Ralph's quantum discrete log

Ralph knows elliptic curve cryptography is based on the difficulty of computing discrete logarithms. Discrete log is the inverse of modular exponentiation. Both can be simply represented by

$$g^r \equiv x (\mathrm{mod}\, p) \tag{1}$$

Modular exponentiation involves finding x given g, r, and p which is easy. On the other hand, the discrete log involves finding r given g, x, and p which is believed to be difficult (otherwise elliptic curve cryptography fails — see Ralph's elliptic curve cryptography). Shor's quantum factoring algorithm (see Ralph's quantum factoring) can be adapted to solve the discrete log problem much faster with a quantum computer than via classical computation as is the case for factoring and breaking RSA cryptography.

A quantum algorithm for finding the discrete log r given g, x, and p follows.[1]

1. Create three registers where each register is t qubits, $p < q = 2^t < 2p$.

$$\frac{1}{(p-1)} \sum_{a,b=0}^{p-2} |a\rangle\, |b\rangle\, |0\rangle \tag{2}$$

2. Apply the function $f(a,b) = x^a g^{-b} (\mathrm{mod}\, p)$ to the third register where the modular inverse $g^{-b} (\mathrm{mod}\, p)$ is the value z such that $z g^b \equiv 1 (\mathrm{mod}\, p)$.

$$\frac{1}{(p-1)} \sum_{a,b=0}^{p-2} |a\rangle\, |b\rangle |x^a g^{-b}\rangle \tag{3}$$

3. Apply the quantum inverse Fourier transform to the first two registers.

$$\frac{1}{(p-1)^2} \sum_{a,b,c,d=0}^{p-2} \zeta^{ac} \zeta^{bd} |c\rangle\, |d\rangle |x^a g^{-b}\rangle \tag{4}$$

where $\zeta = \exp\left(\frac{2\pi i}{p-1}\right)$.

4. Measure the first two registers (with the third register implicitly measured). As usual the measurement probability is the square of the amplitude (since the amplitudes are complex numbers the square is the product of the amplitude and its complex conjugate). Most probabilities are zero so we observe one of a few realizations.

$$\left[\frac{1}{(p-1)^2} \sum_{a=0}^{p-2} \zeta^{\,ac+ard}\right] \left[\frac{1}{(p-1)^2} \sum_{a=0}^{p-2} \zeta^{\,-(ac+ard)}\right] \tag{5}$$

If $c + rd \equiv 0 (\mathrm{mod}\, p-1)$ then the probability simplifies as $\frac{1}{(p-1)^2}$.

[1] This is a shortened, composite version of Shor's algorithm and the algorithm described by Fang Xi Lin, "Shor's algorithm and quantum Fourier transform."

5. Recover r by computing $-d^{-1}c \equiv r \pmod{p-1}$. The algorithm fails if $c = 0$ or $d = 0$ or if d and $p-1$ are not relatively prime as the modular inverse doesn't exist. In this case, the algorithm is repeated.

Suggested:

Suppose $g = 5, x = 4, p = 7, q = 2^t = 2^3 = 8$ (this means the three quantum registers are $2^9 = 512$ element qubits).

1. Classically verify the order or discrete log is $r = 2$ and the period is 6.

2. Apply the quantum discrete log algorithm and verify $r = 2$.

Appendix.

Intuition for the recovery of the order by Shor's discrete log algorithm is discussed in this appendix by reference to the typical case.

Why does $-d^{-1}c \equiv r \bmod (p-1)$ where measurement of the first two registers produces the post-measurement state $|c\rangle |d\rangle$ identify r?

Prior to measurement but following the Fourier transformation the state is

$$\frac{1}{(p-1)^2} \sum_{a,b,c,d=0}^{p-2} \zeta^{ac} \zeta^{bd} |c\rangle |d\rangle |x^a g^{-b}\rangle$$

There are $(p-1)$ identical component states which combine to create identical component states $\frac{p-1}{(p-1)^2} \zeta^{ac+bd} |c\rangle |d\rangle \left|x^a b^{-b}\right\rangle$.

There are $(p-1)$ blocks of $(p-1)$-block length nonzero component states $|c\rangle |d\rangle |j\rangle, j = 1, \ldots, (p-1)$ (for a total of $(p-1)^2$ nonzero, equally likely potential post-measurement states when measuring the first two registers).

Measuring the first two registers produces post-measurement state $|c\rangle |d\rangle$.

Since each nonzero component state has probability $\frac{1}{(p-1)^2}$, each block has $\Pr(|c\rangle |d\rangle) = \frac{p-1}{(p-1)^2} = \frac{1}{p-1}$.

Recovery of the discrete log or order r is motivated by post-measurement state $|c\rangle |d\rangle |1\rangle$.

Since $g^r \equiv x \bmod p$, $xg^{-r} \equiv 1 \bmod p$ and $x^a g^{-ar} \equiv 1 \bmod p$. Hence, when $b = ar$ the third register is $|x^a g^{-ar}\rangle$ and the probability amplitudes are $\zeta^{ac+bd} = \zeta^{ac+ard} = \zeta^{a(c+rd)}$ where $\zeta = \exp\left[\frac{2\pi i}{p-1}\right]$.

Now, suppose $c + rd = n(p-1)$ then

$\zeta^{a(c+rd)} = \zeta^{an(p-1)} = \exp\left[\frac{2\pi i an(p-1)}{p-1}\right] = \exp[2\pi an] = \cos 2\pi = 1$.

Therefore, r is recoverable from $c + dr \equiv 0 \bmod (p-1)$ or $-d^{-1}c \equiv r \bmod (p-1)$ when d and $p-1$ are relatively prime and neither c or $d = 0$. Both failure conditions are increasingly unlikely as p becomes large and discovery of the discrete log becomes more challenging.