Ключові слова: паралельна модель обчислень, асиметрична криптографія, багаторозрядна арифметика, багаторозрядне множення, ДПФ, ШПФ.

OPTIMIZATION OF MULTI-DIGIT MULTIPLICATION BASED ON FFT IN PARALLEL COMPUTATIONAL MODEL

It is considered the operation of multi-digit multiplication for parallel computational model, that has biggest influence on performance of asymmetric cryptographic computer systems. It is given modification of N-digit multiplication algorithm based on FFT and DTF`s coefficients previously computed. New algorithm operates with multi-digits of the length of N, contrary to standard algorithm that uses multi-digits of the length of 2N. Algorithm reduces in two times the number of used parallel processors keeping the same computational complexity of each processor in comparison with standard algorithm. Given algorithm is also efficient in sequential computational model.

Key words: parallel computational model, asymmetric cryptography, multidigit arithmetic, multidigit multiplication, DFT, FFT.

Терещенко Андрій Миколайович, кандидат фізико-математичних наук, старший інженер-програміст ТОВ «СімКорп – Україна».
E-mail: teramidi@ukr.net
Терещенко Андрей Николаевич, кандидат физико-математических наук, старший инженер-программист ООО «СимКорп – Украина».
Tereshchenko Andrii, Ph.D in physics and mathematics Senior software developer LLC «SimCorp – Ukraine».

УДК 511.512

ПРОГРАММНО-МОДЕЛИРУЮЩИЙ КОМПЛЕКС ВРС АЛГОРИТМА ПОТОЧНОГО ШИФРОВАНИЯ И ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ ВИДЕОСИГНАЛОВ, ПЕРЕДАВАЕМЫХ С БОРТА БПЛА

Анатолий Белецкий, Артем Максименко, Денис Навроцкий, Анастасия Свердлова, Александр Семенюк

Поточный ВРС (Block Packet Cipher) алгоритм ориентирован на криптографическую защиту и помехоустойчивое кодирование дискретной видеоинформации, передаваемой с Борта подвижного летательного аппарата на Землю. Шифрование осуществляется поразрядным сложением по модулю 2 блоков исходного текста, размер которых составляет 128, 256, 512 или 1024 бит, с равными по длине блоками двоичных псевдослучайных чисел (ключами, или гаммами). Потоки гамм, синхронно генерируемых как на Борту, так и на Земле, вырабатываются совокупностью криптографических преобразований (примитивов) секретного базового общего ключа, загружаемого на этапе предполетного обслуживания в бортовую и наземную аппаратуру шифрования. Помехоустойчивое кодирование блоков зашифрованных видеосигналов осуществляется одним из трех алгоритмов: Хемминга, БЧХ или Рида-Соломона. Совокупность блоков данных, число которых пропорционально размеру гаммы, образует пакет зашифрованной информации. Переходу к формированию очередного пакета предшествует преобразование общего ключа шифрования, который в свою очередь управляет параметрами блочных ключей (функций гаммирования). Моделирующий комплекс допускает возможность исключения или модификации одного или нескольких примитивов, принимающих участие в образовании шифрующих гамм.

Ключевые слова: *криптографические примитивы, поточные шифры, программно-моделирующий комплекс.*

I. Введение и постановка задачи.

Беспилотные летательные аппараты (БПЛА) в настоящее время составляют основу авиации специального применения. БПЛА используются для патрулирования границ, аэрофотосъемки, разведки геофизическими методами, контроля радиационного фона, а также для сбора различной информации по заявкам гражданских и военных ведомств. Из приведенного краткого, но неуклонно расширяющегося списка областей применения БПЛА однозначно вытекает, как следствие, необходимость обеспечения надлежащей криптографической защиты каналов передачи данных между летательным аппаратом, именуемым также для краткости как «Борт», и наземным пунктом управления (НПУ), который иначе будем обозначать термином «Земля». Пренебрежение такой защитой чревато опасностью несанкционированного вмешательства противника в канал управления БПЛА, что может привести к захвату аппарата.

К важнейшим видам информации, которыми обмениваются Борт и Земля, относятся командная, телеметрическая и видеоинформация [1-3].

Командная информация представляет собой цифровые блоки (пакеты) фиксированной длины, которые поступают по радиоканалу с Земли на Борт для корректировки положения органов управления аппарата с целью выполнения маневров, задаваемых оператором НПУ. *Телеметрическая информация*, передаваемая с Борта на Землю также в виде цифровых пакетов, содержит сведения о положении органов управления БПЛА. И, наконец, *видеоинформация* представляет собой широкополосные сигналы, снимаемые с бортовых цифровых видеокамер (или тепловизоров).

