Федеральное государственное автономное образовательное учреждение высшего образования
Национальный исследовательский ядерный университет «МИФИ»

Кафедра «Криптология и кибербезопасность»

Криптографические протоколы

курс лекций

Запечников Сергей Владимирович,
профессор кафедры «Криптология
и кибербезопасность» НИЯУ МИФИ

Москва – 2018

Криптографические протоколы

курс лекций

Лекция 5.
Протоколы распределения ключей (окончание)

15 марта 2018 г.

Протокол MTI

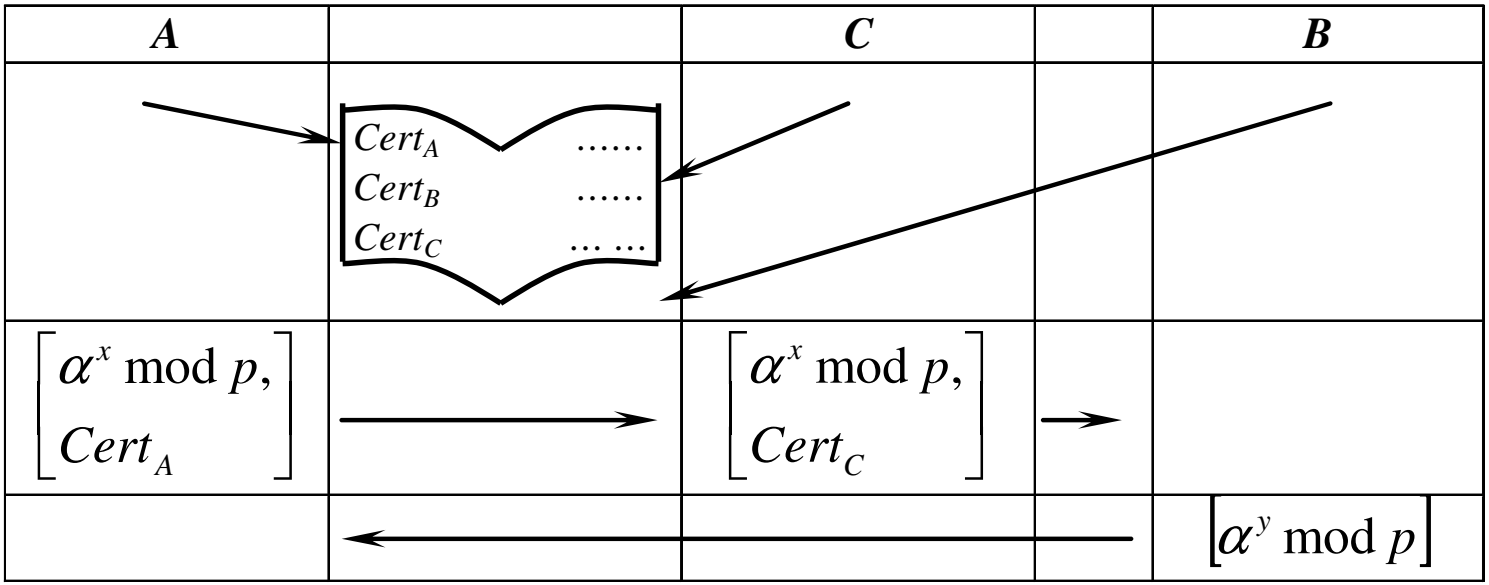
<table>
<tr><th colspan="4">Предварительный этап</th></tr>
<tr><th colspan="2">A</th><th></th><th>B</th></tr>
<tr><td colspan="2">a – случ., $1 \le a \le p-2$
$\left[z_A = \alpha^a \bmod p\right]$ →</td><td>p, α,
$Cert_A(z_A)$, $Cert_B(z_B)$
p – простое число,
$\alpha \in Z_p^*$ – образ. элемент,
$2 \le \alpha \le p-2$</td><td>← b – случ., $1 \le b \le p-2$
$\left[z_B = \alpha^b \bmod p\right]$</td></tr>
<tr><th colspan="4">Рабочий этап</th></tr>
<tr><th></th><th>A</th><th></th><th>B</th></tr>
<tr><td>1</td><td>x – случ.,
$1 \le x \le p-2$
$\left[m_{AB} = \alpha^x \bmod p\right]$</td><td>→</td><td></td></tr>
<tr><td>2</td><td></td><td>←</td><td>y – случ., $1 \le y \le p-2$
$\left[m_{BA} = \alpha^y \bmod p\right]$</td></tr>
</table>

