КОМПЬЮТЕРНАЯ МАТЕМАТИКА

УДК 629.735.05

Б.М. ШЕВЧУК, Е.В. ЗАВИРЮХА, С.В. ФРАЕР

РЕАЛИЗАЦИЯ ЭФФЕКТИВНОЙ КРИПТОСТОЙКОЙ ПЕРЕДАЧИ ПАКЕТОВ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

В работе на информационном уровне предложена реализация криптостойкой защиты информации абонентами радиосетей путем формирования псевдохаотических пакетов информации. На основе анализа и исследования работы криптостойких генераторов псевдослучайных последовательностей обосновано выполнение абонентами элементарных операций, необходимых для формирования криптостойких пакетов, подлежащих передаче по радиоканалу и каналам связи сетей общего пользования.

Введение. Широкое применение беспроводных компьютерных сетей (радиосетей) в промышленности, при решении задач мониторинга состояний удаленных объектов различного назначения и природы, в телемедицине, в процессе контроля функциональных состояний операторов, спортсменов и других областях человеческой деятельности достигается за счет решения комплекса проблем обеспечения надежной и защищенной передачи информации по радиоканалам. Поскольку минимальной единицей посылки данных в радиоканале является информационный пакет (ИП), то надежность и защищенность радиосвязи определяется энергетическим соотношением сигнал/шум битовых посылок ИП, эффективностью алгоритмов помехоустойчивого кодирования/декодирования данных, а также степенью защиты массивов данных, из которых формируются ИП.

Современные компьютерные сети строятся по иерархическому принципу и для обеспечения информационной безопасности использования ресурсов сети, особенно ресурсов общего пользования, применяются различные элементы системы безопасности, которым свойственна многоуровневая иерархия в пределах территории, здания, этажа, блока. При этом с применением системного подхода решаются следующие задачи: идентификация сетевых ресурсов абонентов, ассоциирование их с сетевыми адресами; защита информации и ресурсов от несанкционированного доступа и от подмены данных; активный

динамический контроль за использованием сети абонентами (пользователями); обнаружение атак на критически важные ресурсы и подсети. Для решения этих задач применяются маршрутизаторы и межсетевые экраны, осуществляющие фильтрацию пакетов и ограничение прохождения определенного (разрешенного) трафика, а также устройства кэширования и анализа контента. В радиосетях для защиты информации широкого распространения получили потоковые методы шифрования данных [1, 2], обеспечивается комплекс мероприятий по аутентификации и авторизации абонентов сети и защиты трафика данных с использованием MAC (Media Access Control)-фильтрации и WPA и WPA2 (Wi-Fi Protecting Access)-шифрования. В сенсорных беспроводных сетях ISM диапазона радиочастот (ISM – Industrial, Scientific, Medical: 433 МГц, 688 МГц, 902–928 МГц (для США), 2,4 ГГц) используется 128-битное AES-шифрование (AES – Advanced Encryption Standard).

В беспроводных сенсорных, локально-региональных и глобальных (спутниковых) сетях удаленные и подвижные абоненты должны быть уверены, что конфиденциальная информация передается только тому абоненту, которому она предназначена. Точками утечки информации в таких сетях является радиоканал и сети передачи информации компьютерных сетей общего пользования, которые связывают удаленных абонентов разнородных сетей. Поэтому актуальной проблемой построения криптостойких беспроводных сетей широкого применения являются разработка и эффективное использование методов и алгоритмов оперативной защиты информации в местах зарождения информационных потоков путем формирования абонентами сетей безизбыточных криптостойких массивов данных, подлежащих передаче по радиоканалам и другим каналам связи между парами абонентов «отправители – получатели» ИП.