Бортовые видеокамеры необходимы для формирования панорамы в «поле зрения» БПЛА с целью обнаружения различных объектов на местности и определения их координат, разведки районов лесных и торфяных пожаров, крупных техногенных катастроф, экологического мониторинга и др. Отдельные тактические задачи, решаемые на основе бортовой видеоинформации, носят закрытый характер и подлежат защите от несанкционированного доступа. Простое решение проблемы криптографической защиты информации (КЗИ) в широкополосных системах передачи видеосигналов состоит в применении для этих целей поточных шифров.

Главная задача, достижению которой посвящена данная статья, состоит в разработке программно-моделирующего комплекса шифра, обеспечивающего скоростное поточное криптографическое преобразование широкополосных сигналов, формируемых цифровыми видеокамерами, устанавливаемыми на борту БПЛА.

II. Принципы организации КЗИ.

Следует отметить, что в открытой отечественной и зарубежной печати практически отсутствует информация о способах построения систем КЗИ в каналах связи «Земля – БПЛА – Земля». Ниже изложены отдельные подходы к решению указанной проблемы, которые не претендуют на «истину в последней инстанции» и отражают лишь предварительный опыт, накопленный авторами статьи в процессе работы над созданием систем КЗИ в БПЛА, разрабатываемых в НАУ.

Обозначим отличительные особенности предлагаемого BPC (Block Packet Cipher) алгоритма поточного шифрования видеосигналов в каналах передачи информации «БПЛА – Земля»:

1. Шифрование осуществляется поразрядным сложением по модулю 2 блоков видеосигналов, размер которых составляет 128, 256, 512 или 1024 бит, с равными по длине блоками двоичных псевдослучайных чисел (ключами, или гаммами).

2. Потоки гамм, синхронно генерируемых как на Борту, так и на Земле, вырабатываются последовательностью криптографических преобразований (примитивов) секретного базового ключа, загружаемого на этапе предполетного обслуживания в бортовую и наземную аппаратуру шифрования.

3. Совокупность блоков данных, число которых пропорционально размеру гаммы, образует пакет зашифрованной информации. Переходу к формированию очередного пакета предшествует преобразование общего ключа шифрования, который в свою очередь управляет параметрами блочных ключей (функций гаммирования).

4. Для обеспечения синхронизации потоков генерируемых на Борту и на Земле шифрующих гамм каждый двоичный блок видеосигнала дополняется со стороны младших битов совокупностью синхробайтов, предназначенных для записи номеров блоков и пакетов видеосигналов, а также специального сегмента «свой-чужой» (сегмента С-Ч).

5. Синхронизация сеансовых ключей шифрования осуществляется посредством сопоставления номеров сеансов связи, независимо подсчитываемых наземными и бортовыми электронными системами. Под *сеансом связи* понимается процесс передачи с Борта и приема на Земле одного зашифрованного блока видеосигналов вместе с синхробайтами и сегментом С-Ч.

6. В каждом сеансе связи осуществляется смена ключа шифрования (сеансового ключа), что практически сводит к нулю вероятность оперативного взлома шифра.

7. Вне зависимости от значения номеров блоков и пакетов синхробайты и сегменты С-Ч зашифровываются на Борту и расшифровываются на Земле одним и тем же синхроключом, сохраняющимся неизменным на весь период полета беспилотника. Синхроключ загружается в аппаратуру шифрования одновременно с загрузкой базового секретного ключа.

Таким образом, синхронизация сеансовых ключей шифрования блоков видеосигналов, передаваемых по каналу «БПЛА – Земля», осуществляется посредством сопоставления номеров сеансов связи, независимо подсчитываемых наземными и бортовыми электронными системами. Это означает, что номера сеансов связи взаимно однозначно связаны со значениями стохастических сеансовых ключей шифрования.

Передача видеоинформации с борта БПЛА на Землю осуществляется по принципу односторонней радиосвязи, схема которой показана на рис. 1.

Передающий блок, расположенный на борту (Board) БПЛА, содержит: источник видеоинформации (InText-B), которым является бортовая видеокамера; бортовой микроконтроллер (MCB), осуществляющий зашифрование (Encryption) видеосигналов блоками шифрующих гамм, вырабатываемыми генератором ключей (GenKey-B); и непосредственно передатчик (Transceiver) с излучающей антенной.

