Contents

1 Benchmark

1.1 Arithmetic Gmw Operation

Table 1.1: Run-times in microseconds for arithmetic gmw operations (128-bit) of two parties

Protocol	Preproc. (ms)	Total (ms)	Sent (ms)	Sent Msg	Rec (ms)	Rec Msg
EQ	1,186.1	1,323.34	0.57	647	1.07	647
EQC	1,389.71	1,591.22	0.57	647	1.07	647
EQZ	1,350.89	1,646.96	0.57	647	1.07	647
LTBits	429.2	990.76	0.15	1,539	0.15	1,539
LTTBits	403.71	942.42	0.17	1,795	0.17	1,795
LTC	1,373.04	2,090.71	0.83	3,205	1.32	3,205
LTEQC	1,921.1	2,500.22	1.36	3,462	2.36	3,462
LTS	517.66	1,239.06	0.56	3,078	0.56	3,078
LTEQS	855.15	1,799.94	0.7	3,207	0.7	3,207
LTZ	1,250.4	1,550.61	0.63	1,029	1.12	1,029
LT	1,408.83	1,654.6	0.63	1,029	1.12	1,029
ModPow2m	1,211.68	1,718.64	0.69	1,782	1.18	1,782
ObliviousModPow2m	4,025.39	4,957.78	3.83	2,565	5.82	2,565
LogicalRShift slow	1,262.67	1,671.18	0.69	1,786	1.2	1,786
LogicalRShift	1,169.73	1,449.84	0.63	1,029	1.12	1,029
LogicalLShift	0.64	2.78	0	3	0	3
ArithmeticRShift	1,110.35	1,412.02	0.63	1,029	1.12	1,029
ArithmeticLShift	0.44	2.69	0	3	0	3
TruncPr	1,182.06	1,186.16	0.55	393	1.05	265
TruncPriv	1,972.99	2,680.97	1.76	2,053	2.75	2,053
TruncateAndReduce	591.67	1,240.56	0.74	3,591	0.74	3,591
UnsignedExtension	672.66	1,417.96	0.74	3,592	0.75	3,592
SignedExtension	566.56	1,194.49	0.74	3,592	0.75	3,592
EdaBit	1,172.52	1,175.53	0.55	390	1.03	262
B2U	1,924.4	2,748.05	1.76	2,311	2.75	2,311
Demux	567.27	581.45	$5.3 \cdot 10^{-2}$	407	$5.3 \cdot 10^{-2}$	407
DigitDecomposition	743.26	3,200.27	1.81	10,876	1.59	10,876
Pow2	1,357.7	1,866.31	1.16	1,412	1.66	1,412
Int2FL	2,248.67	3,191.83	1.5	2,265	2.69	2,265
Int2Fx	0.44	7.55	0	3	0	3

1.2 Floating-Point Operations

Table 1.2: Run-times in microseconds for floating-point operations based on boolean circuit (bgmw, 64-bit, SIMD = 1) of two parties

Protocol	Preproc. (ms)	Total (ms)	Sent (ms)	Sent Msg	Rcv (ms)	Rec Msg
Add	501.69	2,336.22	0.89	9,115	0.89	9,115
Sub	416.21	2,874.56	0.88	8,995	0.88	8,995
Mul	529.69	4,684.19	2.23	22,525	2.23	22,525
Div	621.76	21,576.67	4.42	45,871	4.42	45,871
Lt	427.36	933.71	0.12	1,243	0.12	1,243
Gt	497.06	933.68	0.12	1,243	0.12	1,243
Eq	437.91	623.33	$4.7 \cdot 10^{-2}$	515	$4.7 \cdot 10^{-2}$	515
EQZ	429.87	552.47	$4.7 \cdot 10^{-2}$	515	$4.7 \cdot 10^{-2}$	515
LTZ	0.31	2.27	0	3	0	3
Exp2	554.4	21,948.46	4.29	43,251	4.29	43,251
Log2	629.38	19,093.09	3.96	39,971	3.96	39,971
Exp	662.35	22,535.52	5.33	53,757	5.33	53,757
Ln	520.78	43,854.15	7.04	71,925	7.04	71,925
Sqr	455.05	2,814.48	1.34	13,581	1.34	13,581
Sqrt	535.3	11,461.13	2.5	25,801	2.5	25,801
Ceil	404.27	1,363.52	0.16	1,689	0.16	1,689
Floor	537.48	1,545.27	0.16	1,691	0.16	1,691
FL2Int	472.61	1,995.88	0.33	3,323	0.33	3,323
MulPow2m	489.46	629.29	$5.3 \cdot 10^{-2}$	579	$5.3 \cdot 10^{-2}$	579
DivPow2m	406.98	549.65	$5.7 \cdot 10^{-2}$	613	$5.7 \cdot 10^{-2}$	613
ClampB	407.94	549.76	$5.8 \cdot 10^{-2}$	591	$5.8 \cdot 10^{-2}$	591
RoundToNearestInt	369	900.87	0.24	2,491	0.24	2,491

