Лекция 4

Понятие совместной ЦП

Определение

В некоторых случаях требуется, чтобы сообщение m было одновременно подписано несколькими агентами $A_1, A_2, ..., A_k$. Соответствующая ЦП называется **совместной ЦП** и обозначается $< m >^s_{A_1...A_k}$.

Примеры совместной ЦП

Примеры

1. $< m >^s_{A_1...A_k} = (< m >^s_{A_1}, ..., < m >^s_{A_k})$;
2. $< m >^s_{A_1...A_k} = {A_k}^-(...({A_1}^-(h(m)))...)$ (в данном случае агенты $A_1, A_2, ..., A_k$ используют общий алгоритм симметричного шифрования;
3. параметры: открытые $n, u \in N$, ХФ h со значениями в Z_u,
   $\forall i = 1, ..., k \qquad s_{A_i} \in_r Z^*_n, \qquad v_{A_i} = {s_{A_i}}^{-u}$.
   $< m >^s_{A_1...A_k} = (c, d)$, где $\qquad c = h(m, r_1^u ... r_k^u)$,
   $d = r_1 s^c_{A_1} ... r^k s^c_{A_k}, \qquad \forall i = 1, ..., k \qquad r_i \in_r Z_n \backslash \{0\}$.

Проверка подлинности: $c = h(m, d^u v^c_{A_1} ... v^c_{A_k})$.

Совместная ЦП Брикелла – Ли – Якоби

Параметры

простое число p,
элемент $g \in Z_p^*$ порядка $p-1$,
большое $l \in N$,
ХФ h,
$\forall i = 1, ..., k \qquad s_{A_i} = \{s_{i1}, ..., s_{il}\}$,
$v_{A_i} = \{v_{i1}, ..., v_{il}\}$, где
$\forall j = 1, ..., l \qquad s_{ij} \in_r Z_{p-1}, \qquad v_{ij} = g^{-s_{ij}}$.

Совместная ЦП Брикелла – Ли – Якоби

В вычислении ЦП $< m >^s_{A_1,...,A_k}$ принимает участие доверенный посредник I, с которым элементы $A_1, ..., A_k$ могут обмениваться сообщениями с использованием общего алгоритма симметричного шифрования.

Совместная ЦП Брикелла – Ли – Якоби

Протокол вычисления $< m >^{s}_{A_1,...,A_k}$:

$$\forall i = 1, ..., k \quad A_i \to I: \qquad I^{+}(y_i), \qquad y_i = g^{r_i}, \qquad x_i \in_r Z_{p-1},$$

$$I \to \{A_1, ..., A_k\}: \qquad y = y_1 ... y_k;$$

$$A_i \to I: \qquad z_i = x_i + \sum_{j \in \{1,...,l\},\, b_j = 1} s_{ij}, \qquad b_j — \text{ i-й бит } g^{h}(m, y, A),$$

где A — конкатенация (объединение) имен агентов $A_1, ..., A_k$;

$$I: \qquad < m >^{s}_{A_1,...,A_k} = z = \sum_{i=1}^{k} z_i.$$

Совместная ЦП Брикелла – Ли – Якоби

Проверка подлинности:

$$g^{z} \prod_{i=1}^{k} \prod_{j \in \{1,...,l\},\, b_j = 1} v_{ij} = y.$$

Замечание.

Данный протокол обеспечивает нулевое разглашение $s_{A_1}, ..., s_{A_k}$. Если совместная ЦП не может быть создана по причине того, что некоторые агенты отказались вносить свой вклад в ее создание, в то время как другие агенты свой вклад уже внесли, то по результату работы агентов, внесших вклад в создание общей ЦП, невозможно идентифицировать этих агентов.