www.phoronix-test-suite.com

cryptography-z-1

AMD Ryzen 5 3400G testing with a LENOVO 3706 (O4DKT35A BIOS) and AMD Picasso 2GB on Ubuntu 20.04 via the Phoronix Test Suite.

Test Systems:

AMD Ryzen 5 3400G

Processor: AMD Ryzen 5 3400G @ 3.70GHz (4 Cores / 8 Threads), Motherboard: LENOVO 3706 (O4DKT35A BIOS), Chipset: AMD Raven/Raven2, Memory: 14GB, Disk: 500GB Western Digital WD5000LPVX-8, Graphics: AMD Picasso 2GB (1400/1333MHz), Audio: AMD Raven/Raven2/Fenghuang, Monitor: DP2VGA V226, Network: Realtek RTL8111/8168/8411 + Realtek RTL8821CE 802.11ac PCIe

OS: Ubuntu 20.04, Kernel: 5.4.0-80-generic (x86_64), Desktop: GNOME Shell 3.36.9, Display Server: X Server 1.20.9, Compiler: GCC 9.3.0, File-System: ext4, Screen Resolution: 1024x768

Kernel Notes: Transparent Huge Pages: madvise
Compiler Notes: --build=x86_64-linux-gnu --disable-vtable-verify --disable-werror --enable-checking=release --enable-clocale=gnu --enable-default-pie --enable-gnu-unique-object --enable-languages=c,ada,c++,go,brig,d,fortran,objc,obj-c++,gm2 --enable-libstdcxx-debug --enable-libstdcxx-time=yes --enable-multiarch

cryptography-z-1

--enable-multilib --enable-nls --enable-objc-gc=auto --enable-offload-targets=nvptx-none=/build/gcc-9-HskZEa/gcc-9-9.3.0/debian/tmp-nvptx/usr,hsa --enable-plugin --enable-shared --enable-threads=posix --host=x86_64-linux-gnu --program-prefix=x86_64-linux-gnu- --target=x86_64-linux-gnu --with-abi=m64 --with-arch-32=i686 --with-default-libstdcxx-abi=new --with-gcc-major-version-only --with-multilib-list=m32,m64,mx32 --with-target-system-zlib=auto --with-tune=generic --without-cuda-driver -v
Processor Notes: Scaling Governor: acpi-cpufreq ondemand (Boost: Enabled) - CPU Microcode: 0x8108102
Java Notes: OpenJDK Runtime Environment (build 1.8.0_302-b08)
Python Notes: Python 3.8.10
Security Notes: itlb_multihit: Not affected + l1tf: Not affected + mds: Not affected + meltdown: Not affected + spec_store_bypass: Mitigation of SSB disabled via prctl and seccomp + spectre_v1: Mitigation of usercopy/swapgs barriers and __user pointer sanitization + spectre_v2: Mitigation of Full AMD retpoline IBPB: conditional STIBP: disabled RSB filling + srbds: Not affected + tsx_async_abort: Not affected

	AMD Ryzen 5 3400G
Crypto++ - All Algorithms (MiB/s)	1562
Standard Deviation	0.7%
Crypto++ - Keyed Algorithms (MiB/s)	626.876962
Standard Deviation	0.1%
Crypto++ - Unkeyed Algorithms (MiB/s)	343.637844
Standard Deviation	0.1%
Crypto++ - I.E.C.P.K.A (MiB/s)	4715
Standard Deviation	0.2%
BLAKE2 (Cycles/Byte)	8.8
Standard Deviation	0%
Xmrig - Monero - 1M (H/s)	1124
Standard Deviation	0.4%
Xmrig - Wownero - 1M (H/s)	1478
Standard Deviation	0.4%
Chia Blockchain VDF - Square Plain C++ (IPS)	149733
Standard Deviation	0.6%
Chia Blockchain VDF - S.A.O (IPS)	142933
Standard Deviation	0.5%
Bork File Encrypter - F.E.T (sec)	10.600
Standard Deviation	33.7%
Nettle - aes256 (Mbyte/s)	5790
Standard Deviation	0%
Nettle - chacha (Mbyte/s)	911.80
Standard Deviation	0%
Nettle - sha512 (Mbyte/s)	581.99
Standard Deviation	0%
Nettle - poly1305-aes (Mbyte/s)	2409
Standard Deviation	0.1%
Botan - KASUMI (MiB/s)	95.635
Standard Deviation	0.2%
Botan - KASUMI - Decrypt (MiB/s)	91.549
Standard Deviation	0%
Botan - AES-256 (MiB/s)	5604
Standard Deviation	0.2%
Botan - AES-256 - Decrypt (MiB/s)	5620
Standard Deviation	0.2%
Botan - Twofish (MiB/s)	367.699
Standard Deviation	0.3%
Botan - Twofish - Decrypt (MiB/s)	366.474
Standard Deviation	0.2%
Botan - Blowfish (MiB/s)	449.509

