УДК 681.3

РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ В ГРУППАХ С ДИНАМИЧЕСКИМ СОСТАВОМ УЧАСТНИКОВ

И.А. Фомина, А.В. Капренин

Нижегородский госуниверситет им. Н.И. Лобачевского

fomis54@mail.ru

Поступила в редакцию 23.03.2010

Обсуждается проблема обмена ключами между абонентами для передачи информации по открытым каналам связи. Особое внимание уделяется вопросам распределения ключей в группах с динамическим составом участников. Рассматриваются основные операции, необходимые для реализации протокола обмена. Приводится пример, иллюстрирующий работу предложенного протокола.

Ключевые слова: криптографическая система, открытый и закрытый ключ, протоколы распределения ключей, эллиптические кривые.

Проблема обеспечения компьютерной безопасности – многоаспектная задача, решить которую можно только с помощью комплексного подхода, используя совокупность правовых, организационных, технических и программных средств защиты информации. Одним из наиболее эффективных программных средств обеспечения информационной безопасности в информационно-телекоммуникационных системах являются криптографические средства и методы защиты информации. В основе криптографических методов лежит понятие криптографического преобразования информации. Основные задачи криптографии – обеспечение конфиденциальности (защита информации от внешнего противника), обеспечение целостности (гарантия обеспечения поступления информации из достоверного источника и в неискаженном виде), обеспечение «неотслеживаемости» сообщений (гарантия анонимности отправителя и получателя информации).

Одним из наиболее важных компонентов любой криптографической системы является ключ. Еще в IX веке голландцем Киркхофором было сформулировано основное правило стойкости криптосистемы: «стойкость шифра должна определяться только секретностью ключа» (алгоритм считается известным). Отсюда следует, что как бы ни были сложны и надежны криптографические системы, их слабое место при практической реализации – проблема *распределения ключей*. Для того чтобы был возможен обмен конфиденциальной информацией между двумя субъектами, ключ должен быть сгенерирован одним из них, а затем каким-то образом в конфиденциальном порядке передан другому.

Проблема распределения ключей в криптосистеме является одной из наиболее важных и дорогостоящих процедур, так как основным требованием конфиденциальности и аутентичности является смена ключей после каждого сеанса обмена информацией. Криптосистема обладает прогрессивной секретностью, если компрометация долгосрочного секретного ключа в какой-то момент времени не приводит к нарушению конфиденциальности, осуществлявшейся с использованием этого ключа.

В современной криптографии задача управления ключами решается с помощью криптографических протоколов, основой которых является генерация и распределение ключей между пользователями. Существуют схемы распределения ключей в симметричных криптографических системах, где обязательным компонентом является наличие защищенного канала связи, по которому происходит передача секретного ключа [1]. Однако наиболее эффективными являются методы двухключевой криптографии (системы с открытыми ключами), позволяющие осуществить передачу секретного ключа по открытым каналам связи. Суть их состоит в том, что каждым адресатом генерируются два ключа, связанных между собой по определенному правилу. Один ключ объявляется *открытым*, а другой *закрытым*. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне.

Проблема распределения ключей была рассмотрена в работе Диффи и Хеллмана [2], где разработана схема шифрования с открытым ключом. Их протокол распределения ключей, названный протоколом Диффи – Хеллмана об-

мена ключей, позволяет двум сторонам достигнуть соглашения о секретном ключе по открытому каналу связи без предварительной личной встречи. Его стойкость основывается на трудноразрешимой проблеме дискретного логарифмирования в конечной абелевой группе A. Алгоритмы, лежащие в основе криптосистем с открытым ключом, имеют следующие недостатки:

- генерация ключей основана на генерации больших простых чисел;
- процедуры шифрования и расшифровки связаны с возведением в степень по модулю многозначных чисел.

Обе эти процедуры занимают много процессорного времени, в связи с этим быстродействие криптосистем с открытым ключом в сотни, тысячи раз меньше, чем в классических симметричных системах.

Криптография с использованием эллиптических кривых – подход, который появился сравнительно недавно (ECC – Elliptic curve cryptography) [3]. Здесь, вместо работы строго с остатками по модулю p, рассматриваются геометрические отношения. Привлекательность подхода на основе эллиптических кривых заключается в том, что в сложных геометрических вычислениях существует более трудный для раскрытия аналог проблемы дискретного логарифма. Кроме того, для этой задачи требуются более короткие простые числа, и работать с ними криптографические алгоритмы будут значительно быстрее. Современные реализации алгоритмов на основе эллиптических кривых показывают, что они более эффективны, чем другие системы с открытыми ключами (их производительность приблизительно на порядок выше, чем производительность RSA, Диффи – Хеллмана, DSA).

