Сударев Игорь Васильевич, доктор технических наук

# ОТКРЫТОЕ РАСПРОСТРАНЕНИЕ КЛЮЧЕЙ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

На практике для защиты передаваемых по каналам связи сообщений от несанкционированного доступа к их содержимому широко используется передача этих сообщений в преобразованном виде. При этом преобразование сообщений осуществляется с помощью систем, реализующих различные криптографические преобразования. В таких системах выбор конкретного преобразования осуществляется с помощью ключа криптографического преобразования, который должен храниться в тайне как на передающей, так и на приемной сторонах.

В этой связи необходимо заметить, что если даже для преобразования сообщений используются самые лучшие из известных криптографических преобразований, их применение окажется бесполезным в случае попадания используемых ключей в руки злоумышленников. Поэтому распространение ключей криптографического преобразования является одной из основных проблем при обеспечении защиты сообщений от несанкционированного доступа.

В симметричных криптографических системах, т.е. системах, в которых используется один и тот же ключ как на передающей, так и на приемной сторонах, эта проблема решается следующими основными способами.

Наиболее известным и широко используемым является способ создания секретного канала передачи ключей криптографического преобразования удаленным пользователям с помощью курьерской службы. Основными недостатками этого способа являются достаточно высокая стоимость его реализации, а также сравнительно большое время доставки. Особенно это проявляется при большом числе пользователей. К тому же доставку ключей с помощью курьера трудно назвать высоконадежной, т.к. в этом случае существует принципиальная возможность раскрытия ключей или их подмены.

Более надежным является способ, основанный на делении ключа криптографического преобразования на несколько частей и доставке этих частей пользователям по различным каналам. Очевидно, что в этом случае злоумышленнику для раскрытия ключа необходимо иметь возможность осуществлять контроль всех этих каналов. Однако, несмотря на более высокую надежность этого способа по сравнении с ранее рассмотренным, он не получил широкого распространения из-за высоких матери-

альных затрат.
С целью сокращения числа используемых ключей криптографического преобразования, а, следовательно, повышения надежности их доставки, возможно применение центров доверия или центров распределения ключей, через которые организуется защищенная связь между пользователями. Однако в этих случаях центры доверия становятся основной мишенью для злоумышленников, т.к. в них находятся ключи всех пользователей системы. Основные недостатки этого способа заключаются в том, что довольно часто на практике трудно найти третью, незаинтересованную сторону, пользующуюся доверием всех пользователей, а также в том, что в этих центрах возникают колоссальные нагрузки из-за генерации ключей и одновременного взаимодействия со многими пользователями. Последнее, в конечном итоге, снижает надежность и оперативность защищенной связи.
Для исключения рассмотренных недостатков на практике могут быть применены способы, в основе которых лежит использование открытой информации для формирования одинаковых ключей криптографического преобразования у пар пользователей, которая либо передается по незащищенным каналам связи, либо опубликовывается в специальных справочниках.
Рассмотрим некоторые из этих способов, являющиеся наиболее простыми и эффективными при распространении ключей криптографического преобразования.
Заметим, что основой для разработки таких способов послужило замечание К.Шеннона, сделанное в статье «Теория связи в секретных системах» о том, что «проблема создания хорошего шифра является, по существу, проблемой нахождения наиболее сложных задач, удовлетворяющих определенным условиям... Можно составить наш шифр таким образом, чтобы раскрытие его было эквивалентно ... решению некоторой проблемы, про которую известно, что для ее решения требуется большой объем работ». Это замечание нашло отклик в плодотворных работах американских ученых Диффи и Хеллмана. В своей статье «Новые направления в криптологии» они привели результаты исследований, из которых следовал ошеломляющий по тем временам вывод о возможности создания стойких систем, вообще не требующих передачи ключа криптографического преобразования.
Эти системы получили название **систем с открытыми ключами**.
Диффи и Хеллманом было показано, что в основе построения таких сис-

