# Схемы разделения секрета с реализацией на языке Haskell

О. Н. Хритоненков

*Направление подготовки:* Фундаментальная информатика и информационные технологии
*Руководитель:* асс. каф. ИВЭ А. М. Пеленицын

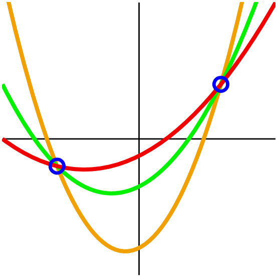
Южный федеральный университет
Институт математики, механики и компьютерных наук имени И. И. Воровича

21 июня 2016

# Постановка задачи

- Обоснование свойств совершенности и идеальности схем разделения секрета Шамира и Блэкли
- Анализ вычислительной сложности схем Шамира и Блэкли
- Реализация схем Шамира и Блэкли на языке Haskell

# Схема Шамира: идея



Через 2 точки можно провести неограниченное число графиков, заданных полиномами степени 2. Чтобы выбрать из них единственный, нужна третья точка.

# Схема Шамира: алгоритм

1. выбирается простое число $p > max(s, n)$
2. $a_0 = s$ – свободный член секретного многочлена
3. $a_1, \ldots, a_{k-1}, 0 \leq a_j \leq p - 1$ выбираются случайно
4. $f(x) = \sum_{j=0}^{k-1} a_j x^j$
5. вычисляются значения в $n$ различных точках
   $\sigma_i = f(i) \bmod p, 1 \leq i \leq n$
6. участникам раздаются доли $(i, \sigma_i)$
7. для восстановления секрета используется
   интерполяционный полином Лагранжа

# Обоснование свойств: схема Шамира

## Идеальность

формула Хартли: $m = \log_2 p$
$B_s = m$ бит
$B_{s_i} = \log_2 p + \log_2 1 = m$ бит
$B_{s_i} = B_s \Rightarrow$ схема Шамира является идеальной

## Совершенность

Секрет может быть восстановлен путем решения системы сравнений
Решение системы из менее чем $k$ сравнений с $k$ неизвестными – множество точек на гиперплоскости в $k$-мерном пространстве
$\Rightarrow$ схема Шамира является совершенной

# Анализ вычислительной сложности: схема Шамира

### Разделение

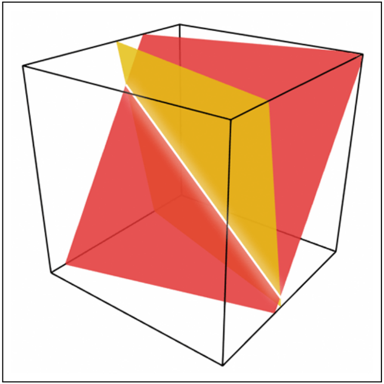
1. $O(1)$
2. $O(k)$
3. $O(kn)$
4. $O(n)$

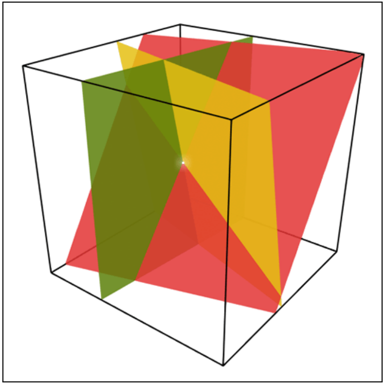
### Восстановление

- $O(k^2)$

общая оценка сложности алгоритма составит $O(kn)$

# Схема Блэкли: идея





Для восстановления всех координат точки в трехмерном пространстве нужны три пересекающиеся в нужной точке плоскости.

# Схема Блэкли: алгоритм

1. выбирается простое число $p > max(s, n)$
2. $b_1 = s$ – первая координата секретной точки
3. $b_2, \ldots, b_k, 0 \le b_j \le p - 1$ выбираются случайно
4. для каждого из $n$ участников $a_{1_i}, \ldots, a_{1_k}, 0 \le a_{1_i} \le p - 1$ выбираются случайно
5. для каждого из $n$ участников $d_i = -(a_{1_i}s + a_{2_i}b_2 + \ldots + a_{k_i}b_k)$ mod $p$
6. участникам раздаются доли $a_{1_i}, \ldots, a_{1_k}, d_i$
7. для восстановления секрета необходимо решить систему линейных уравнений

# Обоснование свойств: схема Блэкли

### Идеальность

$B_s = m$ бит

$B_{s_i} = k \log_2 p = km$ бит

$B_{s_i} \neq B_s \Rightarrow$ схема Блэкли не является идеальной

### Совершенность

Решение СЛАУ из менее чем $k$ уравнений с $k$ неизвестными – множество точек на гиперплоскости в $k$-мерном пространстве $\Rightarrow$ схема Блэкли является совершенной

# Анализ вычислительной сложности: схема Блэкли

## Разделение

1. $O(1)$
2. $O(k)$
3. $O(kn)$
4. $O(n)$

## Восстановление

- $O(k^3)$

общая оценка сложности алгоритма составит $O(kn) + O(k^3)$

# Реализация схем Шамира и Блэкли

$shamir :: Integer - > Integer - > Integer - > Integer - > IO()$

$blakley :: Integer - > Integer - > Integer - > Integer - > IO()$

параметры $s\ k\ n\ k'$
где
$s$ – разделяемый секрет,
$k, n$ определяют $(k, n)$–пороговую схему
$k'$ – количество участников, пытающихся восстановить секрет

# Пример работы программы

**(3,4)−пороговая схема Шамира с 3 участниками**

ghci> *shamir* 9895 3 4 3

secret = 9895
shares = [(1,243),(2,1288),(3,2297),(4,3270)]
secret = 9895

**(3,4)−пороговая схема Шамира с 2 участниками**

ghci> *shamir* 157693 3 4 2

secret = 157693
shares = [(1,282708),(2,128374),(3,165342),(4,393612)]
secret = 437042

# Пример работы программы

**(3,4)−пороговая схема Блэкли с 3 участниками**

ghci> *blakley* 105 3 4 3

```
secret = 105
shares =
[[280,218,300,30],[127,270,92,139],[176,16,222,66],[271,254,140,37]]
secret = 105
```

**(3,4)−пороговая схема Блэкли с 2 участниками**

ghci> *blakley* 78 3 4 2

```
secret = 78
shares = [[70,103,84,11],[52,163,123,19],[107,69,147,172],[154,20,12,44]]
secret = 34
```

# Полученные результаты

- Получено обоснование свойств совершенности и идеальности схем разделения секрета Шамира и Блэкли
- Проведен анализ вычислительной сложности схем Шамира и Блэкли
- Схемы Шамира и Блэкли реализованы на языке Haskell
- Исходный код доступен в Git-репозитории: https://github.com/coastline7/Shamir-and-Blakley-Secret-Sharing