УДК 621.396.96

КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ ЗАЩИТЫ ИНФОРМАЦИИ В РАДИОКАНАЛАХ СЕТЕВЫХ СПУТНИКОВЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ АСИММЕТРИЧНЫХ АЛГОРИТМОВ

А. А. Корниенко,
доктор техн. наук, профессор
Санкт-Петербургский государственный университет путей сообщения
С. В. Штанько,
канд. техн. наук
Военно-космическая академия им. А. Ф. Можайского

Изложен подход к разработке криптографических протоколов для безопасной передачи информации по радиоканалам сетевых спутниковых систем на основе использования асимметричных алгоритмов на эллиптических кривых.

An approach to the construction of cryptographic protocols for secure information exchange in satellite radio channels using asymmetric algorithms on elliptic curves is described.

Развитие сетевых спутниковых технологий управления и передачи информации приводит к значительному возрастанию информационных потоков в радиоканалах. Информация, циркулирующая по радиоканалам управления и информационного обмена, может иметь критическое значение для пользователя, т. е. раскрытие информации посторонними лицами (в дальнейшем «нарушителем») может привести к значительному ущербу для пользователя. Такая информация является конфиденциальной и требует защиты от различных угроз. Под угрозой безопасности информации будем понимать потенциально возможное воздействие на информацию, которое прямо или косвенно может нанести ущерб ее безопасности. Под безопасностью информации будем понимать состояние информации, при котором с требуемой вероятностью обеспечивается защита информации от различных угроз.

Среди множества угроз безопасности информации в сетевых спутниковых системах можно выделить:

– перехват в радиоканале (контроль трафика);

– воздействие преднамеренных помех;

– несанкционированное декодирование и дешифрование информации;

– информационную перегрузку за счет передачи большого количества фрагментов ложной информации;

– передачу ложной информации (в том числе ложной командно-программной информации), постановку имитирующих помех;

– физическое воздействие на оконечные устройства.

Учитывая пространственную доступность радиоканалов управления и информационного обмена с космическим аппаратом (КА) в сетевых спутниковых системах, значительное внимание необходимо уделять вопросам защиты информации от несанкционированного доступа (НСД) к ее смысловому содержанию [1]. Основным инструментом защиты информации в этом случае является криптографическая защита, построенная на основе различных алгоритмов шифрования. Кроме того, при осуществлении передачи конфиденциальной информации по сетевым спутниковым системам принципиально необходимо выполнение процедуры аутентификации – подтверждения подлинности абонента.

В сетевых спутниковых системах целесообразнее использовать асимметричные криптосистемы, которые обладают следующими преимуществами:

– в сетях с большим количеством абонентов часто возникают ситуации, когда абоненты не могут доверять друг другу, а асимметричные криптосистемы позволяют строить эффективные алгоритмы аутентификации;

– использование для защиты информации в сетях с большим количеством абонентов только симметрич-

ных криптосистем требует распространения большого числа ключевой информации, а асимметричные криптосистемы свободны от данного недостатка.

В общем случае системы управления и информационного обмена с КА могут быть разнородными и использовать различные протоколы на различных уровнях модели взаимодействия открытых систем. В таких сетях могут быть использованы различные каналы передачи информации, в том числе проводные, радио, оптические и др. Кроме того, в интересах управления и информационного обмена с КА возможно использование сетевых спутниковых систем связи общего пользования. В связи с этим наиболее целесообразно размещать криптографические функции на уровне представления или прикладном уровне семиуровневой модели взаимодействия открытых систем, что аналогично «туннелированию» при создании закрытых каналов в компьютерных сетях [2]. Шифрование всей передаваемой информации в этом случае осуществляется до ее поступления в терминальную абонентскую аппаратуру. За счет этого становится возможной аутентификации абонентов с последующим переходом к информационному обмену в закрытом режиме работы.

Шифрование передаваемых сообщений в этом случае производится только конечными абонентами. Зашифрованный пакет информационного обмена абонентов инкапсулируется в пакет по стандарту, принятому в используемой сети связи.

