

The hidden subgroup problem is at present the keystone problem in quantum computation. We are given a function $f: G \rightarrow S$, with the property that f is constant on cosets of an unknown subgroup $H \leq G$, and distinct on distinct cosets. Here f is given as an oracle or as an efficient classical program, and S is an arbitrary set. The problem is to determine the hidden subgroup H . (A closely related problem, the "stabilizer problem", was formulated by Kitaev [6].) The difficulty of the task depends on the type of group G . The abelian case can be efficiently computed with a quantum computer by repetition of coset state preparation and Fourier sampling (the "standard method" developed by Simon [11] and Shor [10]). In particular this method is the heart of Shor's solution of the discrete logarithm and factoring problems.