Standard Deviation 0.2%

Botan - Blowfish - Decrypt (MiB/s) 448.978

Standard Deviation 0%

Botan - CAST-256 (MiB/s) 145.258

Standard Deviation 2.1%

Botan - CAST-256 - Decrypt (MiB/s) 145.200

Standard Deviation 2.1%

Botan - ChaCha20Poly1305 (MiB/s) 503.991

Standard Deviation 0.2%

Botan - ChaCha20Poly1305 - Decrypt (MiB/s) 501.986

Standard Deviation 0.2%

John The Ripper - Blowfish (Real C/S) 9002

Standard Deviation 1.6%

John The Ripper - MD5 (Real C/S) 259208

Standard Deviation 0.2%

Gcrypt Library (sec) 224.678

Standard Deviation 0.9%

OpenSSL - R.4.b.P (Signs/sec) 856.3

Standard Deviation 0.5%

Aircrack-ng (k/s) 7097

Standard Deviation 0.8%

Cpuminer-Opt - Magi (kH/s) 164.18

Standard Deviation 3.1%

Cpuminer-Opt - x25x (kH/s) 120.84

Standard Deviation 2.3%

Cpuminer-Opt - Deepcoin (kH/s) 2355

Standard Deviation 16.8%

Cpuminer-Opt - Ringcoin (kH/s) 912.34

Standard Deviation 0.6%

Cpuminer-Opt - Blake-2 S (kH/s) 86925

Standard Deviation 6.5%

Cpuminer-Opt - Garlicoin (kH/s) 626.68

Standard Deviation 0.1%

Cpuminer-Opt - Skeincoin (kH/s) 18413

Standard Deviation 11.2%

Cpuminer-Opt - Myriad-Groestl (kH/s) 7061

Standard Deviation 3.7%

Cpuminer-Opt - LBC, LBRY Credits (kH/s) 6377

Standard Deviation 11.5%

Cpuminer-Opt - Q.S.2.P (kH/s) 33597

Standard Deviation 1.2%

Cpuminer-Opt - T.S.2.O (kH/s) 44197

Standard Deviation 1%

SecureMark - SecureMark-TLS (marks) 206318

Standard Deviation 0.8%

Cryptsetup - PBKDF2-sha512 (Iterations/sec) 1566603

Standard Deviation 0.2%

Cryptsetup - PBKDF2-whirlpool (Iterations/sec) 673606

Standard Deviation 0.3%

Cryptsetup - A.X.2.E (MiB/s) 2796

Standard Deviation 3.2%

Cryptsetup - A.X.2.D (MiB/s) 2805

Standard Deviation 3%

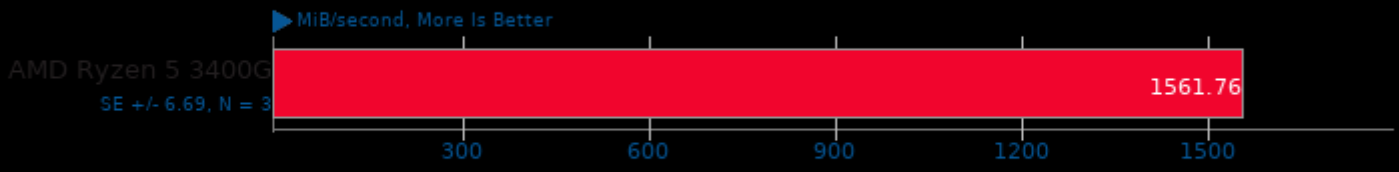
cryptography-z-1

Cryptsetup - S.X.2.E (MiB/s)	392.4
Standard Deviation	0.8%
Cryptsetup - S.X.2.D (MiB/s)	389.1
Standard Deviation	0.9%
Cryptsetup - T.X.2.E (MiB/s)	398.2
Standard Deviation	3%
Cryptsetup - T.X.2.D (MiB/s)	391.3
Standard Deviation	3.5%
Cryptsetup - A.X.5.E (MiB/s)	2411
Standard Deviation	2%
Cryptsetup - A.X.5.D (MiB/s)	2397
Standard Deviation	2.4%
Cryptsetup - S.X.5.E (MiB/s)	393.5
Standard Deviation	0.4%
Cryptsetup - S.X.5.D (MiB/s)	389.3
Standard Deviation	0.8%
Cryptsetup - T.X.5.E (MiB/s)	401.0
Standard Deviation	2%
Cryptsetup - T.X.5.D (MiB/s)	394.4
Standard Deviation	2.1%
GnuPG - 2.7.S.F.E (sec)	74.212
Standard Deviation	10%

