УДК 681.3.06:519.248.681

И.Д. ГОРБЕНКО, д-р. техн. наук., А.А.ПОЛЯКОВ, асп.
Е.В. ПОПОВИЧ, асп., Е.С. КОРОБЕЛЬНИКОВ, магистр.

СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА: СУЩНОСТЬ, ОСНОВНЫЕ МЕТОДЫ И СРЕДСТВА РЕАЛИЗАЦИИ

Введение

Важнейшей интенсивно развивающейся в последние годы областью криптологии являются специфические протоколы, которые получили название схем разделения секрета. По сути схемы разделения секрета являются многосторонними протоколам, основной функцией которых является установления ключей. Под установлением ключей понимается процесс или прикладной протокол посредством выполнения которого общий секрет становится доступным объектам системы (технологии), что позволяет им выполнять криптографические преобразования с необходимым качеством [1-3]. Разделение секрета первоначально осуществлялось для защиты криптографических ключей от потери или для создания резервной копии ключей. Применение схемы разделения секрета позволяет также решить задачи обеспечения криптографической живучести или совместного управления действиями в системе (технологии) с использованием криптографических преобразований.

Анализ показывает, что важнейшей составляющей обеспечения реальной криптостойкости в условиях возможной компрометации одной или нескольких частей общего секрета (ключа) является криптографическая живучесть. Кроме того, анализ показал, что основным предназначением схем разделения секрета [ ] является распределенное управление доверием или совместный контроль за критичными действиями (например открытие банковских хранилищ, подписание множественных соглашений, корпоративных, чеков и д.р.). При этом управление такими действиями осуществляется по принципу участия (согласия) не менее k объектов или субъектов из общего их числа n.

Идея разделения общего секрета заключается в том, чтобы общий секрет разделить на n – частей которые называются *частями секрета.* При объедении не менее k объектов или субъектов, общий секрет восстанавливается однозначно. По своей сути в схемах разделения секрета реализуется метод предварительного распределения ключей, обеспечивающий одноразовое установление ключей, когда ключ задается предварительно и может быть одинаковым или различным для различных групп.

Одним из важнейших приложений схем разделения секрета является совместное управление k объектами критичными действиями в системе, неправильное выполнение которых может привести к существенным или катастрофическим последствиям. В этом случае восстановленный секрет является сигналом на разрешение выполнения критического действия. Примерами таких приложений является управление статическим или тактическим оружием, атомными станциями, беспилотными самолетами и космическими аппаратами, особо опасными и опасными производствами и др.

Проведенный анализ показал, что известные схемы разделения секрета можно классифицировать следующим образом.

1. Схемы предварительного разделения секрета. В таких схемах вся конфиденциальная информация, кроме одной, части (доли), заранее устанавливается в общий секрет. При необходимости эта часть может быть предоставлена для формирования общего секрета, например с использованием специальных средств управления ключами или других средств.
2. Схемы динамического разделения секрета. К таким схемам относятся схемы, в которых секреты, восстанавливаемые различными санкционированными подмножествами, являются или могут быть различными в зависимости от предоставленных значений частей секрета.

3. Многозначные схемы разделения секрета. В таких схемах различные подмножества восстанавливают различные общие секреты, которые могут активизировать различные критические действия. То есть основным признаком таких систем является связывание различных подмножеств с различными санкционированными подмножествами.
4. Схемы разделения секрета со взаимным недоверием предназначены для защиты от злоумышленных действий со стороны одного или нескольких объектов каждого подмножества санкционированных объектов, а также доверительной стороны, которая вырабатывает общий и части секрета, и распределяет части общего секрета.
5. Криптографические пороговые схемы разделения секрета. К ним можно отнести пороговые (k,n) схемы, которые обладают тем свойством, что при компрометации одной из частей, (k,n) пороговая схема становится $(k-1,n)$ схемой. Причем $(k-1,n)$ схема обеспечивает надежное восстановление общего секрета.

Проведенный анализ показал [1–7], что известные схема разделения могут быть реализованы с использованием преобразований по модулю, полиномиальной интерпретации, геометрической интерпретации, с использованием известных избыточных кодов, например Рида-Саломона и др.

