A. V. Barkhatov, A. S. Kozlov
Saint Petersburg Electrotechnical University "LETI"

Radar amplitude-range-doppler surface fast calculation on graphics processing units

The paper describes the algorithm of fast calculation of the amplitude-range-Doppler surface. The features of the software implementation of the algorithm are drawn. The nuances of parallel computing of the surface on graphics processing units of the gaming graphics card are shown. The result, the sixteen surfaces parallel computing time for multichannel radar, is presented.

Radar, digital processing, ambiguity function, cross-correlation, Doppler shift, delay, fast Fourier transformation, graphics processing units, parallel computing

Статья поступила в редакцию 7 сентября 2015 г.

УДК 621.396.9

С. В. Штанько, Д. А. Лесняк
Военно-космическая академия им. А. Ф. Можайского

Алгоритмы защищенного информационного обмена в радиоканалах космической навигационной системы

Для повышения защищенности информационного обмена по радиоканалам космической навигационной системы с целью предотвращения несанкционированного использования системы предложено использовать криптографические методы защиты сигнала высокой точности. Эту задачу позволяет решить криптографическая система, реализующая защищенные протоколы аутентификации, передачи ключей и информационного обмена.

Космическая навигационная система, межспутниковые каналы, алгоритм Диффи–Хеллмана, криптографическая защита

В настоящее время околоземное космическое пространство является сферой ведения военно-космической деятельности и применения космических средств различного назначения, а также рассматривается как стратегическая космическая зона.

На современном этапе развития радиотехнических систем особое место занимают космические навигационные системы (КНС).

Пространственная электромагнитная доступность, являющаяся свойством любых радиоканалов, создает условия для реализации угроз несанкционированного доступа к радиоканалам космического аппарата (КА). Нормальное функционирование КНС может быть нарушено в результате различных деструктивных воздействий.

Применение существующих протоколов защиты информации в радиоканалах навигационной системы ограничено особенностями ее функционирования, связанными в первую очередь с тем, что в ней существуют только однонаправленные каналы передачи информации "навигационный космический аппарат (НКА) – наземная аппаратура потребителя (НАП)", что накладывает существенные ограничения на процедуры аутентификации и обмена ключевой информацией.

Одним из способов смены ключей является генерация новых ключей на основе совершения циклической операции со старым ключом (например, шифрование на старом ключе очередного числа, поступающего от датчика псевдослучайных чисел одинаковой для всех абонентов структуры) [1]. В этом случае, если наземный абонент не может расшифровать полученную информацию, он генерирует новый ключ и пытается расшифровать информацию с его помощью. Это позволяет абоненту восстановить текущий ключ системы независимо от того, сколько циклов смены ключа он пропустил [2]. Недостатком рассмотренного способа является возможность вскрытия структуры датчика псевдослучайных чисел, если вероятный нарушитель сможет получить в свое распоряжение экземпляр НАП. В дальнейшем, вскрыв один ключ, он также может получать последующие ключи с использованием датчика псевдослучайных чисел.

При использовании описанной схемы секретность зависит не только от сохраняемой в секрете структуры датчика псевдослучайной последовательности (ПСП), но и от ключевой информации. Кроме того, такой датчик также может быть построен на основе использования криптографических функций (например, с использованием математического аппарата эллиптических кривых) [3]. Это позволит периодически (либо по команде) менять ключ, определяющий начальное состояние генератора ПСП. При этом ключ генератора ПСП необходимо менять реже, чем ключи шифрования. Этот ключ можно доставлять абонентам (НКА и НАП) одним из описанных способов.

Значительно облегчает задачу распространения ключей наличие в навигационной системе межспутниковых каналов. В случае их отсутствия передачу новых ключей на НКА необходимо выполнять индивидуально для каждого НКА в ходе сеанса управления (СУ). Если же есть возможность передачи информации по межспутниковым каналам, то в предельном случае ключи можно передать только на один НКА, остальные НКА получат ключи по межспутниковым каналам. Компьютерное моделирование показало, что в случае использования межспутниковых каналов среднее время доведения информации (в том числе ключевой) до каждого НКА (для примера был использован состав группировки из 24 КА) ограничивается только скоростью передачи информации и составляет десятки секунд–единицы минут. В случае отсутствия межспутниковых каналов и доведения информации до каждого НКА в ходе СУ среднее время доведения определяется средним временем ожидания СУ и составляет от нескольких часов до полусуток.

Использование асимметричных алгоритмов и наличия у каждого КА своей пары ключей (открытого $k_{\text{о}}$ и закрытого $k_{\text{з}}$), помимо возможности осуществления аутентификации навигационной информации, предоставляет еще одну дополнительную возможность реализации закрытого режима работы при передаче навигационной информации. В этом случае для приема навигационной информации с каждого КА можно будет формировать свой уникальный ключ на основе использования алгоритма Диффи–Хеллмана [4]. Использование при формировании ключа временно́й метки τ позволит сделать этот ключ уникальным для каждой передачи информационного массива.

