Лекция 11. Безопасные многосторонние вычисления

1 Общий вид задачи

Имеется m — участники, у каждого есть вход x_i и у всех вместе есть функционал $f : (x_1, \ldots, x_m) \mapsto (y_1, \ldots, y_m)$, возможно вероятностный.

Нужно, чтобы всё, что узнали нечестные участники, они могли бы узнать лишь исходя из своих x_i, y_i.

Получестная модель: все выполняют протокол, но могут анализировать промежуточные результаты. Можно также рассматривать две нечестные модели: в первой из них любое количество участников могут быть нечестными и отклоняться от протокола, при этом нет защиты от прекращения общения; во второй модели нечестными могут быть строго меньше половины участников и есть защита от преждевременной остановки.

Дополнительный аспект, проявляющийся, когда сторон становится больше двух, — это отличие между двухсторонними каналами и широковещательными.

Также разумно поставить вопрос о подслушивании и адаптивном подслушивании (когда противник может подслушать часть сообщений, а потом перехватить контроль над какой-то стороной по своему желанию).

2 Получестная модель

Функция f вычисляется арифметической схемой. Пусть имеется a, b, хранящиеся распределенно: $a = a_1 \oplus \ldots a_m$, $b = b_1 \oplus \ldots \oplus b_m$. Хотим посчитать $c = a \wedge b$.

$$\begin{aligned} c &= a \wedge b \\ &= \left(\sum a_i\right)\left(\sum b_j\right) \\ &= \sum a_i b_i + \sum_{1 \leqslant i < j \leqslant m} (a_i b_j + a_j b_i) \\ &= \sum a_i b_i + \sum_{1 \leqslant i < j \leqslant m} (a_i + a_j)(b_i + b_j) - \sum_{1 \leqslant i < j \leqslant m} (a_i b_i + a_j b_j) \\ &= \sum (a_i + a_j)(b_i + b_j) + m \sum a_i b_i. \end{aligned}$$

Участники i, j вычисляют c_{ij}^i, c_{ij}^j такие, что $c_{ij}^i \oplus c_{ij}^j = (a_i + a_j) \oplus (b_i \oplus b_j)$. $c_i = \sum\limits_{i \neq j} c_{ij}^i + m a_i b_i$.

c_{ij}^i вычисляются случайно, 4 варианта:

- $d_{00} = c_{ij}^i \oplus a_i b_i$;
- $d_{01} = c_{ij}^i \oplus a_i (b_i \oplus 1)$;

- $d_{10} = c_{ij}^i \oplus (a_i \oplus 1)b_i$;
- $d_{11} = c_{ij}^i \oplus (a_i \oplus 1)(b_i \oplus 1)$.

Используется протокол пересылки вслепую.

Теперь можно смоделировать работу всей схемы:

- Разделение секрета;
- Моделирование отдельных шагов;
- Восстановление ответа (все стороны присылают свои биты, соответствующие ответу данной стороны).

3 Двухсторонние и широковещательные каналы

В нечестных моделях может быть важен тип канала, однако мы покажем, что при помощи односторонней перестановки с секретом можно моделировать одно на базе другого.

Чтобы смоделировать двусторонний канал с помощью широковещательного используем шифрование с открытым ключом:

- Каждая сторона генерирует пару ключей и посылает всем открытый;
- Для отправки сообщения i-я сторона может воспользоваться j-м открытым ключом и послать шифрованное сообщение j-й стороне, которая сможет расшифровать его с помощью своего закрытого ключа.

В другую сторону чуть менее тривиально — используем так называемое Византийское соглашение. Нам нужно, чтобы все честные участники получили одно и то же, притом, если отправитель честный, то все получили то, что он и послал.

- Первая сторона рассылает $v_2, \ldots, v_m$ вместе с подписями $s_2, \ldots, s_m$;
- Сторона j пересылает полученное сообщение (с подписью) вместе со своей подписью;
- Следующие стадии происходят аналогично, если в цепочке подписей не было подписи стороны j.
- В конце каждая сторона проверяет исходное сообщение и все подписи.

4 Нечестные модели

Для решения проблем с нечестными участниками можно моделировать протокол получестных вычислений. Для этого нужно сделать следующее:

- Привязка ко входу;
- Генерация приватных, но проверяемо-случайных битов;
- Моделирование получестного протокола.

Такая модель никак не застрахована от подмены входа (от этого застраховаться нельзя в принципе), но также подверженна и преждевременной остановке — сторона может получить свой ответ и отказаться посылать что-либо еще.

Чтобы решить проблему преждевременной остановки можно воспользоваться продвинутым разделением секрета «t из m». Если a исходный секрет, по нему формируется $a_1, \ldots, a_m$ такие, что по любым $a_{i_1}, \ldots, a_{i_t}$ можно изнуть a, а по любому меньшему количеству невозможно.

Функция разделения секрета: выбирается простое число $p > m$ и генерируется случайный многочлен степени $t-1$ над $\mathbb{F}_p$ со свободным членом a. $a_1, \ldots, a_m$ тогда можно положить равными заначению многочлена в точках $1, \ldots, m$. Тогда по любым t точкам многочлен интерполируется, а из любых $t-1$ точек никакой информации про свободный член извлечь нельзя.

Тогда, если честные замечают, что кто-то прекратил действовать по протоколу, они собираются вместе, рассекречивают исходный секрет и продолжают вычисления, эмулируя действия отключившейся стороны. Если же сторона отключилась с самого начала, то можно считать, например, что она подменила свой вход на 0.