В настоящее время актуальной задачей является распределение ключей не только для двух, но и для группы участников. Такая задача возникает при организации безопасной связи внутри групп абонентов, при аутентификации участников группы, при формировании групповой цифровой подписи, при организации конференц-связи и т.д. Протоколы распределения ключей для конференц-связи являются обобщением протоколов распределения ключей для двух сторон. При этом необходимо учитывать, что, несмотря на внешнюю схожесть, протоколы распределения ключей фундаментально отличаются от динамического распределения ключей между двумя сторонами. Основные требования к протоколам распределения ключей для конференц-связи:

- различные группы участников конференц-связи должны вырабатывать различные сеансовые ключи;
- сеансовые ключи должны распределяться динамически;
- каждая сторона должна индивидуально вычислять сеансовый ключ.

Протокол обмена ключами для групп с динамическим составом участников на основе эллиптических кривых. В основу реализации этих протоколов были положены протоколы обмена ключами в циклических группах простого порядка [4, 5].

Рассмотрим основные операции, которые позволяют реализовать такой протокол.

1. *Операции для одного участника группы* включают в себя добавление или удаление одного участника группы. Данные ситуации появляются, когда кто-то хочет присоединиться к группе или покинуть ее.

2. *Операции для нескольких участников* также включают в себя добавление и удаление. Однако есть отличия, обусловленные желанием проводить операции с несколькими участниками сразу, а не с каждым в отдельности:

- массовое присоединение: несколько участников хотят присоединиться к существующей группе;
- слияние групп: две или более групп желают соединиться в одну;
- массовый выход из группы: несколько участников хотят покинуть группу;
- разделение групп: группа распадается на две или более частей.

3. *Операции по обновлению ключа* обусловлены двумя причинами:

- ограничением шифртекста, получаемого на одном ключе для ограничения возможности получения пар открытый текст/шифртекст с целью проведения криптоанализа (время жизни ключа определяется выбранной политикой);
- предохранением от компрометации текущего ключа или вклада каждого участника.

В качестве основы для этого протокола используется аутентичный протокол для групп n участников на основе эллиптических кривых. Пусть $M=\{M_1, M_2,..., M_n\}$ – множество пользователей, которым необходимо выработать общий ключ S_n. Протокол выполняется в три этапа. На первом этапе ($n-1$ шагов) идет сбор информации от отдельных участников группы. Участник M_i выбирает случайное число $r_i \in Z_p^*$, $i = 1,\ldots, n-1$ (Z_p^* – циклическая группа поряд-

ка p конечного поля), которое будет использоваться в качестве кратковременного секретного ключа i-го участника. Затем он передает следующему $(i+1)$-му участнику сообщение, содержащее i значений, которые являются комбинацией ключей, известных ему, дополненное собственным ключом. На втором этапе всем рассылается материал для вычисления общего ключа. Участник M_n выбирает случайное число $r_n \in Z_p^*$ и отправляет всем участникам значения полученных им ключей: $M_n \to M_i$. Групповой ключ M_n вычисляет как $S_n = r_1 r_2 \ldots r_n G$ (G – образующая точка эллиптической кривой, $r_i G$ – кратковременный открытый ключ i-го участника). И, наконец, на третьем этапе каждый участник вычисляет групповой ключ $S_n = r_i\left(\frac{r_1 \ldots r_n}{r_i} K_{in} G\right) K_{in}^{-1} = r_1 r_2 \ldots r_n G$ (K_{in} – общий долговременный секрет пары участников i и n, $k_i k_n G \to Q_x \to Q_x^{-1} = K_{in}^{-1}$, k_i – долговременный секретный ключ i-го участника). Последний участник M_n называется *контролирующим группы*, так как через него проводятся все ключевые операции протокола.

