Курс лекций по теоретической криптографии

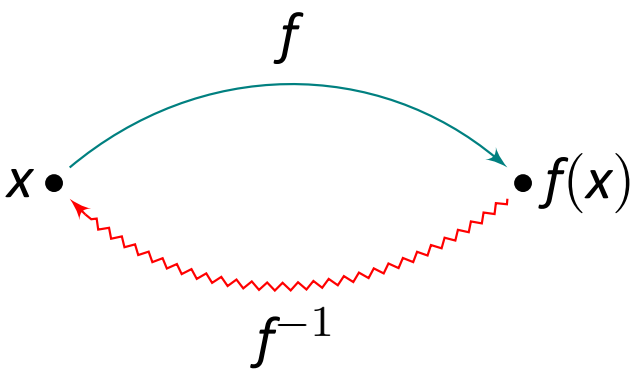
Тема 4. **Односторонняя функция и трудный предикат. Часть 1**

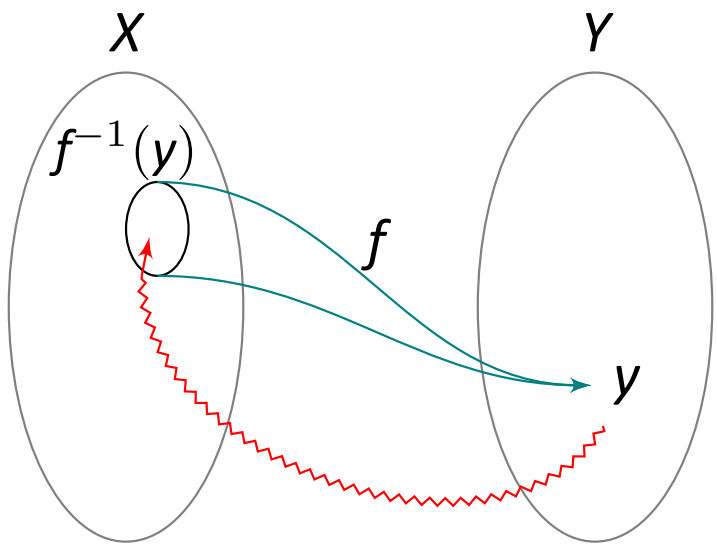
Шокуров А.В.

29.11.2022

Основная идея

Для стойкости многих основных типов криптографических протоколов необходимо и достаточно существования функций, которые «легко» вычислить, но «трудно (в среднем)» инвертировать, то есть находить для заданных значений функции отображаемые в них значения аргумента.





Соглашения об использовании некоторых терминов

Все дискретные объекты, с которыми работают алгоритмы, отождествляются с двоичными строками. Под длиной объекта понимаем длину соответствующей строки. В частности, если не оговорено противное, целые числа заданы своими двоичными записями наименьшей длины.

Полиномом будем называть произвольную функцию $p : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ такую, что $p(n) = cn^d$, где $c \in \mathbb{N} \setminus \{0\}$ и $d \in \mathbb{N}$.

Запись *poly* в неравенствах означает, что существует некоторый полином, существование которого подрзумевается. Запись *poly* в разных местах обозначает, вообще говоря, разные многочлены.

Соглашения об использовании некоторых терминов

Под словом алгоритм подразумевается машина Тьюринга. Оракулом в теории вычислений называется внешнее по отношению к алгоритмам устройство, которое в ответ на запрос произвольного алгоритма выдает значение функции на этом запросе. При этом как обращение к оракулу, так и получение ответа от него занимают один такт работы алгоритма. Ответ оракула может быть неоднозначным, а представлять собой значение некоторой случайной величины, зависящей от запроса как параметра. В этом случае оракул называется вероятностным.

Соглашения об использовании некоторых терминов

Уточним, как будем представлять вероятностный алгоритм. Будем называть алгоритм *A* вероятностным, если он имеет доступ к вероятностному оракулу *RB* (например, он бросает монетку), выдающему независимые случайные равномерно распределенные биты $b \in_U \{0, 1\}$. В этом случае при вычислении на входе *x* алгоритм *A* выдает значение некоторой случайной величины, обозначаемой через $A(x)$. Если алгоритм *A* не делает запросов к *RB*, то это детерминированный алгоритм. Для таких алгоритмов значение $A(x)$ определяется однозначно по *x*.