cryptography-z-1

Crypto++ 8.2

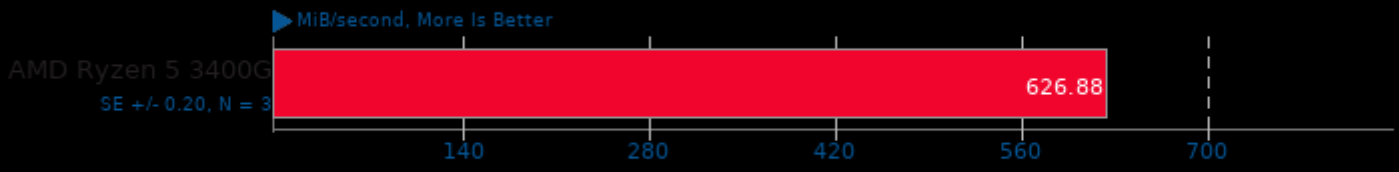
Test: All Algorithms



1. (CXX) g++ options: -g2 -O3 -fPIC -pthread -pipe

Crypto++ 8.2

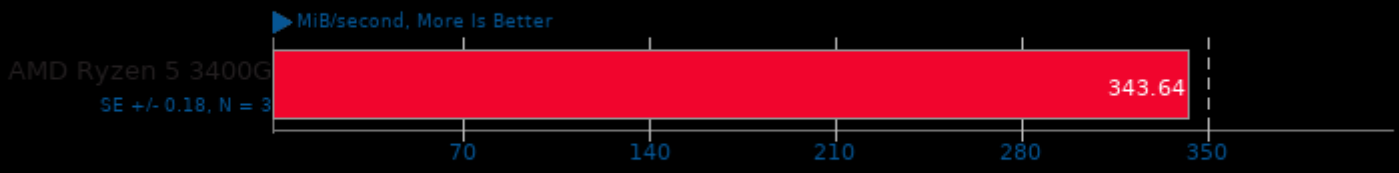
Test: Keyed Algorithms



1. (CXX) g++ options: -g2 -O3 -fPIC -pthread -pipe

Crypto++ 8.2

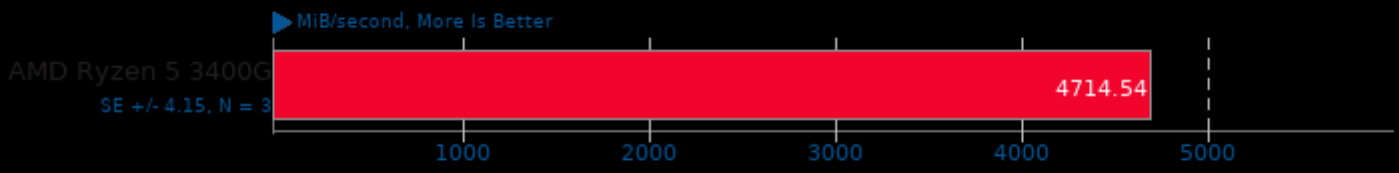
Test: Unkeyed Algorithms



1. (CXX) g++ options: -g2 -O3 -fPIC -pthread -pipe

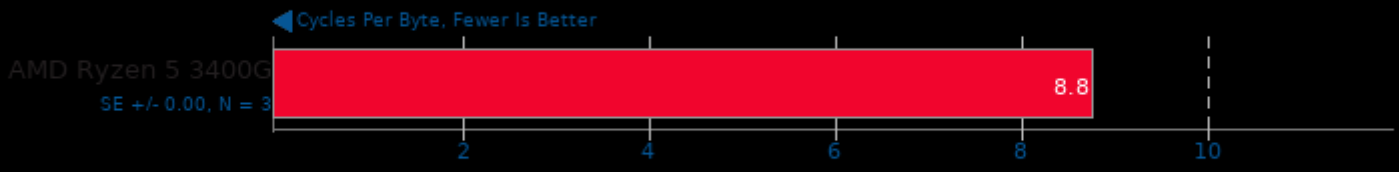
Crypto++ 8.2

Test: Integer + Elliptic Curve Public Key Algorithms



1. (CXX) g++ options: -g2 -O3 -fPIC -pthread -pipe

BLAKE2 20170307

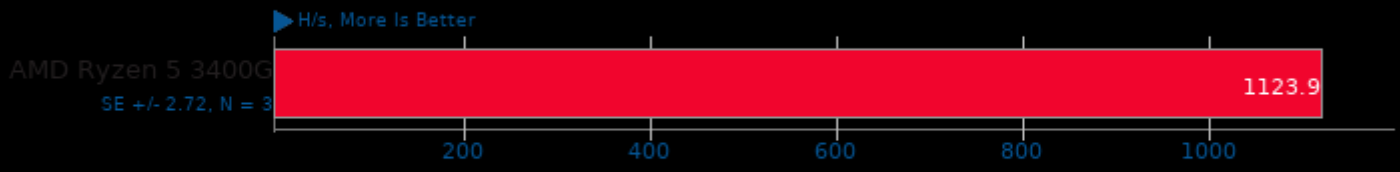


1. (CC) gcc options: -O3 -march=native -lcrypto -lz

cryptography-z-1

Xmrig 6.12.1

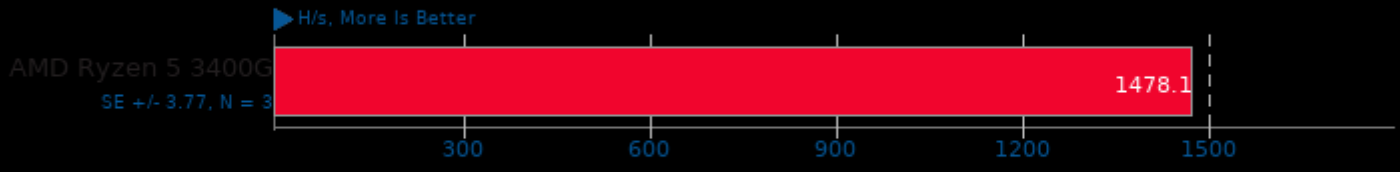
Variant: Monero - Hash Count: 1M



1. (CXX) g++ options: -fexceptions -fno-rtti -maes -O3 -Ofast -static-libgcc -static-libstdc++ -rdynamic -lssl -lcrypto -luv -lpthread -lrt -ldl -lhwloc

Xmrig 6.12.1

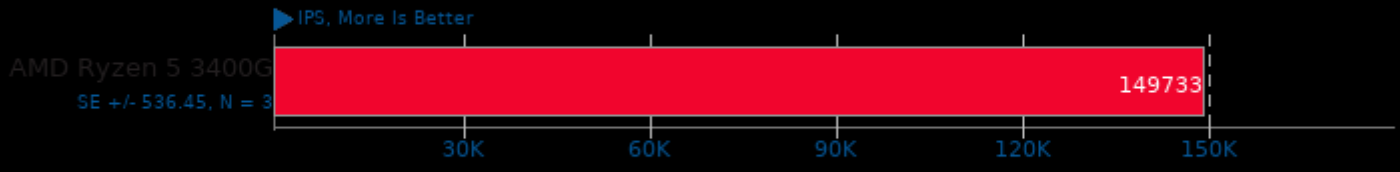
Variant: Wownero - Hash Count: 1M



1. (CXX) g++ options: -fexceptions -fno-rtti -maes -O3 -Ofast -static-libgcc -static-libstdc++ -rdynamic -lssl -lcrypto -luv -lpthread -lrt -ldl -lhwloc

