Лекция 8

Шифрование с открытым ключом

(Конспект: Д. Соколов)

8.1 Семейство односторонних перестановок с секретом

В этом параграфе мы рассмотрим новый криптографический примитив — односторонние перестановки с секретом. Раньше под перестановкой мы понимали биективную функцию, сохраняющую длину. Но никаких примеров функций, которые могли бы быть односторонними перестановками в таком смысле нет. Поэтому мы дадим другое более реалистичное определение односторонних перестановок.

Определение 8.1. Распределения D и D' называются статистически неразличимыми, если последовательность $\sum\limits_{x\in\{0,1\}^n} |D_n(x) - D'_n(x)|$ — пренебрежимо мала.

Статистическая неразличимость распределений — это более сильное свойство, чем вычислительная неразличимость.

Лемма 8.1. *Если распределения D_n и D'_n статистически неразличимы, то они и вычислительно неразличимы.*

Доказательство. Пусть D_n и D'_n вычислительно различимы, тогда существует полином $p(n)$ и алгоритм A такой, что для бесконечного числа n выполняется
$\Pr_{x\leftarrow D_n}[A(x)=1] - \Pr_{y\leftarrow D'_n}[A(y)=1] \geq \frac{1}{p(n)}$
Преобразуем данное выражение:

$$\frac{1}{p(n)} \leq \sum_{x\in\{0,1\}^n} \Pr[A(x)=1]D_n(x) - \sum_{x\in\{0,1\}^n} \Pr[A(x)=1]D'_n(x)$$
$$= \sum_{x\in\{0,1\}^n} \Pr[A(x)=1](D_n(x) - D'_n(x)) \leq \sum_{x\in\{0,1\}^n} |D_n(x) - D'_n(x)|$$

□

Теперь мы можем определить односторонние перестановки.

Определение 8.2. Пусть $S_n \subseteq \{0,1\}^n$, функция $f : S_n \to S_n$ является биекцией. (Формально говоря, эта запись неудачная, поскольку функция определена на объединении $\bigcup_n S_n$, но мы будем так писать, чтобы не усложнять обозначения). Функция f называется односторонней перестановкой, если для любого полинома $p(n)$, для любого вероятностного полиномиального алгоритма A для всех достаточно больших n выполнено следующее соотношение: $\Pr_{x \leftarrow U(S_n)}[A(f(x)) = x] < \frac{1}{p(n)}$. При этом существует полиномиально моделируемое распределение D_n, которое статистически неразличимо от равномерного распределения на S_n.

Нетрудно проверить, что для так определенных односторонних перестановок тоже существует трудный бит и из них можно построить генератор псевдослучайных чисел. Мы приведем тут только определения и конструкции, доказательства утверждений полностью аналогичны тем, что были ранее.

По односторонней перестановке f можно построить перестановку g, которая будет определена только на строках длины $2n$, $g(xr) = f(x)r$, где $|x| = |r| = n$. Если f переставляет S_n, то g переставляет $S'_n = S_n \times \{0,1\}^n$. Нетрудно видеть, что из полиномиально моделируемого распределения, которое статистически неотличимо от равномерного распределения на S_n строится полиномиально моделируемое распределение, которое статистически не отличается от равномерного на S'_n. Для функции $B(xr) =< x, r >$ является трудным битом для функции g. Тут это надо понимать так: для любого вероятностного алгоритма A для любого полинома p для всех достаточно больших n выполняется $\Pr_{y \leftarrow U(S'(n))}[A(g(y)) = B(y)] < \frac{1}{2} + \frac{1}{p(n)}$. (Важно, что y берется только из S'_n)

Лемма 8.2. *Пусть $f : S_n \to S_n$ — односторонняя перестановка. $B : S_n \to \{0,1\}$ — трудный бит. Полиномиально моделируемое распредление D_n статистически неотличимо от $U(S_n)$. Тогда распределение, которое задает случайная величина $B(x)f(x)$, где $x \leftarrow D_n$ вычислительно неотличимо от распределения случайной величины by, где b равномерно распределен на $\{0,1\}$, а $y \leftarrow D_n$.*