Цель работы – исследование и обоснование методов формирования псевдохаотических криптостойких пакетов информации парами абонентов радиосети «отправитель – получатель» ИП с применением абонентских генераторов криптостойких псевдослучайных последовательностей (ПСП). При этом законы генерации криптостойких ПСП, методы кодирования/декодирования данных должны быть известны текущей паре абонентов радиосети, участвующих в приеме/передаче криптостойких ИП. Применяемые абонентами стандартные алгоритмы и средства защиты информации дополнительно гарантируют повышенную степень защиты данных в сетях.

Кодирование, формирование и передача криптостойких ИП в радиосетях. В радиосетях передача информации (сигналов, изображений, массивов данных) осуществляется в пакетном режиме, при котором двоичные массивы данных разбиваются на короткие информационные кадры (ИК) пакетов данных, как правило, переменной длины или объема. Для надежной защиты информации каждый абонент радиосети должен иметь секретный ключ (длинное число), который не должен быть известен другим абонентам сети. При этом процесс передачи информации предполагает, что пара абонентов «отправитель – получатель» ИП должны владеть информацией о текущих секретных ключах (СК),

которые используются для шифрования/дешифрования ИК пакетов данных. Согласно теории К. Шеннона о построении секретных систем передачи информации [3], текущий СК должен использоваться только один раз, т. е. после шифрования и передачи битов текущего ИК данный СК должен быть заменен на другой. При этом в теоретически стойких секретных системах связи СК по объему не должен быть меньшим объема первичных данных $\{X_i\}$ и шифрограммы $\{Y_i\}$, где $i=1,n$, n – количество бит ИК. На практике шифрование данных с одноразовым ключом (шифр Вернама) осуществляется на основе выполнения операции суммирования по модулю 2 битовых последовательностей первичного массива данных $X=x_1, x_2, \ldots, x_i, \ldots, x_n$ и соответствующей последовательности битов ПСП текущего СК $K=k_1, k_2, \ldots, k_i, \ldots, k_n$. Для j-й операции шифрования парой абонентов, которые принимают участие в приеме/передаче ИП, генерируется текущая ПСП битов $k_j=k_{1j}, k_{2j}, \ldots, k_{ij}, \ldots, k_{nj}$. Таким образом, базовыми операциями защиты массивов данных ИП на абонентских системах (АС) являются операции генерирования длительных ПСП, из которых для j-й операции шифрования/дешифрования данных выбираются соответствующие n-битовые фрагменты ПСП, или генерирование ограниченных по длительности j-ых ПСП, а также операции гаммирования соответствующих массивов данных, формирования хэш-функций массивов данных и проверочных кодов ИК, перемешивание битов ИК и битов проверочных кодов ИК [4, 5]. Величина степени защиты информации P_z пропорциональна величине массивов данных, подлежащих гаммированию: $P_z \geq \max [2^m]$, где m – минимально необходимая длина текущей ПСП, которая используется в операциях гаммирования для надежной защиты информации ($m \geq 2048$ бит).

Таким образом для достижения практически стойкой криптографической защиты информации необходимо каждый ИК текущего пакета данных шифровать своим секретным шифром, который меняется от пакета к пакету. При этом каждый абонент сети имеет закрытый секретный ключ, который неизвестен другим абонентам, а также имеет базу данных кодовых ключей для генерации криптостойких ПСП [5]. При необходимости передачи пакетов данных s-у абоненту сети r-й абонент передает s-у абоненту короткий пакет-запрос и после получения подтверждения от s-го абонента, передает последнему сеансовый ключ, зашифрованный средствами ассиметричной криптографии. После этого осуществляется передача ИП, зашифрованных своими секретными сеансовыми ключами. С целью реализации криптостойкой и замаскированной (в шумах радиоканала) передачи информации неизвестными для других абонентов должны быть методы сжатия-защиты данных, методы формирования сигналов, которые подлежат передаче по радиоканалу, а также структура этих сигналов. Поэтому защита данных абонентами радиосети должна быть реализована на различных уровнях: на информационном уровне, на уровне формирования сигнально-кодовых конструкций, на энергетическом уровне.