В данном случае пакет будет состоять из служебной части и области данных (рис. 1). В служебной части передаются номер пакета (n), адреса абонентов (идентификаторы Id_A и Id_B), другая служебная информация (например, флаги). В области данных передается зашифрованный пакет информационного обмена абонентов. В случае, если длина зашифрованного пакета превышает размер области данных пакета используемой сети связи, последний может быть разбит на несколько частей в соответствии с принятыми стандартами.

Для построения асимметричных криптоалгоритмов предпочтительнее использовать математические конструкции на эллиптических кривых, как обладающие наибольшей стойкостью и скоростью криптографических преобразований по сравнению с другими типами асимметричных алгоритмов защиты информации [3].

Рассмотрим математические основы использования эллиптических кривых в криптографических целях. Рассмотрим эллиптическую группу по модулю p, где p является простым числом. Выберем два неотрицательных целых числа a и b, меньшие p и удовлетворяющие условию

$$4a^3 + 27b^2 (\mathrm{mod}\ p) \neq 0.$$

Эллиптическую кривую (ЭК) над конечным полем Галуа GF_p можно представить в виде

$$E_p(a, b):\ y^2 = x^3 + ax + b\ (\mathrm{mod}\ p),$$

где $E_p(a, b)$ – эллиптическая группа по модулю p, элементами которой (x, y) являются пары неотрицательных чисел, меньших p и удовлетворяющих уравнению кривой, а также точка в бесконечности O.

Операция обращения точки для кривой записывается следующим образом: $-(x, y) = (x, -y)$. Групповой закон сложения точек $P_1 \oplus P_2$ имеет вид $P_1 \oplus P_2 = (x_3, y_3)$, где

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_2 - x_1;$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1.$$

При $P_1 = P_2 = (x_1, y_1)$ получаем $2P_1 = (x_2, y_2)$:

$$x_2 = \frac{(3x_1^2 + a)^2}{4y_1^2} - 2x_1;$$

$$y_2 = \frac{(3x_1^2 + a)}{2y_1}(x_1 - x_2) - y_1.$$

Непосредственно из формул видно, что точка в бесконечности получается при удвоении точки P_1 с нулевой координатой y либо при сложении двух различных точек с одинаковой координатой x.

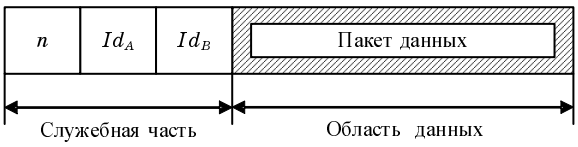
Чтобы построить криптографическую систему, используя ЭК, нужно найти «вычислительную проблему», которую можно использовать в качестве односторонней функции с секретом.

Пусть p – простое число, а G – примитивный элемент или генератор аддитивной циклической подгруппы группы точек ЭК; P – произвольная точка, принадлежащая данной кривой. Тогда любую точку P кривой $E(GF_p)$ можно представить как кратную генератору подгруппы в виде

$$P = n \times G = \underbrace{G \oplus G \oplus \ldots \oplus G}_{n\ раз},$$

где n – кратность данной точки генератору подгруппы; «$\oplus$» – знак групповой операции в группе точек кривой.

Групповой закон сложения точек аддитивной абелевой группы ЭК обладает следующим криптографическим свойством: нахождение числа n по двум заданным элементам группы P и G при $n \to \infty$ является вычислительно сложной задачей [2]. Таким образом, групповой закон сложения точек ЭК рассматривается в качестве функции криптографического преобразования.



■ ***Рис. 1.*** *Структура пакета*

Несмотря на то что среди асимметричных алгоритмов алгоритмы на ЭК являются наиболее быстрыми, они также обладают основным недостатком асимметричных криптосистем – медленным быстродействием по сравнению с симметричными криптосистемами. Для того чтобы этого недостатка избежать, был разработан комбинированный алгоритм, сочетающий в себе достоинства асимметричных и симметричных криптосистем. В комбинированном алгоритме использованы элементы как асимметричных криптоалгоритмов на ЭК, позволяющих строить эффективные схемы аутентификации и обладающих высокой криптостойкостью, так и симметричных, обладающих значительно большим быстродействием.

