Übung zu Betriebssysteme

x64-Assembler im Detail

28. November 2019

Andreas Ziegler, Bernhard Heinloth, Christian Eichler

Lehrstuhl für Informatik 4
Friedrich-Alexander-Universität Erlangen-Nürnberg

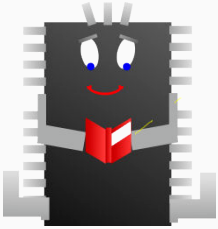
Lehrstuhl für Verteilte Systeme
und Betriebssysteme

FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

TECHNISCHE FAKULTÄT

Mensch vs. CPU

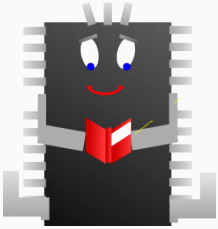
```
48 83 ec 18
be a0 38 02 01
bf a0 3c 02 01
e8 cd bb ff ff
31 d2
be 25 00 00 00
bf 00 3d 02 01
e8 8c c2 ff ff
be 16 c2 00 01
bf a0 3c 02 01
e8 0d f3 ff ff
be e0 b5 00 01
48 89 c7
e8 a0 f6 ff ff
e8 ab d3 ff ff
bf 00 38 02 01
e8 61 ba ff ff
e8 ec d2 ff ff
e8 c7 7f ff ff
fb
90
48 8d 7c 24 08
c7 44 24 08 00 00 00 00
c7 44 24 0c 00 00 00 00
e8 eb f6 ff ff
...
```



Quellen: publicdomainvectors.org (Glühbirne, Prozessor), VectorStock (Programmierer)

Mensch vs. CPU

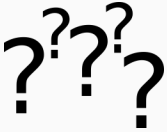
```
48 83 ec 18
be a0 38 02 01
bf a0 3c 02 01
e8 cd bb ff ff
31 d2
be 25 00 00 00
bf 00 3d 02 01
e8 8c c2 ff ff
be 16 c2 00 01
bf a0 3c 02 01
e8 0d f3 ff ff
be e0 b5 00 01
48 89 c7
e8 a0 f6 ff ff
e8 ab d3 ff ff
bf 00 38 02 01
e8 61 ba ff ff
e8 ec d2 ff ff
e8 c7 7f ff ff
fb
90
48 8d 7c 24 08
c7 44 24 08 00 00 00 00
c7 44 24 0c 00 00 00 00
e8 eb f6 ff ff
...
```

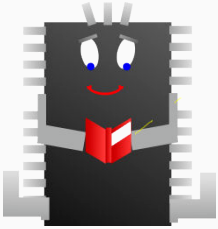


Quellen: publicdomainvectors.org (Glühbirne, Prozessor), VectorStock (Programmierer)

Mensch vs. CPU

```
48 83 ec 18
be a0 38 02 01
bf a0 3c 02 01
e8 cd bb ff ff
31 d2
be 25 00 00 00
bf 00 3d 02 01
e8 8c c2 ff ff
be 16 c2 00 01
bf a0 3c 02 01
e8 0d f3 ff ff
be e0 b5 00 01
48 89 c7
e8 a0 f6 ff ff
e8 ab d3 ff ff
bf 00 38 02 01
e8 61 ba ff ff
e8 ec d2 ff ff
e8 c7 7f ff ff
fb
90
48 8d 7c 24 08
c7 44 24 08 00 00 00 00
c7 44 24 0c 00 00 00 00
e8 eb f6 ff ff
...
```

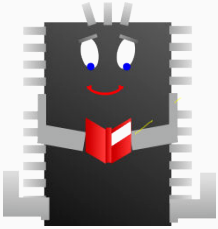




Quellen: publicdomainvectors.org (Glühbirne, Prozessor), VectorStock (Programmierer)

Mensch vs. CPU

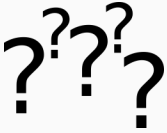
```
extern "C" int main() {
    CGA_Stream::arrange(kout, dout);
    kout.setpos(37, 0);
    kout << "MPStuBs" << endl;

    IOAPIC::init();
    keyboard.Keyboard::plugin();

    unsigned int numCPUs = System::getNumberOfCPUs();
    DBG_VERBOSE << "Number of CPUs: " << numCPUs << endl;
    ApplicationProcessor::boot();

    CPU::Interrupt::enable();

    Application application(0);
    KeyboardApplication kapp(0);

    application.action();
    kapp.action();

    return 0;
}
```

