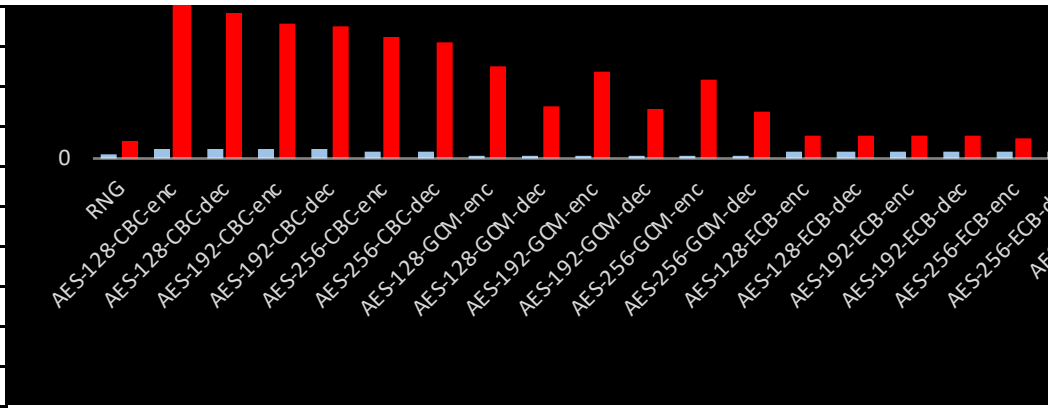
Algorithm	woPAA	wPAA
RNG	18.988	80.002
AES-128-CBC-enc	42.782	677.604
AES-128-CBC-dec	43.371	628.27
AES-192-CBC-enc	36.671	589.566
AES-192-CBC-dec	37.129	571.165
AES-256-CBC-enc	32.094	521.956
AES-256-CBC-dec	32.419	506.769
AES-128-GCM-enc	10.581	405.265
AES-128-GCM-dec	10.577	225.299
AES-192-GCM-enc	9.764	371.994
AES-192-GCM-dec	9.752	214.773
AES-256-GCM-enc	9.197	343.703
AES-256-GCM-dec	9.192	204.954
AES-128-ECB-enc	34.18	100.37
AES-128-ECB-dec	34.931	101.443
AES-192-ECB-enc	30.173	95.151
AES-192-ECB-dec	30.741	96.11
AES-256-ECB-enc	27.01	90.892
AES-256-ECB-dec	27.473	91.766
AES-128-CTR	42.109	817.165
AES-192-CTR	36.19	747.383
AES-256-CTR	31.725	691.804
AES-CCM-Enc	21.533	123.027
AES-CCM-Dec	21.482	121.355
3DES	8.003	7.675
MD5	148.831	144.729
SHA	108.038	108.015
SHA-224	43.771	567.15
SHA-256	43.773	564.354
SHA-384	65.186	124.718
SHA-512	65.187	124.745
SHA3-224	67.74	67.821
SHA3-256	64.147	64.215
SHA3-384	49.564	49.586
SHA3-512	34.721	34.712
AES-128-CMAC	40.288	175.138
AES-256-CMAC	30.671	148.137
HMAC-MD5	148.865	144.562
HMAC-SHA	108.038	108.025
HMAC-SHA224	43.76	567.221
HMAC-SHA256	43.691	567.245
HMAC-SHA384	65.538	124.724
HMAC-SHA512	65.528	124.699
PBKDF2	4.902	21.003

RSA KeyGen (1024)	1.903	1.865
RSA KeyGen (2048)	0.423	0.9
RSA public key	226.043	4074.352
RSA private key	13.271	120.561
DH KeyGen	62.463	250.623
DH KeyAgree	29.574	250.298
ECC KeyGen	112.114	7143.951
ECDHE Agree	112.424	1964.669
ECDSA Sign	110.338	4451.298
ECDSA Verify	166.677	1746.164