Наибольшим быстродействием обладают потоковые криптосистемы гаммирования, так как процесс зашифровывания заключается в поразрядном сложении передаваемого сообщения и гаммы шифра. В них скорость шифрования определяется в основном скоростью генерации псевдослучайной последовательности (ПСП), используемой в качестве гаммы.

На основе примитива генерации общего сеансного ключа Диффи – Хеллмана с использованием конструкций на ЭК был разработан комбинированный алгоритм генерации общего сеансного ключа и поточного шифрования, который сочетает в себе преимущества симметричных и асимметричных криптосистем. В качестве симметричной части предлагается использовать поточное шифрование, обладающее высоким быстродействием. Алгоритм (рис. 2) определяет порядок выработки общего сеансного ключа на основе протокола Диффи – Хеллмана [4] с использованием ЭК (асимметричная часть) с последующим шифрованием потока информации методом гаммирования (симметричная часть). Начальные состояния обоих генераторов определяются ключом, полученным в результате алгоритма генерации сеансного ключа. Данный алгоритма позволяет двум абонентам вырабатывать общий сеансный ключ и работать в дальнейшем с использованием быстрого поточного шифра.

Параметры алгоритма:

GF_p – конечное поле простой характеристики p;

$E_p(a, b)$ – ЭК над полем GF_p в форме Вейрштрасса (кривая может быть задана простым GF_p или расширенным GF_q^n полем в аффинных либо проективных координатах);

$\#E(GF_p)$ – порядок группы точек кривой;

G – базовая точка – генератор подгруппы;

q – порядок циклической подгруппы;

h – односторонняя хеш-функция, принимающая значения в множестве двоичных векторов длины 256, определенная стандартом Р 34.11–94.

Указанные параметры должны быть известны всем абонентам КРС, участвующим в информационном обмене.

Алгоритм выработки общего секретного ключа.

1. Абонент A генерирует закрытый ключ – целое число $k_з^A \in [1,\ q-1]$ и вычисляет открытый ключ – точку $k_о^A = k_з^A \times G$, которую передает абоненту B.

2. Абонент B генерирует закрытый ключ – целое число $k_з^B \in [1,\ q-1]$ и вычисляет открытый ключ – точку $k_о^B = k_з^B \times G$, которую передает абоненту A.

3. Абонент A вычисляет общий ключ $k_A = k_о^B \times k_з^A$, а абонент B вычисляет общий ключ $k_B = k_з^B \times k_о^A$.

Выход алгоритма: d – точка, секретный ключ, такая, что

$$d = k_A = k_B = k_о^B \times k_з^A = k_з^B \times k_о^A =$$
$$= k_з^A \times (k_з^B \times G) = k_з^B \times (k_з^A \times G) = k_з^A \times k_з^A \times G.$$

Таким образом, оба абонента получают общий секретный ключ d, который определяет начальные состояния генераторов гаммы аппаратуры криптозащиты абонентов. Теперь оба генератора будут вырабатывать одинаковую двоичную псевдослучайную последовательность $\gamma = f(d)$.

Рассмотрим работу непосредственно алгоритма шифрования при передаче информации абонентом A абоненту B.

Вход алгоритма шифрования: M–сообщение.

Выход алгоритма шифрования: C–криптограмма.

Преобразование шифрования:

1) абонент A представляет сообщение M длиной l в виде последовательности бит $m_i = \{0, 1\}$, $i = 1, ..., l$;

2) абонент A складывает биты сообщения по модулю два с битами полученной гаммы: $c_i = m_i \oplus \gamma_i$, $i = 1, ..., l$.

Вход алгоритма расшифровывания: C–криптограмма.

Выход алгоритма расшифровывания: M–сообщение.

