Лекция 9

Электронные подписи

(Конспект: Ю. Беляева)

В этой лекции будет рассказано о построении электронного аналога «обычной» подписи ручкой на бумажном документе.

9.1 «Одноразовая» электронная подпись

Мы говорим об электронной подписи как об одноразовой в том смысле, что описываемые далее протоколы будут надёжными при условии, что взломщик может «попросить» подписать ровно одно сообщение, и будет взламывать протокол зная только подпись этого одного сообщения.

9.1.1 Электронная подпись одного бита

Определение 9.1. Пусть есть тройка алгоритмов (G, S, V) с параметром надёжности n (который далее будет часто опускаться), где G — вероятностный полиномиальный алгоритм, а S и V — детерминированные полиномиальные алгоритмы. При этом:

- $G(1^n) = (e_n, d_n)$, G — *генератор ключей*, e_n — *открытый ключ*, d_n — *секретный ключ*;
- $S(\sigma, e_n, d_n) = s$, S — *подписывающий алгоритм*, $\sigma \in \{0, 1\}$ — подписываемое сообщение (состоящее из одного бита), s — подпись сообщения (строка);
- $V(\sigma, s, e_n) \in \{0, 1\}$, V — *проверяющий алгоритм*, возвращает 1, если подпись верна, 0 — иначе.

Тройка (G, S, V) называется протоколом электронной подписи одного бита, если выполняются следующие свойства:

1. Корректная подпись успешно проходит проверку т.е. $V(\sigma, S(\sigma, e_n, d_n), e_n) = 1$.

2. Ни один противник не может подделать подпись. В данном случае противник это пара семейств вероятностных схем C_n, D_n. Схема C_n по открытому ключу генерирует бит $\sigma = C_n(e_n) \in \{0,1\}$. Подписывающий алгоритм S подписывает этот бит $S(\sigma, e_n, d_n) = s$. После этого схема D_n зная подпись бита σ должна получить подпись бита $\overline{\sigma}$: $D_n(e_n, \sigma, s) = s'$. Необходимо чтобы $\forall C_n, D_n$ вероятность принятия проверяющим алгоритмом строки s' в качестве подписи $\overline{\sigma}$ была пренебрежимо мала: для любого полинома p начиная с некоторого n было бы верно $\Pr[V(\overline{\sigma}, s', e_n) = 1] \leq \frac{1}{p(n)}$.

Замечание 9.1. До этого момента в этом курсе все противники были не схемами, а алгоритмами. Однако замена алгоритмов на схемы в большинстве случаев не изменит приведённых доказательств.

Замечание 9.2. Подписывание и проверку можно считать детерминированными («зашив» в схемы «самые лучшие» случайные биты).

Теорема 9.1. *Если существуют односторонние функции, то существует протокол электронной подписи одного бита.*

Доказательство. Пусть $f : \{0,1\}^n \to \{0,1\}^n$ — односторонняя функция. Построим протокол следующим образом. Секретным ключом будут пара строк $d_0, d_1 \leftarrow U_n$. Открытым ключом будет пара строк e_0, e_1, где $e_0 = f(d_0)$, $e_1 = f(d_1)$. Подписывающий алгоритм S получает на вход бит $\sigma \in \{0,1\}$ и возвращает его подпись $d_\sigma = S(\sigma, d_0, d_1)$ (т.е. подписывающий алгоритм открывает половину секретного ключа). Проверяющий алгоритм V для проверки подписи s применят функцию f к подписи и сравнивает результат с e_σ, а именно $V(\sigma, s, e_0, e_1) = (f(s) == e_\sigma)$.

