

Contents

1	Comparing: (plain) vs (+SSBD) vs (+SSBD+v1) vs (+SSBD+v1+RSB)	2
2	Comparing: (-SSBD+v1+RSB) vs (+SSBD+v1+RSB)	7
3	Comparing: Code size	10

1 **Comparing: (plain) vs (+SSBD) vs (+SSBD+v1) vs (+SSBD+v1+RSB)**

Table 1: Performance: 11700K - fastest implementations.

Primitive	Impl.	Op.	Alt	plain	+SSBD	+SSBD+v1	+SSBD+v1+RSB	increase %
ChaCha20	avx2	1 KiB	-	1198	1202	1244	1246	4.01
		1 KiB xor	1230	1208	1212	1248	1250	3.48
		16 KiB	-	19040	19052	19066	19068	0.15
		16 KiB xor	18960	19070	19086	19096	19110	0.21
Poly1305	avx2	1 KiB	704	670	672	720	718	7.16
		1 KiB verif	-	674	676	726	724	7.42
		16 KiB	8590	8942	8948	8990	8986	0.49
		16 KiB verif	-	8942	8984	8984	8984	0.47
XSalsa20Poly1305	avx2	128 B	1834	1206	1212	1250	1246	3.32
		128 B open	2698	1964	1970	2044	2046	4.18
		1 KiB	5956	3140	3142	3190	3188	1.53
		1 KiB open	6858	3900	3904	3988	3988	2.26
		16 KiB	82642	32598	32574	32604	32602	0.01
		16 KiB open	83582	33292	33274	33358	33362	0.21
X25519	mulx	smult	121730	102848	104150	104424	104428	1.54
Kyber512	avx2	keypair	28802	27676	28106	28040	28090	1.50
		enc	31032	37050	38332	38876	38792	4.70
		dec	38816	29302	30444	30590	30714	4.82
Kyber768	avx2	keypair	48036	43432	45708	45860	46548	7.17
		enc	49016	57006	59316	60028	60674	6.43
		dec	60682	46138	48418	48532	49294	6.84

Table 2: Performance: 11700K - fastest implementations - step by step overhead.

Primitive	Impl.	Op.	plain	+SSBD	%	+SSBD+v1	%	+SSBD+v1+RSB	%	increase %
ChaCha20	avx2	128 B	344	344	0.00	398	15.70	398	0.00	15.70
		128 B xor	350	350	0.00	402	14.86	400	-0.50	14.29
		1 KiB	1198	1202	0.33	1244	3.49	1246	0.16	4.01
		1 KiB xor	1208	1212	0.33	1248	2.97	1250	0.16	3.48
		16 KiB	19040	19052	0.06	19066	0.07	19068	0.01	0.15
		16 KiB xor	19070	19086	0.08	19096	0.05	19110	0.07	0.21
Poly1305	avx2	128 B	138	142	2.90	182	28.17	180	-1.10	30.43
		128 B verif	142	146	2.82	180	23.29	178	-1.11	25.35
		1 KiB	670	672	0.30	720	7.14	718	-0.28	7.16
		1 KiB verif	674	676	0.30	726	7.40	724	-0.28	7.42
		16 KiB	8942	8948	0.07	8990	0.47	8986	-0.04	0.49
		16 KiB verif	8942	8948	0.07	8984	0.40	8984	0.00	0.47
XSalsa20Poly1305	avx2	128 B	1206	1212	0.50	1250	3.14	1246	-0.32	3.32
		128 B open	1964	1970	0.31	2044	3.76	2046	0.10	4.18
		1 KiB	3140	3142	0.06	3190	1.53	3188	-0.06	1.53
		1 KiB open	3900	3904	0.10	3988	2.15	3988	0.00	2.26
		16 KiB	32598	32574	-0.07	32604	0.09	32602	-0.01	0.01
		16 KiB open	33292	33274	-0.05	33358	0.25	33362	0.01	0.21
SHAKE256	avx2	128 B \leftarrow 128 B	1206	1324	9.78	1390	4.98	1390	0.00	15.26
		256 B \leftarrow 128 B	2334	2450	4.97	2534	3.43	2546	0.47	9.08
		512 B \leftarrow 128 B	4588	4700	2.44	4796	2.04	4826	0.63	5.19
		1 KiB \leftarrow 128 B	9102	9216	1.25	9400	2.00	9384	-0.17	3.10
X25519	mulx	smult	102848	104150	1.27	104424	0.26	104428	0.00	1.54
Kyber512	avx2	keypair	27676	28106	1.55	28040	-0.23	28090	0.18	1.50
		enc	37050	38332	3.46	38876	1.42	38792	-0.22	4.70
		dec	29302	30444	3.90	30590	0.48	30714	0.41	4.82
Kyber768	avx2	keypair	43432	45708	5.24	45860	0.33	46548	1.50	7.17
		enc	57006	59316	4.05	60028	1.20	60674	1.08	6.43
		dec	46138	48418	4.94	48532	0.24	49294	1.57	6.84

Table 3: Performance: 11700K - ref implementations.

