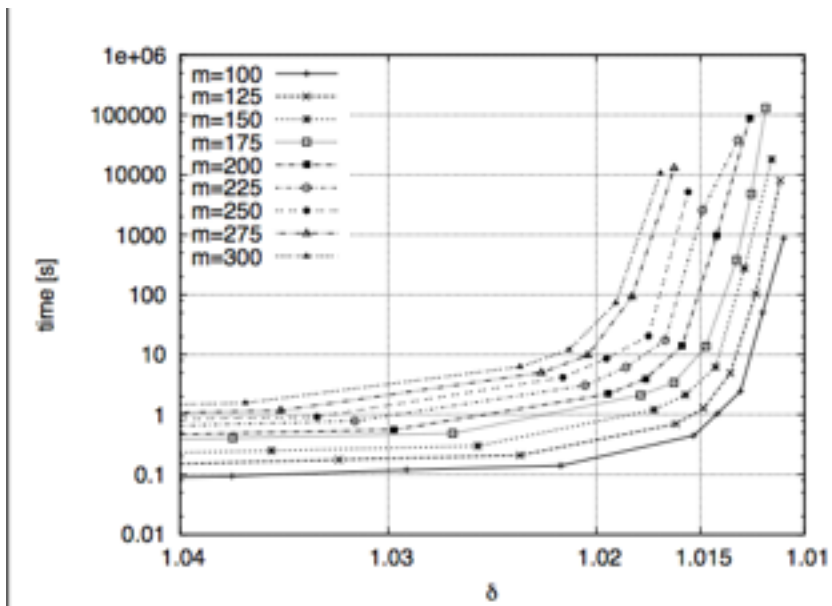
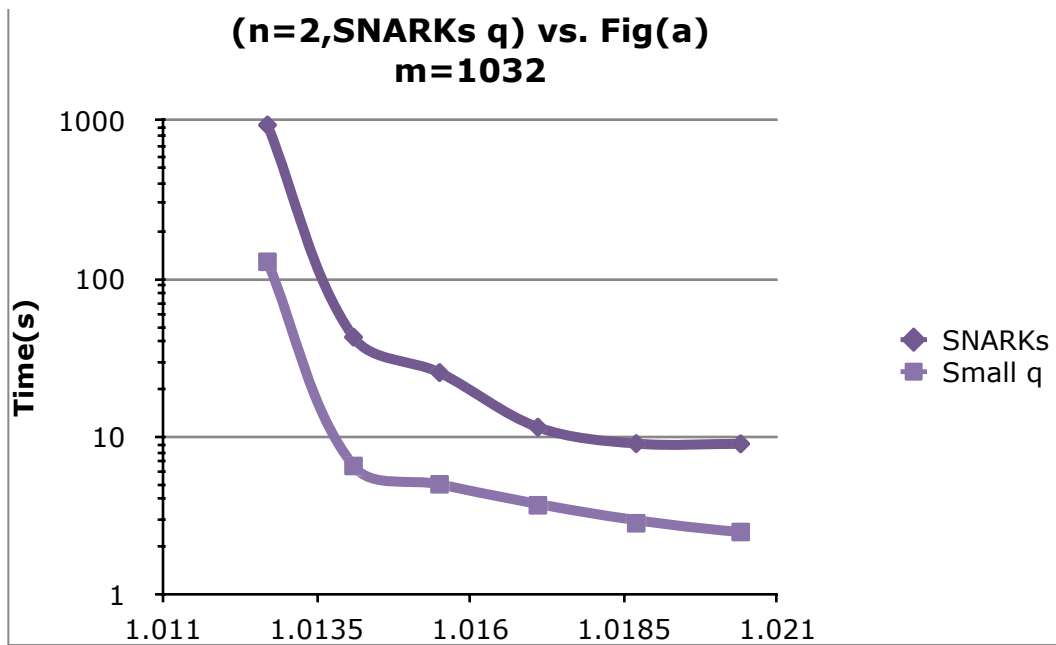


Fig(a) Logarithmic running time in seconds on Intel i7 3.4GHz using the same settings in Fig(b).



(b) Logarithmic running time in seconds for prime  $q \approx n^3$  and selected  $100 \leq m \leq 300$  and  $1.01 < \delta \leq 1.04$ .



delta

Fig(c) shows that because of numerical (big number) issue SNARKs need additional time to attack.