Доказательство. Предположим, что это не так, тогда рассмотрим $b_0 f(x)$, где $b_0 \leftarrow U_1$. Либо $B(x)f(x)$ вычислительно отличимо от $b_0 f(x)$, либо $b_0 f(x)$ вычислительно отличимо от by. В первом случае получаем противоречие с тем, что $B(x)$ — трудный бит (доказательство см. в лекции 3), а во втором с тем, что $f(D_n)$ тоже статистически неотличимо от $U(S_n)$, а значит по лемме 8.1 и вычислительно неотличимо. □

Лемма 8.3. *Пусть $f : S_n \to S_n$ — односторонняя перестановка. $B : S_n \to \{0,1\}$ — трудный бит для f. Полиномиально моделируемое распределение D_n статистически неотличимо от $U(S_n)$. Тогда распределение случайной величины $B(x)B(f(x))\dots B(f^{p(n)-n}(x))f^{p(n)-n+1}(x)$, где $x \leftarrow D_n$ вычислительно неотличимо от распределения случайной величины $b_1 b_2 \dots b_{p(n)-n} y$, где $\forall i\ b_i \leftarrow U_1, y \leftarrow D_n$.*

Доказательство. Аналогично тому, что было в лекции 3. □

Аналогично опредедению семейства односторонних функций можно определить семейство односторонних перестановок.

Определение 8.3. Семейством односторонних перестановок называется полиномиальный вероятностный алгоритм $G : 1^n \mapsto (s, e)$, где s, e — булевы схемы.

$s : \{0,1\}^{\epsilon(n)} \to \{0,1\}^n$ — генератор "трудных" входов ($\epsilon(n)$ — некоторый полином). $e : \{0,1\}^n \to \{0,1\}^n$ — перестановка на $s(\{0,1\}^{\epsilon(n)})$.

И выполняются следующие условия:

- Для любого полинома $p(n)$ для любого вероятностного полиномиального алгоритма A для всех достаточно больших n $\Pr_{x \leftarrow U(\{0,1\}^{\epsilon(n)})}[A(e(s(x))) = s(x)] < \frac{1}{p(n)}$, где вероятность также берется по случайным битам алгоритма G
- $s(U_{\epsilon(n)})$ статистически неотличимо от $U_{s(\{0,1\}^{\epsilon(n)})}$

Упражнение 8.1. Будет ли существование семейства односторонних перестановок эквивалентно существованию одной односторонней перестановки?

Теперь можно определить основное понятие этого раздела —- семейства односторонних перестановок с секретом.

Аналогично определяется семейство односторонних перестановок с секретом. Вместе с односторонней перестановкой генератор будет генерировать секрет, дополнительную информацию с помощью которой перестановку можно эффективно обратить.

Определение 8.4. Семейством односторонних перестановок с секретом называется полиномиальный вероятностный алгоритм $G : 1^n \mapsto (s, e, d)$, где s, e, d — булевы схемы.

$s : \{0,1\}^{\epsilon(n)} \to \{0,1\}^n$ — генератор "трудных" входов ($\epsilon(n)$ — некоторый полином). $e : \{0,1\}^n \to \{0,1\}^n$ — перестановка на $s(\{0,1\}^{\epsilon(n)})$. $d : \{0,1\}^n \to \{0,1\}^n$ — секрет, схема, которая обращает схему e.

И выполняются следующие условия:

- Для любого полинома $p(n)$ для любого вероятностного полиномиального алгоритма A для всех достаточно больших n $\Pr_{x \leftarrow U(\{0,1\}^{\epsilon(n)})}[A(e(s(x))) = s(x)] < \frac{1}{p(n)}$, где вероятность также берется по случайным битам алгоритма G
- $s(U_{\epsilon(n)})$ статистически неотличимо от $U_{s(\{0,1\}^{\epsilon(n)})}$
- Для любого $x \in s(\{0,1\}^{\epsilon(n)})$ выполняется $d(e(x))) = x$.

Приведем два примера перестановок с секретом. Секрет в этих примерах будет не схемой, которая эти перестановки обращает, а просто дополнительной информацией, которой хватит, чтобы эти перестановки обратить.

Пример 8.1. Функция Рабина. Генератор G генерирует два n битных простых числа p и q вида $4k + 3$. Функция рабина является перестановкой множества квадратичных вычетов по модулю pq. Генерировать равномерное распределение на множестве S_{pq} квадратичных вычетов просто: сгенерировать некоторое число от 0 до $pq - 1$ и возвести его в квадрат по модулю pq. Сама функция действует так: $f(x) = x^2 \bmod pq$. Нетрудно понять, что f переставляет множество S_{pq}. В качетстве упражнения покажите, что зная числа p и q, обратить f просто.