тем должны лежать односторонние функции вида $y=\Psi(x)$, которые обладают следующими свойствами:
значение величины y является легко вычислимым по значению величины x;
значение величины $x=\Psi^{-1}(y)$ является трудно вычислимым по значению величины x.
При этом «трудновычислимость» понимается в смысле отсутствия другого алгоритма определения значения величины $x=\Psi^{-1}(y)$ по значению величины y за исключением алгоритма тотального перебора возможных значений величины x или определение значения величины $x=\Psi^{-1}(y)$ вычислительно не осуществимо в случае наличия самого экономного из алгоритмов.
В качестве простейших односторонних функций были предложены функции вида

$$y = \gamma^x(\mathrm{mod}q),$$

где x — целое число от 1 до q-1 включительно;
γ — целое число, степени которого $\gamma^1, \gamma^2,..., \gamma^{q-1}$ при вычислении по modq в некотором порядке равны 1,2,...,q-1;
q — большое простое число.
Заметим, что число q является простым, если оно делится само на себя и на число, равное 1. Например, числа 1,3,5,7,11 являются простыми.
В алгебре целое число γ называется примитивным элементом и известно, что такое число всегда существует.
Например, если q=7, то γ =3. Действительно, $3^1(\mathrm{mod}7)=3$, $3^2(\mathrm{mod}7)=2$, $3^3(\mathrm{mod}7)=6$, $3^4(\mathrm{mod}7)=4$, $3^5(\mathrm{mod}7)=5$, а $3^6(\mathrm{mod}7)=1$.
Поскольку $y = \gamma^x(\mathrm{mod}q)$, то $x=\log_\gamma y(\mathrm{mod}q)$. Доказано, что даже при очень больших значениях величины q , например, при $q\approx 2^{1000}$, можно достаточно просто вычислить значение величины $y = \gamma^x(\mathrm{mod}q)$ путем возведения в квадрат, умножения и приведения по modq. В то же время вычисление значения величины $x=\log_\gamma y(\mathrm{mod}q)$ вызывает существенные трудности. Это обусловлено тем, что под знаком логарифма находится число, полученное в результате выполнения операции приведения по modq.
Известно, что вычисление значения величины $y = \gamma^x(\mathrm{mod}q)$ требует не более $2\log_2 q$ простых операций умножения и приведения по modq, а вычисление значения величины $x=\log_\gamma y(\mathrm{mod}q)$ по самому экономному из известных алгоритмов — порядка $q^{0,5}$ таких операций.

Поэтому, если $q \approx 2^{1000}$, то для вычисления величины $x=\log_\gamma y(\mathrm{mod} q)$ потребуется выполнить порядка $2^{500}$ операций, что практически не осуществимо.

Рассмотрим теперь некоторые алгоритмы обмена ключами криптографического преобразования, базирующиеся только на открытых сообщениях.

Самым первым, простым и удобным для практического использования алгоритмом обмена ключами является алгоритм, предложенный Диффи и Хеллманом.

Содержание этого алгоритма заключается в следующем.

Предположим, что пользователям A и B известны значения величин $\gamma$ и q. Пользователь A случайным образом выбирает некоторое целое число $\alpha$, заключенное в пределах от 1 до q-1, и сохраняет его в секрете. Далее пользователь A вычисляет значение величины $Y\alpha = \gamma^{\alpha}(\mathrm{mod} q)$, которое опубликовывается путем помещения этого значения в специальный справочник вместе с адресными данными пользователя A.

Аналогичные операции осуществляет пользователь B.

Если у пользователей A и B возникает необходимость обеспечения защищенной с помощью криптографических преобразований связи, то пользователь A возьмет из справочника значение величины $Y_\beta = \gamma^{\beta}(\mathrm{mod} q)$ и с помощью значения $\alpha$, содержащегося в секрете, вычислит значение $Z_{\alpha,\beta}$ по формуле:

$$Z_{\alpha,\beta}=(Y_\beta)^{\alpha}=[\gamma^{\beta}(\mathrm{mod} q)]^{\alpha}=\gamma^{\beta\alpha}(\mathrm{mod} q).$$

Таким же образом пользователь B вычислит значение $Z_{\beta,\alpha}$:

$$Z_{\beta,\alpha}=(Y_\alpha)^{\beta}=[\gamma^{\alpha}(\mathrm{mod} q)]^{\beta}=\gamma^{\alpha\beta}(\mathrm{mod} q).$$

Из полученных зависимостей следует, что $Z_{\alpha,\beta}=Z_{\beta,\alpha}$. Поэтому пользователи с этого момента времени могут использовать значение величины $Z_{\alpha,\beta}(Z_{\beta,\alpha})$ в качестве обычного ключа криптографического преобразования.

