Обзор современных теоретико-информационных подходов к решению основных задач криптографии и стеганографии*

В. А. Монарёв
Институт вычислительных технологий СО РАН, Новосибирск, Россия
e-mail: viktor.monarev@gmail.com

А. Н. Фионов
Сибирский государственный университет телекоммуникаций и информатики, Новосибирск, Россия
e-mail: fionov@sibsutis.ru

Ю. И. Шокин
Институт вычислительных технологий СО РАН, Новосибирск, Россия
e-mail: shokin@ict.nsc.ru

Теоретико-информационные подходы к криптографии и стеганографии позволяют строить системы защиты информации, стойкость которых доказывается математически строго и не зависит от каких-либо предположений о вычислительной трудоемкости некоторых задач или осуществимости новых вычислительных схем, например, квантовых компьютеров. В связи с этим возникает большой интерес исследователей к таким системам. В статье дается обзор основных направлений исследований в указанной области.

Ключевые слова: криптография, стеганография, теоретико-информационная стойкость, совершенные криптосистемы, идеальные шифры, совершенные стегосистемы.

Введение

Для современных информационных систем характерны две тенденции. С одной стороны, постоянно возрастают объем и ценность информации, с другой — среда для передачи данных становится все более открытой. Это вызывает особый интерес исследователей к разработке новых, адекватных современным системам, средств защиты информации. В настоящем обзоре рассматриваются два класса таких средств: средства криптографической и стеганографической защиты информации. Во всех системах защиты существуют понятия "законных" отправителей и получателей информации, которых будем называть (легальными) *пользователями* системы, и неких третьих лиц, от которых скрывается информация и которых коллективно будем называть *противником*.

*Работа выполнена в рамках НИР по гос. контракту № 02.740.11.0396.

Классическая задача криптографии — скрыть содержание передаваемых или хранимых данных (сообщений) от противника. Эта задача решается путем шифрования данных, т. е. применения к ним некоторых математических преобразований, зависящих от секретного ключа, известного только легальным пользователям. В настоящее время предложено и практически применяются множество шифров. Некоторые из них (DES, Rijndael (AES), ГОСТ 28147-89) закреплены в соответствующих государственных стандартах. Многие из этих шифров весьма эффективны с вычислительной точки зрения. Однако основной их недостаток состоит в отсутствии доказанных гарантий секретности, или стойкости. Стойкость этих шифров существенным образом зависит от уровня развития средств вычислительной техники и успехов криптоанализа. Так, повышение производительности компьютеров позволяет вскрывать шифры путем перебора ключей. Фактически это произошло с шифром DES, который использовался в течение десятилетий финансовыми и правительственными институтами США. Сегодня DES может быть взломан за несколько дней с помощью относительно недорогого оборудования. В результате злоумышленник, сохранивший данные межбанковского обмена, может получить ценную информацию о счетах, заинтересованные организации могут прочитать секретные сообщения, переданные несколько лет назад конкурентами, и т. д. Успехи постоянно совершенствующегося криптоанализа представляют еще большую угрозу, так как ведут к появлению более быстрых алгоритмов взлома шифров, чем простой перебор ключей. Наконец, серьезные проблемы со стойкостью возникают в связи с появлением новым парадигм вычислений, таких как квантовые вычисления. Квантовые компьютеры за счет присущего им массового параллелизма позволяют эффективно решать многие классически трудные задачи.

В одной из первых работ в области научной криптографии [?] Шеннон с помощью теоретико-информационных аргументов показал принципиальную возможность построения шифров, стойкость которых не зависит от мощности вычислительных средств и криптоаналитических методов противника. Такие шифры называются *безусловно стойкими*, и их построение тесно связано с теоретико-информационным подходом к синтезу и анализу. Безусловно стойкий шифр не может быть раскрыт даже при полном переборе ключей: противник в этом случае будет получать множество правдоподобных вариантов решения шифра (криптограмм) без какой-либо возможности выбрать один из них, в действительности зашифрованный. Так как безусловная стойкость шифров доказывается математически строго на теоретико-информационном уровне, данный класс шифров также называют *доказуемо стойкими*.

Классическая задача *стеганографии* — передать сообщение так, чтобы сам факт передачи оставался скрытым. Стеганографическая защита информации, несмотря на то что ее принципы были известны еще в древности, стала привлекать внимание исследователей в последние два десятилетия, поскольку позволяет эффективно решать такие задачи, как аутентификация данных, установление авторства, защита от несанкционированного копирования и др. Чаще всего задача скрытия факта передачи сообщения решается путем встраивания сообщения в некоторый контейнер, например, графический файл, передача которого осуществляется на регулярной основе и не вызывает подозрений. Исходный контейнер называется пустым, а контейнер с внедренным сообщением — заполненным (в реальных стегосистемах контейнеры могут заполняться лишь на некоторую долю их емкости). Кроме того, в современных системах сообщение обычно встраивается в контейнер в зашифрованном виде. Внедренное сообщение нарушает “естественные” информационные связи и зависимости в контейнере, в частности,

искажает его статистическую структуру, что дает возможность выявления скрытых сообщений во многих практически реализованных стегосистемах.

В работе [?] Кашен впервые сформулировал понятие *совершенной стегосистемы*, не позволяющей определить факт наличия скрытого сообщения. Это понятие близко к соответствующим понятиям теории шифров Шеннона и базируется на теоретико-информационных принципах. Чтобы построить идеальную стегосистему, необходимо разработать такие методы внедрения сообщений, которые не искажали бы статистическую структуру контейнера. Иными словами, пустой и заполненный контейнеры должны быть статистически неразличимы.

В современных сложных информационных системах средства криптографической и стеганографической защиты объединяются для более полного решения задач информационной безопасности. Поэтому в настоящем обзоре рассмотрены оба эти средства. Как будет показано, они часто базируются на похожих конструкциях.

