Abstract

We show in some detail how to implement Shor's efficient quantum algorithm for discrete logarithms for a particular case of elliptic curve groups. It turns out that for this problem a smaller quantum computer can solve problems further beyond current computing than for integer factorisation. A 160 bit elliptic curve cryptographic key could be broken on a quantum computer using around 1000 qubits while factoring the security-wise equivalent 1024 bit RSA modulus would require about 2000 qubits. In this paper we only consider elliptic curves over GF(p) and not yet the equally important ones over GF(2^n) or other finite fields. The main technical difficulty is to implement Euclid's gcd algorithm to compute multiplicative inverses modulo p. As the runtime of Euclid's algorithm depends on the input, one difficulty encountered is the "quantum halting problem". On an (even) more theoretical note we also point out that there are quantum circuits which make the discrete logarithm algorithm exact.