Целью статьи является проведение классификации и сравнительного анализа схем разделения секрета, а также рассмотрение основных приложений, в которых они могут применяться, естественно с попытками оценить их возможности и особенности применения.

1. Схемы выработки общего секрета на основе преобразований по модулю

Такие схемы является одними из первых схем. Они позволяет вырабатывать общий секрет в случае предоставления всем и n субъектам своих частей секрета. Общий секрет и доли секрета вырабатываются доверенной стороной. Пусть общий секрет есть M, он имеет определенный смысл если или является ключом. Доверенная сторона генерирует n случайных долей ключа $R_1, R_2, ..., R_n$, например являются ключами типа "отрывной блокнот". Затем доверенная сторона вычисляет защищенный открытый общий секрет S_i, причем

$$S_i = M_i \oplus \sum_{j=i}^{n} R_i, \; i = \overline{1,l}, \tag{1}$$

где l – длина общего и частей секрета.

Здесь мы применили термин защищенный открытый секрет в том смысле, что относительно S_i должны быть обеспечены его целостность, подлинность, доступность и наблюдаемость. Требование же обеспечения конфиденциальности к нему предъявляются не всегда. К общему же секрету M предъявляются требования обеспечения всех услуг безопасности, в том числе конфиденциальности как наиболее важнейшей услуги.

Затем доверенная сторона рассылает части секрета R_i с обеспечением их конфиденциальности, целостности, подлинности, доступности и наблюдаемости всем объектам. Подчеркнем, что S_i значение тоже является частью общего секрета и может использоваться для выработки общего секрета. Она при необходимости может использоваться также как и R_i, и выдаваться объектам.

При необходимости общий секрет вырабатывается на основании предоставленных конфиденциальных частей $R_1, R_2, ..., R_n$ и S_i. Значение S_i может быть также и контрольным значением и хранится у особо доверенного субъекта или объекта. При формировании общего секрета в специальном устройстве выработки общего секрета вычисляется сумма по модулю

$$\sum_{j=1}^{n} R'_j \oplus S'_i = \sum_{j=1}^{n} R'_j \oplus M_i \oplus \sum_{j=1}^{n} R_j, \; i = \overline{1,l}. \qquad (2)$$

Если все $R'_i = R_i$ и $S'_i = S_i$, то в результате вычисления (2) в специальном устройстве формируется общий секрет M_i, который может использоваться в качестве ключа, пароля, общего секрета состоятельного протокола, начального приближения вычисления ключа, команды на выполнение критического действия и др.

Рассматриваемая схема может обеспечивать различные уровни стойкости: безусловную стойкость, т.е. теоретическую недешифруемость, вычислительную стойкость, доказуемую [8] и даже временную стойкость. Уровень стойкости определяется свойствами частей секрета R_i. Так если R_i есть случайная последовательность, то в системе при длине каждого R_i, $l_R > l_{ДОЛ}$, т.е. больше допустимой, обеспечивается безусловная стойкость и схема разделения *секрета абсолютно безопасная. Если* R_i *– псевдослучайные последовательности,* то стойкость схемы определяется стойкостью этих последовательностей. По сути, если R_i – случайные (хотя бы одна), то в схеме разделения секрета может быть обеспечена безусловная стойкость. если $j = 1$, т.е. используется одна R_i последовательность, тогда как следует из (1) и (2), можно сформировать две части общего секрета R_i и S_i. Если R_i – случайное с длиной l_R, то единственной, а такой на схему будет атака «грубая сила», сложность которой определяется

$$I = 2^{\ell_R}. \qquad (3)$$

При разделении секретов на n частей стойкость определяется как:

$$I_{CX} = n\left(2^{\ell_R}\right)^{n+1} = 2^{l_R(n+1)}. \qquad (4)$$

К основным недостаткам такой схемы можно отнести:

- необходимость полного доверия к доверительной стороне, в смысле отсутствия подозрений на его злоумышленные действия;
- зависимость стойкости схемы выработки общего секрета от режима секретности у доверенной стороны;
- невозможность проверки каждым из объектов подлинности и целостности частей секрета;
- при злоумышленном или непреднамеренном искажении части секрета, общий секрет восстановить невозможно.