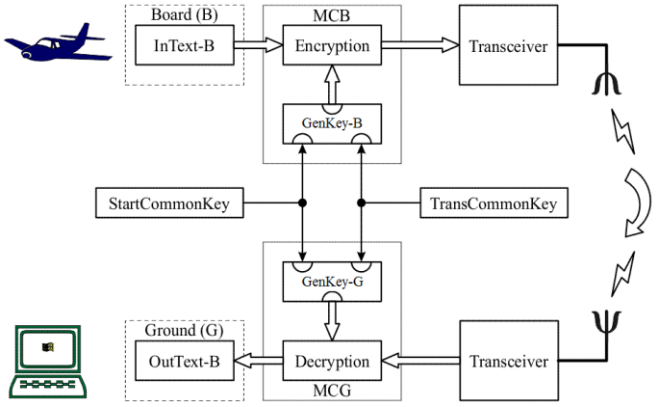

Рис. 1. Структурно-логическая схема канала передачи видеоинформации с борта БПЛА на Землю

Наземный приемный блок включает: приемное устройство (Transceiver) с антенной; микроконтроллер (MCG), который производит расшифрование (Decryption) поразрядным сложением по модулю 2 входного текста с гаммами, поступающими от генератора (GenKey-G); и наземный (Ground) компьютер, осуществляющий обработку выходного текста (Out-Text-B), поступающего с MCG.

Стартовый общий ключ (StartCommonKey) шифрования (*SCK*) загружается во время предполетного обслуживания летательного аппарата в микроконтроллеры БПЛА и аппаратуру НПУ. В бортовом микроконтроллере (MCB) для пакетов видеосигналов вырабатывается последовательность зашифровывающих гамм и синхронно с ними в наземном микроконтроллере (MCG) аппаратуры НПУ – такая же последовательность расшифровывающих гамм.

Шифрование всех последующих пакетов видеосигналов осуществляется под управлением модифицируемых общих ключей (TransCommonKey), или для краткости – *TCK* .

III. Алгоритм шифрования сигналов.

Обобщенная структурная схема алгоритма блочно-пакетного шифрования видеосигналов представлена на рис. 2.

Верхней линейкой окон на рис. 2 обозначены две выполняемые функции: параметризации шифра (окно Parametrization) и генерирования стартового ключа шифрования *SCK* (окно Generation). Более подробные пояснения операций параметризации приведены в разделе V.

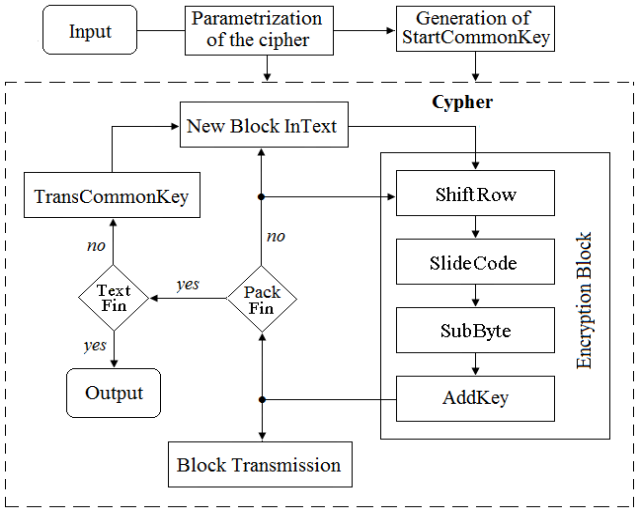

Рис. 2. Структурно-логическая схема алгоритма шифрования последовательности видео блоков

Процесс зашифровки видеосигналов на борту БПЛА и расшифровки потока принятых на Земле блоков происходит практически по схожим алгоритмам. Поэтому ниже более детально будет описан алгоритм зашифрования видеосигналов.

Основная схема шифрования (Cypher), выделенная на рис. 2 пунктирной штриховкой, содержит два вложенных цикла. Внутренним циклом осуществляется поточное шифрование видео блоков, которое состоит в следующем. Общий ключ шифрования, которым является *SCK* – для первого шифруемого пакета, или *TCK* – для всех последующих пакетов, перед шифрованием очередного блока подвергается модификации посредством трех криптографических примитивов: стохастического сдвига (ShiftRow), «скользящего кодирования» (SlideCode) и нелинейной подстановки (SubByte), которые описаны в разделе 4. Способ управления примитивами для общего 128-битного ключа поясняется его структурной схемой, приведенной на рис. 3.

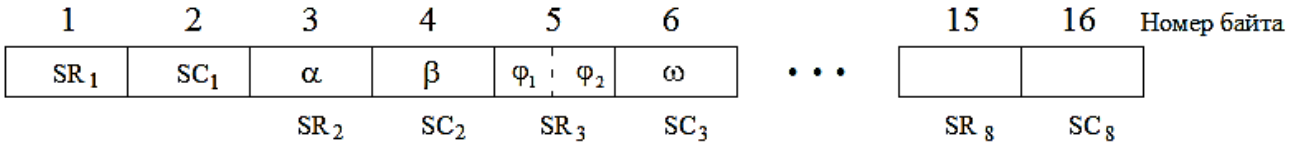

Рис. 3. Формат 128-битного общего ключа шифрования

В пределах пакета шифруемых блоков видеосигналов параметры примитива нелинейной подстановки (SubByte, называемым иначе $S-$блоком), а именно аддитивные компоненты α и β, два примитивных полинома (ПрП) f_1 и f_2 восьмой степени, а также $\omega-$образующий элемент матрицы Галуа, сохраняются неизменными. Способ формирования таблицы $S-$блока детализирован в разделе IV. Байты SR_i и SC_i, $i=\overline{1,NB/2}$, где $NB-$число байт общего ключа шифрования *CKE* (Common Key Encryption), предназначены для управления параметрами примитивов стохастического сдвига и «скользящего кодирования» соответственно.