Соглашения об использовании некоторых терминов

Если число запросов к *RB* вероятностного алгоритма *A* на произвольном входе *x* не превосходит некоторого числа $\rho(x) \in \mathbb{N}$, то алгоритм *A* можно рассматривать как детерминированный с дополнительным входом $r \in_U \{0,1\}^{\rho(x)}$, где *x* — основной вход. А именно, алгоритм *A* использует бит $r_{[i]}$ вместо ответа оракула *RB* на *i*-й запрос к оракулу. В этом случае выход вероятностного алгоритма *A* будет обозначаться через $A(x, r)$

Предварительные определения и обозначения

Определение

Функция $\nu : \mathbb{N} \to \mathbb{R}^+$ называется *пренебрежимо малой* (*negligible*), если для любого полинома p существует такое $n_0 \in \mathbb{N}$, что $\nu(n) \leqslant \frac{1}{p(n)}$ для всех $n \geqslant n_0$.

Обозначение: $\mathrm{negl}(n)$, под полиномом $p(n)$ степени k понимаем $p(n) = \alpha n^k$, где $\alpha > 0$.

Определение

Функция $f : X \to Y$ ($X, Y \subseteq \mathbb{B}^*$) называется *полиномиально вычислимой*, если существуют полиномиальная (детерминированная) машина Тьюринга M, такая, что

$$\forall x \in X \;\; M(x) = f(x).$$

Обозначения:

- $\mathcal{U}$ — равномерное распределение вероятностей (*Uniform distribution*);
- $x \in_{\mathcal{U}} Z$ значит, что элемент x выбран случайно из (конечного) множества Z в соответствии с равномерным распределением вероятностей на этом множестве;
- $y \leftarrow M(x)$ значит, что y — (случайный) выход **в.** м. Т. M, на вход которой был подан x.

Пусть N — бесконечное подмножество $\mathbb{N}$, удовлетворяющее условию:
определить, входит ли произвольное натуральное i в N,
можно за полиномиальное от i время.

Определения односторонности

Определение

Функция $f : \bigcup\limits_{n \in N} \mathbb{B}^n \to \mathbb{B}^*$ называется *(сильно) односторонней* (*strongly one-way*), если

1. f полиномиально вычислима;
2. для любой п. в. м. Т. A
$$\Pr_{x \in_{\mathcal{U}} \mathbb{B}^n} \left[A\left(1^n, f(x)\right) \in f^{-1}\left(f(x)\right) \right] = \mathrm{negl}(n).$$

Определение

Функция $f : \bigcup\limits_{n \in N} \mathbb{B}^n \to \mathbb{B}^*$ называется *слабо односторонней* (*weakly one-way*), если

1. f полиномиально вычислима;
2. для некоторого полинома p, для любой п. в. м. Т. A найдётся такое $n_0 \in \mathbb{N}$, что для всех $N \ni n \geqslant n_0$ $\left(\exists p \, \forall A \, \exists n_0 \, \forall n \geqslant n_0 \right)$
$$\Pr_{x \in_{\mathcal{U}} \mathbb{B}^n} \left[A\left(1^n, f(x)\right) \in f^{-1}\left(f(x)\right) \right] \leqslant 1 - \frac{1}{p(n)}.$$

NB Можно не подавать 1^n на вход машине A, но тогда надо требовать, чтобы f была *честной* (*honest*) функцией: $\forall x \in X \ \ |x| \leqslant \mathrm{poly}(|f(x)|)$ (то есть не слишком сильно сжимала вход).