Chia Blockchain VDF 1.0.1

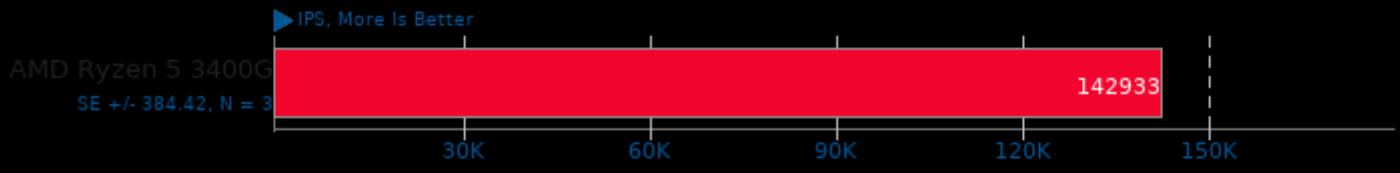
Test: Square Plain C++



1. (CXX) g++ options: -flto -no-pie -lgmpxx -lgmp -lboost_system -pthread

Chia Blockchain VDF 1.0.1

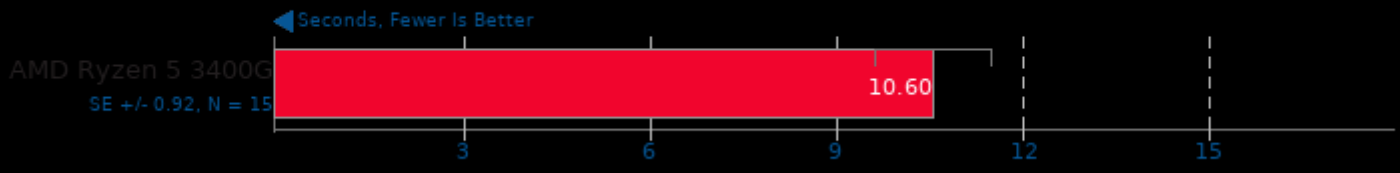
Test: Square Assembly Optimized



1. (CXX) g++ options: -flto -no-pie -lgmpxx -lgmp -lboost_system -pthread

Bork File Encrypter 1.4

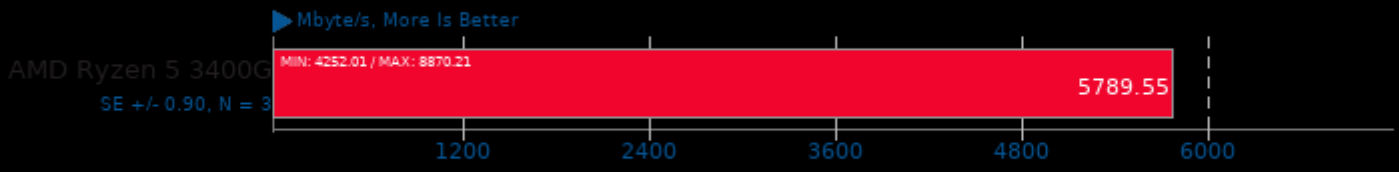
File Encryption Time



cryptography-z-1

Nettle 3.5.1

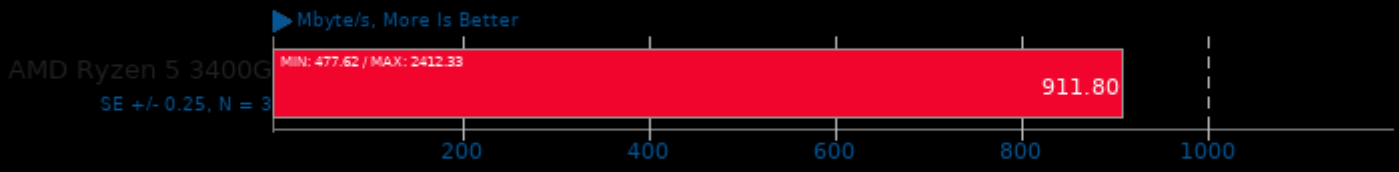
Test: aes256



1. (CC) gcc options: -O2 -ggdb3 -lhogweed -lnettle -lgmp -lm -lcrypto

Nettle 3.5.1

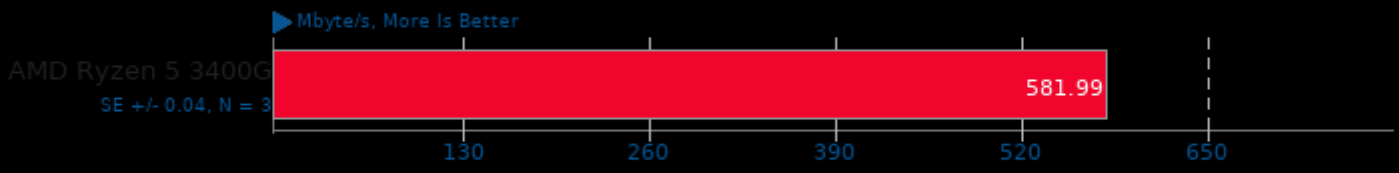
Test: chacha



1. (CC) gcc options: -O2 -ggdb3 -lhogweed -lnettle -lgmp -lm -lcrypto

Nettle 3.5.1

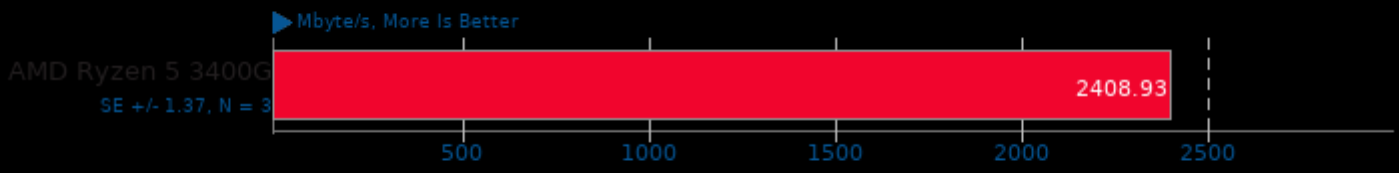
Test: sha512



1. (CC) gcc options: -O2 -ggdb3 -lhogweed -lnettle -lgmp -lm -lcrypto

Nettle 3.5.1

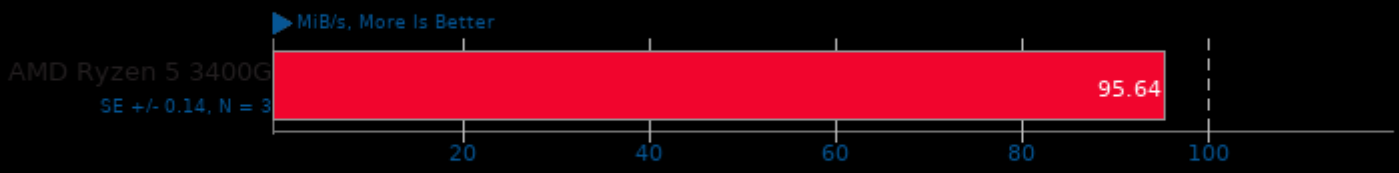
Test: poly1305-aes



1. (CC) gcc options: -O2 -ggdb3 -lhogweed -lnettle -lgmp -lm -lcrypto

Botan 2.17.3

Test: KASUMI



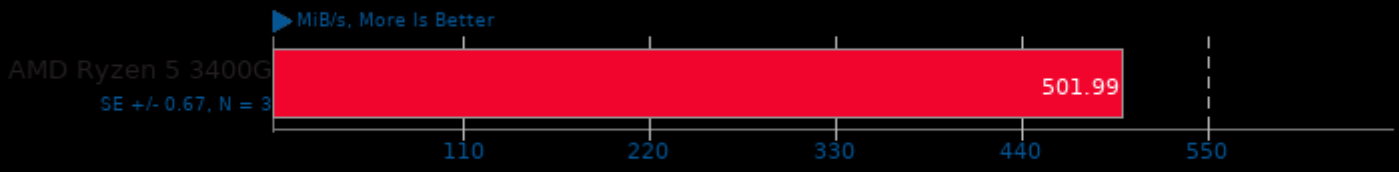
1. (CXX) g++ options: -fstack-protector -m64 -pthread -lbotan-2 -ldl -lrt

cryptography-z-1


Botan 2.17.3
Test: Blowfish
MiB/s, More Is Better
AMD Ryzen 5 3400G
SE +/- 0.39, N = 3
449.51
100
200
300
400
500
1. (CXX) g++ options: -fstack-protector -m64 -pthread -lbotan-2 -ldl -lrt
Botan 2.17.3
Test: Blowfish - Decrypt
MiB/s, More Is Better
AMD Ryzen 5 3400G
SE +/- 0.07, N = 3
448.98
100
200
300
400
500
1. (CXX) g++ options: -fstack-protector -m64 -pthread -lbotan-2 -ldl -lrt
Botan 2.17.3
Test: CAST-256
MiB/s, More Is Better
AMD Ryzen 5 3400G
SE +/- 1.74, N = 3
145.26
30
60
90
120
150
1. (CXX) g++ options: -fstack-protector -m64 -pthread -lbotan-2 -ldl -lrt
Botan 2.17.3
Test: CAST-256 - Decrypt
MiB/s, More Is Better
AMD Ryzen 5 3400G
SE +/- 1.78, N = 3
145.20
30
60
90
120
150
1. (CXX) g++ options: -fstack-protector -m64 -pthread -lbotan-2 -ldl -lrt
Botan 2.17.3
Test: ChaCha20Poly1305
MiB/s, More Is Better
AMD Ryzen 5 3400G
SE +/- 0.54, N = 3
503.99
110
220
330
440
550
1. (CXX) g++ options: -fstack-protector -m64 -pthread -lbotan-2 -ldl -lrt

