Лекция 6. Интерактивный протокол бросания монетки

1 Общая схема задачи

Алиса и Боб ненавидят друг друга. Неоходимо получить общий случайный бит в условиях полного недоверия. A и B представляют собой два рандомизированных полиномиальных алгоритма с независимыми случайными битами. Они общаются протоколу и после завершения выдают по одному биту σ, τ.

Нужно, чтобы оказалось так, чтобы $\sigma = \tau, P(\sigma = 0) \approx \frac{1}{2}$. Для этого есть полиномиальный алгоритм J, который получает протокол и возвращает $A, B, \perp_A, \perp_B$ — либо сторону-победителя, либо сторону, которая первая нарушила протокол.

Требуемые свойства:

- Корректность: если обе стороны используют предписанные алгоритмы, то $P(J = A) = P(J = B) = \frac{1}{2}$.
- Интересы Алисы: $\forall B^* \to P(J \in \{0, \perp_B\}) \approx \frac{1}{2}$.
- Интересы Боба: $\forall A^* \to P(J \in \{1, \perp_A\}) \approx \frac{1}{2}$.

Если бы можно было обмениваться сообщениями одновременно, то можно было бы каждому послать случайный бит и в качестве результата взять их $\oplus$. Однако, одновременных сообщений не предусмотрено, поэтому используется привязка к биту (bit commitment). Такие протоколы неформально «запечатывают» бит в конверт так, чтобы его уже нельзя было подменить, но и нельзя посмотреть, не вскрыв конверт.

2 Неинтерактивный протокол привязки к биту

Неинтерактивная версия протокола подразумевает следующее: σ — запечатаныый бит, r — случайные биты, $c(\sigma, r)$ — привязка, $k(\sigma, r)$ — ключ, $d(c, k) \in \{0, 1, \perp\}$ — процедура вскрытия (все алгоритмы полиномиальны и детерменированы). Условия на протокол следующие:

- Корректность: $d(c(\sigma, r), k(\sigma, r)) = \sigma$.
- Неразглашение: $c(0, r) \sim c(1, r)$.
- Неподменяемость: $\nexists c, k_0, k_1 : d(c, k_0) = 0, d(c, k_1) = 1$.

Замечание. В условии неразглашения требовать статистическую неотличимость не получится, так как третье условие говорит о том, что привязка расшировывается однозначно либо в 1, либо в 0, то есть $c(0, r)$ и $c(1, r)$ вообще распределены на разных множествах. Поэтому требуется вычислительная неотличимость, добиться которой можно.

Функция привязки строится на базе односторонней перестановки f, из которой по теореме Левина-Голдрайха получается односторонняя перестановка g с трудным битом h. А именно $c(\sigma, r) = (\sigma \oplus h(r), g(r))$.

Можно считать, что $k(\sigma, r) = \sigma r$, так как распаковщик сам может провести все нужные вычисления. Каноническая процедура вскрытия может просто вычислять $c(0, r), c(1, r)$, сравнивать его с c и возвращать $0, 1$ или $\perp$ в зависимости от результата. То есть, формально $k(\sigma, r) = (\sigma, r)$, $d((\tau, s); (\sigma, r)) = \tau \oplus h(r)$ если $g(r) = s$ и $\sigma = h(r)$, иначе $\perp$. Корректность такого алгоритма очевидна.

Трудность бита h означает, что $(g(r), h(r)) \sim (g(r), \gamma)$, где γ — случайный бит. Отсюда $(g(r), 1 \oplus h(r)) \sim (g(r), 1 \oplus \gamma) \sim (g(r), \gamma)$, то есть $(g(r), h(r)) \sim (g(r), 1 \oplus h(r))$, откуда следует неразглашение.

В свою очередь, так как g — инъекция, то $\forall s \exists \leqslant 1 r : g(r) = s$, то есть подменить ключ в самом деле не получится.