Варианты построения протокола MTI

№ п/п	m_{AB}	m_{BA}	K_A	K_B	Общий ключ K
1	α^x	α^y	$m_{BA}^a \cdot z_B^x$	$m_{AB}^b \cdot z_A^y$	α^{bx+ay}
2	z_B^x	z_A^y	$m_{BA}^{a^{-1}} \cdot \alpha^x$	$m_{AB}^{b^{-1}} \cdot \alpha^y$	α^{x+y}
3	z_B^x	z_A^y	$m_{BA}^{a^{-1}x}$	$m_{AB}^{b^{-1}y}$	α^{xy}
4	z_B^{xa}	z_A^{yb}	m_{BA}^x	m_{AB}^y	α^{abxy}

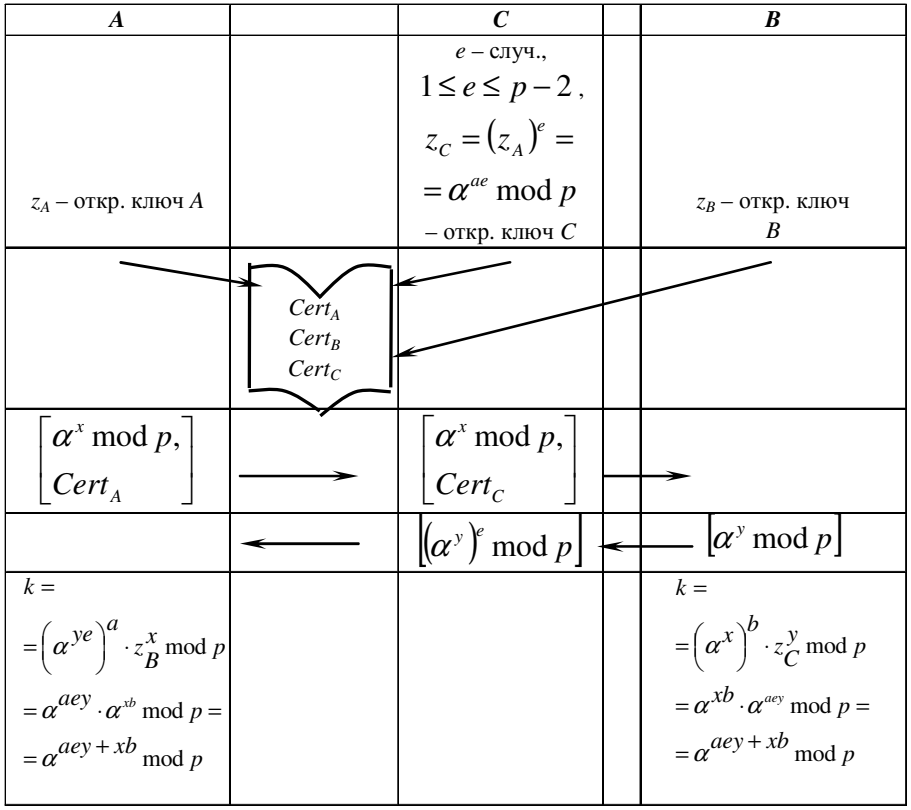
Атака на протокол MTI методом подстановки источника (с одинаковыми открытыми ключами)

Злоумышленник *C* регистрирует в удостоверяющем центре сертификат с таким же открытым ключом, как и *A*, а затем модифицирует сообщение, передаваемое от *A* к *B*. В результате *B* считает, что последующие сообщения зашифрованы на ключе $k = \alpha^{bx+ay} \bmod p$, исходящем от *C*, в то время как только *A* знает ключ *k* и может производить такие сообщения. Для избежания атаки необходимо проверять уникальность открытого ключа при регистрации сертификатов.



