Гащенко Александр Валерьевич, 012

# Разделение Секрета (Secret Sharing)

## Словарь основных используемых терминов и сокращений с переводами:

*Secret* – секрет

*Share* – часть

*Secret Sharing* – разделение секрета

*Secret Sharing Algorithm* - алгоритм разделения секрета

*Secret Sharing Scheme* – схема разделения секрета

*Secret Sharing Scheme Participant* – участник схемы разделения секрета

*Key verification* – проверка ключей

*Dealer* – дилер

*Cheater* – злоумышленник

*Threshold Scheme* – пороговая схема

*Secure Circuit Evaluation* - безопасное обращение секретов

## 1. Введение

Чтобы дать хотя бы какое-то представление о том, что же такое Secret Sharing, рассмотрим следующий наглядный пример:

Во дворце правителя есть тайная, очень важная и опасная комната. И, согласно закону, только правителю вместе с тремя стражами комнаты дозволен вход туда. И ни правитель одиночку, ни правитель с одним или двумя стражами не может быть допущен туда.

Как осуществить исполнение этого закона на деле? Использовать алгоритм разделения секрета (Secret Sharing Algorithm). Эти алгоритмы позволяют разделить некоторый секрет (secret, например, секретный ключ) на несколько частей (share) так, чтобы владельцы этих частей имели бы возможность воссоздать (собрать) его впоследствии.

В большинстве криптографических алгоритмов защита, в конечном счете, основывается на некотором секретном ключе. Это весьма рискованно, поскольку если злоумышленнику удается завладеть этим ключом, защищаемая информация автоматически оказывается в его руках. Таким образом, безопаснее разделить секретный ключ k между n участниками. Каждый участник i будет владеть частью $s_i$ секретного ключа k. Ключ k может быть восстановлен из n частей, однако любых n-1 частей для этого недостаточно. Изначально, протоколы разделения секрета создавались с целью предотвращения резервного копирования ключей. Без создания резервных копий ключа последний легко утратить. Слишком же большое число таких копий также порождает большие проблемы – низкий уровень секретности. Потенциальным решением этой проблемы и явились алгоритмы разделения секрета – с их помощью можно поднять надежность, не увеличивая степени риска.

Существуют две основные области применения схем разделения секрета:

- Разделение секретов, используемых в криптографических операциях
- Проверка ключей (key verification) – секрет хранится в системе. Если восстановленный по частям совпадает с хранящимся в системе, доступ к защищенной информации будет открыт.

## 2. Простой пример

Ниже приведен простейший пример схемы разделения секрета:

1. Двое людей, Андрей и Анюта, хотят разделить ключ К.
2. Они генерируют случайную строку битов А, совпадающую по длине с ключом К.
3. Используют операцию XOR чтобы получить строку B = A + K
4. Они делят секрет: Анюта получает часть А, а Андрей – В.
5. Для воссоздания секрета им необходимо лишь провести обратную операцию:

K =A + B

Метод можно распространить на случай n человек (n>=2). В общем случае:

$S_n = K + S_1 + S_2 + \ldots + S_{n-1}$

**2.1. Простая схема контроля частей (Simple shared control scheme):**

1) Двойственный контроль при помощи сложения по модулю(Dual control by modular addition):

Если секретный ключ S, $0 \le S \le m-1$ где $m$ –целое число, модуль, должен стать ключом к криптографической системе, но по известным причинам нежелательно, чтобы любой другой участник протокола, отличный от стороны, ведущей протокол, которой доверяют все участники протокола(назовем ее дилер-dealer), знал это число S, в этом случае используется схема двойственного контроля. Дилер T генерирует случайным образом число $0 \le S_1 \le m-1$ и раздает числа $S_1$ *и* $S$-$S_1$ *(mod m)* двум участвующим сторонам *A* и B соответственно. A и B затем независимо вводят свои значения в устройство, которое суммирует их по модулю m и восстанавливает тем самым *S*. Если A и B не находятся в сговоре, никто из них не имеет достаточной информации для восстановления S, таким образом число, которое им необходимо находится в диапазоне *(0; m-1).* Это пример схемы разделения знаний об исходном параметре – информация о секретном числе *S* распределена между двумя людьми(участниками). В таком случае говорят, что любые действия по восстановлению секрета S находятся под двойственным контролем – необходимы двое, чтобы восстановить секретный ключ.