Таким образом, в пределах каждого пакета выполняется зашифрование $NB/2$ видеоблоков, которое осуществляется поразрядным сложением по модулю 2 блоков видеосигналов с блочными ключами шифрования, которые обозначим *BKE* (Block Key Encryption). Каждый зашифрованный видео блок поступает в передатчик (Block Transmission) и излучается антенной БПЛА.

Ключи *BKE* образуются из общих ключей *CKE* в результате криптографических преобразований примитивами (рис. 2) в соответствии с параметрами, приведенными на рис. 3. Для первого шифруемого пакета ключ *CKE* совпадает со стартовым ключом *SCK*. После окончания обработки последнего видео блока пакета ключ *CKE* модифицируется в блоке TransCommonKey (рис. 4) и далее внутренний цикл шифрования продолжается над очередным пакетом сигналов.

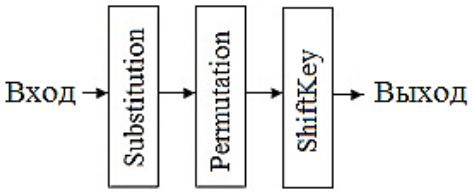

Рис. 4. Примитивы блока TransCommonKey

Параметры примитива Substitution блока *TCK* совпадают с соответствующими параметрами $S-$блока последнего шифрованного пакета видеосигналов. Описания оставшихся примитивов Permutation и Shift даны в разделе IV.

Собственно зашифрование видеосигнала реализуется поразрядным сложением по модулю 2 в блоке AddKey (рис. 2) ключа *BKE* с шифруемым блоком. Расшифрование принятых на Земле зашифрованных видео блоков осуществляется по той же самой схеме, которая применяется для зашифрования видеосигналов. Повторным наложением блочных ключей *BKE* (по схеме XOR) на зашифрованные блоки восстанавливаются исходные видеосигналы.

IV. Криптографические примитивы.

Примитив SubByte осуществляет нелинейную подстановку байтов преобразуемого текста [4] по формуле

$$y=(x+\alpha)_{f_1}^{-1}\cdot A_{f_2}^{(\omega)}+\beta, \qquad (1)$$

где $z_{f_1}^{-1}-$мультипликативное обратное (МО) байта z по модулю неприводимого полинома (НП) f_1 и $A_{f_2}^{(\omega)}-$матрица Галуа над НП f_2 и образующим элементом ω, причем f_1 и f_2 – ПрП восьмой степени, адреса которых заданы полубайтами φ_1 и φ_2 соответственно (рис. 3).

В полном множестве, состоящем из 30 НП восьмой степени, 16 являются ПрП и, естественно, что их удобно адресовать полубайтными векторами, которыми как раз и являются полубайты φ_1 и φ_2. Этим, собственно, и объясняются причины, по которым в S-блоке (1) используются именно примитивные полиномы.

Если образующий элемент $\omega=0$, то матрица A замещается единичной матрицей E. Компонента z_f^{-1} как раз и доставляет нелинейные свойства $S-$блоку.

Преобразование (1) является обобщением классического преобразования

$$y=x_f^{-1}\cdot A+\gamma, \qquad (2)$$

которое лежит в основе построения $S-$блока шифра AES [5]. Все компоненты (f, A и γ) выражения (2) являются детерминированными, тогда как компоненты α, β и ω в (1), так же как и ПрП, зависят от секретного ключа, что повышает криптостойкость ВРС шифра.

Примитив SlideCode («скользящее кодирование», или кратко СК) реализует операцию кодирования Грея «наоборот», под которым понимается следующее: прямое «скользящее кодирование» (обратное СК в шифре ВРС отсутствует) выполняется по схеме обратного классического, называемого левосторонним, кодирования Грея [6, 7], показанного на рис. 5.

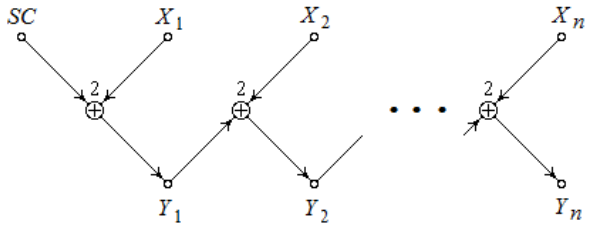

Рис. 5. Левостороннее «скользящее кодирование»

На приведенной схеме СК переменные X_i и Y_i, $i=\overline{1,n}$, являются байтами ключа *BKE* соответственно до и после операции СК, причем $n=N/8$, где N есть длина *BKE* в битах, а SC – байт общего ключа шифрования *ComKey* (рис. 3). Отметим, что СК выполняется над соответствующими битами переменных X_i и Y_i по схеме последовательного или параллельного кодирования.