Атака на протокол MTI методом подстановки источника (с разными открытыми ключами)

C **регистрирует в удостоверяющем центре сертификат с открытым ключом** $\alpha^{ae} \bmod p$ **и подменяет сообщения, передаваемые участниками протокола друг другу. После осуществления такой атаки** ***A*** **полагает, что он выполнил обмен ключами с** ***B*****, а** ***B*** **полагает, что он выполнил обмен ключами с** ***C*****. Злоумышленник** ***C*** **не способен сам вычислить ключ** ***k*****, но вынуждает** ***B*** **делать неверные выводы. Для избежания атаки необходимо проверять знание секретного ключа при регистрации сертификатов.**



Протокол STS (station-to-station)

Протокол использует симметричную схему шифрования (E,D) и две схемы цифровой подписи вида $S_X(m) = (H(m))^{d_X} \bmod n_X$, $X = \{A, B\}$, ***H(m)<n_X*. На эту роль подходят схемы RSA или Рабина.**

Предварительный этап		
A		***B***
$n_A = p_A q_A$ (e_A, n_A) →	p, α, (e_A, n_A), (e_B, n_B)	← (e_B, n_B) $n_B = p_B q_B$
$d_A : e_A d_A \equiv$ $\equiv 1 \bmod (p_A - 1)(q_A - 1)$	p – простое число, $\alpha \in Z_p^*$ – образ. элемент, $2 \le \alpha \le p - 2$	$d_B : e_B d_B \equiv$ $\equiv 1 \bmod (p_B - 1)(q_B - 1)$

Рабочий этап			
	A		***B***
1	x – случ., $1 \le x \le p - 2$ $[\alpha^x \bmod p]$	→	
2		←	y – случ., $1 \le y \le p - 2$ $k = (\alpha^x)^y \bmod p$ $[\alpha^y \bmod p, E_k(S_B(\alpha^y, \alpha^x))]$
3	$k = (\alpha^y)^x \bmod p$, расшифровывает E_k, проверяет подпись B, в случае положительного исхода формирует $[E_k(S_A(\alpha^x, \alpha^y))]$	→	
4			расшифровывает E_k, проверяет подпись A, в случае положительного исхода принимает ключ k как общий с A

Конференц-связь

Конференц-связь **– это многосторонняя рассылка сообщений в режиме реального времени (число участников одновременного обмена сообщениями – не менее трех).**

В случае обмена секретной информацией всем участникам обмена необходимо иметь общий секретный ключ. *Протокол распределения ключей конференц-связи* – это обобщение протокола двустороннего распределения ключей с целью обеспечения трех или более участников общим секретным ключом.

Пусть *N* – множество участников системы конференц-связи, $M \subseteq N$ **– множества (группы) участников конференций,** $|N| = n, |M| = t, t \le n$ **.**

Требования к распределению ключей конференц-связи

К распределению ключей конференц-связи выдвигается несколько вполне очевидных требований:

1) различные группы участников *M* вырабатывают различные секретные ключи, так как участникам одной конференции не должны быть доступны данные, передаваемые в других конференциях);

2) эти сеансовые ключи – динамические (т.е. протоколы с предраспределенными ключами исключаются), более того, в различных конференциях, даже при одинаковом составе участников, должны быть различные ключи, так как очень высок риск их компрометации;

3) информация, которой обмениваются участники в процессе выполнения протокола распределения ключей – несекретная, т.е. передается по открытым каналам;

4) каждая сторона индивидуально вычисляет сеансовый ключ (это следствие из предыдущего требования).

Распределение ключей конференц-связи: протокол № 1

№ шага, r	U_0	…	$U_{i(-)1}$	U_i	$U_{i\oplus 1}$	…	U_{t-1}
$r=1$		…		x_i – случ.: $1 \le x_i \le p-1$ $\left[M_{i1} = g^{x_i} \bmod p\right]$		…	
…	…	…	…	…	…	…	…
$r \ge 2$		…		$\left[M_{i(-)1,r-1}\right]$ $M_{ir} = M_{i(-)1,r-1}^{x_i} \bmod p$ $\left(= g^{x_{i(-)(r(-)1)} \cdots x_{i(-)1} x_i} \bmod p\right)$ $\left[M_{ir}\right]$		…	
…	…	…	…	…	…	…	…
$r=t$		…		$\left[M_{i(-)1,t-1}\right]$ $M_{it} = M_{i(-)1,t-1}^{x_i} \bmod p$ $k_i = M_{it}$		…	

$k = k_0 = k_1 = \ldots = k_i = \ldots = k_{t-1} = g^{x_0 x_1 \ldots x_{t-1}} \bmod p$ – ключ конференции

