Криптография, Лекция № 12

1 декабря 2014 г.

1 Задача Безопасных Вычислений

Есть некоторое количество участников A_i и каждый из них что-то знает x_i, и что-то хочет узнать $f_i(x_1, \ldots, x_n)$. Задача: все стороны должны узнать $f_i(x_1, \ldots, x_n)$ но ничего сверх того.

Example 1.
A имеет x_1 рублей, B имеет x_2 рублей; и они хотят узнать у кого больше
$f_1(x_1, x_2) = f_2(x_1, x_2) = I(x_1 \geq x_2)$

Definition 1.
Протокол решения задачи - набор из n полиномиальных вероятностных интерактивных алгоритмов.

В идеальной модели есть независимая доверенная сторона, все ей отправляют x_i, она возвращает $f_i(x_1, \ldots, x_n)$.

Парадигма: в реальной модели не должно быть возможным ничего, что невозможно в идеальной.

Есть несколько видов поведения агентов:

- Честное поведение:
  Даже если агент узнал что-то не то, он сразу же "забывает"
- Полу-честное (Semi-honest):
  В идеальной модели агент может что-то вычислить на основе входа и выхода. В реальной модели агент действует по протоколу, но на базе промежуточной, входной и выходной информации может что-то вычислить.
- Нечестное (Malicious):
  В идеальной модели агент может подменить ход, или вообще отказаться участвовать. В реальной модели агент может делать что угодно (действует не про протоколу, подменяет вход), только в условиях полиномиальной ограниченности.

Definition 2. (Надежность в полу-честной модели)
П - протокол, $VIEW_i^{\Pi}(x, y)$ - все сообщения, которые получает сторона i при выполнении протокола П на входе (x, y).

П надёжен в полу-честной модели, если при любом $i\ in\{1,2\}$ существует полиномиальный алгоритм S_i такой, что

$$S_i(x_i, f_i(x1, x_2))\text{вычислительно не отличима от}VIEW_i^{\Pi}(x,y)$$

Remark 1.
Аналогично записывается определение надежности для более чем двух сторон.

Definition 3. (Слепая предача (oblivious transfer), OT_1^k)
Вход: $x = (\sigma_1, \ldots, \sigma_k), \sigma_j \in \{0,1\}\ y = i \in \{1, \ldots, k\}$.
Выход: $f_1(x,y) = f(x,y) = \varepsilon;\ f_2(x,y) = g(x,y) = \sigma_i$

Example 2. *(Применение OT_1^4)*
Пусть f вычисляется арифметической схемой, работающей с битами, то есть схемой из функциональных элементов $\bigwedge$ и $\oplus$. Агент A выбирает случайное r, запоминает его и посылает $r \odot x$. После этого A имеет r, B имеет r'; r, r' - случайные, но $r \oplus r' = x$. Далее B выбирает случайное s, запоминает его и передает $s \oplus y$.

Сложение:
A знает a_1, b_1, $a_1 \oplus a_2 = a$
B знает a_2, b_2, $b_1 \oplus b_2 = b$
Пусть $c_1 = (a_1 \oplus b_1)$, $c_2 = (a_2 \oplus b_2)$, тогда $c_1 \oplus c_2 = (a_1 \oplus b_1) \oplus (a_2 \oplus b_2) = a \oplus b$

Умножение:
A знает a_1, b_1, $a_1 \oplus a_2 = a$
B знает a_2, b_2, $b_1 \oplus b_2 = b$
Нужно:
A получил c_1 B получил c_2 такие, что $c_1 \oplus c_2 = (a_1 \oplus b_1) \bigwedge (a_2 \oplus b_2)$

A выбирает c_1 случайно
Вычисляет $\sigma_1 = c_1 \oplus a_1 \cdot b_1$ - для $a_2 = 0, b_2 = 0$
$\sigma_2 = c_1 \oplus a_1 \cdot (b_1 \oplus 1)$ - *для* $a_2 = 0, b_2 = 1$
$\sigma_3 = c_1 \oplus (a_1 \oplus 1) \cdot b_1$ - *для* $a_2 = 1, b_2 = 1$
$\sigma_4 = c_1 \oplus (a_1 \oplus 1) \cdot (b_1 \oplus 1)$ - *для* $a_2 = 1, b_2 = 1$
Итого A знает 4 варианта, B знает, какой из них нужен, вот и получается задача OT_1^4.

1.1 Протокол OT_1^k

S выбирает (α, τ) и посылает α. Где α - номер одностороней перестановки, τ - система для ее обращения.
R выбирает $x_1, \ldots, x_k \in D_\alpha$ - область определения перестановки f_α. И при $i \neq j \to y_j = x_j; i = j \to y_j = f_\alpha(x_i)$. Посылает $y_1, \ldots, y_k$.
S вычисляет $f_\alpha^{-1}(y_j)$, $\tau_j = \sigma_j \oplus b_j(z_j)$, где b_α - трудный бит. Отправляет $\tau_1, \ldots, \tau_k$.
Ответ: $\tau_i \oplus b(x_i)$