Metric
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
MB/s
KB/s

ops/sec
ops/sec
ops/sec
ops/sec
ops/sec
ops/sec
ops/sec
ops/sec
ops/sec
ops/sec



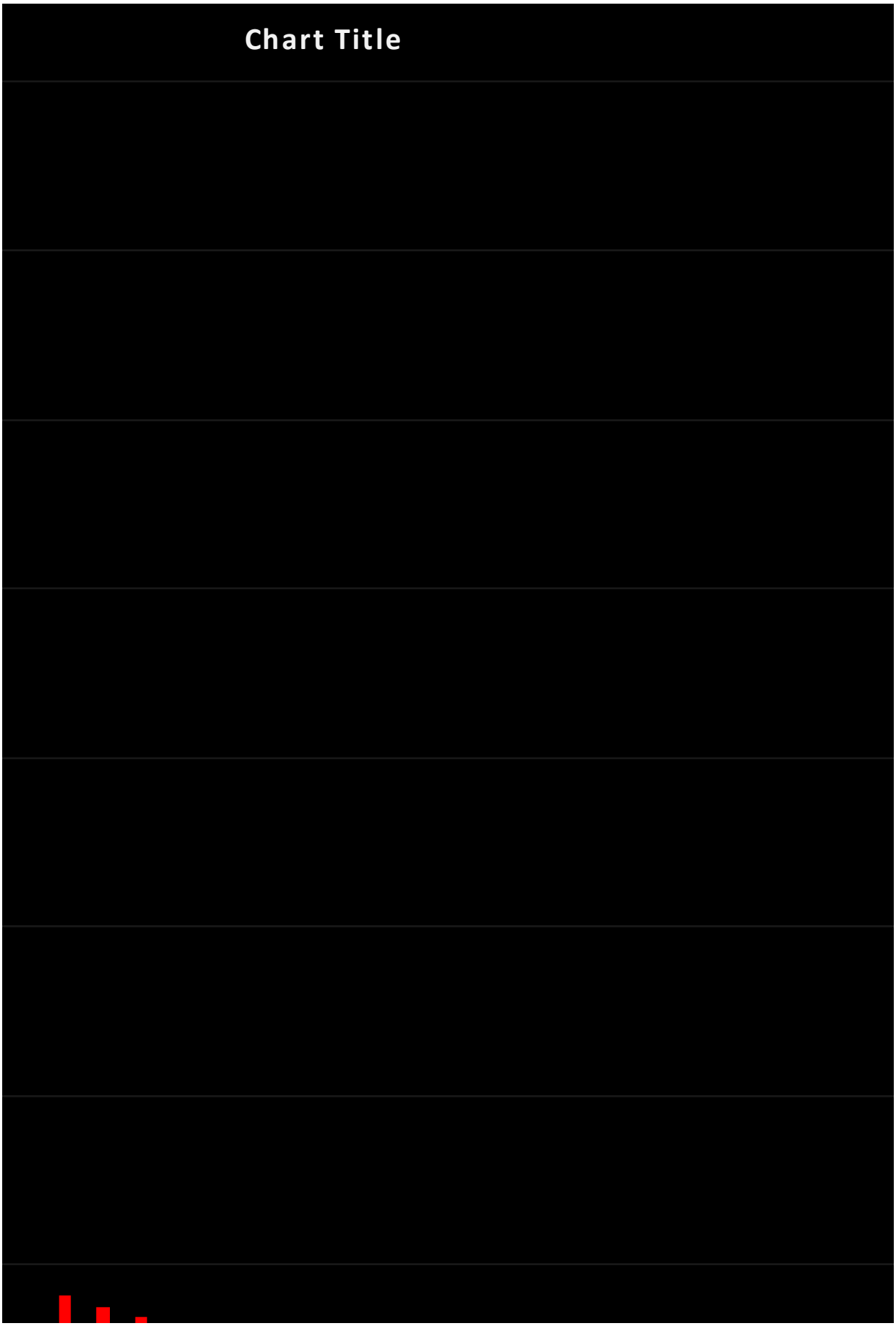
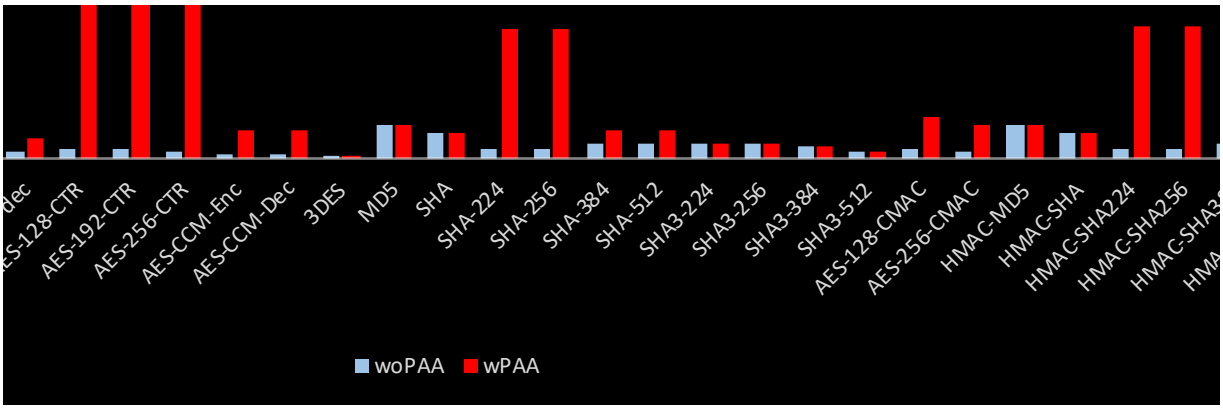
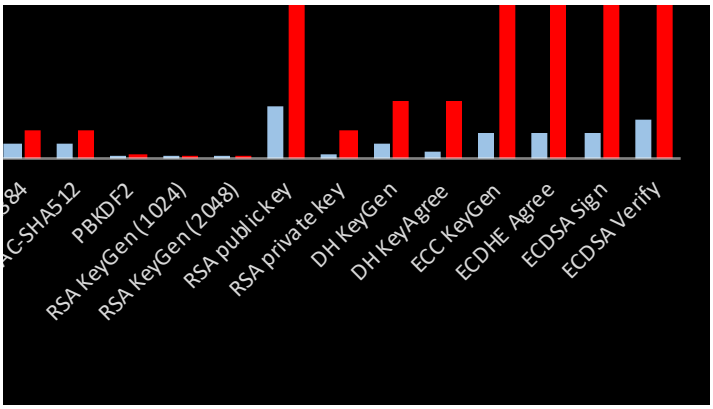