Распределение ключей конференц-связи: протокол № 2

№ шага	U_0	…	$U_{i(-)1}$	U_i	$U_{i\oplus 1}$	…	U_{t-1}
1				r_i – случ., $1 \le r_i \le p-2$, $Z_i = \alpha^{r_i} \bmod p$			
	←	…		… $[Z_i]$ …	→	…	
2			→	$[Z_{i(-)1}]$ $[Z_{i\oplus 1}]$ ← $X_i = \left(\frac{Z_{i\oplus 1}}{Z_{i(-)1}}\right)^{r_i} \bmod p$ $\left(= \alpha^{r_{i\oplus 1} r_i - r_i r_{i(-)1}}\right)$			
	←	…	←	… $[X_i]$ …	→	…	
3			→	$[X_0]$ … $[X_{i(-)1}]$ $[X_{i\oplus 1}]$ … $[X_t]$ ← $K_i = \left(Z_{i(-)1}\right)^{tr_i} \cdot X_i^{t-1} \cdot X_{i\oplus 1}^{t-2} \cdot \ldots \cdot X_{i\oplus(t(-)3)}^{2} \cdot X_{i\oplus(t(-)2)} \bmod p$			
	→	…	→		←	…	
$K = K_0 = \ldots = K_i = \ldots = K_t$ – ключ конференции							

Схемы разделения секрета

Постановка задачи

Предположим, есть важная секретная информация, которую можно потерять. Ее опасно доверять кому-то одному. Возникает вопрос, как повысить надежность и безопасность ее хранения?

Первый путь **– сделать несколько копий этих данных и хранить их в разных местах. Резервирование обеспечивает высокую надежность хранения, но если скомпрометирована хотя бы одна копия, то секретность всей информация будет потеряна.**

Второй путь **– разделить секрет на несколько частей и хранить их в разных местах, при необходимости собирая вместе. Самый простой способ разделить секрет *s* на *n* частей – выбрать *n*-1 случайное число $s_1, s_2, ..., s_{n-1}$, а *n*-ю часть определить так: $s_n = s \oplus s_1 \oplus s_2 \oplus ... \oplus s_{n-1}$. Каждое число $s_i, i = \overline{1,n}$ носит название *доли секрета* (share). Доли создает носитель секрета *s*. Иногда это один из *n* участников, получающих доли, иногда – постороннее лицо, которое в этом случае называется *дилер*. Каждая доля s_i должна быть передана соответствующему участнику конфиденциально. Если эту долю видят и другие участники протокола, эта схема уже не работает. Для восстановления секрета *s* необходимо присутствие всех *n* сторон, имеющих доли секрета, которые должны выполнить операцию сложения: $s = s_1 \oplus s_2 \oplus ... \oplus s_n$. Так приходим к идее *схем разделения секрета* *(secret sharing scheme)* - сокращенно СРС. Такая схема обеспечивает высокую конфиденциальность (чтобы восстановить секрет, надо получить все его доли), но низкую надежность (если потеряна хотя бы одна доля, восстановить секрет уже будет невозможно).**

Пороговые схемы разделения секрета (СРС)

Мы хотим построить более гибкую схему. Пусть есть *n* участников криптосистемы. Мы хотим, чтобы любые *t* из них могли восстановить секрет, но никакие *t*-1 из них не смогли бы получить информацию о секрете. Число *t* (*t*<*n*) – параметр схемы, называемый порогом. Схема, обладающая такими свойствами, называется *(t,n)-пороговой СРС*. Она лучше, чем предыдущая, так как, если кто-то из участников потеряет свою долю или не будет участвовать в восстановлении секрета, секрет все равно можно восстановить и без этих долей.

Известны несколько математических методов реализации такой схемы. Однако далеко не все из них удобны на практике.