Botan 2.17.3

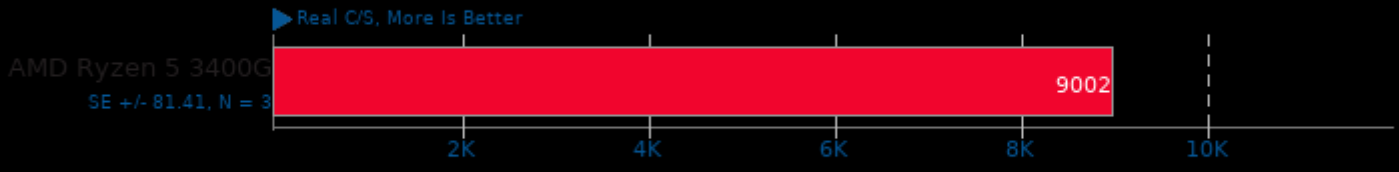
Test: ChaCha20Poly1305 - Decrypt



1. (CXX) g++ options: -fstack-protector -m64 -pthread -lbotan-2 -ldl -lrt

John The Ripper 1.9.0-jumbo-1

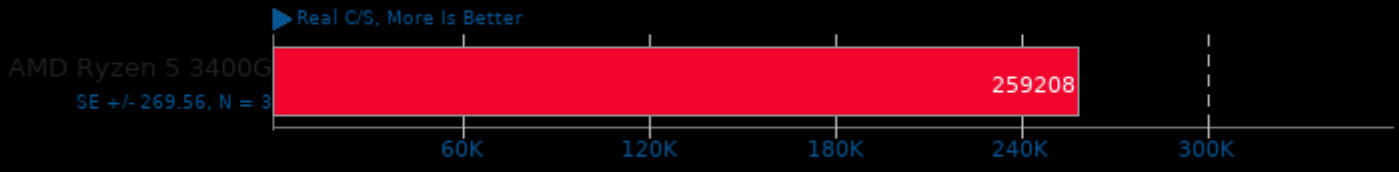
Test: Blowfish



1. (CC) gcc options: -m64 -lssl -lcrypto -fopenmp -lgmp -pthread -lm -lz -ldl -lcrypt

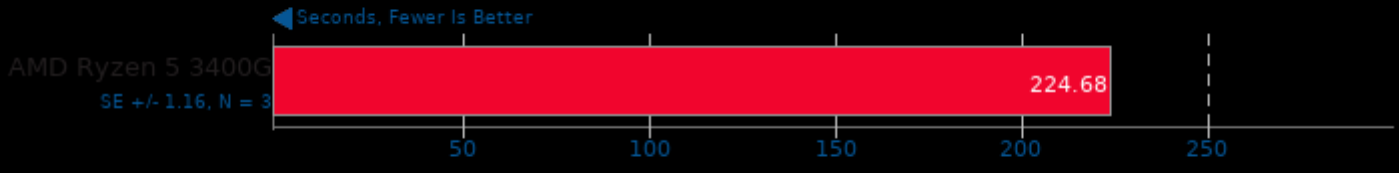
John The Ripper 1.9.0-jumbo-1

Test: MD5



1. (CC) gcc options: -m64 -lssl -lcrypto -fopenmp -lgmp -pthread -lm -lz -ldl -lcrypt

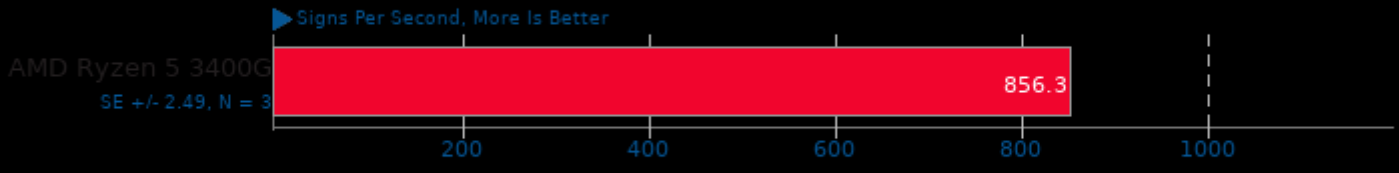
Gcrypt Library 1.9



1. (CC) gcc options: -O2 -fvisibility=hidden

OpenSSL 1.1.1

RSA 4096-bit Performance



1. (CC) gcc options: -pthread -m64 -O3 -lssl -lcrypto -ldl

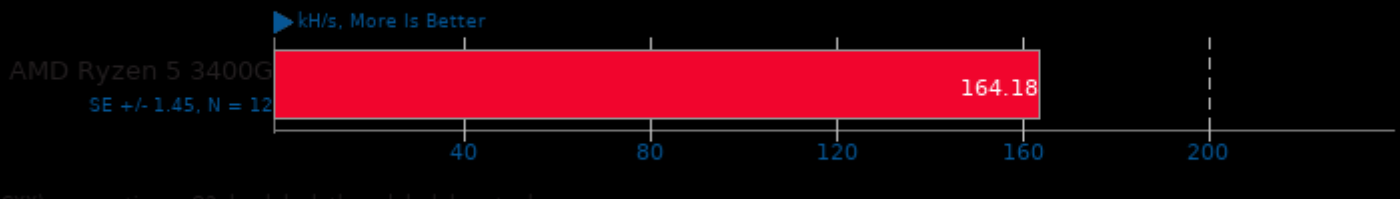
cryptography-z-1

Aircrack-ng 1.5.2

1. (CXX) g++ options: -O3 -fvisibility=hidden -masm=intel -fcommon -rdynamic -lpthread -lz -lcrypto -lhwloc -ldl -lm -pthread

