Специальные разделы криптологии

Савчук М.Н.

2 апреля 2015 г.

Глава 1

Алгоритм Шора для факторизации

1.1 Введение

Есть число N

$$N = a \cdot b, \qquad a \neq b$$

Задача факторизации: для числа $N = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$

- либо получить каноническую форму
- либо получить нетривиальный делитель

Число $a \in \mathbb{Z}_N$ **принадлежит показателю** δ, если δ — минимальное число, для которого $a^\delta \equiv 1 \mod n$. Обозначаем $\delta_N(a)$.

Показатель существует только если a и N взаимно просты ($a \in \mathbb{Z}_N$) и по сути является порядком a в группе $\mathbb{Z}_N : \delta_n(a) = ord_N(a)$. Если $gcd(a, N) \neq 1$, то мы нашли нетривиальный делитель.

Допустим, что для заданного $a \in \mathbb{Z}_N$ у нас есть оракул O_f, который возвращает показатель числа. Если этот оракул полиномиален, то можно факторизовать число (вероятностно)

Пусть r — чётное и $gcd\left(a^{r/2} + 1, N\right) = 1$, где $O_f(a) = r$

$$a^r \geq 1 \mod N$$
$$\left(a^{r/2} - 1\right) \cdot \left(a^{r/2} + 1\right) \equiv 0 \mod N$$

Но $a^{r/2} \neq 1 \mod N$, потому что иначе r — не минимальное число (нарушение определения показателя). Значит, $\left(a^{r/2} - 1\right)$ и N имеет нетривиальный общий делитель.

Важно: условие $gcd\left(a^{r/2} + 1, N\right) = 1$ можно заменить на условие $a^{r/2} + 1 \vdots N$.

Утверждение 1.1.1. *Пусть* $N = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ *и*

$$S = \left\{ a \in \mathbb{Z}_N : ord\,(a)\, mod 2 = 0 \vee a^{ord(a)/2} + 1 \vdots N \right\}$$

Тогда

$$|S| \leq \frac{\varphi\,(N)}{2^k}$$

То есть, подходящих нам a очень мало.

1.2 Алгоритм факторизации с оракулом

1. Генерируем такое a, чтобы при $r = O_f\,(a)$ выполняось

$$r = 2 \cdot r_1, a^{r_\alpha} + 1 \vdots N$$

2. $gcd\,(a^{r_1} - 1, N)$ — нетривиальный делитель.

Утверждение 1.2.1. *В классической модели найти оракул* O_f *не получилось. Шору удалось построить его в квантовой модели.*

Рассмотрим функцию $f : \mathbb{Z}_N \to \mathbb{Z}_N$

$$f\,(x) = a^x \mod N$$

Это почти непериодическая функция — её период не кратен N.

1.3 Квантовая система

У нас есть $|0\rangle$, $|1\rangle$; кубит находится в суперпозиции состояний $\lambda_1 \cdot |0\rangle + \lambda_2\,|1\rangle$, над которыми можно выполнять унитарные операции.

Набор кубитов — одна из возможных интерпретаций квантово-механической системы. Другой вариант — N-уровневая система, в которое есть N состояний $|0\rangle$, $|1\rangle$, $\ldots$, $|N-1\rangle$, и эти состояния ортонормированы (то есть, при измерении выпадают только эти состояния и ничего среднего между ними).

Глава 2

Задача о скрытой подгруппе

Оглавление