1. Теоретико-информационная стойкость криптографических систем

1.1. Определение критериев стойкости

Рассмотрим классическую схему секретной связи. Пользователь A передает данные пользователю B по открытому каналу связи, который прослушивается противником (криптоаналитиком) E. A и B используют шифр с секретным ключом, причем ключ передается по особому "закрытому" каналу, обычно обладающему низкой пропускной способностью. Предполагаем, что противник имеет неограниченные вычислительные возможности. Какими свойствами в этих условиях должен обладать шифр, чтобы обеспечить секретность передаваемых сообщений?

Пусть сообщение $X = x_1x_2, \ldots, x_n$ шифруется при помощи секретного ключа $K = k_1k_2, \ldots, k_s$, в результате чего получается зашифрованное сообщение $Y = y_1y_2, \ldots, y_\ell$. Обозначим через $H(X) = H(x_1x_2, \ldots, x_n)$ энтропию сообщения, через $H(Y)$ и $H(K)$ — соответственно энтропии шифротекста и ключа. Тогда $H(x_1x_2, \ldots, x_n|Y)$ представляет неопределенность, или неоднозначность (equivocation), сообщения, а $H(K|Y)$ — неопределенность ключа при условии, что известен шифротекст Y. Шеннон ввел следующие определения для шифров.

Шифр называется совершенным, если

$$H(x_1x_2, \ldots, x_n|Y) = H(x_1x_2, \ldots, x_n) \quad \textit{для любых } n.$$

Шифр называется идеальным, если

$$H(x_1x_2, \ldots, x_n|Y) > 0 \quad \textit{и} \quad H(K|Y) > 0 \quad \textit{при } n \to \infty.$$

Наконец, *шифр называется строго идеальным, если*

$$H(x_1x_2, \ldots, x_n|Y) = H(K|Y) = H(K) \quad \textit{при } n \to \infty.$$

Неформально, если шифр совершенен, то после перехвата криптограммы противник имеет ту же неопределенность о переданном сообщении, какую он имел *a priori*. Известная реализация совершенного шифра (шифр Вернама, см. [?]) состоит в сложении по

модулю 2 бит сообщения с битами секретного ключа при условии, что ключ выбирается полностью случайно, используется только один раз и его длина равна длине сообщения. Идеальность шифра означает, что независимо от объема перехваченного шифротекста и своих вычислительных возможностей криптоаналитик не может получить однозначного решения криптограммы, т. е. у него всегда будет оставаться *какая-то* неопределенность в том, какое сообщение было передано и какой ключ использован. Строгая идеальность означает, что эта неопределенность равна неопределенности ключа, т. е. (при случайно выбираемых ключах) количество решений криптограммы равно количеству различных ключей и все решения равновероятны. До недавнего времени все эти системы представляли в основном теоретический интерес, так как эффективных методов их реализации не было.

В качестве одного из направлений исследования рассматривались другие, менее пессимистичные меры степени секретности. Например, в [?] предлагалась мера секретности криптосистемы в терминах среднего (ожидаемого) числа правдоподобных сообщений, т. е. среднего числа комбинаций сообщение—ключ, которые могут приводить к появлению наблюдаемой криптограммы. В то же время предполагается, что число сообщений заданной длины n, имеющих смысл в некотором языке, очень мало по сравнению с полным набором возможных векторов длины n. Еще одно определение дано в [?]. В этой работе рассматриваются условно совершенная система и конструкция рандомизированного шифра при малой энтропии ключа, обеспечивающая секретность в шенноновском смысле при условии, что с большой вероятностью криптоаналитик не может решить вычислительно трудную задачу. В [?] Мерхав, рассматривая источники без памяти, предлагает следующий критерий секретности. Очевидно, что вероятность правильного угадывания сообщения на основе знания лишь распределения вероятностей источника

$$\max_X P(X) = \left[\max_x P(x)\right]^n = 2^{-n\Gamma_S},$$

где x — отдельный символ сообщения, X — строка длины n, $\Gamma_S = -\log \max_x P(x)$. В таком случае как много бит ключа $K(X)$ должно быть использовано для гарантии того, что вероятность правильной расшифровки убывает с такой же экспоненциальной скоростью как $2^{-n\Gamma_S}$? Мерхав дает ответ на этот вопрос. Рейт (rate) ключа $R(X) = K(X)/n$ должен быть не меньше, чем $\Gamma_S - D(Q \parallel P)$, где второй терм представляет собой расхождение Куллбака – Ляйблера между оценочным и реальным распределением вероятностей источника (т. е., по существу, длину универсального кода). Если это расхождение равно нулю, то соответствующий минимальный достижимый средний рейт ключа оказывается отрицательным логарифмом вероятности наиболее вероятной буквы сообщения, что в общем случае меньше энтропии. Такой подход к понятию секретности приводит к ситуации: если в некоторой системе удается правильно расшифровать 99 % сообщений, но 1 % остается скрытым, то система считается стойкой. Очевидно, что это может считаться удовлетворительным далеко не во всех случаях.

