Лекция 1

Односторонние функции

(Конспект: К. Шмаков)

Часто в криптографии используется понятие односторонней функции. Одностороннюю функцию можно интуитивно представить себе как эффективно вычислимую функцию, обратную к которой никто (в том числе наш противник) не может вычислить эффективно.

1.1 Функции, односторонние в наихудшем случае

В качестве “первого приближения” рассмотрим вариант, когда обратная функция просто не вычислима на детерминированной машине Тьюринга за полиномиальное время.

Теорема 1.1. *Пусть* $\mathbf{P} \neq \mathbf{NP}$. *Тогда существует такая* $f \in \widetilde{\mathbf{P}}$ *(т.е. вычислимая на полиномиальной детерминированной машине Тьюринга), что* $f^{-1} \notin \widetilde{\mathbf{P}}$.

Доказательство. Действительно, пусть Φ — формула в КНФ, а A — набор значений переменных. Определим одностороннюю функцию:

$$f(\Phi, A) = \begin{cases} (\Phi, 1^{|A|}), & \text{if } \Phi[A] = \texttt{True}, \\ (\Phi, 0^{|A|}), & \text{otherwise}. \end{cases}$$

Если бы могли обратить эту функцию, мы могли бы найти выполняющий набор для любой выполнимой формулы, вычислив

$$f^{-1}(\Phi, 1^{\text{кол-во переменных}}).$$

Но мы знаем, что эта задача $\widetilde{\mathbf{NP}}$-полна. $\square$

Определение 1.1. Функция f называется *честной*, если у любой точки y её образа имеется прообраз, длина которого полиномиально (от длины y) ограничена.

В дальнейшем все рассматриваемые односторонние функции и прочие конструкции, основанные на них, — по существу, честные (даже если определения допускают иное).

Упражнение 1.1 ([1]). В условии теоремы "$\Rightarrow$" заменить на "$\Leftrightarrow$" в предположении, что f — честная.

К сожалению, построенная нами функция может быть легко обращена во многих точках. Поэтому понятие односторонней функции нуждается в корректировке.

1.2 Односторонние функции

Определение 1.2. Функция $f\colon \{0,1\}^* \to \{0,1\}^*$ называется *односторонней* (*one-way function, owf*), если

- f вычислима за полиномиальное время на ДМТ[2],
- $\forall$ВМТ[3] A
  $\forall k \in \mathbb{N}$
  $\exists N$
  $\forall n > N$
  $$\Pr\{A(f(x), 1^n) \in f^{-1}(f(x))\} < \frac{1}{n^k},$$
  где вероятность берётся по случайным числам, используемым A, и равномерному распределению по входным строкам $x \in \{0,1\}^n$.

Замечание 1.1. Заметим, что наличие 1^n у взломщика предоставляет ему возможность хотя бы пытаться взламывать нечестные функции. В каком случае A может самостоятельно вычислить n? Ясно, что это так, например, если длина $f(x)$ — инъективная функция от n.

Замечание 1.2. Иногда так определённые односторонние функции называют *сильно* односторонними функциями. Мы слово "сильно" будем опускать.

[1] Решено на семинаре.

[2] ДМТ — детерминированная машина Тьюринга

[3] ВМТ — вероятностная машина Тьюринга — (детерминированная) машина Тьюринга, использующая случайные числа.

Упражнение 1.2 ([4]). Что будет, если при вычислении f разрешить использовать случайные числа: изменится ли понятие, будет ли существование старых owf эквивалентно существованию новых owf?

Варианты: f может быть вычислима всегда правильно, но лишь за *ожидаемое* полиномиальное время (Las Vegas), либо же f может быть вычислима с константной ошибкой (Monte Carlo).

Упражнение 1.3. Что будет, если рассматривать лишь детерминированные A: как будут соотноситься понятия односторонних функций?

Упражнение 1.4. А если f или A, или оба будут последовательностью схем, то изменится ли что-то? А в предположениях упражнений 1.2 и 1.3?

Упражнение 1.5 ([5]). Что будет, если x будет распределено на $\{0,1\}^n$ не равномерно, а иначе (но вычислимо за полиномиальное время)?

1.3 Семейства односторонних функций

Много кому надо шифровать — значит, каждому нужна своя собственная односторонняя функция!