Геометрическая интерпретация пороговых СРС (1)

Схема Шамира **(*A. Shamir, 1979*) основана на хорошо известном математическом факте, который заключается в том, что через любые *t* точек на плоскости можно провести бесконечное множество кривых, описываемых многочленом *t*-го порядка, но через любые *t*+1 различные точки можно провести только единственную кривую, описываемую многочленом *t*-го порядка. Так, через любую точку на плоскости проходит бесконечное множество прямых линий, но через две различные точки – только единственная. Через любые две точки можно провести бесконечное множество парабол, но через любые три различные точки – только одну и т.д. Таким образом, если каждому из участников криптосистемы «выдать» по одной точке, то восстановить кривую можно будет только при достаточном количестве участников.**

Геометрическая интерпретация пороговых СРС (2)

Схема Блейкли **(*A. Blackley, 1979*) основана на следующих геометрических фактах. Одна прямая на плоскости описывает бесконечное множество точек, но любые две непараллельные прямые задают единственную точку их пересечения. Любые две некомпланарные плоскости в трехмерном пространстве пересекаются по прямой, которая задает бесконечное множество точек, но любые три некомпланарные плоскости пересекаются в единственной точке. Эти наблюдения по аналогии можно продолжить и в пространствах больших размерностей. Если каждому из участников криптосистемы «выдать» по одному уравнению плоскости (или гиперплоскости в пространствах размерности больше 3), то определить единственную точку их пересечения можно будет опять-таки при достаточном числе этих уравнений. В схеме Блейкли увеличение числа участников сопровождается ростом размерности пространства, в котором решается задача, что усложняет решение системы уравнений.**

Пример применения пороговых СРС

http://www.cryptopro.ru/products/hsm/atlix-hsm/description

«Атликс HSM в первую очередь предназначен для обеспечения безопасного хранения и использования закрытого ключа уполномоченного лица удостоверяющего центра, что обеспечивается выполнением всех криптографических операций, в том числе по генерации ключа уполномоченного лица в криптомодуле. ***Защита ключа уполномоченного лица удостоверяющего центра обеспечивается в том числе с использованием "раздельных секретов"*****, то есть** ***для активизации закрытого ключа одновременно необходимы три из пяти дополнительных закрытых ключей*****, хранящихся на процессорных картах РИК (российская интеллектуальная карта). Кроме этого, взаимодействие центра сертификации с криптомодулем возможно только после двусторонней криптографической аутентификации.»**

Математические основы СРС Шамира

В криптосистемах широко используется пороговая СРС Шамира, так как она допускает удобную геометрическую интерпретацию и легко обобщается для многочленов над конечными полями. Пусть *F* – конечное поле, $f(x)=a_0+a_1x+...a_{t-1}x^{t-1}, a_i \in F$ **– многочлен над полем *F*, т.е.** $f(x) \in F[x]$**. Известно, что такой многочлен обладает следующими свойствами.**

***1. Интерполируемость*. По данным *t* точкам многочлена:** $(x_1, y_1),...,(x_t, y_t)$**, где все** $x_1,...,x_t$ **различны,** $y_i = f(x_i)$**, можно найти его коэффициенты** $a_0, a_1,...,a_{t-1}$**. Алгоритм, делающий это, называется алгоритмом интерполяции.**

***2. Секретность*. По данным любым *t*-1 точкам полинома:** $(x_1, y_1),...,(x_{t-1}, y_{t-1})$**, где** $y_i = f(x_i)$**, никто не может ничего предполагать об a_0 – свободном члене *f(x)*.**

Эти свойства делают многочлены над конечными полями инструментом для построения пороговых криптосистем.

Протоколы СРС Шамира (1)

Рассмотрим (*t*,*n*)-пороговую СРС Шамира над полем Z_p, где *p* – большое простое число. Схема включает несколько протоколов.

Фаза инициализации. **Дилер *D* выбирает *n* различных ненулевых элементов поля Z_p, которые обозначаются $x_i, 1 \le i \le n, p \ge n+1$ – это точки, к которым «привязаны» участники. Часто выбирают $x_i \equiv i$, т.е. просто всем участникам схемы присваиваются порядковые номера. *D* передает x_i участнику P_i.**

***Распределение долей*:**

1) *D* хочет разделить секретный ключ $K \in Z_p$. *D* секретно, случайно и независимо друг от друга выбирает *t*-1 элемент поля $a_1, \ldots, a_{t-1}$, где $a_i \in Z_p$;

2) *D* конструирует многочлен степени, меньшей либо равной *t*-1, и вычисляет для $i = \overline{1,n}$: $y_i = a(x_i)$, где $a(x) = K + \sum_{m=1}^{t-1} a_m x^m \pmod p$, т.е. $K = a(0)$. Коэффициенты многочлена дилер хранит в секрете;

3) дилер по секретному и аутентичному каналу рассылает каждую из долей y_i соответствующему участнику P_i для всех $i = \overline{1,n}$.

