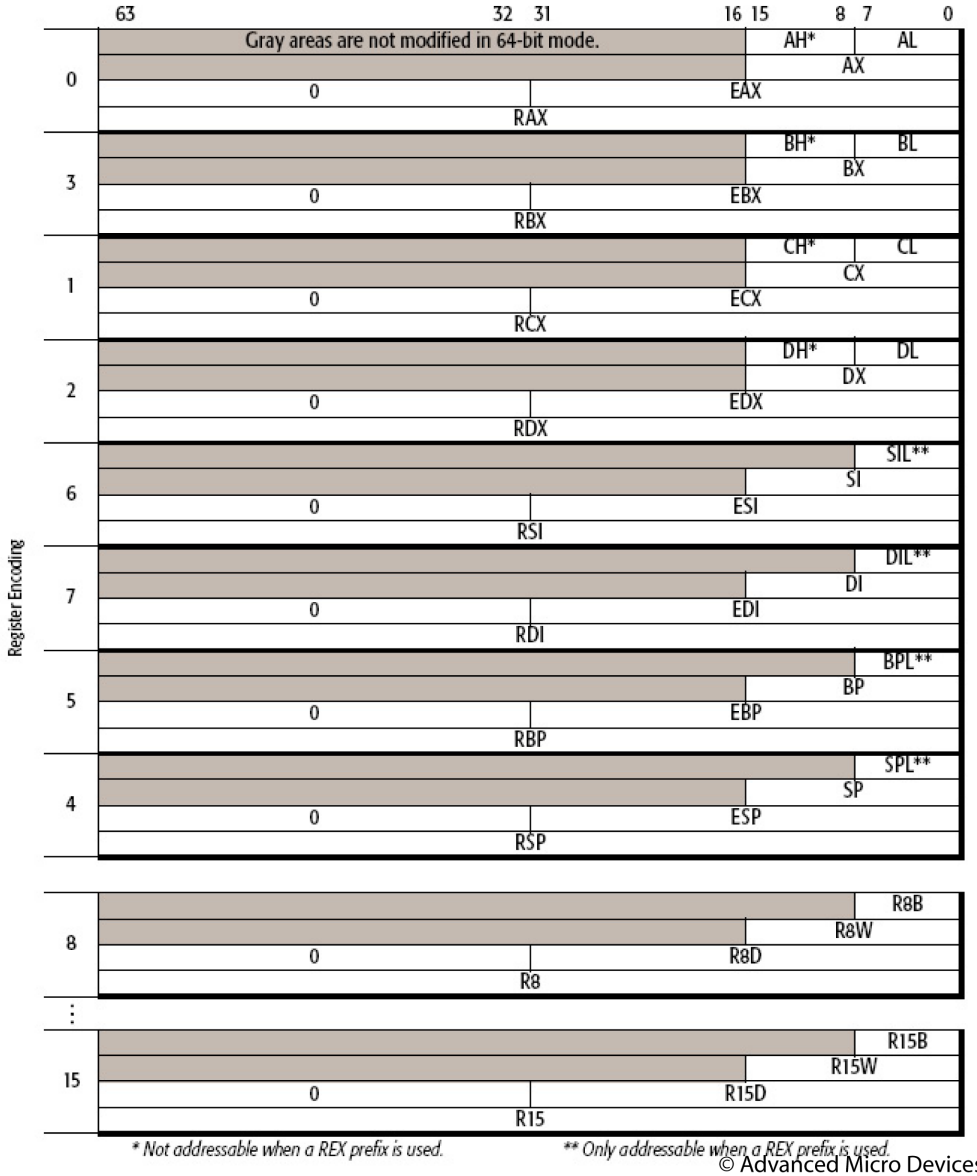
Modos de execução

Modo de operação		Sistema operacional	Endereçamento	Operando Padrão
Modo	**Submodo**			
Long	64-bit	64-bit	64-bit	32-bit
Long	Compatibilidade	64-bit	32/16-bit	32/16-bits
Legado	Protegido	32-bit	32/16-bit	32/16-bit
Legado	Virtual	32-bit	16-bit	16-bit
Legado	Real	16-bit	16-bit	16-bit

Registradores

- Os registradores do x86 foram extendidos para 64 bits e receberam o prefixo 'R'.
  - Registrador de 64 bits correspondente ao EAX $\rightarrow$ RAX.
- Foram acrescentados mais 8 registradores de uso geral: R8-R15.
- Também foram acrescentados 8 registradores XMM: XMM8-XMM15
- O apontador de instrução, EIP, foi ampliado também, e agora se chama RIP
- Registrador de FLAGS aumentou, embora não foram acrescentadas novas flags

Registradores (cont.)



