Решения задач прошлых виртуальных занятий

М. И. Анохин

30 мая 2020 г.

Виртуальное занятие 25 мая 2020 г. (последнее)

1. Доказать, что если для языка L существует протокол интерактивного доказательства с границей полноты, отличной от 0 для всех n, в котором проверяющий никогда не принимает доказательства для строк не из L, то $L \in \mathrm{NP}$. См. также [Gol, Volume 1, Subsection 4.12.4, Exercise 5] (там есть указание к решению).

Решение. Пусть (P, V) — такой протокол интерактивного доказательства для L. Пусть также $x \in \{0,1\}^*$. Если $x \in L$, то существует значение случайной величины $\mathrm{view}_V^P(x)$ (разумеется, представимое двоичной строкой полиномиальной длины от $|x|$), при котором V принимает доказательство для x. Напомним, что $\mathrm{view}_V^P(x)$ состоит из случайной строки алгоритма V и последовательности сообщений (в хронологическом порядке), полученных этим алгоритмом в процессе совместного вычисления P и V на общем входе x. Выходное значение алгоритма V при этом вычислении детерминированно зависит от $\mathrm{view}_V^P(x)$ и может быть вычислено за полиномиальное от $|x|$ время. Если же $x \notin L$, то V никогда не принимает доказательство для x. Это показывает, что $L \in \mathrm{NP}$ (в качестве NP-доказательства (witness) используется вышеуказанное значение случайной величины $\mathrm{view}_V^P(x)$).

2. Доказать, что если для языка L существует однораундовый протокол интерактивного доказательства (в котором пересылается лишь одно сообщение от доказывающего к проверяющему) с границами полноты и корректности $2/3$ и $1/3$ соответственно и с вычислительно нулевым разглашением, то $L \in \mathrm{BPP}$.

Решение. Пусть (P, V) — такой протокол интерактивного доказательства для L. Рассмотрим совместное вычисление P и V на общем входе $x \in \{0,1\}^*$. В процессе этого вычисления P посылает V единственное сообщение, обозначаемое нами через $P(x)$ (которое мы считаем двоичной строкой), после чего V должен возвратить свое выходное значение. Это выходное значение мы обозначим через $V(x, w)$, где w — сообщение полученное алгоритмом V. Разумеется, как $P(x)$, так и $V(x, w)$ являются случайными величинами. Таким образом, $\mathrm{view}_V^P(x) = (\widetilde{r}_x, P(x))$, где $\widetilde{r}_x$ — случайная строка алгоритма V, используемая при вычислении на входе x. По условию вычислительно нулевого разглашения существует полиномиальный вероятностный алгоритм S (симулятор) такой, что семейства случайных величин $(\mathrm{view}_V^P(x) \mid x \in L)$ и $(S(x) \mid x \in L)$ вычислительно неотличимы. Не ограничивая общности, считаем, что $\operatorname{supp} S(x) \subseteq \{0,1\}^* \times \{0,1\}^*$ для всех $x \in \{0,1\}^*$. Действительно, пусть $f(u) = u$, если $u \in \{0,1\}^* \times \{0,1\}^*$, и $f(u)$ — произвольная фиксированная пара двоичных строк в противном случае. Тогда функция f полиномиально вычислима, $f(u) \in \{0,1\}^* \times \{0,1\}^*$ для любого u и f оставляет на месте все значения случайной величины $\mathrm{view}_V^P(x)$. Поэтому алгоритм, полученный из S применением к выходу функции f, будет симулятором для взаимодействия V с P, всегда возвращающим пары двоичных строк. (Напомним, что применение полиномиально вычислимой функции сохраняет вычислительную неотличимость семейств случайных величин.)

Обозначим через $T(x)$ второй элемент пары $S(x)$ ($x \in \{0,1\}^*$). Тогда семейства случайных величин $(P(x) \mid x \in L)$ и $(T(x) \mid x \in L)$ вычислительно неотличимы. Идея решения состоит в замене строки $P(x)$ (вообще говоря, не генерируемой по x за полиномиальное время) на симулированную строку $T(x)$ (которую можно сгенерировать по x за полиномиальное время). Очевидно, что $V(x, T(x))$ может быть сгенерировано по x за полиномиальное время. Пусть сначала $x \in L$. Тогда $|\Pr[V(x, P(x)) = 1] - \Pr[V(x, T(x)) = 1]| \leqslant \mathrm{negl}(|x|)$, где $\Pr[V(x, P(x)) = 1] \geqslant 2/3$ ввиду условия полноты протокола. Следовательно, $\Pr[V(x, T(x)) = 1] \geqslant 2/3 - \mathrm{negl}(|x|)$. Если же $x \in \{0,1\}^* \setminus L$, то $\Pr[V(x, T(x)) = 1] \leqslant 1/3$ ввиду условия корректности протокола. Таким образом, $L \in \mathrm{BPP}$.

Виртуальное занятие 18 мая 2020 г. (предпоследнее)

1. (Для разминки.) Пусть существует протокол электронной подписи, стойкий против экзистенциальной подделки на основе адаптивной атаки с выбором сообщений. Доказать, что существует протокол электронной подписи (с теми же пространствами сообщений), удовлетворяющий тому же условию стойкости и такой, что по произвольной допустимой подписи для сообщения m (относительно некоторого открытого ключа) можно эффективно вычислить это сообщение m. См. также [Gol, Volume 2, Subsection 6.6.7, Exercise 4].

Решение. Пусть (G, S, V) — протокол электронной подписи, стойкий против экзистенциальной подделки на основе адаптивной атаки с выбором сообщений. Выберем полиномиальный вероятностный алгоритм S' который на произвольном входе вида $(1^n, s, m)$ возвращает (m, w), где $\mathrm{w} \leftarrow S(1^n, s, m)$. Пусть также полиномиальный детерминированный алгоритм V' принимает u в качестве подписи для сообщения m при открытом ключе v (т. е. $V'(1^n, v, m, u) = 1$), если и только если $u = (m, w)$ и $V(1^n, v, m, w) = 1$. Тогда очевидно, что (G, S', V') — протокол электронной подписи с тем же семейством пространств сообщений, что и (G, S, V), причем по произвольной допустимой в (G, S', V') подписи для сообщения m (относительно некоторого открытого ключа) можно эффективно вычислить m. Осталось доказать стойкость (G, S', V') против экзистенциальной подделки на основе адаптивной атаки с выбором сообщений. Пусть $(\mathrm{s}, \mathrm{v}) \leftarrow G(1^n)$ и A — произвольный полиномиально ограниченный противник, осуществляющий экзистенциальную подделку на основе адаптивной атаки с выбором сообщений для (G, S', V') (имеющий доступ к оракулу $S'(1^n, \mathrm{s}, \cdot)$). Построим полиномиально ограниченного противника B, осуществляющего экзистенциальную подделку на основе адаптивной атаки с выбором сообщений для (G, S, V) (имеющего доступ к оракулу $S(1^n, \mathrm{s}, \cdot)$), следующим образом. Противник B не входе $(1^n, \mathrm{v})$ запускает противника A (т. е. соответствующий алгоритм) на том же входе. Если A делает запрос q к оракулу $S'(1^n, \mathrm{s}, \cdot)$ в процессе осуществления адаптивной атаки с выбором сообщений, то B передает этот запрос оракулу $S(1^n, \mathrm{s}, \cdot)$, получает $\mathrm{y} \leftarrow S(1^n, \mathrm{s}, q)$ и передает A в качестве ответа на запрос пару (q, y). Пусть теперь A нашел пару (m, u), где m — сообщение (отличное от сообщений, которые A выбрал в качестве запросов к оракулу $S'(1^n, \mathrm{s}, \cdot)$ при осуществлении атаки), а u — допустимая в (G, S', V') подпись для m относительно открытого ключа v (т. е. $u = (m, w)$ и $V(1^n, \mathrm{v}, m, w) = 1$). Тогда B возвращает (m, w), где w — допустимая в (G, S, V) подпись для m относительно открытого ключа v. В противном случае B возвращает сообщение об ошибке. Очевидно, что вероятность успеха противника A равна вероятности успеха противника B, которая пренебрежимо мала как функция от n.