*В качестве иллюстрации рассмотрим следующий простой пример.*

*Пусть q=7, а $\gamma$ =3. Далее пусть пользователь A случайным образом выбирает число $\alpha$=3, а пользователь B — число $\beta$=4. Тогда $Y_\alpha=\gamma^{\alpha}(\mathrm{mod} q)=3^3(\mathrm{mod} 7)=6$, а $Y_\beta=\gamma^{\beta}(\mathrm{mod} q)=3^4\ (\mathrm{mod} 7)=4$.*

*Для получения ключа криптографического преобразования пользователи A и B осу-*

*ществляют следующие действия. Пользователь А берет число $Y_\beta$ и возводит в степень, равную 3, т.к. $\alpha=3$, получая в результате этого число $Z_{\alpha,\beta}=(Y_\beta)^\alpha=4^3(mod7)=1$. Пользователь В берет число $Y_\alpha$ и возводит его в степень, равную 4, т.к. $\beta=4$, получая число $Z_{\beta,\alpha}=(Y_\alpha)^\beta=6^4(mod7)=1$.*

*Из рассмотренного следует, что в результате выполнения этих действий у пользователей А и В появляется ключ криптографического преобразования, равный 1.*

Из анализа алгоритма Диффи—Хеллмана следует, что в результате его использования у пользователей формируется одинаковый ключ криптографического преобразования, значение которого до момента формирования им было неизвестно. Очевидно, что это свойство алгоритма позволяет обеспечить более высокую защищенность сообщений от несанкционированного доступа, поскольку ключ практически «возникает» в системе только к моменту начала криптографического преобразования сообщений.

Рассмотренный алгоритм с небольшими изменениями может быть использован в различных технических системах, предназначенных для криптографического преобразования дискретных или непрерывных сообщений, передаваемых по каналам связи.

Эти изменения заключаются в том, что вычисленные значения $Y_\alpha$, $Y_\beta$ не опубликовываются в справочнике, а передаются по каналу связи между пользователями А и В.

Тогда алгоритм обмена ключами будет иметь следующее содержание. Пусть у пользователя А имеется криптографическая система $A_k$, а у пользователя В — $B_k$. В исходном состоянии в этих системах отсутствуют ключ криптографического преобразования k.

Если у пользователя А возникает необходимость передачи преобразованного с помощью криптографического преобразования сообщения, он передает пользователю В запрос на такую передачу и после получения от пользователя В подтверждения о готовности включает систему $R_\alpha$, реализующую алгоритм открытого распространения ключей. Пользователь В после передачи подтверждения о готовности также включает аналогичную систему $R_\beta$.

В системе $R_\alpha$ выполняются следующие операции. Устройство управления системы запускает датчик случайных чисел, который формирует случайное целое число α.. Это число запоминается в устройстве памяти и выдается в устройство формирования открытого сообщения, которое формирует сообщение, содержащее число $Y_\alpha=\gamma^\alpha(modq)$. Сформированное сообщение передается по каналу связи пользователю В.

Устройство управления системы $R_\beta$ пользователя B при поступлении этого сообщения в устройство приема открытого сообщения выдает его в устройство формирования ключа криптографического преобразования и запускает датчик случайных чисел, который формирует случайное число $\beta$. Число $\beta$ запоминается в устройстве памяти, выдается в устройство формирования ключа криптографического преобразования, где осуществляется формирование ключа с помощью зависимости

$$Z_{\beta,\alpha}=[\gamma^{\alpha}(\mathrm{mod}q)]^{\beta}=\gamma^{\alpha\beta}(\mathrm{mod}q),$$

и в устройство формирования открытого сообщения, в котором формируется сообщение, содержащее число $Y_\beta=\gamma^{\beta}(\mathrm{mod}q)$. Сформированное сообщение передается по каналу связи пользователю A.

Устройство управления системы $R_\alpha$ пользователя A при получении этого сообщения устройством приема открытого сообщения выдает его в устройство формирования ключа криптографического преобразования, считывает из памяти случайное число $\alpha$, которое также выдает в это устройство. В устройстве формирования ключа криптографического преобразования происходит формирование ключа с помощью зависимости

$$Z_{\alpha,\beta}=[\gamma^{\beta}(\mathrm{mod}q)]^{\beta}=\gamma^{\alpha\beta}(\mathrm{mod}q).$$

Поскольку $Z_{\alpha,\beta} = Z_{\beta,\alpha}$ то эти числа, являющиеся ключом криптографического преобразования k, выдаются в соответствующие криптографические системы пользователей A и B.