2. Пороговые схемы разделения секрета

В пороговой схеме общий секрет делится на n-частей. Однако восстановление секрета может выполнено по $k \le n$ частным подлинным секретам [ ]. В этой схеме доверенная сторона также формирует общий секрет S и из него вычисляет частные секреты S_i каждого объекта P_i. При этом на S_i накладываются также ограничения, чтобы каждые k объектов, представив k подлинных секретов S_i могли бы вычислить общий секрет S. Более того, если при вычислении S используется $k+v$ частных секретов, то v из них могут быть ложными или искаженными, а k подлинных всё равно обеспечивают формирование общего секрета. Подчеркнём, что на этапе разделения и использования секрета значения S_i должны распространятся и хранится с обеспечением целостности, подлинности, конфиденциальности, доступности и наблюдаемости. Кроме того, в такой схеме ни одна

группа, знающая только $k-1$ частный секрет, восстановить S не может (безусловно или вычислительно).

В дальнейшем будем использовать также понятие совершенной пороговой схемы разделения секрета. Совершенной будем называть такую пороговую схему, в которой знание $k-1$ или менее частных секретов не даёт злоумышленнику никакой информации как о частных так и о общем секрете. Здесь никакой используется в информационно-теоретическом смысле. Это свойство обеспечивается и при многократном формировании общего секрета, однако в этом случае необходимо использовать разные частные секреты. Следует заметить, что в таких схемах нужно обеспечить управление доступом к общему секрету, например за счет использования доверенного устройства выработки общего секрета.

Построение известной пороговой схемы Ади Шамира базируется на полиномиальной интерполяции и на том факте, что одномерный полином $f(x)$ степени $k-1$ над полем Галуа *уникально задаётся по* k *точкам. Полиномы могут быть заданы над* p*-ичным расширенным* полем. При этом коэффициенты полинома $f(x)=a_0+a_1x+a_2x^2+...+a_{k-1}x^{k-1}$, a_i – задаются над полем $GF(p)$ как элементы поля Z_p. Основными параметрами такой схемы являются числа (k,n), где k есть минимальное число частей секрета, с использованием которых может быть восстановлен общий секрет, а n – общее число долей секрета, причем $1\le k\le n$.

Коэффициенты a_i определяются или задаются числом n долей секрета. Затем случайным образом формируется общий секрет S, который должен быть разделен на доли секрета S_i, $i=\overline{1,n}$. Предлагаемая схема должна быть такой, чтобы любые k объектов или субъектов, объединив свой k частных секретов могли однозначно восстановить общий секрет S. При этом все доли секрета S_i являются конфиденциальными, и на протяжении их жизненного цикла должны быть обеспечены целостность, подлинность, конфиденциальность, и доступность.

При выполнении приведенных выше требований и условий пороговая схема разделения секрета А. Шамира реализуется следующим образом.

1. Формируется большое простое число P, которое заведомо больше допустимого $P_{\text{Д}}$, т.е.
$$P>P_{\text{доп}}$$
2. Формируется случайным образом общий секрет S, который является элементом поля $GF(p)$, т.е. целое S которое удовлетворяет условию.
$$1<S<P$$
3. Случайно формируется $k-1$ коэффициентов полинома $f(x)$ – $a_1,a_2,...,a_{k-1}$ которые объявляются конфиденциальными.
4. В качестве a_0 принимается значение общего секрета S, т.е. $a_0=S$.
5. Доверенная сторона разделяет общий секрет, вычислив доли секрета $S_i=f(i)$, где i – числовой идентификатор или номер каждого из объектов или субъектов, причем $1\le i\le p-1$. Разделение секрета может заключаться в присвоении каждому из объектов или субъектов уникального случайного идентификатора.
6. Все доли секрета S_i транспортируются и устанавливаются или вкладываются каждому из объектов или субъектов с обеспечением конфиденциальности, подлинности, целостности, доступности и наблюдаемости.

В дальнейшем мы рассмотрим отдельно алгоритм контроля подлинности каждой из частей секрета.

Восстановление общего секрета производится на основе использования не менее k целостных и подлинных долей секрета, или $k+v \le n$ частных секретов, не более чем v из которых могут быть сформированы объектом или субъектом злоумышленником или искажены. Эти v и менее частных секретов с нарушенной целостностью обнаруживаются и не учитываются при выработке общего секрета. Восстановление общего секрета выполняется в следующем порядке.