Primitive	Impl.	Op.	plain	+SSBD	+SSBD+v1	+SSBD+v1+RSB	increase %
ChaCha20	ref	128 B	768	794	822	820	6.77
		128 B xor	774	798	826	824	6.46
		1 KiB	5932	6098	6140	6130	3.34
		1 KiB xor	5984	6148	6190	6176	3.21
		16 KiB	94420	96926	97220	97228	2.97
		16 KiB xor	95218	97708	98066	98010	2.93
Poly1305	ref	128 B	138	142	180	178	28.99
		128 B verif	142	144	186	188	32.39
		1 KiB	1126	1130	1154	1154	2.49
		1 KiB verif	1120	1126	1158	1156	3.21
		16 KiB	17542	17548	17568	17570	0.16
		16 KiB verif	17542	17580	17580	17574	0.18
XSalsa20Poly1305	ref	128 B	1626	1648	1680	1678	3.20
		128 B open	2384	2410	2478	2478	3.94
		1 KiB	7860	7916	7926	7926	0.84
		1 KiB open	8596	8666	8718	8720	1.44
		16 KiB	113852	114990	114892	114880	0.90
		16 KiB open	114662	115934	115758	115760	0.96
SHAKE256	ref	128 B \leftarrow 128 B	1176	1226	1242	1230	4.59
		256 B \leftarrow 128 B	2274	2368	2386	2370	4.22
		512 B \leftarrow 128 B	4454	4654	4670	4746	6.56
		1 KiB \leftarrow 128 B	8824	9214	9238	9284	5.21
X25519	ref4	smult	121300	125798	126252	126286	4.11

Table 4: Performance: 11700K - ref implementations - step by step overhead.

Primitive	Impl.	Op.	plain	+SSBD	%	+SSBD+v1	%	+SSBD+v1+RSB	%	increase	%
ChaCha20	avx2	128 B	768	794	3.39	822	3.53	820	-0.24	6.77	
		128 B xor	774	798	3.10	826	3.51	824	-0.24	6.46	
		1 KiB	5932	6098	2.80	6140	0.69	6130	-0.16	3.34	
		1 KiB xor	5984	6148	2.74	6190	0.68	6176	-0.23	3.21	
		16 KiB	94420	96926	2.65	97220	0.30	97228	0.01	2.97	
		16 KiB xor	95218	97708	2.62	98066	0.37	98010	-0.06	2.93	
Poly1305	avx2	128 B	138	142	2.90	180	26.76	178	-1.11	28.99	
		128 B verif	142	144	1.41	186	29.17	188	1.08	32.39	
		1 KiB	1126	1130	0.36	1154	2.12	1154	0.00	2.49	
		1 KiB verif	1120	1126	0.54	1158	2.84	1156	-0.17	3.21	
		16 KiB	17542	17548	0.03	17568	0.11	17570	0.01	0.16	
		16 KiB verif	17542	17548	0.03	17580	0.18	17574	-0.03	0.18	
XSalsa20Poly1305	avx2	128 B	1626	1648	1.35	1680	1.94	1678	-0.12	3.20	
		128 B open	2384	2410	1.09	2478	2.82	2478	0.00	3.94	
		1 KiB	7860	7916	0.71	7926	0.13	7926	0.00	0.84	
		1 KiB open	8596	8666	0.81	8718	0.60	8720	0.02	1.44	
		16 KiB	113852	114990	1.00	114892	-0.09	114880	-0.01	0.90	
		16 KiB open	114662	115934	1.11	115758	-0.15	115760	0.00	0.96	
SHAKE256	avx2	128 B \leftarrow 128 B	1176	1226	4.25	1242	1.31	1230	-0.97	4.59	
		256 B \leftarrow 128 B	2274	2368	4.13	2386	0.76	2370	-0.67	4.22	
		512 B \leftarrow 128 B	4454	4654	4.49	4670	0.34	4746	1.63	6.56	
		1 KiB \leftarrow 128 B	8824	9214	4.42	9238	0.26	9284	0.50	5.21	
X25519	mulx	smult	121300	125798	3.71	126252	0.36	126286	0.03	4.11	

2 Comparing: $(-SSBD+v1+RSB)$ vs $(+SSBD+v1+RSB)$

Table 5: Performance: 11700K - fastest implementations

Primitive	Impl.	Op.	-SSBD+v1+RSB	+SSBD+v1+RSB	increase %
ChaCha20	avx2	128 B	398	398	0.00
	avx2	128 B xor	400	400	0.00
	avx2	1 KiB	1244	1246	0.16
	avx2	1 KiB xor	1242	1250	0.64
	avx2	16 KiB	19052	19068	0.08
	avx2	16 KiB xor	19106	19110	0.02
Poly1305	avx2	128 B	182	180	-1.10
	avx2	128 B verif	176	178	1.14
	avx2	1 KiB	720	718	-0.28
	avx2	1 KiB verif	724	724	0.00
	avx2	16 KiB	8988	8986	-0.02
	avx2	16 KiB verif	8980	8984	0.04
XSalsa20Poly1305	avx2	128 B	1252	1246	-0.48
	avx2	128 B open	2044	2046	0.10
	avx2	1 KiB	3196	3188	-0.25
	avx2	1 KiB open	3998	3988	-0.25
	avx2	16 KiB	32612	32602	-0.03
	avx2	16 KiB open	33390	33362	-0.08
X25519	mulx	smult	102728	104428	1.65
Kyber512	avx2	keypair	28132	28090	-0.15
	avx2	enc	37620	38792	3.12
	avx2	dec	29806	30714	3.05
Kyber768	avx2	keypair	44454	46548	4.71
	avx2	enc	58398	60674	3.90
	avx2	dec	47336	49294	4.14