Операция присоединения. Операция добавляет нового участника M_{n+1} к группе из n участников. Во время операции вычисляется новый групповой ключ S_{n+1}, и M_{n+1} становится новым контролирующим группы. В предположении, что M_n является текущим контролирующим группы, протокол выглядит следующим образом:

Этап 1. Контролирующий группы M_n вырабатывает новое случайное значение $r_n' \in Z_p^*$ и вычисляет множество $M = \left\{\frac{r_1 \ldots r_n'}{r_i} G\right\} \bigcup \{r_1 \ldots r_{n-1} G\} \bigcup \{r_1 \ldots r_{n-1} r_n' G\}$ для всех $i \in [1, n-1]$

$$M_n \to M_{n+1}: M.$$

Этап 2. M_{n+1} вырабатывает случайное значение $r_{n+1} \in Z_p^*$

$$M_{n+1} \to M_i: \frac{r_1 \ldots r_{n-1} r_n' r_{n+1}}{r_i} K_{in+1} G, i \in [1, n-1]$$

$$M_{n+1} \to M_n: r_1 \ldots r_{n-1} r_{n+1} K_{nn+1} G.$$

Здесь $K_{in+1} = Q_x$ – общий долговременный секрет участников M_i и M_{n+1}, где $Q = k_i k_{n+1} G$, а Q_x – x-координата этой точки.

Групповой ключ M_{n+1} вычисляет как $S_{n+1} = r_1 r_2 \ldots r_n' r_{n+1} G$.

Этап 3. Участник M_i находит:

$$k_i k_{n+1} G \to Q_x \to Q_x^{-1} = K_{in+1}^{-1}.$$

Каждый участник M_i вычисляет групповой ключ:

$$S_{n+1} = r_i\left(\frac{r_1 \ldots r_{n+1}}{r_i} K_{in+1} G\right) K_{in+1}^{-1} = r_1 r_2 \ldots r_{n+1} G.$$

Оценим число операций умножения на точку кривой, требуемых для выполнения присоединения участника:

на этапе $1 - n - 1 + 1 + 1 = n + 1$;

на этапе $2 - n + 1$ (вычисление ключа);

на этапе $3 - n$.

Итак, получаем $3n + 2$ операции умножения на точку. Однако можно считать, что на последнем этапе все участники выполняют действие (вычисление группового ключа) одновременно, и принять число операций как 1. Тогда получаем $2n + 3$ операций умножения.

Операция слияния. Операция используется для добавления $k > 0$ участников к существующей группе из $n > 1$ участников. Пусть $m = n + k$. Во время операции вырабатывается новый групповой ключ S_m, и M_m становится новым контролирующим группы. В предположении, что M_n является текущим контролирующим группы, протокол выглядит следующим образом:

Этап 1. Контролирующий группы M_n вырабатывает новое случайное значение $r_n' \in Z_p^*$

$$M_n \to M_{n+1}: r_1 \ldots r_{n-1} r_n G\, r_n^{-1}\ r_n' = r_1 \ldots r_{n-1}\ r_n' G.$$

Этап 2. Участник M_j ($j \in [n+1, m-1]$) вырабатывает случайное значение $r_j \in Z_p^*$

$$M_j \to M_{j+1}: r_1 \ldots r_{n-1}\ r_n' r_{n+1} \ldots r_j G.$$

Этап 3. Участник M_m вырабатывает случайное значение $r_m \in Z_p^*$

$M_m \to$ всем участникам:

$r_1 \ldots r_{n-1}\ r_n'\ r_{n+1} \ldots r_{m-1} G.$

Групповой ключ M_m вычисляет как $S_m = r_1 r_2 \ldots\ r_n' \ldots r_{m-1} r_m G$.

Этап 4

$$M_i \to M_m: \frac{r_1 \ldots r_n' \ldots r_{m-1}}{r_i} G, i \in [1, m-1]$$

Этап 5

$$M_m \to M_i: \frac{r_1 \ldots r_n' \ldots r_{m-1} r_m}{r_i} K_{im} G, i \in [1, m-1]$$

Этап 6. Участник M_i ($i \in [1, m-1]$) вычисляет групповой ключ:

$$r_i \frac{r_1 \ldots r'_n \ldots r_{m-1} r_m}{r_i} K_{im} K_{im}^{-1} G = r_1 \ldots r_m G .$$

На первый взгляд может показаться, что этапы 4–5 являются лишними и на 4 этапе можно сразу же пересылать участникам $r_1 r_2 \ldots r'_n \ldots r_{m-1} r_m K_{im} G$. Однако в таком случае протокол не будет обладать свойством совершенной опережающей секретности (при компрометации долговременного секрета K_{im} злоумышленник сможет найти сеансовый ключ).