Полезные свойства

- Любую (сильно / слабо) одностороннюю функцию можно продолжить с $\bigcup_{n\in N}\mathbb{B}^n$ на всё $\mathbb{B}^*$, то есть определить всюду:
  - представим каждый $x \in \mathbb{B}^*$ в виде $x = x'x''$, где x' — префикс максимальной длины, на котором определена f: $|x'| \in N$, но $|x'|+1,\ \ldots,|x'|+|x''| \notin N$;
  - определим функцию g равенством $g(x) = f(x')$ по всем $x \in \mathbb{B}^*$;
  - g — всюду определённая (сильно / слабо)[1] односторонняя функция.

- Любую (сильно / слабо) одностороннюю функцию можно преобразовать так, чтобы она сохраняла длину аргумента:
  - выберем какой-нибудь полином $m(n) > n$, существующий в силу определения полиномиальной вычислимости функции f ($\forall x:\ |x| \in N\ \ |f(x)| < m(|x|)$);
  - определим функцию h на множестве $\bigcup\limits_{n\in N}\mathbb{B}^{m(n)}$, для чего представим каждый x из этого множества в виде $x = x'x''$, где $x' \in \mathbb{B}^n,\ x'' \in \mathbb{B}^{m(n)-n}$, и положим

$$h(x) = f(x')\,1\,0^{m(|x'|)-|f(x')|-1} \Longrightarrow |h(x)| = |f(x')| + m(|x'|) - |f(x')| = m(n);$$

  - h — (сильно / слабо) [1] односторонняя функция со свойством $|h(x)| = |x|$ для всех x из области определения этой функции ($\bigcup\limits_{n\in N}\mathbb{B}^{m(n)}$).

[1] Соответственно функции f.

Односторонние перестановки

Определение

Функция $f : \bigcup\limits_{n \in N} \mathbb{B}^n \to \mathbb{B}^*$ называется *перестановкой* (*permutation*), если f инъективна и сохраняет длину ($|f(x)| = |x|$), то есть для каждого $n \in N$ функция f задаёт взаимно однозначное отображение $\mathbb{B}^n$ на себя.

Определение

Перестановка $f : \bigcup\limits_{n \in N} \mathbb{B}^n \to \mathbb{B}^*$ называется *(сильно) односторонней*, если

1. f полиномиально вычислима;
2. для любой п. в. м. Т. A
$$\Pr_{x \in_{\mathcal{U}} \mathbb{B}^n}\left[A\left(f(x)\right) = x\right] = \mathrm{negl}(n).$$

Определение

Перестановка $f : \bigcup\limits_{n \in N} \mathbb{B}^n \to \mathbb{B}^*$ называется *слабо односторонней*, если

1. f полиномиально вычислима;
2. для некоторого полинома p, для любой п. в. м. Т. A найдётся такое $n_0 \in \mathbb{N}$, что для всех $N \ni n \geqslant n_0$
$$\Pr_{x \in_{\mathcal{U}} \mathbb{B}^n}\left[A\left(f(x)\right) = x\right] \leqslant 1 - \frac{1}{p(n)}.$$

Кандидаты в односторонние функции

Односторонняя функция — гипотетический объект (не доказано ни её существование, ни её невозможность).

Но есть примеры, удовлетворяющие определению при предположении о трудности тех или иных вычислительных задач.

- Произведение простых чисел:
  $f_{\Pi} : \{x', x''\} \mapsto x' \cdot x'', \quad x', x'' \in \mathbb{P}$
- Функции Рабина:
  $f_{\text{Rabin}} : x \mapsto x^2 \mod N$
- Функции RSA:
  $f_{\text{RSA}} : x \mapsto x^k \mod N$
- Сумма подмножества («рюкзачные» функции):
  $f_{\text{SubsetSum}} : x = x^{[1]} \ldots x^{[n]} \mapsto \sum_{i=1}^{n} x^{[i]} g_i$

Обозначения:
$x^{[i]}$ — i-й бит строки x,
$x^{[i \ldots j]}$ — подстрока в x, состоящая из битов начиная с i-го и заканчивая j-м

Один из наиболее популярных примеров — дискретную экспоненту (в предположении, что задача дискретного логарифмирования вычислительно трудна) — рассмотрим подробнее.