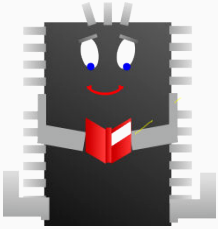


Quellen: publicdomainvectors.org (Glühbirne, Prozessor), VectorStock (Programmierer)

Mensch vs. CPU

```
extern "C" int main() {
    CGA_Stream::arrange(kout, dout);
    kout.setpos(37, 0);
    kout << "MPStuBs" << endl;

    IOAPIC::init();
    keyboard.Keyboard::plugin();

    unsigned int numCPUs = System::getNumberOfCPUs();
    DBG_VERBOSE << "Number of CPUs: " << numCPUs << endl;
    ApplicationProcessor::boot();

    CPU::Interrupt::enable();

    Application application(0);
    KeyboardApplication kapp(0);

    application.action();
    kapp.action();

    return 0;
}
```

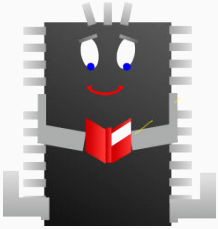




Quellen: publicdomainvectors.org (Glühbirne, Prozessor), VectorStock (Programmierer)

Mensch vs. CPU

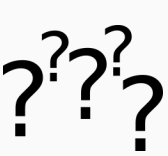
```
extern "C" int main() {
    CGA_Stream::arrange(kout, dout);
    kout.setpos(37, 0);
    kout << "MPStuBs" << endl;

    IOAPIC::init();
    keyboard.Keyboard::plugin();

    unsigned int numCPUs = System::getNumberOfCPUs();
    DBG_VERBOSE << "Number of CPUs: " << numCPUs << endl;
    ApplicationProcessor::boot();

    CPU::Interrupt::enable();

    Application application(0);
    KeyboardApplication kapp(0);

    application.action();
    kapp.action();

    return 0;
}
```

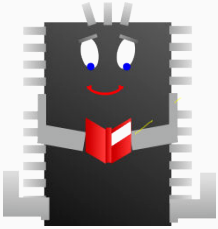


Quellen: publicdomainvectors.org (Glühbirne, Prozessor), VectorStock (Programmierer)

Mensch vs. CPU

```
extern "C" int main() {
    CGA_Stream::arrange(kout, dout);
    kout.setpos(37, 0);
    kout << "MPStuBs" << endl;

    IOAPIC::init();
    keyboard.Keyboard::plugin();

    unsigned int numCPUs = System::getNumberOfCPUs();
    DBG_VERBOSE << "Number of CPUs: " << numCPUs << endl;
    ApplicationProcessor::boot();

    CPU::Interrupt::enable();

    Application application(0);
    KeyboardApplication kapp(0);

    application.action();
    kapp.action();

    return 0;
}
```





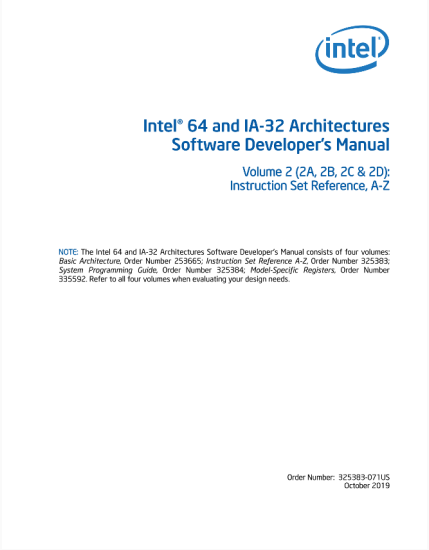
Quellen: publicdomainvectors.org (Glühbirne, Prozessor), VectorStock (Programmierer)