Далее осуществляется криптографическое преобразование системой $A_k$ исходного сообщения, предназначенного для передачи пользователю B, и передача этого преобразованного сообщения пользователю B.

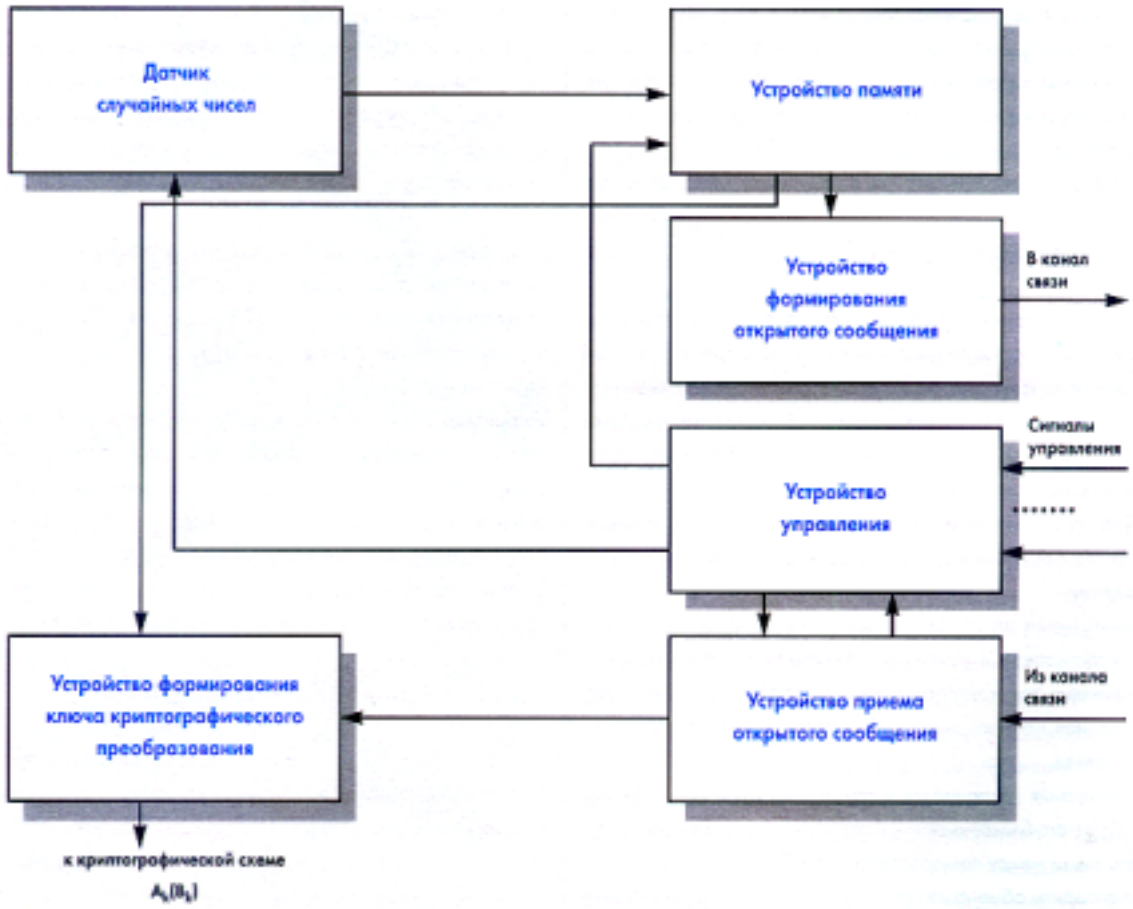
После завершения передачи преобразованного сообщения или обмена преобразованными сообщениями между пользователями устройства управления систем $R_\alpha$ и $R_\beta$ осуществляют выдачу в устройства памяти сигналов, по которым происходит стирание случайных чисел $\alpha$ и $\beta$.

