Ссылка на статью:
// Ученые записки УлГУ. Сер. Математика и информационные технологии. 2023, № 2, с. 99–103.
Поступила: 27.10.2023
Окончательный вариант: 27.10.2023

УДК 519.7

Схема разделения секрета с заданным на множестве участников отношением порядка

Рацеев С.М.[*], ***Иванцов А.М.***

[*]ratseevsm@mail.ru
УлГУ, Ульяновск, Россия

Приводится схема разделения секрета с заданным на множестве участников отношением порядка, в которой правомочными являются все такие коалиции, которые содержат все терминальные вершины. Данная схема обладает свойством совершенности и свойством идеальности.

Ключевые слова: *схема разделения секрета, структура доступа, иерархическая схема*

Введение

Схемы разделения секрета позволяют распределить конфиденциальную информацию среди группы участников таким образом, что любая правомочная коалиция этой группы сможет восстановить секрет, но любая неправомочная коалиция этого сделать не сможет. Схемы разделения секрета являются важным инструментом в криптографии и используются в качестве основы для многих защищенных протоколов, например, в протоколах безопасных многосторонних вычислений, в пороговой криптографии и т. д.

Впервые схемы разделения секрета были введены Блэкли Д. [4] и Шамиром А. [6] в 1979 г. для пороговых схем. Ито М., Саито А. и Нишизеки Т. [5] в 1987 г. представили схему разделения секрета для произвольной структуры доступа. На данный момент имеется большое число конструкций схем разделения секрета, обладающих различными свойствами. Более подробно о схемах разделения секрета и их применении в безопасных многосторонних вычислениях можно посмотреть, например, в работах [2, 3].

Схема разделения секрета с заданным на множестве участников отношением порядка

В пороговых схемах разделения секрета предполагается, что все участники разделения секрета равноправны. Рассмотрим случай, когда на множестве участников V задан частичный порядок. Это отношение частичного порядка определяет ориентированный граф (V, E), описывающий иерархию участников. Множество вершин этого графа определяется множеством участников V, а на множество ребер E накладывается требование отсутствия ориентированных циклов. Основная идея использования отношения порядка в схеме разделения секрета заключается в следующем: чем выше в иерархии участники разделения секрета, тем меньшее их число необходимо для восстановления секрета.

Схема разделения секрета для древовидной структуры. Пусть V — множество участников разделения секрета, s — секрет. Напомним, что ориентированным деревом называют граф, в котором в каждую вершину, кроме одной, называемой корнем дерева, заходит ровно одно ребро. В корень дерева ни одно ребро не заходит. Вершины, из которых не выходит ни одно ребро, называются листьями.

Пусть отношение частичного порядка на множестве V определяет ориентированное дерево $T = (V, E)$. Пусть $L = \{v_{i_1}, \ldots, v_{i_m}\}$ — множество всех листьев дерева T, $m = |L|$. Для подмножества $X \subseteq V$ обозначим через $L(X)$ множество всех таких листьев $v \in L$, для каждого из которых существует ориентированный путь от некоторой вершины $u \in X$, зависящей от v, до листа v. Определим структуру доступа следующим образом:

$$\Gamma = \{X \subseteq V \mid L(X) = L\}.$$

В этом случае множество $\Gamma_{\min}$ содержит такие правомочные коалиции $X \in \Gamma$, для каждой из которых выполнено следующее свойство: для любого листа $v \in L(X)$ существует ровно одна вершина $u \in X$, для которой существует ориентированный путь от u до v.

Пример 1. Пусть $V = \{1, 2, 3, 4, 5, 6\}$ — вершины дерева T, которое изображено на рис. 1.