Kompromiss: Assembler Language

```
sub    rsp,0x18
mov    esi,0x10238a0
mov    edi,0x1023ca0
call   1007ac0 <CGA_Stream::arrange(CGA_Stream&, CGA_Stream*)>
xor    edx,edx
mov    esi,0x25
mov    edi,0x1023d00
call   1008190 <CGA_Window::setpos(int, int)>
mov    esi,0x100c216
mov    edi,0x1023ca0
call   100b220 <O_Stream::operator<<(char const*)>
mov    esi,0x100b5e0
mov    rdi,rax
call   100b5c0 <O_Stream::operator<<(O_Stream& (*)(O_Stream&))>
call   10092d0 <IOAPIC::init()>
mov    edi,0x1023800
call   1007990 <Keyboard::plugin()>
call   1009220 <System::getNumberOfCPUs()>
call   1003f00 <ApplicationProcessor::boot()>
sti
nop
lea    rdi,[rsp+0x8]
mov    [rsp+0x8],0x0
mov    [rsp+0xc],0x0
call   100b640 <Application::action()>
lea    rdi,[rsp+0xc]
call   100b690 <KeyboardApplication::action()>
xor    eax,eax
add    rsp,0x18
ret
```

- Schnittstelle der **ISA**
- **Mnemonics** statt Bytes
- 1:1-Übersetzung der Befehle in Maschinencode durch Assembler

Befehle der x64-Architektur



Intel® 64 and IA-32 Architectures
Software Developer's Manual

Volume 2 (2A, 2B, 2C & 2D):
Instruction Set Reference, A-Z

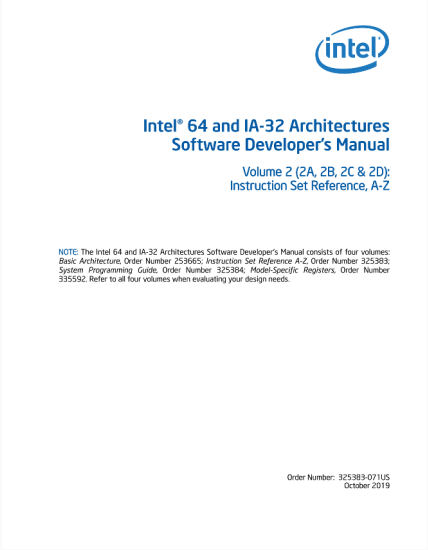
NOTE: The Intel 64 and IA-32 Architectures Software Developer's Manual consists of four volumes: *Basic Architecture*, Order Number 253665; *Instruction Set Reference A-Z*, Order Number 325383; *System Programming Guide*, Order Number 325384; *Model-Specific Registers*, Order Number 335592. Refer to all four volumes when evaluating your design needs.

Order Number: 325383-071US
October 2019

- Dokumentation der Instruktionen: Intel-Manual, Volume 2

Quelle: KnowYourMeme

Befehle der x64-Architektur



Intel® 64 and IA-32 Architectures
Software Developer's Manual

Volume 2 (2A, 2B, 2C & 2D):
Instruction Set Reference, A-Z

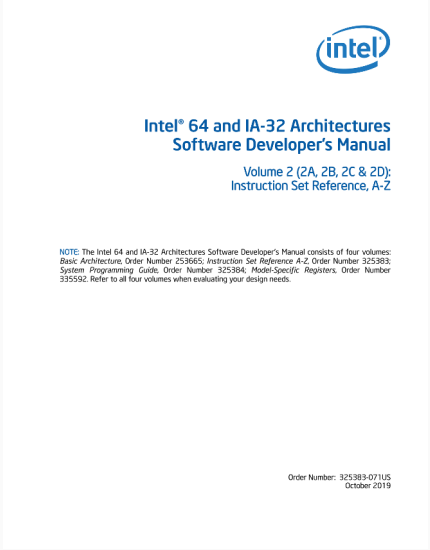
NOTE: The Intel 64 and IA-32 Architectures Software Developer's Manual consists of four volumes: *Basic Architecture*, Order Number 253665; *Instruction Set Reference A-Z*, Order Number 325383; *System Programming Guide*, Order Number 325384; *Model-Specific Registers*, Order Number 335592. Refer to all four volumes when evaluating your design needs.