1.2. Криптография в каналах с шумами

В классической системе Шеннона предполагалось, что восстановление зашифрованного сообщения на стороне законного получателя свободно от ошибок и шифрование и расшифрование производятся с использованием одного и того же секретного ключа. В работе [?] первое предположение ослаблено и рассмотрен случай, когда восстановление сообщения на стороне законного получателя производится с ошибкой, т. е. допустим

определенный уровень искажения. Выходная последовательность источника представляется как независимые реализации некоторой случайной величины S, а секретный ключ — как случайная величина, не зависящая от S. Предполагается, что основной канал ($A \longrightarrow B$) менее шумный, чем канал прослушивания ($A \longrightarrow E$). Безопасность системы может быть измерена неопределенностью или минимально достижимым искажением на стороне противника, который получает только выход канала E. Для каждого случая определяется разрешенная область параметров. Полученные результаты могут быть переформулированы с учетом новых критериев секретности Мерхава [?]. Одной из систем, которые могут приводить к подобного рода ситуации, является система, предложенная в [?]. В этой работе описан метод шифрования с последующим сжатием. Каждый бит секретного ключа выбирает один из двух символов алфавита источника, выбранные символы складываются с символами сообщения (по модулю размера алфавита), затем преобразованное таким образом (зашифрованное) сообщение сжимается, причем ключ выступает в роли сопутствующей информации (side information) на стороне отправителя. Рассматриваются две возможности: сжатие без потерь с использованием кода Слепиана — Вольфа или сжатие с потерями с помощью кода Вайнера — Зива. В работе [?] ослаблено второе предположение Шеннона о равенстве ключей у отправителя и получателя. Предполагается, что ключ передается по каналу с очень низкой пропускной способностью и, чтобы повысить надежность шифрования, отправитель ключа передает его со скоростью, превышающей пропускную способность этого канала, допуская некоторое искажение сообщения после дешифрования получателем. Для такой постановки задачи дана характеристика области достижимости в пространстве трех параметров: секретности (измеряемой в терминах неоднозначности), сжимаемости криптограммы и искажения, ассоциируемого с реконструкцией сообщения источника. Показано, что наилучшая стратегия состоит в стремлении к совершенному соответствию между ключами шифрования и расшифрования путем применения надежного канального кодирования бит ключа и управления искажением только посредством кодирования сообщения источника перед шифрованием.

Следующее направление исследований в области теоретической стойкости криптосистем связано с рассмотрением ситуации, когда и получатель, и противник пользуются каналами с шумами, причем уровень шумов у противника, как правило, больше, чем у получателя. Канал, доступный противнику, обычно называется каналом прослушивания (wiretap channel). В одной из первых работ по этой тематике [?] было введено понятие емкости секретности (secrecy capacity), определяемой как максимальный рейт кода, все еще обеспечивающий секретность на стороне плохого канала перехватчика, причем неопределенность равна безусловной энтропии источника (как в совершенной системе Шеннона), что делает информацию, доступную перехватчику, бесполезной. Предложена следующая схема, реализующая эту идею. Создается достаточно длинный код, надежно декодируемый на стороне легального получателя сообщения и представляющий собой иерархию рандомизированных подкодов, каждый из которых индивидуально надежно декодируется противником. Однако биты, декодируемые противником, — это только биты рандомизации, которые не несут никакой информации об источнике сообщения. В последующие годы развитию данного направления было посвящено много исследований. Особенное внимание в них уделяется гауссовским каналам прослушивания. Для таких каналов емкость секретности представляет собой просто разность между пропускными способностями основного (законного) канала и канала прослушивания [?]. Другая модель изучается в [?]. Здесь основной канал связи бесшумный, но против-

ник имеет доступ только к некоторому подмножеству кодовых бит. В [?] модель канала прослушивания расширяется на два параллельных широковещательных канала, соединяющие передатчик и приемник, и оба канала прослушиваются противниками, которые, однако, не взаимодействуют между собой. В [?] область рассмотрения расширяется в двух направлениях: секретный ключ имеется у отправителя и получателя сообщений, но допускается некоторое искажение при восстановлении получателем зашифрованного сообщения. Основная теорема кодирования предлагает принцип разделения, который утверждает, что асимптотическая оптимальность схемы не теряется, если кодер вначале применяет RD-код (т. е. код с задаваемым рейтом, допускающий искажение данных) и шифрует сжатые биты, а затем — хороший код для канала прослушивания.

Ряд работ развивают идеи интерференции в каналах прослушивания, когда кодер имеет доступ к интерференционному сигналу в качестве сторонней информации [?]. Хайаши [?] установил несколько формул неасимптотического характера для разрешимости канала и емкости идентификации. Формулы применены к каналам прослушивания. Изучена наиболее общая постановка задачи, так как не делалось предположений о стационарности канала и отсутствии в нем памяти, в результате чего решена открытая проблема Хана и Верду. Более того, получены нижние границы экспонент вероятностей ошибок и количества информации, получаемой перехватчиком через канал прослушивания. В [?] изучается задача совместного внедрения, сжатия и шифрования информации, т. е. проводится связь исследований в области криптографии с задачами стеганографии. Устанавливается принцип троекратного разъединения, согласно которому асимптотически для длинных блоковых кодов оптимальность не теряется, если вначале к источнику водяного знака применить RD-код с заданным уровнем искажения, затем зашифровать сжатое кодовое слово и, наконец, внедрить его в покрывающий текст. Фундаментальные пределы и методы кодирования для каналов прослушивания изучаются в [?]. В этой работе дано альтернативное рассмотрение доказательства емкости секретности для каналов прослушивания и показано, как корректирующие коды, достигающие границ производительности, могут использоваться для достижения емкости секретности для любого канала прослушивания. Здесь же рассматриваются двоичный канал со стираниями и двоичный симметричный канал как частные случаи для каналов прослушивания и предлагаются специфические практические коды. В некоторых случаях предложенные коды достигают емкости секретности, в других — обеспечивают рейт более низкий, чем емкость секретности. Для особого случая бесшумного основного канала и двоичного канала со стираниями рассматривается дизайн кодера и декодера для кодов, достигающих секретности для каналов прослушивания. Показано, что можно построить коды секретности, декодируемые за линейное время, на базе LDPC-кодов.