С целью повышения надежности системы криптографической защиты можно предложить следующую схему осуществления закрытой передачи навигационной информации. Пара ключей шифрования асимметричной криптосистемы $k_{\text{о}}$ и $k_{\text{з}}$ используется как мастер-ключи, или ключи первого уровня, для выработки сеансовых ключей, или ключей второго уровня. Передача навигационной информации осуществляется следующим образом:

1. Абонент A формирует информационный массив (суперкадр) m для передачи абоненту B.

2. Абонент A генерирует случайное число (или набор чисел) R.

3. С помощью числа R и закрытого ключа $k_{\text{з}}$ формируется пара "закрытый сеансовый ключ $k_{\text{з.с}}$", а из него открытый сеансовый ключ $k_{\text{о.с}}$.

4. Информационный массив m шифруется на ключе $k_{\text{о.с}}$: $c = m \otimes k_{\text{о.с}}$ ($\otimes$ – операция шифрования сообщения m на ключе k).

5. Случайное число (набор чисел) R и полученная криптограмма $c' = R \| c$ передаются абоненту B ($\|$ – операция присоединения блока c к блоку R).

6. Абонент B принимает криптограмму c'.

7. Абонент B выделяет из полученной криптограммы число R.

8. Абонент B с помощью числа R и закрытого ключа $k_{\text{з}}$ формирует закрытый сеансовый ключ $k_{\text{з.с}}$.

9. Абонент B расшифровывает криптограмму c', получая на сеансовом закрытом ключе $k_{\text{з.с}}$ информационный массив $m' = c' \otimes k_{\text{з.с}}$, который считает совпадающим с исходным массивом m.

Аналогичным образом описанный алгоритм можно использовать и для реализации симметричной схемы. В этом случае у каждого абонента имеется общий секретный мастер-ключ k, а с помощью случайного числа R формируются сеансовые секретные ключи $k_{\text{с}}$.

Общая архитектура системы криптографической защиты каналов КНС с использованием комбинированных алгоритмов может выглядеть следующим образом.

Симметричная часть. Шифрование передаваемой информации осуществляется симметричным алгоритмом методом гаммирования [5]. Гамма шифра при этом может вырабатываться на основе алгоритма, предусмотренного ГОСТ 28147–89 [6], либо на основе алгоритмов на эллиптических кривых (ЭК) [3]. Может быть разработан новый или

использован существующий потоковый шифр, обладающий высокими криптографическими, статистическими и скоростными свойствами, в случае если он будет сертифицирован для использования.

Асимметричная часть. Используется для генерации сеансовых ключей и осуществления аутентификации в случае необходимости (аутентификация НКА абонентами в НАП, аутентификация НКА друг другом в случае реализации межспутниковых каналов) [7]. Основой асимметричной части целесообразно выбрать математический аппарат ЭК.

Архитектура системы смены ключей. Сеансовые ключи симметричной системы для шифрования и асимметричной для аутентификации (в случае необходимости) генерируются на основе алгоритма Диффи–Хеллмана с использованием долговременных ключей асимметричной системы и случайного числа либо меток времени (или того и другого), для того чтобы сеансовые ключи отличались друг от друга. При этом, если генерируются ключи для осуществления передачи данных по межспутниковым каналам, можно использовать полноценный асимметричный алгоритм на основе алгоритма Диффи–Хеллмана. При передаче кадра навигационной информации наземному абоненту алгоритм Диффи–Хеллмана является упрощенным в том смысле, что у всех наземных абонентов долговременные ключи одинаковы и алгоритм не зависит от того, какому абоненту передается информация и не требует передачи информации от наземного абонента.

Пример использования алгоритма. Рассмотрим использование алгоритма передачи информации по каналу НКА–НАП с осуществлением криптографической защиты.

Рассмотрение базируется на следующих параметрах:

$E_d(\cdot)$ – шифрующее преобразование симметричного алгоритма;

$D_d(\cdot)$ – расшифровывающее преобразование симметричного алгоритма;

GP_p – конечное поле простой характеристики p;

$E_p(a, b)$ – эллиптическая кривая над полем GP_p в форме Вейрштрасса (кривая может быть задана на простым полем GP_p или расширенным полем GP_{q^n} в аффинных либо в проективных координатах);

G – базовая точка – генератор подгруппы;

q – порядок циклической подгруппы;

h – односторонняя хеш-функция, принимающая значения во множестве двоичных векторов длины 256, определенная ГОСТ Р 34.10-2012 [8];

i – номер НКА;

$k_{\text{о}_{\text{КА}i}}$ – открытый долговременный ключ НКА (точка ЭК);

$k_{\text{з}_{\text{КА}i}} = k_{\text{о}_{\text{КА}i}} \times G$ – закрытый долговременный ключ НКА (число) ("×" – символ умножения точки на число);

$k_{\text{з}_{\text{НАП}}}$ – закрытый долговременный ключ наземных абонентов (число);

$k_{\text{о}_{\text{НАП}}} = k_{\text{з}_{\text{НАП}}} \times G$ – открытый долговременный ключ наземных абонентов (точка ЭК);

d – секретный сеансовый ключ шифрования данных (число);

r – случайное число.