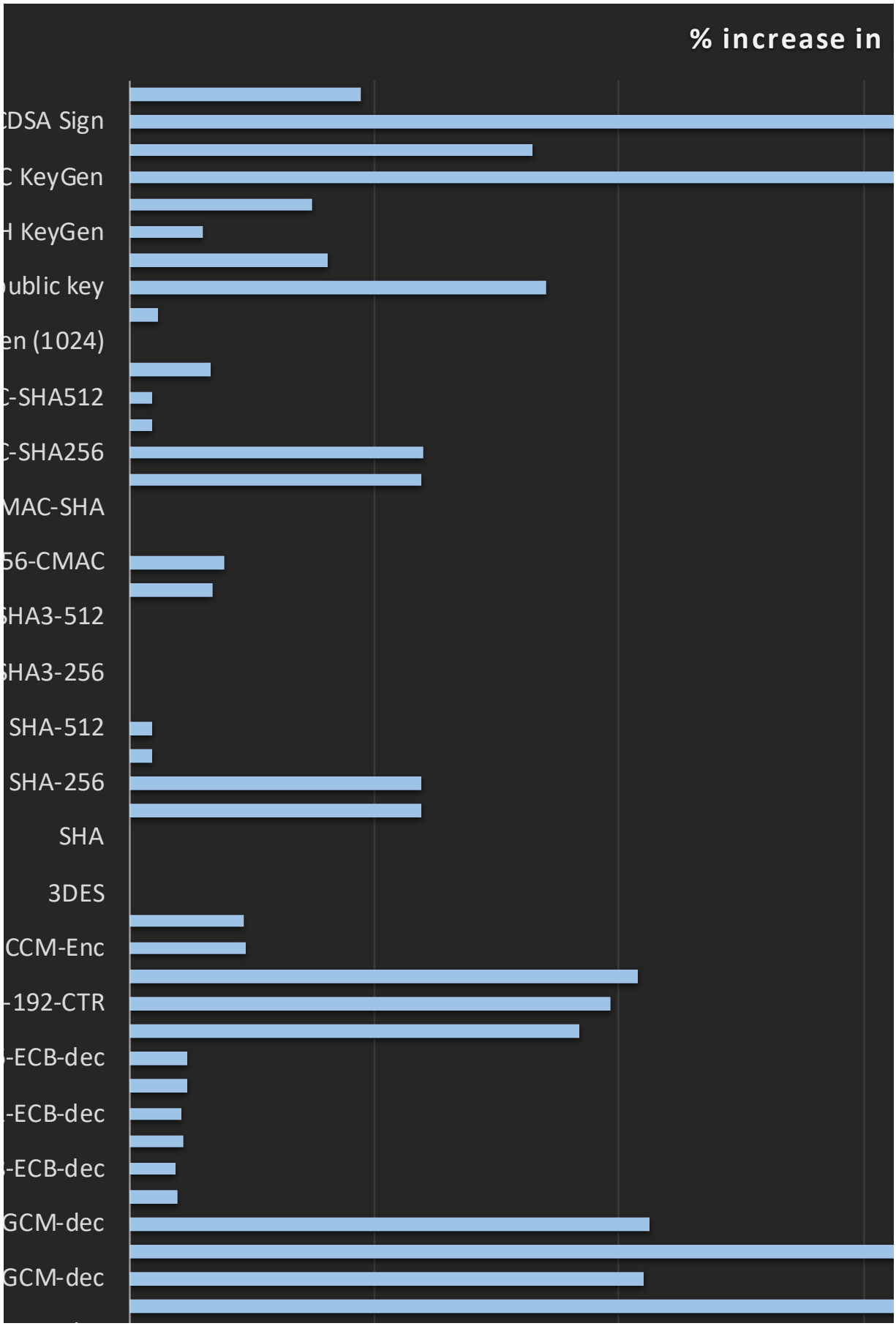
Chart Title

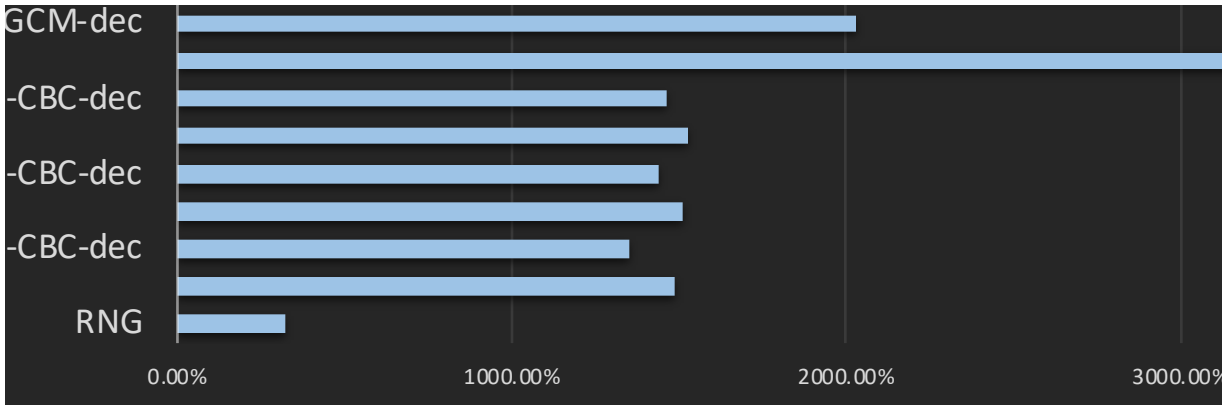

AES-128-CTR
AES-192-CTR
AES-256-CTR
AES-CCM-Enc
AES-CCM-Dec
3DES
MD5
SHA
SHA-224
SHA-256
SHA-384
SHA-512
SHA3-224
SHA3-256
SHA3-384
SHA3-512
AES-128-CMAC
AES-256-CMAC
HMAC-MD5
HMAC-SHA
HMAC-SHA224
HMAC-SHA256
woPAA
wPAA