При шифровании данных на информационном уровне с применением одноразовых шифров степень защиты информации существенно зависит от характеристик генератора ПСП. Надежно защищенные данные должны быть безизбыточными псевдохаотическими последовательностями битовых посылок, характеристики которых приближаются к характеристикам криптостойких генераторов ПСП.

Анализ функциональных характеристик криптостойких генераторов ПСП. Генератор ПСП, ориентированный на использование в системах защиты информации, должен соответствовать таким требованиям: криптографическая стойкость; хорошие статистические свойства; большой период генерированных последовательностей; эффективная аппаратная и программная реализация [6]. Основным свойством криптостойкого генератора ПСП является непредсказуемость влево, т. е. криптоаналитик, знающий принцип работы такого генератора, имеющий возможность анализировать фрагмент $\gamma_i\ \gamma_{i+1}\ \gamma_{i+2}\ldots\ \gamma_{i+(t-1)}$ выходной последовательности, но не знающий используемой ключевой информации для определения предыдущего выработанного элемента последовательности γ_{i-1} не может предложить лучшего способа, чем подбрасывание жребия [6].

В рамках другого подхода к построению качественного генератора ПСП предлагается свести задачу построения криптографически сильного генератора к задаче построения статистически сильного генератора. Статистически безопасный генератор ПСП должен удовлетворять следующим требованиям: ни один статистический тест (из подборки Кнута, NIST или др.) не обнаруживает в ПСП каких-либо закономерностей, иными словами не отличает эту последовательность от истинно случайной; нелинейное преобразование F_k, зависящее от секретной информации (ключа k), используемое для построения генератора, должно обладать свойством «размножения» искажений – все выходные (преобразованные) вектора e' возможны и равновероятны независимо от исходного вектора e; при инициализации случайными значениями генератор порождает статистически независимые ПСП.

Проанализируем работу генератора ПСП CryptMT, который является криптостойкой модификацией вихря Мерсенна (Mersenne Twister). Материнский генератор вихрь Мерсенна – 32-х битный и имеет 19937 бит внутреннего состояния и период $2^{19937} - 1$. Алгоритм CryptMT вычисляет результат работы вихря Мерсенна и использует наиболее значимые 8 бит в качестве секретных случайных чисел. Его период составляет $2^{19937} - 1$, этот генератор работает в 1,5–2 раза быстрее, чем наиболее оптимизированный AES в режиме счетчика [7]. Идея CryptMT состоит в том, чтобы используя небезопасный генератор псевдослучайных чисел, применить к результату его работы некоторые преобразования, чтобы получить криптостойкую ПСП. Вихрь Мерсенна генерирует последовательность беззнаковых 32-битных целых чисел (слов). Ключ и начальное значение конкатенируются и передаются в инициализационную схему вихря

Мерсенна. Берется переменная accum размера слова и устанавливается ее начальное значение 1. Следующий процесс происходит в цикле [7]: с помощью вихря Мерсенна генерируется псевдослучайное слово *gen_ran*; *gen_rand* умножается на accum: *accum*←*accum*×(*gen_rand* | 1); выводятся 8 наиболее значимых бит accum. Возвращение к первому шагу. Для увеличения безопасности первые 64 бита полученной последовательности отбрасываются. Здесь знак «|» обозначает побитовое *или*. Умножение производится по модулю 2^{32}. Этот метод генерирует псевдослучайные последовательности байт, которые удовлетворяют обычные требования к поточным шифрам. При построении CryptMT авторы руководствовались такими принципами: использовать следует быстрый линейный генератор с огромным внутренним состоянием (к примеру, тысячи бит); результат работы материнского генератора следует фильтровать с помощью нелинейного преобразования с конечным числом состояний, причем состояния должны быть относительно невелики (к примеру, одно слово); результатом должна быть только небольшая часть информации состояний (например, 8 бит из 32) [7].