Примитивом ShiftRow производится стохастический сдвиг формируемой гаммы на нечетное число Z. Для шифруемых блоков длины 1024 бит параметр прокрутки Z определяется значением младшего байта гаммы, который обозначим B. Нечетность байта B обеспечивается принудительной записью единицы в его младший бит. Если размер ключа *BKE* составляет 512, 256 или 128 бит, то параметр прокрутки Z считывается из младших 7, 6 или 5 битов байта B соответственно.

Примитив Substitution блока TransCommonKey (рис. 4) выполняется точно так же, как примитив SubByte, входящий в состав Encryption Block (рис. 2), в то время как **примитив ShiftKey** (циклический сдвиг CommonKey) этого же блока инициализируется по схеме, фрагментарно показанной на рис. 6.

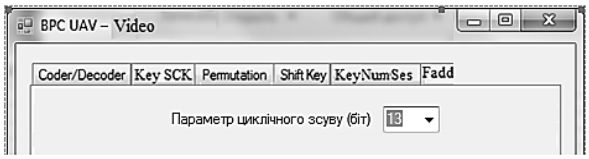

Рис. 6. Параметризация примитива ShiftKey

Параметр циклического сдвига ключа ShiftKey выбирается прокруткой из множества простых чисел в интервале от 3 до 251.

Примитив Permutation (блок Permut) осуществляет табличную перестановку элементов формируемой гаммы блоками, длина которых составляет $l=N/r$ бит, где $N-$размер гаммы, а $r-$ число элементов, на которое разбивается гамма [8].

В BPC шифре параметр r (порядок таблицы перестановки) равен 8, 16 или 32 и выбирается прокруткой, как показано на рис. 7.

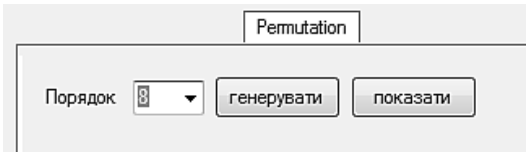

Рис. 7. Параметризация примитива Permutation

Таблица перестановки содержит r строк, каждая из которых представляет собой стохастическую последовательность чисел из интервала $\overline{0,r-1}$.

Содержимое ячейки формируемой гаммы (ключа шифрования) переносится в ячейку, номер которой указан в строках таблицы. В свою очередь номер строки таблицы выбирается из младших разрядов шифрующей гаммы.

V. Моделирующий комплекс BPC шифра.

Окна (и клавиши) инициализации основных примитивов и выполняемых функций моделирующего комплекса показаны на базовом интерфейсе (рис. 8).

Верхняя линейка клавиш предназначена для параметризации примитивов. Нижним рядом клавиш базового интерфейса предусматривается возможность включения (ON), или выключения (OFF) тех или иных примитивов из процесса шифрования. По окончании работы программы на тело интерфейса выводится значение машинного времени и указывается энтропия и размер файлов.

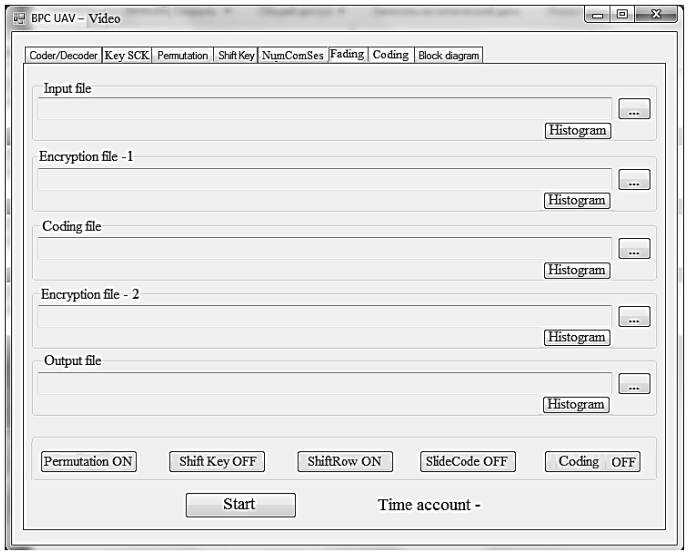

Рис. 8. Базовый интерфейс BPC программно-моделирующего комплекса

Клавишей Key SCK вызывается окно, предназначенное для размещения стартового ключа шифрования. Посредством кнопки «Генерировать» запускается генератор случайных чисел, которым формируется ключ SCK, записываемый в 16-ричной форме в нижних линейках окна интерфейса. На рис. 9 приведен пример 512-битного ключа, представленного в 16-ричной системе счисления.

