

Special Algorithms

AES KeyGen Assist

AES aeskeygenassist

NOTE: Assist in expanding the AES cipher key by computing steps towards generating a round key for encryption cipher using data from a and an 8-bit round constant specified in imm.

Miscellaneous

Pause

pause

is a spin-wait loop. This can help improve the performance and power consumption of spin-wait

Load Loading data into an SSE register

Set Reversed

AVX setr

NOTE: Sets and returns an SSE register with input values. E.g.,

register with imput vanues. L.g., epi3 wersion takes 16 input parameters. The order in the register is reversed, i.e. the first input gets stored in the lowest bits. The 128bit epi64 version takes two MMX registers. For 256bit, there is only an epi64x

Stream Load

sse2 stream_load

device without going through the cache hierachy.

mi stream_load_si128(mi* ptr

Fast Unaligned

Load

1ddqu

OTE: Loads 128bit integer data

into SSE register. Is faster than loadu if value crosses cache line boundary. Should be preferred

mi lddqu_si128(mi* ptr)

Load Unaligned

sse2 loadu

pd, ps, sil6-sil28 NOTE: Loads 128 bit or less (for

Aligned Stream

Store stream

Unaligned

Store

sse storeu

v storeu_pd(v* ptr,m a)

Store Storing data from an SSE register into memory or registers

Aligned Store Storing data to a memory address which must be 16-byte aligned (or 32-byte for 256bit instructions)

Unaligned Store Storing data to a memory address which does not have to be aligned to a specific boundary

Aligned

Reverse Store

storer

TE: Stores the elements from

pd,ps[SSE]

order. Memory must be 16-byte

v storer_pd(d* ptr,md a)

Store High

storeh

Store

NOTE: Loads 128 bit from

NOTE: Provide a hint to the

AES Inverse Mix

Columns

AES aesimc

columns transformation on the

Memory

address range triggers the monitoring hardware. Specify

Register I/O Loading data into an SSE register or storing data from an SSE register

Set Register Inserting data into an register without loading from memory

set

m128/m128d/i [AVX

NOTE: Sets and returns an SSE

Load Aligned

OTE: Loads 128 bit from

md load_pd(d* ptr)

Unaligned Load Load In Loading data from a memory address which does not have to be aligned to a specific boundary

Load High/Low

loadh/l

Load Single

stored in the highest bits.

Aligned Load

Loading data from a memory address which must be 16-byte aligned (or 32-byte for 256bit instructions)

Insert

loadr_ps(f* ptr

monitor



x86 Intrinsics Cheat Sheet

Jan Finis finis@in.tum.de

Legend