Table 1.3: Run-times in microseconds for floating-point operations based on boolean circuit amortized over 1000 SIMD (bgmw, 64-bit) of two parties

Protocol	Preproc. (ms)	Total (ms)	Sent (ms)	Sent Msg	Rcv (ms)	Rec Msg
Add	20.31	22.51	$6.94 \cdot 10^{-2}$	9.12	$6.94 \cdot 10^{-2}$	9.12
Sub	20.33	22.28	$6.85 \cdot 10^{-2}$	9	$6.85 \cdot 10^{-2}$	9
Mul	51.37	54.49	0.18	22.53	0.18	22.53
Div	102.95	130.03	0.36	45.87	0.36	45.87
Lt	2.48	2.8	$6.83 \cdot 10^{-3}$	1.24	$6.83 \cdot 10^{-3}$	1.24
Gt	2.72	3.06	$6.83 \cdot 10^{-3}$	1.24	$6.83 \cdot 10^{-3}$	1.24
Eq	0.6	0.77	$1.04 \cdot 10^{-3}$	0.52	$1.04 \cdot 10^{-3}$	0.52
EQZ	0.79	0.9	$1.04 \cdot 10^{-3}$	0.52	$1.04 \cdot 10^{-3}$	0.52
LTZ	$6.46 \cdot 10^{-4}$	$9.76 \cdot 10^{-3}$	0	$3 \cdot 10^{-3}$	0	$3 \cdot 10^{-3}$
Exp2	97.55	119	0.34	43.25	0.34	43.25
Log2	91.41	107.76	0.32	39.97	0.32	39.97
Exp	131.68	155.49	0.42	53.76	0.42	53.76
Ln	183.39	226.62	0.57	71.93	0.57	71.93
Sqr	36.11	38.79	0.11	13.58	0.11	13.58
Sqrt	64.19	80.57	0.2	25.8	0.2	25.8
Ceil	4.11	4.75	$1.04 \cdot 10^{-2}$	1.69	$1.04 \cdot 10^{-2}$	1.69
Floor	4.05	4.83	$1.04 \cdot 10^{-2}$	1.69	$1.04 \cdot 10^{-2}$	1.69
FL2Int	8.27	9.87	$2.34 \cdot 10^{-2}$	3.32	$2.34 \cdot 10^{-2}$	3.32
MulPow2m	1.09	1.36	$1.55 \cdot 10^{-3}$	0.58	$1.55 \cdot 10^{-3}$	0.58
DivPow2m	1.03	1.3	$1.83 \cdot 10^{-3}$	0.61	$1.83 \cdot 10^{-3}$	0.61
ClampB	1.42	1.64	$2.64 \cdot 10^{-3}$	0.59	$2.64 \cdot 10^{-3}$	0.59
RoundToNearestInt	6.81	7.59	$1.68 \cdot 10^{-2}$	2.49	$1.68 \cdot 10^{-2}$	2.49

Table 1.4: Run-times in microseconds for floating-point operations based on arithmetic gmw (128-bit) of two parties

Protocol	Preproc. (ms)	Total (ms)	Sent (ms)	Sent Msg	Rcv (ms)	Rec Msg
Add	10,022.89	12,623.8	6.8	7,206	11.49	7,206
Sub	9,529.35	12,602.21	6.8	7,206	11.49	7,206
Mul	4,033.73	5,352.73	1.83	2,319	3.32	2,319
Div	21,873.93	22,888.4	10.28	2,534	19.93	2,534
Lt	3,438.32	4,028.59	1.8	1,950	3.3	1,950
Gt	3,257.77	3,757.67	1.8	1,950	3.3	1,950
Eq	2,523.06	2,765.25	1.14	916	2.14	916
EQZ	0.58	6.37	0	3	0	3
LTZ	0.49	7.3	0	3	0	3
Exp2	$1.5 \cdot 10^5$	$1.84 \cdot 10^5$	99.34	$1.07 \cdot 10^5$	180.9	$1.07 \cdot 10^5$
Log2	$2.65 \cdot 10^5$	$3.37 \cdot 10^5$	205.22	$2.04 \cdot 10^5$	360.18	$2.04 \cdot 10^5$
Sqrt	68,981.07	93,437.32	62.83	65,772	110.57	65,772
Ceil	7,479.74	9,928.18	6.71	4,645	11.18	4,645
Floor	7,397.75	10,345.52	6.71	4,645	11.18	4,645
Neg	0.59	53.41	0	3	0	3
FL2Int	0.47	2.85	0	3	0	3

