Криптография, Лекция № 7

20 октября 2014 г.

1 Привязка к биту (bit commitment)

Немножко говорили об этом в курсе сложностей вычислений. Для начала нужно определить требования. Неформально: во-первых, нужно, чтобы нельзя было подменить бит (завешенный шторкой). Во-вторых, шторка не прозрачная - это сообщение, и по нему ничего нельзя понять про бит.

1.1 Неинтерактивный протокол

Definition 1.
Неинтерактивный протокол - пара (S, R). S, R - вероятностные полиномиальные алгоритмы. R может быть и детерминированным при условии, что S - полиномиальный в среднем. S получает бит; при помощи этого бита делает две вещи: c - привязку и k - ключ.

$$S\colon \sigma \mapsto c, k$$

$$R\colon c, k \mapsto \{0, 1, \perp\}$$

Требования:

1. $R(c_\sigma, k_\sigma) = \sigma$ (в вероятностном случае вероятсность стремится быстрее любого полинома). Это требование в интересах получателя.

2. $R(c_\sigma, k^*) \in \{\sigma, \perp\}$ - так же требование получателя.

3. c_0 и c_1 - вычислительно не отличимы. (Из первых двух требований следует, что c_0 и c_1 должны принимать значения из разных множеств).

Конструкция на базе одностороneей перестановки. Если есть одностороняя перестановка, то можно построить перестановку с трудным битом. Пусть g - односторонняя перестановка, а h - трудный бит. Тогда:

$$c_\sigma = (\sigma \oplus h(x), g(x))$$

$$k_\sigma = x$$

Из-за того, что h - трудный бит, $(h(x), g(x))$ вычислительно не отличимо от $(r, g(x))$, то $(\sigma \oplus h(x), g(x))$ вычислительно не отличимо от $(\sigma \oplus r, g(x))$, что не отличимо от $(r, g(x))$. Отсюда следует c_0 вычислительно не отличимо от c_1.

$$R((b,y),k) = \begin{cases} b \oplus h(k) & \text{при } g(k) = y \\ \perp & \text{при } g(k) \neq y \end{cases}$$

g - перестановка, следовательно $g(k) \neq g(k')$ при $k \neq k'$.

1.2 Интерактивный протокол

В предыдущем подходе получатель играл пассивную роль. Построем протокол в котором он будет что-то делать.

Definition 2.
Интерактивный протокол - 3 алгоритма: R, S, T. R, S - вероятностные полиномиальные алгоритмы. T - детерминированный полиномиальный алгоритм, котороый получает протокол общения и должен сказать, что же там было запечатано. Он возвращает $0, 1$ либо ошибки $\perp_R, \perp_S$.

2 фазы протокола:

1. Привязка. $<R, S(\sigma)>$ - протокол общения R и S.
2. Раскрытие. S посылает свои биты S.

Требования:

1. $T(<R, S(\sigma)>, S) = \sigma$ - требование корректности.
2. $T(<R^*, S(\sigma)>, s) \in \{\sigma, \perp_R\}$ - усиленная корректность. (Жульничующий R не может заставить S привязаться к другому биту).
3. $\forall S^* \ \exists \sigma^* \ \forall s^* \ T(<R, S^*>, S^*) \in \{\sigma^*, \perp_S\}$ - требование надежности.
4. $<R^*, S(0)>$ и $<R^*, S(1)>$ вычислительно не отличимы. (До раскрытия R ничего не узнает о бите, то есть все, что он увидит будет вычислительно неотличимо друг от друга.)

Конструкция на базе генератора $G\colon \{0,1\}^n \mapsto \{0,1\}^{3n}$:

$$S \xleftarrow{r \in \{0,1\}^{3n}} R, \text{ r - случайное}$$

S выбирает случайное $s \in \{0,1\}^n$

$$S \longrightarrow R$$

T получает q - сообщение R, m - сообщение S, s - случайные биты S.

$$T(q,m,s) = \begin{cases} 0 & \text{при } m \oplus G(s) = 0^{3n} \\ 1 & \text{при } m \oplus G(s) = q \\ \perp_S & \text{иначе} \end{cases}$$

Вычислительная неотличимость: $(q, G(s)) \sim (q, t) \sim (q, t \oplus q) \sim (q, G(s) \oplus q)$, где t - случайное, длины $3n$.

Надежность - выполнена с вероятностью (по $r \in \{0,1\}^{3n}$) не меньше $1 - \frac{1}{2^n}$.
Покажем это рассмотрев неоднозначное раскрытие:
$\exists s_1 \; m \oplus G(s_1) = 0^{3n}$ и $\exists s_2 \; m \oplus G(s_2) = r$.
При выполнении обоих условий $\exists s_1, s_2 \; G(s_1) \oplus G(s_2) = r$. Вероятность этого не превосходит $\frac{2^{2n}}{2^{3n}} = 2^{-n}$.

1.3 Интерактивное получение бита

3 алгоритма: A, B, J. Первые два - детерминированные полиномиальные, последний - детерминированный. $J\colon \; <A, B> \mapsto \{a, b\}$.

$$\forall B^* \; \forall p \; \exists N \; \forall n > N \; Pr\{J(<A, B^*>) = a\} \geq \frac{1}{2} - \frac{1}{p(n)}$$

$$\forall A^* \; \forall p \; \exists N \; \forall n > N \; Pr\{J(<A^*, B>) = a\} \geq \frac{1}{2} - \frac{1}{p(n)}$$

$\sigma \in \{0,1\}$ - случайный бит.

$$A \xrightarrow{c_\sigma} R, \text{ r - случайное}$$

B выбирает случайное $\tau \in \{0,1\}$.

$$A \xleftarrow{\tau} B$$

$$A \xrightarrow{k_\sigma} B$$

$$J(c, \tau, k) = \begin{cases} a & \text{при } \tau \oplus R(c,k) = 0 \\ b & \text{при } \tau \oplus R(c,k) = 1 \\ & \text{при } R(c,k) = 1 \end{cases}$$

Если бы не было вычислительных ограничений, то выиграл бы B.