МРНТИ 27.47.17 https://doi.org/10.26577/RCPh.2020.v73.i2.09

А.К. Амангелдина, К.Б. Хайрошева*

Казахский национальный университет им. аль-Фараби,
Казахстан, г. Алматы,*e-mail: khairosheva.k@gmail.com

КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ БЕСПРОВОДНЫХ СЕТЕЙ НА ОСНОВЕ ИНФОРМАЦИОННО-ТЕОРЕТИЧЕСКОГО ПОДХОДА

В современных системах связи существует четкое разделение между шифрованием данных и исправлением ошибокв потоке сообщений. На физическом уровне открытой системы передачи данных реализовано исправление ошибок, позволяющее более высоким уровням абстрагировать данный уровень как идеальный битовый канал. Шифрование, основанное на криптографических принципах, происходит на более высоких уровнях.Такое разделение долгое время было очевидным решением в большинстве систем связи, но в последнее время растёт интерес к обеспечению безопасности непосредственно на физическом уровне путем использования свойств базового канала связи. При таком подходе безопасность обеспечивается теоретико-информационным подходом, который не требует трудно вычисляемых функций, как в традиционной криптографии. Информационно-теоретическая безопасность, впервые введенная Шенноном и получившая широкое признание как самая строгая нотация безопасности, становится все более привлекательной для многих киберфизических систем, беспроводных сетей, систем распределенного управления и других приложений.Тем не менее, остается много открытых вопросов для полной интеграции теоретико-информационной безопасности в будущие системы связи. В данной статье рассмотрены аутальные результаты в области теоретической защиты информации.

Ключевые слова: беспроводные сети, теория Шеннона, условная энтропия, информационно-теоретическая безопасность.

A.K. Amangeldina, K.B. Khayrosheva*

Al-Farabi Kazakh National University, Kazakhstan, Almaty,
*e-mail: khairosheva.k@gmail.com

Confidentiality of wireless network data based on an information-theoretical approach

In modern communication systems, there is a clear separation between data encryption and error correction in the message flow. At the physical level of an open data transmission system, error correction is implemented that allows higher levels to abstract this level as an ideal bit channel. Encryption based on cryptographic principles occurs at higher levels. This separation has long been an obvious solution in most communication systems, but recently there has been an increasing interest in providing security directly at the physical level by using the properties of the basic communication channel. With this approach, security is ensured by an information-theoretic approach that does not require difficult to compute functions, as in traditional cryptography. Information and theoretical security, first introduced by Shannon and widely recognized as the most stringent security notation, is becoming increasingly attractive to many cyber-physical systems, wireless networks, distributed control systems and other applications. Nevertheless, many open questions remain for the full integration of information and theoretical security into future communication systems. This article discusses the autonomous results in the field of theoretical information security.

Key words: wireless network, Shannon theory, conditional entropy, information-theoretic security.

Ә.К. Амангелдина, Қ.Б. Хайрошева*

Әл-Фараби атындағы Қазақ ұлттық университеті, Қазақстан, Алматы қ.
*e-mail: khairosheva.k@gmail.com

Ақпараттық-теориялық тәсіл негізінде сымсыз желі деректерінің құпиялығы

Қазіргі заманғы байланыс жүйелерінде мәліметтерді шифрлеу мен хабарлама ағынындағы қателерді түзету арасында нақты алшақтық бар. Деректерді берудің ашық жүйесінің физикалық деңгейінде қателіктерді түзету жүзеге асырылады, бұл жоғары деңгейлерге идеалды биттік канал ретінде осы деңгейден абстракциялауға мүмкіндік береді. Криптографиялық принциптерге негізделген шифрлау жоғары деңгейлерде жүреді. Бұл бөлу бұрыннан бері көптеген байланыс жүйелерінде айқын шешім болды, бірақ соңғы уақытта негізгі байланыс арнасының қасиеттерін пайдалану арқылы қауіпсіздікті тікелей физикалық деңгейде қамтамасыз етуге қызығушылық артуда. Бұл тәсілмен қауіпсіздік дәстүрлі криптографиядағыдай функцияларды есептеуді қажет етпейтін ақпараттық-теориялық тәсілмен қамтамасыз етіледі. Шеннон алғаш рет енгізген және қауіпсіздіктің ең қатаң белгілері ретінде кеңінен танымал болған ақпараттық және теориялық қауіпсіздік көптеген киберфизикалық жүйелерге, сымсыз желілерге, таратылған басқару жүйелеріне және басқа қосымшаларға барған сайын тартымды бола түсуде. Соған қарамастан, болашақ байланыс жүйелеріне ақпараттық және теориялық қауіпсіздікті толық енгізу үшін көптеген ашық сұрақтар қалады. Бұл мақалада теориялық ақпараттық қауіпсіздік саласындағы автономды нәтижелер қарастырылады.