Для сравнительной оценки на рис. 1 и 2 показаны характеристики двух генераторов ПСП: рис. 1, а, 2, а, в – характеристики генератора ПСП C++ random, рис. 1, б, 2, б, г – характеристики генератора ПСП CryptMT.

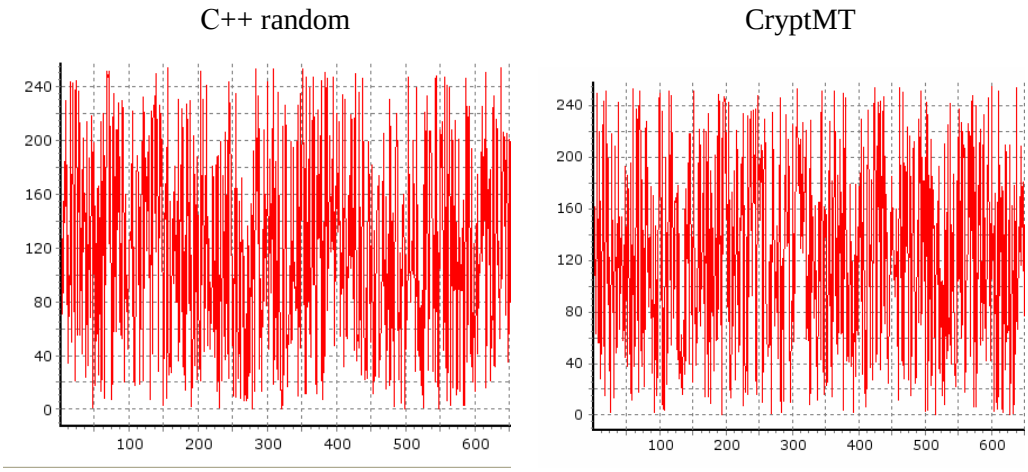

РИС. 1. Внешний вид выходных сигналов генераторов ПСП

На рис. 2 показаны распределения q-битовых символов (q = 7,8) для двух видов генераторов ПСП. Распределения q-битовых символов (частота встречи амплитудных значений q-битовых символов) выходных массивов данных криптостойких генераторов ПСП характеризуются практически равномерным распределением символов.