Проверим, что этот протокол надёжен. Допустим, что протокол взламывается парой схем C_n, D_n. Тогда существует полином p, такой что для бесконечной последовательности длин входов n вероятность того, что схема D_n угадает подпись s', будет больше чем $\frac{1}{p(n)}$. В части этих случаев, схема C_n сгенерирует бит $\sigma = 0$ (т.е. D_n будет угадывать подпись 1), в оставшихся случаях C_n сгенерирует 1 (и D_n будет подписывать 0). Тогда:

$$\begin{aligned}\frac{1}{p(n)} \leq \Pr[V(\overline{\sigma}, s', e_0, e_1) = 1] = \\ = \Pr[(V(0, s', e_0, e_1) = 1) \wedge (\sigma = 1)] + \Pr[(V(1, s', e_0, e_1) = 1) \wedge (\sigma = 0)] \leq \\ \leq \Pr[f(D_n(e_0, 1, f(e_1))) = e_0] + \Pr[f(D_n(e_1, 0, f(e_0))) = e_1].\end{aligned}$$

Для того, чтобы неравенство было выполнено, одна из вероятностей в последней сумме должна быть больше, чем $\frac{1}{2 \cdot p(n)}$. Так как данное неравенство должно выполняться для бесконечного числа n, то одно из слагаемых в последней сумме окажется больше чем $\frac{1}{2 \cdot p(n)}$ бесконечное число раз. Допустим, это первое слагаемое. Т.е. для бесконечного числа n при помощи схемы D_n мы сможем с вероятностью $\frac{1}{2 \cdot p(n)}$ обратить функцию f, вычисляя $D_n(e_0, 1, f(e_1))$, что противоречит односторонности функции f. □

9.1.2 Электронная подпись фиксированного числа битов

Электронная подпись фиксированного числа битов позволяет подписывать сообщения длины $p(n)$, где p — это фиксированный полином.

Определение 9.2. Электронная подпись фиксированного числа бит определяется аналогично электронной подписи одного бита (см. определение 9.1). Кроме алгоритмов G, S, V и параметра надёжности n в определение входит полином p, задающий длину подписываемого сообщения. Таким образом, подписывающий алгоритм S принимает на вход в качестве сообщения не один бит, а $p(n)$. Протокол электронной подписи фиксированного числа битов должен удовлетворять следующим свойствам:

1. Корректная подпись успешно проходит проверку т.е. $V(\sigma, S(\sigma, e_n, d_n), e_n) = 1$ (аналогично свойству 1 протокола подписи одного бита).

2. Ни один противник не может подделать подпись. К паре семейств вероятностных схем C_n, D_n из определения 9.1 добавляется третье семейство E_n, отвечающее за генерацию сообщений, взламываемых данным противником. Схема C_n по открытому ключу e_n генерирует сообщение $x \in \{0,1\}^{p(n)}$, которое подаётся на вход подписывающему алгоритму S: $S(x, e_n, d_n) = s$. По подписи s схема E_n генерирует строку $x' = E(x, s, e_n) \in \{0,1\}^{p(n)}$. Схема D_n должна получить подпись сообщения x': $D_n(e_n, x, s, x') = s'$. Необходимо чтобы для любых C_n, D_n, E_n вероятность того, что s' есть корректная подпись строки x' была пренебрежимо мала: для любого полинома q начиная с некоторого n верно $\Pr[(x \neq x') \wedge (V(x', s', e_n) = 1)] \leq \frac{1}{q(n)}$.

Теорема 9.2. *Если существует протокол электронной подписи одного бита, то существует протокол подписи фиксированного числа битов.*

Доказательство. Пусть G, S, V — протокол электронной подписи одного бита. Используя его будем строить протокол электронной подписи $p(n)$ бит. Сгенерируем при помощи G $p(n)$ пар ключей $(e^{(1)}, d^{(1)}), \ldots (e^{(p(n))}, d^{(p(n))})$. Открытым ключом нового протокола будет набор $e = e^{(1)}, \ldots, e^{(p(n))}$, секретным ключом — $d = d^{(1)}, \ldots, d^{(p(n))}$. Новый протокол будет подписывать каждый бит сообщения по отдельности при помощи своей пары ключей:

$$S'(x, e, d) = S'(x_1, \ldots, x_{p(n)}, e, d) = S(x_1, e^{(1)}, d^{(1)}) S(x_2, e^{(2)}, d^{(2)}) \ldots S(x_{p(n)}, e^{(p(n))}, d^{(p(n))}).$$

Верификация подписи будет также производиться по отдельности для каждого бита сообщения.