Түйін сөздер: сымсыз желілер, Шеннон теориясы, шартты энтропия, ақпараттық-теориялық қауіпсіздік

Введение

Традиционно безопасность рассматривается как независимая функция, адресованная выше физического уровня, и все широко используемые криптографические протоколы (например, RSA, DES и AES) разрабатываются и реализуются при условии, что физический уровень уже установлен и обеспечивает безошибочную связь. В отличие от этого, существуют как теоретические, так и практические вклады, которые поддерживают идею безопасности физического уровня для значительного укрепления безопасности цифровых систем связи.

Основной принцип информационно-теоретической безопасности требует сочетания криптографических методов с методами канального кодирования, которые используют случайность каналов связи для гарантиии, что отправленные сообщения не могут быть перехвачены или расшифрованы третьей стороной, злонамеренно подслушивающей на беспроводном носителе [1].

Информационно-теоретический подход к обеспечению безопасной связи открыло новое многообещающее направление для решения проблем безопасности беспроводных сетей. Такой подход был инициирован Винером [2] и Цисзар и Корнером [3] в 1970-х годах XX века, которые показали, что конфиденциальные данные могут передаваться безопасно без использования ключа шифрования. Согласование же секретного ключа (включая генерацию и распространение) с помощью теоретического анализа информации было позднее предложено в работах Маурера [4-5] и в работе Альсведе и Чисзара [6], которые показали, что два или несколько абонента (Алиса и Боб) могут договориться о ключе (для последующего шифрования), хранящемся в секрете от других (от Евы).

В 1970-1980-х годах влияние этих работ было ограниченным, отчасти из-за отсутствия практических кодов прослушивания, но главным образом потому, что строго положительная секретность в классической настройке канала прослушивания требует, чтобы законный отправитель и получатель имели некоторое преимущество над нарушителем, с точки зрения качества канала. В 1976 году Диффи и Хеллман [7] опубликовали основные принципы криптографии с открытым ключом, которые должны были быть приняты почти всеми современными схемами защиты. Алгоритмы с открытым ключом просты, с точки зрения управления ключами, но требуют значительных вычислительных ресурсов [8]. По сравнению с алгоритмами с открытым ключом алгоритмы с секретным ключом являются вычислительно эффективными и обеспечивают более высокую пропускную способность данных, одновременно создавая проблемы для управления ключами, такие как безопасное хранение и распространение ключей

[9-12]. Так, для облегчения управления ключами и достижения высокой эффективности на практике используются гибридные криптосистемы [13-14], в которых секретный ключ распределяется по алгоритмам с открытым ключом, а шифрование и дешифрование могут затем использоваться алгоритмы с секретным ключом. Однако некоторые недостатки алгоритмов с открытым ключом представляют серьезную проблему для гибридных криптосистем. Помимо высокой вычислительной стоимости, алгоритмы с открытым ключом не являются доказуемо абсолютно безопасными и уязвимы для так называемой атаки "человек посередине" (атака MiTM). Кроме того, использование алгоритмов с открытым ключом для распределения секретных ключейдобавляет еще один уровень сложности в проектирование сетей. Также нужно отметить, что обеспечение безопасной связи по беспроводным сетям с использованием криптографических подходов представляет дополнительные значительные проблемы из-за:

- открытого характера беспроводной среды, которая позволяет подслушивающим устройствам и злоумышленникам перехватывать передачу информации (в частности, передачу секретных ключей) или ухудшать качество передачи;
- отсутствия инфраструктуры в децентрализованных сетях, что затрудняет распределение ключей;
- динамической топологии мобильных сетей (например, мобильных специальных сетей), что делает управление ключами дорогостоящим.