2. Пусть $(I_n \mid n \in \mathbb{N})$ — семейство непустых попарно непересекающихся подмножеств $\{0,1\}^*$ и $I = \bigcup_{n\in\mathbb{N}} I_n$. Пусть также функция $\nu\colon I \to \mathbb{N}$ ставит в соответствие каждому $i \in I$ единственное число $n \in \mathbb{N}$ такое, что $i \in I_n$. Мы предполагаем, что функция $i \mapsto 1^{\nu(i)}$ $(i \in I)$ полиномиально вычислима. Предположим также, что каждого $n \in \mathbb{N}$ заданы множества $X_n, M_n \subseteq \{0,1\}^{\leqslant \mathrm{poly}(n)}$ и распределения вероятностей $\mathcal{G}_n$ и $\mathcal{X}_n$ на множествах $I_n \times \{0,1\}^*$ и X_n соответственно, причем условие $w \in X_n$ может быть проверено по $(1^n, w)$ за полиномиальное время и семейства распределений вероятностей $(\mathcal{G}_n \mid n \in \mathbb{N})$ и $(\mathcal{X}_n \mid n \in \mathbb{N})$ полиномиально конструируемы, когда индексы заданы в унарной записи. Пусть теперь $(f_i\colon X_{\nu(i)} \to M_{\nu(i)} \mid i \in I)$ — семейство сюръективных функций с секретом относительно семейств распределений вероятностей $(\mathcal{G}_n \mid n \in \mathbb{N})$ и $(\mathcal{X}_{\nu(i)} \mid i \in I)$. Рассмотрим протокол электронной подписи (G, S, V) с семейством пространств сообщений $(M_n \mid n \in \mathbb{N})$, в котором

- G на входе 1^n $(n \in \mathbb{N})$ выбирает $(\mathrm{i}, \mathrm{t}) \leftarrow \mathcal{G}_n$ и возвращает $((\mathrm{i}, \mathrm{t}), \mathrm{i})$ (т. е. (i, t) — секретный ключ, а i — открытый ключ);
- S на входе $(1^n, (i, t), m)$, где $n \in \mathbb{N}$, $(i, t) \in \operatorname{supp} \mathcal{G}_n$ и $m \in M_n$, возвращает некоторый элемент $f_i^{-1}(m)$ (вычисляемый с помощью алгоритма инвертирования из п. 2 определения 12.1 конспекта лекций);
- $V(1^n, i, m, w) = 1$ (т. е. w принимается в качестве подписи для сообщения $m \in M_n$ при открытом ключе $i \in I_n$, где $n \in \mathbb{N}$), если и только если $w \in X_n$ и $f_i(w) = m$.

Сформулировать условие стойкости протокола электронной подписи (G, S, V), вытекающее из односторонности семейства $(f_i \mid i \in I)$.

Решение. Этот протокол является стойким против угрозы нахождения допустимой подписи для случайного сообщения $f_{\widetilde{i}}(\widetilde{x})$ (где $(\widetilde{i}, \widetilde{t}) \leftarrow \mathcal{G}_n$ и $\widetilde{x} \leftarrow \mathcal{X}_n$) на основе атаки с открытым ключом.

Виртуальное занятие 27 апреля 2020 г.

1. (См. начало раздела 2 конспекта лекций, где даны все необходимые определения.) Пусть N — полиномиально перечислимое множество целых неотрицательных чисел и $f\colon \bigcup_{n\in N}\{0,1\}^n \to \{0,1\}^*$. Доказать, что

- если функция f является односторонней в смысле определения 2.2 конспекта лекций, то она также является односторонней в смысле определения 2.1 конспекта лекций;
- если функция f является односторонней в смысле определения 2.1 конспекта лекций, то функция $x \mapsto 1^n 0 f(x)$ ($n \in N$, $x \in \{0,1\}^n$) является односторонней в смысле определения 2.2 конспекта лекций.

Решение. Предположим сначала, что f является односторонней в смысле определения 2.2. Выберем полином p такой, что $|x| \leqslant p(|f(x)|)$ для всех $x \in \bigcup_{n\in N}\{0,1\}^n$. Пусть A — полиномиальный вероятностный алгоритм (пытающийся инвертировать f в смысле определения 2.1). Определим полиномиальный вероятностный алгоритм B (пытающийся инвертировать f в смысле определения 2.2), который на произвольном входе $y \in \{0,1\}^*$ вычисляет $\mathrm{x}_i \leftarrow A(1^i, y)$ для каждого $i \in \{0,\ldots,p(|y|)\}$. Если $f(\mathrm{x}_i) = y$ для некоторого такого i, то алгоритм B возвращает x_i и заканчивает работу. Легко видеть, что

$$\Pr[A(1^n, f(\widetilde{u}_n)) \in f^{-1}(f(\widetilde{u}_n))] \leqslant \Pr[B(f(\widetilde{u}_n)) \in f^{-1}(f(\widetilde{u}_n))] = \mathrm{negl}(n),$$

так как если $y \in \operatorname{supp} f(\widetilde{u}_n)$, то $0 \leqslant n \leqslant p(|y|)$ ($n \in N$). Альтернативный вариант алгоритма B на произвольном входе $y \in \{0,1\}^*$ выбирает $\mathrm{i} \leftarrow \mathcal{U}(\{0,\ldots,p(|y|)\})$, вычисляет $A(1^{\mathrm{i}}, y)$ и возвращает полученное выходное значение. Тогда если $\widetilde{i} \leftarrow \mathcal{U}(\{0,\ldots,p(|f(\widetilde{u}_n)|)\})$, то

$$\begin{aligned}\Pr[A(1^n, f(\widetilde{u}_n)) \in f^{-1}(f(\widetilde{u}_n))] &= \Pr[A(1^{\widetilde{i}}, f(\widetilde{u}_n)) \in f^{-1}(f(\widetilde{u}_n)) \,|\, \widetilde{i} = n] \\ &\leqslant \mathrm{poly}(n)\Pr[A(1^{\widetilde{i}}, f(\widetilde{u}_n)) \in f^{-1}(f(\widetilde{u}_n)),\, \widetilde{i} = n] \leqslant \mathrm{poly}(n)\Pr[B(f(\widetilde{u}_n)) \in f^{-1}(f(\widetilde{u}_n))] = \mathrm{negl}(n),\end{aligned}$$

так как

$$\Pr[\widetilde{i} = n] = \mathsf{E}_x\left[\frac{1}{p(|f(x)|)+1}\right] \geqslant \frac{1}{\mathrm{poly}(n)},$$

где математическое ожидание берется по x, распределенной равномерно на $\{0,1\}^n$ ($n \in N$). Таким образом, f является односторонней в смысле определения 2.1.