Table 6: Performance: 11700K - reference implementations

Primitive	Impl.	Op.	-SSBD+v1+RSB	+SSBD+v1+RSB	increase %
ChaCha20	ref	128 B	804	820	1.99
	ref	128 B xor	806	824	2.23
	ref	1 KiB	5982	6130	2.47
	ref	1 KiB xor	6024	6176	2.52
	ref	16 KiB	94736	97228	2.63
	ref	16 KiB xor	95426	98010	2.71
Poly1305	ref	128 B	182	178	-2.20
	ref	128 B verif	188	188	0.00
	ref	1 KiB	1156	1154	-0.17
	ref	1 KiB verif	1158	1156	-0.17
	ref	16 KiB	17568	17570	0.01
	ref	16 KiB verif	17576	17574	-0.01
XSalsa20Poly1305	ref	128 B	1666	1678	0.72
	ref	128 B open	2464	2478	0.57
	ref	1 KiB	7868	7926	0.74
	ref	1 KiB open	8664	8720	0.65
	ref	16 KiB	113890	114880	0.87
	ref	16 KiB open	114720	115760	0.91

3 Comparing: Code size

Table 7: Object size in bytes.

Impl.	plain	+v1	+v1+RSB
crypto-hash/sha256/amd64/ref	10952	10856	
crypto-hash/sha3-224/amd64/avx2	6248	6704	
crypto-hash/sha3-224/amd64/ref	8576	8416	
crypto-hash/sha3-256/amd64/avx2	6248	6704	
crypto-hash/sha3-256/amd64/ref	8576	8416	
crypto-hash/sha3-384/amd64/avx2	6248	6704	
crypto-hash/sha3-384/amd64/ref	8576	8416	
crypto-hash/sha3-512/amd64/avx2	6248	6704	
crypto-hash/sha3-512/amd64/ref	8576	8416	
crypto-kem/kyber/kyber512/amd64/avx2	145424	150776	
crypto-kem/kyber/kyber768/amd64/avx2	193088	204952	
crypto-onetimeauth/poly1305/amd64/avx2	9560	9560	
crypto-onetimeauth/poly1305/amd64/avx	10128	10160	
crypto-onetimeauth/poly1305/amd64/ref	2472	2496	
crypto-scalarmlt/curve25519/amd64/mulx	18912	18816	
crypto-scalarmlt/curve25519/amd64/ref4	11616	11536	
crypto-scalarmlt/curve25519/amd64/ref5	13568	13504	
crypto-secretbox/xsalsa20poly1305/amd64/avx2	24816	24784	
crypto-secretbox/xsalsa20poly1305/amd64/avx	24456	24456	
crypto-secretbox/xsalsa20poly1305/amd64/ref	11736	11496	
crypto-stream/chacha/chacha12/amd64/avx2	18648	18648	
crypto-stream/chacha/chacha12/amd64/avx	16856	16856	
crypto-stream/chacha/chacha12/amd64/ref	5288	5312	
crypto-stream/chacha/chacha20/amd64/avx2	18648	18648	
crypto-stream/chacha/chacha20/amd64/avx	16856	16856	
crypto-stream/chacha/chacha20/amd64/ref	5288	5312	
crypto-stream/chacha/chacha20-ietf/amd64/avx2	19176	19208	
crypto-stream/chacha/chacha20-ietf/amd64/avx	17216	17216	
crypto-stream/chacha/chacha20-ietf/amd64/ref	5400	5416	
crypto-stream/salsa20/salsa2012/amd64/avx2	11784	11816	
crypto-stream/salsa20/salsa2012/amd64/avx	11056	11088	
crypto-stream/salsa20/salsa2012/amd64/ref	5880	5912	
crypto-stream/salsa20/salsa20/amd64/avx2	11728	11760	
crypto-stream/salsa20/salsa20/amd64/avx	11008	11040	
crypto-stream/salsa20/salsa20/amd64/ref	5840	5872	
crypto-stream/xsalsa20/amd64/avx2	13544	13320	
crypto-stream/xsalsa20/amd64/avx	12704	12480	
crypto-stream/xsalsa20/amd64/ref	7000	7032	
crypto-xof/shake128/amd64/avx2	6344	6832	
crypto-xof/shake128/amd64/ref	8688	8528	
crypto-xof/shake256/amd64/avx2	6344	6832	
crypto-xof/shake256/amd64/ref1	4416	4416	
crypto-xof/shake256/amd64/ref	8688	8528	
crypto-xof/shake256/amd64/spec	9408	8960	