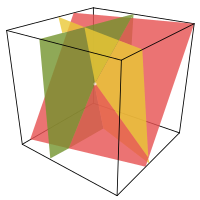
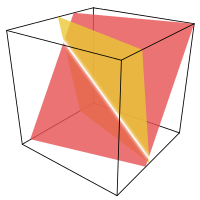
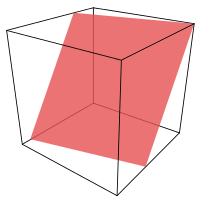
**Схема разделения секрета Блэкли**

Идея разделяемого секрета в схеме Блэкли является одна из координат точки в -мерном пространстве. Долями секрета, раздаваемые сторонам, являются уравнения -мерных гиперплоскостей. Для восстановления точки необходимо знать уравнений гиперплоскостей. Менее, чем сторон не смогут восстановить секрет, так как множеством пересечения плоскостей является прямая, и секрет не может быть восстановлен.



Разделение секрета

Вход: – минимальная длина простого модуля , – секрет, – число генерируемых долей секрета, – количество долей секрета, необходимое для восстановления всего секрета.

Выход: – большое простое число, долей секрета.

1. Разбить секрет (в двоичном виде) на примерно равных по длине долей и определить как точку -мерного пространства.

2. Сгенерировать большое простое число , большее наибольшей координаты точки .

3. Алгоритм: генерация матрицы коэффициентов

1. составить нулевую матрицу ;
2. в каждой строке значение случайного элемента присвоить ;
3. остальные элементы матрицы заполнить случайными числами из ;
4. вычислить элементы по формуле из пункта 3 генерации: ;
5. матрица удовлетворяет условию линейной-независимости любых строк с вероятностью , где

Каждая строка матрицы – -ая доля секрета, представляющая собой уравнение в : .

Восстановление секрета

Вход: , долей секрета

1. Составить следующую систему уравнений (все вычисления проводить в поле :

и решить её любым методом. Единственное возможное решение есть вектор . Объединив всего его компоненты в двоичном виде в одно число получим исходный секрет .