В последнее время появление и все более широкое распространение беспроводных сетей вызвало значительный интерес к информационно-теоретическому подходу обеспечения безопасной связи. Информационно-теоретическая защита означает, что любой алгоритм имеет незначительную вероятность нарушения свойства безопасности. Это то же самое, что и безусловная безопасность: она не опирается на какие-либо вычислительные предположения и не ограничивается вероятностными нарушителями. В этой статье представлен обзор последних исследований по обеспечению безопасности беспроводной связи, также в начале статьи рассмотрена идея теоретико-информационного подхода для безопасной передачи конфиденциальных сообщений.

Модель безопасности Шеннона

Рассмотрим криптосистему Шеннона, представленную на рисунке 1[1]. Исходное сообщение X шифруется в текст Y, ключом K, совместно используемым передатчиком и приемником. Подслушивающий, который знает семейство функций шифрования (ключей) и вероятность выбора ключей, может перехватить зашифрованный текст Y. Система считается совершенно безопасной, если апостериорные вероятности события X заданного Y равны априорным вероятностям X для всех Y, т.е. $P(X|Y) = P(X)$. Количество различных ключей должно быть по меньшей мере таким же большим, как и количество сообщений для достижения надежного засекречивания.

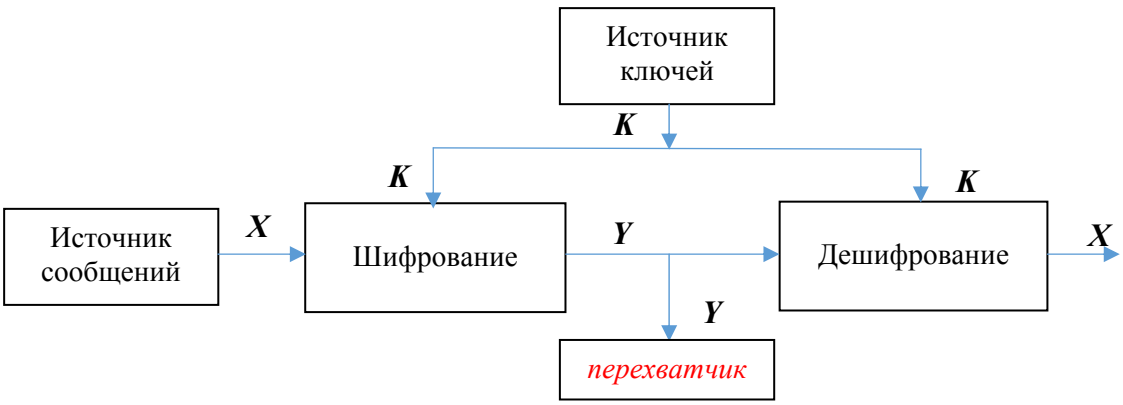

Рисунок 1 – Криптосистема Шеннона

Для измерения количества информации, связанной с сообщением, и количества неопределенности, связанной с возможностями ключа, введено понятие энтропии $H(X)$ и $H(K)$, соответственно,

$$H(X) = -\sum_{i=0}^{N-1} P(x_i) \log_2 P(x_i), \quad (1)$$

здесь X (Алиса) может принимать значения из набора исходных сигналов $\mathcal{K} = \{x_0, x_1, \dots, x_{N-1}\}$; Y(Боб) может принимать значения из набора принятых сигналов $\mathcal{Y} = \{y_0, y_1, \dots, y_{M-1}\}$. Энтропия указывает на среднюю длину двоичной последовательности (в битах), необходимую для представления случайной величины x_i (с малой вероятностью ошибки). Для измерения неопределенности подслушивающего лица (Ева) относительно сообщения Шеннон также ввёл понятия условной энтропии (или equivocation) $H(X|Y)$:

$$H(X|Y) = -\sum_{i=0}^{N-1} \sum_{j=0}^{M-1} P\left(x_i|y_j\right) \log_2 P(x_i). \quad (2)$$