Алгоритм передачи информации по каналу НКА–НАП с осуществлением криптографической защиты:

1. НКА формирует сеансовый массив m.

2. НКА генерирует случайное число r.

3. НКА вычисляет сеансовый ключ

$$d = h\left(k_{\text{з}_{\text{КА}i}} \times r \times k_{\text{о}_{\text{НАП}}}\right) = h\left(k_{\text{з}_{\text{КА}i}} \times r \times k_{\text{з}_{\text{НАП}}} G\right).$$

4. НКА шифрует кадр m на ключе d: $c = E_d(m)$;

5. НКА передает комбинацию $i \| c \| r$;

6. НАП, получив комбинацию $i \| c \| r$, в матрице доступности находит открытый ключ i-го НКА $k_{\text{о}_{\text{КА}i}}$.

7. НАП вычисляет сеансовый ключ

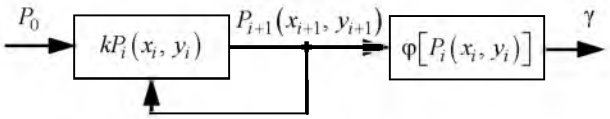
$$d = h\left(k_{\text{з}_{\text{НАП}}} \times r \times k_{\text{о}_{\text{КА}i}}\right) = h\left(k_{\text{з}_{\text{НАП}}} \times r \times k_{\text{о}_{\text{КА}i}} G\right).$$

8. НАП расшифровывает полученный кадр $m = D_d(c)$.

В качестве r может быть использовано как собственно случайное число, так и временна́я метка τ, а также их совокупность $R = r\tau$.

Сеансовый ключ также может быть относительно коротким (100…150 бит), так как актуальность навигационной информации сохраняется достаточно короткое время (порядка секунды). Точная длина ключей может быть определена в зависимости от используемых алгоритмов и требований по стойкости, заданных вероятностью раскрытия за определенный период.

Долговременные ключи меняются периодически на основе проведения циклической операции



со старыми ключами. Смена может производиться как на заранее заданной временно́й сетке, так и по команде центра. Используем в качестве аппарата, осуществляющего циклическую операцию, генератор на ЭК. Примером может служить генератор, основанный на умножении точки на число в группе точек эллиптической кривой, заданной в аффинных координатах, следующего вида:

$$P_{i+1}(x_{i+1}, y_{i+1}) = kP_i(x_i, y_i);\ \gamma = \varphi(P_{i+1}).$$

Текущим состоянием генератора является точка ЭК P_i. Следующее состояние P_{i+1} получается умножением некоторой константы k на текущее состояние. Схема построения генераторов на эллиптических кривых представлена на рисунке.

Функция $\varphi(P_{i+1}) = h(x_{i+1} \| y_{i+1})$ определяет выход генератора.

Число k может быть как неизменяемой константой, так и псевдослучайным числом, поступающим с другого датчика, либо случайным числом, передаваемым центром. В последнем случае должны быть задействованы каналы доведения информации до НАП, не связанные с КНС.

Примерный алгоритм смены долговременных ключей всеми абонентами (НКА и НАП) предлагается реализовать следующим образом.

1. По привязке ко времени или по команде центра абонент вычисляет очередную точку: $P_{i+1}(x_{i+1}, y_{i+1}) = k \times P_i(x_i, y_i)$. Если вычисление осуществляется по команде центра, то в качестве k используется случайное число, передаваемое вместе с командой.

2. Абонент запоминает новую точку P_{i+1} для последующей генерации.

3. Абонент вычисляет

$$k_{3,\,i+1} = k_{3,\,i}^{\varphi(P_{i+1})} \pmod p = h(x_{i+1} \| y_{i+1}).$$

4. Абонент вычисляет $k_{0,\,i+1} = k_{3,\,i+1} \times G$.

Генераторы после однократной установки в одно и то же начальное состояние будут воспроизводить одинаковое значение $\varphi(P_{i+1})$. Это позволит НКА вычислить текущие ключи НАП на основании предыдущих, а абонентам НАП вычислить ключи всех НКА. После вычисления все значения закрытых ключей других абонентов сразу же уничтожаются, остаются только значения открытых ключей.