Cpuminer-Opt 3.15.5

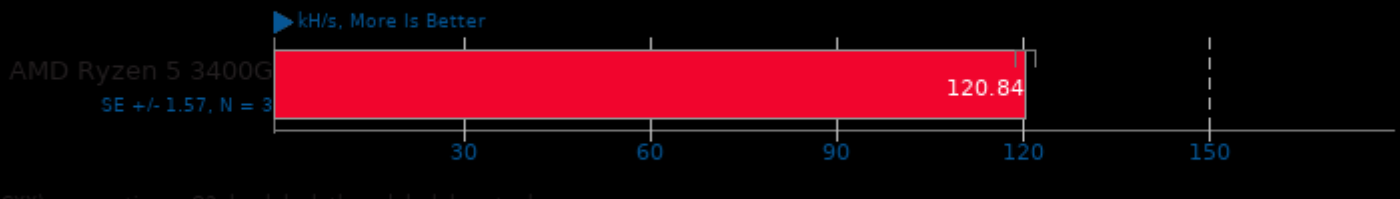
Algorithm: Magi



1. (CXX) g++ options: -O2 -lcurl -lz -lpthread -lssl -lcrypto -lgmp

Cpuminer-Opt 3.15.5

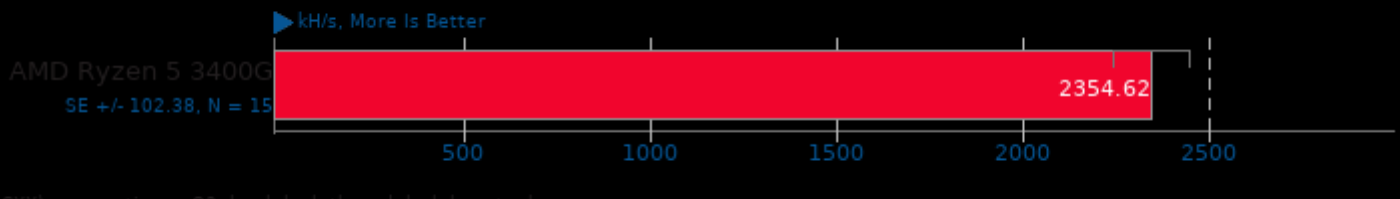
Algorithm: x25x



1. (CXX) g++ options: -O2 -lcurl -lz -lpthread -lssl -lcrypto -lgmp

Cpuminer-Opt 3.15.5

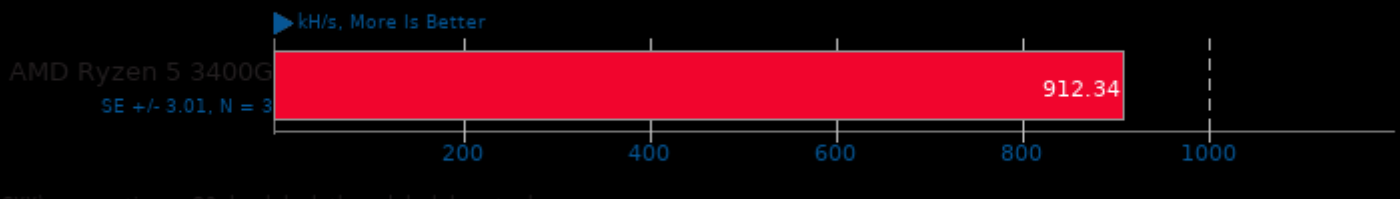
Algorithm: Deepcoin



1. (CXX) g++ options: -O2 -lcurl -lz -lpthread -lssl -lcrypto -lgmp

Cpuminer-Opt 3.15.5

Algorithm: Ringcoin



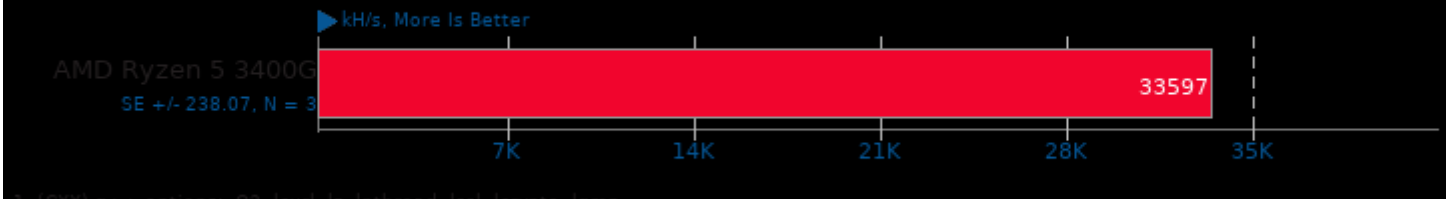
1. (CXX) g++ options: -O2 -lcurl -lz -lpthread -lssl -lcrypto -lgmp