Замечание. Практически, одностороннюю перестановку удобно иметь не на $\{0, 1\}^*$, а на любой области D. В таком случае хочется сказать, что нужно уметь проверять условие $r \in D$, однако это не практично (например, если брать одностороннюю перестановку на базе RSA, мы не можем проверить, является ли это число произведением больших простых чисел). Поэтому уточнение такое: нужно уметь генерировать случайную величину, которая либо равномерно распределена на D, либо принимает фиктивное значение (пустую строку, к примеру). В таком случае, мы можем пытаться открывать конверт, пока он не откроется, то есть либо в среднем за полиномиальное время, либо за гарантированный полином с маленькой вероятностью ошибки.

3 Интерактивный протокол привязки к биту

Такой протокол действует в две стадии, условно изображённые на схеме:

$$\begin{tikzcd}
\text{1 стадия: } \sigma \arrow[r] & S \arrow[r, equal] \arrow[d] & T \arrow[d] & \\
\text{2 стадия: } & k \arrow[r] & R(k, c) \arrow[r] & \sigma
\end{tikzcd}$$

Где $c = c_{T,S(\sigma)}$ — протокол общения между S, T, а алгоритм верификации R проверяет его и возвращает что-то $\{0, 1, \perp_S, \perp_T\}$. Условия на протокол похожие с поправкой на то, что жульничать могут обе стороны:

- Корректность: $R(k_{T,S(\sigma)}, c_{T,S(\sigma)}) = \sigma$.
- Неразглашение: $\forall T^* \to c_{T^*,S(0)} \sim c_{T^*,S(1)}$.
- Неподменяемость: $\forall S^*$ с пренебрежимо малой вероятностью могут произойти события:
  - $\exists k_0, k_1 R(k_0, c_{T,S^*}) = 0, R(k_1, c_{T,S^*}) = 1$.

– $\exists k_1 : R(k_1, c_{T,S^*}) = \perp_T$.

Конечно, неинтерактивный протокол можно без труда переделать в интерактивный. Однако, для существования интерактивного протокола будет достаточно меньшего предположения, а именно существования генератора $G : \{0,1\}^n \to \{0,1\}^{3n}$. Протокол устроен так:

- T посылается случайный вектор $t \in \{0,1\}^{3n}$.
- S имеет собственный случайный вектор $s \in \{0,1\}^n$ и посылает $m = G(s) \oplus (t \cdot \sigma)$.
- Верификатор $R(t, m, s)$ выдает:
  - $\perp_T$, если $|t| \neq 3n$.
  - $\perp_S$, если $|m| \neq 3n$ или $|s| \neq n$ или $m \oplus G(s) \notin \{t, 0^{3m}\}$.
  - 0, если $m \oplus G(s) = 0^{3n}$.
  - 1, иначе.

Корректность как всегда ясна (по модулю случая, когда $t = 0^{3n}$, его нужно либо запретить с небольшим перекосом в распределении, либо допустить малую вероятность некорректности).

$G(s)$ неотличимы от равномерных, значит какими бы ни были t, $G(s) \oplus t$ тоже неотличимы от равномерных, что даёт неразглашение.

С неподменяемостью нужно разобрать некоторые случаи. Вероятность $\perp_T$ просто равна 0. Остается только первое условие: в нём множество плохих $t = G(s_0) \oplus G(s_1)$ имеет размер не больше 2^{2n}, значит вероятность выбрать такое t экспоненциально мала, даже для любой константы $2 + \varepsilon$ вместо 3.

4 Протокол бросания монетки

Протокол выглядит так:

- Алиса запукает протокол привязки к своему случайному биту σ. После этого у нее остается ключ k, а у Боба появляется привязка c.
- Боб отправляет случайный бит τ прямым текстом.
- Алиса отправляет ключ к привязке k.
- Судья проверяет корректность всех действий и выдаёт $\tau \oplus \sigma$.

Протокол очевидно корректен. Если B^* отклоняется от протокола, то он может использовать T^* и взять τ в зависимости от c. Однако, так как привязка к 0 и привязка к 1 вычислительно неотличимы, то он не может существенно повлиять на конечную вероятность, иначе он бы был отличителем привязок. Таким образом, интересы Алисы следуют из неразглашения.

Интересы Боба же следуют из неподменяемости: так как Боб посылает реально случайный бит τ, она не может жульничать с самим битом σ, единственное, что она может попытаться сделать — это привязаться одновременно к 0 и 1, что невозможно в силу неподменяемости.