Пусть теперь f является односторонней в смысле определения 2.1. Обозначим через g функцию $x \mapsto 1^n 0 f(x)$ ($n \in N$, $x \in \{0,1\}^n$). Честность и полиномиальная вычислимость функции g очевидны. Пусть A — полиномиальный вероятностный алгоритм (пытающийся инвертировать g в смысле определения 2.2). Определим полиномиальный вероятностный алгоритм B (пытающийся инвертировать f в смысле определения 2.1), который на произвольном входе вида $(1^n, y)$, где $n \in N$ и $y \in \{0,1\}^*$, вычисляет $A(1^n 0 y)$ и возвращает полученное выходное значение. Очевидно, что если $x \in \bigcup_{n\in N}\{0,1\}^n$, то $x' \in g^{-1}(g(x))$ тогда и только тогда, когда $|x'| = |x|$ и $x' \in f^{-1}(f(x))$. Поэтому

$$\begin{aligned}\Pr[A(g(\widetilde{u}_n)) \in g^{-1}(g(\widetilde{u}_n))] &= \Pr[B(1^n, f(\widetilde{u}_n)) \in g^{-1}(g(\widetilde{u}_n))] \\ &\leqslant \Pr[B(1^n, f(\widetilde{u}_n)) \in f^{-1}(f(\widetilde{u}_n))] = \mathrm{negl}(n),\end{aligned}$$

так как $A(g(\widetilde{u}_n))$ и $B(1^n, f(\widetilde{u}_n))$ совпадают как случайные величины ($n \in N$). Таким образом, g является односторонней в смысле определения 2.2.

2. Доказать, что если существует IND-CPA-стойкая система шифрования с секретным (открытым) ключом, то существует IND-CPA-стойкая система шифрования с секретным (соответственно открытым) ключом и с теми же пространствами сообщений, для которой CCA позволяет найти секретный ключ. См. также [Gol, Volume 2, Subsection 5.5.7, Exercise 35] (там есть указание к решению).

Решение. Идея решения состоит в том, чтобы сузить множество шифртекстов, генерируемых алгоритмом шифрования (например, сделать, чтобы эти шифртексты начинались с 0), а на остальных строках заставить алгоритм дешифрования раскрывать секретный ключ.

Пусть (G, E, D) — IND-CPA-стойкая система шифрования с секретным (открытым) ключом. Пусть также $n \in \mathbb{N}$ и $(e, d) \in \operatorname{supp} G(1^n)$, где e — ключ шифрования, а d — (секретный) ключ дешифрования. Выберем полиномиальный вероятностный алгоритм E', который на произвольном входе

$(1^n, e, q)$, где $q \in \{0,1\}^*$, вычисляет $\mathrm{v} \leftarrow E(1^n, e, q)$ и возвращает $0\mathrm{v}$. Определим полиномиальный детерминированный алгоритм D следующим равенством:

$$D'(1^n, d, w) = \begin{cases} D(1^n, d, v), & \text{если } w = 0v, \text{ где } v \in \{0,1\}^*; \\ d & \text{в противном случае.} \end{cases}$$

Тогда легко видеть, что (G, E', D') — система шифрования с секретным (соответственно открытым) ключом и с тем же семейством пространств сообщений, что и (G, E, D). Очевидно, что CCA для (G, E', D') позволяет найти секретный ключ d (например, как $D'(1^n, d, 0)$). Осталось доказать IND-CPA-стойкость системы шифрования (G, E', D'). Пусть $(\mathrm{e}, \mathrm{d}) \leftarrow G(1^n)$ и A — произвольный полиномиально ограниченный противник, осуществляющий угрозу различения шифртекстов на основе CPA для (G, E', D') (имеющий доступ к оракулу $E'(1^n, \mathrm{e}, \cdot)$). Построим полиномиально ограниченного противника B, осуществляющего угрозу различения шифртекстов на основе CPA для (G, E, D) (имеющего доступ к оракулу $E(1^n, \mathrm{e}, \cdot)$), следующим образом. Противник B не входе 1^n запускает противника A (т. е. соответствующий алгоритм) на том же входе. Если A делает запрос q к оракулу $E'(1^n, \mathrm{e}, \cdot)$ в процессе осуществления CPA, то B передает этот запрос оракулу $E(1^n, \mathrm{e}, \cdot)$, получает $\mathrm{v} \leftarrow E(1^n, \mathrm{e}, q)$ и передает A в качестве ответа на запрос строку $0\mathrm{v}$. Пусть теперь A выбрал пару (m_0, m_1) сообщений одинаковой длины. Тогда B выбирает ту же пару сообщений, получает $\mathrm{z} \leftarrow E(1^n, \mathrm{e}, m_\mathrm{b})$, где $\mathrm{b} \leftarrow \mathcal{U}(\{0,1\})$, и передает $0\mathrm{z}$ противнику в качестве случайного значения $E'(1^n, \mathrm{e}, m_\mathrm{b})$. Когда A выдаст предполагаемое значение b' бита b, это же значение выдает и B. Очевидно, что вероятность успеха противника A равна вероятности успеха противника B, которая не превосходит $1/2 + \mathrm{negl}(n)$.

Виртуальное занятие 20 апреля 2020 г.

1. Пусть $((e_i \colon M \to C \mid i \in K), \mathcal{K})$ — система секретной связи. Найти множество всех распределений вероятностей $\mathcal{M}$ на M таких, что система секретной связи $(((e_i, \dots, e_i) \colon M^n \to C^n \mid i \in K), \mathcal{K})$ совершенна относительно $\mathcal{M}^n$ для всех $n \in \mathbb{N}$. (Разумеется, $(e_i, \dots, e_i)(m_1, \dots, m_n) = (e_i(m_1), \dots, e_i(m_n))$ для всех $i \in K$ и $(m_1, \dots, m_n) \in M^n$.)

Решение. Это множество есть множество всех распределений вероятностей на M с одноэлементными носителями. Действительно, пусть $\mathcal{M}$ — распределение вероятностей на M. Очевидно, что $\operatorname{supp}(\mathcal{M}^n) = (\operatorname{supp}\mathcal{M})^n$ для любого $n \in \mathbb{N}$. Поэтому если $|\operatorname{supp}\mathcal{M}| = 1$, то и $|\operatorname{supp}(\mathcal{M}^n)| = |\operatorname{supp}\mathcal{M}|^n = 1$, а любая система секретной связи совершенна относительно всякого априорного распределения вероятностей с одноэлементным носителем (это следует из замечания 13.4 конспекта лекций). Пусть теперь $|\operatorname{supp}\mathcal{M}| \geqslant 2$. Тогда $|\operatorname{supp}(\mathcal{M}^n)| = |\operatorname{supp}\mathcal{M}|^n > |\operatorname{supp}\mathcal{K}|$ для всех достаточно больших $n \in \mathbb{N}$. Согласно предложению 13.5 конспекта лекций для таких n система секретной связи $(((e_i, \dots, e_i) \colon M^n \to C^n \mid i \in K), \mathcal{K})$ не может быть совершенной относительно $\mathcal{M}^n$.