cryptography-z-1

cryptography-z-1

Cpuminer-Opt 3.15.5

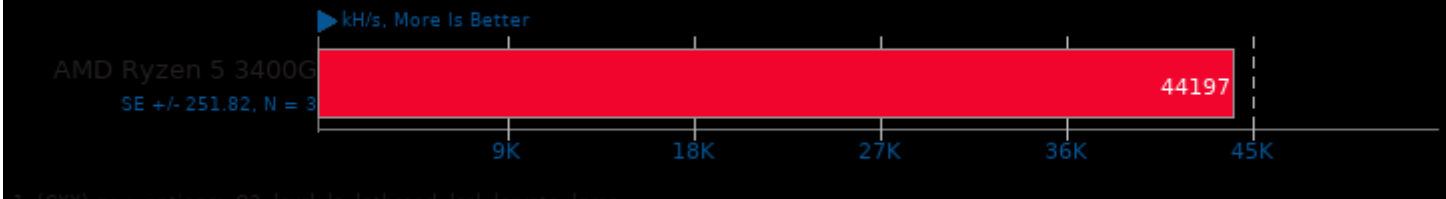
Algorithm: Quad SHA-256, Pyrite



1. (CXX) g++ options: -O2 -lcurl -lz -lpthread -lssl -lcrypto -lgmp

Cpuminer-Opt 3.15.5

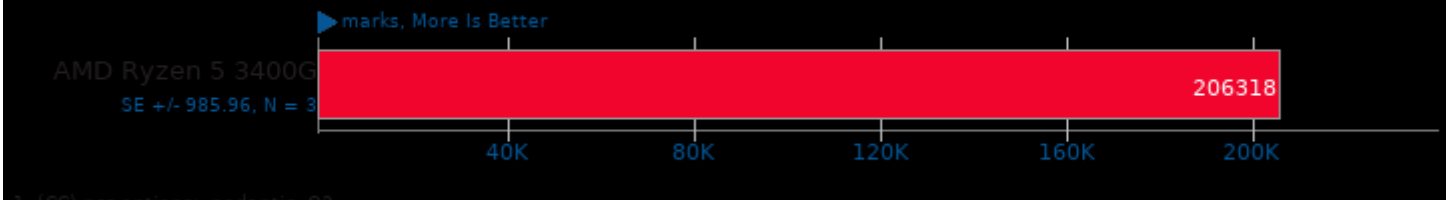
Algorithm: Triple SHA-256, Onecoin



1. (CXX) g++ options: -O2 -lcurl -lz -lpthread -lssl -lcrypto -lgmp

SecureMark 1.0.4

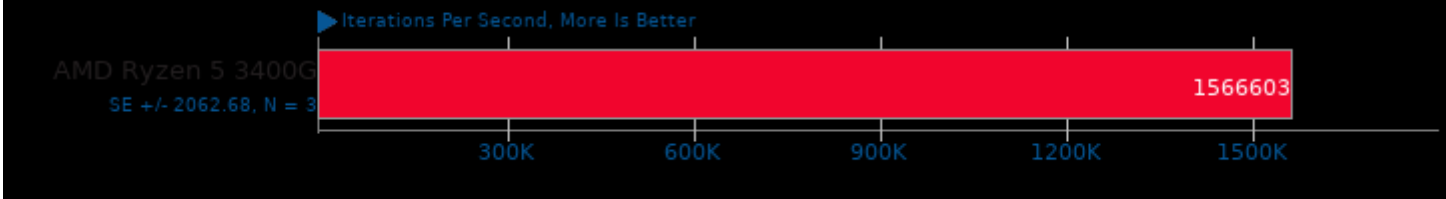