2)Соглашение по контролю между неопределенным числом участников с помощь сложения по модулю*(Unanimous consent control by modular addition):*
Схема двойственного контроля описанная выше легко обобщается: секрет S может быть распределен между t участниками, причем присутствие всех необходимо для воссоздания секретного ключа *S*. Схема следующая: дилер *T* генерирует случайным образом t-1 независимое число $S_i$, $0 \le S_i \le m-1$, $1 \le i \le t-1$. Участникам с $P_1$ по $P_{t-1}$ выдаются части $S_i$ $1 \le i \le t-1$, а участнику Pt вычисляется $S_t = S - \sum_{i=1}^{t-1} S_i \pmod m$. Секретный ключ восстанавливается при наличии всех частей как $S = \sum_{i=1}^{t} S_i \pmod m$. В схеме двойственного контроля и в данной схеме операции сложения по модулю m могут быть заменены операцией *XOR* между значениями S и Si фиксированной битовой длины *lg(m).*

Замечание: Составляющие ключа в схеме контроля с разделением должны быть полноценными(той же разрядовой длины, что и ключ) . Это обеспечивает большую надежность нежели разделение r-битного ключа на r частей, каждая из которых длинной r/t. Например, для *r=56 и t=2*, если две части по *28* бит каждая, непосредственный подбор потребует $2^{28}$ комбинаций, тогда как *56*-битные части требуют $2^{56}$ комбинаций перебора.

## 3. Основные определения, касающиеся разделения секрета

Дилер – лицо, не являющееся, как правило, одним из участников схемы разделения секрета. Его основная задача состоит в выборе ключа и распределении его частей.

Злоумышленник - цель злоумышленника – получить доступ к секрету, используя фальшивую его часть.

# 4. Пороговая Схема Шамира (The Shamir Threshold Scheme)

Итак, необходимо, чтобы ключ к мог бы быть воссоздан при наличии t или более частей, но, при этом, количество частей меньше t не должно позволить получить никакой информации о к. Такие схемы называют «(t;w)-пороговыми схемами разделения секрета». Пороговая схема Шамира базируется, как мы увидим ниже, на полиномиальной интерполяции. Пороговые схемы были независимо разработаны Шамиром и Блэкли в 70-х годах прошлого столетия.

## 4.1 Определение

Ниже дано неформальное определение пороговой схемы Шамира по Стинсону:

Пусть t;w – целые положительные числа, причем t≤w. (t;w)-пороговой схемой разделения секрета называется метод разделения ключа К между w участниками (обозначим их через Р) так, что любые t участников могут вычислить значение К, но никакая группа из t-1 или менее участников сделать этого не может.

## 4.2 Математическая реализация и анализ пороговых схем

### 4.2.1 Интерполяция Лагранжа

Ниже на рисунке 3 представлена (3;w)-пороговая схема с тремя или более участниками. В данном случае, (3;4)-пороговая схема.