Преобразование расшифровывания:

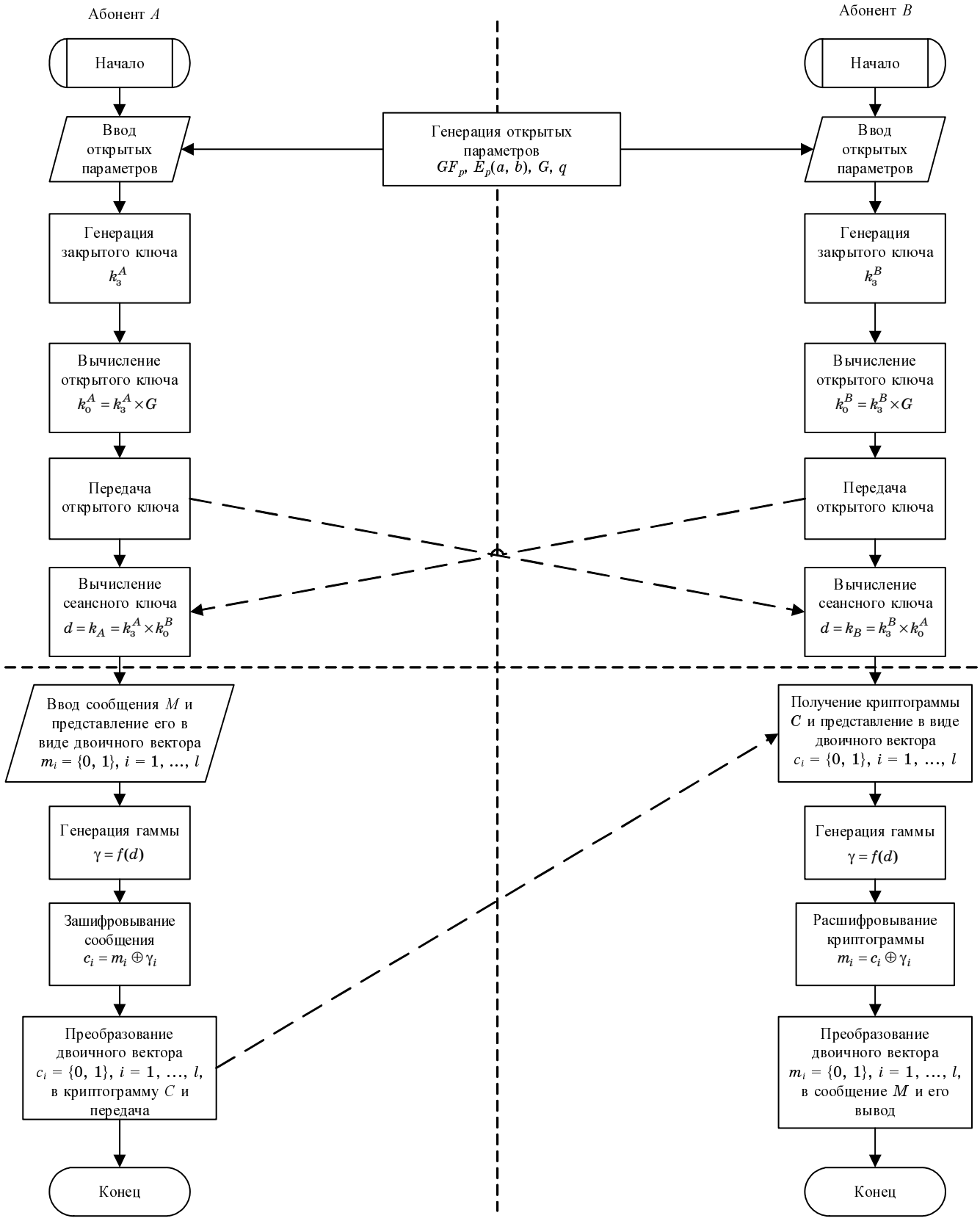
1) абонент B складывает биты криптограммы по модулю два с битами гаммы: $m_i = c_i + \gamma_i$, $i = 1, ..., l$;

2) последовательность m_i преобразуется в сообщение M.

