Д.В.Мусатов
Задачи к курсу «Протоколы электронных выборов»

Лекция 1: доказательства с нулевым разглашением

Для получения зачёта по этому листку достаточно решить любые 2 задачи. Будет также ещё хотя бы один листок.

На лекции мы изучили концепцию доказательств с нулевым разглашением, когда одна сторона (Алиса) убеждает другую (Боба) в существовании некоторого объекта, при этом не разглашая никакой информации про сам этот объект. Точных определений не давалось, но мы изучили два примера:

- **Задача об изоморфизме графов.** Пусть Алиса знает перенумерацию (перестановку) вершин φ, которая превращает граф G_0 в граф G_1, а Боб — только сами графы. Тогда протокол таков: Алиса выбирает случайную перестановку вершин σ и посылает Бобу $H = \sigma(G_1)$. Затем Боб случайно выбирает $b \in \{0, 1\}$. Алиса присылает τ, такую что выполнено $H = \sigma(G_b)$, а Боб проверяет это равенство. Если Алиса действительно знает φ, то она пришлёт либо σ при $b = 1$, либо $\sigma \circ \varphi$ при $b = 0$, и проверка пройдёт всегда. При этом Боб узнал какой-то граф и изоморфизм его либо с G_0, либо G_1, он мог узнать такую пару и без диалога с Алисой. А если графы неизоморфны, то Алиса успешна с вероятностью не больше половины. За счёт многократного независимого повторения последнюю вероятность можно сделать близкой к нулю. Такого рода протоколы называются доказательствами с *совершенно нулевым разглашением*.

- **Задача о судоку.** Головоломка судоку выглядит так: дано поле 9×9, разбитое на 9 квадратов 3×3. Изначально на некоторых полях стоят цифры от 1 до 9. Нужно дорасставить цифры на остальных полях, чтобы в каджой строке, каждом столбце и каждом из квадратов разбиения встречались все цифры от 1 до 9 по одному разу. Пусть Алиса знает решение головоломки судоку, а Боб — только условие. Алиса случайным образом переставляет цифры в ответе (например, все единицы заменяет на семёрки, все двойки на четвёрки и т.д.) и закрывает все поля непрозрачными крышками. Боб снимает крышки либо со всех полей одного столбца, либо со всех полей одной строки, либо со всех сторон одного квадрата, либо со всех исходной занятых полей. В первых трёх случаях проверяется, что все открытые цифры различны, в последнем — что открытые поля действительно получены перестановкой условия. В таком случае если Алиса знает решение, то проверка пройдёт всегда, но Боб узнает только случайную перестановку цифр от 1 до 9 либо саму по себе, либо применённую к условию головоломки. А если решения нет, то проверка пройдёт с вероятностью не больше $\frac{27}{28}$. За счёт многократного повторения эту вероятность можно снова сделать близкой к нулю. Такого рода протоколы (с непрозрачными крышками) называются доказательствами с *вычислительно нулевым разглашением*.

Попробуйте по аналогии построить протоколы в следующих задачах.

Задача 1. Придумайте доказательство с совершенно нулевым разглашением для множества квадратичных вычетов. Более подробно, $\mathsf{QR} = \{(a, m) \mid \exists x\ a \equiv x^2 \mod m\}$. Алиса знает этот x и должна убедить Боба в его существовании, но не раскрыть его.

Задача 2. Придумайте доказательство с вычислительно нулевым разглашением для множества графов, раскрашиваемых в 3 цвета. Более подробно, Алиса знает, как раскрасить неориентированный граф в 3 цвета, чтобы любые две соседние вершины были разных цветов. А Боб знает только исходный граф. Алиса должна убедить Боба в существовании раскраски, но не раскрыть никаких деталей про неё.

