РАЗДЕЛЕНИЕ СЕКРЕТА

§1. Постановка вопроса

Для того, чтобы составить представление о задачах, для решения которых потребовалось создавать схемы разделения секрета, приведем следующий исторический пример. В книге «Gent und seine Schoenheiten» (Thill-Verlag, Bruessel,1990) описывается следующий исторический пример. В IIX-XIVвв. в бельгийском городе Генте была построена ратушная башня. В «секрете», то есть самом надежном помещении, хранились уставы и привилегии, имевшие важное значение. Помещение имело две двери, каждая с тремя замками. Ключи от этих замков находились во владении различных цехов. Документы хранились в шкафу, запиравшемся на три замка. Один ключ от шкафа хранился у фогта, а два других – у главного шеффена. Таким образом, получить доступ к документам могли только совместно собравшиеся представители трех цехов, фогт и шеффен. Поэтому интерес к протоколам разделения секрета возник задолго до появления криптографических протоколов как научного направления.

Протоколы разделения секрета применяются для распределенного хранения информации. Чаще всего такой информацией оказываются секретные ключи или пароли какого-либо абонента. Например, главный бухгалтер предприятия держит секретную рабочую информацию зашифрованной, а ключ, длиной 64 бита, хранит в надежном месте, известном только ему. Но что случится, если главный бухгалтер уволится или тайник с ключом сгорит? Тогда ключ будет утерян, а дешифрование в современных криптосистемах может занять миллионы лет! Можно выдать по копии ключа заместителю главного бухгалтера и директору предприятия. Но если заместитель захочет занять место главного бухгалтера, воспользуется своей копией ключа и подменит важную информацию? Или продаст ее конкурентам?

Можно предложить следующий выход: разделить ключ на четыре части по 16 бит и выдать одну часть генеральному директору, другую – его заместителю, третью – заместителю главного бухгалтера, а четвертую – супругу (супруге) главного бухгалтера. Но что, если заместители договорятся сместить своих начальников и воспользуются своими частями ключа? Тогда для того, чтобы восстановить ключ, злоумышленникам потребуется подобрать всего лишь 32 бита, что потребует всего $2^{32} \approx 4{,}3 \cdot 10^9$ операций вместо $2^{64} \approx 18{,}5 \cdot 10^{18}$ при подборе 64 битов. Злоумышленники смогут восстановить ключ за вполне обозримое время.

Разумным будет разделить этот 64-битовый ключ K так, чтобы каждому досталось по 64 бита. Как это сделать? Генеральному директору, и заместителям можно выдать по случайной 64-битовой

строке S_1, S_2, S_3 соответственно, а супругу(е) главного бухгалтера – строку

$$S_4 = K - S_1 - S_2 - S_3 (\mathrm{mod}\, 2^{64}).$$

Тогда каждый из них будет обладать случайной строкой бит, по которой ключ можно восстановить только перебором 64-битового числа. Даже соединив три любых части, нельзя получить никакой информации о ключе, и нельзя уменьшить количество перебираемых битов. Но, при соединении всех четырех частей

$$S_1 + S_2 + S_3 + S_4 \equiv K (\mathrm{mod}\, 2^{64})$$

ключ вычисляется однозначно.

Мы только что описали простейшую схему разделения секрета с одной разрешенной группой участников, состоящей из 4-х абонентов.

§2. Основные понятия разделения секрета

Протоколы разделения секрета призваны решить проблему хранения информации так, чтобы те группы людей, которым позволено знать секрет, могли бы его восстановить, а те группы, которым секрет знать не позволено, восстановить его не смогли даже путем перебора.

В протоколе разделения секрета имеются n участников (абонентов) $P_1, P_2, ..., P_n$ и один выделенный участник D, называемый ***дилером*** (***раздающим***). Пусть через $P = \{P_1, P_2, ..., P_n\}$ обозначено множество всех абонентов. Введем следующую терминологию:

- ***группа доступа*** (***разрешенная группа)*** **–** непустое подмножество A участников множества P, которые, собравшись вместе, имеют право восстановить секрет;
- ***структура доступа*** *Г* будем называть непустое множество всех групп доступа.

Далее будем полагать, что любой участник $P_1, P_2, ..., P_n$ входит хотя бы в одну группу доступа, иначе присутствие его присутствие бессмысленно. Также считаем, что Г замкнуто, то есть если $A \subset B \subset P$ и $A \subset$ *Г*, то $B \subset$ *Г.* Действительно, если абоненты $P_1, P_2, ..., P_k$ могут совместно восстановить секрет, то, если к ним присоединятся дополнительные участники $P_{k+1}, P_{k+2}, ...$, то получившаяся группа тем более сможет восстановить секрет.