1. Каждый из объектов(субъектов) передает и/или устанавливает частные секрет $S_i = f(i)$ в доверенное устройство выработки общего секрета с обеспечением конфиденциальности, целостности и подлинности.
2. Доверенное устройство контролирует целостность и подлинность частных секретов, если эта функция реализована в схеме разделения секрета, а затем выбирает из них k подлинных.
3. По k значениям $f(i_1),...,f(i_k)$ в доверенном устройстве производится восстановление $f(x)$ с использованием интерполяционной формулы Лагранжа:

$$f(x) = \sum_{e=1}^{k} f(i_e) \prod_{j \ne l} \frac{x - i_j}{i_e - i_j}. \qquad (5)$$

4. Общий секрет формируется в виде

$$S = a_0 = f(0).$$

В дальнейшем S может использоваться в качестве ключа, пароля, общего секрета и др.

Таким образом выработка общего секрета в доверенном(исполняющем) устройстве производится на основе восстановления полинома $f(x)$, т.е. вычисления вектора коэффициентов $a_1, a_2, ..., a_{k-1}$, а затем определении общего секрета как $S = a_0 = f(0)$

Проведенный анализ показывает [ ], что свойства пороговой схемы разделения секрета Ади-Шамира позволяют построить протокол с нулевыми знаниями. При соответствующем выборе параметров знание $k-1$ значения $f(i_1),...,f(i_{k-1})$ не дает никакой информации об общем секрете. Его стойкость базируется на интерполяционной формуле Лагранжа, а также зависит от длины модуля преобразований P и длин S_i-ых долей секрета. Рассмотрим возможные атаки на схему Шамира. Основной задачей атак является определение общего секрета $S = a_0$. Значение a_0 можно определить непосредственно или через определение значений частных секретов $f(l_1),...,f(l_k)$. Если $a_0 = S$ и формируется доверенной стороной случайно, то сложность атаки типа "грубая сила" по определению a_0 можно оценить через вероятность P_0 ее осуществления

$$P_0 = \frac{1}{p-2} \approx \frac{1}{p} = p^{-1}. \qquad (8)$$

Сложность атаки "грубая сила" по определению a_0 через значения $f(i_1), f(i_2),..., f(i_k) \in GF(p)$ можно оценить

$$P_f = \left(\frac{1}{(p-1)^k} \right) = (p-1)^{-k} \approx p^{-k}. \qquad (7)$$

Предварительные сравнения (6) и (7) показывают, что более предпочтительной является атака по непосредственному определению a_0. Сложность этой атаки зависит только от

величины модуля p. Если p есть открытый общесистемный параметр, известный криптоаналитику, то сложность атаки можно определить так же через безопасное время

$$\mathrm{T_б} = T_б = \frac{I_0}{\zeta K} \approx \frac{P}{\zeta K} \tag{8}$$

где $I_0 \approx p$ есть число попыток подбора значения a_0 с вероятностью 1, ζ – производительность криптоаналитической системы, $K = 3{,}1 \cdot 10^7$ сек/год – количество секунд в году. При этом условии $T_б$ измеряется в годах. Если a_0 должно быть определено с вероятностью P_q, то $T_б$ с такой вероятностью определяется из соотношения

$$T_б^{\mathrm{P}_q} = \frac{p}{\zeta K}\mathrm{P}_q. \tag{9}$$

В таблице 1 приведены значения $I_0 = p$ и $T_б$ при $\zeta_k = 10^{12}$ и 10^{16} вар/сек. (в знаменателе)

Сложность восстановления общего секрета схемы Ади – Шамира

Таблица 1

p	2^{64}	2^{128}	2^{256}	2^{512}	2^{1024}
$T_б$ **(лет)** $P_д = 1$	$\frac{6*10^{-1}}{6*10^{-5}}$	$\frac{10^{19}}{10^{15}}$	$\frac{4*10^{58}}{4*10^{54}}$	$\frac{10^{134}}{10^{130}}$	$\frac{10^{288}}{10^{284}}$
$T_д$ **(лет)** $P_д = 10^{-16}$	$\frac{6*10^{-17}}{6*10^{-21}}$	$\frac{10^{3}}{10^{-1}}$	$\frac{4*10^{42}}{4*10^{38}}$	$\frac{10^{118}}{10^{114}}$	$\frac{10^{272}}{10^{268}}$