Определение 1.3. *Семейство односторонних функций* (*one-way function family, owff*) — это детерминированный полиномиальный по времени алгоритм G, который по входу, состоящему из 1^n и (случайной строки) r_g, генерирует e и s — две булевы схемы, задающие функции

- $e\colon \{0,1\}^n \to \{0,1\}^{\epsilon(n)}$ (encryptor — собственно односторонняя функция),
- $s\colon \{0,1\}^{\sigma(n)} \to \{0,1\}^n$ (sampler — по (случайной) строке r_s генерирует вход для функции e),

причём
$\forall$ВМТ A
$\forall k \in \mathbb{N}$
$\exists N$
$\forall n > N$

$$\Pr\{A(e(x), 1^n, e, s) \in f^{-1}(f(x))\} < \frac{1}{n^k},$$

[4]Решено на семинаре.
[5]Решено на семинаре.

где

$G(1^n, r_g) = (e, s)$,

$s(r_s) = x$,

вероятность берётся по случайным числам, используемым A, и по (равномерно распределённым) r_g и r_s.

Мотивация для наличия s следущая: e не обязана быть односторонней всюду; s выбрасывает из области определения e "простые" точки. Взломщик A получает s на входе, так как сама односторонняя функция должна быть целиком известна публике.

Упражнение 1.6 ([6]). А нужно ли передавать взломщику s?

Упражнение 1.7. Выполнить упражнения 1.1–1.5 для семейств.

Оказывается, что owf и owff существуют или не существуют одновременно.

Теорема 1.2. *$\exists f$ — односторонняя функция $\Leftrightarrow$ $\exists G$ — семейство односторонних функций.*

Доказательство. "$\Rightarrow$". Построим по f семейство следующим образом. Получая 1^n и r_g, про r_g забываем, а по n строим e как схему, которая отражает результат работы машины Тьюринга, вычисляющей f, на входе длины n (см. курс прошлого семестра). В качестве s возьмём тождественную функцию $s(x) = x$.

Если получившееся — не семейство односторонних функций, то существует его взломщик A. Но тогда имеется и взломщик A' для исходной owf f: чтобы вызвать A, нам (в дополнение к 1^n и собственно $f(x)$) требуется e (мы его только что построили по n) и s (тривиально строящееся по n). На вход A подаётся в точности $f(x)$ для равномерно распределённого $x \in \{0,1\}^n$, и результат требуется ровно тот же, что и требовался для owff.

"$\Leftarrow$". Построим f по G: f делит[7] свой вход на ν, r_g и r_s (в соответствии с "положенными" согласно G длинами для r_s и r_g на длине $n = |\nu|$) и и запускает $e(s(r_s))$ (где $G(1^n, r_g) = (e, s)$); итого,

$$f(\nu, r_g, r_s) = (e(s(r_s)), e, s).$$

Предположим, что получилась не односторонняя функция, т.е. f ломается на некоторое полиномиальной доле. Но тогда и исходное семейство можно взломать тем же самым взломщиком: строки r_g и r_s распределены, как и положено, равномерно, так как это части входа для f;

[6] Решено на семинаре.

[7] Проблема: а если не делится? Упражнение 1.8!

первые n битов на происходящее не влияют, и распределены они также равномерно; на вход взломщику подаётся привычное ему распределение $e(s(r_s))$ вместе с e и s. А доля будет по-прежнему полиномиальна, так как $n + |r_s(n)| + |r_g(n)|$ ограничено полиномом от n. □

Упражнение 1.8 ([8]). Что делать с тем, что в доказательстве теоремы входная строка для f может “не разделиться” на ν, r_g и r_s?

Замечание 1.3. В принципе можно определить односторонние функции как многопараметрические функции. Тогда можно было бы не “делить” одну строку на три, а спокойно расставить запятые между ν, r_g и r_s.

Упражнение 1.9. Что произойдёт, если ограничиться $e\colon \{0,1\}^n \to \{0,1\}^n$ или, наоборот, разрешить[9] $e\colon \{0,1\}^{p(n)} \to \{0,1\}^{p(n)}$?

Упражнение 1.10. Сравнить определение односторонней функции с определением из какой-нибудь книги[10] и понять, эквивалентны ли они.

1.4 Слабо односторонние функции

Можно ослабить определение односторонней функции.

Определение 1.4. Функция $f\colon \{0,1\}^* \to \{0,1\}^*$ — слабо односторонняя функция, если

- f вычислима за полиномиальное время на ДМТ,
- $\exists k \in \mathbb{N}$
  $\forall$ВМТ A
  $\exists N$
  $\forall n > N$
  $$\Pr\{A(f(x), 1^n) \in f^{-1}(f(x))\} < 1 - \frac{1}{n^k},$$
  где вероятность берётся по случайным числам, используемым A, и равномерному распределению по входным строкам $x \in \{0,1\}^n$.

Оказывается, что такое ослабление никак не влияет на существование односторонней функции.