Протоколы СРС Шамира (2)

Восстановление секрета **возможно двумя способами.**

I способ. Предположим, участники $P_{i_1},...,P_{i_t}$ **хотят восстановить секретный ключ *K*. Они имеют** (x_{i_j}, y_{i_j}) **и знают, что** $y_{i_j} = a(x_{i_j}), j = \overline{1,t}$**, где** $a(x) \in Z_p[x]$ **– неизвестный многочлен, выбранный *D*. Так как** $a(x)$ **имеет степень, меньшую либо равную *t*-1,** $a(x)$ **может быть записан в виде:**

$$a(x) = a_0 + a_1 x + ... + a_{t-1} x^{t-1},$$

где $a_0, a_1, ..., a_{t-1}$ **– неизвестные элементы поля Z_p, и** $a_0 = K$**.**

Они получают систему *t* линейных уравнений с *t* неизвестными $a_0, a_1, ..., a_{t-1}$ **над полем Z_p:**

$$y_{i_j} = a_0 + \sum_{m=1}^{t-1} a_m x_{i_j}^m, j = \overline{1,t}.$$

Если уравнения линейно независимы, система имеет единственное решение. Они могут решить систему относительно неизвестных коэффициентов и получить a_0.

Утверждение. **(*t*,*n*)-пороговая СРС Шамира позволяет однозначно восстанавливать секрет любой группе из *t* участников схемы и обеспечивает совершенную секретность (теоретико-информационную стойкость) против попытки вычисления секрета любой группой из *j* участников, обладающих неограниченной вычислительной мощностью (*j*<*t*).**

Доказательство утверждения о свойствах СРС Шамира

У каждого участника схемы есть пара точек: $(x_{i_j}, y_{i_j}): y_{i_j} = a(x_{i_j}), j = \overline{1,t}$, где $a(x) = a_0 + a_1 x + ... + a_{t-1} x^{t-1}$, $a_0 = K$. Получается следующая система линейных уравнений, решаемая в Z_p:

$$\begin{cases} a_0 + a_1 x_{i_1} + a_2 x_{i_1}^2 + ... + a_{t-1} x_{i_1}^{t-1} = y_{i_1} \\ a_0 + a_1 x_{i_2} + a_2 x_{i_2}^2 + ... + a_{t-1} x_{i_2}^{t-1} = y_{i_2} \\ ..... \\ a_0 + a_1 x_{i_t} + a_2 x_{i_t}^2 + ... + a_{t-1} x_{i_t}^{t-1} = y_{i_t} \end{cases},$$

или в матричной форме:

$$\begin{pmatrix} 1 & x_{i_1} & x_{i_1}^2 & ... & x_{i_1}^{t-1} \\ 1 & x_{i_2} & x_{i_2}^2 & ... & x_{i_2}^{t-1} \\ ... & ... & ... & ... & ... \\ 1 & x_{i_t} & x_{i_t}^2 & ... & x_{i_t}^{t-1} \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ ... \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_{i_1} \\ y_{i_2} \\ ... \\ y_{i_t} \end{pmatrix}.$$

В левой части системы стоит матрица коэффициентов A, имеющая специальный вид: каждая j-я ее строка состоит из коэффициентов x_{i_j}, последовательно возводимых во все степени от 0 до t-1. Это так называемая матрица Вандермонда. Ее определитель вычисляется по формуле:

$$\det A = \prod_{1 \le j < k \le t} \left(x_{i_k} - x_{i_j} \right) \bmod p \, .$$

Так как все x_i различны, $\forall \left(x_{i_k} - x_{i_j} \right) \neq 0$. Произведение вычисляется в поле Z_p. Произведение ненулевых элементов в поле всегда отлично от 0. Следовательно, $\det A \neq 0$. Следовательно, система имеет единственное решение над полем Z_p, а значит, любая группа из t участников может однозначно восстановить ключ $K=a_0$.