В одной из последних работ [?] система секретности Шеннона изучается в постановке, когда как получатель, так и противник имеют доступ к сопутствующей информации, коррелированной с источником, но противник получает как кодированную, так и сопутствующую информацию через каналы более шумные, чем соответствующие каналы у получателя, который, кроме того, разделяет общий секретный ключ с отправителем. Для такой системы рассматривается оптимальное соотношение между пятью параметрами: неоднозначность сообщения и ключа у перехватчика, искажение при восстановлении сообщения у получателя, фактор расширения полосы кодированных каналов, рейт секретного ключа относительно источника и средняя стоимость передачи.

1.3. Криптография в каналах множественного доступа

Тематика каналов с гауссовским шумом получила развитие в исследованиях, связанных с проблемами теоретической секретности в каналах множественного доступа и в беспроводных сетях. Гауссовский канал множественного доступа с прослушиванием, где отправитель и получатель пользуются несколькими антеннами, а перехватчик прослушивает эфир с помощью одной антенны, описывается следующими уравнениями:

$$Y = HX + N_Y, \quad z = G^T X + n_z,$$

где X — передаваемый сигнал; Y и z — сигналы, принимаемые соответственно получателем и противником; N_Y — гауссовский случайный вектор с нулевым средним и единичной ковариационной матрицей; n_z — гауссовская случайная величина с нулевым ожиданием и единичной дисперсией. Передаваемый сигнал удовлетворяет ограничению по средней энергии:

$$\frac{1}{n}\sum_{i=1}^{n} X_i^T X_i \leq P.$$

Емкость секретности $C(P)$ определяется как максимальное число бит, которые могут быть верно переданы получателю, в то время как противник, получивший свой сигнал z, не узнает практически никакой информации о переданном сигнале:

$$C(P) = \max_{p(U,X)} \left[I(U;Y) - I(U;z) \right],$$

где максимум находится по всем распределениям, удовлетворяющим $U \to X \to Y_z$. Таким образом, задача нахождения емкости секретности — это задача поиска распределения $p(U,X)$, максимизирующего указанную разность взаимных информаций.

В работе [?] определена емкость секретности для гауссовского MISO-канала прослушивания (Multiple Input Single Output), а также рассмотрена возможность наличия у противника множества антенн. В [?] рассматриваются обобщенный гауссовский канал множественного доступа с прослушиванием и гауссовский двусторонний канал с прослушиванием. В модели обобщенного канала множество пользователей передают сообщения получателю в присутствии противника, который прослушивает их сигналы посредством другого подобного канала. В модели двустороннего канала с прослушиванием два пользователя обмениваются друг с другом по общему гауссовскому каналу, который (также посредством отдельного канала) прослушивает противник. Для обоих случаев определяются точки распределения мощности, максимизирующие достижимый суммарный рейт секретности. Из анализа видно, что оптимальная политика может предотвращать передачу от некоторых терминалов, чтобы сохранить секретность системы. На основе этой идеи предлагается схема совместного подавления, где пользователи, передача которых заблокирована вследствие политики распределения мощности, подавляют противника, помогая таким образом остальным пользователям. Установлено, что эта схема увеличивает достижимый суммарный рейт секретности. В работе [?] показано, что правильно построенное пространственно-временное распределение антенн передатчика может улучшить информационную безопасность и скрытность передачи, в частности, существенный выигрыш достигается, когда передатчик и приемник клиента информированы о своем канале, в то время как передатчик и приемник противника не имеют информации об этом канале. В мультитерминальных сетях важна кооперация пользователей [?]. Одна из моделей содержит произвольное число терминалов, каждый

из которых получает отдельную компоненту сообщения дискретного множественного источника без памяти, причем разрешена неограниченная и интерактивная открытая связь между терминалами. Показано, что подмножество этих терминалов может служить в качестве помощников для остальных терминалов в генерации секретности. Авторы [?] предлагают схему, возможную в случае, когда передатчик использует множество антенн для передачи лишь в нуль-пространстве канала прослушивания, делая само прослушивание невозможным. Авторы [?] изучают гауссовский SIMO-канал прослушивания (Single Input Multiple Output) и показывают, что он эквивалентен скалярному гауссовскому каналу, для которого применимы результаты работы [?].

Авторы [?] рассматривают независимые квазистатические каналы с затуханием для пользователей и противника. На базе проведенного анализа разработан практический протокол секретной связи, который для обеспечения беспроводной теоретико-информационной секретности применяет следующую процедуру: 1 — создание общей случайности (common randomness) посредством альтернативной передачи (opportunistic transmission), 2 — согласование сообщений (message reconciliation), 3 — генерация общего ключа посредством усиления приватности и 4 — защита сообщений с помощью секретного ключа. Введена процедура согласования сообщений, базирующаяся на многоуровневом кодировании и оптимизированных LDPC-кодах, которая позволяет достичь рейтов передачи, близких к фундаментальным пределам. Установлен набор метрик для оценки средних рейтов безопасной генерации ключей, и показано, что протокол эффективен в плане безопасного обновления ключей даже при наличии несовершенной информации о состоянии канала. В работе [?] исследуется широковещательный конфиденциальный канал с затуханиями, где узел источника имеет общую информацию для двух приемников и конфиденциальную информацию, предназначенную только для первого из них. Конфиденциальная информация для второго приемника должна оставаться настолько секретной, насколько это возможно. В дополнение к аддитивному гауссовскому шуму канал от источника к приемникам подвержен затуханию. Предполагается, что информация о состоянии канала известна как отправителю, так и получателям. Вначале изучается параллельный канал с независимыми подканалами, который служит теоретико-информационной моделью для широковещательного канала с затуханием. Установлены области емкости секретности для параллельного канала с деградирующими подканалами и параллельного гауссовского канала, выведены оптимальные точки распределения мощности, достигающие границ этой области. Полученные результаты применяются для исследования широковещательного канала с затуханием. Изучается эргодическая производительность, выводятся эргодическая область емкости секретности и оптимальные точки распределения мощности, в которых достигается граница этой области. Авторы [?] изучают эргодический канал с затуханием в присутствии противника. Предлагается простая стратегия включения-выключения мощности, достигающая характеристик, близких к оптимальным. Делается вывод о позитивном влиянии затухания в канале на емкость секретности. Показано, что адаптация рейтов, базирующаяся на данных о состоянии основного канала, является критичной при обеспечении секретной передачи по медленно затухающим каналам связи. Более общий подход предлагается в [?]. В этой работе рассматривается ситуация, когда и передатчик, и приемник имеют множественные антенны, а перехватчик — только одну, вследствие чего авторы назвали такой канал прослушивания 2-2-1 MIMO. Емкость секретности канала определяется с помощью предлагаемой схемы достижимости, для которой разработана плотная верхняя граница, удовлетворяющая предложенному достижимому рейту