Анализ данных таблицы показывает что применение значения $T_б$ для криптографических преобразований достигаются уже при величине модуля p порядка 2^{256}. Так из таблицы следует, что при длине модуля $p = 2^{256}$ вероятность с которой может осуществлён криптоанализ с $\mathrm{P} = 10^{-16}$ и производительности криптоаналитической системы 10^{16}, безопасное время составляет не менее 10^{38} лет. Поэтому в перспективных схемах разделения секрета величины модулей p должны составлять порядка $2^{256} - 2^{512}$.

Основным и свойством и пороговой схемы Ади-Шамира являются следующие

1. Совершенность – при знании любых $k-1$ и менее долей секрета S_i все значения общего секрета S остаются равновероятными и теоретически могут выбираться из интервала $0 \le S \le p-1$.
2. отсутствие не доказанных допущений. В отличие от вероятностно-стойких схем, схема А. Шамира не базируется ни на каких недоказанных допущениях (например сложности решения таких задач как факторизация модуля, нахождения дискретного логарифма и т.д.).
3. Расширяемость при появлении новых пользователей. Это свойство заключается в том, что новые части секрета могут быть вычислены и распределены без влияния на уже существующие части.

4. Идеальность, под которой понимается тот факт, что все части общего секрета и сам общий секрет имеют одинаковый размер и могут принимать значения над полем $GF(p)$ с равной вероятностью.

Особенностью пороговой схемы разделения секрета является то, что она требует выполнения модульных операций над большим полем $GF(p)$, сложность которых имеет полиномиальный характер. Кроме того, доверенное устройство должно иметь возможность контролировать целостность и подлинность частей секрета перед выработкой общего секрета.

3. Конструкция и свойство протокола проверяемого секрета.

Вначале рассмотрим конструкцию протокола проверяемого разделения секрета над простым полем Галуа $GF(p)$. Предназначением этого протокола является проверка целостности и подлинности каждой из частей секрета, а также проверка частей секретов при их поступлении в доверенное устройство, т.е. перед выработкой общего секрета. Протокол может быть построен следующим образом. Доверенная сторона выбирает случайный полином

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} (\mathrm{mod}\, p).$$

Как и ранее $a_0 = S$.

Все объекты или субъекты системы знают общесистемные параметры θ_v и p_j; где θ_v – первообразный элемент поля $GF(p_j)$, причем p_j и p разные простые числа соответствующего размера. Затем доверенная сторона по a_i вычисляет отдельные составляющие

$$R_i = \theta_v^{a_i} (\mathrm{mod}\, p),\ i = \overline{1, k-1} \qquad (10)$$

Открытые составляющие преобразуются в сертификаты, которые опубликовываются или хранятся в общедоступной базе сертификатов (данных) и являются доступными субъектам и объектам, которые разделяют секрет.

После этого вычисляются части секрета $S_i = f(i)$, для необходимого числа n объектов(субъектов). Далее части секрета доставляются всем объектам(субъектам), разделяющим секрет, с обеспечением конфиденциальности, подлинности, целостности, наблюдаемости и доступности.

Каждый из объектов(субъектов) может проверить подлинность и целостность своей части секрета, проверяя равенство

$$\theta_v^{S_i} = R_0 \cdot (R_1)^{i} \cdot (R_2)^{i^2} \cdot \ldots \cdot (R_{k-1})^{i^{k-1}} (\mathrm{mod}\, p_j) \qquad (11)$$

$$\Theta_v^{S_i} = \mathrm{R_0}*(\mathrm{R_1})^{\mathrm{I}} * (\mathrm{R_{1\backslash 2}})^{i^2} * \ldots * (\mathrm{R_{k\text{-}1}})^{i^{k-1}} (\mathrm{mod}\ \mathrm{P_j}) \quad (**)$$

