

Криптографические протоколы

Лекция 9

Протоколы распределения ключей (Часть 2).
Предварительное распределение ключей/Распределение
ключевой информации

Деркач Максим Юрьевич

November 2, 2020

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

Предварительное распределение ключей

Основные понятия и свойства

Предварительное распределение ключей необходимо для уменьшения объёма распределяемой (передваемой) и хранимой информации.

Задача распределения КИ заключается в следующем:

- ▶ $A_1, \dots, A_n, n > 2$ - 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, \dots, r_n - в открытом доступе)

Предварительное распределение ключей

Основные понятия и свойства

Схема предварительного распределения ключей:

$$S(n) = (K, P, Q, R, A_0, A_1)$$

1. $A_0 : P \times R \rightarrow Q$ - алгоритм формирования секретных ключевых материалов.

$$A_0(p_i, r_i) = q_i, \quad 1 \leq i \leq n$$

2. $A_1 : Q \times R \rightarrow K$ - 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.

Предварительное распределение ключей

Схема разделения секрета Шамира

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.

Предварительное распределение ключей

Схема разделения секрета Шамира

Первая фаза:

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

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

$F(x) = (a_{k-1}x^{k-1} + \dots + a_1x + M) \bmod p$ - многочлен над полем Z_p

Предварительное распределение ключей

Схема разделения секрета Шамира

Генерация секрета:

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

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}, \dots, a_1 и сам секрет M удаляются.

Предварительное распределение ключей

Схема разделения секрета Шамира

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.

$$F(x) = \sum_i L_i(x) y_i \bmod p,$$

$$L_i(x) = \prod_{i \neq j} \frac{x - x_j}{x_i - x_j} \bmod p,$$

где $(x_i, y_i) \equiv (i, q_i)$ - координаты точек многочлена.

Предварительное распределение ключей

Схема разделения секрета Блома

Инициализация:

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

Доверенная сторона (центр распределения) 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:

$$f(x, y) = \sum_{s=0}^m \sum_{t=0}^m a_{st} x^s y^t, \quad a_{st} = a_{ts}, \quad s \neq t, \quad s, t = 0, \dots, m$$

Предварительное распределение ключей

Схема разделения секрета Блома

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.

Предварительное распределение ключей

Схема разделения секрета Блома

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.