секретности. Показано, что гауссовское сигналирование в форме лучеобразования оптимально и не требуется предварительной обработки информации.

В контексте множественного доступа отдельное внимание уделяется задаче передачи секретного сообщения в случае, когда отправитель и получатель используют n каналов, а противнику доступно только t каналов, причем $t < n$. По-видимому, первой в этом направлении является работа [?]. Авторы предлагают двухраундовую совершенную схему секретной передачи данных по n каналам и выводят нижнюю оценку скорости передачи, равную n. Затем авторы [?] вводят и изучают модель противника второго порядка (когда $n \geq 2t+1$) и модель третьего порядка ($n \geq 3t+1$). Показано, что модель третьего порядка необходима и достаточна для реализации однораундовой совершенной системы секретной передачи данных. Авторы [?] предлагают двухраундовую совершенную схему секретной передачи данных по n каналам со скоростью передачи $O(n)$. Однако вычислительная сложность их схемы оказывается экспоненциальной по n. Наконец, в одной из последних работ [?] предложена такая двухраундовая совершенная система секретной передачи данных для $n = 2t + 1$, что не только скорость передачи растет как $O(n)$, но и вычислительные затраты отправителя и получателя полиномиальны по n. Все указанные работы базируются на подходах, близких к кодам с коррекцией ошибок. Новизна подхода в последней работе состоит во введении в теорию кодирования понятия псевдобазиса.

1.4. Криптография в моделях с ограниченной памятью

Совершенно другой подход к построению секретных систем с доказуемой стойкостью развивается в серии работ, использующих идею общей случайности и ограничений по памяти. Здесь проблема стойкости криптографических протоколов рассматривается в перспективе будущих достижений в области вычислительных технологий и в исследованиях алгоритмов. Вычисления, которые в настоящее время кажутся невыполнимыми, в течение лет или десятилетий могут стать возможными благодаря улучшению оборудования и/или прорыву в алгоритмах взлома. В этом случае безопасность исторических, но тем не менее строго конфиденциальных данных может быть нарушена. Модель ограниченной памяти предполагает наличие противника, который не ограничен *временем* вычислений, а ограничен только объемом доступной *памяти* для запоминания результатов вычислений. Ограничение по памяти может быть произвольно большим (например, 100 Тбайт), но обязательно должно быть фиксированным. В одной из первых работ-предвестников этого направления [?] было дано общее исследование проблемы усиления приватности путем публичной дискуссии, ранее сформулированной для специального сценария. Усиление приватности — это процесс, который позволяет двум сторонам выделить секретный ключ из общей случайной переменной, о которой противник имеет частичную информацию. Две стороны обычно ничего не знают об информации противника за исключением того, что она удовлетворяет определенному ограничению. Результаты работы применимы к безусловно стойким протоколам установления ключей и к квантовой криптографии и служат усилению определения емкости секретности в каналах прослушивания и широковещательных каналах, создавая таким образом связь нового направления исследований с вышеизложенными работами. Доклад [?] стал основой для будущих исследований. В нем впервые были предложены криптосистема с секретным ключом и протокол установления ключа по открытому каналу связи, являющиеся безусловно стойкими при выполнении только одного условия: емкость памяти

противника должна быть ограниченна. При этом не делалось никаких предположений о вычислительной мощности противника. Сценарий предполагает, что строка случайных бит длины немного большей, чем емкость памяти противника, может быть принята всеми сторонами. Строка случайных бит может, например, широковещательно передаваться спутником либо через незащищенный канал связи между обменивающимися сторонами. Стойкость системы базируется на той идее, что противник не знает, какие части переданной общей случайности были использованы для построения ключей пользователей и в то же время не может запомнить *все* случайные биты, чтобы провести криптоанализ в будущем. Предлагаемая схема требует очень высокой пропускной способности каналов, что затрудняет ее практическое применение. Сформулированные идеи получили строгий теоретический анализ в [?].

В работе [?] представлена схема эффективной двусторонней связи с доказуемой бесконечно продолжительной секретностью. Секретность гарантируется при любых технологических достижениях с условием ее соблюдения при текущем состоянии техники. Более того, секретность сообщений гарантируется, если секретный ключ шифрования и расшифрования станет известен в будущем. Схема базируется на модели ограниченной памяти и обеспечивает теоретико-информационную секретность в рамках данной модели. При заданной границе объема памяти предлагаемые протоколы гарантируют, что даже вычислительно неограниченный противник не получает никакой информации о сообщении (кроме ее части с экспоненциально малой вероятностью). Граница на объем памяти противника должна существовать только на момент передачи сообщения. Поэтому никакая дополнительная память или вычисления в будущем ему не помогут. В работе представлено два протокола: первый, основанный на ауторегрессионном протоколе Ауманна и Рабина, использует короткий секретный ключ, размер которого не зависит от длины сообщения, но требует большого числа общедоступных случайных бит, второй использует оптимальное число общедоступных случайных бит, но требует значительно более длинного ключа.