2. Доказать, что если существует универсальное одностороннее семейство хэш-функций $(h_{n,d} \colon \{0,1\}^{k(n)} \to \{0,1\}^{m(n)} \mid n \in \mathbb{N}, d \in \{0,1\}^{l(n)})$ относительно семейства распределений вероятностей $(\mathcal{U}(\{0,1\}^{l(n)}) \mid n \in \mathbb{N})$, где $m(n) < k(n) - 1$, $l(n) < k(n)$ и $2^{-l(n)} = \mathrm{negl}(n)$, то существует универсальное одностороннее семейство хэш-функций (относительно того же семейства распределений), не являющееся семейством хэш-функций с трудно обнаружимыми коллизиями (относительно любого семейства распределений на $\{0,1\}^{l(n)}$). См. также [Gol, Volume 2, Subsection 6.6.7, Exercise 20] (там есть указание к решению).

Решение. Пусть $H = (h_{n,d} \colon \{0,1\}^{k(n)} \to \{0,1\}^{m(n)} \mid n \in \mathbb{N}, d \in \{0,1\}^{l(n)})$ — универсальное одностороннее семейство хэш-функций относительно семейства $(\mathcal{U}(\{0,1\}^{l(n)}) \mid n \in \mathbb{N})$, причем $m(n) < k(n) - 1$, $l(n) < k(n)$ и $2^{-l(n)} = \mathrm{negl}(n)$ для всех $n \in \mathbb{N}$. Для произвольных $n \in \mathbb{N}$, $d \in \{0,1\}^{l(n)}$ и $x \in \{0,1\}^{k(n)}$ положим

$$h'_{n,d}(x) = \begin{cases} 0^{m(n)+1}, & \text{если } d = x_{[1,\dots,l(n)]}; \\ 1h_{n,d}(x) & \text{в противном случае.} \end{cases}$$

Очевидно, что семейство $H' = (h'_{n,d} \colon \{0,1\}^{k(n)} \to \{0,1\}^{m(n)+1} \mid n \in \mathbb{N}, d \in \{0,1\}^{l(n)})$ полиномиально вычислимо, причем $m(n) + 1 < k(n)$ для всех $n \in \mathbb{N}$. Это семейство не является семейством хэш-функций с трудно обнаружимыми коллизиями относительно любого семейства распределений на $\{0,1\}^{l(n)}$, так как $(d0^{k(n)-l(n)}, d1^{k(n)-l(n)})$ — коллизия $h'_{n,d}$, которую можно легко найти по $(1^n, d)$, где $n \in \mathbb{N}$ и $d \in \{0,1\}^{l(n)}$. Пусть теперь A — произвольный полиномиальный вероятностный алгоритм

поиска специфических коллизий семейства H'. Тогда A — алгоритм поиска специфических коллизий семейства H и

$$\begin{aligned}\Pr[(A(1^n), A(1^n, \widetilde{d})) \text{ — коллизия } h'_{n,\widetilde{d}}] &= \Pr[(A(1^n), A(1^n, \widetilde{d})) \text{ — коллизия } h'_{n,\widetilde{d}},\ \widetilde{d} = A(1^n)_{[1,\ldots,l(n)]}] \\ &\quad + \Pr[(A(1^n), A(1^n, \widetilde{d})) \text{ — коллизия } h'_{n,\widetilde{d}},\ \widetilde{d} \neq A(1^n)_{[1,\ldots,l(n)]}] \\ &= \Pr[\widetilde{d} = A(1^n)_{[1,\ldots,l(n)]}] + \Pr[(A(1^n), A(1^n, \widetilde{d})) \text{ — коллизия } h_{n,\widetilde{d}}] = \mathrm{negl}(n) + \mathrm{negl}(n) = \mathrm{negl}(n),\end{aligned}$$

где $\widetilde{d} \leftarrow \mathcal{U}(\{0,1\}^{l(n)})$. Здесь использовано то, что

$$\Pr[\widetilde{d} = A(1^n)_{[1,\ldots,l(n)]}] = \frac{1}{2^{l(n)}} = \mathrm{negl}(n)$$

(так как $\widetilde{d}$ и $A(1^n)_{[1,\ldots,l(n)]}$ независимы) и то, что если (x, y) — коллизия $h'_{n,d}$ и $d \neq x_{[1,\ldots,l(n)]}$, то (x, y) — коллизия $h_{n,d}$. Таким образом, H' — универсальное одностороннее семейство хэш-функций относительно семейства $(\mathcal{U}(\{0,1\}^{l(n)}) \mid n \in \mathbb{N})$.

Виртуальное занятие 13 апреля 2020 г.

1. (Для разминки.) Пусть $f_{N,e}(x) = x^e \bmod N$ $(x \in \mathbb{Z}_N^\star)$ для всех $N, e \geqslant 2$. Пусть также A — полиномиальный вероятностный алгоритм, инвертирующий функцию $f_{N,e}$ на случайном аргументе $\widetilde{x} \leftarrow \mathcal{U}(\mathbb{Z}_N^\star)$ с вероятностью $\delta_{N,e}$, т. е. такой, что $\Pr[A(N, e, f_{N,e}(\widetilde{x})) \in f_{N,e}^{-1}(f_{N,e}(\widetilde{x}))] = \delta_{N,e}$ для всех $N, e \geqslant 2$. Доказать, что существует полиномиальный вероятностный алгоритм B, инвертирующий функцию $f_{N,e}$ на произвольном аргументе с той же вероятностью $\delta_{N,e}$, т. е. такой, что $\Pr[B(N, e, f_{N,e}(x)) \in f_{N,e}^{-1}(f_{N,e}(x))] = \delta_{N,e}$ для всех $N, e \geqslant 2$ и $x \in \mathbb{Z}_N^\star$. (Мы предполагаем, что генерация случайных элементов $\mathrm{r} \leftarrow \mathcal{U}(\mathbb{Z}_N^\star)$ выполнима по N за полиномиальное время.)

Решение. Утверждение доказывается аналогично доказательству рандомизированной самосводимости для задачи дискретного логарифмирования. А именно, выберем полиномиальный вероятностный алгоритм B, работающий на произвольном входе (N, e, y), где $N, e \geqslant 2$ и $y \in \mathbb{Z}_N^\star$, следующим образом:

1. Выбрать $\mathrm{r} \leftarrow \mathcal{U}(\mathbb{Z}_N^\star)$.
2. Вычислить $A(N, e, yr^e \bmod N)$.
3. Если на предыдущем шаге получен выход $x' \in \mathbb{Z}_n^\star$, то возвратить $x'r^{-1} \bmod N$ (Очевидно, что $x'r^{-1} \bmod N$ — корень e-й степени из y (в $\mathbb{Z}_N^\star$) тогда и только тогда, когда x' — корень e-й степени из $yr^e \bmod N$).

Пусть $N, e \geqslant 2$, $x \in U(\mathbb{Z}_N^\star)$ и $\widetilde{r} \leftarrow \mathcal{U}(\mathbb{Z}_N^\star)$. Тогда непосредственно проверяется, что

$$\Pr[B(N, e, f_{N,e}(x)) \in f_{N,e}^{-1}(f_{N,e}(x))] = \Pr[A(N, e, f_{N,e}(x\widetilde{r} \bmod N)) \in f_{N,e}^{-1}(f_{N,e}(x\widetilde{r} \bmod N))] = \delta_{N,e},$$

так как случайная величина $x\widetilde{r} \bmod N$ распределена равномерно на $\mathbb{Z}_N^\star$.

