Алгоритм Шора

1. Основные шаги

1) Выбрать случайный остаток a по модулю N.
2) Проверить НОД(a,N)=1
3) Найти порядок r остатка a по модулю N
4) Если r четен, вычислить НОД(ar2-1,N)

С большой вероятностью число, полученное на 4-м шаге, будет нетривиальным делителем числа N.

Трудность алгоритма заключается в нахождении порядка a по модулю N.

2) Разбор алгоритма

Пусть имеется некоторое число N.

Тогда с большой вероятностью (φ(N)N) случайно взятое число a будет взаимнопросто с числом N. При необходимости этот шаг повторяется несколько раз, пока не будет найдено требуемое число a.

С помощью квантового компьютера получаем: ar≡1 mod N.

Если r – нечетен возвращаемся к шагу выбора числа a.

Если r – четен можно записать:

ar22≡1 mod N

ar22-1≡0 mod N

ar2-1(ar2+1)≡0 mod N

ar2-1(ar2+1)≡c N

, где c – некоторая константа.

Т.к. r – порядок a по модулю N, то ar2-1≠0 mod N. Т.о. если a – ненулевой и не единичный элемент Z/NZ и r – четное, то НОД(ar2-1,N есть нетривиальный делитель N.

3) Реализация

Пусть n — число для факторизации, а q — некоторое число из промежутка [N2; 2N2) , являющееся степенью двойки, т.е. q = 2s для некоторого натурального s. Пусть также x — случайный элемент Z/NZ, порядок которого и будет определяться описываемым ниже алгоритмом.

Шаг 0: Привести все кубиты квантовых регистров в нулевое состояние:

ψ0 = |0>|0>.

Шаг 1: Применить гейт Адамара к каждому кубиту первого регистра:

ψ1 = 1q12r=0q-1|r>|0>.

Шаг 2: Вычислить значение xr (mod n) во втором регистре

ψ2 = 1q12r=0q-1|r>|ar (mod n)>.

Шаг 3: Выполнить квантовое преобразование Фурье на первом регистре. Тогда общее состояние запишется в виде.
ψ3 = 1qr=0q-1c=0q-1exp□(□□□ 2 /п)i >rcq|a┤ (mod n)>.

Шаг 4: Измерить состояние регистров квантового компьютера
|c>|ak (mod n)>
Где 0 ≤k<r