Условная энтропия $H(X|Y)$ может быть интерпретирована как величина неопределенности, остающаяся относительно случайной величины X или исходного выходного сигнала, при условии, что мы знаем, какое значение принимал принятый сигнал Y. Дополнительное знание об Y должно уменьшить неопределенность относительно X, и можно показать, что [15]

$$H(X|Y) \leq H(X).$$

Исходя из свойств энтропии, получаем [1]

$$H(K,X) = H(K) + H(X), \quad (3)$$

$$H(K,X) = H(K,X,Y) = \\ = H(K,Y) = H(Y) + H(K|Y), \quad (4)$$

$$H(K,X) = H(K,X,Y) \geq H(X,Y) = \\ = H(Y) + H(X|Y). \quad (5)$$

В случае полной секретности, т.е. при

$$H(X) = H(X|Y) \quad (6)$$

согласно (3) и (5) подразумевается, что

$$H(K) \geq H(Y). \quad (7)$$

Более того, по (3) и (4), если

$$H(Y) = H(X), \text{ то } H(K) = H(K|Y), \quad (8)$$

т.е. никакая информация о ключе не может быть выведена из зашифрованного текста Y.С другой стороны, если

$$H(Y) = H(X) + H(K), \quad (9)$$

то согласно (3) и (4) $H(K|Y) = 0$, т.е. ключ может быть определён из Y.Значит значение

$$H(Y) = H(X) + H(K) \quad (10)$$

определяет расстояние уникальности, т.е. минимальную длину зашифрованного текста, который гарантирует восстановление ключа, используемого для шифрования.

Фундаментальное стремление Шеннона к совершенной секретности говорит о том, что энтропия источника не может быть больше энтропии секретного ключа, изначально разделяемого отправителем и законным получателем. Мэсси [16] дал информационно-теоретическое доказательство этого результата, и его доказательство не требует независимости ключа и исходного сообщения. При дальнейшем допущении независимости могут быть показаны некоторые более сильные результаты, которые определяют распределение вероятностей ключа и зашифрованного текста. Эти результаты показывают, что энтропия ключа не меньше логарифма размера выборки сообщений в любом шифре, обеспечивающем идеальную секретность, даже если распределение источника фиксировано. То же самое относится и к энтропии зашифрованного текста. Эти результаты остаются в силе, если исходное сообщение было сжато до шифрования.

Безопасность на беспроводном уровне

Интерес к теоретической безопасности вновь возник, возможно, благодаря работе Маурера [5] (1993 г.), который доказал, что даже когда законные пользователи сети (Алиса и Боб) имеют худший канал, чем перехватчик (Ева), они могут генерировать секретный ключ через общение по небезопасному, но аутентифицированному каналу. Появление беспроводной связи, которая особенно восприимчива к прослушиванию из-за широковещательного характера среды передачи, побудило более внимательно проанализировать потенциал секрет-

ности беспроводных сетей на физическом уровне.

Суть схемы Маурера заключалась в совместной разработке секретного ключа передатчиком и получателем посредством связи по общедоступному (небезопасному) и безошибочному каналу обратной связи. Предполагается, что Алиса, Боб и Ева знают случайные величины X, Y, Z, соответственно, с совместным распределением вероятности P_{XYZ}. У Евы нет информации о величинах X и Y, кроме Z, т.е. $I(XY; T/2)$, где T суммирует полную информацию Евы о сети. Алиса и Боб изначально не имеют секретного ключа, кроме ключа, необходимого для гарантии подлинности и целостности сообщений, отправляемых по общедоступному каналу, но предполагается, что они знают P_{XYZ}. Ева может перехватывать каждое сообщение между Алисой и Бобом, но Ева не может вставлять свои сообщения или изменять истинные сообщения в общедоступном канале без обнаружения.