Пусть теперь группа из t-1 участников $P_{i_1},...,P_{i_{t-1}}$ пытается вычислить K. Они получат систему из t-1 уравнений с t неизвестными. Пусть y_0 – какое-то предполагаемое (или случайно взятое) ими значение ключа. Так как известно, что $K = y_0 = a_0 = a(0)$, это соотношение дает им t-е уравнение. Матрица коэффициентов результирующей системы из t уравнений с t неизвестными снова будет матрицей Вандермонда, а значит, снова будет иметь единственное решение.

Следовательно, для каждого предполагаемого значения ключа существует полином $a_{y_0}(x) : y_{i_j} = a_{y_0}\left(x_{i_j}\right), j = \overline{1, t-1}, y_0 = a_{y_0}(0)$, коэффициенты которого получены из решения системы. Таких полиномов существует столько же, сколько может быть различных значений ключа $K=y_0$. Значит, никакая группа из t-1 участников не может получить никакой дополнительной информации о ключе. Лучший способ узнать ключ – это попытаться угадать его, что возможно с вероятностью $\frac{1}{2^{|K|}}$ и соответствует понятию о теоретико-информационной безопасности криптосистемы по Шеннону. Утверждение доказано.

Протоколы СРС Шамира (3)

<u>II способ.</u> Восстановить разделенный секрет можно и другим, более простым способом. Воспользуемся интерполяционной формулой Лагранжа:

$$a(x)=\sum_{j=1}^{t} y_{i_j} \prod_{\substack{1\le k\le t,\\ k\ne j}} \frac{x-x_{i_k}}{x_{i_j}-x_{i_k}}.$$

Мы имеем *t* пар чисел $(x_{i_j}, y_{i_j}), j=\overline{1,t}$ **, и доказали, что многочлен единственный. Следовательно, формула Лагранжа даст нам единственный верный результат.**

Формулу можно упростить, так как участникам группы не нужно вычислять все коэффициенты многочлена, а только свободный член *K=a(0)*:

***x*=0** $$K=\sum_{j=1}^{t} y_{i_j} \prod_{\substack{1\le k\le t,\\ k\ne j}} \frac{x_{i_k}}{x_{i_k}-x_{i_j}}.$$

Обозначим коэффициенты интерполяции в формуле Лагранжа: $b_j=\prod_{\substack{1\le k\le t,\\ k\ne j}} \frac{x_{i_k}}{x_{i_k}-x_{i_j}}, j=\overline{1,t}$ **. Они могут быть вычислены предварительно, так как все** x_{i_j}, x_{i_k} **общеизвестны. Остается вычислить ключ как линейную комбинацию *t* долей секрета:** $K=\sum_{j=1}^{t} b_j y_{i_j}$ **.**

Схема проверяемого разделения секрета Фельдмана (1)

В СРС Шамира нечестный дилер *D* может раздать участникам $P_1,...,P_n$ несовместные доли, из которых они никогда не восстановят секретный ключ *K*. Необходимо предложить такую схему, в которой можно было бы проверить совместимость долей секрета. Известны две СРС, решающих эту задачу, основанные на сложности задачи дискретного логарифмирования: СРС Фельдмана и СРС Педерсена.

Пусть *p,q* – большие простые числа, $p-1\equiv 0(\bmod q)$. *g* – элемент порядка *q* группы Z_p^*, т.е. $g^q\equiv 1(\bmod p)$. Для любой доли y_i вычисляется открытая величина $z_i=g^{y_i}(\bmod p)$, которая по свойству гомоморфизма функции экспоненцирования позволяет каждому P_i проверять, что его собственная доля секрета совместима с открытой информацией.

***D* выбирает многочлен $a(x)\in Z_q[x]$ с коэффициентами $a_0=K,a_1,...,a_{t-1}$ и раздает всем участникам соответствующие проверочные значения $g^{a_0},g^{a_1},..,g^{a_{t-1}}$.**

Положим $x_i\equiv i,i=\overline{1,n}$. Дилер *D* секретно передает каждому участнику схемы P_i предназначенную ему долю $y_i=a(i)\bmod q$.

Схема проверяемого разделения секрета Фельдмана (2)

Каждый участник P_i проверяет свою долю, используя проверочное уравнение:

$$g^{y_i} \stackrel{?}{=} \left(g^{a_0}\right) \cdot \left(g^{a_1}\right)^i \cdot \left(g^{a_2}\right)^{i^2} \cdot \ldots \cdot \left(g^{a_{t-1}}\right)^{i^{t-1}} \left(\mathrm{mod}\, p\right).$$

В случае положительного результата проверки P_i распространяет всем остальным участникам схемы сообщение, что он принял свою долю, так как $y_i = a_0 + a_1 i + a_2 i^2 + \ldots + a_{t-1} i^{t-1} \left(\mathrm{mod}\, q\right)$. В случае отрицательного результата он делает вывод, что ему дилером была выдана неверная доля.