Пример 8.2. Функция RSA. Генератор G генерирует два n битных простых числа p и q. Функция RSA будет перестановкой на множестве чисел от 1 до $pq-1$, которые взаимно просты с pq. $f(x) = x^d \bmod pq$, где d также является частью открытого ключа. Секретом является разложение pq на множители. Зная p и q, можно найти e, что $ed-1$ делится на $\varphi(pq) = (p-1)(q-1)$, тогда $f(x)^e = x \bmod pq$.

8.2 Шифрование с открытым ключом

Определение 8.5. Протоколом с открытым ключом называется тройка вероятностных полиномиальных алгоритмов G, E, D.

$G : 1^n \mapsto (e_n, d_n)$ — генератор ключей, e_n — публичный ключ, он известен всем и используется для шифрования сообщений.

$E : (1^n, e_n, x) \mapsto m_n$ — шифратор, который с помощью публичного ключа и сообщения x получает зашифрованное сообщение m_n.

$D : (1^n, e_n, d_n, m_n) \mapsto x$ — дешифратор, который по зашифрованному сообщению и секретному ключу восстанавливает сообщение.

При этом выполнены следующие условия:

- $D(1^n, e_n, d_n, E(1^n, e_n, x)) = x$
- Для любого полинома $p(n)$, для любой последовательности сообщений α_n, β_n длины $p(n)$ случайные величины $E(1^n, e_n, \alpha_n)$ и $E(1^n, e_n, \beta_n)$ вычислительно неразличимы.

Теорема 8.1. *Если существует семейство односторонних перестановок с секретом, то существует протокол шифрования с открытым ключом для кодирования однобитовых сообщений.*

Доказательство. Пусть G — генератор для семейства односторонних перестановок с секретом.

$G : 1^n \mapsto (s, f, d)$, где d — секретный ключ. В нашей конструкции протокола d будет секретным ключом, а f и s будет частью открытого ключа. f — перестановка множества $s(\{0,1\}^n)$. Тогда для f можно построить трудный бит B_f.[1]

Частью открытого ключа также будет случайная строка $r \leftarrow U_{\epsilon(n)}$.

Определим шифратор и дешифратор: $E(s, f, r, x) = (B_f(s(r)) \oplus x) f(s(r))$, где x — это сообщение из одного бита.

$D(s, f, r, d, by) = b \oplus B_f(d(y))$, где b — это один бит.

Проверим выполнение свойств:

- $D(s, f, r, d, E(f, x)) = (B_f(s(r)) \oplus x) \oplus B_f(d(f(s(r)))) = B_f(s(r)) \oplus x \oplus B_f(s(r)) = x$

[1] B_f будет трудным битом немного в другом смысле, чем мы понимали раньше, вероятность надо будет рассматривать в том числе и по случайным битам генератора G. Формально существование трудного бита для семейства односторонних перестановок с секретом надо доказавать, но реально доказательство дословно повторяет то доказательство, которое у нас уже встречалось в лекции 2.

- Пусть коды нуля и единицы вычислительно различимы, тогда любо код нуля, либо код единицы можно отличить от распределения $yf(s(r))$, где $y \leftarrow U_1$. Если код нуля можно отличить от этого распределения, то $B_f(s(r))f(s(r))$ отличается от $yf(s(r))$, что противоречит лемме 8.2. Если код единицы можно отличить от $yf(s(r))$, то код нуля тоже (инвертируем первый бит и отличим).

□

Замечание 8.1. Коды нуля и единицы — это два непересекающихся **NP** множества, вычислительно неразличимых. Это значит, что из существания протокола с открытым ключом для кодирования сообщений из одного бита следует, что существует пара дизъюнктных **NP** множеств, которые не разделимы полиномиальным алгоритмом.

Теорема 8.2. *Если существует протокол с открытым ключом для сообщений из 1 бита, то существует протокол с открытым ключом для сообщений произвольной полиномиальной длины.*

Доказательство. Достаточно каждый бит сообщения зашифровать с помощью протокола шифрования одного бита. Детали остаются в качестве упражнения. □