Протокол разделения секрета состоит из ***двух основных фаз***.

1. ***Разделение секрета – фаза раздачи***, когда дилер, знающий секрет M, генерирует n долей $m_1, m_2, ..., m_n$ секрета и выдает каждому

участнику его долю по защищенному каналу связи. Раздачу нужно организовать так, чтобы разрешенные группы участников, собравшись вместе, могли однозначно восстановить секрет, а неразрешенные – не могли.

2. ***Фаза восстановления*** секрета, когда какая–либо группа из структуры доступа *Г* объединяет свои доли секретов и получает секрет.

Далее, в качестве примера, приведем три пороговые схемы разделения секрета.

§ 3. Пороговые схемы разделения секрета

(k,n)-пороговой схемой разделения секрета $(k \le n)$ называется такая схема, в которой секрет разделяется между n участниками, причем разрешенной группой является любая группа из не менее, чем k участников.

СХЕМА БЛЕКЛИ

Как известно, система k линейно независимых сравнений с k неизвестными по простому модулю имеет ровно одно решение.

На этом основана пороговая схема Блекли, созданная в 1979 году. Секрет M разделяется между n участниками, любая группа, состоящая не менее, чем из k участников, является разрешенной.

Параметрами схемы являются:

p – большое простое число (больше любого секрета, который предполагается разделять в этой схеме). Тогда $M \in Z_p$.

n – число долей секрета.

k – минимальное число долей, необходимое для восстановления секрета (размер разрешенной группы).

1) Подготовительная фаза: дилер случайным образом выбирает числа

$$x_2^*, x_3^*, ..., x_k^* \in Z_p,$$

и образует секретную точку $Q(M, x_2^*, x_3^*, ..., x_k^*)$.

2) Фаза раздачи секрета: для i-го участника $(i = 1,2,...,n)$ дилер выбирает случайные равномерно распределенные на Z_p коэффициенты $a_{1i}, a_{2i}, a_{3i} ..., a_{ki}$ и вычисляет

$$b_i = a_{1i}M + a_{2i}x_2^* + a_{3i}x_3^* + ... + a_{ki}x_k^* \bmod p$$

После чего дилер посылает i-му участнику сравнение

$$a_{1i}x_1 + a_{2i}x_2 + a_{3i}x_3 + ... + a_{ki}x_k \equiv b_i \bmod p$$

(а, точнее, его коэффициенты) с неизвестными $x_1, x_2, x_3, ..., x_k$.

При этом дилер должен следить за тем, чтобы любые k сравнений были линейно независимы.

3) Фаза восстановления секрета: собравшись вместе, k участников могут составить из своих сравнений систему

$$\begin{cases} a_{11}x_1 + a_{21}x_2 + a_{31}x_3 + ... + a_{k1}x_k \equiv b_1 \bmod p \\ a_{12}x_1 + a_{22}x_2 + a_{32}x_3 + ... + a_{k2}x_k \equiv b_2 \bmod p \\ ..... \\ a_{1k}x_1 + a_{2k}x_2 + a_{3k}x_3 + ... + a_{kk}x_k \equiv b_k \bmod p \end{cases}$$

решив которую они найдут точку Q, первая координата которой является разделяемым секретом M.

Замечание 1: если коэффициенты сравнений выбираются случайно, то при достаточно большом модуле проверкой линейной независимости сравнений можно пренебречь, так как вероятность нарушения этого условия крайне низка.

Замечание 2: если свои доли секретов объединят $t < k$ участников (то есть неразрешенная группа), то система сравнений, составленная ими, даст в качестве решения не точку, а множество точек, лежащих на гиперплоскости порядка t в k-мерном пространстве, и определить наверняка, какая из них содержит секрет, невозможно. В этом случае секретом может оказаться любое значение из Z_p с равной вероятностью.

Пример. Построить (3,3) – пороговую схему Блекли для разделения секрета $M = 5$, выбрав модуль $p = 11$.

Р е ш е н и е.

Подготовительная фаза: выбираем числа $x_2{*} = 2$, $x_3{*} = 1$ и образуем секретную точку $Q(5, 2, 1)$

Фаза раздачи: вычислим доли секрета для каждого абонента.