Если все $P_i, i = \overline{1,n}$ распространили сообщения о принятии долей, фаза распределения долей завершилась успешно. Такая же проверка может выполняться при восстановлении секрета.

Заметим, что в схеме проверяемого разделения секрета каждый может проверить только свою долю, но не чужую – для этого нужны схемы публично проверяемого разделения секрета.

Схема проверяемого разделения секрета Педерсена (1)

Числа *p,q,g,K* определяются так же, как и в предыдущей схеме. $h \in Z_p^*$ **– открытое общедоступное число, но такое, что** $d \in Z_q$**, где** $g^d = h(\mathrm{mod}\ p)$ **неизвестно.**

Чтобы распределить секрет *K*, дилер выбирает два многочлена $\delta(\cdot), \gamma(\cdot)$ **степени *t*-1 над полем Z_q с коэффициентом** $\delta_0 = K$ **и случайными коэффициентами** $\{\delta_m\}_{m\in\{1,\ldots,t-1\}}$ **и** $\{\gamma_m\}_{m\in\{0,\ldots,t-1\}}$ **соответственно, т.е.**

$$\delta(z) = \delta_0 + \delta_1 z + \delta_2 z^2 + \ldots + \delta_{t-1} z^{t-1} \in Z_q[z], \qquad \delta_0 = K,$$

$$\gamma(z) = \gamma_0 + \gamma_1 z + \gamma_2 z^2 + \ldots + \gamma_{t-1} z^{t-1} \in Z_q[z], \qquad \gamma_0 \text{ - случ.,}$$

и распространяет всем участникам схемы $P_i, i = \overline{1,n}$ **величину** $\varepsilon_m = g^{\delta_m} \cdot h^{\gamma_m} (\mathrm{mod}\ p), m = \overline{0,t-1}$**. Затем дилер *D* секретно пересылает всем P_i,** $i = \overline{1,n}$ **их доли** $\{u_i, w_i\}$**, где** $u_i = \delta(i), w_i = \gamma(i)$**.**

Проверочное уравнение для участника P_i:

$$g^{u_i} h^{w_i} \stackrel{?}{=} (\varepsilon_0) \cdot (\varepsilon_1)^i \cdot (\varepsilon_2)^{i^2} \cdot \ldots \cdot (\varepsilon_{t-1})^{i^{t-1}} (\mathrm{mod}\ p).$$

Схема проверяемого разделения секрета Педерсена (2)

При положительном результате проверки будет выполнено равенство:

$$\left(g^{\delta_0}h^{\gamma_0}\right)\cdot\left(g^{\delta_1}h^{\gamma_1}\right)^{i}\cdot\ldots\cdot\left(g^{\delta_{t-1}}h^{\gamma_{t-1}}\right)^{i^{t-1}} = g^{\delta_0+\delta_1 i+\ldots+\delta_{t-1}i^{t-1}}\cdot h^{\gamma_0+\gamma_1 i+\ldots+\gamma_{t-1}i^{t-1}} =$$

$$= g^{\delta(i)}\cdot h^{\gamma(i)}(\mathrm{mod}\ p).$$

Схема Педерсена обеспечивает теоретико-информационную секретность, так как, даже если вычислительно неограниченный противник, видящий $g^{K}h^{\gamma_0}(\mathrm{mod}\,p)$, умеет решать задачу дискретного логарифмирования и может вычислить $K+d\gamma_0(\mathrm{mod}\,q)$, это все равно не дает ему никакой информации о секрете *K*. Таким образом, схема Педерсена не позволяет противнику вычислить g^{K}, тогда как схема Фельдмана обладает лишь теоретико-сложностной стойкостью относительно знания противником g^{K}.

Пороговая криптография

- **Пороговые схемы цифровой подписи**
- **Пороговые схемы открытого шифрования**
- **Пороговые симметричные схемы шифрования**
- **Пороговые симметричные схемы аутентификации**

и др.