Подставив (10) в (11) имеем

$$R_0 \cdot R_1^{i} \cdot R_2^{i^2} \cdot \ldots \cdot R_{k-1}^{i^{k-1}} = \theta_v^{a_0} \cdot \theta_v^{a_1 i} \cdot \theta_v^{a_2 i^2} \cdot \ldots \cdot \theta_v^{a_{k-1} i^{k-1}} = \theta^{a_0 + a_1 i + a_2 i^2 + \ldots + a_{k-1} i^{k-1}} (\mathrm{mod}\, p) = \theta_v^{f(i)} (\mathrm{mod}\, p) \qquad (12)$$

Значит $S_i = f(i)$ и по набору R_i обеспечивается проверка частных секретов S_i.

Таким образом, каждый объект, используя только свою часть секрета S_i, общие для системы параметры θ_v и p_i, а так же базу открытых ключей $R_0, R_1, \ldots, R_{k-1}$, может проверить целостность и подлинность своего части секрета. Рассмотренный протокол обеспечивает

контроль целостности и подлинности частных секретов, т.е. от различных злоумышленных действий доверенной стороны и в процессе их транспортировки.

Восстановление секрета. Если доверенное устройство не является злоумышленником, то протокол восстановления общего секрета выполняется следующим образом.

Каждый объект A_j посылает доверенному устройству – объекту A_v свою часть S_i секрета, обеспечивая его целостность, подлинность, конфиденциальность, наблюдаемость и доступность. Доверенная сторона может проверить подлинность и целостность всех принимаемых S частей секрета, используя описанный выше алгоритм выражения (10) – (11).

Части секрета, которые не прошли проверку, не используются. Если честных объектов предоставивших частные секреты, не менее чем K, то доверенное устройство получает не менее K частей общего секрета и может восстановить общий секрет используя схему Шамира, описанную выше.

4. Другие схемы разделения секрета

Среди других схем разделения секрета необходимо выделить схему Беркли и схемы построенные на основе кодов Рида Саломона.

Схема разделения секрета Блэкли имеет геометрическую основу [5]. Секрет представляет собой точку в k-мерном пространстве. При этом для случая $k > 2$ все геометрические построения выполняются над конечным полем $GF(p)$.

Каждая из n проекций задается как гиперплоскость в m-мерном пространстве. Определение секрета сводится к нахождению точки пересечения m гиперплоскостей. В исходном виде схема не является совершенной. На рис. 1 представлен специальный случай схемы Блэкли.

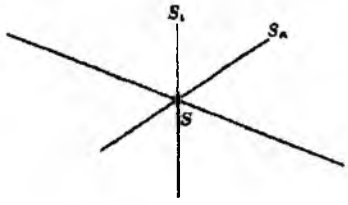

Рисунок 1. Схема Блэкли

Для восстановления секрета необходимо иметь две проекции. Секрет задается как точка на плоскости. Каждая проекция — прямая, проходящая через эту точку. Таким образом, секрет может быть получен по двум проекциям (как точка пересечения двух прямых).

Схема Шамира тесно связана с кодами Рида-Соломона, широко известными в теории помехоустойчивого кодирования [ ]. Обозначим через $(a_1, a_2, ..., a_{k-1})$ список ненулевых элементов конечного поля $GF(p)$. Последовательность входных символов $a = (a_0, a_1, ..., a_{p-1})$,

$$a_i \in GF(p)$$

кодируется в кодовое слово $D = (D_1, D_2, ..., D_{p-1})$, где a_i примитивный элемент поля

$$a_0 = -\sum_{i=1}^{p-1} D_i .$$

Секрет задается как

$$D_i = \sum_{j=0}^{k-1} a_j a_i^j .$$

В качестве долей выбираются D_i. Предположим, t из s проекций содержат ошибки (ошибки, например, могли возникнуть при передаче по каналу связи). Согласно существующей модели, ошибки, возникающие в канале связи, рассматриваются как сумма по модулю 2 ошибочного значения и символа кодового слова. Таким образом, суть процедуры декодирования с исправлением ошибок заключается в определении позиции и значения ошибки (для кода Рида-Соломона и то и другое – элементы поля). Помимо ошибок