Заметим, что аналогичные операции будут также выполняться в системах, если инициатором передачи сообщения будет являться пользователь B. Очевидно, что рассмотренный алгоритм, хотя и позволяет обойтись без защищенного канала для передачи ключей криптографического преобразования, не устраняет необходимости аутентификации передаваемой открытой информации, т.е. установления факта, что полученное сообще-

ние передано именно тем пользователем, с которым планируется организация защищенной связи.
Для решения этой задачи достаточно эффективно может быть использован электронный код подписи, алгоритм формирования которого изложен во втором номере журнала «Специальная техника» (см. статью: Сударев И.В. Новая технология защиты сообщений, передаваемых в вычислительных сетях).
На рис.1 приведена обобщенная схема системы $R_\alpha$ ($R_\beta$), которая реализует рассмотренный алгоритм открытого распространения ключей.

Рис. 1

Обобщенная схема системы $R_\alpha$ ($R_\beta$)




Очевидно, что для практической реализации этого алгоритма необходимо уметь выполнять операции возведения примитивного элемента $\gamma$ в степень, которая может иметь достаточно большое значение.

С этой целью представляется возможным использовать следующий достаточно простой алгоритм.

**Шаг 1. Получить двоичное представление числа α:**
**$\alpha_k\ \alpha_{k-1}\ \ldots\ \alpha_0$.**

**Шаг 2 Установить $Y_\alpha = 1$.**

**Шаг 3. Для j = k, k-l,...,0 повторить выполнение следующих операций:**

**а) присвоить величине $Y_\alpha$ значение, равное остатку от деления величины $Y_\alpha^2$ на q;**

**б) проверить значение величины $x_j$: если $x_j = 1$, то величине $Y_a$ присвоить значение, равное остатку от деления величины $Y_\alpha \times \gamma$ на q.**

**Шаг 4. Прекратить выполнение алгоритма. Значение величины $Y_\alpha$ является искомым значением.**

*В качестве иллюстрации этого алгоритма рассмотрим следующий пример.*
*Пусть необходимо определить $Y_\alpha = 5^\alpha (mod 7)$, где α = 6.*
*Двоичное представление числа 6 равно 110. Тогда $Y_\alpha = 5^{110} (mod 7)$. Очевидно, что при выполнении шага 2 будем иметь $Y_\alpha = 1$. Поскольку $Y_\alpha^2 = 1$, то остаток от деления величины $Y_\alpha^2 = 1$ на 7 будет равен 1. Проверим теперь значение величины $x_2 : x_2 = 1$, поэтому остаток от деления $Y_\alpha \times \gamma = 1 \times 5$ на 7 будет равен 5 и, следовательно, $Y_\alpha = 5$. Присвоим теперь переменной j значение, равное 1. Тогда $Y_\alpha^2 = 25$, а остаток от деления $Y_\alpha \times \gamma = 20$ на 7 будет равен 6, и, следовательно, $Y_\alpha = 6$. Присвоим переменной j значение, равное 0. Тогда $Y_\alpha = 36$, а остаток от деления величины $Y_\alpha^2 = 36$ на 7 будет равен 1, поэтому $Y_\alpha$ присвоим значение, равное 1. Так как $x_0 = 0$, то окончательно будем иметь $Y_\alpha = 1$. Аналогичный результат может быть получен при использовании известных зависимостей.*
*Действительно,*

$$Y_\alpha = 5^6 (mod 7) = [5^2 (mod 7) 5^2 (mod 7) 5^2 (mod 7)] = [(4x4)(mod 7) 4(mod 7)] = [2(mod 7) 4(mod 7)] = 1(mod 7) = 1.$$

Объективным развитием рассмотренного алгоритма является другой алгоритм открытого распространения ключей криптографического преобразования, позволяющий путем передачи открытых сообщений сформировать у каждого пользователя строго определенный ключ.

В основе этого алгоритма лежат следующие положения теории чисел.

1. Число p является простым относительно числа q, если это число не имеет общих делителей с числом q.

Например, числа 1, 5 являются простыми относительно числа 6.