Если НАП не будет функционировать в момент смены долговременных ключей, для получения новых ключей в следующий момент необходимо выполнить циклическую операцию. Если же было пропущено несколько смен ключей, циклическую операцию необходимо повторять несколько раз до тех пор, пока НАП не сможет расшифровывать навигационную информацию. Такую процедуру можно выполнять только в том случае, если k постоянно. Если же операция умножения выполняется на основе случайного числа, то для восстановления текущего ключа абоненту требуются случайные числа всех циклов.

Генераторы всех абонентов синхронизируются (выставляются в начальное состояние) посредством мастер-ключа. В качестве такого ключа может выступать генератор подгруппы G в группе точек ЭК. Чтобы синхронно изменить начальное состояние генераторов гаммы, необходимо всем абонентам передать новое значение G. Эту операцию можно производить достаточно редко, например только в случае необходимости, по команде центра, в угрожаемый период. При этом на НКА новое значение передается в ходе СУ, а наземным абонентам либо в зашифрованном виде с НКА, либо, что надежнее, но сложнее, по другим каналам передачи информации.

Генераторы НКА могут работать и асинхронно с НАП. В этом случае каждый НКА генерирует свою пару долговременных ключей и передает открытый ключ в открытом виде в каждом кадре. Таким образом, любой абонент НАП может сгенерировать сеансовый ключ на основе своих закрытого и окрытого ключей НКА. НКА же будет получать единый долговременный открытый ключ НАП в ходе СУ с использованием межспутниковых каналов. Генераторы НАП должны работать синхронно в любом случае, так как ключи для всех абонентов НАП являются едиными. Синхронно с ними должен работать и генератор в центре, для того чтобы иметь возможность доводить ключи НАП до НКА в ходе СУ.

Представленный в работе алгоритм позволяет использовать для защиты навигационной информации симметричные и асимметричные криптосистемы. Предпочтительным является использование комбинированных криптосистем, использующих преимущество первых по скорости и вторых по широким возможностям построения схем аутентификации и доставки ключей. Окончательный вариант архитектуры зависит от тре-

бований, предъявляемых к криптографической системе защиты навигационной информации, наличия межспутниковых каналов, способов доставки ключей до НАП и т. д.

В качестве алгоритмов асимметричной части комбинированной схемы рекомендуется использовать математический аппарат эллиптических кривых, обладающий наилучшими криптографическими и скоростными характеристиками по сравнению с другими типами асимметричных алгоритмов.

СПИСОК ЛИТЕРАТУРЫ

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / пер. с англ. М.: Триумф, 2012. 816 с.

2. Столингс В. Криптография и защита сетей: принципы и практика / пер. с англ. 2-е изд. М.: 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. Diffie W., Hellman M. E. New Directions in Cryptography // IEEE Trans. on inf. theory. 1976. Vol. IT-22, iss. 11. P. 644–654.

5. Ростовцев А. Г., Маховенко Е. Б. Теоретическая криптография. СПб.: Профессионал, 2004. 479 с.

6. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. М.: Изд-во стандартов, 1996. 28 с.

7. Штанько С. В., Жукова Н. А. Схемы аутентификации данных и пользователей в распределенных информационных системах // Изв. СПбГЭТУ "ЛЭТИ". 2012. № 8. С. 46–51.

8. ГОСТ Р 34.10–2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Изд-во стандартов, 2012. 24 с.

S. V. Shtanko, D. A. Lesnyk
Mozhaisky Military Space Academy

Algorithms of the protected information exchange in radio channels of a space navigation system

To improve the security of information exchange throw navigation space system radio channels to prevent unauthorized use of the system is proposed to use high accuracy cryptographic methods to protect signal. This task allows to solve a cryptographic system that implements secure authentication protocols, key collection and information exchange.

Space navigation system, inter-satellite channels, Diffi–Hellman's algorithm, cryptographic protection

Статья поступила в редакцию 29 сентября 2015 г.

УДК 621.391

А. И. Соколов, Ю. С. Юрченко
Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В. И. Ульянова (Ленина)

Использование пространственной информации в комплексных инерциально-спутниковых навигационных системах летательных аппаратов

Рассмотрены алгоритмы работы тесно связанной схемы комплексирования инерциальной системы навигации и спутниковой радионавигационной системы с последовательной обработкой наблюдений псевдодальностей и псевдоскоростей. Предложено учитывать информацию инерциальной системы навигации о положении источника сигнала относительно диаграммы направленности антенны и останавливать поиск при кратковременном отключении радиосигнала из-за маневра летательного аппарата.

Инерциальные навигационные системы, спутниковые радионавигационные системы, информация о пространственной ориентации летательного аппарата, комплексирование