Докажем, что это надёжный протокол. Допустим что для этого протокола есть взломщик — схемы C_n, D_n, E_n. Существует полином q такой что для бесконечного числа номеров n выполняется соотношение

$$\frac{1}{q(n)} \leq \Pr[(x \neq x') \wedge (V'(x', s', e_n) = 1)] \leq \sum_{i=1}^{p(n)} \Pr[(x_i \neq x'_i) \wedge (V'(x', s', e_n) = 1)],$$

где x и x' строки, сгенерированные C_n и E_n. Существует индекс i, для которого для бесконечно большого числа номеров n строки x и x' будут отличаться в бите i и при этом соответствующее слагаемое в последней сумме будет как минимум $\frac{1}{p(n)q(n)}$. Пользуясь этим фактом, построим взломщика C'_n, D'_n для протокола электронной подписи одного бита следующим образом.

Допустим мы хотим взломать протокол электронной подписи одного бита S,V с открытым ключом $\widetilde{e}$. Сгенерируем $p(n)-1$ пар ключей для протокола электронной подписи одного бита $(e^{(1)}, d^{(1)}), \dots (e^{(p(n)-1)}, d^{(p(n)-1)})$. Из них составим ключи e, d для протокола электронной подписи фиксированного числа бит:

$$e = e^{(1)}, \dots, e^{(i-1)}, \quad \widetilde{e}, e^{(i)}, \dots, e^{(p(n)-1)}$$
$$d = d^{(1)}, \dots, d^{(i-1)}, \quad \widetilde{d}, d^{(i)}, \dots, d^{(p(n)-1)}$$

Здесь $\widetilde{d}$ — это некая строка, содержание которой нам неважно. Схема C'_n будет возвращать i-й бит x_i строки $x = C_n(e)$. Допустим, $s = S'(x, e, d)$. Заметим, что подпись бита i этой строке «не правильна»: секретный ключ $\widetilde{d}$ не соответствует открытому $\widetilde{e}$. Поэтому часть, соответствующую подписи бита i в строке s, заменим на $S(x_i)$. Обозначим получившуюся строку $\widetilde{s}$.

Теперь схема D'_n должна угадать подпись бита $\overline{x_i}$. Для этого, при помощи E_n будет генерироваться строка x' и подписываться запуском $D_n(e, x, \widetilde{s}, x') = s'$. В бесконечном числе случаев с вероятностью не менее $\frac{1}{p(n)q(n)}$ в i-й позиции строки s' будет стоять верная подпись бита $\overline{x_i}$, что противоречит предположению о надёжности протокола электронной подписи одного бита. □

9.1.3 Электронная подпись сообщения произвольной длины

От электронной подписи фиксированного числа битов перейдём к подписи произвольного числа битов. Протоколы подписи произвольного числа битов могут подписывать сообщения произвольной полиномиально ограниченной длины. Для построения такого протокола понадобится понятие *семейство хеш-функций с труднообнаружимыми коллизиями (СТОК)*. Неформально говоря, хочется построить функцию h, для которой было бы сложно обнаружить пару (x, y) такую что $x \neq y$ и при этом $h(x) = h(y)$ (подобные пары называются *коллизиями*).