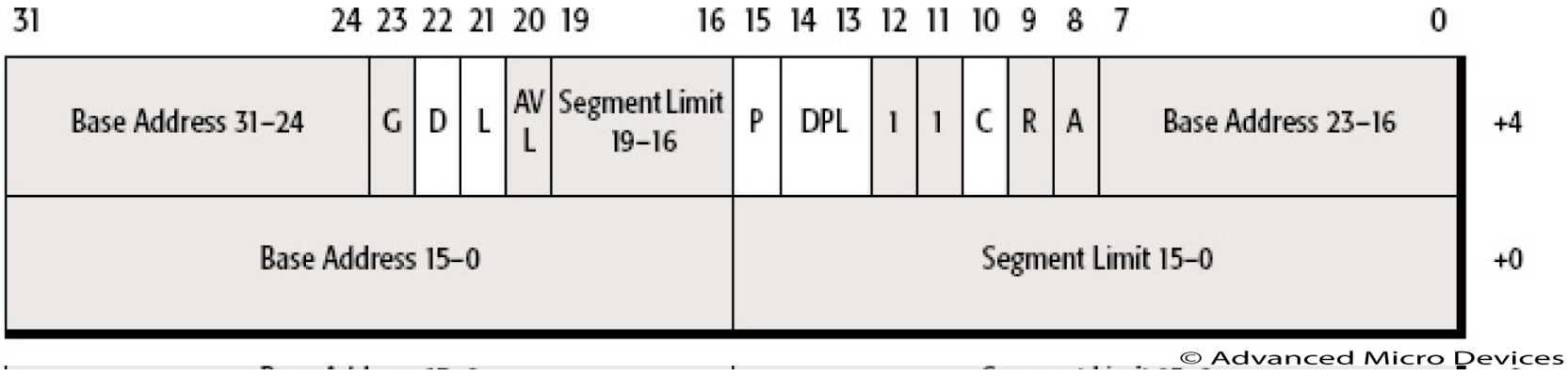
Endereçamento

- Em 64 bits, a memória é “achatada”, um espaço de 64 bits não-segmentado
  - Sistemas operacionais modernos já tratam a memória como um espaço contíguo, ignorando a segmentação
  - Manejamento de memória se torna mais simples no S.O.
  - Registradores de segmento não são mais utilizados, com algumas exceções
- O processador ainda lê o descritor de segmento
- Registradores GS e FS ainda são utilizados, em algumas ocasiões

Endereçamento (cont.)

- É possível endereçar memória relativa ao RIP, não apenas em operações de mudança de controle
- O maior desvio é de 32 bits — para desvios maiores é necessário fazer endereçamento indireto
- Programas de 16 ou 32 bits executando em modo de 64 bits só conseguem acessar os 4G inferiores da memória virtual

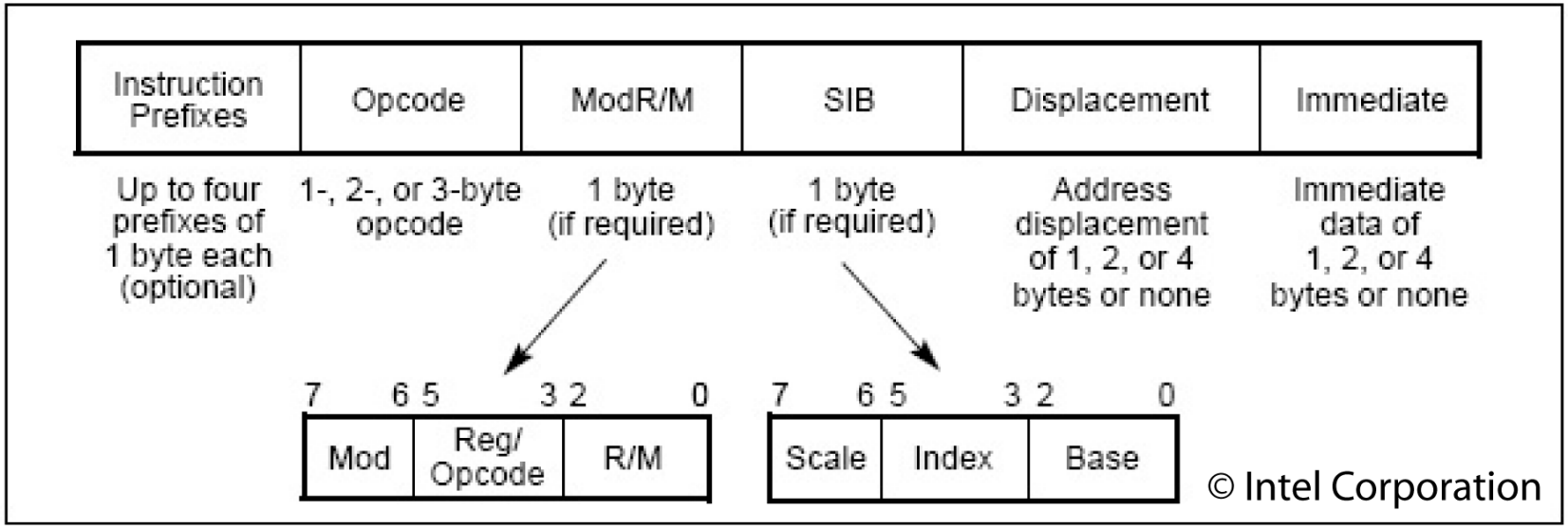
O descritor de segmento de código em 64 bits