Order Number: 325383-071US
October 2019

- Dokumentation der Instruktionen: Intel-Manual, Volume 2
- $>$ **2300** Seiten

Quelle: KnowYourMeme

Befehle der x64-Architektur



- Dokumentation der Instruktionen: Intel-Manual, Volume 2
- $>$ **2300** Seiten

Quelle: KnowYourMeme

Syntaxunterschiede bei x86-Assembler

Intel:

```
mov ebx, 0x17
```

(Ziel, Quelle)

`objdump -M intel`

AT&T:

```
mov $0x17, %ebx
```

(Quelle, Ziel)

Standard bei `objdump`

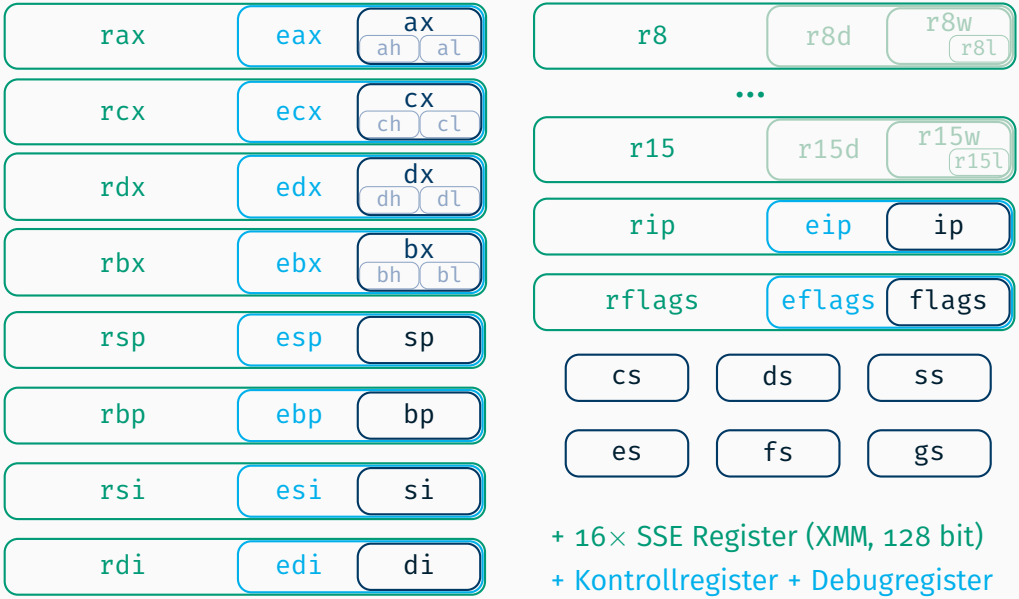
Eine einfache Einführung

- Ab hier: **Intel-Syntax** (`<Op> <Ziel> <Quelle>`)
  - Wird von NASM (Netwide Assembler) verwendet

Eine einfache Einführung

- Ab hier: **Intel-Syntax** (`<Op> <Ziel> <Quelle>`)
  - Wird von NASM (Netwide Assembler) verwendet
- Grundlegender Aufbau der x64-Architektur
  - 16 General-Purpose-Register
  - Instruktionszeiger
  - Stack Pointer (zeigt auf **zuletzt abgelegtes** Datum)

x64 (Long Mode) Register



+ 16× SSE Register (XMM, 128 bit)
+ Kontrollregister + Debugregister

Programmieren in Assembler: `mov`

Berechnungen generell auf Registern

Wie kommen Daten dort hin?

Programmieren in Assembler: `mov`

Berechnungen generell auf Registern

Wie kommen Daten dort hin?

→ `mov`-Instruktion

Register ← **Konstante** `mov rax, 42`

Programmieren in Assembler: `mov`

Berechnungen generell auf Registern

Wie kommen Daten dort hin?

→ `mov`-Instruktion

Register ← **Konstante** `mov rax, 42`

Register ← **Register** `mov rax, rcx`

Programmieren in Assembler: mov

Berechnungen generell auf Registern

Wie kommen Daten dort hin?