1.5. Идеальные криптосистемы

Проведенный анализ показывает, что большинство современных исследований в области безусловно стойких криптосистем сосредоточено на представлениях, далеких от конечного пользователя, который не имеет непосредственного доступа к шумящим каналам, множеству антенн и т. д. Вместе с тем в работах [16, 44, 59] была показана возможность построения безусловно стойких криптосистем с близкой к линейной сложностью на стороне обычных пользователей. Основная идея предложенных систем состоит в применении специальных методов кодирования сообщений, обеспечивающих неотличимость кодовой последовательности, или хотя бы ее части, от последовательности равновероятных и независимых бит. Было показано, как можно построить коды с явно отделимой “случайной” компонентой для источников с неизвестной статистикой. Секретный ключ прилагается только к этой случайной компоненте. В результате прямой перебор ключей приводит к получению множества равновероятных решений криптограммы и получается идеальная или даже строго идеальная система Шеннона. Предложенные алгоритмы достаточно быстры для их практического применения. Так, строго идеальный шифр, основанный на нумерации, требует $O(n)$ бит памяти и $O(n \log^3 n \log\log n)$ битовых операций, где n — размер блока. Идеальный шифр, построенный на базе омофонного кода, требует $O(n)$ бит памяти и $O(n \log^2 n)$ битовых операций. Более того,

если значение $\log n$ умещается в машинном слове, что и происходит на практике, то трудоемкость составляет $O(n)$ машинных операций (включая умножение и деление чисел одинарной точности). Приведенные оценки свидетельствуют о достаточно высоких скоростных свойствах методов. Однако рассмотрение в основном касалось источников без памяти, что пока ограничивает область применения этих методов.

2. Теоретико-информационные подходы в стеганографии

2.1. Теоретико-информационные модели стегосистем

Впервые теоретико-информационная модель стеганографии была представлена в [?]. Понятие стойкости стегосистемы формализовано на основе относительной энтропии, показывающей, что распределение пустых и заполненных контейнеров почти одно и то же. Была предложена конструкция, удовлетворяющая этому понятию стойкости. В основе конструкции лежит энтропийное кодирование, реализуемое с помощью арифметического кодера. Стойкость системы достигается только асимптотически, так как арифметический код имеет небольшую избыточность. Следующий шаг в теоретической формализации задачи сделан в работе [?]. Здесь введено понятие емкости встраивания (embedding capacity) и показана связь между тремя величинами: достижимые рейты встраивания информации и разрешенные уровни искажений для пользователя (скрывающего информацию) и его противника (того, кто пытается выявить наличие скрытой информации). Предпринят теоретико-игровой подход к решению задачи оптимального согласования этих трех величин. Емкость встраивания рассматривается как цена игры между лицом, скрывающим информацию, и его противником. Оптимальная стратегия атаки представляет собой решение определенной задачи искажающего кодирования, оптимальная стратегия внедрения — решение задачи кодирования для канала. Таким образом, было продемонстрировано внутреннее единство стеганографии и стегоанализа. Показано также, что многие существующие системы скрытия данных работают намного ниже емкости встраивания. Кашен в [?] предложил интерпретацию задачи криптоанализа как задачу проверки гипотез. Относительная энтропия между распределениями пустого и заполненного контейнера определяет границы способности выявления наличия скрытой информации у противника. Предложена универсальная стегосистема, не нуждающаяся в знании распределений вероятностей символов покрывающего текста (контейнера). Авторы [?] проанализировали различные метрики безопасности для стеганографических систем, а именно, стойкость, или обнаружимость (detectability), устойчивость (robustness) и секретность, или трудность, извлечения. Они предложили новую метрику безопасности, использующую вместо относительной энтропии вариационное расстояние. Эта метрика может служить верхней границей выигрыша пассивного противника.

В работе [?] изучаются ограничения стеганографии в ситуациях, когда отправитель не использует никаких свойств канала, кроме его энтропии и возможности делать выборки. В негативном плане показано, что число выборок, которые отправитель должен сделать, экспоненциально по рейту стегосистемы. В позитивном плане представлена первая стегосистема с секретным ключом, соответствующая этой нижней границе независимо от энтропии канала. Более того, для высокоэнтропийных каналов представлена первая стегосистема с секретным ключом, удовлетворяющая этой нижней границе даже без синхронизированного состояния между отправителем и получателем.

Теоретико-информационная модель стеганографии в присутствии активных противников, расширяющая подходы предыдущих работ, рассмотрена в [?]. Здесь изучаются стегосистемы, безусловно стойкие по отношению к атакам по незащищенному каналу, в котором противник может читать и писать сообщения. Показана общая конструкция стегосистем, стойких по отношению к активным атакам, базирующаяся на аутентичном шифровании.

Первая просто реализуемая конструкция совершенной стегосистемы была представлена в [?]. Эта конструкция базируется на нумерации множества равновероятных последовательностей. Сообщение источника разбивается на блоки некоторой фиксированной длины. Обозначим один такой блок через u и рассмотрим множество S_u равновероятных последовательностей, одним из элементов которого является u. Например, если $u = bac$ и известно, что буквы независимы и одинаково распределены, то $S_u = \{abc, acb, bac, bca, cab, cba\}$. Основная идея здесь состоит в использовании битов зашифрованного сообщения в качестве номера, по которому из S_u выбирается последовательность v, которая затем записывается в контейнер вместо u. Так как последовательности v и u равновероятны, то статистическая структура контейнера не изменяется, что дает в результате совершенную стегосистему.

