

## 1. Цель работы

Реализовать схему разделения секрета на китайской теореме об остатках. Разработка двух независимых модулей: первый должен принимать на вход секрет и возвращать его проекции, второй должен брать проекции и возвращать секрет. Отчет должен содержать описание протокола с указанием особенностей реализации, примеры работы программы.

## 2. Описание алгоритма:

Для реализации схемы разделения секрета на китайской теореме об остатках будет использована схема Миньотта. Совместное использование секрета состоит в восстановлении секрета  $S$  из набора общих ресурсов, каждый из которых содержит частичную информацию о секрете. Китайская теорема об остатках (CRT) утверждает, что для данной системы уравнений решение уникально. Таким образом, совместное использование секретов может использовать китайскую теорему об остатках для получения общих ресурсов, представленных в уравнениях, и секрет может быть восстановлен путем решения системы сравнений, чтобы получить уникальное решение, которое будет секретом для восстановления.

Генерируем последовательность попарно взаимно простых чисел  $p_0 < \dots < p_n$  таких что  $p_{n-k+2} \cdot \dots \cdot p_k < p_1 \cdot \dots \cdot p_k$ .

Затем генерируется случайное целое  $S$  такое что  $p_{n-k+2} \cdot \dots \cdot p_k < S < p_1 \cdot \dots \cdot p_k$ . Доли вычисляются как  $I_i = S \bmod p_i$ , где  $i$  от 1 до  $n$ . Полученные доли используются для китайской теоремы об остатках.

$$\begin{cases} x \equiv I_{i_1} \bmod p_{i_1} \\ \vdots \\ x \equiv I_{i_k} \bmod p_{i_k} \end{cases}$$

Решив эту систему, получаем секрет.

## 3. Описание реализации:

Для работы с большими числами используется библиотека Arbitrary Precision. В данном примере  $SIZE = 1024$ , но он может быть увеличен при необходимости.

- `generateParams(vector<ap_uint<SIZE>> &p_numbers, int n)` – генерация простых чисел, удовлетворяющих условиям  $p_0 < \dots < p_n$  таких что  $p_{n-k+2} \cdot \dots \cdot p_k < p_1 \cdot \dots \cdot p_k$ .
- `generateParts(vector<vector<ap_uint<SIZE>>> &pr, vector<ap_uint<SIZE>> &p_numbers, ap_uint<SIZE> S)` – вычисление долей
- `CRT(vector<vector<ap_uint<SIZE>>> &pr)` – китайская теорема об остатках

### 3. Пример работы программы:

```
p1: 79
p2: 101
p3: 139
p4: 149
p5: 173
p6: 359
alfa: 1286298077
beta: 28588780937
S: 1286305477
1) 64 = 1286305477 mod 79
2) 80 = 1286305477 mod 101
3) 33 = 1286305477 mod 139
4) 99 = 1286305477 mod 149
5) 134 = 1286305477 mod 173
6) 220 = 1286305477 mod 359
1) x = 64 mod 79
2) x = 80 mod 101
3) x = 33 mod 139
4) x = 99 mod 149
5) x = 134 mod 173
x: 1286305477
```

Рис 1. Пример работы программы при  $n = 6$  и  $k = 5$

### 4. Вывод:

Была реализована схема Миньотта, разделяющая секрет с помощью китайской теоремы об остатках. Поскольку китайская теорема об остатках предоставляет нам метод однозначного определения чисел по модулю относительно простых целых чисел, идея состоит в том, чтобы построить схему, которая определит секрет  $S$  с учетом любых  $k$  долей (в данном случае остаток от  $S$  по модулю каждого из чисел  $p_i$ ), но не раскроет секрет  $S$ , которому дано менее  $k$  долей.