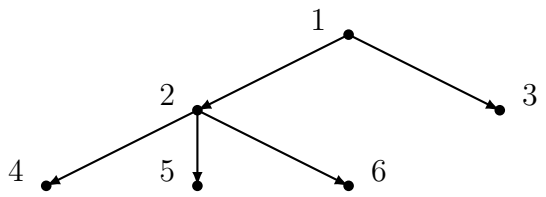

Рис. 1. Древо T

В данном случае $L = \{3, 4, 5, 6\}$ — множество листьев дерева T. Пусть, к примеру, $X = \{2, 3\}$. От вершины 2 в дереве T существуют пути до листьев 4, 5, 6. От вершины 3 существует путь до листа 3. Поэтому $L(X) = L$.

Обозначим через X_1 — все подмножества множества $\{1, 2, 3, 4, 5, 6\}$, которые содержат элемент 1. Также обозначим через $X_{2,3}$ — все подмножества в $\{1, \ldots, 6\}$, которые содержат

элементы 2 и 3. Тогда структура доступа примет такой вид:

$$\Gamma = \{X_1, X_{2,3}, \{3, 4, 5, 6\}\}.$$

При этом

$$\Gamma_{\min} = \{\{1\}, \{2, 3\}, \{3, 4, 5, 6\}\}.$$

В работе [1] описана схема разделения секрета для древовидной структуры с использованием алгоритмов шифрования E_k и расшифрования D_k на ключе k, а также с использованием функции хеширования h. Процесс разделения секрета состоит из следующих шагов.

- Ориентированному дереву T сопоставляется помеченное ориентированное дерево T_D по правилу: каждой вершине v_i ориентированного дерева T приписывается метка — уникальный идентификатор ID_i. Далее ориентированное дерево T_D называется деревом доступа.

- Пусть $s_1,\ldots,s_m$ — доли (m, m)-пороговой схемы разделения секрета, где m — число листьев дерева T. Для восстановления секрета s требуются все эти доли.

- Для корня v_1 дерева доступа T_D фиксируется некоторый ключ k_1.

- Для каждой вершины v_i, $i > 1$, ключ k_i вычисляется на основе хеш-функции h следующим образом. Пусть $(v_j, v_i) \in E$ и для вершины v_j ключ k_j уже вычислен. Тогда $k_i = h(k_j \parallel ID_i)$, где $\parallel$ — операция конкатенации.

- Пусть $k_{i_1},\ldots,\ k_{i_m}$ — вычисленные ключи для листьев из множества $L = \{v_{i_1}, \ldots, v_{i_m}\}$. На основе этих ключей и долей $s_1,\ldots,\ s_m$ получается набор зашифрованный долей: $y_1 = E_{k_{i_1}}(s_1),\ldots,\ y_m = E_{k_{i_m}}(s_m)$.

- Каждому участнику $v_i \in V$ передается дерево доступа T_D, ключ k_i и набор $y_1, \ldots, y_m$.

Пусть $X \subseteq V$ — некоторая правомочная коалиция, $\widetilde{X} \subseteq X$ — минимальная правомочная коалиция. Для восстановления секрета участники коалиции $\widetilde{X}$ проделывают следующие шаги.

- На основе ключей участников коалиции $\widetilde{X}$ с помощью хеш-функции h вычисляются ключи $k_{i_1},\ldots,\ k_{i_m}$.

- На этих ключах расшифровываются доли $s_1 = D_{k_{i_1}}(y_1),\ldots,\ s_m = D_{k_{i_m}}(y_m)$.

- На основе долей $s_1,\ldots,\ s_m$ (m, m)-пороговой схемы восстанавливается секрет s.

Несложно видеть, что если вспомогательная (m, m)-схема является совершенной, то полученная схема разделения секрета также является совершенной. При этом идеальной данная схема не является.

Усовершенствование рассмотренной схемы. Модифицируем эту схему таким образом, что в ней не будет функций хеширования, алгоритмов шифрования/расшифрования, при этом схема будет совершенной и идеальной. Пусть, как и ранее, $T = (V, E)$ — исходное ориентированное дерево. Пусть $s \in G$ — секрет, где G — аддитивная абелева группа. Сгенерируем случайным равновероятным образом доли $s_{i_1}, \ldots, s_{i_{m-1}} \in G$, а долю s_{i_m} вычислим следующим образом: $s_{i_m} = s - (s_{i_1} + \ldots + s_{i_{m-1}})$. Тогда для восстановления секрета нужны все доли: $s = s_{i_1} + \ldots + s_{i_m}$. Доли $s_{i_1}, \ldots, s_{i_m}$ соответствуют листьям $v_{i_1}, \ldots, v_{i_m}$ соответственно. Процесс разделения секрета состоит из следующих шагов.