→ mov-Instruktion

Register ← Konstante	`mov rax, 42`
Register ← Register	`mov rax, rcx`
Register ↔ Speicher	`mov rax, [0xb8000]`
	`mov [0xb8000 + 4], rax`
	`mov rax, [rcx + rdx]`
	`mov rax, [rsp]`
	~~`mov [0xb8000], [0xb8002]`~~

Besonderheiten bei `mov`

- Was passiert beim Schreiben von Teilen von Registern?

Besonderheiten bei `mov`

- Was passiert beim Schreiben von Teilen von Registern?

  `mov eax, XX` `eax` wird gesetzt, obere Hälfte **genullt**

Besonderheiten bei `mov`

- Was passiert beim Schreiben von Teilen von Registern?

  `mov eax, XX` `eax` wird gesetzt, obere Hälfte **genullt**

  `mov ax, XX` `ax` wird gesetzt, **Rest unverändert**

  `mov al, XX` `al` wird gesetzt, **Rest unverändert**

  Falls Rest gesetzt werden muss: `movzx`, `movsx`

Details zur Performance bei partiellem Schreiben: → StackOverflow

movfuscator - the single instruction C compiler

mov auf x86 ist Turing-vollständig!

→ https://github.com/xoreaxeaxeax/movfuscator

movfuscator - the single instruction C compiler

mov auf x86 ist Turing-vollständig!

```
int is_prime(int x)
{
  int  i;
  if (x==1) {
    return 0;
  }
  if  (x==2)  {
    return 1;
  }
  for  (i=2; i*i<=x; i++) {
    if  (x%i==0)  {
      return  0;
    }
  }
  return 1;
}
```

→ https://github.com/xoreaxeaxeax/movfuscator

movfuscator - the single instruction C compiler

mov auf x86 ist Turing-vollständig!

```c
int is_prime(int x)
{
  int  i;
  if (x==1) {
    return 0;
  }
  if  (x==2)  {
    return 1;
  }
  for  (i=2; i*i<=x; i++) {
    if  (x%i==0)  {
      return  0;
    }
  }
  return 1;
}
```

```
<is_prime>:
  push  ebp
  mov   ebp,esp
  sub   esp,0x10
  cmp   DWORD PTR [ebp+0x8],0x1
  jne   8048490 <is_prime+0x13>
  mov   eax,0x0
  jmp   80484cf <is_prime+0x52>
  cmp   DWORD PTR [ebp+0x8],0x2
  jne   804849d <is_prime+0x20>
  mov   eax,0x1
  jmp   80484cf <is_prime+0x52>
  mov   DWORD PTR [ebp-0x4],0x2
  jmp   80484be <is_prime+0x41>
  mov   eax,DWORD PTR [ebp+0x8]
  cdq
  idiv  DWORD PTR [ebp-0x4]
  mov   eax,edx
  test  eax,eax
  jne   80484ba <is_prime+0x3d>
  mov   eax,0x0
  jmp   80484cf <is_prime+0x52>
  add   DWORD PTR [ebp-0x4],0x1
  mov   eax,DWORD PTR [ebp-0x4]
  imul  eax,DWORD PTR [ebp-0x4]
  cmp   eax,DWORD PTR [ebp+0x8]
  jle   80484a6 <is_prime+0x29>
  mov   eax,0x1
  leave
  ret
```