2. В этой задаче используются обозначения примера 12.5 конспекта лекций. Для произвольного нечетного числа $N \geqslant 3$ положим

$$\alpha_N(x) = \begin{cases} x, & \text{если } x \in \{1, \ldots, (N-1)/2\}, \\ N - x, & \text{если } x \in \{(N+1)/2, \ldots, N-1\}, \end{cases}$$

и $M_N = \{x \in \{1, \ldots, (N-1)/2\} \mid \left(\frac{x}{N}\right) = 1\}$, где $\left(\frac{x}{N}\right)$ — символ Якоби. Доказать, что при том же предположении, что и в теореме 12.6 конспекта лекций $(\alpha_i(\mathrm{Rabin}_i \mid_{M_i}) \mid i \in I)$ является семейством перестановок с секретом относительно семейств распределений вероятностей $(\mathcal{G}_n \mid n \in \mathbb{N})$ и $(\mathcal{U}(M_i) \mid i \in I)$. См. также [Gol, Volume 2, Section C.1].

Решение. Пусть $N = pq$, где p и q — различные простые числа такие, что $p \equiv q \equiv 3 \pmod 4$ (т. е. N — число Блюма). Для каждого $x \in \mathbb{Z}_N^\star$ положим $J(x) = (\left(\frac{x}{p}\right), \left(\frac{x}{q}\right))$. Из приведенного выше сравнения следует, что $J(N-1) = (-1, -1)$ и, следовательно, $\left(\frac{N-1}{N}\right) = \left(\frac{-1}{N}\right) = 1$. Обозначим через Z множество всех элементов группы $\mathbb{Z}_N^\star$, являющихся квадратичными вычетами по модулю N. Очевидно, что $x \in Z \iff J(x) = (1, 1)$. Для каждого $z \in Z$ положим $\sqrt{z} = \{x \in \mathbb{Z}_N^\star \mid x^2 \bmod N = z\}$, т. е. $\sqrt{z}$ — множество всех квадратных корней из z в группе $\mathbb{Z}_N^\star$.

Пусть $z \in Z$. Для каждых $\varepsilon, \delta \in \{-1, 1\}$ обозначим через $x_{\varepsilon,\delta}$ единственный элемент $\mathbb{Z}_N^\star$, удовлетворяющий сравнениям $x_{\varepsilon,\delta} \equiv \varepsilon z^{(p+1)/4} \pmod p$ и $x_{\varepsilon,\delta} \equiv \delta z^{(q+1)/4} \pmod q$. Тогда легко видеть (см. доказательство теоремы 12.6 конспекта лекций), что $\{x_{\varepsilon,\delta} \mid \varepsilon, \delta \in \{-1, 1\}\} = \sqrt{z}$. Это показывает, что $J|_{\sqrt{z}}$ — биекция $\sqrt{z}$ на $\{-1, 1\}^2$. Кроме того, для любого $x \in \mathbb{Z}_N^\star$ ровно один из элементов x и $N - x$ принадлежит $\{1, \ldots, (N - 1)/2\}$, причем $\left(\frac{x}{N}\right) = \left(\frac{N-x}{N}\right)$ (так как $\left(\frac{-1}{N}\right) = 1$). Следовательно, в множестве $\sqrt{z}$ существует единственный элемент из M_N.

Покажем, как при известных p и q эффективно решать по $y \in M_N$ уравнение $y = \alpha_N(x^2 \bmod N)$ относительно $x \in M_N$ за полиномиальное время. (Под эффективностью в решении этой задачи мы понимаем полиномиальность от $\lceil \log N \rceil$.) Положим $z = y$, если $J(y) = (1, 1)$, и $z = N - y$, если $J(y) = (-1, -1)$. Тогда $z \in Z$ и решением вышеуказанного уравнения является существует единственный элемент из $\sqrt{z} \cap M_N$. Очевидно, что этот элемент может быть найден эффективно. В частности, функция $\alpha_N(\mathrm{Rabin}_N|_{M_N})$ действительно является перестановкой множества M_N. (Включение $\alpha_N(\mathrm{Rabin}_N(M_N)) \subseteq M_N$ вытекает из того, что $\left(\frac{\alpha_N(x)}{N}\right) = \left(\frac{x}{N}\right)$ для всех $x \in \mathbb{Z}_N^\star$.)

Ввиду теоремы 12.6 конспекта лекций для завершения решения задачи осталось доказать, что если мы можем эффективно находить x по $\alpha_N(\mathrm{x}^2 \bmod N)$ при $\mathrm{x} \leftarrow \mathcal{U}(M_N)$, то мы можем эффективно находить некоторый квадратный корень из $\mathrm{y}^2 \bmod N$ при $\mathrm{y} \leftarrow \mathcal{U}(\mathbb{Z}_N^\star)$ с той же вероятностью (разумеется, N также предполагается известным). (Переход к случайному N очевиден.) Итак, пусть даны N и $\mathrm{y}^2 \bmod N$. Из доказанного выше следует, что распределения $\mathrm{x}^2 \bmod N$ и $\mathrm{y}^2 \bmod N$ (рассматриваемых как случайные величины) совпадают (а именно, оба эти распределения равномерны на Z). Следовательно, распределения $\alpha_N(\mathrm{x}^2 \bmod N)$ и $\alpha_N(\mathrm{y}^2 \bmod N)$ также совпадают, поэтому мы можем найти $r \in M_N$, для которого $\alpha_N(\mathrm{r}^2 \bmod N) = \alpha_N(\mathrm{y}^2 \bmod N)$. Из последнего равенства вытекает, что $r^2 \equiv y^2 \pmod N$ или $r^2 \equiv -y^2 \pmod N$. Но последнее сравнение невозможно, так как $N - 1 \notin Z$. Таким образом, r — квадратный корень из $\mathrm{y}^2 \bmod N$.

Виртуальное занятие 6 апреля 2020 г.

1. Доказать, что если $(\widetilde{x}_n \mid n \in \mathbb{N})$ и $(\widetilde{y}_n \mid n \in \mathbb{N})$ — вычислительно неотличимые семейства случайных величин (когда индексы заданы в унарной записи), причем $\widetilde{x}_n$ и $\widetilde{y}_n$ принимают значения в $\{0, 1\}^n$, то $|\Pr[\widetilde{x}_n \in L] - \Pr[\widetilde{y}_n \in L]| = \mathrm{negl}(n)$ для любого языка $L \in \mathrm{BPP}$. См. также [Gol, Volume 1, Subsection 3.8.4, Exercise 4].