Для первого участника: пусть $a_{11} = 1, a_{21} = 1, a_{31} = 1$, тогда

$$b_1 = a_{11}M + a_{21}x_2{*} + a_{31}x_3{*} \bmod p = 1 \cdot 5 + 1 \cdot 2 + 1 \cdot 1 \bmod 11 \equiv 8$$

Для второго участника: пусть $a_{12} = 3, a_{22} = 2, a_{32} = 7$, тогда

$$b_2 = a_{12}M + a_{22}x_2{*} + a_{32}x_3{*} \bmod p = 3 \cdot 5 + 3 \cdot 2 + 7 \cdot 1 \bmod 11 \equiv 4$$

Для третьего участника: пусть $a_{13} = 8, a_{23} = 1, a_{33} = 10$, тогда

$$b_3 = a_{13}M + a_{23}x_2{*} + a_{33}x_3{*} \bmod p = 8 \cdot 5 + 1 \cdot 2 + 10 \cdot 1 \bmod 11 \equiv 8$$

После фазы раздачи у каждого из участников оказалось по 4 коэффициента линейного сравнения.

Фаза восстановления:

Участники P_1, P_2, P_3 составляют систему из трех линейных сравнений относительно трех неизвестных. Если матрица системы невырожденная, то система имеет единственное решение.

$$\begin{cases} x_1 + x_2 + x_3 \equiv 8 (\mathrm{mod} 11), \\ 3x_1 + 2x_2 + 7x_3 \equiv 4 (\mathrm{mod} 11), \\ 8x_1 + x_2 + 10x_3 \equiv 8 (\mathrm{mod} 11). \end{cases}$$

Решим систему методом Гаусса, учитывая, что операции производятся в Z_{11}.

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 8 \\ 3 & 2 & 7 & 4 \\ 8 & 1 & 10 & 8 \end{array}\right)_{11} \sim \left(\begin{array}{ccc|c} 1 & 1 & 1 & 8 \\ 0 & -1 & 4 & -20 \\ 0 & -7 & 2 & -56 \end{array}\right)_{11} \sim \left(\begin{array}{ccc|c} 1 & 1 & 1 & 8 \\ 0 & -1 & 4 & -20 \\ 0 & 0 & -26 & -16 \end{array}\right)_{11} \sim$$

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 8 \\ 0 & 10 & 4 & 2 \\ 0 & 0 & 7 & 7 \end{array}\right)_{11} \sim \left(\begin{array}{ccc|c} 1 & 1 & 1 & 8 \\ 0 & 5 & 2 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right)_{11}.$$

$$\begin{cases} x_1 + x_2 + x_3 \equiv 8 (\mathrm{mod} 11), \\ 5x_2 + 2x_3 \equiv 1 (\mathrm{mod} 11), \\ x_3 \equiv 1 (\mathrm{mod} 11) \end{cases} \Rightarrow \begin{cases} x_1 = 5, \\ x_2 = 2, \\ x_3 = 1 \end{cases}$$

Решив систему сравнений, участники нашли единственную точку $Q(5,2,1)$ и восстановили секрет $M = 5$.

Посмотрим, что случится, если свои секреты объединят не три, а два участника. Удастся ли им узнать значение M, или хотя бы очертить круг возможных его значений?

Пусть секрет пытаются восстановить участники P_1 и P_2. Тогда расширенная матрица системы, составленной ими, будет

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 8 \\ 3 & 2 & 7 & 4 \end{array}\right)_{11} \Rightarrow \left(\begin{array}{ccc|c} 1 & 1 & 1 & 8 \\ 0 & -1 & 4 & -20 \end{array}\right)_{11} \Rightarrow$$

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 8 \\ 0 & 1 & 7 & 9 \end{array}\right)_{11} \Rightarrow \left(\begin{array}{ccc|c} 1 & 0 & 1 & 10 \\ 0 & 1 & 7 & 9 \end{array}\right)_{11}$$

Решение, полученное этими участниками, будет

$$M = x_1 = 10 - x_3 \bmod 11,$$

$$x_2 = 9 - 7x_3 \bmod 11$$

Но тогда M может принимать любое значение от 0 до 10, то есть участники P_1 и P_2, собравшись вместе, не увеличили своих знаний о секрете.

СХЕМА ШАМИРА

Идея, на которой основана данная схема, заключается в том, что для интерполяции многочлена степени $k-1$ требуется k точек. Если известно меньшее количество точек, то интерполяция будет невозможной. Обозначим:

p – большое простое число (больше любого секрета M, который предполагается разделять в этой схеме). Тогда $M \in Z_p$.

n – число долей секрета.

k – минимальный размер разрешенной группы.

