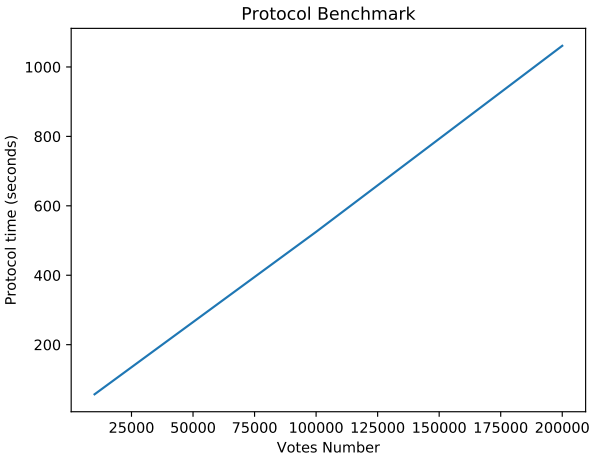
Table 1: Hat shuffle mix-net benchmark

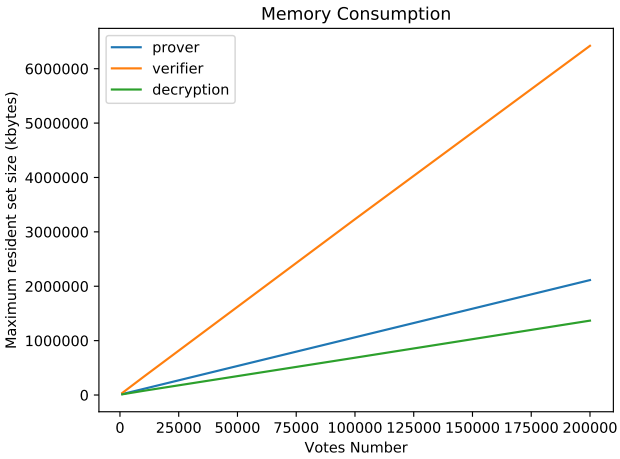
module	phase	10.000	10.000-P	100.000	100.000-P	200.000	200.000-P	1.000.000**
crs	Generation	3.6220s	2.2555s	27.1784s	10.8926s	49.5121s	19.4441s	218.1849s
	Serialization	1.7291s	—	15.1980s	—	29.1654s	—	152.4044s
	Total	5.3511s	—	42.3764s	—	78.6775s	—	370.5893s
generate_votes		0.9358s	—	6.0873s	—	13.0127s	—	66.1600s
encrypt	CRS Deserialization	0.4397s	—	3.3140s	—	6.2664s	—	31.2038s
	Votes Deserialization	0.0946s	—	0.5895s	—	1.0446s	—	4.0429s
	Encryption	27.0073s	—	270.0997s	—	542.9835s	—	2700.1721s
	Ciphertexts Serialization	0.4681s	—	4.6864s	—	9.4914s	—	50.7118s
	Total	28.0097s	—	328.6896s	—	559.7859s	—	2786.1306s
prove	CRS Deserialization	1.0799s	—	8.5572s	—	16.3996s	—	56.2043s**
	Ciphertexts Deserialization	0.7445s	—	7.2519s	—	14.2327s	—	45.9318s**
	Prove	13.3515s	9.2914s	112.8631s	69.9510s	220.3691s	138.3695s	389.7539s**
	Proofs Serialization	2.7578s	—	22.1532s	—	52.1241s	—	101.1021s**
	Total	17.9337s	—	150.8254s	—	303.1255s	—	603.2646s**
verify	CRS Deserialization	0.9295s	—	8.5857s	—	17.2045s	—	58.4569s**
	Ciphertexts Deserialization	0.6768s	—	6.8215s	—	14.3577s	—	42.6796s**
	Proofs Deserialization	1.4613s	—	14.9167s	—	30.0238s	—	103.6393s**
	Verify	26.4480s	8.2774s	248.5492s	74.1561s	494.0374s	150.2706s	1655.6244s**
	Total	29.5156s	—	278.8731s	—	555.6234s	—	1860.4001s**
decrypt	Votes Deserialization	0.0895s	—	0.5400s	—	1.1618s	—	2.0494s**
	Ciphertexts Deserialization	0.5507s	—	5.7847s	—	11.5266s	—	36.8059s**
	Table	9.4963s	—	93.6353s	—	184.4576s	—	408.1059s**
	Decryption	9.0543s	—	91.3663s	—	190.1704s	—	381.1743s**
	Votes Serialization	0.0144s	—	0.1591s	—	0.2904s	—	0.5766s**
	Total	19.2052s	—	191.4854s	—	387.6068s	—	828.7121s**
mix *		0:47m	0:25m	7:10m	3:35m	14:19m	7:18m	41:03m**

* mix = Prove + Verify
** MacOSX: 16GB RAM
-P: Parallel
vm specs: Ubuntu LTS 16.04 (image), 4 (CPUs), 8192MB (RAM), 40GB (System Disk)

Table 1: JSON files sizes

File	1.000	10.000	100.000	200.000	1.000.000
ciphertexts	829K	8.1M	81M	162M	809M
crs	1.3M	13M	124M	248M	1.2GB
votes	87K	865K	8.5M	17M	84M
proofs	2.2M	21M	210M	420M	2GB


Protocol Benchmark
Protocol time (seconds)
1000
800
600
400
200
25000
50000
75000
100000
125000
150000
175000
200000
Votes Number


Memory Consumption
prover
verifier
decryption
Maximum resident set size (kbytes)
6000000
5000000
4000000
3000000
2000000
1000000
0
0
25000
50000
75000
100000
125000
150000
175000
200000
Votes Number