packetscale

aesaes

хеш функция с общо предназначение

packetscale

хеш функция

packetscale

хеш функция с общо предназначение

(non-cryptographic, general purpose)

packetscale

Hash tables, Caches, Bloom filters, Finding duplicate records

packetscale

MurmurHash3

популярна такава
бърза, добро разпределение

https://code.google.com/p/smhasher/

packetscale

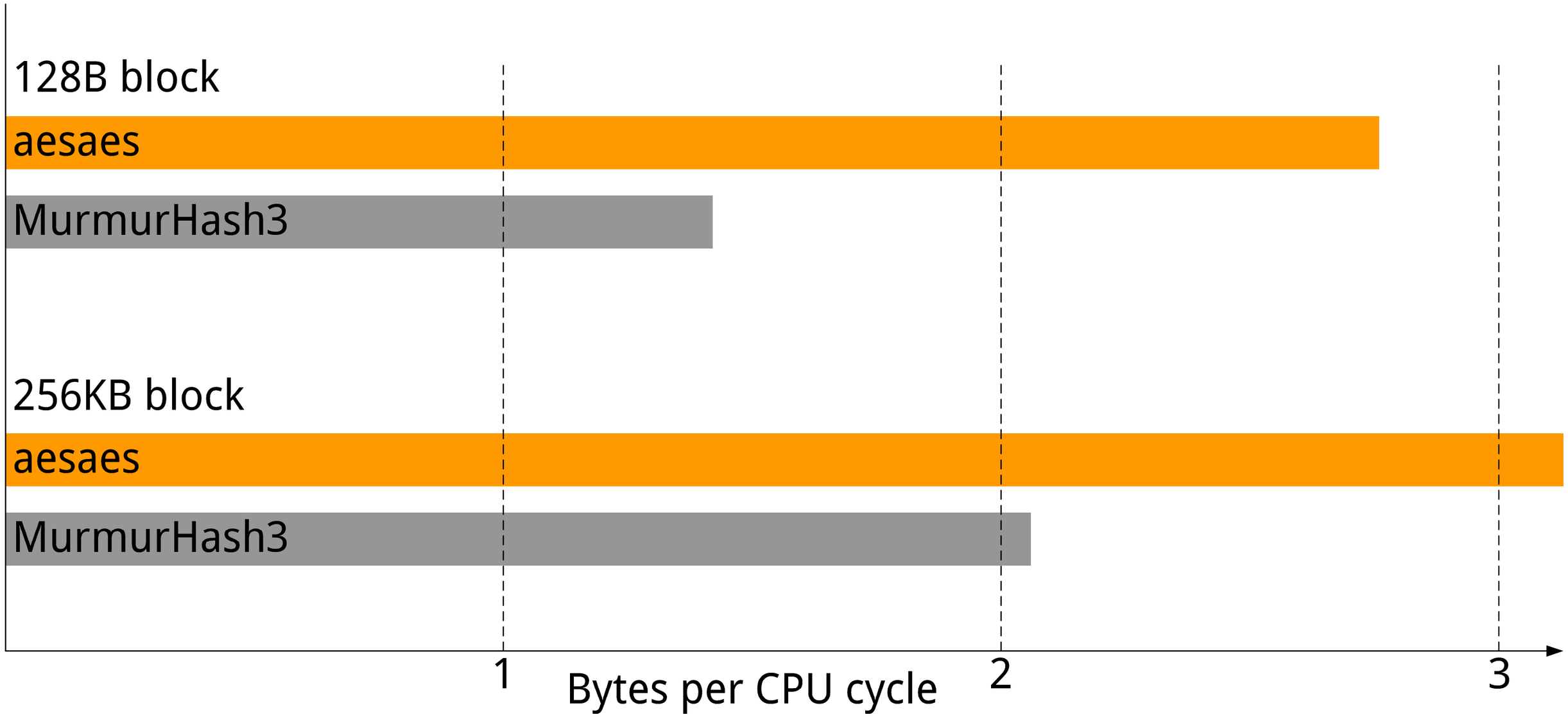
aesaes

наше откритие
по-бърза, също толкова добра

http://packetscale.com/aesaes

Скорост

packetscale



Разпределение

неразличимо от случайно

1M 128-битови стойности

в 2M кофи

~224000 кофи с колизии

максимална дълбочина = 7

Псевдокод


```
state = 0

for b in blocks
        tmp = b
        tmp = tmp.SubBytes.ShiftRows.MixColumns
        tmp = tmp.SubBytes.ShiftRows.MixColumns
        state = state XOR tmp

return state[0]
```

(прилича на 2 рунда от AES-128; ползва същите примитиви)

packetscale

IA32 разширение - AES-NI

2008

(почти) всички нови процесори от Intel и AMD

Лиценз

2-clause BSD

Зов за помощ

сайт и инструменти за разработчици

други варианти на функцията

“avalanche” и “bit bias” тестове

aesaes@packetscale.com

packetscale

Благодаря!


```
uint32_t
aesaes_string(void *_data, int size)
{
        __m128i                 *v = (__m128i*)_data;
        union __ZZ              tmp, state, key;

        state.v = key.v = _mm_setzero_si128();

        while (size > 0)
        {
                tmp.v = *v;

                v++;
                size -= sizeof( *v );

                tmp.v = _mm_aesenc_si128( tmp.v, key.v );
                tmp.v = _mm_aesenc_si128( tmp.v, key.v );

                state.v ^= tmp.v;
        }

        return state.vals[0];
}
```