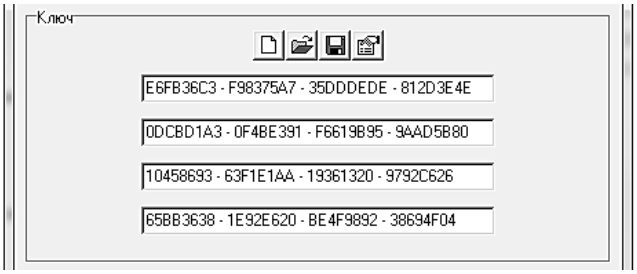

Рис. 9. Вариант стартового ключа длины 512 бит

Нажатием на клавишу Permutation вызывается окно (рис. 7), в котором задается порядок таблицы перестановки. В этом же окне размещается и сама таблица, как это для $r = 8$ показано на рис. 10.

dec	0	1	2	3	4	5	6	7
0	3	2	0	1	5	7	6	4
1	4	1	6	5	3	7	2	0
2	0	1	7	3	5	2	4	6
3	6	3	7	2	4	0	5	1
4	1	6	7	4	2	3	0	5
5	5	2	4	6	7	0	1	3
6	3	4	0	2	1	7	6	5
7	5	7	4	1	2	0	6	3

Рис. 10. Пример перестановочной таблицы

С помощью клавиши NumComSes (Number communication session) или для краткости – NCS, осуществляется параметризация ключа, предназначенного для зашифрования на Борту и расшифрования на Земле номера сеанса связи. Нажатием на клавишу NumComSes на плоскости интерфейса появляется кнопка NCS и окно, в которое записывается 32-битный ключ NCS, как это фрагментарно показано на рис. 10. Повторным нажатием на кнопку NCS можно изменить значение ключа.

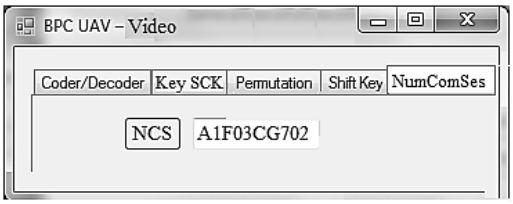

Рис. 10. Параметризация ключа NCS

Клавиша Fading предназначена для того, чтобы иметь возможность записать в соответствующем блоке, показанном на рис. 11, номера блоков видеосигнала, подверженных замиранию и, в силу этого, исключаемых из канала передачи.

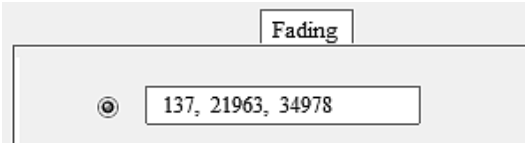

Рис. 11. Параметризация оператора Fading

Нажатием на верхнюю клавишу HamCode в базовом интерфейсе выводится окно (рис. 12), в которое может быть записано число информационных бит (не менее четырех) кода Хемминга.

Рис. 12. Параметризация Хемминг кода

В завершающей части раздела кратко отметим особенности файлов, указанных на рис. 8. *Входным* (Input file) является файл данных, которые могут быть получены как от реального источника видеосигналов, например, видеокамеры, так и от файлов с произвольным расширением. *Шифрофайл*-1 (Encryption file-1) представляет собой последовательность блоков, образованных поразрядным сложением ключей ***BKE*** с блоками входных данных. Каждый такой блок дополняется шифрованным 40-битным номером сеанса связи. Результат помехоустойчивого кодирования данных шифрофайла-1 одним из алгоритмов (Хемминга, циклического или Рида-Соломона) образует *Кодированный файл*, а декодирование последнего приводит к формированию *Шифрофайла*-2 (Encryption file-2), причем 40-битные номера сеансов связи из данного файла исключаются. Обратным криптографическим преобразованием содержимого шифрофайла-2, что приводит к образованию *выходного файла*, восстанавливаются входные данные, за исключением блоков, подверженных федингу.

Способ создания сегмента С-Ч является конфиденциальным и по этой причине не включен авторами статьи в описание программно-моделирующего комплекса.

Анализ эффективности ВРС алгоритма по критерию приближения псевдослучайных последовательностей (потока гамм), генерируемых шифром, к белому шуму проведен по методу, изложенному в [8]. Как подтвердили результаты

анализа, статистические характеристики последовательности шифрующих гамм достаточно близки к характеристикам белого шума.