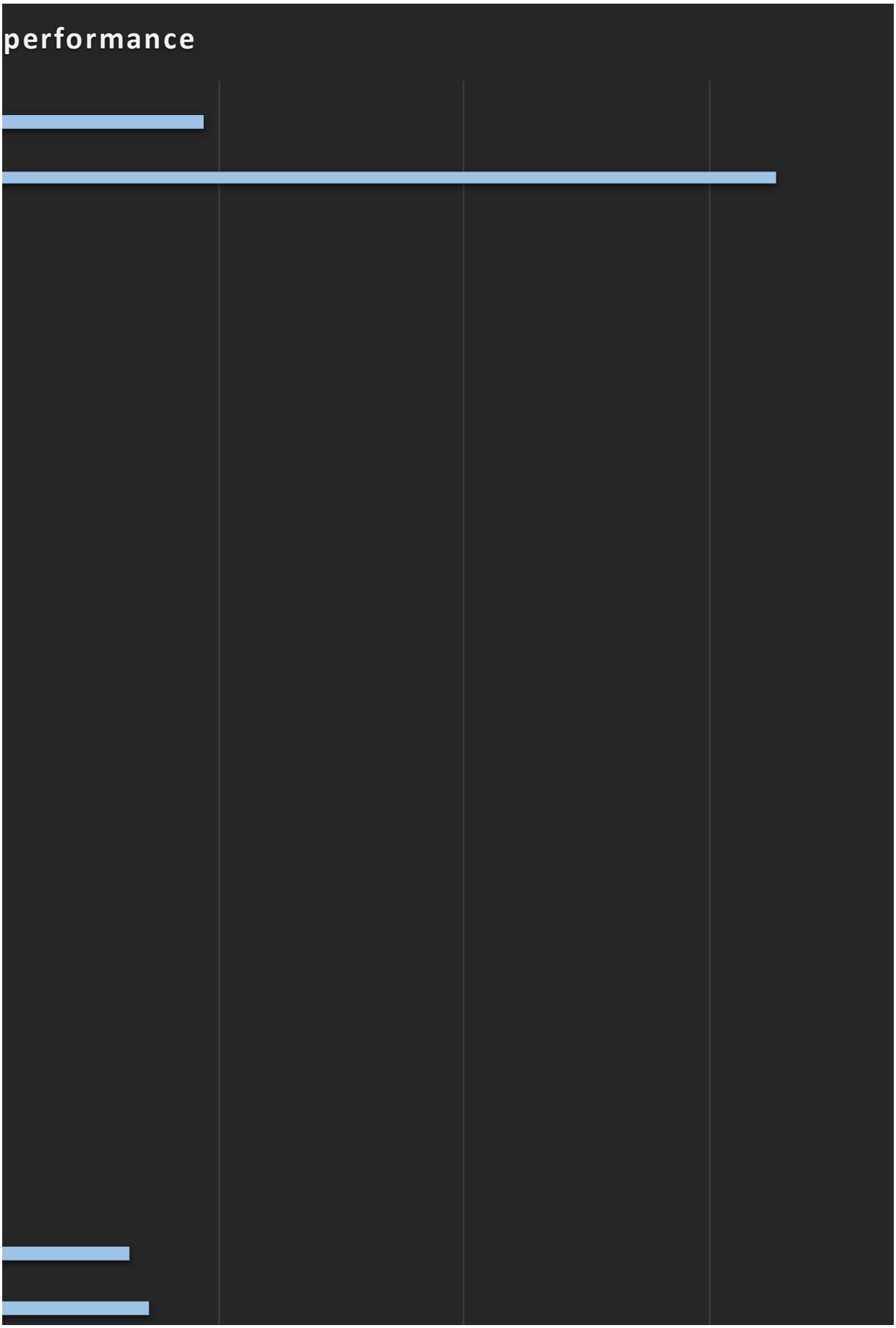

384
AC-SHA512
PBKDF2
RSA KeyGen (1024)
RSA KeyGen (2048)
RSA public key
RSA private key
DH KeyGen
DH KeyAgree
ECC KeyGen
ECDHE Agree
ECDSA Sign
ECDSA Verify

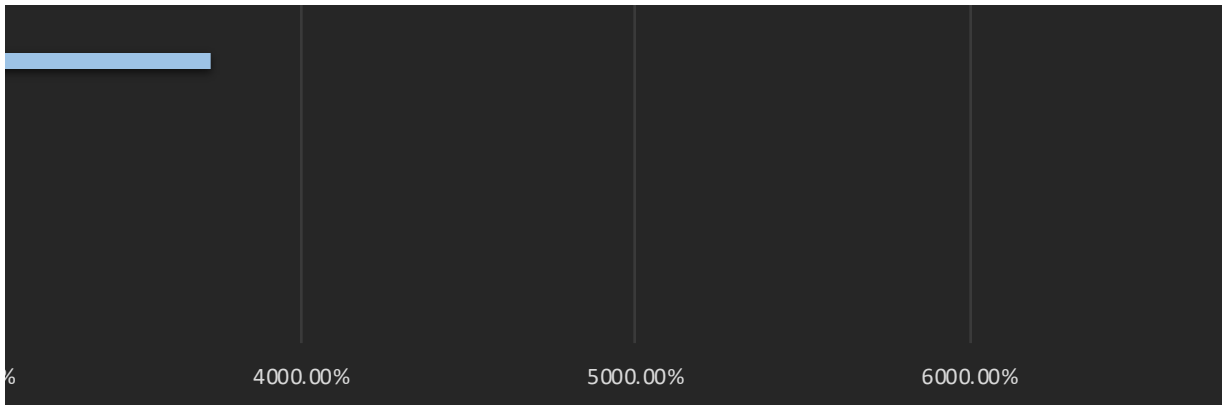
Algorithm	% increase in performance	woPAA	wPAA	Metric
RNG	321.33%	18.988	80.002	MB/s
AES-128-CBC-enc	1483.85%	42.782	677.604	MB/s
AES-128-CBC-dec	1348.59%	43.371	628.27	MB/s
AES-192-CBC-enc	1507.72%	36.671	589.566	MB/s
AES-192-CBC-dec	1438.33%	37.129	571.165	MB/s
AES-256-CBC-enc	1526.34%	32.094	521.956	MB/s
AES-256-CBC-dec	1463.19%	32.419	506.769	MB/s
AES-128-GCM-enc	3730.12%	10.581	405.265	MB/s
AES-128-GCM-dec	2030.08%	10.577	225.299	MB/s
AES-192-GCM-enc	3709.85%	9.764	371.994	MB/s
AES-192-GCM-dec	2102.35%	9.752	214.773	MB/s
AES-256-GCM-enc	3637.12%	9.197	343.703	MB/s
AES-256-GCM-dec	2129.70%	9.192	204.954	MB/s
AES-128-ECB-enc	193.65%	34.18	100.37	MB/s
AES-128-ECB-dec	190.41%	34.931	101.443	MB/s
AES-192-ECB-enc	215.35%	30.173	95.151	MB/s
AES-192-ECB-dec	212.64%	30.741	96.11	MB/s
AES-256-ECB-enc	236.51%	27.01	90.892	MB/s