Решение. Пусть $L \in \mathrm{BPP}$. Заметим, что если $L \in \mathrm{P}$, то утверждение задачи очевидно. Действительно, пусть A — полиномиальный детерминированный алгоритм, распознающий язык L, т. е. такой, что $A(z) = 1$, если $z \in L$ и $A(z) = 0$ в противном случае. Пусть также D — полиномиальный алгоритм, который на входе $(1^n, z)$ запускает алгоритм A на входе z и выдает результат. Тогда $D(1^n, z) = 1 \iff z \in L$ и, следовательно,

$$|\Pr[\widetilde{x}_n \in L] - \Pr[\widetilde{y}_n \in L]| = |\Pr[D(1^n, \widetilde{x}_n) = 1] - \Pr[D(1^n, \widetilde{y}_n) = 1]| = \mathrm{negl}(n).$$

Для случая, когда $L \in \mathrm{BPP}$, доказательство проводится аналогично. Разница в том, что теперь $\Pr[\widetilde{x}_n \in L]$ и $\Pr[D(1^n, \widetilde{x}_n) = 1]$ не обязательно равны, а отличаются на пренебрежимо малую величину. То же самое верно для $\Pr[\widetilde{y}_n \in L]$ и $\Pr[D(1^n, \widetilde{y}_n) = 1]$.

Выберем полиномиальный вероятностный алгоритм A такой, что $\Pr[A(z) = 1] \geqslant 1 - \mathrm{negl}(n)$ при $z \in \{0, 1\}^n \cap L$ и $\Pr[A(z) = 1] \leqslant \mathrm{negl}(n)$ при $z \in \{0, 1\}^n \setminus L$ для всех $n \in \mathbb{N}$. Определим полиномиальный вероятностный алгоритм D как указано выше. Положим

$$p(n) = \begin{cases} \Pr[A(\widetilde{x}_n) = 1 \mid \widetilde{x}_n \in L], & \text{если } \Pr[\widetilde{x}_n \in L] \neq 0; \\ 1 & \text{в противном случае} \end{cases}$$

и

$$q(n) = \begin{cases} \Pr[A(\widetilde{x}_n) = 1 \mid \widetilde{x}_n \notin L], & \text{если } \Pr[\widetilde{x}_n \notin L] \neq 0; \\ 0 & \text{в противном случае.} \end{cases}$$

Тогда $1 - \mathrm{negl}(n) \leqslant p(n) \leqslant 1$ и $0 \leqslant g(n) \leqslant \mathrm{negl}(n)$, поэтому $0 \leqslant 1 - p(n) + q(n) \leqslant \mathrm{negl}(n) + \mathrm{negl}(n) = \mathrm{negl}(n)$. Следовательно,

$$\begin{aligned} |\Pr[\widetilde{x}_n \in L] - \Pr[D(1^n, \widetilde{x}_n) = 1]| &= |\Pr[\widetilde{x}_n \in L] - p(n) \Pr[\widetilde{x}_n \in L] - q(n) \Pr[\widetilde{x}_n \notin L]| \\ &= |\Pr[\widetilde{x}_n \in L] - p(n) \Pr[\widetilde{x}_n \in L] - q(n) + q(n) \Pr[\widetilde{x}_n \in L]| \\ &= |(1 - p(n) + q(n)) \Pr[\widetilde{x}_n \in L] - q(n)| \\ &\leqslant |1 - p(n) + q(n)| + q(n) = \mathrm{negl}(n) + \mathrm{negl}(n) = \mathrm{negl}(n) \end{aligned}$$

(напомним, что $\Pr[A(\widetilde{x}_n) = 1] = \Pr[D(1^n, \widetilde{x}_n) = 1]$). Аналогично показывается, что

$$|\Pr[\widetilde{y}_n \in L] - \Pr[D(1^n, \widetilde{y}_n) = 1]| = \mathrm{negl}(n).$$

Таким образом,

$$\begin{aligned}|\Pr[\widetilde{x}_n \in L] - \Pr[\widetilde{y}_n \in L]| &\leqslant |\Pr[\widetilde{x}_n \in L] - \Pr[D(1^n, \widetilde{x}_n) = 1]| \\ &\quad + |\Pr[D(1^n, \widetilde{x}_n) = 1] - \Pr[D(1^n, \widetilde{y}_n) = 1]| + |\Pr[D(1^n, \widetilde{y}_n) = 1] - \Pr[\widetilde{y}_n \in L]| \\ &= \mathrm{negl}(n) + \mathrm{negl}(n) + \mathrm{negl}(n) = \mathrm{negl}(n).\end{aligned}$$

2. Доказать, что если существуют семейства хэш-функций с трудно обнаружимыми коллизиями, то существуют односторонние семейства функций (и, следовательно, односторонние функции). См. также [Gol, Volume 2, Subsection 6.6.7, Exercise 14].

Решение. Пусть $(h_{n,d}\colon \{0,1\}^{k(n)} \to \{0,1\}^{m(n)} \mid n \in \mathbb{N},\ d \in D_n)$ — семейство хэш-функций с трудно обнаружимыми коллизиями относительно семейства распределений $(\mathcal{D}_n \mid n \in \mathbb{N})$. Не ограничивая общности, мы считаем, что $2^{m(n)-k(n)} = \mathrm{negl}(n)$ (этого можно добиться с помощью конструкции Меркле–Дамгорда, см. предложение 10.4 конспекта лекций). Положим $I = \{(1^n, d) \mid n \in \mathbb{N},\ d \in D_n\}$. Для каждого $n \in \mathbb{N}$ обозначим через $\mathcal{I}_n$ распределение случайной величины $(1^n, \widetilde{d})$, где $\widetilde{d} \leftarrow \mathcal{D}_n$. Очевидно, что семейство $(\mathcal{I}_n \mid n \in \mathbb{N})$ распределений вероятностей полиномиально конструируемо, когда индексы заданы в унарной записи, а семейство $(\mathcal{U}(\{0,1\}^{k(n)}) \mid (1^n, d) \in I)$ — полиномиально конструируемо. Покажем, что семейство функций $(h_{n,d} \mid (1^n, d) \in I)$ является односторонним относительно этих семейств вероятностей. Полиномиальная вычислимость этого семейства функций очевидна. Пусть теперь A — произвольный полиномиальный вероятностный алгоритм (пытающийся инвертировать данное семейство). Выберем полиномиальный вероятностный алгоритм B, работающий на произвольном входе $(1^n, d)$, где $n \in \mathbb{N}$ и $d \in D_n$, следующим образом:

1. Выбрать $\mathrm{x} \leftarrow \mathcal{U}(\{0,1\}^{k(n)})$.
2. Вычислить $A(1^n, (1^n, d), h_{n,d}(\mathrm{x}))$.
3. Если на предыдущем шаге получен выход $y \in \{0,1\}^{k(n)} \setminus \{\mathrm{x}\}$ такой, что $h_{n,d}(y) = h_{n,d}(\mathrm{x})$, то возвратить пару (x, y) (являющуюся, очевидно, коллизией функции $h_{n,d}$).