Выводы. Разработанный программно-моделирующий комплекс реализует один из возможных алгоритмов помехоустойчивой криптографически защищенной передачи широкополосных видеосигналов с борта БПЛА на Землю. Для обеспечения передачи «живого видео», обуславливающего необходимость осуществления обработки информации с высокой скоростью, криптографические преобразования видеосигналов осуществляются посредством поточного шифрования, которым предусмотрено поразрядное логическое сложение битов входных блоков с битами шифрующих гамм, т.е. длина гаммы совпадает с размером блоков видеосигналов. Отличительная особенность алгоритма состоит в том, что шифрующие гаммы модифицируются в каждом сеансе передачи очередного блока, обеспечивая тем самым высокий уровень криптографической защиты информации.

ЛИТЕРАТУРА

[1]. Слюсар В. Передача данных с борта БПЛА: стандарты НАТО. – ЭЛЕКТРОНИКА: НТБ, 2010, № 3. – С. 80–86. [Электронный ресурс] – Режим доступа: www. slyusar.kiev.ua/UAV-1.pdf

[2]. Слюсар В. Радиолинии связи с БПЛА. Примеры реализации. – ЭЛЕКТРОНИКА: НТБ, 2010, № 5. – С. 56–60. [Электронный ресурс] – Режим доступа: www. slyusar.kiev.ua/ENTB_5_10.pdf

[3]. Илюшко В.М. Система передачи данных на базе высотного беспилотного летательного аппарата (СПД «Фаэтон») / Илюшко В.М., Нарытник Т.М. // Зв'язок, 2004, № 7. – С. 38–39.

[4]. Белецкий А.А. Программно-моделирующий комплекс криптографических AES-подобных примитивов нелинейной подстановки / А.А. Белецкий, А.Я. Белецкий, Д.А. Навроцкий, А.И. Семенюк // Захист інформації. – 2014. – Т 16, № 1. – С. 12-22.

[5]. Advanced Encryption Standard (AES) – FIPS 197 [Электронный ресурс] – Режим доступа: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[6]. Grey F. Pulse code communication / F. Grey. – Pat. USA, № 2632058, 1953.

[7]. Белецкий А.Я. Преобразования Грея. Монография в 2-х томах. / А.Я. Белецкий, А.А. Белецкий, Е.А. Белецкий. Т.1. Основы теории. – К.: Кн. Изд-во НАУ, 2007. – 412 с.

[8]. Белецкий А.Я. Программно-моделирующий комплекс SCSPS алгоритма поточного шифрования / А.Я. Белецкий, Д.А. Навроцкий, А.И. Семенюк // Захист інформації. – 2014. – Т 16, № 2. – С. 113-121.

REFERENCES

[1]. Slyusar V. Data transmission from the board of the UAV: NATO standards. – ELECTRONICS: NTB, 2010, № 3. – P. 80-86. http:// www.slyusar.kiev.ua /UAV-1.pdf

[2]. Slyusar V. A radio link with the UAV. A examples of implementation. - ELECTRONICS: NTB, 2010, № 5. – P. 56-60. http: // www.slyusar.kiev.ua /ENTB_ 5_10.pdf

[3]. Ilyushka V.M., Narytnik T.M. The data transmission system based on high-altitude unmanned aerial vehicle (SPD «Phaeton») // Communication, 2004, № 7. – P. 38–39.

[4]. Beletsky A.A. Software-modeling complex cryptographic primitives like AES-nonlinear substitution / A.A. Beletsky, A.J. Beletsky, D.A. Navrotskyi, A.I. Semeniuk // Data Protection, V.1, 2014. – P. 113-121.

[5]. Advanced Encryption Standard (AES) – FIPS 197 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[6]. Grey F. Pulse code communication / F. Grey. – Pat. USA, № 2632058, 1953.

[7]. Beletsky A.Ja. Gray conversion. Monograph in 2 vols. / A.Ja. Beletsky, A.A. Beletsky, E.A. Beletsky. V.1. Fundamentals of the theory. – K.: Book House NAU, 2007. – 412 p.

[8]. Beletsky A.Ja. Software-modeling complex SCSPS stream encryption algorithm / A.Ja. Beletsky, D.A. Navrotskyi, A.I. Semeniuk // Data Protection, Tom 16, V.2, 2014. – P. 113-121.