Дискретная экспонента

Пусть задано следующее:

- $p \in \mathbb{P} \cap \mathbb{B}^n$ — строка длины n, являющаяся бинарной записью простого числа;
- $G = \mathbb{Z}_p^* = \{1, 2, \ \ldots, p-1\}$ — группа с операцией умножения по модулю p;
- g — порождающий элемент циклической группы G, $\quad G = \langle g \rangle$.

Функция *дискретной экспоненты* (*discrete exponentiation*) определяется равенством

$$f_{DE}(p, g; x) = g^x \mod p,$$

где $x \in \mathbb{Z}_{p-1} = \{0, 1, \ \ldots, p-2\}$ (группа с операцией сложения по модулю $p-1$).

Дискретное логарифмирование (*discrete logarithm*) — инвертирование этой функции.

Соответствующая задача

$$p, g, g^x \mod p \mapsto x$$

считается вычислительно трудной.

Теорема о дискретной экспоненте

Теорема

Пусть A — п. в. м. Т., для которой найдётся такой полином q, что для любых p, g

$$\Pr_{x \in_U \mathbb{Z}_{p-1}} \left[A(p, g, f_{DE}(p, g; x)) = x \right] \geqslant \frac{1}{q(n)}$$

для бесконечного количества значений n.

Тогда существует п. в. м. Т. S^A, такая, что для любых p, g, x

$$\Pr \left[S^A(p, g, f_{DE}(p, g; x)) = x \right] \geqslant \frac{1}{2}.$$

Из предположения, что f_{DE} не односторонняя, следует,
что S^A решает предположительно трудную задачу её инвертирования.
Таким образом, если задача дискретного логарифмирования трудна,
то f_{DE} — односторонняя функция.

Это утверждение можно интерпретировать следующим образом:
либо дискретная экспонента *почти всюду* трудна для инвертирования,
либо она *всюду* инвертируется легко.

Доказательство теоремы

Доказательство. Определим действия машины S^A на входе (p, g, y), где $y \in G$:

Цикл до $q(n)$ раз:

1. $z_1 \in_U \mathbb{Z}_{p-1}$
2. $y_1 = y \cdot g^{z_1} \mod p$
3. $z_2 = A(p, g, y_1)$
4. если $g^{z_2} = y_1 \mod p$, то $S^A(p, g, y) = (z_2 - z_1) \mod (p-1)$;
   иначе переходим к 1.

Очевидно, машина S^A полиномиальна.

Оценим вероятность неудачи S^A в вычислении дискретного логарифма y:

- в одном цикле, поскольку y_1 — случайный элемент G, это вероятность неудачи A, которая по условию $\leqslant 1 - \frac{1}{q(n)}$;
- в $q(n)$ циклах получается $\leqslant (1 - \frac{1}{q(n)})^{q(n)} = e^{q(n)\ln(1-\frac{1}{q(n)})} \leqslant e^{-1} < \frac{1}{2}$.

В предпоследнем неравенстве использовано соотношение $\ln a \leqslant a - 1$. □

NB Фактически вычисление дискретного логарифма *произвольного фиксированного* элемента $y \in G$ сведено к вычислению дискретного логарифма *случайного* элемента $y_1 \in_U G$. Такое свойство задач называется *рандомизированной самосводимостью*.

Теорема Яо

Теорема

Если существует слабо односторонняя функция,
то существует и (сильно) односторонняя функция

Схема доказательства. Пусть f — некоторая слабо односторонняя функция и

$$g(x_1, \ldots, x_t) = \big(f(x_1), \ldots, f(x_t)\big).$$

- Предположим, что g — не односторонняя функция:
существует п. в. м. Т. B, которая с существенной[2] вероятностью инвертирует функцию g.
- Построим п. в. м. Т. A, которая, используя машину B, инвертирует функцию f:
A приписывает к своему входу y значения $f(x_i)$ на случайных аргументах x_i, так, чтобы получилось похоже на значение функции g, и подаёт это на вход машине B. Внутри выхода машины B мы ожидаем найти прообраз y относительно f. Проделывая это достаточное число раз, мы получим этот прообраз (то есть инвертируем f) с вероятностью, превышающей $1 - \frac{1}{p(n)}$ для любого заданного полинома p.
Это противоречит условию теоремы. □

? Докажите, что если $f : \mathbb{B}^* \to \mathbb{B}^*$ — слабо односторонняя функция, то функция $g : \mathbb{B}^* \to \mathbb{B}^*$, определённая так: $g(x'0) = x'0$, $g(x'1) = f(x')1$, — слабо односторонняя, но не односторонняя.