Пусть $n \in \mathbb{N}$, $d \in D_n$, $i = (1^n, d)$, $h = h_{n,d}$ и $\widetilde{x} \leftarrow \mathcal{U}(\{0,1\}^{k(n)})$. Обозначим через Z множество всех $z \in h(\{0,1\}^{k(n)})$ таких, что $\Pr[A(1^n, i, z) \in h^{-1}(z)] \neq 0$. Пусть также Z_0 — множество всех $z \in Z$, для которых $|h^{-1}(z)| \geqslant 2$. Тогда

$$\begin{aligned}&\Pr[B(1^n, d) \text{ — коллизия } h_{n,d}] = \Pr[A(1^n, i, h(\widetilde{x})) \in h^{-1}(h(\widetilde{x})) \setminus \{\widetilde{x}\}] \\ &\quad = \sum_{z \in Z} \Pr[A(1^n, i, z) \neq \widetilde{x}, A(1^n, i, z) \in h^{-1}(z), \widetilde{x} \in h^{-1}(z)] \\ &\quad = \sum_{z \in Z} \Pr[A(1^n, i, z) \neq \widetilde{x} \mid A(1^n, i, z) \in h^{-1}(z), \widetilde{x} \in h^{-1}(z)] \Pr[A(1^n, i, z) \in h^{-1}(z), \widetilde{x} \in h^{-1}(z)] \\ &\quad = \sum_{z \in Z} \left(1 - \frac{1}{|h^{-1}(z)|}\right) \Pr[A(1^n, i, z) \in h^{-1}(z), \widetilde{x} \in h^{-1}(z)] \\ &\quad \geqslant \frac{1}{2} \sum_{z \in Z_0} \Pr[A(1^n, i, z) \in h^{-1}(z), \widetilde{x} \in h^{-1}(z)] \\ &\quad = \frac{1}{2} \Pr[A(1^n, i, h(\widetilde{x})) \in h^{-1}(h(\widetilde{x})), \widetilde{x} \in h^{-1}(Z_0)] \\ &\quad = \frac{1}{2}(\Pr[A(1^n, i, h(\widetilde{x})) \in h^{-1}(h(\widetilde{x}))] - \Pr[A(1^n, i, h(\widetilde{x})) \in h^{-1}(h(\widetilde{x})), \widetilde{x} \in h^{-1}(Z \setminus Z_0)]) \\ &\quad \geqslant \frac{1}{2}(\Pr[A(1^n, (1^n, d), h_{n,d}(\widetilde{x})) \in h_{n,d}^{-1}(h_{n,d}(\widetilde{x}))] - 2^{m(n)-k(n)}).\end{aligned}$$

Здесь мы воспользовались следующими фактами:

- при условии $A(1^n, i, z) \in h^{-1}(z), \widetilde{x} \in h^{-1}(z)$ случайная величина $\widetilde{x}$ распределена равномерно на $h^{-1}(z)$ и независима от случайной величины $A(1^n, i, z)$ $(z \in Z)$;
- $1 - 1/|h^{-1}(z)| \geqslant 1/2$ при $z \in Z_0$ и $1 - 1/|h^{-1}(z)| = 0$ при $z \in Z \setminus Z_0$;

- $|h^{-1}(Z \setminus Z_0)| = |Z \setminus Z_0| \leqslant 2^{m(n)}$.

Следовательно,

$$\Pr[A(1^n, (1^n, d), h_{n,d}(\widetilde{x})) \in h_{n,d}^{-1}(h_{n,d}(\widetilde{x}))] \leqslant 2\Pr[B(1^n, d) \text{ — коллизия } h_{n,d}] + 2^{m(n)-k(n)}.$$

Взяв математическое ожидание обеих частей последнего неравенства по d, распределенному в соответствии с $\mathcal{D}_n$, получим, что

$$\begin{aligned}\Pr[&A(1^n, (1^n, \widetilde{d}), h_{n,\widetilde{d}}(\widetilde{x})) \in h_{n,\widetilde{d}}^{-1}(h_{n,\widetilde{d}}(\widetilde{x}))] \\ &\leqslant 2\Pr[B(1^n, \widetilde{d}) \text{ — коллизия } h_{n,\widetilde{d}}] + 2^{m(n)-k(n)} = 2\operatorname{negl}(n) + \operatorname{negl}(n) = \operatorname{negl}(n),\end{aligned}$$

где $\widetilde{d} \leftarrow \mathcal{D}_n$.

3. Доказать, что если $(h_{n,d}\colon \{0,1\}^{k(n)} \to \{0,1\}^{m(n)} \mid n \in \mathbb{N},\ d \in D_n)$ — универсальное одностороннее семейство хэш-функций, то $2^{-m(n)} = \operatorname{negl}(n)$.

Решение. Для произвольного распределения вероятностей $\mathcal{Z}$ на конечном множестве Z число $\mathrm{CP}(\mathcal{Z})$ (CP означает Collision Probability) определяется как $\Pr[\widetilde{z}_1 = \widetilde{z}_2]$, где $\widetilde{z}_1, \widetilde{z}_2 \leftarrow \mathcal{Z}$. Другими словами, $\mathrm{CP}(\mathcal{Z}) = \sum_{z \in Z} (\Pr_{\mathcal{Z}}\{z\})^2$. Легко проверяемое равенство

$$\mathrm{CP}(\mathcal{Z}) - \frac{1}{|Z|} = \sum_{z \in Z} \left(\Pr_{\mathcal{Z}}\{z\} - \frac{1}{|Z|}\right)^2$$

показывает, что $\mathrm{CP}(\mathcal{Z}) \geqslant 1/|Z|$, причем равенство достигается только при $\mathcal{Z} = \mathcal{U}(Z)$.

Пусть $(h_{n,d}\colon \{0,1\}^{k(n)} \to \{0,1\}^{m(n)} \mid n \in \mathbb{N},\ d \in D_n)$ — универсальное одностороннее семейство хэш-функций относительно семейства распределений вероятностей $(\mathcal{D}_n \mid n \in \mathbb{N})$. Выберем полиномиальный вероятностный алгоритм A поиска специфических коллизий этого семейства, который, получив на вход 1^n при произвольном $n \in \mathbb{N}$, возвращает $x \leftarrow \mathcal{U}(\{0,1\}^{k(n)})$, а после получения $d \in D_n$ возвращает $y \leftarrow \mathcal{U}(\{0,1\}^{k(n)})$. Тогда если $\widetilde{d} \leftarrow \mathcal{D}_n$ и $\widetilde{x}, \widetilde{y} \leftarrow \mathcal{U}(\{0,1\}^{k(n)})$, то

$$\begin{aligned}\operatorname{negl}(n) &= \Pr[A(1^n, \widetilde{d}) \text{ — коллизия } h_{n,\widetilde{d}}] = \Pr[h_{n,\widetilde{d}}(\widetilde{x}) = h_{n,\widetilde{d}}(\widetilde{y})] - \Pr[\widetilde{x} = \widetilde{y}] \\ &\geqslant \frac{1}{2^{m(n)}} - \frac{1}{2^{k(n)}} \geqslant \frac{1}{2^{m(n)}} - \frac{1}{2^{m(n)+1}} = \frac{2^{-m(n)}}{2}\end{aligned}$$

ввиду приведенных выше фактов о CP. Следовательно, $2^{-m(n)} = 2\operatorname{negl}(n) = \operatorname{negl}(n)$. См. также [Gol, Remark 2.5].

Виртуальное занятие 23 марта 2020 г.

1. Пусть $x_n \in X_n \subseteq \{0,1\}^{m(n)}$ для всех $n \in \mathbb{N}$ (где m — полиномиальный параметр), причем

- проблема вхождения в X_n для строк из $\{0,1\}^{m(n)}$ разрешима за полиномиальное от n время;
- $|X_n|/2^{m(n)} = \delta_n \geqslant 1/p(n)$ для некоторого полинома p;
- функция $1^n \mapsto x_n$ полиномиально вычислима.