Задача 3. Придумайте доказательство с вычислительно нулевым разглашением для головоломки Instant Insanity. Правила такие: даны N кубиков, на гранях которых стоят какие-то числа от 1 до N, возможно, повторяющиеся. Нужно построить башню, поворачивая кубики любым способом, такую что на каждой из 4 боковых сторон башни встречаются все метки от 1 до N. Алиса знает решение, а Боб — только набор кубиков. Алиса должна убедить Боба в существовании решения.

Д.В.Мусатов

Задачи к курсу «Протоколы электронных выборов»

Лекция 2: протоколы привязки к сообщению

Для получения зачёта по этому листку достаточно решить любые 2 задачи.

На лекции мы изучили протоколы привязки к сообщению. Неформально говоря, они моделируют закрывание объекта непрозрачной крышкой. Формально есть две функции: f превращает сообщение m в пару из привязки c и ключа k, а g выполняет обратное преобразование из пары в исходное сообщение. При этом f может быть вероятностной, а g — не всюду определённой). Кроме того, функции должны быть вычислимыми за полиномиальное время и удовлетворять следующим свойствам:

1) Корректность. Для любого m должно быть выполнено $g(f(m)) = m$.

2) (Абсолютная) неподменяемость. Не может существовать величин c, k, k', таких что $g(c, k)$ и $g(c, k')$ определены и не равны.

3) (Вычислительная) непрозрачность. Не существует полиномиального алгоритма, который на входе c возвращает m.

Мы рассмотрели такой протокол для привязки к одному биту: $f(b)$ выбирает случайное $x = pq$, где p и q — различные простые вида $4n+3$, случайное $y \in (0, \frac{x-1}{2})$, взаимно простое с x, и возвращает $c = (x, y^2 \mod x, y_0 \oplus b)$, где y_0 — младший бит y, и $k = y$.

Задача 4. Придумайте аналогичный протокол, в котором $c = (x, y^2 \mod x)$, при этом x выбирается точно так же, но y может выбираться иначе. Указание: подумайте, где тут может фигурировать b.

Задача 5. Придумайте на основе любого протокола привязки протокол бросания монетки по телефону. То есть Алиса и Боб запускают полиномиальные вероятностные алгоритмы и посылают друг другу какие-то сообщения, возможно, в несколько раундов. В результате они должны сгенерировать бит, распределённый равномерно. Этот бит должен быть однозначно установлен любым наблюдателем, прочитавшим все сообщения диалога. Отклонение одной стороны от протокола (например, генерирование очередных сообщений не случайно, а с использованием предыдущих сообщений) не должно сдвинуть результат в пользу этой стороны (например, Алиса выигрывает, если выпал орёл, а Боб — если решка).

Задача 6. В этой задаче мы познакомимся со схемой привязки, основанной на сложности задачи дискретного логарифмирования. На этих же формулах основана система шифрования Эль-Гамаля.

а) Пусть q является простым делителем $p-1$, f есть случайный остаток по модулю p, а $g = f^{\frac{p-1}{q}} \not\equiv 1 \mod p$. Докажите, что $1, g, \ldots, g^{q-1}$ различны. Говорят, что g является генератором группы порядка q. Указание: нужно использовать малую теорему Ферма.

б) Докажите, что выбор другого f приведёт к той же самой группе. (Т.е. множества $\{1, g, \ldots, g^{q-1}\}$ и $\{1, h, \ldots, h^{q-1}\}$ совпадают). Указание: можно использовать, что по простому модулю число корней многочлена не больше его степени.

в) Пусть зафиксированы генераторы g и h, а мы хотим привязаться к $x = g^k$. Покажите, что привязка $E_a(x) = (g^a, x \cdot h^a)$ удовлетворяет абсолютной неподменяемости, а установление x по привязке эквивалентно решению задачи Диффи-Хеллмана, т.е. умению находить по генератору g и двум числам g^a и g^b числа g^{ab}. Покажите, как каждую из этих задач можно решить, если уметь вычислять дискретный логарифм (т.е. по генератору g и числу z вычислить b, такое что $g^b = z$).