[2] То есть не пренебрежимо малой.

Доказательство теоремы Яо

Теорема

Если существует слабо односторонняя функция, то существует и (сильно) односторонняя функция

Доказательство. Пусть f — слабо односторонняя функция, w.l.o.g. сохраняющая длину, то есть $\forall n \in \mathbb{N}\ f(\mathbb{B}^n) \subseteq \mathbb{B}^n$.
Зафиксируем некоторый полином p из определения слабой односторонности: для **любой** п. в. м. Т. A и для всех достаточно больших n

$$\Pr_{x \in_{\mathcal{U}} \mathbb{B}^n}\left[\mathcal{A}_x\right] \leqslant 1 - \frac{1}{p(n)}.$$

$\mathcal{A}_x$ — обозначение для события $A\big(f(x)\big) \in f^{-1}\big(f(x)\big)$
(успешное инвертирование машиной A функции f на входе $f(x)$).

$$g(x_1, \ldots, x_t) = \big(f(x_1), \ldots, f(x_t)\big), \quad x_i \in \mathbb{B}^n, \ t = t(n) = n \cdot p(n).$$

Предположим, что g — не односторонняя функция:
существуют такие п. в. м. Т. B, полином q и бесконечное множество $N \subseteq \mathbb{N}$, что

$$\forall n \in N \qquad \Pr_{u \in_{\mathcal{U}} \mathbb{B}^{nt}}\left[\mathcal{B}_u\right] > \frac{1}{q(nt)}.$$

$\mathcal{B}_u$ — обозначение для события $B\big(g(u)\big) \in g^{-1}\big(g(u)\big)$
(успешное инвертирование машиной B функции g на входе $g(u)$).

Доказательство теоремы Яо

- Определим вероятностную машину A_0: на входе y
  для $i = 1, \ldots, t$
  1. $x_j \in_{\mathcal{U}} \mathbb{B}^n$ для каждого $j \in \{1, \ldots, i-1, i+1 \ldots, t\}$
  2. $z = B\big(f(x_1), \ldots, f(x_{i-1}), y, f(x_{i+1}), \ldots, f(x_t)\big)$
  3. если $z = (z_1, \ldots, z_t), z_k \in \mathbb{B}^n$, и $f(z_i) = y$, то $A_0(y) = z_i$ и A_0 останавливается.
- Определим вероятностную машину A: на входе y она k раз выполняет A_0 на этом входе, где $k = k(n) = 2n^2 p(n) q(n^2 p(n))$; если для некоторого i машина A_0 возвращает z_i, то $A(y) = z_i$, иначе A заканчивает работы без выходного значения.

Очевидно, A_0 и A — полиномиальные машины.

Введём обозначение $E_n = \{x \in \mathbb{B}^n \mid \Pr\big[A_0\big(f(x)\big) \in f^{-1}\big(f(x)\big)\big] > \frac{n}{k}\}$, $n \in \mathbb{N}$.

Лемма (1)

$$\forall n \in \mathbb{N}\ \forall x \in E_n \quad \Pr\big[\mathcal{A}_x\big] > 1 - \frac{1}{e^n}.$$

Лемма (2)

$$\exists n_0 \in \mathbb{N}\ \forall n \geqslant n_0 \quad \Pr_{x \in_{\mathcal{U}} \mathbb{B}^n}\big[x \in E_n\big] > 1 - \frac{1}{2p(n)}.$$

Доказательство теоремы Яо и леммы (1)

