Криптография, Лекция № 10

17 ноября 2014 г.

Продолжаем разговор о протоколах электронной подписи с открытым ключом. Две стороны подписывающий, проверяющий, у подписывающего есть закрытый ключ, у проверяющего - открытый. Хотим уметь проверять подпись подписывающего; неправильную подпись хотим уметь почти наверное отвергать. Сегодня поговорим о кодировании сообщений произвольной длины.

Idea 1. *(Одноразового протокола)*
Вводится семейство хэш-функций:

$$h_s \colon \{0,1\}^* \to \{0,1\}^{l(n)}$$

S вычисляет $h_s(x)$. Открытый ключ - (e,s), закрытый ключ - (d,s). Подпись - пара $(h_s(x)$, подпись под$h_s(x)$при помощи ключа $d)$. Если враг сумел взломать подпись, то либо он смог взломать хэш-функцию(нашел коллизию), либо взломал вторую подпись.

Idea 2. *(Многоразового протокола ("с памятью"))*
Вместе с каждым сообщением посылается открытый ключ для проверки следующего сообщения. Тогда получается, если взломщик взломал такую подпись, то он либо взломал одноразовую подпись, либо взломал генерацию ключей. Если мы подписываем биты одного сообщения, то взломщик мог подписать префикс сообщения. Для избежания этого можно использовать бесперфиксное кодирование. Схема: (слово $\to$ беспрефиксный код $\to$ сообщения фиксированной длины $\to$ посылка).

Definition 1. (Семейства хэш-функций с трудно отыскиваемыми коллизиями (collision-free)) По номеру функции трудно найти x, x', такие, что значения на них соответсвующей функции совпадают.

$$\forall C_n \ \forall p \ \forall^\infty n \ Pr_s\{C_n(s) = (x,x') \colon h_s(x) = h_s(x')\} < \frac{1}{p(n)}$$

где C_n - схема полиномиального размера. $s \in \{0,1\}^{k(n)}$, где $k(n)$ - некоторый полином. Вероятность берется по некоторому априорному распределению, такому же как и в протоколе.

Claim 1.
Такого семейства достаточно для надежной схемы электронной подписи одного сообщения произвольной длины.

Если есть взломщик подписи, имеющий открытый ключ e, идекс функции s. Генерирует x, получает $h_s(x)$ и подпись под $h_s(x)$, генерирует x' и фальшивую подпись.

C_n получает s, генерирует пару (d, e), генерирует x, генерирует $h_s(x)$ и подпись при помощи d, генерирует x' как взломщик и фальшивую подпись.

Либо $x \neq x'$ и $h_s(x) = h_s(x')$, тогда взломали хэш-функцию, либо $h_s(x) \neq h_s(x')$ тогда взломали электронную подпись.

Откуда можно брать такие семейства функций?

Definition 2.

$$f_s^0 \colon \{0,1\}^{m(n)} \to \{0,1\}^{l(n)}$$
$$f_s^1 \colon \{0,1\}^{m(n)} \to \{0,1\}^{l(n)}$$

Зацепление в системе $\{f_s\}$ - пара (x, y) такая, что $f_s^0(x) = f_s^1(y)$.

Definition 3. (Семейства функций с трудно отыскиваемыми зацеплениями (claw-free))

$$\forall C_n \ \forall p \ \forall^\infty n \ Pr_s\{C_n(s) = (x,y) \colon (x,y) - \text{зацепление}\} < \frac{1}{p(n)}$$

Claim 2.
По системе с трудно отыскиваемыми зацеплениями можно построить систему с трудно отыскиваемыми коллизиями.

Доказательство.
$x \mapsto \hat{x}$ - беспрефиксный код. Для любого кодового слова $\beta_s \in D_s$.

$$h_s(x) = f_s^{\hat{x}_1}(f_s^{\hat{x}_2}(\ldots(f_s^{\hat{x}_p}(\beta_s))\ldots))$$

$$h_s(x) = h_s(x'), x \neq x' \Rightarrow \exists i \ \hat{x}_i \neq \hat{x}'_j$$

□

Claim 3.
По "односторонней"функции Рабина можно построить систему функций с трудно отыскиваемыми зацеплениями.

Доказательство.

$$f_{x,m}^0(y) = x \cdot y^2 \ (mod \ m)$$
$$f_{x,m}^1(y) = y^2 \ (mod \ m)$$

Если $f_{x,m}^0(y) = f_{x,m}^1(z)$, то $x \cdot y^2 = z^2 \ (mod \ m)$. Отсюда $(\frac{z}{y})^2 = x$, можно извлечь корень и получить противоречие с необратимостью функции Рабина. □

1 Альтернативные концепции хэш-функций

Definition 4. (Универсальное семейство односторонних хэш-функций)

$$h_s \colon \{0,1\}^{p(n)} \to \{0,1\}^n$$

Отличие в полиноме.

Еще одно отличие - ограничение на поиск коллизий

Definition 5. (Семейства универсальных хэш-функций с трудно отыскиваемыми коллизиями)

$$\forall C_n \ \forall p \ \forall \{x_n\} \ \forall^\infty n \ Pr_s\{h_s(x_n) = h_s(C_n(s))\} < \frac{1}{p(n)}$$

То есть универсальное семейство - более слабая концепция.

Theorem 1. *(б/д)*
Если существует односторонняя функция, то существует универсальное семейство.

Theorem 2. *(б/д)*
Если существует односторонняя перестановка, то существует универсальное семейство.

1.1 Конструкция одноразовой подписи одного сообщения произвольной длины на базе универсального семейства

Идея такая, как мы обсуждали в начале. Есть (S, V) - протокол надежной одноразовой подписи сообщения длины $n+1$. Строим $(\hat{S}, \hat{V})$. $\hat{S}$ генерирует $(e_2, d_2), \ldots, (e_m, d_m)$. Исходные ключи - $(d, s), (e, s)$. Подпись под $(\sigma_1 \ldots \sigma_m)$:

$$(e_2, e_3, \ldots, e_n, S(d, h_s(e_2)\sigma_1), S(d_2, h_s(e_3)\sigma_2), \ldots, S(d_m, h_s(e_{m+1})\sigma_m))$$