→ https://github.com/xoreaxeaxeax/movfuscator

movfuscator - the single instruction C compiler

mov auf x86 ist Turing-vollständig!

```c
int is_prime(int x)
{
  int  i;
  if (x==1) {
    return 0;
  }
  if  (x==2)  {
    return 1;
  }
  for  (i=2; i*i<=x; i++) {
    if  (x%i==0)  {
      return  0;
    }
  }
  return 1;
}
```

```
<is_prime>:
  push  ebp
  mov   ebp,esp
  sub   esp,0x10
  cmp   DWORD PTR [ebp+0x8],0x1
  jne   8048490 <is_prime+0x13>
  mov   eax,0x0
  jmp   80484cf <is_prime+0x52>
  cmp   DWORD PTR [ebp+0x8],0x2
  jne   804849d <is_prime+0x20>
  mov   eax,0x1
  jmp   80484cf <is_prime+0x52>
  mov   DWORD PTR [ebp-0x4],0x2
  jmp   80484be <is_prime+0x41>
  mov   eax,DWORD PTR [ebp+0x8]
  cdq
  idiv  DWORD PTR [ebp-0x4]
  mov   eax,edx
  test  eax,eax
  jne   80484ba <is_prime+0x3d>
  mov   eax,0x0
  jmp   80484cf <is_prime+0x52>
  add   DWORD PTR [ebp-0x4],0x1
  mov   eax,DWORD PTR [ebp-0x4]
  imul  eax,DWORD PTR [ebp-0x4]
  cmp   eax,DWORD PTR [ebp+0x8]
  jle   80484a6 <is_prime+0x29>
  mov   eax,0x1
  leave
  ret
```

```
<is_prime>:
  mov  eax,ds:0x83fc638
  mov  edx,0x88048744
  mov  ds:0x81fc4c0,eax
  mov  DWORD PTR ds:0x81fc4c4,edx
  mov  eax,0x0
  mov  ecx,0x0
  mov  edx,0x0
  mov  al,ds:0x81fc4c0
  mov  ecx,DWORD PTR [eax*4+0x8056ad0]
  mov  dl,BYTE PTR ds:0x81fc4c4
  mov  dl,BYTE PTR [ecx+edx*1]
  mov  DWORD PTR ds:0x81fc4b0,edx
  mov  al,ds:0x81fc4c1
  mov  ecx,DWORD PTR [eax*4+0x8056ad0]
  mov  dl,BYTE PTR ds:0x81fc4c5
  mov  dl,BYTE PTR [ecx+edx*1]
  mov  DWORD PTR ds:0x81fc4b4,edx
  mov  al,ds:0x81fc4c2
  mov  ecx,DWORD PTR [eax*4+0x8056ad0]
  mov  dl,BYTE PTR ds:0x81fc4c6
  mov  dl,BYTE PTR [ecx+edx*1]
  mov  DWORD PTR ds:0x81fc4b8,edx
  mov  al,ds:0x81fc4c3
  mov  ecx,DWORD PTR [eax*4+0x8056ad0]
  mov  dl,BYTE PTR ds:0x81fc4c7
  mov  dl,BYTE PTR [ecx+edx*1]
  mov  DWORD PTR ds:0x81fc4bc,edx
  mov  eax,ds:0x81fc4b0
  mov  edx,DWORD PTR ds:0x81fc4b4
<...> (5710 more lines)
```