Утверждение теоремы следует из лемм (1) и (2):

$$\Pr_x\left[\mathcal{A}_x\right] \geqslant \Pr_x\left[\mathcal{A}_x \mid x \in E_n\right] \cdot \Pr_x\left[x \in E_n\right] > \left(1 - \frac{1}{e^n}\right)\left(1 - \frac{1}{2p(n)}\right),$$

что при достаточно больших n противоречит слабой односторонности функции f. □

Лемма (1)

$$\forall n \in \mathbb{N}\ \ \forall x \in E_n \quad \Pr\left[\mathcal{A}_x\right] > 1 - \frac{1}{e^n}.$$

Доказательство. Возьмём произвольные $n \in \mathbb{N}$ и $x \in E_n$.
По определению E_n и A, вероятность неудачи машины A

$$\Pr\left[\ \overline{\mathcal{A}_x}\ \right] < \left(1 - \frac{n}{k}\right)^k = e^{k \ln(1 - \frac{n}{k})} \leqslant e^{-n},$$

откуда получаем $\Pr\left[\mathcal{A}_x\right] > 1 - \frac{1}{e^n}$. □

Доказательство теоремы Яо и леммы (2)

Лемма (2)

$$\exists n_0 \in \mathbb{N}\ \ \forall n \geqslant n_0 \qquad \Pr_{x \in_{\mathcal{U}} \mathbb{B}^n}\left[x \in E_n\right] > 1 - \frac{1}{2p(n)}.$$

Доказательство. Будем рассуждать от противного:
пусть M — некоторое бесконечное подмножество в $\mathbb{N}$ и для всех $n \in M$

$$\Pr_{x}\left[x \in E_n\right] \leqslant 1 - \frac{1}{2p(n)}.$$

Возьмём $n \in M$. Пусть $x_i \in_{\mathcal{U}} \mathbb{B}^n,\ 1 \leqslant i \leqslant t, \quad u = (x_1, \ \ldots, x_t)$.
Оценим вероятности

$$s_1(n) = \Pr_{x_i}\left[\mathcal{B}_u,\ \exists i\ \ x_i \notin E_n\right],$$
$$s_2(n) = \Pr_{x_i}\left[\mathcal{B}_u,\ \forall i\ \ x_i \in E_n\right]$$

$$s_1(n) \leqslant \sum_{i=1}^{t} \Pr_{x_i}\left[\mathcal{B}_u,\ x_i \notin E_n\right] \leqslant \sum_{i=1}^{t} \Pr_{x_i}\left[\mathcal{B}_u \mid x_i \notin E_n\right] \leqslant$$

$$\leqslant \sum_{i=1}^{t} \Pr_{x_i}\left[A_0\left(f(x_i)\right) \in f^{-1}\left(f(x_i)\right) \mid x_i \notin E_n\right] \leqslant \frac{tn}{k}.$$

Доказательство теоремы Яо и леммы (2)

$$s_2(n) = \Pr_{x_i}\left[\mathcal{B}_u,\ \forall i\ \ x_i \in E_n\right] \leqslant \Pr_{x_i}\left[\forall i \in \{1,\ \ldots, t\}\ \ x_i \in E_n\right] = \prod_{i=1}^{t} \Pr_{x_i}\left[x_i \in E_n\right]$$

$$\leqslant \left(1 - \frac{1}{2p(n)}\right)^t = e^{t \ln\left(1 - \frac{1}{2p(n)}\right)} \leqslant e^{-\frac{t}{2p(n)}}.$$

Но по предположению о неодносторонности функции g

$$\frac{1}{q(nt)} < \Pr_u\left[\mathcal{B}_u\right] = s_1(n) + s_2(n) \leqslant \frac{tn}{k} + \frac{1}{e^{t/2p(n)}}.$$

Подставляя выражение $k(n) = 2n \cdot t(n) \cdot q(n \cdot t(n))$, получим

$\frac{1}{q} \leqslant \frac{1}{2q} + \frac{1}{e^{t/2p}}$, то есть $\frac{1}{e^{t/2p}} \geqslant \frac{1}{2q}$ для всех $n \in M$ — противоречие. □

? Докажите, что из условия существования слабо односторонней перестановки следует существование (сильно) односторонней перестановки.