Криптографические протоколы

Лекция 9
Протоколы распределения ключей (Часть 2). Предварительное распределение ключей

Деркач Максим Юрьевич

November 13, 2019

Ссылки

https://habr.com/en/post/431392/

Предварительное распределение ключей нужно для уменьшения объёма распределяемой и хранимой информации.

$A_1, ..., A_n$ - абоненты.
K - множество ключей.
P - множество исходных ключевых параметров (p_i - пароль каждого абонента).
Q - множество значений ключевых материалов абонентов (q_i - секрет каждого абонента).
R - множество значений открытой информации ($r_1, ..., r_n$ - в открытом доступе).

Схема предварительного распределения ключей:
$S(n) = (K, P, Q, R, A_0, A_1)$

1. $A_0 : P \times R -> Q$ - алгоритм формирования секретных ключевых материалов.
   $A_0(p_i, r_i) = q_i, \; 1 \leq i \leq n$
2. $A_1 : Q \times R -> K$ - алгоритм вычисления ключа парной связи.
   $A_1(q_i, r_j) = A_1(q_j, r_i)$,
   $K_{ij} = A_1(q_i, r_j), i = j$: либо не рассматривается либо некий личный секретный ключ.

$A_0(p, r_i) = Q_i \subseteq K^{t_i} \subseteq Q, \; 1 \leq i \leq n$

Предложение 1
$\forall r_i \in R,\ q_i \in Q,\ 1 \leq i \leq n$
$A_0(p, r_i) = q_i$ - имеет одинаковое число решений относительно $p \in P$.

Предложение 2
$\forall r_i \in R,\ k \in K,\ 1 \leq i \leq n$
$A_1(q_i, r_i) = k$ - имеет одинаковое число решений относительно $q_i \in Q$.

Схема Шамира

Схема разделения секрета, широко используемая в криптографии.
Схема Шамира позволяет реализовать (k, n) — пороговое разделение секретного сообщения (секрета) между n сторонами так, чтобы только любые k и более сторон $(k \leq n)$могли восстановить секрет. При этом любые $k - 1$ и менее сторон не смогут восстановить секрет.

Первая фаза:

M - секрет, $S(k, n)$ - пороговая схема разделения секрета.

p - простое , $p > M$, p - известно всем участникам протокола

$F(x) = (a_{k-1}x^{k-1} + ... + a_1 x + M)$ mod p - многочлен над полем Z_p

Генерация секрета:

$q_i = A_0^i = F(i)$ - генерация долей серкрета

Аргументы многочлена (номера секретов) не обязательно должны идти по порядку, главное — чтобы все они были различны по модулю p.

После этого каждой стороне, участвующей в разделении секрета, выдаётся доля секрета — q_i вместе с номером i.

Помимо этого, всем сторонам сообщается степень многочлена $k-1$ размер поля p.

Случайные коэффициенты $a_{k-1}, \ldots, a_1$ и сам секрет M удаляються.

Восстановление секрета:

Теперь любые k участников, зная координаты k различных точек многочлена, смогут восстановить многочлен и все его коэффициенты, включая последний из них — разделяемый секрет.

$F(x) = \sum_i L_i(x) y_i \ mod \ p,$
$L_i(x) = \prod_{i \neq j} \frac{x - x_j}{x_i - x_j} \ mod \ p,$
где $(x_i, y_i) \equiv (i, q_i)$ - координаты точек многочлена.

Инициализация:

F - конечное поле, имеющее достаточно большое число элементов(n элементов).

Доверенная сторона (центр распределния) выбирает следующие секретные материалы: $1 \leq m \leq n-2,\ a_{st}$ - секретные материалы, хранимые только в центре распределения.

И строит на их основе полином:
$f(x,y) = \sum_{s=0}^{m} \sum_{t=0}^{m} a_{st} x^s y^t,\ \ a_{st} = a_{ts},\ \ s \neq t,\ \ s,t = 0, ..., m$

Добавление участника:

Когда новый участник хочет присоединиться к группе, доверенная сторона выбирает для него новый открытый ключ r_i. Далее доверенная сторона вычисляет закрытый ключ q_i:

$$q_i = (a_0^{(i)}, a_1^{(i)}, \dots, a_m^{(i)})$$
$$q_i(x) = f(x, r_i) = a_0^{(i)} + a_1^{(i)} x + \dots + a_m^{(i)} x^m$$

Открытый и закрытый ключ сообщаются участнику по надёжному каналу без прослушивания.

Установление сессии:

$$K_{ij} = K_{ji} = f(r_i, r_j) = q_i(r_j) = q_j(r_i)$$

A_i хранит $m+1$ значение ключевых паролей.
Схема Блома является стойкой к m-кратной компрометации ключей.