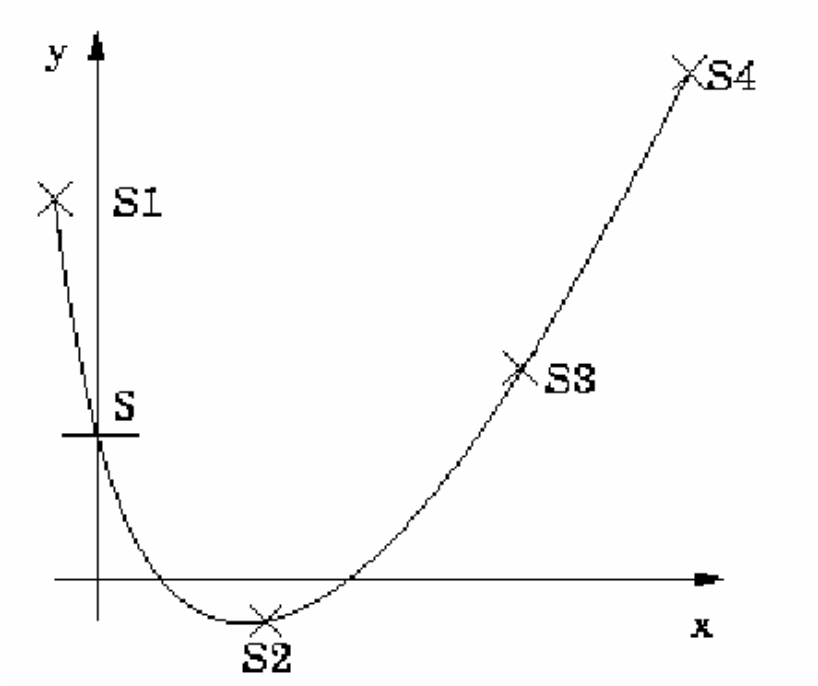


рис.3

Функция f(x) = ax + bx + s, заданная полиномом, представляет собой на графике параболу, легко восстанавливаемую по трем точкам. Поэтому нам необходимо минимум три точки для восстановления секрета S, представленного свободным членом s, являющимся на графике точкой пересечения параболы с осью Y, т.е. f(0) = s.

Для создания w частей секрета необходимо произвольным образом выбрать w точек на параболе.

Можно создать схемы с любым нужным нам значением t, используя функцию, заданную полиномом степени (t-1):

$F(x) = a_{t-1}x^{t-1} + \ldots + a_1x + s$

При t = 2 мы получим прямую. Прямая однозначно восстанавливается по двум точкам.

Для восстановления секрета нам необходимо восстановить полиномиальную функцию порядка (t-1), используя интерполяцию методом Лагранжа:

$$f(x) = \sum_{i=1}^{t} \frac{(x-a_1)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_t)}{(a_i-a_1)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_t)} b_i$$

### 4.2.2. Решение системы уравнений с модулями

Для создания (3;w)-пороговой схемы нам необходимо задать полином вида:

$ax^2 + bx + M \bmod p$

Где: a и b – произвольные числа, p – произвольное известное всем простое число p, превосходящее по модулю коэффициенты a и b, M – секрет.

Для получения частей $s_i$ необходимо получить значение функции в w различных точках:

$s_i = f(x_i)$

Для воссоздания секрета M необходимо решить систему i линейных уравнений с модулем, где i – число частей. С помощью этой методики можно делить секрет на большое число частей. При этом, если используются действительно случайные числа, система так же надежна, как одноразовый шифр, и, как следствие, атака грубой силой обречена на провал.

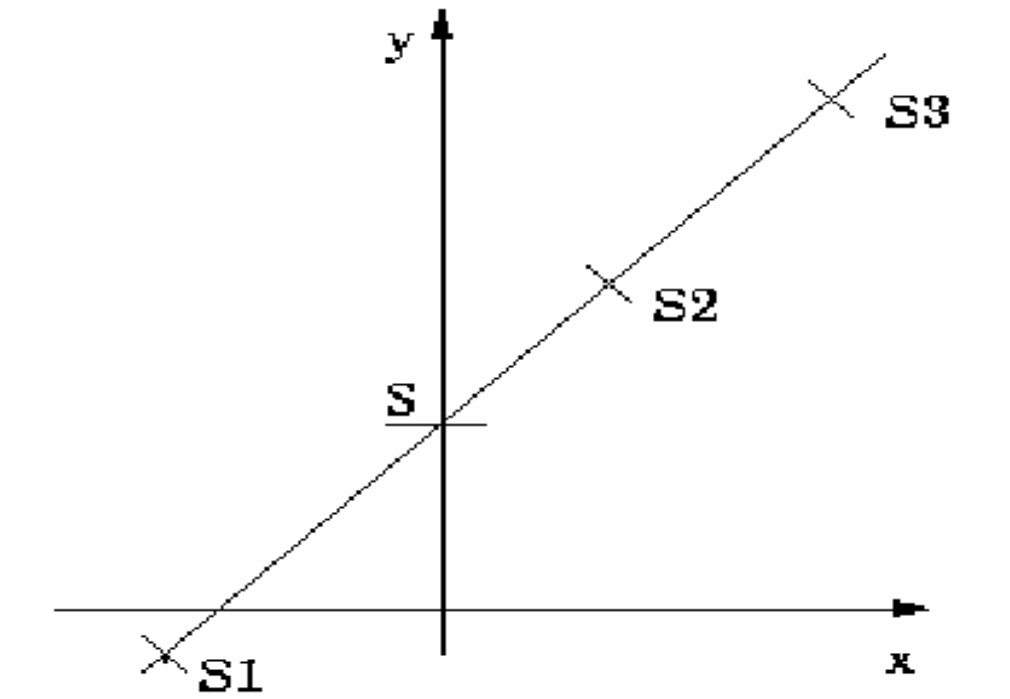


рис.4

### 4.2.3. Особенности пороговой схемы Шамира

1. **Совершенная безопасность (Perfect Security) –** информационная теоретическая безопасность. При наличии t частей секретного ключа возможно единственным образом восстановить S. Зная *t-1* или менее частей секретного ключа и диапазон $0 \le S \le m-1$, восстановление секретного ключа остается сложной задачей. Секретным ключом может быть любой из элементов множества m.

