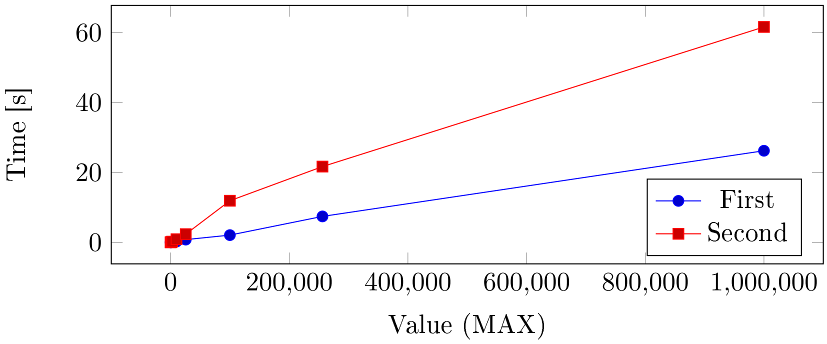
16-124-836
Marcel ZAUDER

4.2 Additively homomorphic ElGamal encryption

Value (MAX)	Time (First)	Time (Second)
100	0.00316	0.0082
256	0.0074	0.0146
1,000	0.02	0.0648
2,560	0.0586	0.2004
10,000	0.2158	0.8932
25,600	0.7774	2.338
100,000	2.0638	11.8982
256,000	7.4154	21.6686
1,000,000	26.1966	61.6154



As we can see for both bit lengths of P and Q the time increases linearly with the value of MAX. Also one can see that the difference between the first stage and second is pretty much equal to a tripling of the time needed. This is what we would expect because the length of P is doubled and $Q \approx 1.5$ times the first value. Therefore the execution time is also linearly dependent from those values.

4.2.BONUS Reduce the time of Decryption

One could make the code multithreaded, such that each thread takes one number from a "token generator" and runs the code with this number. After termination of one thread it gets another number/token from the "token generator" until one found the right value for max and the whole program terminates. The speedup of this code would be equivalent to how many threads one can run because every computational step for each number is independent from each other.