→ https://github.com/xoreaxeaxeax/movfuscator

Operationen mit dem Stack

Register ← **Stack**

```
pop rax
```

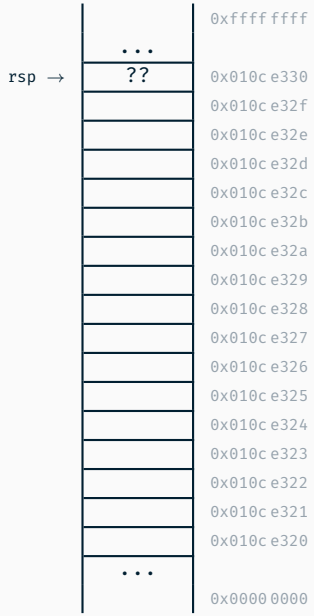
```
mov rax, [rsp]
add rsp, 8
```

Stack ← **Register**

```
push rax
```

```
sub rsp, 8
mov [rsp], rax
```

Stack-Operationen am Beispiel

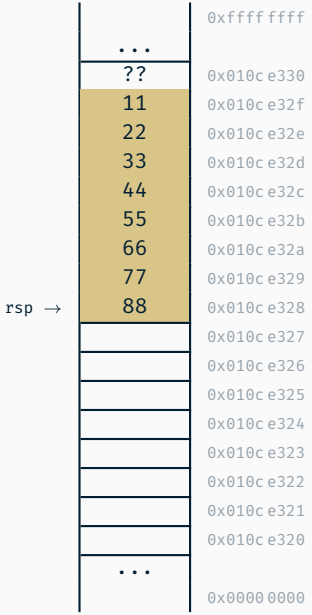


0x1122334455667788 rax

0x???????????????? rcx

```
long long i = 0x11223344556778811;
```

Stack-Operationen am Beispiel

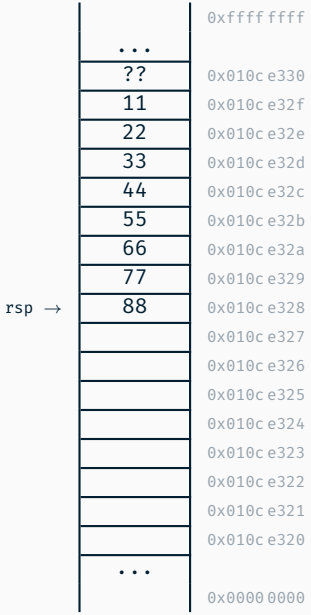


0x1122334455667788 rax

0x???????????????? rcx

```
    mov rax, 0x1122334455667788
→   push rax
    mov eax, 0xaabbccdd
    push rax
    pop rcx
    mov rcx, 0
    push rcx
```

Stack-Operationen am Beispiel

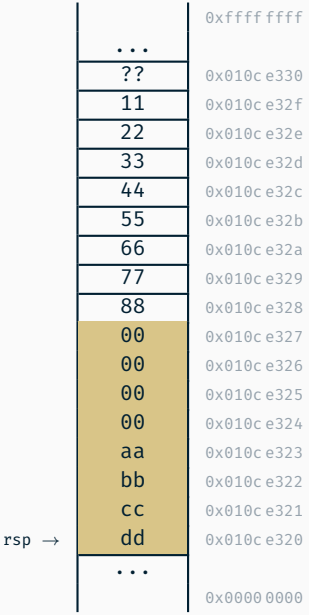


0x00000000aabbccdd rax

0x???????????????? rcx

```
    mov rax, 0x1122334455667788
    push rax
→   mov eax, 0xaabbccdd
    push rax
    pop rcx
    mov rcx, 0
    push rcx
```

Stack-Operationen am Beispiel

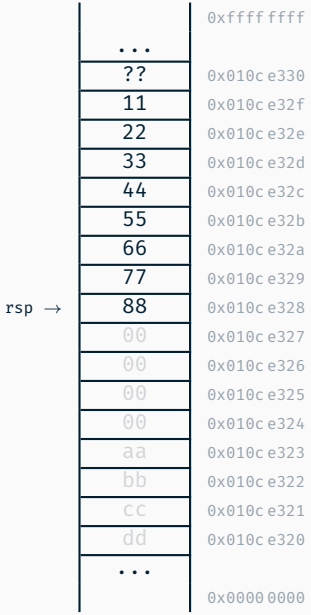


0x00000000aabbccdd rax

0x???????????????? rcx

```
    mov rax, 0x1122334455667788
    push rax
    mov eax, 0xaabbccdd
→   push rax
    pop rcx
    mov rcx, 0
    push rcx
```

Stack-Operationen am Beispiel

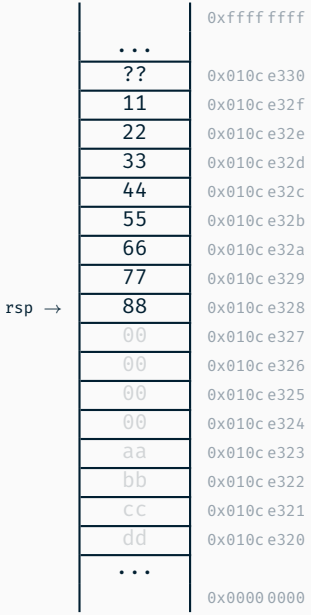


0x00000000aabbccdd rax

0x00000000aabbccdd rcx

```
    mov rax, 0x1122334455667788
    push rax
    mov eax, 0xaabbccdd
    push rax
→   pop rcx
    mov rcx, 0
    push rcx
```

