# Лекция 1. Односторонние функции

## 1 Введение

5 миров Импальяццо.

- Алгоритмика ($\mathbf{P} = \mathbf{NP}$).
- Эвристика ($\mathbf{P} \neq \mathbf{NP}$, но есть быстрый алгоритм в среднем).
- Pessiland ($\mathbf{P} \neq \mathbf{NP}$, нет ни быстрых алгоритмов, ни односторонней функции).
- Миникрипт (есть односторонние функции, но нет односторонних функций с секретом).
- Криптомания (есть односторонние функции с секретом).

В принципе, может статься еще что-то странное навроде $\mathbf{P} = \mathbf{NP}$, но на практике эти алгоритмы очень долгие или $\mathbf{P} \neq \mathbf{NP}$, но наоборот, есть какие-либо квазиполиномиальные быстрые алгоритмы.

Сначала будут обсуждаться примитивы, односторонние функции, доказательства с нулевым разглашением и прочее, потом на базе этого покажем, как построить криптографические протоколы.

Литература: конспект лекций Верещагина «Лекции по математической криптографии», черновик, Glodreich «Foundations of Cryptography», конспекты Goldwasser.

## 2 Односторонние функции

В криптографических задачах полиномиальность будет считаться от параметра безопасности $n$ (неформально, длина ключа) для доказательства надёжности, и от длины шифруемого сообщения при шифровании.

**Определение 1.** $\{f_n\}_{n=1}^{\infty}$ — семейство односторонних функций, если:

- $f$ регулярны по длине: $f_n : \{0,1\}^{k(n)} \to \{0,1\}^{l(n)}$.
- $f$ вычислимы за полиномиальное время.
- $f$ труднообратима (4 варианта: в сильном/слабом смысле, против равномерного/неравномерного обратителя).

Обратимость в слабом смысле: вероятность неудачи обратителя больше, чем некоторый обратный полином.

В сильном смысле: вероятность успеха асимптотически меньше, чем любой обратный полином.

Равномерный обратитель — полиномиальный вероятностный алгоритм.

Неравномерный обратитель — семейство схем полиномиального размера.

Задача обращения: по $f(x)$ найти $x' : f(x') = f(x)$.

Кванторная запись определения труднообратимой функции в сильном смысле: $\forall p(\cdot)\forall\{R_n\}_{n=1}^{\infty}\exists N : \forall n > N \to P_{x\sim U_k(n)}\{f(R(f(x))) = f(x)\} < \frac{1}{p(n)}$.

$R$ в определении пробегает по всем семействам схем или вероятностным обратителям в зависимости от вида обратителя. Определение в слабом смысле отличается первым квантором.

**Задача.** Может ли семейство $f_n : |\mathrm{Im} f_n| = poly(n) = s(n)$ быть труднообратимом в слабом смысле?

Неравномерный обратитель: можно «зашить» в схему по одному прообразу от каждого класса.

Равномерный: берёт случайный $x$, вычисляет $f(x)$, если $y = f(x)$, вернуть $x$. Можно подобрать такое число повторений $N$, чтобы вероятность ошибки была мала. Идея: классы бывают большие (размера $> 2^{l(n)} \cdot \varepsilon$), и маленькие. Вероятность неуспеха для больших классов не больше $(1-\varepsilon)^N$, а для маленького класса можно оценить единицей. Тогда общая вероятность ошибки для слуйчайного $x$ не больше $s(n) \cdot \varepsilon + (1-\varepsilon)^N$. Если $\varepsilon$ взять как $\frac{1}{2s(n)q(n)}$, а $N = \frac{n}{\varepsilon}$, то сумма будет не больше $\frac{1}{q(n)}$ для любого полинома $q(n)$.

**Задача.** $f$ — односторонняя функция. Верно ли, что $g(x) = f(x)f(x)$ тоже одностороняя? Верно ли, что $h(xy) = f(x)f(y)$ будет односторонней?

Если $g$ односторонняя, то $\exists R_g$, которая обращает $g$. Тогда $R_f(y) = R_g(yy)$ обращает $f$.

Если $R_h$ обращает $h$, то можно построить такой обратитель $f$: берём случайный $y$, считаем $f(y)$ и возвращаем первую часть $R_h(f(x)f(y))$, если всё нормально, иначе нужно повторить процедуру.

Хорошие значения $x$ - это те, для которых доля пар $(x, y)$ больше или равна $\varepsilon$. Остальных значений $x$ мало. Аналогичными предыдущей задаче рассуждениями можно получить оценку.