2. Если q является простым числом, а число p является простым относительно q, то выполняется равенство

$$p^{q-1} = 1(\mathrm{mod} q).$$

3. Если число p является простым относительно числа q-1, то всегда существует целое число p*, такое, что

$$pp^*=1[\mathrm{mod}(q-l)].$$

Это число p* называемое мультикативной инверсией числа p по mod(q-l).
Рассмотрим этот алгоритм применительно к случаю, когда пользователям известно только значение величины q.
Для того, чтобы осуществить обмен ключом криптографического преобразования π, инициатором которого является пользователь A, пользователи выполняют следующую последовательность действий.
Каждый из пользователей формирует некоторое нераскрываемое друг другу число, являющееся простым относительно числа q-1. Пусть для определенности пользователь A формирует число δ, а пользователь B — число ε.
Далее пользователь A выбирает случайным образом ключ криптографического преобразования π, π<q, простой относительно q, и передает пользователю B значение

$$\pi_1 = \pi^{\delta}(\mathrm{mod} q).$$

Пользователь B, получив значение $\pi_1$, определяет значение

$$\pi_2=(\pi_1)^{\varepsilon}=[\pi^{\delta}(\mathrm{mod} q)]^{\varepsilon}=\pi^{\delta\varepsilon}(\mathrm{mod} q),$$

которое возвращает пользователю A. Пользователь A, получив значение $\pi_2$, вычисляет значение

$$\pi_3=(\pi_2)^{\delta^*}=\pi^{\delta\varepsilon\delta^*}(\mathrm{mod} q),$$

где δ* — мультикативная инверсия числа δ по mod(q-l), т.е.

$$\delta\delta^*=l[\mathrm{mod}(q-l)].$$

Поскольку

$$\delta\delta^*=1[\mathrm{mod}(q-l)]=k(q-l)+1,$$

где k — некоторое число, то

$$\pi_3=(\pi_2)^{\delta}*=\pi^{\delta\varepsilon\delta^*}(\mathrm{mod}q)=[\pi^{k(q-1)+1}]^{\varepsilon}(\mathrm{mod}q)=[\pi^{k(q-1)}\pi]^{\varepsilon}(\mathrm{mod}q)=\{[\pi^{k(q-1)}(\mathrm{mod}q)]^{\varepsilon}\times \pi^{\varepsilon}(\mathrm{mod}q)\}(\mathrm{mod}q).$$

Поскольку число π является простым относительно числа q, то всегда будет выполнятся равенство

$$\pi^{q-1}=1(\mathrm{mod}q).$$

Поэтому

$$\pi_3=\{[1^k(\mathrm{mod}q)]^{\varepsilon}\pi^{\varepsilon}(\mathrm{mod}q)\}(\mathrm{mod}q)=\pi^{\varepsilon}(\mathrm{mod}q).$$

Полученное значение $\pi_3$ выдается пользователю B.
Пользователь B, получив это значение, определяет значение

$$\pi_4=(\pi_3)^{\varepsilon}*=\pi^{\varepsilon\varepsilon^*}(\mathrm{mod}q),$$

где ε* — мультикативная инверсия числа ε по mod(q-l),
т.е.

$$\varepsilon\varepsilon^*=1[\mathrm{mod}(q-l)].$$

Поэтому, как и в предыдущем случае применительно к пользователю A, пользователь B получит следующее значение

$$\pi_4=\pi^{s(q-1)+1}(\mathrm{mod}q)=\pi(\mathrm{mod}q),$$

где s — некоторое число.
Поскольку $\pi<q$, то $\pi(\mathrm{mod}q)=\pi$.
Следовательно, пользователи A и B обменялись ключом криптографического преобразования π. Заметим, что рассмотренный алгоритм, также как и алгоритм Диффи-Хеллмана, предполагает необходимость аутентификации передаваемой по каналу связи открытой информации.

В то же время рассмотренный алгоритм имеет ряд принципиальных отличий от алгоритма Диффи-Хеллмана. Во-первых, с помощью такого алгоритма представляется возможным передать пользователю значение ключа криптографического преобразования, сформированное другим пользователем; во-вторых, при использовании этого алгоритма передаваемое по каналу связи открытое сообщение формируется с помощью односторонней функции, зависящей от нескольких неизвестных для злоумышленников параметров, например, $\pi$, $\delta$ и т.п., что существенно затрудняет определение злоумышленниками ключа криптографического преобразования и повышает надежность его доведения.
Естественной платой за приобретение этих свойств является увеличение в 1,5 раза времени обмена открытыми сообщениями между пользователями, а также повышение сложности выполняемых ими вычислений по сравнению с алгоритмом Диффи-Хеллмана.