Алиса и Боб используют протокол, в котором на каждом этапе Алиса отправляет сообщение Бобу в зависимости от X и всех сообщений, ранее полученных от Боба, или наоборот с заменой X на Y. Без ограничения рассматриваются только те протоколы, в которых Алиса отправляет сообщение с нечетными шагами $C_1,C_3,\ldots$, а Боб – с четными шагами $C_2,C_4,\ldots$ Алиса и Боб могут без потери общности расширить свои известные случайные величины X и Y случайными битами, статистически независящими от X, Y и Z. В конце t-пошагового протокола Алиса вычисляет ключ S как функцию от X и $C^t = [C_1,\ldots,C_t]$, Боб вычисляет ключ S' как функцию от Y и C^t. Их цель – максимизировать $H(S)$ в условиях, когда Sи S' согласуются с очень высокой вероятностью и, что у Евы мало информации о Sи S'. Более формально

$$H\left(C_i|C^{i-1}X\right) = 0, \text{ для нечетных } i, \quad (11)$$

$$H\left(C_i|C^{i-1}Y\right) = 0, \quad \text{для четных } i. \quad (12)$$

Для каждого протокольного соглашения о ключе [5]

$$H(S) \le I(X;Y|Z) + H(S|S') + I(S;\ C^tZ). \quad (13)$$

Следует отметить, что $I(X,Y) < I(X;\ Y|Z)$ вполне выполнимо.

Гауссовский канал прослушивания телефонных разговоров – это самая базовая модель для беспроводного канала, имеющая линейные не зависящие от времени мультипликативные каналы, искаженные аддитивным белым гауссовским шумом [17]. Когда Алиса передает сигнал X_i, то принятые сигналы Боба $Y_{B,i}$ и Евы $Y_{E,i}$ при использовании канала iмогут быть выражены как

$$Y_{B,i} = h_BX_i + N_{B,i} \text{и} Y_{E,i} = h_EX_i + N_{E,i}, \quad (14)$$

где h_B и h_E – коэффициенты усиления между Алисой и Бобом и между Алисой и Евой, соответственно.$N_{B,i}$ и $N_{E,i}$ – аддитивный белый гауссовский шум с ненулевым средним и дисперсиями σ_B^2,σ_E^2 соответственно.С учётом ограничения средней мощности передачи P секретность пропускной способности гауссовского канала прослушивания будет

$$C_S = \frac{1}{2}log\left(1 + \frac{P|h_B|^2}{\sigma_B^2}\right) - \frac{1}{2}log\left(1 + \frac{P|h_E|^2}{\sigma_E^2}\right). \quad (15)$$

Стратегия достижения секретности – это передача с полной мощностью P и выбор входных сигналов в соответствии с распределением Гаусса. Этот последний выбор ни в коем случае не очевиден, так как гауссовский ввод макмимизирует поток информации к Бобу, но в тоже время и к Еве. Секретная емкость в этом случае оказывается равной разнице между пропускной способностью Шеннона основного канал и пропускной способностью Шеннона подслушивающего канала. Из этого следует, что безопасная связь возможна тогда и только тогда, когда у Боба канал лучше, чем у Евы, в том смысле, что отношение SNR основного канала должно быть больше, чем у Евы, т.е.

$$\frac{|h_B|^2}{\sigma_B^2} > \frac{|h_E|^2}{\sigma_E^2}.$$

В работе Hero [18] предлагается теоретико-информационная основа для исследования информационной безопасности в беспроводных каналах с множественными входами и выходами (MIMO). Отправной точкой этого исследования является то, что хорошо спроектированная безопасная линия связи должна иметь низкую вероятность перехвата (LPI) и низкую вероятность обнаружения (LPD) по отношению к несанкционированному перехватчику. Пока-

зано, что дополнительная защита от обнаружения или перехвата может быть достигнута путем пространственно-временного кодирования на нескольких антеннах на передатчике и приемнике. В частности, когда такая информация доступна для передатчика, можно разработать пространственно-временную модуляцию / демодуляцию для использования известных характеристик распространения и помех в канале, доступных для клиента, но не для подслушивателя. Для каналов без памяти это соответствует пространственному (многоканальному) шифрованию и скрытию информации, где информация общего канала играет роль общего закрытого ключа, который можно использовать для разблокировки сообщения.

