Charts v2

Thursday, July 18, 2019 6:30 AM

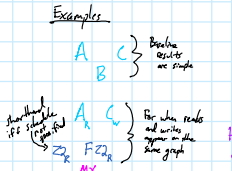
6x WORM & Freeram Experiments, Random & Sequential

Along w/ figures 4, 7, and 11 from v1

Experiments (6x)
- Baseline Freeram Sequential
- Scheduled Freeram Sequential
- Scheduled WORM Sequential
- Baseline Freeram Random
- Scheduled Freeram Random
- Scheduled WORM Random

Baseline (no wfq cipher scheduling)
Freeram == baseline WORM, have to test instead of 8a!
READ ONLY & READS
READ ONLY & READS

Examples



MX1 Mirrored schedule chacha 8 x chacha 20 w/ 1/4 storage crypthell w/ same cipher
SX2 Selective schedule chacha 8 x chacha 20 w/ 1/2 of storage crypthell w/ same cipher
SZ1 Selective schedule chacha 8 x Freestyle Fast w/ 1/4 storage crypthell w/ same cipher
FY3 Forward schedule chacha 20 x Freestyle Fast w/ 3/4 storage crypthell w/ same cipher
#Y3 etc.

Scheduling Ciphers
- A Chacha 8
- B Chacha 20
- C Freestyle Fast
- D, etc. Other ciphers

Cipher Pairs (scheduled)
- X Chacha 8 x Chacha 20
- Y Chacha 20 x Freestyle Fast
- Z Chacha 8 x Freestyle Fast

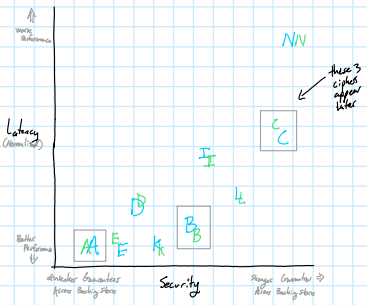
↑ primary ↑ swap

Ratio
- 1 1/4 swap, 3/4 primary
- 2 2/4 swap, 2/4 primary
- 3 3/4 swap, 1/4 primary

Scheduler
- M Mirrored
- S Selective
- F0,1,2 Forward 0, 1, 2 (respectively)

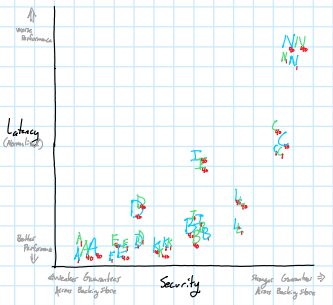
Notes
- All examples could exist for more than just 40MB results
- Normalized Y axis to max(Y) where appropriate
- Expand x to multiple charts w/ all combinations for dissertation
- Security of cipher pairs can be calculated w/: $S = c_1 + |c_1 - c_2|\lambda$, λ = ratio

1.1 Baseline cipher performance, 40MB reads, no scheduling



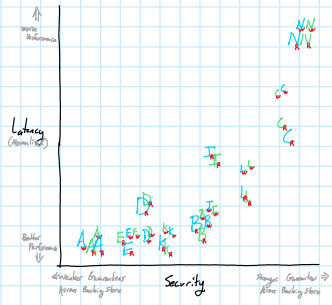
1.2 Baseline cipher performance, 40MB vs 1KB reads, no scheduling

(could separate into own charts instead)



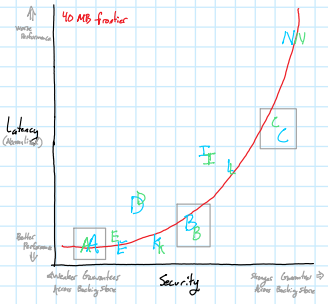
1.3 Baseline cipher performance, 40MB reads vs writes, no scheduling

(could separate into own charts instead)



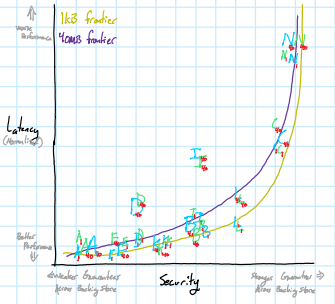
Argues that a rich tradeoff space exists between stream cipher in a storage context