1). Подготовительная фаза.

Дилер выбирает случайным образом коэффициенты $s_1, s_2, ..., s_{k-1} \in Z_p$ и составляет секретный многочлен

$$S(x) = s_{k-1}x^{k-1} + s_{k-2}x^{k-2} + ... + s_1 x + M \bmod p$$

где M – разделяемый секрет, а остальные коэффициенты – произвольные элементы поля (коэффициенты многочлена дилер хранит в тайне). Очевидно, $S(0) = M$.

Далее дилер выбирает n различных несекретных ненулевых элементов $r_1, r_2, ..., r_n$ из Z_p, каждый из которых ставит в соответствие одному участнику схемы.

2). Фаза раздачи секрета.

Дилер вычисляет значения многочлена $c_1 = S(r_1)$, $c_2 = S(r_2), \ldots, c_n = S(r_n)$, Доля каждого пользователя **A** $_i$ – это пара чисел (r_i, c_i), $i = 1, 2, ..., n$. Доли раздаются участникам схемы.

3) Фаза восстановления секрета.

Чтобы восстановить секрет M, надо воспользоваться ***интерполяционной формулой Лагранжа***: если нужно построить многочлен $S(x)$ степени $(k-1)$, который при $x_1, x_2, ..., x_k$ принимает соответственно значения $y_1, y_2, ..., y_k$, то этим многочленом будет:

$$S(x) = \sum_{i=0}^{k-1} y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}.$$

Так как в схеме разделения секрета многочлен положено выбрать так, чтобы $S(0) = M$, то из формулы Лагранжа следует

$$M = \sum_{i=0}^{k-1} c_i S_i, \text{ где } \quad S_i = \prod_{i \neq j} \frac{r_j}{r_j - r_i}.$$

Пример. Разделить секрет $M = 11$ по $(3,5)$-пороговой схеме, в которой любые 3 из 5 пользователей человек могут восстановить

секрет. Показать, как 2-ой, 3-ий и 5-ый человек вместе могут восстановить секрет.

Р е ш е н и е. $k=3$, $n=5$. Пусть $p=13$.

1). Фаза раздачи секрета.

Выбираем секретный многочлен

$$S(x)=7x^2+8x+11(\mathrm{mod}13).$$

и несекретные ненулевые элементы $r_1=1$, $r_2=2$, $r_3=3$, $r_4=4$, $r_5=5$ поля. Вычисляем

$$c_1=S(r_1)=S(1)=7+8+11(\mathrm{mod}13)\equiv 0(\mathrm{mod}13);$$
$$c_2=S(r_2)=S(2)=7\cdot 4+8\cdot 2+11(\mathrm{mod}13)\equiv 3(\mathrm{mod}13);$$
$$c_3=S(r_3)=S(3)=7\cdot 9+8\cdot 3+11(\mathrm{mod}13)\equiv 7(\mathrm{mod}13);$$
$$c_4=S(r_4)=S(4)=7\cdot 16+8\cdot 6+11(\mathrm{mod}13)\equiv 12(\mathrm{mod}13);$$
$$c_5=S(r_5)=S(5)=7\cdot 25+8\cdot 5+11(\mathrm{mod}13)\equiv 5(\mathrm{mod}13).$$

Доли каждого пользователя: $(1,0),(2,3),(3,7),(4,12),(5,5)$.

2) Фаза восстановления секрета.

Восстановим секрет, собрав доли 2-ого, 3-ого и 5-ого пользователей:

$$M=c_2S_2+c_3S_3+c_5S_5;$$

$$S_2=\prod_{i\neq j}\frac{r_j}{r_j-r_2}=\frac{r_3}{r_3-r_2}\cdot\frac{r_5}{r_5-r_2}=\frac{3}{3-2}\cdot\frac{5}{5-2}=3\cdot 5\cdot 3^{-1}\equiv 5(\mathrm{mod}13);$$

$$S_3=\frac{r_2}{r_2-r_3}\cdot\frac{r_5}{r_5-r_3}=\frac{2}{2-3}\cdot\frac{5}{5-3}=-2\cdot 5\cdot 2^{-1}\equiv 8(\mathrm{mod}13);$$

$$S_5=\frac{r_2}{r_2-r_5}\cdot\frac{r_3}{r_3-r_5}=\frac{2}{2-5}\cdot\frac{3}{3-5}=-2\cdot 3^{-1}\cdot(-3)\cdot 2^{-1}(\mathrm{mod}13)\equiv 1(\mathrm{mod}13)$$