Теорема 1.3. *$\exists f_w$ — слабо односторонняя функция $\Leftrightarrow$ $\exists f_s$ — сильно односторонняя функция.*

[8] Решено на семинаре.
[9] **NB:** в книге Голдрейха именно так.
[10] К примеру, Oded Goldreich, *Foundations of Cryptography.*

Доказательство. “$\Leftarrow$”. Тривиально.

“$\Rightarrow$”. Построим

$$f_s(x_1, x_2, \ldots, x_m) = (f_w(x_1), f_w(x_2), \ldots, f_w(x_m)),$$

где $m = m(n)$; полином $m(n)$ мы определим позже (с учётом k_w, определяющего “необратимую” долю $1/n^{k_w}$ для f_w).

Предположим, что существуют A_s и k_s, такие, что A_s обращает f_s хотя бы с вероятностью $1/n^{k_s}$. Построим A'_w, обращающий f_w на строке y, следующим образом: для каждого $1 \le j \le m$ он порождает $x_1, \ldots, x_m$ случайным образом и запускает

$$A_s(f_w(x_1), \ldots, f_w(x_{j-1}), y, f_w(x_{j+1}), \ldots, f_w(x_m)).$$

Если A_s хотя бы для одного значения j сработает успешно, то мы получим элемент $f^{-1}(y)$ (мы его легко распознаем, применив f).

Рассмотрим

$$S_n = \{x \in \{0,1\}^n |\ \Pr\{A'_w(f_w(x), 1^n) \in f_w^{-1}(f_w(x))\} > \frac{n}{a(n)}\},$$

где многочлен a мы определим позднее. Неформально говоря, S_n — *множество тех x, на которых A'_w достаточно успешен*; a priori понятно лишь, что он успешен в среднем по всем возможным x — на каких-то [конкретных] x сколько его не повторяй, успеха не добьёшься; а мы бы хотели повторениями увеличить вероятность успеха — повторённый многократно A'_w и будет нашим взломщиком A_w.

Вероятность успеха A'_w, повторённого $a(n)$ раз:

$$\Pr\{A_w(f_w(x), 1^n)\} \ge \Pr\{x \in S_n\} \times \Pr\{A_w(f_w(x), 1^n)|\ x \in S_n\}.$$

Правый сомножитель легко оценить: вероятность одной неудачи A'_w для такого x — это $1 - \frac{n}{a(n)}$, а после $a(n)$ повторений —

$$\left(\left(1 - \frac{1}{a(n)/n}\right)^{a(n)/n}\right)^n \sim \frac{1}{e^n}.$$

Покажем, что $\Pr\{x \in S_n\} \ge 1 - \frac{n}{m}$ — тогда, взяв достаточно быстро растущий многочлен m, мы сможем взломать f_w с вероятностью, большей любой наперёд заданной доли вида $1 - \frac{1}{n^{k_w}}$, что противоречит определению слабо односторонней функции.

Пусть, напротив, $\Pr\{x \in S_n\} < 1 - \frac{n}{m}$. Оценим вероятность успеха A_s сверху по формуле полной вероятности, разделив два случая: среди его m аргументов все оказались из S_n — или же не все?

В первом случае вероятность события — это $\left(\left(1-\frac{1}{m/n}\right)^{m/n}\right)^n \sim \frac{1}{e^n}$, и даже оценив (условную) вероятность успеха в этом случае единицей, мы получим экспоненциально маленькое слагаемое. Напротив, во втором случае мала вероятность успеха. Достаточно оценить эту вероятность при условии, что первый аргумент — не из S_n (слагаемое для всех аргументов будет разве что лишь в m раз больше).

Эта вероятность — не больше, чем вероятность успеха A'_w в этом случае, так как для $j = 1$ алгоритм A'_w с первым аргументом $f(x)$ как раз запустит A_s на этом $f(x)$. По определению множества S_n эта вероятность — не больше $\frac{n}{a(n)}$. Выбрав $a(n) = 2mn^{1+k_s}$, получим, что общая вероятность успеха A_s — не больше $\frac{nm}{a(n)} + \frac{1}{e^{\Omega(n)}}$. Это меньше, чем $1/n^{k_s}$ для больших n, т.е. противник A_s вовсе не обращает f_s с заявленной вероятностью. Противоречие. □

Замечание 1.4. Мы были вынуждены раздуть вход в полиномиальное число раз и, в частности, значительно увеличить N, с которого наша функция надёжна. Можно поступить гораздо экономнее (мы это изучим на семинаре).

Упражнение 1.11 ([11]). Можно ли перенести эту теорему на случай owff?

Упражнение 1.12 ([12]). f_s получилась определённой на довольно редком множестве. Как быть со входами длины, отличной не mn?

[11] Тривиальное.

[12] В общих чертах решено на семинаре.