AES-256-ECB-dec	234.02%	27.473	91.766	MB/s
AES-128-CTR	1840.59%	42.109	817.165	MB/s
AES-192-CTR	1965.16%	36.19	747.383	MB/s
AES-256-CTR	2080.63%	31.725	691.804	MB/s
AES-CCM-Enc	471.34%	21.533	123.027	MB/s
AES-CCM-Dec	464.91%	21.482	121.355	MB/s
3DES	NOT ACCELERATED	8.003	7.675	MB/s
MD5	NOT ACCELERATED	148.831	144.729	MB/s
SHA	NOT ACCELERATED	108.038	108.015	MB/s
SHA-224	1195.72%	43.771	567.15	MB/s
SHA-256	1189.27%	43.773	564.354	MB/s
SHA-384	91.33%	65.186	124.718	MB/s
SHA-512	91.36%	65.187	124.745	MB/s
SHA3-224	NOT ACCELERATED	67.74	67.821	MB/s
SHA3-256	NOT ACCELERATED	64.147	64.215	MB/s
SHA3-384	NOT ACCELERATED	49.564	49.586	MB/s
SHA3-512	NOT ACCELERATED	34.721	34.712	MB/s
AES-128-CMAC	334.72%	40.288	175.138	MB/s
AES-256-CMAC	382.99%	30.671	148.137	MB/s
HMAC-MD5	NOT ACCELERATED	148.865	144.562	MB/s
HMAC-SHA	NOT ACCELERATED	108.038	108.025	MB/s
HMAC-SHA224	1196.21%	43.76	567.221	MB/s
HMAC-SHA256	1198.31%	43.691	567.245	MB/s
HMAC-SHA384	90.31%	65.538	124.724	MB/s
HMAC-SHA512	90.30%	65.528	124.699	MB/s
PBKDF2	328.46%	4.902	21.003	KB/s

