AGH University of Science and Technology

Selected Topics in Cryptography
Quantum cryptanalysis

Szymon Szozda

Department of Telecommunications

04.12.2017

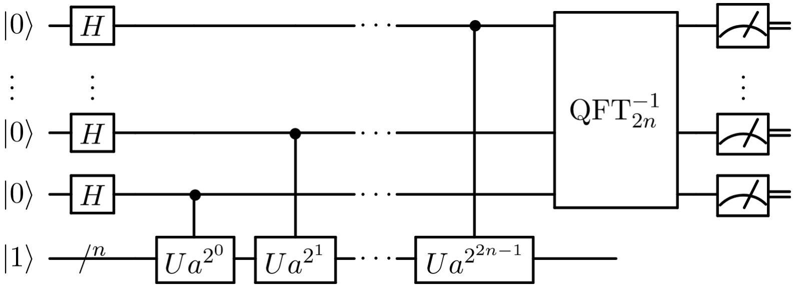
Shor

Overview

Pick a random number $a < N$.
Compute $gcd(a, N)$. This may be done using the Euclidean algorithm.
If $gcd(a, N) \neq 1$, then this number is a nontrivial factor of N, so we are done. Otherwise, use the period-finding subroutine (below) to find r, the period of the following function:
$f(x) = a^x \bmod N$

Shor

Scheme



$|0\rangle$
H
$|0\rangle$
H
$|0\rangle$
H
$|1\rangle$
n
Ua^{2^0}
Ua^{2^1}
$Ua^{2^{2n-1}}$
QFT_{2n}^{-1}

Fast exponentiation

We can calculate $A^B mod C$ quickly, using modular multiplication rules:

$$A^2 mod C = (A * A) mod C = ((A mod C) * (A mod C)) mod C$$

Quantum fourier transform

xyz

NNR

Overview

General Steps