Batched Inversion Results on SIDH Signatures (Yoo et. al)

Robert Gorrie – McMaster University – September 15, 2017

1 Batched Partial-Inversion Procedure

describe how the procedure works
describe where the procedure can be used in SIDH/signatures

2 Performance

2.1 Numbers

All results are measured in clock cycles, executed on a single-core, 1.70 GHz Intel Celeron CPU. All benchmarks are averages computed from 100 randomized sample runs.

Procedure	Perf. Without Batching	Perf With Batching
KeyGen	68881331	68881331
Signature Sign	15744477032	15565738003
Signature Verify	11183112648	10800158871

In the following table, "Batched Inversion" signifies running the batched partial-inversion procedure on 248 $\mathbb{F}_{p^2}$ elements. The procedure uses the binary GCD $\mathbb{F}_p$ inversion function which, unlike regular $\mathbb{F}_{p^2}$ montgomery inversion, is not constant time.

Procedure	Performance
Batched Inversion	1721718
$\mathbb{F}_{p^2}$ Montgomery Inversion	874178

2.2 Analysis

check notes in "averages" file