Системы разделения секрета, основанные на схеме Шамира

Введение

Задача *разделения секрета* заключается в представлении некоторой секретной информации в виде набора равнозначных фрагментов, распределяемых среди нескольких участников. При этом полный набор фрагментов должен однозначно определять исходную информацию, однако любое неполное их подмножество не должно предоставлять возможности восстановить секрет.

Формально задача требует разделения некоторых данных S на n компонент $s_1, \ldots, s_n$ при выполнении следующих условий.

- Знание любых l или более частей s_i делает исходную информацию S легко вычислимой.
- Задача отыскания S по любым $l-1$ или менее частям s_i является трудно разрешимой и не даёт дополнительной информации о значении S.

1. Схема Шамира

Основная идея схемы Шамира базируется на том, что полином степени $l-1$ может быть однозначно восстановлен по его значениям в l различных точках. Пусть исходный секрет является элементом некоторого конечного поля F (на практике — поля вычетов по некоторому простому модулю). Тогда базовый алгоритм разделения секрета будет иметь следующий вид.

1. Положить $a_0 = S$, случайным образом выбрать $a_1, \ldots, a_{l-1} \in F$, а затем построить полином $f(x) = \prod_{i=0}^{l-1} a_i x^i$ с выбранными коэффициентами.
2. Некоторым образом выбрать *различные* $x_1, \ldots, x_n \in F$, после чего вычислить $s_k = (x_k, f(x_k))$.

Полученные n значений полинома могут быть в дальнейшем распределены (вообще говоря, неравномерно) между участниками, разделяющими секрет.

Удовлетворение схемой требований задачи разделения следует из рассмотрения системы:

$$\begin{pmatrix} 1 & y_1 & \cdots & y_1^{l-1} \\ 1 & y_2 & \cdots & y_2^{l-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & y_l & \cdots & y_l^{l-1} \end{pmatrix} \begin{pmatrix} S \\ a_1 \\ \vdots \\ a_{l-1} \end{pmatrix} = \begin{pmatrix} f(y_1) \\ f(y_2) \\ \vdots \\ f(y_l) \end{pmatrix},$$

где $y_1, \ldots, y_l$ — некоторые точки, значения полинома $f(y_1), \ldots, f(y_l)$ в которых известны.

Система линейных уравнений имеет единственное решение тогда и только тогда, когда определитель матрицы системы не равен нулю. Определитель данной системы есть определитель Вандермонда, который не равен нулю в случае различных $y_1, \ldots, y_n$. Следовательно, исходный секрет S может быть восстановлен единственным образом:

$$S = \sum_{i=1}^{l} \left(f(y_i) \prod_{\substack{j=1 \\ j \neq i}}^{l} \frac{y_j}{y_j - y_i} \right).$$

Достоинства схемы Шамира:

- абсолютная криптографическая стойкость,
- размер распределяемых между участниками фрагментов не превосходит размера исходного секрета,
- простота изменения числа участников при фиксированном числе фрагментов l,
- возможность многократного шифрования одного и того же секрета за счёт изменения $a_0, \ldots, a_{l-1}$.

Основной недостаток непосредственного применения схемы — отсутствие способа верификации отдельных ключей, передаваемых участникам, а также возможности проверки достоверности любого их поднабора размера l (для предотвращения подмены отдельных частей секрета).

2. Обеспечение достоверности

2.1. Схема Фельдмана

Рассмотрим модификацию схемы Шамира, позволяющую каждому из n участников, получив свою часть секрета, убедиться в её достоверности.

Ограничим введённое выше поле F случаем циклической группы вычетов по простому модулю p, порождённой элементом b. Пусть по схеме Шамира k-й участник получает часть секрета $s_k = (x_k, f(x_k))$. Тогда при разделении секрета для обеспечения проверки достоверности могут быть опубликованы значения $c_0 = b^S, c_1 = b^{a_1}, \ldots, c_{l-1} = b^{a_{l-1}}$. Полученный участником ключ v_k совпадает с истинным значением $f(x_k)$ (а значит, является достоверным) при условии:

$$b^{v_k} = \prod_{i=0}^{l-1} c_i^{x_k^i} = \prod_{i=0}^{l-1} b^{a_i x_k^i} = b^{\sum_{i=0}^{l-1} a_i x_k^i} = b^{f(x_k)}.$$

Отметим, что специфический выбор F необходим для того, чтобы задача дискретного логарифмирования была трудноразрешимой и не позволяла восстановить a_i по открытым значениям c_i.

2.2. Схема Бенало

Важным качеством системы разделения секрета является возможность, не раскрывая исходной информации, убедиться, что любые l из распределённых между участниками ключей достоверно восстанавливают её. Реализация этого качества схемы Шамира достигается на основе следующих двух утверждений.

1. Если набор $s_1, \ldots, s_n$ корректен, интерполяционный полином Лагранжа, построенный по этим точкам, имеет степень не выше $t - 1$.

2. Если $\deg(g + h) \leq t$ для некоторого $t \in \mathbb{N}$, где g и h — полиномы, то либо $\deg g \leq t$ и $\deg h \leq t$, либо $\deg g > t$ и $\deg h > t$.

Таким образом, схема разделения секрета может быть дополнена процедурой проверки подлинности ключей. Для этого, наряду с $f(x)$, генерируются полиномы $f_1(x), \ldots, f_k(x)$ степени $l - 1$, для которых тем же способом, что и для $f(x)$, строятся k наборов ключей. Чтобы убедиться в подлинности секрета, восстанавливаемого по розданным ключам, участник может выбрать некоторый набор $f_{j_1}(x), \ldots, f_{j_m}(x)$ и затребовать соответствующие каждому из них наборы ключей, а также набор ключей построенных с помощью полинома

$$f_0(x) = f(x) + \sum_{\substack{i=1 \\ i \neq j_1 \\ \cdots \\ i \neq j_m}}^{k} f_i(x).$$

По ключам для $f_0(x), f_{j_1}(x), \ldots, f_{j_m}(x)$ участник, используя утверждение 1, может убедиться в том, что полиномы действительно имеют степень $l - 1$. Из этого, согласно утверждению 2, следует, что степень $l - 1$ имеет и $f(x)$.

Однако сам полином $f(x)$, использующийся для разделения секрета, при этом остаётся закрытым.

Список литературы

[1] Лифшиц Ю. Курс «Современные задачи криптографии». http://yury.name/cryptography/

[2] «Введение в криптографию», под ред. Ященко В. В. — СПб.: Питер, 2001. — 288 с.