Подсчитаем число операций умножения, требующихся для выполнения слияния:

- на этапе 1 – 1;
- на этапе 2 – $m - n - 1$;
- на этапе 3 – 1;
- на этапе 4 – $m - 1$ (или 1, если считать вычисления одновременными);
- на этапе 5 – $m - 1$;
- на этапе 6 – $m - 1$ (или 1, если считать вычисления одновременными).

Таким образом, общее число операций умножения на точку при слиянии равно: $4m - n - 2$ или $2m - n + 2$ (если на шагах 4, 6 считать выполнение операций одновременно), где $m = n + k$.

Операция присоединения также может быть использована для добавления k участников к группе. Это потребует повторить операцию присоединения k раз – соответственно возрастает трудоемкость операции. Таким образом, для массового добавления участников группы лучше использовать операцию слияния. В то же время для добавления одного участника можно использовать операцию слияния. В этом случае получаем: $2(n + 1) - n + 2 = n + 4$ операций умножения, в то время как при присоединении одного участника требовалось $2n + 3$ операций умножения. Из этого следует, что при добавлении любого числа новых участников группы лучше использовать операцию слияния.

Операция выхода из группы. Пусть из группы выходят k участников. Во время операции вычисляется новый групповой ключ S_{n-k}. Обозначим $\{d\}$ множество индексов выходящих участников. При этом если из группы не выходит контролирующий, то он остается им в новой группе, если выходит – то новым контролирующим становится последний невышедший (по индексу) участник. Отметим, что операция выхода из группы также может быть реализована несколькими способами. Приведем два варианта реализации.

Вариант 1

Этап 1. Новый контролирующий группы $M_{n'}$ вырабатывает новое случайное значение $r'_{n'} \in Z_p^*$ ($n' = n$, если старый контролирующий не выходит из группы, и $n' = n - j$, если контролирующим становится последний не вышедший из группы участник).

$$M_{n'} \to M_i: \frac{r_1 \ldots r'_{n'}}{r_i} K_{in'} G, i \notin \{d\}$$

Групповой ключ $M_{n'}$ вычисляет как $S_{n-k} = r_1 r_2 \ldots r'_{n'} G$.

Этап 2. Участник M_i вычисляет групповой ключ как

$$S_{n-k} = r_i \frac{r_1 \ldots r'_{n'}}{r_i} K_{in'} K_{in'}^{-1} G, i \notin \{d\} .$$

Пример, иллюстрирующий работу протокола. Пусть в группе 5 участников. В соответствии с аутентичным протоколом для групп ключ формируется следующим образом:

Этап 1

$M_1 \to M_2$: $r_1 G$
$M_2 \to M_3$: $r_1 G$, $r_2 G$, $r_1 r_2 G$
$M_3 \to M_4$: $r_1 r_2 G$, $r_1 r_3 G$, $r_2 r_3 G$, $r_1 r_2 r_3 G$
$M_4 \to M_5$: $r_1 r_2 r_3 G$, $r_1 r_2 r_4 G$, $r_1 r_3 r_4 G$, $r_2 r_3 r_4 G$, $r_1 r_2 r_3 r_4 G$

Этап 2

$M_5 \to M_1$: $r_2 r_3 r_4 r_5 K_{15} G$
$M_5 \to M_2$: $r_1 r_3 r_4 r_5 K_{25} G$
$M_5 \to M_3$: $r_1 r_2 r_4 r_5 K_{35} G$
$M_5 \to M_4$: $r_1 r_2 r_3 r_5 K_{45} G$
$S_5 = r_1 r_2 r_3 r_4 r_5 G$

Этап 3

M_1, M_2, M_3, M_4: $S_4 = S_5 = r_1 r_2 r_3 r_4 r_5 G$

а) из группы выходят участники M_2, M_3 (контролирующим остается M_5)

Этап 1

$M_5 \to M_1$: $r_2 r_3 r_4 r'_5 K_{15} G$
$M_5 \to M_4$: $r_1 r_2 r_3 r'_5 K_{45} G$

Этап 2

$S'_5 = r_1 r_2 r_3 r_4 r'_5 G$

б) из группы выходят участники M_3, M_5 (контролирующим становится M_4)

Этап 1

$M_4 \to M_1$: $r_2 r_3 r'_4 K_{14} G$
$M_4 \to M_2$: $r_1 r_3 r'_4 K_{24} G$

Этап 2

$S'_3 = r_1 r_2 r_3 r'_4 G$

Отметим, что в этом варианте реализации протокола участникам требуется хранить информацию, которую они получают при формировании ключа в первый раз (так как она используется при создании нового ключа). Это, очевидно, требует дополнительных затрат.