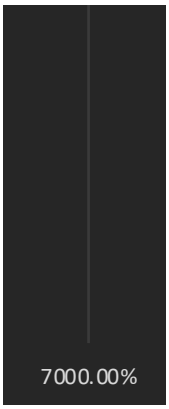
RSA KeyGen (1024)	NOT ACCELERATED	1.903	1.865	ops/sec	AES-128-(
RSA KeyGen (2048)	112.77%	0.423	0.9	ops/sec	
RSA public key	1702.47%	226.043	4074.352	ops/sec	AES-256
RSA private key	808.45%	13.271	120.561	ops/sec	
DH KeyGen	301.23%	62.463	250.623	ops/sec	AES-192
DH KeyAgree	746.34%	29.574	250.298	ops/sec	
ECC KeyGen	6272.04%	112.114	7143.951	ops/sec	AES-128
ECDHE Agree	1647.55%	112.424	1964.669	ops/sec	
ECDSA Sign	3934.24%	110.338	4451.298	ops/sec	
ECDSA Verify	947.63%	166.677	1746.164	ops/sec	


% increase in
CDSA Sign
C KeyGen
H KeyGen
ublic key
en (1024)
C-SHA512
C-SHA256
MAC-SHA
56-CMAC
SHA3-512
SHA3-256
SHA-512
SHA-256
SHA
3DES
CCM-Enc
-192-CTR
-ECB-dec
-ECB-dec
-ECB-dec
GCM-dec
GCM-dec


GCM-dec
-CBC-dec
-CBC-dec
-CBC-dec
RNG
0.00%
1000.00%
2000.00%
3000.00%


performance


%
4000.00%
5000.00%
6000.00%


7000.00%

```
Starting                                                        Power   On      Self
Power                                                           On      Self    Test
------------------------------------------------------------------------------

                                                                wolfSSL version 4.5.0
------------------------------------------------------------------------------

wolfCrypt                                                       Benchmark (block bytes
RNG                                                                  20 MB    took
AES-128-CBC-enc                                                      45 MB    took
AES-128-CBC-dec                                                      45 MB    took
AES-192-CBC-enc                                                      40 MB    took
AES-192-CBC-dec                                                      40 MB    took
AES-256-CBC-enc                                                      35 MB    took
AES-256-CBC-dec                                                      35 MB    took
AES-128-GCM-enc                                                      15 MB    took
AES-128-GCM-dec                                                      15 MB    took
AES-192-GCM-enc                                                      10 MB    took
AES-192-GCM-dec                                                      10 MB    took
AES-256-GCM-enc                                                      10 MB    took
AES-256-GCM-dec                                                      10 MB    took
AES-128-ECB-enc                                                      34 MB    took
AES-128-ECB-dec                                                      35 MB    took
AES-192-ECB-enc                                                      30 MB    took
AES-192-ECB-dec                                                      31 MB    took
AES-256-ECB-enc                                                      27 MB    took
AES-256-ECB-dec                                                      27 MB    took
AES-128-CTR                                                          45 MB    took
AES-192-CTR                                                          40 MB    took
AES-256-CTR                                                          35 MB    took
AES-CCM-Enc                                                          25 MB    took
AES-CCM-Dec                                                          25 MB    took
3DES                                                                 10 MB    took
MD5                                                                 150 MB    took
SHA                                                                 110 MB    took
SHA-224                                                              45 MB    took
SHA-256                                                              45 MB    took
SHA-384                                                              70 MB    took
SHA-512                                                              70 MB    took
SHA3-224                                                             70 MB    took
SHA3-256                                                             65 MB    took
SHA3-384                                                             50 MB    took
SHA3-512                                                             35 MB    took
AES-128-CMAC                                                         45 MB    took
AES-256-CMAC                                                         35 MB    took
HMAC-MD5                                                            150 MB    took
HMAC-SHA                                                            110 MB    took
```