2. **Идеальная (Ideal)** - размер(битовый размер) секретного ключа совпадает с размером каждой из составляющих частей ключа.

3. **Расширяемость(Extendable)** - новые части секретного ключа(для только что появившихся участников протокола) могут быть вычислены и розданы без использования уже созданных частей, просто по средствам просчета дополнительных точек для полинома.

4. **Гибкая(Flexible) –** возможно присваивать различные «веса» различным подмножеством авторизации(см. ниже).

5. **Свойство гомоморфизма (Homomorphic property) –** для схемы Шамира имеет место *(+,+)* гомоморфизм. Например, предположим, что есть два секретных ключа *S и R*. Они зашифрованы по схеме разделения секретов Шамира: *(f(1),…,f(n))*, определенные из полинома *f(X)* *(g(1),…,g(n))* – из полинома *g(X) для S и R* соответственно. Допустим каждый i-тый участник протокола просуммирует: *h(i)=f(i)+g(i) (i=[1..n])*. Каждая из полученных сумм в свою очередь является частью секретного ключа *S+R*, определяемого из полинома *h(X)=f(X)+g(X),* и *h(0)=S+R*.

6. **Эффективный распределенный механизм для арифметических вычислений (Efficient Distributed Mechanism For Arithmetic Calculations) –** например умножение на константу: каждый участник протокола может умножить его часть секретного ключа на константу.

7. **Независимая(Independent) -** в отличии от многих криптографических схем, безопасность схемы разделения секретного ключа напрямую не зависит от сложности ключа.

### 4.2.4. Недостатки пороговой схемы разделения ключей Шамира:

1. **Дилер(Trusted dealer)** – в схеме по умолчанию считается, что дилер абсолютно надежен, что не всегда верно.

2. **Невозможность определения корректности частей секретного ключа(Verify correctness)** – до момента восстановления секретного ключа участники протокола не могут с уверенностью сказать, является ли их часть подлинной.

### 4.2.5 Алгоритмическая сложность пороговой схемы Шамира

- Для вычисления всех коэффициентов для функции *f(x)* из интерполяционных уравнений Лагранжа требуется в среднем $O(k^2)$ шагов (временная сложность). Но оптимизация арифметические вычислений при работе с матрицами позволяет уменьшить число шагов до $k \cdot \log^2 k$.
- В некоторых случаях удобно вместо разделения на части одного длинного секретного ключа S, изначально разделить S на j более маленьких частей и работать непосредственно с каждой из этих частей отдельно. Это позволяет понизить временную сложность от $O(k^2)$ до $O(j(k/j)^2) = O(k^2/j))$.
- Длина (битовая) каждой из частей секретного ключа должна равняться длине секретного ключа.

## 4.3. Градация частей

Для классификации участников разделения секрета можно выдать каждому из них разное количество частей. Проиллюстрируем это на следующем примере:

Пусть в (3;5)-пороговой схеме важный человек A получил две части секрета. Все остальные – по одной. Для воссоздания секрета A понадобится лишь еще один человек, в то время как без A потребуется участие троих.

## 4.4. Атаки на пороговые схемы

Если в число w участников разделения секрета пробрался злоумышленник, у него есть масса возможностей обойти пороговую схему:

- Злоумышленник может использовать неверную часть (например, произвольное число) специально. Тогда группа не получит секрета, но установить кто именно предъявил неверную часть будет невозможно.
- Злоумышленник может спровоцировать начало сессии разделения секрета. Если ему удастся сойти за своего, он сможет получить их прообразы.
- В (3;4)-пороговой схеме, рассмотренной в примере, злоумышленник может притвориться четвертым участником. Поскольку трех участников будет и так достаточно для восстановления секрета. Узнав прообразы трех частей секрета, он сможет воссоздать его и получить впоследствии правильную часть.

## Используемая литература

1. Heiko Heil, “Secret Sharing”, Cryptography Seminar, 2001