1.1-alt Baseline cipher performance, 40MB reads, no scheduling



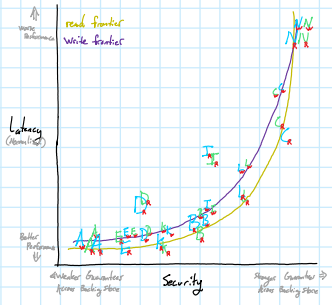
1.2-alt Baseline cipher performance, 40MB vs 1KB reads, no scheduling

(could separate into own charts instead)

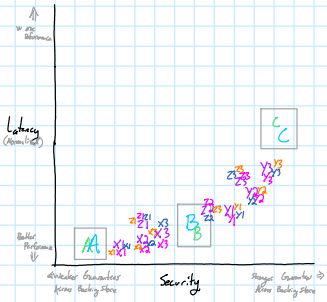


1.3-alt Baseline cipher performance, 40MB reads vs writes, no scheduling

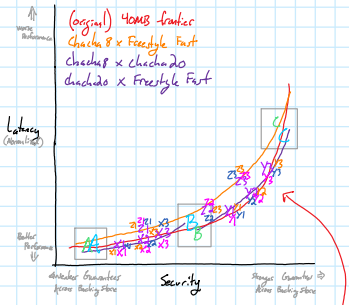
(could separate into own charts instead)



2.1 Cipher pair performance vs baseline, 40MB reads, forward 0 scheduling, all ratios



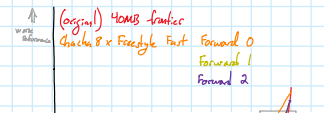
2.1-alt Cipher pair performance vs baseline, 40MB reads, forward 0 scheduling, all ratios



Demonstrates that we have a (new) mechanism to navigate this tradeoff space

Could also draw best-fit lines to make point?

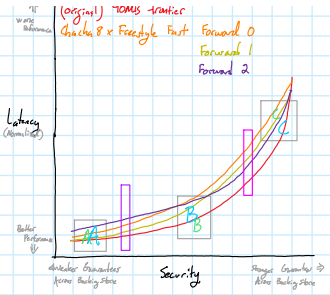
3.1 Cipher pair performance vs baseline, 40MB reads, all forward schedules, all ratios



Would this be a better argument with the curves for chacha 8 x chacha 20 and chacha 20 x Freestyle instead of chacha 8 x Freestyle?

Shows Forward scheduling potential advantages versus each other and baseline (frontier)

Also figure 7 from v1



with the curves for stacker 8 x stacker 0 and stacker 2a x freestyle instead of stacker 8 x Freestyle?

Shows Forward scheduling potential advantages versus each other and baseline (frontier)

Valid comparison if the different workloads yield similar results?

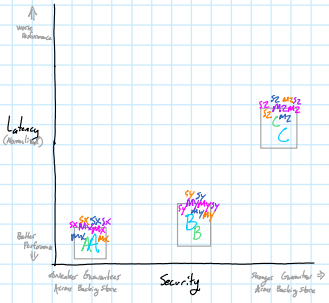
Good graph for the second usecase w/ attempting to shift the storage into a "low power" mode by scheduling cipher swaps from freestyle fast to stacker 8 as the ratio shifts towards 1/4th of the backing store being freestyle

Also figure 7 from v1

Also good for the fourth usecase w/ SSD EoL for the same reason: we can dynamically shift into a higher performance mode when the system determines it is necessary and shift back afterwards.

4.1

Cipher partition performance, 40MB reads, mirrored vs selective schedules vs baseline



Also figure 11 from v1

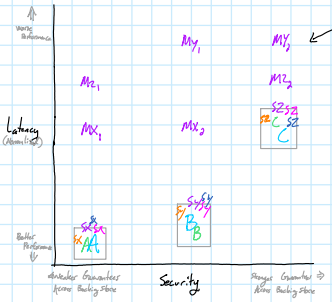
Good graph for the first and third usecases: VSRs and "panic mode". In the case of VSRs, lack of perf degradation despite presence of VSRs (up to a point). For the case of panic mode, see figure 11.

I/O is not "ratio"-ed; operations occur on one partition or the other and the results are measured

Shows selective & mirrored are parity w/ baseline (+ actual)

5.1

Cipher partition performance, 40MB writes, mirrored vs selective schedules vs baseline



Shows that mirrored is slow for writes but as fast as baseline & Selective for reads. Figure 11 shows the benefit of using Mirrored schedule.