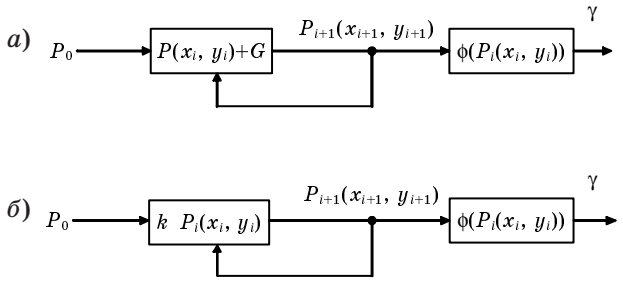
Особенностью математического аппарата ЭК является то, что они позволяют строить криптографически стойкие и достаточно быстродействующие генераторы ПСП. При реализации алгоритма генерации общего сеансного ключа и поточного шифрования в качестве симметричной части алгоритма возможно применение такой ПСП на основе ЭК. Эту ПСП можно в дальнейшем использовать в качестве гаммы для потокового шифрования данных и для генерации случайных чисел, необходимых для генерации ключей в алгоритмах шифрования и аутентификации абонентов.

Для построения генератора криптографически стойкой ПСП необходима необратимая функция [5]. В качестве такой функции можно использовать умножение точки на число либо сложение в группе точек ЭК. Для получения очередного состояния генератора такая функция использует в качестве аргумента его текущее состояние.

Пусть даны ЭК в форме Вейерштрасса $E_p(a, b)$ и базовая точка G. Генератор находится в состоянии, определяемом точкой $P_i(x_i, y_i)$. Получить следующее состояние генератора можно двумя способами:



■ ***Рис. 2.*** *Комбинированный алгоритм генерации общего сеансного ключа и поточного шифрования*



■ ***Рис. 3.*** *Схемы построения генераторов на ЭК: а – по формуле (1); б – по формуле (2)*

$$P_{i+1} = P_i + G; \quad (1)$$

$$P_{i+1} = k \times P_i. \quad (2)$$

Схемы соответствующих генераторов представлены на рис. 3.

Эллиптическая кривая может быть задана как в аффинных, так и в проективных координатах. В результате получаем уравнения для четырех типов генераторов:

$$P_{i+1}(x_{i+1}, y_{i+1}) = P_i(x_i, y_i) + G, \gamma = \phi(P_{i+1}); \quad (3)$$

$$P_{i+1}(x_{i+1}, y_{i+1}) = k \times P_i(x_i, y_i), \gamma = \phi(P_{i+1}); \quad (4)$$

$$P_{i+1}(X_{i+1}, Y_{i+1}, Z_{i+1}) = \\ = P_i(X_i, Y_i, Z_i) + G, \gamma = \phi(P_{i+1}); \quad (5)$$

$$P_{i+1}(X_{i+1}, Y_{i+1,} Z_{i+1}) = \\ = k \times P_i(X_i, Y_i, Z_i), \gamma = \phi(P_{i+1}). \quad (6)$$

В качестве множителя k можно использовать как константу, так и псевдослучайное число, поступающее с выхода другого генератора, что улучшит статистические свойства конструкции. Одним из возможных вариантов является использование в качестве множителя одной из координат точки, определяющей текущее состояние генератора:

$$P_{i+1}(x_{i+1}, y_{i+1}) = (x_i \times i) \bmod q \times P_i(x_i, y_i), \\ \gamma = \phi(P_{i+1}); \quad (7)$$

$$P_{i+1}(x_{i+1}, y_{i+1}) = (x_i + i) \times P_i(x_i, y_i), \gamma = \phi(P_{i+1}). \quad (8)$$

Функция $\phi(P_i)$ преобразует текущее состояние генератора, заданное точкой $P_i(x_i, y_i)$, в выходную последовательность бит. В качестве такой функции можно использовать хеш-функцию, одну из координат точки либо некоторые их разряды, а также конкатенацию координат:

$$\phi(P_{i+1}) = x_{i+1} \| y_{i+1}; \phi(P_{i+1}) = X_{i+1} \| Y_{i+1} \| Z_{i+1}; \quad (9)$$

$$\phi(P_{i+1}) = x_{i+1}; \phi(P_{i+1}) = X_{i+1}; \quad (10)$$

$$\phi(P_{i+1}) = h(x_{i+1} \| y_{i+1}); \phi(P_{i+1}) = h(X_{i+1} \| Y_{i+1} \| Z_{i+1}); \quad (11)$$

$$\phi(P_{i+1}) = h(x_{i+1}); \phi(P_{i+1}) = h(X_{i+1}), \quad (12)$$

где $h(x)$ – хеш-функция, принимающая значения в множестве двоичных векторов длины 256 (в соответствии с ГОСТ Р34.11–94).