Stack-Operationen am Beispiel

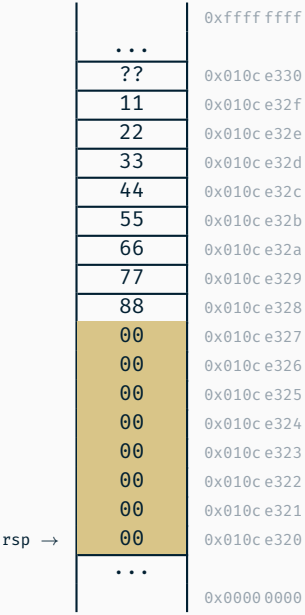


0x00000000aabbccdd rax

0x0000000000000000 rcx

```
    mov rax, 0x1122334455667788
    push rax
    mov eax, 0xaabbccdd
    push rax
    pop rcx
→   mov rcx, 0
    push rcx
```

Stack-Operationen am Beispiel



0x00000000aabbccdd rax

0x0000000000000000 rcx

```
mov rax, 0x1122334455667788
push rax
mov eax, 0xaabbccdd
push rax
pop rcx
mov rcx, 0
→ push rcx
```

Mathematische Operationen

Addition/Subtraktion

```
add rax, 4              x += 4;
sub qword [rax], rcx    *x -= rcx;
inc rax                 x++;
dec rax                 x--;
```

Mathematische Operationen

Addition/Subtraktion	`add rax, 4`	`x += 4;`
	`sub qword [rax], rcx`	`*x -= rcx;`
	`inc rax`	`x++;`
	`dec rax`	`x--;`
Bit-Operationen	`and rax, 0xff`	`x &= 0xff;`
	`or rax, [rcx]`	`x |= *rcx;`
	`xor rax, 0xaa`	`x ^= 0xaa;`
	`not rax`	`x = !x;`
	`neg rcx`	`x = ~x;`
	`shl rax, 1`	`x <<= 1;`
	`shr rax, 1`	`x >>= 1;`

Kontrollfluss-Beeinflussung

Labels als Sprungziele

```
block:
  add rcx, 1
  <...>
```

Einfache Sprünge `jmp block`

Bedingte Sprünge `je/jne/jg/jge/jl/jle/jz block`

Kontrollfluss-Beeinflussung

Labels als Sprungziele

```
block:
  add rcx, 1
  <...>
```

Einfache Sprünge `jmp block`

Bedingte Sprünge `je/jne/jg/jge/jl/jle/jz block`

Woher kommt die Bedingung für einen bedingten Sprung?

Kontrollfluss-Beeinflussung

Labels als Sprungziele
```
block:
  add rcx, 1
  <...>
```

Einfache Sprünge `jmp block`

Bedingte Sprünge `je/jne/jg/jge/jl/jle/jz block`

Woher kommt die Bedingung für einen bedingten Sprung?

- Statusregister (`rflags`)
- Mathematische Operationen und Vergleiche setzen Flags im Statuswort

Vergleiche
```
cmp rax, rdx
cmp rax, 0x10
≅ sub rax, 0x10
  aber rax unverändert
```

Funktionsaufrufe

Funktionsaufruf

```
call function
```

```
push <next RIP>
jmp function
```

Rückkehr aus Funktion

```
ret
```

```
pop rip
```

Rückkehr aus Interrupt

```
iretq
```

Stellt Hardware-Kontext (`rip`, `cs`, `rflags`) wieder her, siehe Übung 2

Parameterübergabe

Verschiedene Konventionen für

- Übergabe von Parametern
- Flüchtigkeit von Registern
- Umgang mit Stack in Aufrufer und aufgerufener Funktion

→ **x86** (32 Bit)

- 12 verschiedene Konventionen ☹
- Linux/C/GCC-Standard (`cdecl`):
  - Parameter auf dem Stack, letzte Parameter zuerst
  - Rückgabewert in `eax`
  - Aufrufer muss `eax`, `ecx`, `edx` sichern, falls Wert noch benötigt

Parameterübergabe (x64)

- **x64**: nur noch zwei Konventionen (Microsoft und System V)
- System V Application Binary Interface:
  - 6 Parameter in Registern (`rdi, rsi, rdx, rcx, r8, r9`), Rest auf dem Stack
  - Rückgabewert in `rax` oder `rdx:rax`
  - **Nicht-**flüchtige Register: `rbx, rbp, r12 - r15`
  - C++-Code: **`this`** ist impliziter erster Parameter

Demotime!

Wir schreiben Code in Assembler