Определение 9.3. Пусть есть полиномиально вычислимая функция $h : \{0,1\}^{l(n)} \times \{0,1\}^* \to \{0,1\}^{k(n)}$. Множество $\{0,1\}^{l(n)}$ называется *индексным множеством*. Пусть α_n — полиномиально моделируемое распределение на индексном множестве. h называется *семейством хеш-функций с труднообнаружимыми коллизиями*, если для любого семейства вероятностных схем C_n вероятность того, что $C_n(\alpha) = (x, y)$ $(x \neq y)$ и $h(\alpha, x) = h(\alpha, y)$ (где α берётся случайно из α_n) пренебрежимо мала.

Замечание 9.3. Из того что h полиномиально вычислима следует, что функции l и k полиномиально ограничены.

Теорема 9.3. *Если существуют $h : \{0,1\}^{l(n)} \times \{0,1\}^* \to \{0,1\}^{k(n)}$ — СТОК и протокол электронной подписи сообщений из $k(n)$ бит, то существует протокол электронной подписи сообщений произвольной длины.*

Доказательство. Пусть e_n, d_n — открытый и закрытый ключи протокола подписи сообщений из $k(n)$ бит, а S и V его подписывающий и проверяющий алгоритмы. Пусть α случайно взятая величина из индексного множества СТОКа α_n. Открытый ключ нашего нового протокола есть пара (e_n, α), а секретный — пара (d_n, α). Подписывающий алгоритм $\widetilde{S}$ вычисляет хеш от подписываемой строки x и отдаёт его на подпись алгоритму S:

$$s = \widetilde{S}(x, e_n, \alpha, d_n) = S(h(\alpha, x), e_n, d_n).$$

Проверяющий алгоритм $\widetilde{V}$ также проверят хеш:

$$\widetilde{V}(x, s, e_n, \alpha) = V(h(\alpha, x), s, e_n).$$

Допустим для такого протокола существует взломщик — схемы C_n, D_n, E_n и полином q, такие что для бесконечно большого числа n выполнено $\Pr[(x \neq x') \wedge (V(h(\alpha, x'), s', e_n) = 1)] \geq \frac{1}{q(n)}$, где x, x', s' сгенерированы взломщиком. Заметим, что если хеши x и x' совпали, то взломщик уже знает, чему равна подпись x', т.к. она равна подписи x. Поэтому распишем вероятность взлома следующим образом:

$$\frac{1}{q(n)} \leq \Pr[(x \neq x') \wedge (V(h(\alpha, x'), s', e_n) = 1)] =$$
$$= \Pr[h(x) = h(x')] + \Pr[(x \neq x') \wedge (V(h(\alpha, x'), s', e_n) = 1) \wedge (h(x) \neq h(x'))].$$

Это означает, что для бесконечного числа n с вероятностью не менее $\frac{1}{2 \cdot q(n)}$ выполняется один из следующих вариантов:

- $h(\alpha, x) = h(\alpha, x')$. Значит, для h можно с большой вероятностью находить коллизии, а это противоречит тому, что h — СТОК.
- $h(\alpha, x) \neq h(\alpha, x')$ и при этом $V(h(\alpha, x), s', e_n) = 1$. Таким образом, мы получили способ, имея подпись строки $h(\alpha, x)$, с большой вероятностью находить подпись другой строки $h(\alpha, x')$, т.е. мы научились взламывать протокол электронной подписи сообщений фиксированной длины, что противоречит надёжности этого протокола.

□

9.1.4 Построение СТОКов и СТОЗов

В разделе 9.1.3 для построения электронной подписи сообщений электронной длины использовались СТОКи. СТОК можно построить, имея *семейство перестановок с труднообнаружимыми зацеплениями (СТОЗ)*.