Другой подход к построению идеальных стегосистем основан на использовании непосредственного вероятностного описания (обычно в виде условных вероятностей) последовательности элементов контейнера. Данный подход может применяться в случаях, когда трудно построить множество равновероятных последовательностей и провести его нумерацию. Идея заключается в кодировании зашифрованного сообщения кодом, в котором алфавит и вероятности появления кодовых символов полностью соответствуют алфавиту и вероятностям символов последовательности x контейнера. Для решения этой задачи могут быть применены так называемые коды со стоимостью (например, арифметическое декодирование), но они не позволяют получить точно требуемой вероятности появления кодовых символов. В [?] предложены коды, которые за счет рандомизации обеспечивают точно заданное распределение кодовых символов. Закодированное таким кодом сообщение просто записывается в контейнер на место последовательности x. Оба эти подхода получили дальнейшее развитие в работах [?, ?].

2.2. Практические стегосистемы

Теоретические исследования в области стеганографии мотивировали создание нового поколения практических систем, значительно более надежных, чем их предшественники. В работе [?] представлен метод цифровой стеганографии, названный Spread Spectrum Image Steganograpy (SSIS — стеганография в изображениях с расширением спектра). Внедряемое сообщение шифруется ключом K_1 и кодируется посредством низкорейтового кода с коррекцией ошибок, образуя закодированное сообщение. Отправитель сообщения использует ключ K_2, задающий работу псевдослучайного генератора шума, и генерирует шумовую последовательность с заданными распределением (например, гауссовским) и уровнем сигнала. Затем используется схема модуляции, объединяющая закодированное сообщение и шумовую последовательность и производящая таким образом композитный сигнал, который пропускается через устройство перемежения и складывается с исходным изображением, производя стегоизображение. Законный получатель знает оба использованных ключа и, производя действия в обратном порядке и декодируя код с исправлением ошибок, восстанавливает сообщение. Стойкость алгоритма к

стегоанализу обусловлена тем фактом, что наложенный стегосигнал, модулированный шумом, трудно отличить от естественного шума в изображении.

Авторы [?] изучают стеганографию с точки зрения теории сложности вычислений. В частности, они доказывают, что существование односторонних функций делает возможным существование вычислительно стойких стеганографических протоколов. В [?] введено понятие адаптивной стойкости по выбранному стеготексту и разработаны эффективные схемы стеганографии с открытыми ключами, стойкие против адаптивных атак по выбранному стеготексту. В [?] разработан стеганографический протокол с открытыми ключами, позволяющий двум сторонам, которые никогда не встречались и не обменивались секретными ключами, посылать скрытые сообщения по открытому каналу таким образом, что противник не может определить, что эти скрытые сообщения посылались. Такая стеганография невозможна с теоретико-информационной точки зрения.

Идеи универсального кодирования использованы в United States Patent 7,239,717 (Fridrich, Goljan, 2005). Основная идея состоит в следующем. Изображение X содержит набор пикселей (численных значений x). Для каждого значения x определяется множество $S(x)$ как подмножество пикселей X, значения которых равны x. Допустим, что можно идентифицировать два значения x и y, близких друг к другу (т. е. модуль разности $|x - y|$ мал), но соответствующие им подмножества $S(x)$ и $S(y)$ существенно различаются в размерах. Следующий шаг состоит в неискажающем сжатии битового потока Z, составленного из элементов $S(x)$ и $S(y)$, где x рассматривается как "0", а y — как "1" и изображение X сканируется в заранее определенной последовательности. После получения сжатой последовательности Z к ней присоединяется внедряемое секретное сообщение и результат внедряется в объединение подмножеств $S(x)$ и $S(y)$ при сканировании изображения X в том же порядке и замене "0" на x и "1" на y. Такое внедрение не слишком искажает X, так как разница между значениями x и y мала. В то же время, поскольку подмножества $S(x)$ и $S(y)$ различны по размеру, последовательность Z будет сжимаемой, что позволит добавить к ней встраиваемые данные.

Другим примером использования идей универсального кодирования и кодов со стоимостью является работа [?], где предложено применять вероятностные модели, аналогичные моделям универсального кодирования, для решения задач стеганографии. В этом случае внедряемое сообщение перекодируется таким образом, чтобы кодовые символы подчинялись тем же оценочным распределениям вероятностей, что и заменяемые ими символы в контейнере. В качестве кода со стоимостью используется арифметическое декодирование. В результате построен алгоритм внедрения информации в растровые изображения, учитывающий статистику младших бит цветовых составляющих в некотором окружающем контексте. Экспериментальные исследования алгоритма показали его заметное преимущество в стойкости по отношению к известным аналогам HIDE4PGP и STEGOTOOLS: увеличение стойкости на 15–40 % на случайной выборке файлов и на 95 % на "удобных" файлах (с плавными переходами цветов).

2.3. Теоретико-информационные модели водяных знаков

Цифровые водяные знаки (digital watermarks) представляют собой особый вид встраиваемых сообщений. Они не только должны минимально искажать структуру контейнера, но и быть устойчивыми к их удалению или искажению. Внедрение водяных знаков является моделью механизма защиты авторских прав, когда оригинальный документ,

или "покрывающий текст", перед публикацией модифицируется, чтобы встроить некоторую дополнительную информацию. Внедрение должно быть прозрачным (т. е. модифицированный документ, или "стеготекст", должен быть подобен исходному тексту) и устойчивым (т. е. внедренная информация должна быть восстановима, если стеготекст дополнительно модифицируется).