Комбинируя функции, определяющие выходы и переходы между состояниями генераторов (3)–(12), получаем 32 варианта построения генераторов ПСП. Исследования показывают, что статистические свойства некоторых вариантов построения генераторов на ЭК превосходят статистические свойства классического генератора BBS (Блюма – Блюма–Шуба), основанного на возведении в степень в конечном поле.

Для защиты информации, передаваемой по каналам сетевой спутниковой системы, предлагается использовать протокол аутентификации абонентов и направленного шифрования на основе рассмотренного алгоритма.

В данном случае для выполнения процедур выработки аутентифицирующих информационных блоков в аппаратуре потребителя может быть использован алгоритм формирования электронной цифровой подписи, описанный в документе [6], а для генерации общего сеансного ключа и шифрования потока информации предлагается использовать рассмотренный алгоритм генерации сеансного ключа и поточного шифрования.

Протокол предназначен для аутентификации абонентов и организации защищенного информационного обмена между абонентами. Суть данного протокола состоит в том, что информация шифруется первым абонентом A на ключе, полученном с помощью открытого ключа второго абонента B, и криптограмму может расшифровать только абонент, которому она предназначается. Таким образом, при реализации протокола направленного шифрования одновременно происходит аутентификация абонента-получателя. Аутентификация абонента-отправителя осуществляется с помощью процедуры формирования аутентифицирующего информационного блока формируемого им запросного пакета при инициализации протокола направленного шифрования (рис. 4). На рисунке приняты следующие обозначения: $k_з$ и $k_о$ – пара долговременных ключей криптозащиты (закрытый и открытый соответственно); $d_з$ и $d_о$ – пара сеансных ключей криптозащиты (закрытый и открытый соответственно); r, s – числа, составляющие аутентифицирующий информационный блок; G – точка, примитивный элемент группы точек эллиптической кривой; *ПРД* – передающее устройство, *ПРМ* – приемное устройство; *ГПСП-1* – генератор псевдослучайной последовательности, предназначенный для генерации сеансных закрытых ключей; *ГПСП-2* – генератор псевдослучайной последовательности – гаммы поточного шифрования; *Sign* и *Unsign* – блоки выработки и проверки аутентифицирующего информационного блока соответственно.

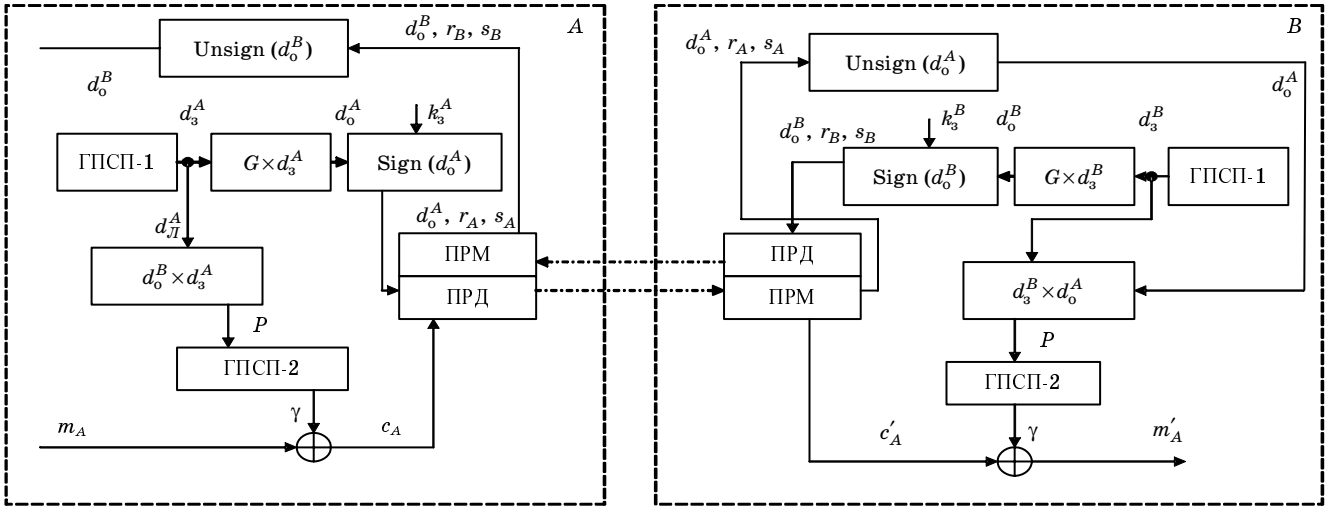
Основные операции протокола направленного шифрования.

