Small-Proof Big-Data Benchmark Result

5/8/2013

Benchmark Result

- Input to Prover/Verifier
  - \# of Updates: 10000
  - \# of Queries: 1000

  Performance (with GDBM)

k	n	Matrix Dim	Prover Update (ms)	Prover Query (ms)	Verifier Update (ms)	Verifier Verification (ms)
32	128	32 * 480	1.2	5.83	0.64	1.45
32	1024	32 * 576	2.95	9.02	0.81	1.67
32	16384	32 * 704	2.83	5.69		
64	128	64 * 1024	8.53	14.05	2.55	5.56
64	1024	64 * 1216	9.14	11.54	3.04	6.44
64	16384	64 * 1472	9.58	23.4		
128	128	128 * 2176	27.4	37.5	14.69	55.76
128	1024	128 * 2560	32.12	32.4	17.71	57.2
128	16384	128 * 3072	39.1	48.42		

Prover Analysis

Operation	Function	Percentage
Matrix-Vector product	gsl_blas_dgemv()	87.51 %
Vector Operation	get_binary_representation() gsl_vector_add	6.46 %
GDBM IO	sgdbm_insert_label() sgdbm_get_node_label() encode_vector() decode_vector_buffer()	2.03 %
Modulus	mod_q	1.79 %