HMAC-SHA224	45	MB	took
HMAC-SHA256	45	MB	took
HMAC-SHA384	70	MB	took
HMAC-SHA512	70	MB	took
PBKDF2	5	KB	took
RSA	1024	key	gen
RSA	2048	key	gen
RSA	2048	public	
RSA	2048	private	
DH	2048	key	gen
DH	2048	agree	
ECC	256	key	gen
ECDHE	256	agree	
ECDSA	256	sign	
ECDSA	256	verify	
Benchmark	complete		

Test
SUCCESS

1048576, min 1 sec each)
1.053 seconds, 18.988 MB/s
1.052 seconds, 42.782 MB/s
1.038 seconds, 43.371 MB/s
1.091 seconds, 36.671 MB/s
1.077 seconds, 37.129 MB/s
1.091 seconds, 32.094 MB/s
1.08 seconds, 32.419 MB/s
1.418 seconds, 10.581 MB/s
1.418 seconds, 10.577 MB/s
1.024 seconds, 9.764 MB/s
1.025 seconds, 9.752 MB/s
1.087 seconds, 9.197 MB/s
1.088 seconds, 9.192 MB/s
1 seconds, 34.18 MB/s
1 seconds, 34.931 MB/s
1 seconds, 30.173 MB/s
1 seconds, 30.741 MB/s
1 seconds, 27.01 MB/s
1 seconds, 27.473 MB/s
1.069 seconds, 42.109 MB/s
1.105 seconds, 36.19 MB/s
1.103 seconds, 31.725 MB/s
1.161 seconds, 21.533 MB/s
1.164 seconds, 21.482 MB/s
1.25 seconds, 8.003 MB/s
1.008 seconds, 148.831 MB/s
1.018 seconds, 108.038 MB/s
1.028 seconds, 43.771 MB/s
1.028 seconds, 43.773 MB/s
1.074 seconds, 65.186 MB/s
1.074 seconds, 65.187 MB/s
1.033 seconds, 67.74 MB/s
1.013 seconds, 64.147 MB/s
1.009 seconds, 49.564 MB/s
1.008 seconds, 34.721 MB/s
1.117 seconds, 40.288 MB/s
1.141 seconds, 30.671 MB/s
1.008 seconds, 148.865 MB/s
1.018 seconds, 108.038 MB/s

1.028	seconds,	43.76	MB/s					
1.03	seconds,	43.691	MB/s					
1.068	seconds,	65.538	MB/s					
1.068	seconds,	65.528	MB/s					
1.001	seconds,	4.902	KB/s					
2	ops	took	1.051	sec,	avg	525.597	ms,	1.903 ops/sec
1	ops	took	2.363	sec,	avg	2363.334	ms,	0.423 ops/sec
300	ops	took	1.327	sec,	avg	4.424	ms,	226.043 ops/sec
100	ops	took	7.535	sec,	avg	75.354	ms,	13.271 ops/sec
63	ops	took	1.009	sec,	avg	16.009	ms,	62.463 ops/sec
100	ops	took	3.381	sec,	avg	33.813	ms,	29.574 ops/sec
113	ops	took	1.008	sec,	avg	8.92	ms,	112.114 ops/sec
200	ops	took	1.779	sec,	avg	8.895	ms,	112.424 ops/sec
200	ops	took	1.813	sec,	avg	9.063	ms,	110.338 ops/sec
200	ops	took	1.2	sec,	avg	6	ms,	166.677 ops/sec

```
Starting                                                    Power   On      Self
Power                                                       On      Self    Test
------------------------------------------------------------------------------

                                                            wolfSSL version 4.5.0
------------------------------------------------------------------------------
wolfCrypt                                                   Benchmark (block bytes
RNG                                                                85 MB    took
AES-128-CBC-enc                                                   680 MB    took
AES-128-CBC-dec                                                   630 MB    took
AES-192-CBC-enc                                                   590 MB    took
AES-192-CBC-dec                                                   575 MB    took
AES-256-CBC-enc                                                   525 MB    took
AES-256-CBC-dec                                                   510 MB    took
AES-128-GCM-enc                                                   410 MB    took
AES-128-GCM-dec                                                   230 MB    took
AES-192-GCM-enc                                                   375 MB    took
AES-192-GCM-dec                                                   215 MB    took
AES-256-GCM-enc                                                   345 MB    took
AES-256-GCM-dec                                                   205 MB    took
AES-128-ECB-enc                                                   100 MB    took
AES-128-ECB-dec                                                   101 MB    took
AES-192-ECB-enc                                                    95 MB    took
AES-192-ECB-dec                                                    96 MB    took
AES-256-ECB-enc                                                    91 MB    took
AES-256-ECB-dec                                                    92 MB    took
AES-128-CTR                                                       820 MB    took
AES-192-CTR                                                       750 MB    took
AES-256-CTR                                                       695 MB    took
AES-CCM-Enc                                                       125 MB    took
AES-CCM-Dec                                                       125 MB    took
3DES                                                               10 MB    took
MD5                                                               145 MB    took
SHA                                                               110 MB    took
SHA-224                                                           570 MB    took
SHA-256                                                           565 MB    took
SHA-384                                                           125 MB    took
SHA-512                                                           125 MB    took
SHA3-224                                                           70 MB    took
SHA3-256                                                           65 MB    took
SHA3-384                                                           50 MB    took
SHA3-512                                                           35 MB    took
AES-128-CMAC                                                      180 MB    took
AES-256-CMAC                                                      150 MB    took
HMAC-MD5                                                          145 MB    took
HMAC-SHA                                                          110 MB    took
```