различают стирания. В отличие от ошибок при исправлении стираний позиции известны Применяя алгоритм декодирования с исправлением ошибок и стираний, можно гарантированно восстановить D, а следовательно, и a_0, при условии что $s-2t \geq k$. Схема Шамира представляет собой специальный случай кода Рида-Соломона, где p простое число, $a_i = i$ и $t = 0$. Рассмотрим ситуацию, в которой злоумышленник препятствует получению секрета легальными пользователями. Для этого он искажает D_i. Однако секрет будет восстановлен при условии, что кроме t искаженных, легальные пользователи предоставят k неискаженных проекций. В общем случае для блокирования работы *(k,n)* пороговой схемы злоумышленник должен исказить более $\lfloor (n-k)/2 \rfloor$ долей. Алгоритм декодирования может применяться для борьбы с ошибками, возникающими вследствие несовершенства носителей (магнитных дисков, лент и т.д.) и устройств хранения информации. Применение декодирования не приводит к существенному возрастанию вычислительной сложности схемы Шамира. Вычислительная сложность алгоритма декодирования с исправлением ошибок и стираний (алгоритм Берлекэмпа-Мэсси в модификации Форни) оценивается по сложности как $O(n^2)$ (известен и более эффективный алгоритм со сложностью $O(n\log^2 n)$ [3].

Заключение

Приведём протокол разделения секрета в системах управления ключами и управления доступом на рисунке 2.

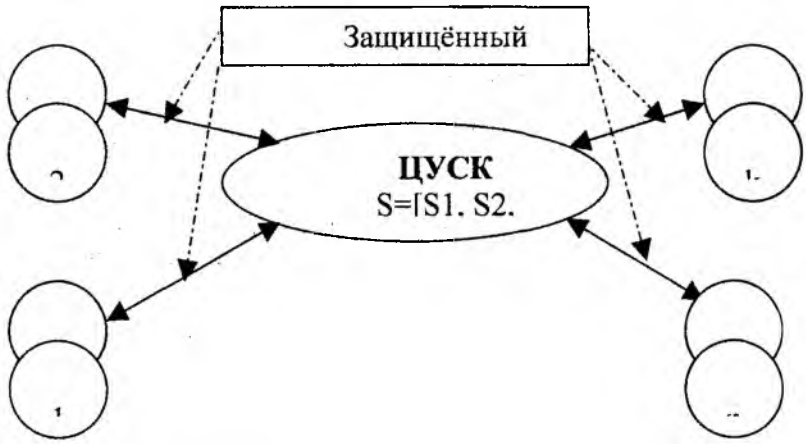

Рисунок 2. Схема установления секретного симметричного ключа путём разделения секрета по схеме Ади - Шамира

Проведённый сравнительный анализ показал, что наиболее предпочтительный криптопротокол разделения секрета, с точки зрения стойкости и надежности, является протокол Ади-Шамира, схема которого является совершённой. Протоколы такого класса могут использоваться в системах и технологиях, в которых требуется совместное управление доступом к критической информации и ресурсам.

Список литературы: 1. Simmons G.J. Contemporary Cryptology – The Science of Information Integrity. IEEE Press, 1992. 2. Shamir A. How to share a secret //Coom. Of the ACM, 1979, v22, № 11, pp. 612-613. 3. Rivest R.L. Multigrade cryptography Manuscript, 1996, ftp://theory.Ics.mit.edu/~rivest/publication.html. 4. McEliece R.J., Sarvate D.V. On sharing secrets and Reed-Solomon codes // Comm. of the ACM, Aug 1981, v. 24, № 9, pp. 583-584. 5. Blakley G.R. Safeguarding cryptographic keys // Proc of AFIPS National Computer Conference, 1979, 48, pp. 313-317. 6. Liu C.L. Introduction to combinatorial mathematics. New-York McGraw-Hill. 1968. 7. DeSantis A., Desmedt Y., Frankel Y., Yung M. How to share a function securely // Proc. of the 26th ACM Symposium on the Theory of Computing, 1994, pp. 522-533. 8. Вильямс криптография и защита систем. Принципы и практика 2-е издание. Изд. Москва-Санкт-Петербург-Киев 2001, 669с.

Харьковский национальный университет радиоэлектроники *Поступила в редколлегию 13.04.2002*