$$M=c_2S_2+c_3S_3+c_5S_5=3\cdot 5+7\cdot 8+5\cdot 1\equiv 11(\mathrm{mod}13).$$

СХЕМА НА ОСНОВЕ КИТАЙСКОЙ ТЕОРЕМЫ ОБ ОСТАТКАХ

Сформулируем китайскую теорему об остатках

Система сравнений вида

$$\begin{cases} x\equiv b_1(\mathrm{mod}\,m_1), \\ x\equiv b_2(\mathrm{mod}\,m_2), \\ \ldots\ldots\ldots\ldots \\ x\equiv b_k(\mathrm{mod}\,m_k), \end{cases}$$

где $m_1, m_2, ..., m_k$ – попарно простые числа, имеет единственное решение

$$x_0 \equiv \sum_{i=1}^{k} b_i M_i M_i^{'} (\mathrm{mod}\, M),$$

где $M = \text{НОК}(m_1, m_2, ..., m_k)$, $M_i = \dfrac{M}{m_i}$, $M_i' = M_i^{-1} (\mathrm{mod}\, m_i)$.

Схема разделения секрета на основе китайской теоремы об остатках выглядит следующим образом:

Пусть N – общий секрет.

1). Фаза раздачи секрета.

Дилер выбирает $p_1, p_2, ..., p_n$ – различные простые числа. Доля секрета, выдаваемая i-му участнику схемы, есть число $x_i \equiv N \bmod p_i$. При выборе чисел $p_1, p_2, ..., p_n$ дилер должен проверить два условия:

- произведение, составленное из k любых этих чисел, должно быть больше, чем N. Это достигается, когда для всех i выполняется $p_i > \sqrt[k]{N}$;
- чтобы гарантировать, что $k-1$ участников не могут восстановить секрет без k-го участника, необходимо, чтобы $p_i \ll \sqrt[k-1]{N}$ для всех i.

2) Фаза восстановления секрета.

Собравшись вместе, k участников составляют и решают систему сравнений относительно неизвестного N:

$$\begin{cases} N \equiv x_1 \left(\mathrm{mod}\, p_1\right) \\ N \equiv x_2 (\mathrm{mod}\, p_2) \\ \qquad ... \\ N \equiv x_k \left(\mathrm{mod}\, p_k\right) \end{cases}.$$

Решение системы дает общий секрет N.

Пример. Построить (3,3) – пороговую схему на основе китайской теоремы об остатках для разделения секрета $N = 549$.

Р е ш е н и е. Простые числа необходимо выбирать их интервала

$$\sqrt[k]{N} < p_i \ll \sqrt[k-1]{N},$$

т.е. $\sqrt[3]{549} < p_i \ll \sqrt{549}$; $8,2 < p_i \ll 23,4$. Пусть

$$p_1 = 11,\ p_2 = 13,\ p_3 = 17.$$

1). Фаза раздачи секрета.

$x_1 = N \bmod p_1 = 549 \bmod 11 = 10;$

$x_2 = N \bmod p_2 = 549 \bmod 13 = 3;$

$x_3 = N \bmod p_3 = 549 \bmod 17 = 5$

Доля $P_1 : (x_1 = 10;\ p_1 = 11);$ доля $P_2 : (x_1 = 3;\ p_1 = 13);$ доля $P_3 : (x_3 = 5;\ p_1 = 17).$

2) Фаза восстановления секрета.

Участники P_1, P_2 и P_3, составляют систему сравнений

$$\begin{cases} N \equiv 10 (\bmod\ 11) \\ N \equiv 3 (\bmod\ 13) \\ N \equiv 5 (\bmod\ 17) \end{cases}$$

и решают ее по китайской теореме об остатках:

$$N = 10 \cdot 221 \cdot 1 + 3 \cdot 187 \cdot 8 + 5 \cdot 143 \cdot 5 \bmod (11 \cdot 13 \cdot 17) \equiv 549$$

Действительно, секрет был восстановлен тремя участниками.

Теперь посмотрим, что случится, если секрет захотят восстановить только два участника – например, P_1 и P_2. Эти участники составят с помощью своих долей секрета систему:

$$\begin{cases} N \equiv 10 (\bmod\ 11) \\ N \equiv 3 (\bmod\ 13) \end{cases}$$

и получат ее решение:

$N = 10 \cdot 13 \cdot 6 + 3 \cdot 11 \cdot 6 \bmod (11 \cdot 13) \equiv 120$ - секрет не восстановлен.