Определение 9.4. Пусть $f : \{0,1\} \times \{0,1\}^{l(n)} \times \{0,1\}^n \to \{0,1\}^n$. Как и в определении СТОКа, множество $\{0,1\}^{l(n)}$ названется *индексным*. Пусть $\alpha_n \subset \{0,1\}^{l(n)}$ — множество индексов (вычисляемое полиномиальным вероятностным алгоритмом) и $\forall \alpha \in \alpha_n$ функции f^0_α, f^1_α являются перестановками множества $D_\alpha \in \{0,1\}^n$, вычислимыми за полиномиальное время. *Зацеплением* для индекса α называется пара (x, y) такая что

$f^0_\alpha(x) = f^1_\alpha(y)$. Говорят, что f задаёт *семейством перестановок с труднообнаружимыми зацеплениями*, если для любого семейства вероятностных схем C_n вероятность того что $C_n(\alpha) = (x, y)$ и $f^0_\alpha(x) = f^1_\alpha(y)$ пренебрежимо мала при $\alpha \in \alpha_n$.

Утверждение 9.1. *Если существует СТОЗ, то существует и СТОК.*

Доказательство. Пусть f — СТОЗ. Рассмотрим строку $x = x_1 \dots x_n$ и её префиксный код $\hat{x} = x_1 x_1 \dots x_n x_n 01 = \hat{x}_1 \hat{x}_2 \dots \hat{x}_l$. Рассмотрим функцию

$$h_t(x) = f_t^{\hat{x}_1}(f_t^{\hat{x}_2}(\dots(f_t^{\hat{x}_l}(\beta_t)))),$$

где $t \in \alpha_n$ — некоторый индекс из индексного множества функции f, $\beta_t \in D_t$ — фиксированная величина для данного t.

Докажем, что h является СТОКом. Действительно, пусть h не СТОК и значит, существует схема C_n, которая с большой вероятностью находит коллизии для h. Допустим что (x, y) — коллизия, найденная этой схемой для индекса t. Не умоляя общности, можно предполагать, что x отличается от y уже в первом бите, т.к. одинаковые биты в начале обеих строк можно просто отбросить (мы считаем, что обе строки закодированы префиксным кодом). Пусть x начинается с единицы, а y с нуля. Тогда

$$f_t^1(f_t^{\hat{x}_2}(\dots(f_t^{\hat{x}_l}(\beta_t)))) = f_t^0(f_t^{\hat{y}_2}(\dots(f_t^{\hat{y}_l}(\beta_t)))).$$

Это означает, что пара

$$(f_t^{\hat{x}_2}(\dots(f_t^{\hat{x}_l}(\beta_t))), f_t^{\hat{x}_2}(\dots(f_t^{\hat{x}_l}(\beta_t))))$$

является зацеплением для f для индекса t. Таким образом, при помощи схемы C_n можно с большой вероятностью находить зацепления для f, а это противоречит тому факту, что f — СТОЗ. □

Для построения СТОЗа нам понадобится *функция Рабина*.

Определение 9.5. Пусть $m = p \cdot q$, где $p, q \in \mathbb{P}$ имеют вид $4k + 3$. Тогда *функцией Рабина* называется функция $f_m(x) = x^2 \pmod m$.

Утверждение 9.2. *Функция Рабина f_m задаёт перестановку на множестве квадратичных вычетов по модулю m.*

Теорема 9.4. *Если функция Рабина односторонняя, то СТОЗ существует.*

Доказательство. Пусть f_m — функция Рабина. Рассмотрим множество D_m — множество квадратичных вычетов по модулю m, взаимнопростых с m. Рассмотрим пару функций:

$$\begin{cases} f^0_{m,x}(y) &= xy^2 \pmod m, \\ f^1_{m,x}(y) &= y^2 \pmod m, \quad \text{где } x, y \in D_m. \end{cases}$$

Докажем, что данная пара функций является СТОЗом (m и x — индексы, y — аргумент). Допустим что существует вероятностная схема C_n, которая находит зацепления для этой пары. Пусть y_1, y_2 — зацепление для некоторых x и m. Тогда $xy_1^2 \equiv y_2^2 \pmod m$. Значит $x \equiv \left(\frac{y_2}{y_1}\right)^2 \pmod m$. Т.е. схема C_n обращает функцию Рабина, что противоречит условию теоремы. □