1.3 Fixed-Point Operations

Table 1.5: Run-times in microseconds for fixed-point operations based on boolean circuit (bgmw, 64-bit, SIMD = 1) of two parties

Protocol	Preproc. (ms)	Total (ms)	Sent (ms)	Sent Msg	Rec (ms)	Rec Msg
Add	534.39	695.29	0.11	1,155	0.11	1,155
Sub	644.15	854.17	0.11	1,155	0.11	1,155
Mul	663.06	2,550.88	0.89	9,043	0.89	9,043
Div	589.42	11,991.24	1.01	10,165	1.01	10,165
Div-Goldschmidt	893.7	22,797.67	10.15	$1.02 \cdot 10^5$	10.15	$1.02 \cdot 10^5$
Lt	609.85	840.53	$7.1 \cdot 10^{-2}$	757	$7.1 \cdot 10^{-2}$	757
Gt	590.79	832.42	$7.1 \cdot 10^{-2}$	757	$7.1 \cdot 10^{-2}$	757
Eq	480.39	633.7	$4.7 \cdot 10^{-2}$	515	$4.7 \cdot 10^{-2}$	515
EQZ	501.19	637.1	$4.7 \cdot 10^{-2}$	515	$4.7 \cdot 10^{-2}$	515
LTZ	0.49	2.13	0	3	0	3
Exp2-P1045	610.09	10,493.93	2.38	23,959	2.38	23,959
Log2-P2508	722.35	22,277.85	10.63	$1.07 \cdot 10^5$	10.63	$1.07 \cdot 10^5$
Exp	769.86	12,939	2.72	27,441	2.72	27,441
Ln	751.91	21,894.24	10.92	$1.1 \cdot 10^5$	10.92	$1.1 \cdot 10^5$
Sqrt	821.58	22,562.44	10.71	$1.08 \cdot 10^5$	10.71	$1.08 \cdot 10^5$
Sqrt-P0132	751.36	12,291.08	5.97	60,125	5.97	60,125
Ceil	575.3	896.91	$7.2 \cdot 10^{-2}$	767	$7.2 \cdot 10^{-2}$	767
Floor	1.31	62.06	0	3	0	3
Fx2Int	675.17	975.68	0.1	1,065	0.1	1,065
Fx2FL-	556.1	2,483.74	0.58	5,831	0.58	5,831

Table 1.6: Run-times in microseconds for fixed-point operations based on boolean circuit amortized over 1000 SIMD (bgmw, 64-bit) of two parties

