t1ha – Fast Positive hash

- Быстрая, Переносимая, 64-битная
- Проходит все тесты SMHasher
- Не для криптографии

- Быстрее xxHash, City64…
- Лучше по качеству других быстрых (*)

https://github.com/leo-yuriev/t1ha

Короткие ключи (1..31 avg)

	MiB/Second	Cycles/Hash
t1ha	12228.80	**35.55**
fasthash64	5578.06	**43.42**
City64	11041.72	**51.77**
xxHash64	11123.15	**56.17**
metrohash	11808.92	**46.33**

Большие ключи (256K)

	MiB/Second	Cycles/Hash
t1ha	**12228.80**	35.55
FarmHash64	**12145.36**	60.12
City64	**11041.72**	51.77
xxHash64	**11123.15**	56.17
Spooky64	**11820.20**	60.39

Скорость / Качество
Скорость / Стойкость

- Стойкость = Циклы, исключают Скорость
- Супер-Качество исключает Супер-Скорость
- Качество НЕ исключает Скорость
- Но всё относительно…

- t1ha = speed with reasonable quality

t1ha - устройство

- Комбинация MUL-XOR и ADD-ROTATE-XOR
- Две injections point с „перекрестным опылением“
- Использование широкого множения
  - 64 x 64 = 128 бит
  - Отлично для x86 и E2K
  - Чуть хуже для ARM и MIPS
  - Плохо для слабых CPU

t1ha – история

- 1Hippeus (shared memory messaging)
  - выравнивание и границы страниц
  - MUL-XOR, ARX (ADD-ROT-XOR)
- 64-биный SEED
- Миксер EMUL (64x64 => 128)
- t1ha_aes, AVX, A/B...
- t1ha0(), t1ha1(), LE/BE

HighwayHash? (Google)

- Не путать с SipHash
- Нет **доказательств** стойкости
  или других качеств
- Только статистическая проверка

- Быстро только с SSE4

t1ha - планы

- t1ha0 – очень быстро, но не зафиксирована
- t1ha1 – быстро, 64 бита, LE

- t1ha2 – быстро, 64 бита, чуть качественнее, ждем E2K…
- t1ha3,4,5 – 128/256, некриптостойкие
- t1ha6,7 – 256/512, крипто-эксперименты

https://github.com/leo-yuriev/t1ha