$\mathbb{F}_{p^2}$ Batched Inverse Benchmarks – April 17, 2017

1 Batched Inversion Times

Execution time for 1000 batched inversions, measured in seconds.

Modulus Size	Regular Batch	Partial ZZ_p	Unbatched
32	0.045887	0.013814	0.015516
64	0.0470929	0.0138798	0.0169492
128	0.0421679	0.015892	0.0268679
256	0.060961	0.0234561	0.043083
512	0.0800149	0.0383809	0.084594
1024	0.172746	0.0831001	0.180252
2048	0.369	0.223628	0.420926

Table 1: Execution time for Batch size 10

Modulus Size	Regular Batch	Partial ZZ_p	Unbatched
32	0.351996	0.13946	0.159744
64	0.335376	0.132932	0.167551
128	0.356995	0.150744	0.299575
256	0.748303	0.207973	0.486726
512	0.655977	0.34409	0.886866
1024	1.49688	0.762736	1.83442
2048	3.44086	2.07405	4.39554

Table 2: Execution time for Batch size 100

Modulus Size	Regular Batch	Partial ZZ_p	Unbatched
32	3.45507	1.35421	1.51127
64	3.4481	1.32611	1.61707
128	3.64458	1.54956	2.95078
256	7.00599	2.18369	4.80218
512	6.563	3.39861	8.87935
1024	14.8953	7.90045	18.3234
2048	36.216	22.2085	42.616

Table 3: Execution time for Batch size 1000

2 Multiplication & Inversion Times

Modulus Size	Mult Time	Inversion Time
32	0.000336885	0.00080204
64	0.000315905	0.00116491
128	0.000372171	0.00434804
256	0.000577927	0.00821996
512	0.00102496	0.015533
1024	0.00268006	0.0190439
2048	0.00599885	0.0388269

Table 4: For 1000 operations, measured in seconds