Protocol	Preproc. (ms)	Total (ms)	Sent (ms)	Sent Msg	Rec (ms)	Rec Msg
Add	2.41	2.67	$6.13 \cdot 10^{-3}$	1.16	$6.13 \cdot 10^{-3}$	1.16
Sub	2.3	2.47	$6.13 \cdot 10^{-3}$	1.16	$6.13 \cdot 10^{-3}$	1.16
Mul	22.81	24.5	$6.89 \cdot 10^{-2}$	9.04	$6.89 \cdot 10^{-2}$	9.04
Div	25.84	40.56	$7.79 \cdot 10^{-2}$	10.17	$7.79 \cdot 10^{-2}$	10.17
Div-Goldschmidt	268.35	293.33	0.81	102.3	0.81	102.3
Lt	1.68	1.75	$2.97 \cdot 10^{-3}$	0.76	$2.97 \cdot 10^{-3}$	0.76
Gt	1.63	1.79	$2.97 \cdot 10^{-3}$	0.76	$2.97 \cdot 10^{-3}$	0.76
Eq	0.83	1	$1.04 \cdot 10^{-3}$	0.52	$1.04 \cdot 10^{-3}$	0.52
EQZ	0.98	1.1	$1.04 \cdot 10^{-3}$	0.52	$1.04 \cdot 10^{-3}$	0.52
LTZ	$7.66 \cdot 10^{-4}$	$1.02 \cdot 10^{-2}$	0	$3 \cdot 10^{-3}$	0	$3 \cdot 10^{-3}$
Exp2-P1045	61.33	71.34	0.19	23.96	0.19	23.96
Log2-P2508	267.09	290.72	0.85	107.13	0.85	107.13
Exp	72.25	83.44	0.22	27.44	0.22	27.44
Ln	296.18	323.74	0.87	110.03	0.87	110.03
Sqrt	281.5	309.62	0.86	107.92	0.86	107.92
Sqrt-P0132	178.97	197.67	0.48	60.13	0.48	60.13
Ceil	1.58	1.8	$3.04 \cdot 10^{-3}$	0.77	$3.04 \cdot 10^{-3}$	0.77
Floor	$5.58 \cdot 10^{-4}$	$4.59 \cdot 10^{-3}$	0	$3 \cdot 10^{-3}$	0	$3 \cdot 10^{-3}$
Fx2Int	2.59	2.98	$5.42 \cdot 10^{-3}$	1.07	$5.42 \cdot 10^{-3}$	1.07
Fx2FL-	14.25	16.42	$4.34 \cdot 10^{-2}$	5.83	$4.34 \cdot 10^{-2}$	5.83

Table 1.7: Run-times in microseconds for fixed-point operations based on arithmetic gmw (128-bit) of two parties

Protocol	Preproc. (ms)	Total (ms)	Sent (ms)	Sent Msg	Rec (ms)	Rec Msg
Add	1.32	6.81	0	3	0	3
Sub	0.39	30.15	0	3	0	3
Mul	1,422.11	1,708.33	0.63	1,033	1.13	1,033
Div	9,563.34	12,512.17	6.25	7,567	11.37	7,567
DivConst	1,435.77	1,796.42	0.63	1,029	1.12	1,029
Lt	1,398.77	1,640.29	0.63	1,029	1.12	1,029
Gt	1,401.34	1,791.02	0.63	1,029	1.12	1,029
RoundTowardsZero	1,503.41	1,746.57	0.63	1,029	1.12	1,029
Neg	1,363.55	1,695.28	0.63	1,029	1.12	1,029
Abs	1,442.05	1,710.46	0.63	1,033	1.13	1,033
Eq	1,458.05	1,611.77	0.58	648	1.08	648
EQZ	1,552.83	1,760.49	0.58	648	1.08	648
LTZ	1,389.09	1,639.21	0.63	1,029	1.12	1,029
Exp2-P1045	27,619.78	35,074.88	19.24	21,388	34.77	21,388
Log2-P2508	18,039.19	22,726.13	12.11	13,693	22.19	13,693
Exp	28,943.22	36,807.57	19.83	22,027	35.86	22,027
Ln	19,579.9	24,555.33	12.7	14,332	23.28	14,332
Sqrt	10,912.64	14,019.12	6.92	8,227	12.62	8,227
Sqrt-P0132	13,245.26	16,865.14	9.09	10,235	16.2	10,235
Fx2FL	2,432.14	3,326.49	1.44	2,166	2.59	2,166

1.4 DP Mechanism

Table 1.8: Run-times in microseconds for DP mechanism based on boolean circuit (bgmw, 64-bit, SIMD = 1) of two parties

Protocol	Preproc. (ms)	Total (ms)	Sent (ms)	Sent Msg	Rec (ms)	Rec Msg
GeoSample	520.63	2,791.7	1.25	12,617	1.25	12,617
UniformFloat	390.9	2,574.19	1.26	12,705	1.26	12,705
SnappingMechanism	643.72	43,103.29	10.23	$1.04 \cdot 10^5$	10.23	$1.04 \cdot 10^5$

Table 1.9: Run-times in microseconds for DP mechanism based on boolean circuit amortized over 1000 SIMD (bgmw, 64-bit) of two parties

Protocol	Preproc. (ms)	Total (ms)	Sent (ms)	Sent Msg	Rec (ms)	Rec Msg
GeoSample	31.38	34.12	$9.74 \cdot 10^{-2}$	12.62	$9.74 \cdot 10^{-2}$	12.62
UniformFloat-0-1	29.72	32.34	$9.81 \cdot 10^{-2}$	12.71	$9.81 \cdot 10^{-2}$	12.71
SnappingMechanism	247.34	302.65	0.83	104.09	0.83	104.09