Системы с MIMO могут значительно улучшить производительность беспроводной передачи, поэтому составляют основу большинства современных беспроводных систем с высокой пропускной способностью. Предполагается, что Алиса, Боб и Ева имеют несколько передающих и приёмных антенн. Когда Алиса передаёт вектор-сигнал $\boldsymbol{X}_i$, принятые сигналы $\boldsymbol{Y}_{B,i}$и $\boldsymbol{Y}_{B,i}$ могут быть выражены как

$$\boldsymbol{Y}_{B,i} = \boldsymbol{H}_B\boldsymbol{X}_i + \boldsymbol{N}_{B,i}, \quad \boldsymbol{Y}_{E,i} = \boldsymbol{H}_E\boldsymbol{X}_i + \boldsymbol{N}_{E,i},$$

где $\boldsymbol{H}_B$ и $\boldsymbol{H}_E$ – матрицы, содержащие мультипликативные усиления канала, $\boldsymbol{N}_{B,i}$ и $\boldsymbol{N}_{E,i}$ – независимые аддитивные вектора гауссовского шума сигналов Боба и Евы с нулевым средним.

Заключение

Теоретико-информационные подходы к безопасности распространяются на модели для физических беспроводных каналов. Безопасность на физическом беспроводном уровне является одним из ключевых приложений этих концепций, поскольку сигнал, передаваемый по беспроводной среде, не только принимается его предполагаемым приемником, но также легко перехватывается нелегитимными приемниками. Несовершенство беспроводной среды поможет установить безопасность за счет использования шумного канала.

Сосредоточившись на теоретических моделях и аналитических результатах, ведущие исследователи показывают, как методы, основанные на принципах кодирования источника и канала, могут обеспечить новые способы решения проблем безопасности данных, встроенной безопасности, конфиденциальности и аутентификации в современных информационных системах.

Основная идея теоретико-информационного подхода для безопасной передачи конфиденциальных сообщений (без использования ключа шифрования) законному получателю состоит в том, чтобы использовать собственную случайность физического носителя (включая шумы и колебания канала из-за замирания) и использовать разницу между каналом для законного получателя и каналом для подслушивающего устройства в интересах законного получателя.

Литература

1 Liang Y., Poor H.V. and Shamai (Shitz)S. Information Theoretic Security //Foundations and Trends R in Communications and Information Theory. – 2008. – Vol 5, Nos 4-5. – P.355-580.

2 Wyner A.D. The wire-tap channel //Bell System Technical Journal. – 1975. –Vol.54. – P.1355-1387.

3 CsiszarI. and Korner J. Broadcast channels with con_dential messages //IEEE Transactions on Information Theory. – 1978. –Vol. 24. – P.339-348.

4 MaurerU.M.Provably secure key distribution based on independent channels //Proc. of the IEEE Information Theory Workshop (ITW), Veldhoven, The Netherlands, June 1990.

5 MaurerU.M.Secret-key agreement by public discussion based on common information //IEEE Transactions on Information Theory. – 1993. –Vol.39. – P.733-742.

6 Ahlswede R. and Csisza rI. Common randomness in information theory and cryptography. Part I: Secret sharing //IEEE Transactions on Information Theory. – 1993. –Vol.39. –P.1121-1132.

7 Diffie W. and Hellman M. New directions in cryptography //IEEE Trans. Inf. Theory. – 1976. –Vol.IT-22, no. 6. – P.644–654.

8 Саломаа А.Криптография с открытым ключом. –М.: Мир, 1995. – 320 с.

9 AsokanN. and GinzboorgP. Key-agreement in ad hoc networks //Computer Communications. – 2000. –Vol.23, no. 17. – P.1627-1637.

10 Naga Satish G., Raghavendran Ch.V., Mehar P.T.K., Dr. Suresh Varma P. Secret key cryptographic algorithm //International Journal of Computer Science, Information Technology and Management. – 2012. – Vol.1, No.1-2.