Вариант 2

Этап 1. Новый контролирующий группы $M_{n'}$ вырабатывает новое случайное значение $r'_{n'} \in Z_p^*$.

$M_{n'} \to M_i$: $\mathrm{S}_n r_{n'}^{-1}, i \notin \{d\}$

Групповой ключ $M_{n'}$ вычисляет как $S_{n-k} = r_{1\ldots} r_{n'}^{-1} r'_{n'} G$.

Этап 2

$$M_i \to M_{n'}: \frac{r_1 \ldots \mathrm{r}_{n'-1} r_{n'+1} \ldots r_n}{r_i} G, \; i \notin \{d\}$$

Этап 3.

$$M_{n'} \to M_i: \frac{r_1 \ldots \mathrm{r}_{n'-1} r'_{n'} r_{n'+1} \ldots r_n}{r_i} K_{in'} G, \; i \notin \{d\}$$

Этап 4. Участник M_i вычисляет групповой ключ как $S_{n-k} = r_i \frac{r_1 \ldots r'_{n'} \ldots r_n}{r_i} K_{in'} K_{in'}^{-1} G, \; i \notin \{d\}$

В этом варианте протокола хранить старую информацию не требуется, для создания нового ключа требуется наличие лишь секретных значений r_i и старого ключа. Однако трудоемкость вычислений при этом оказывается больше, чем в первом варианте.

Операция обновления ключа выполняет замену группового ключа на новый. Эта операция выглядит так же, как и операция выхода из группы с $k = 0$. Подобно операции выхода из группы можно привести 2 варианта реализации обновления ключа.

Вариант 1

Этап 1. Контролирующий группы M_n вырабатывает новое случайное значение $r'_n \in Z_p^*$.

$$M_n \to M_i: \frac{r_1 \ldots r'_n}{r_i} K_{in} G \; .$$

Групповой ключ $M_{n'}$ вычисляет как $S'_n = r_1 r_2 \ldots r'_n G$.

Этап 2. Участник M_i вычисляет групповой ключ как $S'_n = r_i \frac{r_1 \ldots r'_n}{r_i} K_{in} K_{in}^{-1} G$.

Вариант 2

Этап 1. Контролирующий группы M_n вырабатывает новое случайное значение $r'_n \in Z_p^*$.

$M_n \to M_i$: $\mathrm{S}_n r_n^{-1}$.

Групповой ключ M_n вычисляет как $S'_n = r_1 \ldots r_n^{-1} r'_n G$.

Этап 2

$$M_i \to M_n: \frac{r_1 \ldots r_{n-1}}{r_i} G \; .$$

Этап 3

$$M_n \to M_i: \frac{r_1 \ldots r_{n-1} r'_n}{r_i} K_{in} G \; .$$

Этап 4. Участник M_i вычисляет групповой ключ как $r_i \frac{r_1 \ldots r_{n-1} r'_n}{r_i} K_{in} K_{in}^{-1} G$.

Построенный протокол обмена ключами для групп с динамическим составом участников обладает свойствами контрибутивности, совершенной опережающей секретности, аутентичности, может обеспечивать подтверждение ключа.

Список литературы

1. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. СПб.: Изд-во «Лань», 2000. 224 с.

2. Диффи У., Хеллман М.Э. Защищённость и имитостойкость: Введение в криптографию // ТИИЭР. 1979. Т. 67, № 3. С. 71–109.

3. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. М.: Научный мир, 2004. 173 с.

4. Alves-Foss J. An efficient secure authenticated group key exchange algorithm for large and dynamic groups // 23rd National Information Systems Security Conference. URL: http://sceas.csd.auth.gr/php/search.php4?author_id=9494

5. Ateniese G., Steiner M., Tsudik G. Authenticated Group Key Agreement and Friends // 5th ACM Conference on Computer and Communications Security. URL: http://www.informatik.uni-trier.de/~ley/db/conf/ccs/ccs1998.html

KEY ALLOCATION IN GROUPS WITH DYNAMIC MEMBER COMPOSITION

I.A. Fomina, A.V. Kaprenin

The problem of key exchange between subscribers in order to transfer information through open channels is considered. Special attention is given to the key allocation in groups with dynamic member composition. The basic operations essential for Exchange Protocol realization are considered. An example is given that illustrates the operation of the Protocol proposed.

Keywords: cryptographic system, open and security keys, key allocation protocols, elliptic curves.