HMAC-SHA224	570	MB	took
HMAC-SHA256	570	MB	took
HMAC-SHA384	125	MB	took
HMAC-SHA512	125	MB	took
PBKDF2	21	KB	took
RSA	1024	key	gen
RSA	2048	key	gen
RSA	2048	public	
RSA	2048	private	
DH	2048	key	gen
DH	2048	agree	
ECC	256	key	gen
ECDHE	256	agree	
ECDSA	256	sign	
ECDSA	256	verify	
Benchmark	complete		

Test
SUCCESS

1048576, min 1 sec each)
1.062 seconds, 80.002 MB/s
1.004 seconds, 677.604 MB/s
1.003 seconds, 628.27 MB/s
1.001 seconds, 589.566 MB/s
1.007 seconds, 571.165 MB/s
1.006 seconds, 521.956 MB/s
1.006 seconds, 506.769 MB/s
1.012 seconds, 405.265 MB/s
1.021 seconds, 225.299 MB/s
1.008 seconds, 371.994 MB/s
1.001 seconds, 214.773 MB/s
1.004 seconds, 343.703 MB/s
1 seconds, 204.954 MB/s
1 seconds, 100.37 MB/s
1 seconds, 101.443 MB/s
1 seconds, 95.151 MB/s
1 seconds, 96.11 MB/s
1 seconds, 90.892 MB/s
1 seconds, 91.766 MB/s
1.003 seconds, 817.165 MB/s
1.004 seconds, 747.383 MB/s
1.005 seconds, 691.804 MB/s
1.016 seconds, 123.027 MB/s
1.03 seconds, 121.355 MB/s
1.303 seconds, 7.675 MB/s
1.002 seconds, 144.729 MB/s
1.018 seconds, 108.015 MB/s
1.005 seconds, 567.15 MB/s
1.001 seconds, 564.354 MB/s
1.002 seconds, 124.718 MB/s
1.002 seconds, 124.745 MB/s
1.032 seconds, 67.821 MB/s
1.012 seconds, 64.215 MB/s
1.008 seconds, 49.586 MB/s
1.008 seconds, 34.712 MB/s
1.028 seconds, 175.138 MB/s
1.013 seconds, 148.137 MB/s
1.003 seconds, 144.562 MB/s
1.018 seconds, 108.025 MB/s

1.005	seconds,	567.221	MB/s					
1.005	seconds,	567.245	MB/s					
1.002	seconds,	124.724	MB/s					
1.002	seconds,	124.699	MB/s					
1.001	seconds,	21.003	KB/s					
2	ops	took	1.072	sec,	avg	536.137	ms,	1.865 ops/sec
1	ops	took	1.111	sec,	avg	1110.913	ms,	0.9 ops/sec
4100	ops	took	1.006	sec,	avg	0.245	ms,	4074.352 ops/sec
200	ops	took	1.659	sec,	avg	8.295	ms,	120.561 ops/sec
251	ops	took	1.002	sec,	avg	3.99	ms,	250.623 ops/sec
300	ops	took	1.199	sec,	avg	3.995	ms,	250.298 ops/sec
7144	ops	took	1	sec,	avg	0.14	ms,	7143.951 ops/sec
2000	ops	took	1.018	sec,	avg	0.509	ms,	1964.669 ops/sec
4500	ops	took	1.011	sec,	avg	0.225	ms,	4451.298 ops/sec
1800	ops	took	1.031	sec,	avg	0.573	ms,	1746.164 ops/sec