11 Pietro R.D., Mancini L.V., and Jajodia S. Efficient and secure keys management for wireless mobile communications //Proc. of the 2nd ACM International Workshop on Principles of Mobile Computing. Toulouse, France, 2002. – 2002. – P.66-73.

12 Zhu B., Bao F., Deng R.H., Kankanhalli M.S., and Wang G. Efficient and robust key management for large mobile ad hoc networks //Computer Networks. – 2005. –Vol.48. – P. 657-682.

13 Cramer R. and Shoup V., Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack //SIAM Journal on Computing. – 2004. –Vol.33, no. 1. – P.167-226.

14 Dennis H. and Kiltz E. Secure hybrid encryption from weakened key encapsulation //Proc. of the 27th Annual International Cryptology Conference (CRYPTO). Santa Barbara, CA, USA, August 2007. – 2007. –P.553-571.

15 Sayood K. Mathematical Preliminaries for Lossy Coding //in book "Introduction to Data Compression (4th Edition)" – Elsevier, 2012. – P.217-250.

16 MasseyJ.L.An introduction to contemporary cryptology //Proc. IEEE, – 1988. – Vol. 76. – P. 533-549.

17 Vincent PoorH. andSchaefer Rafael F. Wireless physical layer security //PNAS. – 2017. – Vol.114 (1). – P.19-26.

18 Hero A.O. Secure space-time communication //IEEE Transactions on Information Theory. – 2003. – Vol.49,Iss.12. – P.3235-3249.

References

1 Y. Liang, H.V. Poor, and S. Shamai (Shitz), Foundations and Trends R in Communications and Information Theory, 5 (4-)5, 355-580 (2008).

2 A.D. Wyner, Bell System Technical Journal, 54, 1355-1387 (1975).

3 I. Csiszar and J. Korner, IEEE Transactions on Information Theory, 24, 339-348 (1978).

4 U.M. Maurer, Provably secure key distribution based on independent channels, in Proc. of the IEEE Information Theory Workshop (ITW), Veldhoven, The Netherlands, June (1990).

5 U.M. Maurer, IEEE Trans. on Information Theory, 39, 733-742 (1993).

6 R. Ahlswede and I. Csiszar, IEEE Trans. on Information Theory, 39, 1121-1132 (1993).

7 W. Diffie and M. Hellman, IEEE Trans. Inf. Theory, IT-22 (6), 644–654 (1976).

8 A.Salomaa,Kriptografiya s otkrytymklyuchom, (Moscow, Mir, 1995), 320 s. (in Russ.)

9 N. Asokan and P. Ginzboorg, Computer Communications, 23 (17), 1627-1637(2000).

10 G.Naga Satish, Ch.V.Raghavendran, P.T.K.Mehar, Dr. P. Suresh Varma, Intern. J. of Computer Science, Information Technology and Management, 1 (1-2) (2012).

11 R.D. Pietro, L.V. Mancini, and S. Jajodia, Efficient and secure keys management for wireless mobile communications, in Proc. of the 2nd ACM International Workshop on Principles of Mobile Computing, Toulouse, France, 66-73 (2002).

12 B. Zhu, F. Bao, R. H. Deng, M. S. Kankanhalli, and G. Wang, Computer Networks, 48, 657-682 (2005).

13 R. Cramer and V. Shoup, SIAM Journal on Computing, 33 (1), 167-226 (2004).

14 H. Dennis and E. Kiltz, Secure hybrid encryption from weakened key encapsulation, in Proc. of the 27th Annual Intern. Cryptology Conference (CRYPTO),Santa Barbara, CA, USA, August 2007,553-571 (2007).

15 K.Sayood, Mathematical Preliminaries for Lossy Coding //in book "Introduction to Data Compression (4th Edition) (Elsevier, 2012), 217-250.

16 J.L. Massey, An introduction to contemporary cryptology,Proc.IEEE, 76, 533-549 (1988).

17 H. Vincent Poor and Rafael F. Schaefer, PNAS, 114(1), 19-26 (2017).

18 A.O. Hero, IEEE Transactions on Information Theory, 49 (12), 3235-3249 (2003).