ПРОГРАМНО-МОДЕЛЮЮЧИЙ КОМПЛЕКС ВРС АЛГОРИТМУ ПОТОЧНОГО ШИФРУВАННЯ І ЗАВАДОСТІЙКОГО КОДУВАННЯ ВІДЕОСИГНАЛІВ, ЩО ПЕРЕДАЮТЬСЯ З БОРТУ БПЛА

Поточний ВРС (Block Packet Cipher) алгоритм орієнтований на криптографічний захист і завадостійке кодування дискретної відеоінформації, що передається з Борта рухомого літального апарату на Землю. Шифрування здійснюється порозрядним додаванням за модулем 2 блоків вихідного тексту, розмір яких складає 128, 256, 512 або 1024 біт, з рівними по довжині блоками двійкових псевдовипадкових чисел (ключами, або гаммами). Потоки гам, що синхронно генеруються як на Борту, так і на Землі, виробляються сукупністю криптографічних перетворень (примітивів) секретного базової загальної ключа, що завантажується на етапі передпольотного обслуговування в бортову і наземну апаратуру шифрування. Завадостійке кодування блоків зашифрованих відеосигналів здійснюється одним з трьох алгоритмів: Хеммінга, БЧХ або Ріда-Соломона. Сукупність блоків даних, число яких пропорційно розміру гами, утворює пакет зашифрованої інформації. Переходу до формування чергового пакету передує перетворення загального ключа шифрування, який у свою чергу управляє параметрами блокових ключів (функцій гамування).

Моделюючий комплекс допускає можливість виключення або модифікації одного або декількох примітивів, які беруть участь в утворенні гам.
Ключові слова: криптографічні примітиви, поточні шифри, програмно-моделюючий комплекс.

PROGRAM-MODELING COMPLEX BPC ALGORITHM STREAM ENCRYPTION AND NOISELESS CODING VIDEO SIGNALS UAV

Stream BPC (Block Packet Cipher) algorithm is oriented to cryptographic protection and noiseless coding discrete video transmitted from the board of rolling the aircraft to the ground. Encryption is done bitwise addition modulo 2 blocks of the source text, the size of which form the 128, 256, 512 or 1024 bits, with equal length blocks of binary pseudo-random numbers (keys or gammas). Flows of gamma synchronously generated both on board and on the ground, produced a set of cryptographic transformations (primitives) secret base public key is loaded on the stage of pre-service and in ground equipment onboard encryption. Noiseless coding blocks encrypted video by one of the three algorithms: Hamming, BCH or Reed-Solomon. A plurality of blocks of data, the number of which is proportional to the size range of forms packet encrypted information. Forming a transition to the next packet is preceded by conversion of the public encryption key, which in turn controls the parameters of the key block (XOR function). Modeling complex is subject to exclusion or modification of one or more primitives involved in the formation of ciphering schemes.
Keywords: cryptographic primitives, stream ciphers, software-modeling complex.

Белецкий Анатолий Яковлевич, доктор технических наук, профессор кафедры электроники Национального авиационного университета.
E-mail: abelnau@ukr.net
Білецький Анатолій Якович, доктор технічних наук, професор кафедри електроніки Національного авіаційного університету.
Beletsky Anatoly, Doctor of Science, Professor of Department Electronics of National Aviation University.

Максименко Артем Владимирович, бакалавр, кафедра электроники Национального авиационного университета.
E-mail: maxisery@gmail.com
Максименко Артем Володимирович, бакалавр, кафедра електроніки Національного авіаційного університету.
Maksymenko Artem, Bachelor, Department of Electronics of National Aviation University.

Навроцкий Денис Александрович, аспирант кафедры электроники Национального авиационного университета.
E-mail: sg6336@yandex.ua
Навроцький Денис Олександрович, аспірант кафедри електроніки Національного авіаційного університету.
Navrotskyi Denys, Postgraduate student of Department Electronics of National Aviation University.

Свердлова Анастасия Дмитриевна, бакалавр, кафедра электроники Национального авиационного университета.
E-mail: miss.bookmark@yandex.ua
Свердлова Анастасія Дмитрівна. Бакалавр, кафедра електроніки Національного авіаційного університету.
Sverdlova Anstasia, Bachelor, Department of Electronics of National Aviation University.

Семенюк Александр Иванович, бакалавр, кафедра электроники Национального авиационного университета.
E-mail: sovist9@mail.ru
Семенюк Олександр Іванович, бакалавр, кафедра електроніки Національного авіаційного університету.
Semenjuk Alexander, Bachelor, Department Electronics of National Aviation University.

УДК 004.056.52

ADFS АУТЕНТИФИКАЦИЯ В ИНФРАСТРУКТУРЕ ОБЛАЧНЫХ СЕРВИСОВ

Владимир Демчинский

В настоящее время применение облачных вычислений приобретает все большее значение. Основная особенность облачных вычислений — предоставление услуг удаленно, в требуемом объеме и в требуемое время, с гибкой системой управления. Однако, использование облачных вычислений порождает новые угрозы информационной безопасности, а также требует переосмысления традиционных угроз для сетевой инфраструктуры. Одна из ключевых задач безопасности – аутентификация - также требует нового подхода. В статье рассмотрены вопросы обеспечения безопасности облачной инфраструктуры и, в частности, использование служб федераций Active Directory для аутентификации.
Ключевые слова: *службы федераций Active Directory, аутентификация, облачные вычисления.*