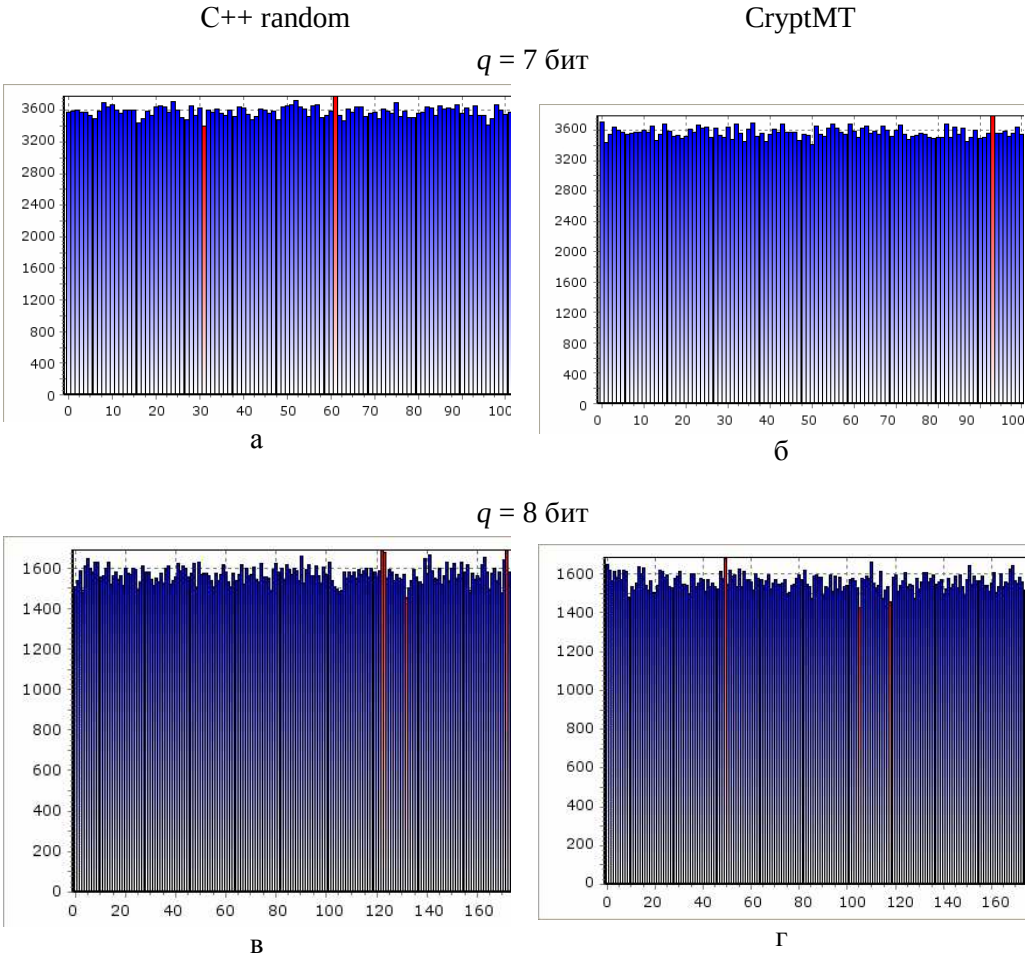

РИС. 2. Распределение q-битовых символов выходных данных генераторов ПСП (q = 7,8)

На рис. 3 показаны хаосграммы выходных массивов данных криптостойких генераторов ПСП, которые отображают хаотическую зависимость амплитудных значений (i+1)-го символа от i-го. Осуществляя гаммирование исходных сжатых последованостей различных данных (сигналов, изображений, массивов данных) с криптостойкими ПСП, получаем защищенные массивы данных, из которых формируются ИК пакетов. В зависимости от времени обработки и кодирования данных операцию гаммирования возможно выполнить одноразово, например, после выполнения операций сжатия данных без потерь, формирования проверочных кодов или хэш-функций. Многоразовое выполнение операций гаммирования данных существенно повышает степень защиты информации за счет контролируемого искажения первичных массивов данных в процессе многоциклового выполнения операции сжатия-защиты двоичных данных [5].

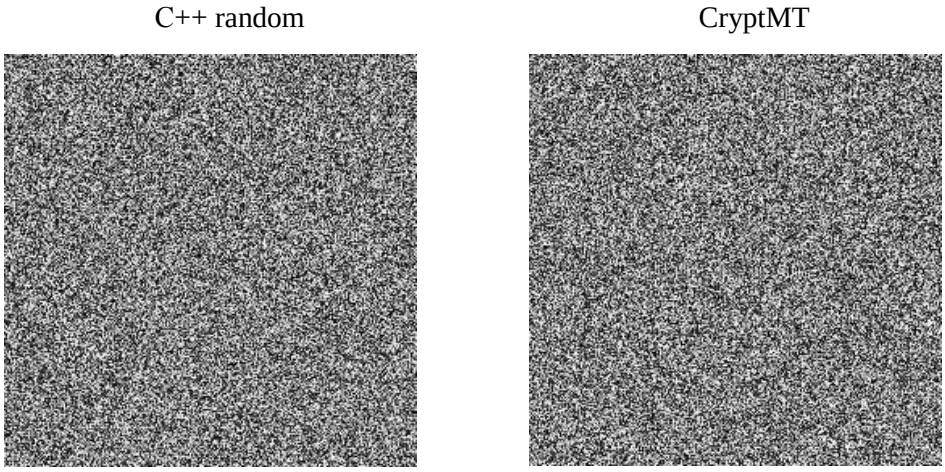

РИС. 3. Хаосграммы генераторов ПСП

Предварительные исследования показали, что достаточно одной операции гаммирования для получения выходных массивов данных, характеристики которых приближаются к криптостойким псевдохаотическим массивам данных. Соответственно без знания сеансовых СК несанкционированным абонентам радиосетей и сетей общего пользования неизвестны параметры исходных массивов данных до и после процедур сжатия-защиты информации.