- Пусть $v \in V$ — очередная вершина дерева T. Для вершины v строится множество листьев $L(\{v\})$ и вычисляется значение $S_v = \sum\limits_{j \in I_v} s_j$, где I_v — множество индексов листьев из L, до которых существуют пути от вершины v, т. е. $j \in I_v$ тогда и только тогда, когда $v_j \in L(\{v\})$.
- Каждому участнику $v \in V$ передается значение S_v.

Перейдем к процессу восстановления секрета. Пусть $X \subseteq V$ — некоторая правомочная коалиция, $\widetilde{X} \subseteq X$ — минимальная правомочная коалиция. Тогда

$$s = \sum_{v \in \widetilde{X}} S_v.$$

Полученная схема обладает свойством совершенности и идеальности.

Схема разделения секрета для ориентированного леса. Обобщим предыдущую схему разделения секрета на ориентированный лес. Пусть (V, E) — ориентированный лес, $L = \{v_{i_1}, \ldots, v_{i_m}\}$ — совокупность всех листьев деревьев этого леса. Для подмножества $X \subseteq V$, как и ранее, обозначим через $L(X)$ множество всех таких листьев $v \in L$, для каждого из которых существует ориентированный путь от некоторой вершины $u \in X$, зависящей от v, до листа v. Определим структуру доступа следующим образом:

$$\Gamma = \{X \subseteq V \mid L(X) = L\}.$$

В этом случае схема разделения и восстановления секрета примет описанный выше вид. Полученная схема также обладает свойством совершенности и идеальности.

Заключение

Значимость совершенных схем разделения секрета состоит в том, что они не зависят от вычислительных возможностей противника. В таких схемах любая правомочная коалиция может восстановить секрет, при этом доли секрета любой неправомочной коалиции не дают никакой информации о секрете (в теоретико-информационном смысле). Также выделяется свойство идеальности, которое означает, что размер секрета и размеры долей секрета совпадают. Для схем с произвольной структурой доступа свойство идеальности чаще всего не

выполняется. Поэтому часто исследуются частные случаи схем разделения секрета, для которых пытаются построить схемы со свойством совершенности и свойством идеальности. Одна из таких схем построена в данной работе.

Список литературы

1. Богаченко Н. Ф. Схема разделения секрета между иерархически связанными участниками // *Математические структуры и моделирование*. 2022. Т. 64, № 4, с. 117–121.
2. Рацеев С. М. *Криптографические протоколы. Схемы разделения секрета* : учебное пособие для вузов. СПб.: Лань, 2024. 336 с.
3. Beimel A. Secret-Sharing Schemes: A Survey // *IWCC, Lecture Notes in Computer Science*. 2011. V. 6639, p. 11–46.
4. Blakley G. R. Safeguarding cryptographic keys // *Proc. of the National Computer Conference*. 1979. P. 313–317.
5. Ito M., Saito A., Nishizeki T. Secret sharing scheme realizing any access structure // *Proc. IEEE Globecom'87*. 1987. P. 99–102.
6. Shamir A. How to share a secret // *Communications of the ACM*. 1979. V. 22, № 11, p. 612–613.

A secret sharing scheme with an order relation on a set of participants

Ratseev, S. M.**, *Ivantsov, A. M.

*ratseevsm@mail.ru

Ulyanovsk State University, Russia

In the paper a secret sharing scheme with an order relation on a set of participants is investigated. In this scheme sets that contain all terminal vertices are qualified. This scheme has the property of perfection and the property of ideality.

Keywords: *secret sharing, access structure, hierarchical secret sharing.*