В одной из первых работ [?] представлены алгоритм внедрения водяного знака в изображение и методология внедрения цифровых водяных знаков, которая может быть обобщена на данные аудио, видео и мультимедиа. Водяной знак конструируется как независимый и одинаково распределенный случайный гауссовский вектор. Затем он вставляется в наиболее значимые спектральные компоненты данных. Внедрение водяного знака в таком режиме делает его устойчивым к операциям обработки (сжатие с потерями, фильтрация, цифро-аналоговое и аналого-цифровое преобразование, реквантование и т. д.) и к стандартным геометрическим преобразованиям (обрезание, масштабирование, перенос и поворот). При условии, что детектор имеет в своем распоряжении оригинал изображения, во всех перечисленных выше случаях он недвусмысленно идентифицирует владельца. В [?] представлена теоретическая модель стеганографии цифровых водяных знаков. Выведены общие нижние границы взаимной информации, определяющие стойкость системы. Рассмотрена совершенная стеганография, представлены новые схемы, достигающие совершенной секретности и устойчивые против некоторых атак. Наконец, оценивается устойчивость некоторых простых схем и выводятся критерии стойкого внедрения информации.

В работе [?] коды, вставляющие водяной знак, анализируются с теоретико-информационной точки зрения как игра между скрывающим информацию и активным противником. Скрывающий информацию внедряет секретное сообщение (водяной знак) в контейнер (обычно текст, изображение, звук или видео) в пределах некоторого уровня искажения, а противник обрабатывает результирующее сообщение с водяным знаком в пределах некоторого дополнительного искажения с целью разрушить водяной знак. Для случая, когда текст порождается источником без памяти, дается однобуквенная характеристика максиминной игры с экспонентой ошибки случайного кодирования, ассоциированного со средней вероятностью ошибочного декодирования водяного знака. Эта однобуквенная характеристика дает нужный эффект, так как если скрывающий информацию для генерации случайных кодовых слов для каждого сообщения-контейнера использует канал без памяти, то противник максимизирует вред, точно так же реализуя канал без памяти. В [33], кроме того, представлены частичные результаты для дуальной минимаксной игры и условия существования седловой точки.

Авторы [?] рассматривают задачу внедрения одного сигнала (например, цифрового водяного знака) в другой сигнал-носитель, чтобы сформировать третий, композитный сигнал. Способ внедрения разрабатывается таким образом, чтобы достичь эффективного сочетания между тремя конфликтующими целями: максимизации рейта внедрения, минимизации уровня искажения и максимизации устойчивости внедренной информации. Вводится новый класс методов внедрения — модуляция индекса квантования (МИК) и МИК с компенсированным искажением (МИК-КИ). Разрабатываются удобные реализации в форме так называемой модуляции дизеринга. При использовании детерминированных моделей для оценки методов цифровых водяных знаков показано, что МИК "доказуемо хороша" против произвольно ограниченных и полностью информированных атак, которые возникают в нескольких приложениях защиты авторских прав, и особенно достигает доказуемо лучших соотношений рейта, искажения и устой-

чивости по сравнению с популярными методами модуляции спектра и младших бит. Более того, показано, что для некоторых важных вероятностных моделей МИК-КИ оптимальна, а обычная МИК — почти оптимальна. Эти модели включают в себя каналы с аддитивным белым гауссовским шумом, являющиеся хорошими моделями для приложений с гибридной передачей данных, например, цифрового аудио. Сюда также включаются каналы ограниченных по среднеквадратичной ошибке атак, которые моделируют приложения с водяными знаками с открытыми ключами.

В работе [?] вычисляется кодовая емкость для гауссовского текста и искажений с квадратичными ошибками. Изучаются публичная версия игры (исходный текст не известен ни противнику, ни декодеру) и приватная версия (исходный текст не известен противнику, но известен декодеру). Хотя емкость внедрения во втором типе игры не может превышать емкости в первом, показано, что они фактически идентичны. Эти емкости существенно зависят от того, должны ли ограничения по степени искажения выполняться в среднем или с вероятностью 1. В первом случае кодовая емкость равна нулю, в то время как во втором случае она совпадает со значением соответствующих игр с нулевой суммой о динамической взаимной информации между полнотой и совершенством информации. Кроме того вычисляется емкость, когда противник ограничен только аддитивными атаками. Эта емкость оказывается строго большей емкости водяного знака, демонстрируя таким образом, что аддитивные атаки субоптимальны.

Авторы [?] изучают *биннинг* как фундаментальный подход к слепому встраиванию данных и к водяным знакам. Однако возможны различные стратегии атак, которые снижают эффективность практических схем биннинга. Задача, которая анализируется в этой статье, состоит в разработке наихудших шумовых распределений против кодов водяных знаков, основанных на модуляции индекса квантования L-мерной решетки. Рассматриваются две функции стоимости: 1 — вероятность ошибки декодера максимального правдоподобия и 2 — граница Бхаттачарьи для вероятности ошибки, которая является плотной при низких рейтах встраивания. Обе задачи рассматриваются при следующих ограничениях на стратегию атаки: шум не зависит от помеченного сигнала, шумовые блоки длины L независимы, шум не превышает заданного квадратичного уровня искажений. Квадратичное искажение для встраивания также ограниченно. Предлагаются три стратегии встраивания: оптимизация параметра раздувания решетки, дизеринг и рандомизированное вращение решетки. В этом анализе критичны свойства симметрии вложенных решеток МИК и свойства конвективности вероятности ошибки и связанных с ними функционалов шумового распределения. Определяются оптимальные минимаксные стратегии встраивания и атаки, а также явные и числовые решения для наихудшего случая шума. Исследована роль памяти атакующего, в частности, продемонстрирована высокая эффективность атак с помощью импульсного шума по мере увеличения L. Оценивается емкость МИК решетки в худшем случае.

Список литературы

[1] Agarwal S., Cramer R., Haan R. Asymptotically optimal two-round perfectly secure message transmission // CRYPTO-06. 2006. P. 394–408.

[2] Ahn L., Hopper N.J. Public-key steganography // