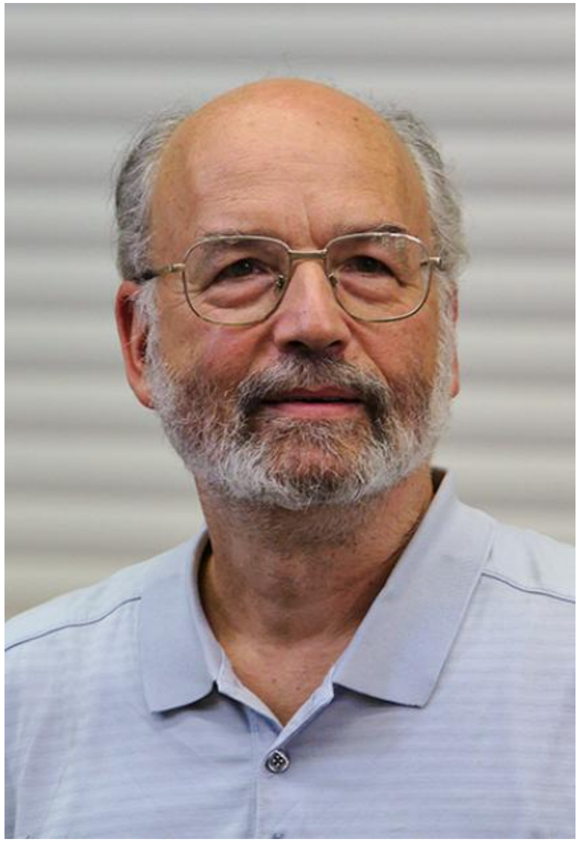
Схемы разделения секрета

Схема разделения секрета (СРС) позволяет «разделить» секрет на n долей, которые в дальнейшем раздать между участниками в соответствии с внутренней политикой ответственности таким образом, чтобы заранее заданные *разрешенные множества долей* могли однозначно восстановить секрет (совокупность этих множеств называется структурой доступа), а неразрешенные — не давали никакой дополнительной к имеющейся априорной информации о возможном значении секрета. СРС с последним свойством называются совершенными (и только они, как правило, рассматриваются в приложениях).

Джордж Ро́берт (Боб) Блэ́кли-младший

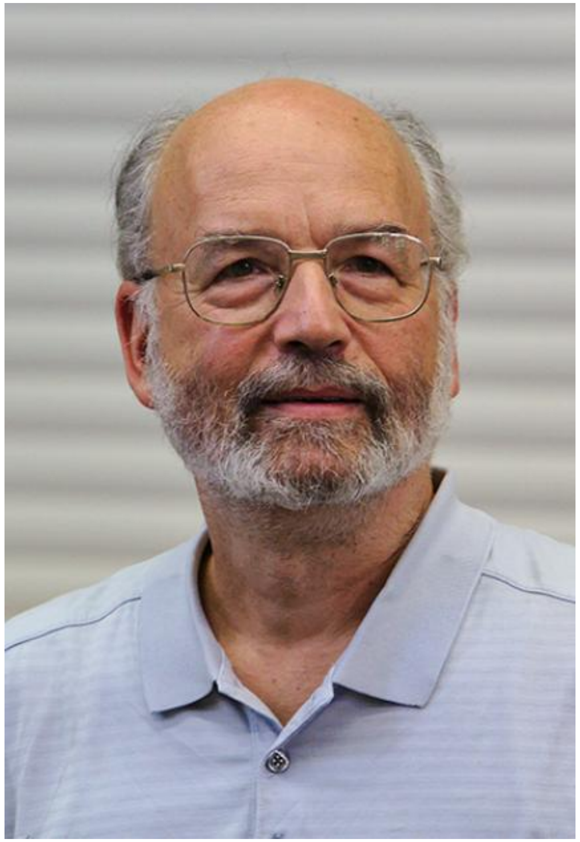


Ади Шамир

Схемы разделения секрета

История СРС начинается с 1979 года, когда эта проблема была поставлена и во многом решена Дж. Блейкли и А. Шамиром для случая пороговых (n, k)-СРС (т. е. разрешенными множествами являются любые множества из k или более долей). Особый интерес вызвали так называемые идеальные СРС, т.е. такие, где «размер» информации одной доли не больше «размера» секрета (а меньше он и не может быть).

Джордж Ро́берт (Боб) Блэ́кли-младший



Ади Шамир

Схемы разделения секрета

Схема разделения секрета Шамира, (n, k) – пороговая схема разделяющая секрет на основе интерполяционных полиномов Лагранжа

Разделение секрета. Доверенный центр T (Трент) выбирает большое простое число p, с условием, что $M < p$. Над простым полем Галуа GF(p) генерируется случайный многочлен степени k – 1 (исходя из числа долей k, достаточных для восстановления секрета):

$$s(x) = (a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_1x + M) \bmod p, \qquad (1)$$

где $a_1, \ldots, a_{k-1}$ — случайные коэффициенты по mod p. Затем вычисляются доли

$$s(x_1) = (a_{k-1}x_1^{k-1} + a_{k-2}x_1^{k-2} + \ldots + a_1x_1 + M) \bmod p$$
$$s(x_2) = (a_{k-1}x_2^{k-1} + a_{k-2}x_2^{k-2} + \ldots + a_1x_2 + M) \bmod p$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s(x_i) = (a_{k-1}x_i^{k-1} + a_{k-2}x_i^{k-2} + \ldots + a_1x_i + M) \bmod p \qquad (2)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s(x_n) = (a_{k-1}x_n^{k-1} + a_{k-2}x_n^{k-2} + \ldots + a_1x_n + M) \bmod p.$$

Долями являются (x_i, $s(x_i)$, p), где x_i могут принимать значения $x_i = 1,\ldots, n$ номеров долей, p — общее простое число для восстановления секреты. После этого многочлен (1) уничтожается, а доли раздаются участникам протокола.

Схемы разделения секрета

Схема разделения секрета Шамира, (*n*, *k*) – пороговая схема разделяющая секрет на основе интерполяционных полиномов Лагранжа

Восстановление секрета. Для восстановления секрета M достаточно собрать k долей из n. По ним составить подсистему (3) системы (2):

$$\begin{aligned} s(x_{i_1}) &= (a_{k-1}x_{i_1}^{k-1} + a_{k-2}x_{i_1}^{k-2} + \ldots + a_1 x_{i_1} + M) \bmod p \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s(x_{i_k}) &= (a_{k-1}x_{i_k}^{k-1} + a_{k-2}x_{i_k}^{k-2} + \ldots + a_1 x_{i_k} + M) \bmod p \end{aligned} \qquad (3)$$

и решить её относительно неизвестных $a_{k-1}, a_{k-2}, \ldots, a_1, M$, и таким образом найти M. Относительно этих переменных данная система будет линейной, совместной и определённой, и её можно решить методом Гаусса над конечным простым полем Галуа GF(p). Но для восстановления многочлена (1) удобнее воспользоваться формулой интерполяционного многочлена Лагранжа. Так как на доли можно смотреть как на точки этого многочлена. Для точек $(x_{i_1}, s(x_{i_1}))$, $(x_{i_2}, s(x_{i_2}))$,…, $(x_{i_k}, s(x_{i_k}))$, существует единственный многочлен степени не больше $k - 1$, который можно вычислить по следующим формулам:

$$s(x) = \sum_{t=1}^{k} s(x_{i_t}) l_t(x), \text{ где } l_t(x) = \prod_{\substack{1 \le j \le k \\ j \ne t}} (x - x_{i_j})(x_{i_t} - x_{i_j})^{-1}.$$

Все вычисления проводятся в поле GF(p) (т.е. по $\bmod p$), обратные элементы $(x_{i_t} - x_{i_j})^{-1}$ вычисляются по расширенному алгоритму Евклида.

Схемы разделения секрета
Векторная схема разделения секрета Блэкли

По-прежнему будем строить (n, k) – пороговую схему разделения секрета M, где $n \geq k$, n — общее число долей, k — число долей, достаточное для восстановления секрета.

Разделение секрета. Доверенный центр T (Трент) генерирует случайную точку в k-мерном аффинном пространстве, одной из координат которой является секрет M. Пусть это будет точка $A(a_1, a_2, \ldots, a_{k-1}, M)$. Далее генерируются n k-мерных векторов:

$$N_1(b_1^{\,1}, b_2^{\,1}, \ldots, b_k^{\,1});$$
$$N_2(b_1^{\,2}, b_2^{\,2}, \ldots, b_k^{\,2});$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$N_n(b_1^{\,n}, b_2^{\,n}, \ldots, b_k^{\,n}).$$

Эти векторы должны обладать тем свойством, что любые k векторов из них являются линейно независимыми. По этим векторам строятся n k-мерных гиперплоскостей, проходящих через точку A:

$$\alpha_i : b_1^{\,i}(x - a_1) + b_2^{\,i}(x - a_2) + \ldots + b_{k-1}^{\,i}(x - a_{k-1}) + b_k^{\,i}(x - M) = 0.$$

Эти гиперплоскости α_i $(1 \leq i \leq n)$ являются долями.

В качестве аффинного пространства можно также рассматривать арифметическое пространство над простым полем Галуа GF(p), где выполняется условие $M < p$.

Схемы разделения секрета
Векторная схема разделения секрета Блэкли

Восстановление секрета. Любые k гиперплоскостей из α_i $(1 \le i \le n)$ пересекаются в единственной точке A, одна из координат которой является секретом M. Любые меньше чем k гиперплоскостей имеют в пересечении не менее, чем одну прямую. Для вычисления пересечения достаточно решить линейную систему уравнений из уравнений гиперплоскостей, которые предложены в качестве k долей, и из полученной точки выделить координату M.

Схемы разделения секрета

Схема разделения секрета Асмута-Блума

Следующая (n, k) – пороговая схема разделения секрета M основана на греко-китайской теореме об остатках.

Разделение секрета. Доверенный центр T (Трент) генерирует простые числа $M < p_0 < p_1 < p_2 < p_3 < \ldots < p_n$, Число p_0 объявляется открытым, и можно полагать, что $M \in Z/p_0Z$. Выбор этих чисел и числа $k \le n$ должен удовлетворять условию

$$p_1 p_2 p_3 \cdot \ldots \cdot p_k > p_0 p_{n-k+2} p_{n-k+3} p_{n-k+4} \cdot \ldots \cdot p_n.$$

Генерируем случайное число r такое, чтобы $0 < s = M + rp_0 < \prod_{i=1}^{k} p_i$.

Ясно, что полученное s удовлетворяет сравнению $M \equiv s (\mathrm{mod}\ p_0)$. Теперь вычисляем доли:

$$s_1 \equiv s \ (\mathrm{mod}\ p_1) \to (s_1, p_1, p_0)$$
$$s_2 \equiv s \ (\mathrm{mod}\ p_2) \to (s_2, p_2, p_0)$$
$$s_3 \equiv s \ (\mathrm{mod}\ p_3) \to (s_3, p_4, p_0)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_n \equiv s \ (\mathrm{mod}\ p_n) \to (s_n, p_n, p_0).$$

Схема разделения завершена.

Схемы разделения секрета

Схема разделения секрета Асмута-Блума

Восстановление секрета. Допустим, получено k долей:

$$s_{i_1} \equiv s \pmod{p_{i_1}}$$

$$s_{i_2} \equiv s \pmod{p_{i_2}}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$s_{i_k} \equiv s \pmod{p_{i_k}}$$

По греко-китайской теореме эта система имеет единственное решение:

$$s_0 \equiv D_{i_1} D'_{i_1} s_{i_1} + D_{i_2} D'_{i_2} s_{i_2} + D_{i_3} D'_{i_3} s_{i_3} + \ldots + D_{i_k} D'_{i_k} s_{i_k} \pmod{\prod_{j=1}^{k} p_{i_j}},$$

где числа D_{i_u}, D'_{i_u} $(1 \le u \le k)$ определяются из условий:

$$D_{i_u} = \frac{\prod_{j=1}^{t} p_{i_j}}{p_{i_u}}, \quad D_{i_u} \cdot D'_{i_u} \equiv 1 \pmod{p_{i_u}}.$$

откуда получаем $M \equiv s_0 \pmod{p_0}$. Секрет восстановлен.

Схемы разделения секрета

Схема разделения секрета Карнина-Грина-Хеллмана

Схема была предложена в 1983г. Это (n, k) – пороговая схема разделения секрета M, основана на векторной алгебре.

Разделение секрета. Доверенный центр T (Трент) генерирует $a_0, a_1, a_2, \ldots, a_n$ $n+1$ k-мерных векторов, из которых векторы $a_1, a_2, \ldots, a_n$ обладают тем свойством, что любые k векторов из них являются линейно независимыми. Далее генерируется случайный k-мерный вектор u с тем условием, что $u^{\mathrm{T}} a_0 = M$ (т.е. скалярное произведение векторов u и a_0 равно M). Долями являются $\{a_i, u^{\mathrm{T}} a_i, a_0\}$ $(1 \le i \le n)$.

В качестве векторного пространства можно также рассматривать пространство над простым полем Галуа GF(p), где выполняется условие $M < p$.

Схемы разделения секрета

Схема разделения секрета Карнина-Грина-Хеллмана

Восстановление секрета. Из любых k и более долей составляется система уравнений вида: $x^{\mathrm{T}} a_i = u^{\mathrm{T}} a_i$, находится решение x_0 и вычисляется секрет $M = x_0^{\mathrm{T}} a_0$.

Схемы разделения секрета

Более сложные схемы разделения секрета

В предыдущих примерах были описаны только простейшие пороговые схемы: секрет делится на n долей таким образом, что, объединив любые k долей, можно раскрыть секрет. На базе этих алгоритмов можно создать намного более сложные схемы. В следующих примерах используется алгоритм Шамира, хотя будут работать и все остальные.

1. Распределение долей в соответствии с уровнем ответственности. Для создания схемы, в которой один из участников важнее других, ему выдается больше долей. Если для восстановления секрета нужно пять долей и у кого-то есть три доли, а у всех остальных - по одной, этот человек вместе с любыми двумя другими может восстановить секрет. Без его участия для восстановления секрета потребуется пять человек.

Более одной доли могут получить два человека и более. Каждому человеку может быть выдано отличное число долей. Вне зависимости от числа розданных долей, для восстановления секрета потребуется любые k из них. Ни один человек, ни целая группа не смогут восстановить секрет, обладая только $k-1$ долями.

Схемы разделения секрета

Более сложные схемы разделения секрета

2. Распределение долей по коалициям.

Например, можно распределить секрет так, чтобы для его восстановления потребовалось двое из 7 участников делегации A и трое из 12 участников делегации B. Создается многочлен степени 3, который является произведением линейного и квадратного выражений.

Каждому участнику делегации A выдается доля, которая является результатом вычисления линейного выражения, а участникам делегации B выдаются результаты вычисления квадратичного выражения.
Для восстановления линейного выражения достаточны любые две доли участников делегации A, но независимо от того, сколько других долей есть у делегации A, ее участники не смогут ничего узнать о секрете. Аналогично для делегации B: ее участники могут объединить три доли, чтобы восстановить квадратичное выражение, но другую информацию, необходимую для восстановления секрета в целом, они получить не смогут. Только объединив свои выражения и перемножив их, участники двух делегаций смогут восстановить секрет.

В общем случае, может быть реализована любая мыслимая схема разделения секрета. Необходимо только написать систему уравнений, соответствующих конкретной системе.

Схемы разделения секрета

Задания

Задание 1. Провести в ручную (в тетради) (5, 3)-пороговую схему Шамира при $p = 17$, $M = 13$.

Задание 2. Провести в ручную (в тетради) (5, 3)-пороговую схему Блэкли при $p = 17$, $M = 13$.

Задание 3. Пусть $M = 10$. Провести (5, 3)-пороговую схему Асмута-Блума.