1. Абонент A генерирует с помощью ГПСП-1 пару сеансных ключей $d_з^A$ и $d_о^A = d_з^A \times G$.

2. Абонент A вырабатывает аутентифицирующий блок открытого ключа $(R_A, S_A) = k_з^A(d_о^A)$.

3. Абонент A формирует сообщение $(d_о^A, R_A, S_A)$ и передает его абоненту B.

4. Абонент B, получив сообщение, проверяет правильность аутентифицирующего блока; если



■ ***Рис. 4.*** *Схема протокола аутентификации абонентов и направленного шифрования*

проверка дала положительный результат, то открытый сеансный ключ d_o^A абонента A признается истинным, в противном случае шаги 2–4 повторяются.

5. Абонент B генерирует пару сеансных ключей $d_з^B$ и $d_o^B = d_з^B \times G$.

6. Абонент B вычисляет общий секретный ключ – точку $d = d_з^B \times d_o^A$.

7. Абонент B вырабатывает аутентифицирующий блок открытого ключа $(R_B, S_B) = k_з^B(d_o^B)$.

8. Абонент B формирует сообщение (d_o^B, R_B, S_B) и передает его абоненту A.

9. Абонент A, получив сообщение, проверяет правильность аутентифицирующего блока если проверка дала положительный результат, то открытый сеансный ключ d_o^B абонента B признается истинным, в противном случае шаги 6–9 повторяются.

10. Абонент A вычисляет общий секретный ключ – точку $d = d_o^B \times d_з^A$.

11. Абонент A вырабатывает гамму шифра γ с помощью генератора ГПСП-2, используя в качестве начального состояния точку d.

12. Абонент A складывает биты сообщения по модулю два с битами полученной гаммы: $c_i = m_i \oplus \gamma_i$, $i = 1, ..., l$, и передает полученную криптограмму абоненту B.

13. Абонент B, получив криптограмму, складывает биты криптограммы по модулю два с битами гаммы: $m'_i = c'_i + \gamma_i$, $i = 1, ..., l$.

Шаги 12 и 13 могут повторяться необходимое число раз для передачи всего запланированного объема информации. Аналогичным образом абонент B может передавать информацию в закрытом режиме работы абоненту A.

Разработанный протокол позволяет выполнять процедуру аутентификации абонентов в начале сеанса информационного обмена между абонентами сетевой спутниковой системы с одновременной генерацией секретного ключа симметричной криптосистемы и последующей работой в закрытом режиме с использованием потокового шифрования. Реализация рассмотренного протокола с использованием математических конструкций на эллиптических кривых осуществляется программным способом и позволяет обеспечивать безопасность управления и передачи информационных потоков.

Литература

1. Многоспутниковые сетевые системы: принципы построения, управления и передачи информации: Сб. науч. тр. / ВИККА. СПб., 1998. 166 с.
2. **Столлингс В.** Криптография и защита сетей: принципы и практика: Пер. с англ. 2-е изд. М.: Издательский дом «Вильямс», 2001. 672 с.
3. **Ростовцев А. Г., Маховенко Е. Б.** Введение в криптографию с открытым ключом СПб.: Мир и Семья, 2001. 336 с.
4. **Иванов М. А.** Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001. 368 с.
5. Криптографические методы защиты информации в локальных вычислительных сетях / Под ред. А. В. Дружинина, А. И. Замарина, Ю. Н. Максимова; ВИККА. СПб., 1998. 194 с.
6. ГОСТ Р 34.10 – 2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Изд-во стандартов, 2001. 24 с.