Benchmark: SecureMark-TLS



1. (CC) gcc options: -pedantic -O3

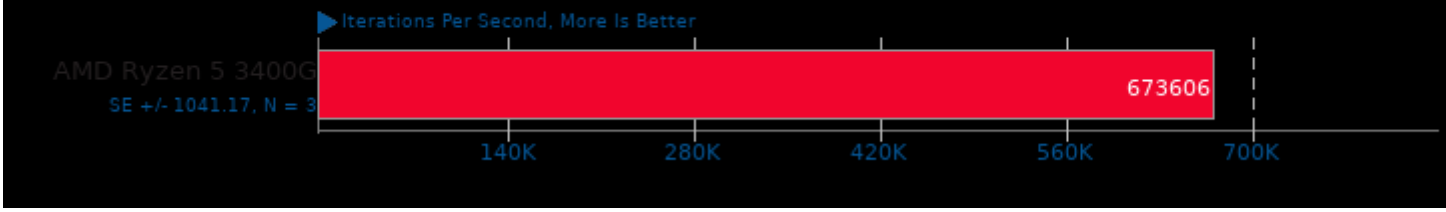
Cryptsetup

PBKDF2-sha512

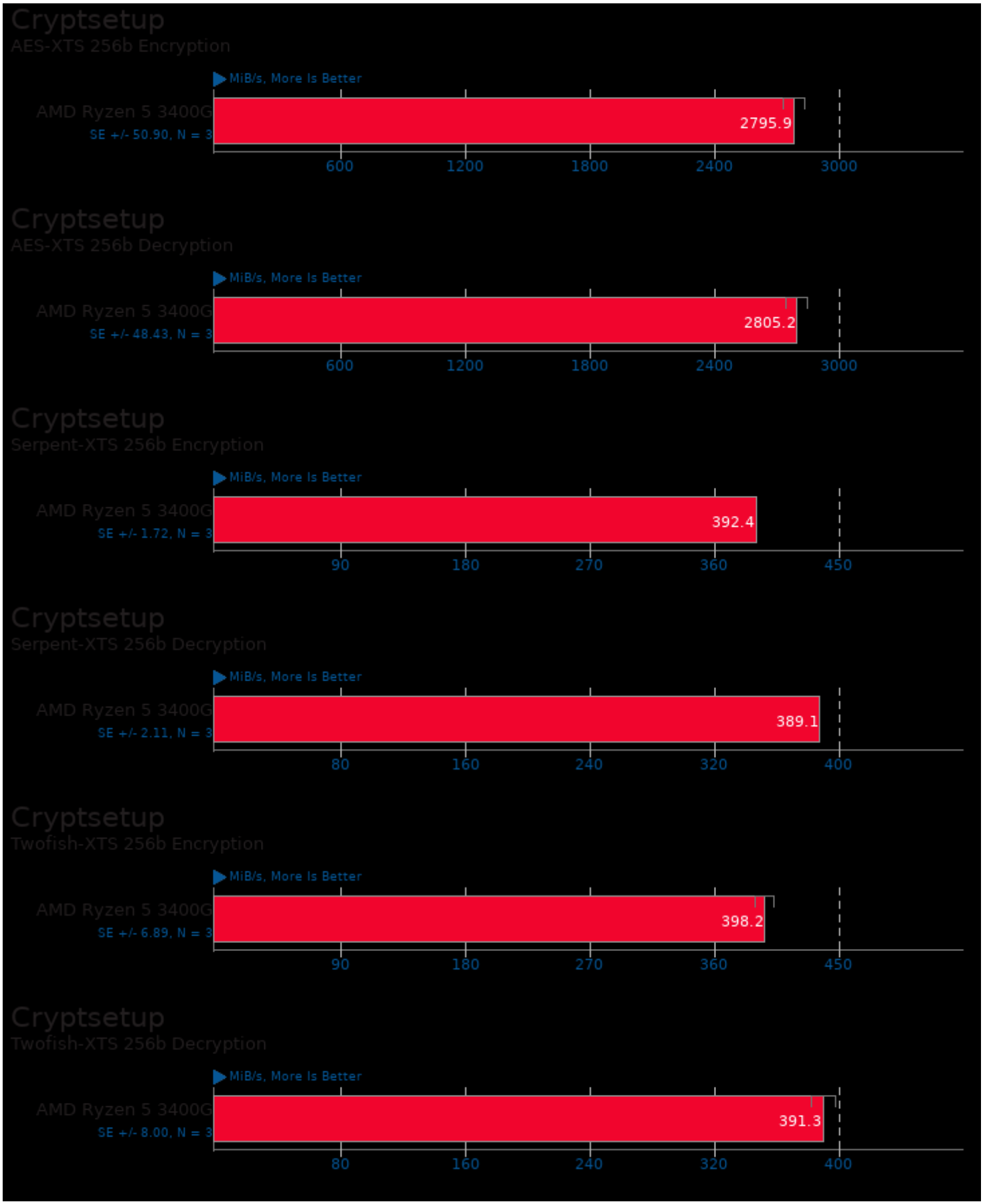


Cryptsetup

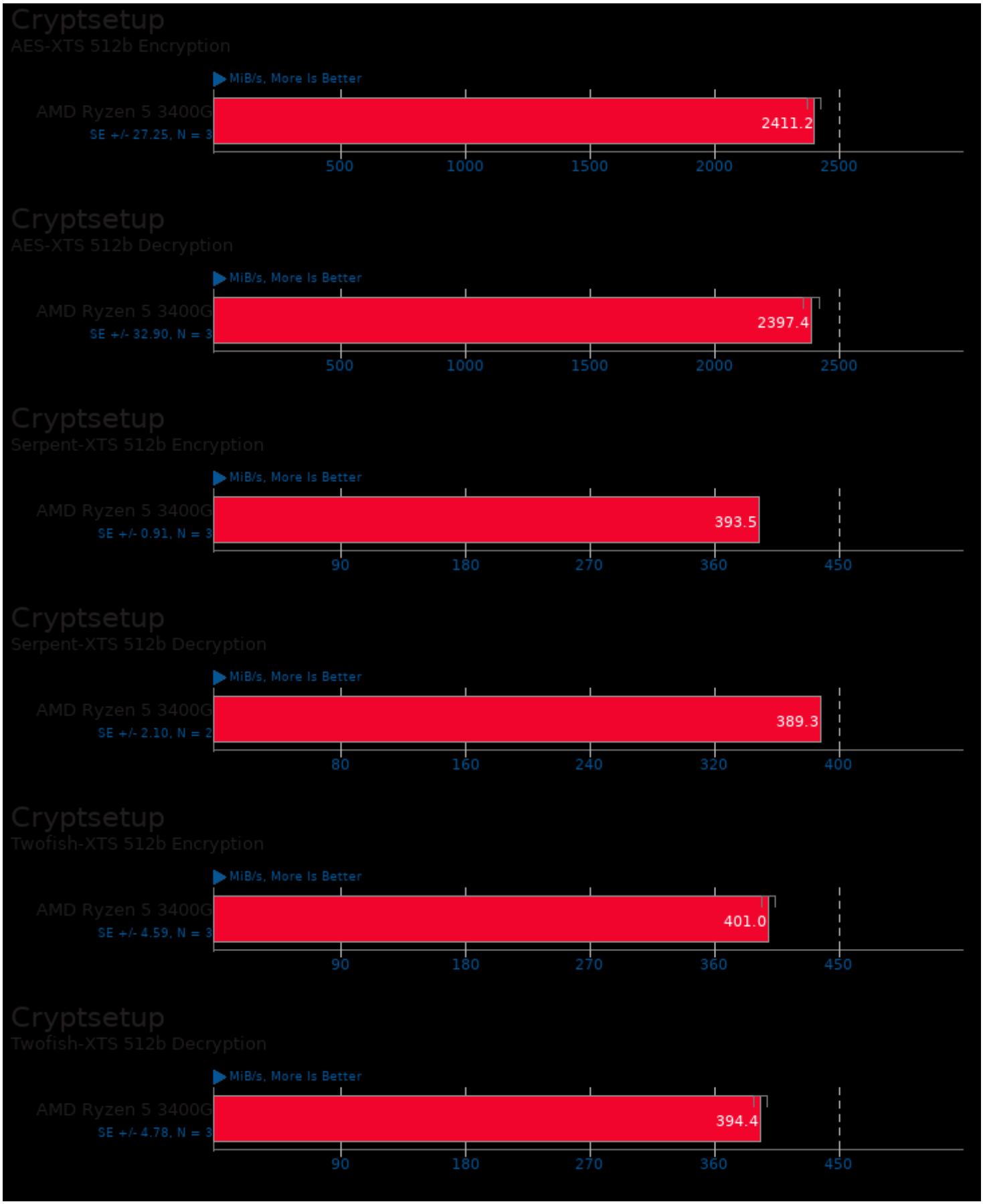
PBKDF2-whirlpool

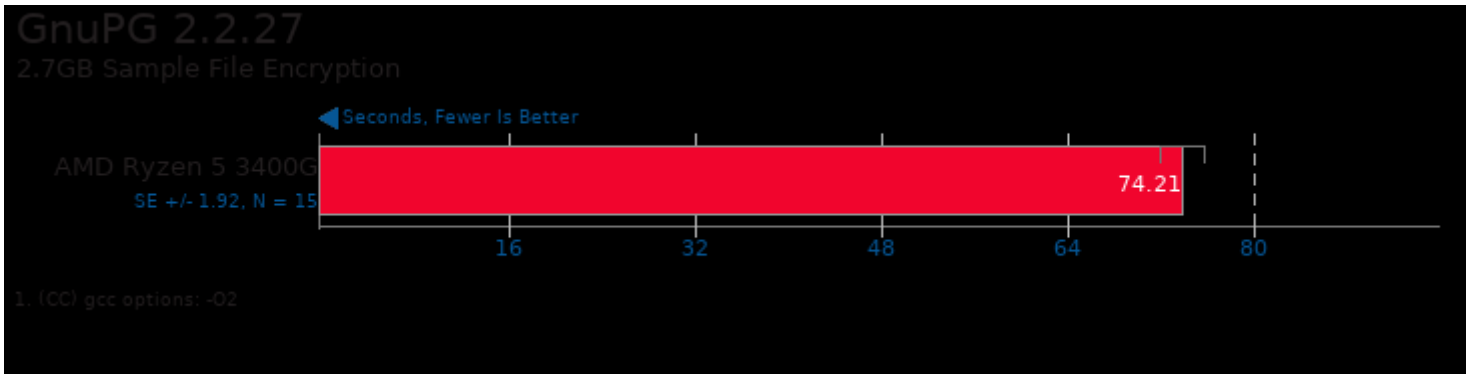


cryptography-z-1



cryptography-z-1





This file was automatically generated via the Phoronix Test Suite benchmarking software on Thursday, 28 March 2024 04:46.