Выводы. В радиосетях и сетях общего пользования процесс передачи информации предполагает, что пара абонентов должны владеть информацией о текущих секретных ключах, с помощью которых реализуется шифрование/дешифрование данных. Для обмена информацией о сеансовых СК наиболее целесообразно удаленным абонентам сетей применять средства асимметричной криптографии. За счет гаммирования исходных сжатых последовательностей различных данных с криптостойкими ПСП получаем криптостойкие данные, из которых формируются псевдохаотические ИК пакетов информации.

1. *Столлингс В.* Основы защиты сетей: приложения и стандарты. – М.: Издательский дом «Вильямс», 2002. – 429 с.
2. *Шахнович Н.В.* Современные технологи беспроводной святи, 2-е изд. / Шахнович И.В. – М.: Техносфера, 2006. – 288 с.
3. *Шеннон К.* Теория связи в секретных системах // Работы по теории информации и кибернетике. – М.: Изд. иностр. лит., 1963. – С. 333–369.
4. *Шевчук Б.М., Задірака В.К., Гнатів Л.О., Фраєр С.В.* Технологія багатофункціональної обробки і передачі інформації в моніторингових мережах. – К.: Наук. думка, 2010. – 370 с.
5. *Шевчук Б.М.* Захист інформації при передачі пакетів даних в інформаційно-ефективних локально-регіональних радіомережах // Штучний інтелект. – 2010. – № 4. – С. 706–711.

6. *Иванов М.А., Чугунков И.В.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.
7. *Makoto Matsumoto, Takuji Nishimura, Mariko Hagita and Mutsuo Saito.* Cryptographic Mersenne Twister and Fubuki Stream / Block Cipher. – http://eprint.iacr.org/2005/165.pdf.

Получено 14.10.2010

Б.М. Шевчук, О.В. Завірюха, С.В. Фраєр

РЕАЛІЗАЦІЯ ЕФЕКТИВНОЇ КРИПТОСТІЙКОЇ ПЕРЕДАЧІ ПАКЕТІВ ІНФОРМАЦІЇ У БЕЗДРОТОВИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

У роботі на інформаційному рівні запропонована реалізація криптостійкого захисту інформації абонентами радіомереж шляхом формування псевдохаотичних пакетів інформації. На основі аналізу і дослідження роботи криптостійких генераторів псевдовипадкових послідовностей обгрунтоване виконання абонентами елементарних операцій, необхідних для формування криптостійких пакетів, які підлягають передачі по радіоканалу і каналах зв'язку мережах загального користування.

B.M. Shevchuk, O.V. Zaviriukha, S.V. Fraier

THE IMPLEMENTATION OF EFFECTIVE CRYPTOGRAPHIC INFORMATION PACKAGES TRANSFER IN WIRELESS COMPUTER NETWORKS

An implementation of information security for radio subscribers using a generation of pseudochaotic information packages is proposed . The execution of elementary operations by subscribers is based on the analysis of cryptographically strong generators operation. The operations are necessary to form cryptographically strong information packages, which are transferred using radio or communication channels of public networks.

Об авторах:

Шевчук Богдан Михайлович,
кандидат технических наук, старший научный сотрудник
Института кибернетики имени В.М. Глушкова НАН Украины,
e-mail: incors@ukr.net

Завирюха Елена Валентиновна,
младший научный сотрудник
Института кибернетики имени В.М. Глушкова НАН Украины,
e-mail: arien@dept140.kiev.ua

Фраер Сергей Владимирович,
младший научный сотрудник
Института кибернетики имени В.М. Глушкова НАН Украины.