§3. Совершенность и идеальность схемы разделения секрета

Пусть M – множество секретов, которые можно разделить по данной схеме. Схема разделения секрета называется ***совершенной***, если любая группа участников, не имеющая доступа к восстановлению секрета, объединив свои доли секрета, не может отвергнуть как невозможный ни один из секретов множества M .

Схема разделения секрета называется ***идеальной***, если все части секрета и сам секрет одинакового размера и могут равновероятно принимать любое значение из допустимых значений в данной схеме.

Схема Блекли не является идеальной, поскольку размер каждой доли секрета в k раз превосходит размер секрета. Но схема Блекли – совершенная, поскольку решением системы $k-1$ линейных сравнений с k неизвестными является множество решений, лежащей на

гиперплоскости в k-мерном пространстве, а значит секрет M может принимать любое значение из множества возможных секретов.

Схема на основе китайской теоремы об остатках не является совершенной, так как участник, зная свою долю (x_i, p_i), может исключить из рассмотрения все секреты, для которых остаток от деления на p_i не равен x_i.

Схема Шамира является совершенной и идеальной. Идеальность следует из того, что размер секрета равен размеру p, как и размер доли, полагающейся каждому участнику. Для того чтобы показать совершенность, положим, что секрет в схеме Шамира восстанавливается путем решения системы сравнений. Неразрешенное множество участников составит систему из менее, чем k сравнений с k неизвестными. Решением такой системы является множество, точек, лежащих на гиперплоскости в k-мерном пространстве, а значит никакое значение секрета не может быть отвергнуто как невозможное.

В §1 в качестве примера было приведено примерное описание (n,n)-пороговой схемы разделения секрета. Опишем теперь ее формально

(n,n)-ПОРОГОВАЯ СХЕМА

Пусть M – секрет, который следует разделить между n участниками, а структура доступа состоит из одного множества $\Gamma = P = \{P_1, P_2, ..., P_n\}$, т.е. восстановить секрет могут только все участники схемы, соединив свои доли. Выбирается модуль $d > M$.

Фаза раздачи секрета.

Дилер выбирает случайные числа $S_1, S_2, ..., S_{n-1}$ из Z_d и вычисляется число

$$S_n = M - S_1 - S_2 - ... - S_{n-1} (\mathrm{mod}\, d)$$

Поскольку $S_1, S_2, ..., S_{n-1}$ – случайные числа, то и S_n тоже будет случайным числом. Затем доли секрета $S_1, S_2, ..., S_n$ дилер рассылаются участникам: i-ый участник получает число S_i.

Фаза восстановления секрета.

Участники $P_1, P_2, ..., P_n$ объединяют свои доли секрета и вычисляют

$$M = S_1 + S_2 + ... + S_{n-1} + S_n (\mathrm{mod}\, d)$$

Описанная схема является совершенной и идеальной. Совершенность следует из того, что, объединив менее чем n долей секрета, участники вычислят случайное число, которое не даст никакой информации о M. Идеальность очевидна, поскольку каждый участник получает долю секрета, размер которой равен размеру самого секрета.

Ранее мы рассмотрели схемы разделения секрета как протокол, в котором участники доверяют раздающему на фазе разделения секрета, и доверяют друг другу на фазе восстановления секрета. Рассмотрим теперь случай, когда некоторые участники протокола могут оказаться противниками. Задачей протокола разделения секрета в таком случае является защита честных участников от мошенничества противников.

Конечно, если противником является раздающий, он может просто саботировать выполнение протокола, и невозможно предложить криптографическую защиту от такого рода действий. Но саботаж протокола мгновенно выявляется и может быть пресечен другими методами. Честные участники в таком случае доверят разделение секретов другим, честным, дилерам.

Для защиты же от более хитрых действий противника возникла идея **проверяемого разделения секрета*.***

Идея такова: на этапе разделения секрета дилер публикует секрет в зашифрованном виде так, чтобы, пользуясь этой информацией, никто не мог восстановить секрет, но чтобы каждый абонент, используя свою долю секрета, мог проверить, с того ли секрета была получена эта доля.

Кроме дилера, злоумышленниками могут являться некоторые из абонентов. Нечестные участники могут попытаться помешать восстановлению секрета, посылая не свои доли секрета, а какие-то другие значения. От протокола требуется, чтобы все честные участники, если их не менее t, всегда правильно восстанавливали значение секрета M .