Instruções

- Formato da instrução é igual ao do x86-32, com tamanho máximo de 15 bytes
- Maioria das instruções de uso geral foram mantidas
  - Instruções mais arcaicas foram removidas, como aquelas que operam sobre valores ASCII ou BCD.
  - Pulos e chamadas de 64 bits não são permitidas, pelo fato do deslocamento ter no máximo 32 bits
- Máximo valor de imediato é de 32 bits

Formato de instrução



Prefixo REX

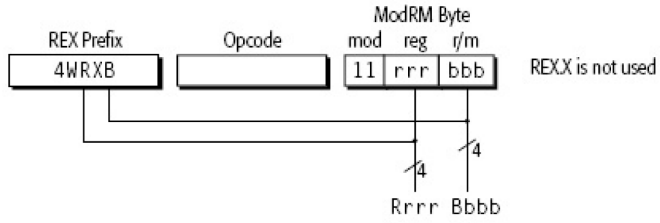
- O prefixo é utilizado para permitir acesso a mais do que os 8 registradores padrão
- Também permite acesso aos registradores de 64 bits
- Permite acesso aos campos dos registradores de maneira mais consistente

Prefixo REX (cont.)

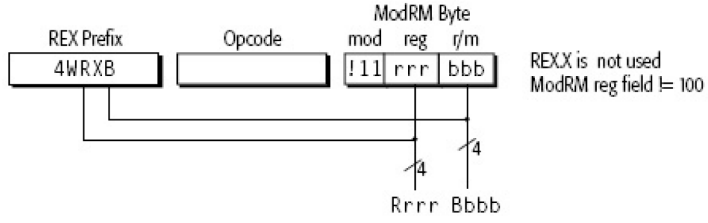
Mnemônico	Posição	Definição
-	7-4	0100
REX.W	3	0=Tamanho de operando padrão 1=Tamanho de operando de 64 bits
REX.R	2	1=Extensão do campo reg do *byte* ModR/M, permitindo acesso a 16 registradores
REX.X	1	1=Extensão do campo *index* do byte SIB, permitindo acesso a 16 registradores
REX.X	0	1=Extensão do campo *r/m* do byte ModR/M, permitindo acesso a 16 registradores

Prefixo REX (cont.)

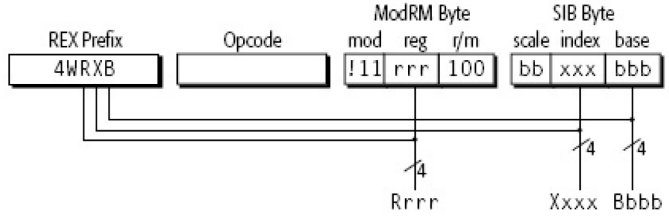
Case 1: Register-Register Addressing (No Memory Operand)



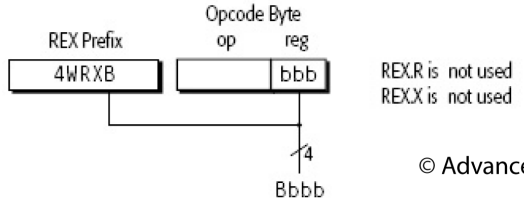
Case 2: Memory Addressing Without an SIB Byte



Case 3: Memory Addressing With an SIB Byte



Case 4: Register Operand Coded in Opcode Byte



513-302.eps

Ponto flutuante

- Arquitetura permite operações de ponto flutuante pela FPU x87, instruções SSE(2/3) e MMX/3DNow!
- AMD recomenda utilizar instruções SSE no lugar das instruções da FPU x87
- Na versão 64 bits do Windows XP os registradores MMX e do FPU não são salvos em mudanças de contexto

Bit NX

- Bit No eXecute, previne que dados sejam executados
- É lido da tabela de páginas, quando aquelas páginas são carregadas
- Acusa GPE caso o bit mais significativo da entrada da página estiver setada
- Intel implementou como bit XD (eXecute Disable) — AMD anunciou como “proteção contra vírus”

Diferenças entre AMD e Intel

- Atualmente iguais: implementam mesmas instruções, incluindo SSE
- Versões anteriores apresentavam pequenas incompatibilidades


Advanced Micro Devices.
AMD64 Architecture Programmer's Manual Volume 1: Applications Programming, 2005.


Advanced Micro Devices.
AMD64 Architecture Programmer's Manual Volume 2: System Programming, 2005.


Advanced Micro Devices.
AMD64 Architecture Programmer's Manual Volume 3: General Purpose And System Instructions, 2005.


Intel Corporation.
IA-32 Intel Architecture Software Developer's Manual Volume 1: Basic Architecture, 2005.


Intel Corporation.
IA-32 Intel Architecture Software Developer's Manual Volume 2A: Instruction Set Reference, A-M, 2005.