Рассмотрим полиномиальный вероятностный алгоритм A, который на входе $(1^k, 1^n)$ $(k, n \in \mathbb{N})$ выполняет следующие шаги не более $kp(n)$ раз:

- Выбрать $\mathrm{w} \leftarrow \{0,1\}^{m(n)}$.
- Если $\mathrm{w} \in X_n$, то возвратить w и закончить работу.

Если же $\mathrm{w} \notin X_n$ на всех $kp(n)$ итерациях, то алгоритм A возвращает x_n. Доказать, что статистическое расстояние между распределением случайной величины $A(1^k, 1^n)$ и равномерным распределением на X_n не превосходит e^{-k} (и, следовательно, 2^{-k}), где e — основание натуральных логарифмов.

Решение. Если $k = 0$, то утверждение тривиально. Считаем теперь, что $k \geqslant 1$. Пусть $S = S_{k,n}$ — событие, состоящее в том, что A на входе $(1^k, 1^n)$ заканчивает работу на одной из итераций, а S' — событие, дополнительное к S. Тогда для любого $M \subseteq X_n$

$$\begin{aligned}
&|\Pr[A(1^k, 1^n) \in M] - \Pr_{\mathcal{U}(X_n)} M| \\
&\quad = |\Pr[A(1^k, 1^n) \in M \mid S] \Pr S + \Pr[A(1^k, 1^n) \in M, S'] - \Pr_{\mathcal{U}(X_n)} M| \\
&\quad = |\Pr[A(1^k, 1^n) \in M, S'] - (\Pr_{\mathcal{U}(X_n)} M)(\Pr S')| \leqslant \Pr S' \\
&\quad = (1 - \delta_n)^{kp(n)} \leqslant (1 - 1/p(n))^{kp(n)} = e^{kp(n)\ln(1-1/p(n))} \leqslant e^{-k}.
\end{aligned}$$

Здесь мы воспользовались следующими фактами:

- при условии S случайная величина $A(1^k, 1^n)$ распределена равномерно на X_n;
- модуль разности двух неотрицательных чисел, не превосходящих $\Pr S'$, не превосходит $\Pr S'$;
- $\ln t \leqslant t - 1$ для любого $t > 0$.

Взяв максимум по всем $M \subseteq X_n$, получим требуемую оценку.

2. Пусть g — псевдослучайный генератор, отображающий $\{0,1\}^n$ в $\{0,1\}^{m(n)}$ для всех $n \in \mathbb{N}$. Пусть также $M_n \subseteq \{0,1\}^n$, причем проблема вхождения в M_n для строк из $\{0,1\}^n$ разрешима за полиномиальное от n время. Определим g' на $\{0,1\}^n$ при каждом $n \in \mathbb{N}$ следующим образом: $g'(x) = 0^{m(n)}$ при $x \in M_n$ и $g'(x) = g(x)$ при $x \in \{0,1\}^n \setminus M_n$. Доказать, что g' — псевдослучайный генератор тогда и только тогда, когда $|M_n|/2^n = \mathrm{negl}(n)$.

Решение. (i) Пусть g' — псевдослучайный генератор. Рассмотрим полиномиальный вероятностный алгоритм D такой, что $D(1^n, y) = 1 \iff y = 0^{m(n)}$ для всех $n \in \mathbb{N}$ и $y \in \{0,1\}^*$. Тогда

$$\Pr[D(1^n, g'(\widetilde{u}_n)) = 1] \geqslant \frac{|M_n|}{2^n} \quad \text{и} \quad \Pr[D(1^n, \widetilde{u}_{m(n)}) = 1] = \frac{1}{2^{m(n)}}.$$

Следовательно,

$$\begin{aligned}
\frac{|M_n|}{2^n} &\leqslant \frac{1}{2^{m(n)}} + \Pr[D(1^n, g'(\widetilde{u}_n)) = 1] - \Pr[D(1^n, \widetilde{u}_{m(n)}) = 1] \\
&\leqslant \mathrm{negl}(n) + |\Pr[D(1^n, g'(\widetilde{u}_n)) = 1] - \Pr[D(1^n, \widetilde{u}_{m(n)}) = 1]| = \mathrm{negl}(n).
\end{aligned}$$

Пусть $|M_n|/2^n = \mathrm{negl}(n)$ и D — произвольный полиномиальный вероятностный алгоритм. Тогда

$$\Pr[D(1^n, g'(\widetilde{u}_n)) = 1] = \Pr[D(1^n, g'(\widetilde{u}_n)) = 1, \widetilde{u}_n \in M_n] + \Pr[D(1^n, g'(\widetilde{u}_n)) = 1, \widetilde{u}_n \notin M_n]$$

и

$$\Pr[D(1^n, g(\widetilde{u}_n)) = 1] = \Pr[D(1^n, g(\widetilde{u}_n)) = 1, \widetilde{u}_n \in M_n] + \Pr[D(1^n, g(\widetilde{u}_n)) = 1, \widetilde{u}_n \notin M_n],$$

где первые слагаемые не превосходят $|M_n|/2^n$, а вторые совпадают. Поэтому

$$|\Pr[D(1^n, g'(\widetilde{u}_n)) = 1] - \Pr[D(1^n, g(\widetilde{u}_n)) = 1]| = \mathrm{negl}(n).$$

Кроме того,

$$|\Pr[D(1^n, g(\widetilde{u}_n)) = 1] - \Pr[D(1^n, \widetilde{u}_{m(n)}) = 1]| = \mathrm{negl}(n),$$

так как g — псевдослучайный генератор. Следовательно,

$$|\Pr[D(1^n, g'(\widetilde{u}_n)) = 1] - \Pr[D(1^n, \widetilde{u}_{m(n)}) = 1]| = \mathrm{negl}(n).$$

Таким образом, g' — псевдослучайный генератор.

3. Пусть $a_n \in \{0,1\}^n$ и $b_n \in \{0,1\}^{m(n)}$, где m — полиномиальный параметр такой, что $m(n) > n$ для всех $n \in \mathbb{N}$. Предположим, что функции $1^n \mapsto a_n$ и $1^n \mapsto b_n$ полиномиально вычислимы. Доказать, что если существуют псевдослучайные генераторы, то существует псевдослучайный генератор g такой, что $g(a_n) = b_n$ для всех $n \in \mathbb{N}$.

Решение. Пусть g — псевдослучайный генератор, отображающий $\{0,1\}^n$ в $\{0,1\}^{m(n)}$ для всех $n \in \mathbb{N}$. Такой генератор существует ввиду следствия 7.7 конспекта лекций. Аналогично предыдущей задаче, определим g' на $\{0,1\}^n$ при каждом $n \in \mathbb{N}$ следующим образом: $g'(a_n) = b_n$ и $g'(x) = g(x)$ при $x \in \{0,1\}^n \setminus \{a_n\}$. Тогда, рассуждая как в п. (ii) решения предыдущей задачи, получим, что g' — псевдослучайный генератор.

Список литературы

[Ano] M. Anokhin. Pseudo-free families of computational universal algebras. Cryptology ePrint Archive (https://eprint.iacr.org/), Report 2018/1178, 2018.

[Gol] O. Goldreich. Foundations of cryptography. Volume 1 (Basic tools). Volume 2 (Basic applications). Cambridge University Press, 2001 (v. 1), 2004 (v. 2).