Криптография, Лекция № 13

8 декабря 2014 г.

Продолжая тему прошлой лекции сегодня поговорим об общем методе превращающем пртокол, надежный в получестной модели в протокол, надежный в общей модели.

Архитектура состоит из трех фаз:

1. Привязка ко входу (что-то такое отправить, после чего нельзя подменить вход)
2. Генерация общих случайных битов
3. Симуляция протокола из получестной модели (ключевой элемент - доказательства с нулевым разглашением)

Схемы привязки ($\rightarrow$ подбрасывание монетки по телефону) $\rightarrow$ ZKP ($\rightarrow$ передача занчения функции, когда принимающая сторона знает хеш $(\alpha, h(\alpha)) \mapsto (\varepsilon, f(\alpha))$) $\rightarrow$ ZKPoK $\rightarrow$ передача значения функции. Существует еще обобщенное подбрасывание монетки, авторизованные вычисления, привязка ко входу. Из этого всего получается итоговый протокол (здесь должна быть схема).

ZKP для языка $\{(u, v) : \exists \alpha\ h(\alpha) = u, f(\alpha) = v\}$
Передача значения: $(\alpha, 1^{|\alpha|}) \mapsto (\varepsilon, f(\alpha))$.
Авторизованные вычисления: $(\alpha, \beta) \mapsto if(\beta == h(\alpha)) \quad (\varepsilon, f(\alpha)) \quad else \quad (\varepsilon, (h(\alpha), f(\alpha)))$

0.1 Протокол

1. Первая сторона выбирает случайное $r' \in \{0,1\}^n, s \in \{0,1\}^{n^2}$
2. При помощи протокола передачи образа передается привязка $c_s(r')$
3. Обычным образом выбирается общее случайное r''.
4. Итоговое $r = r' \oplus r''$
5. Используется протокол авторизованных вычислений для $\alpha = (s, r', r'')$, $\beta = h(\alpha) = (c_s(r'), r'')$, $f(\alpha) = g(r' \oplus r'')$

Если все по честному, то протокол работает правильно. Что может плохого сделать первая сторона? Может выбирать r' не случайно, но ей все-равно придется привязаться, и она не сможет потом его поменять, тогда r'' будет

по честному случайным и, следовательно, r будет по честному случайным.

Привязка ко входу: $(x, 1^{|x|}) \mapsto (r, c_r(x))$, где r случайное из $\{0,1\}^n$.

Считаем, что $n = |x|$.

1. S выбирает случайное $r' \in \{0,1\}^{n^2}$
2. Протокол передачи значения: посылает привязку к x - $c_{r'}(x)$
3. При помощи обобщенного подбрасывания монетки S получает (r, r''), а R получает $c_{r''}(r)$. Здесь $r \in \{0,1\}^{n^2}$, $r'' \in \{0,1\}^{n^3}$
4. Авторизованные вычисления, где $\alpha = (x, r, r', r'')$, $\beta = h(\alpha) = (c_{r'}(x), c_{r''}(x))$, $f(\alpha) = c_r(x)$

Такая многоступенчатая схема нужна для невозможности подменить x и r.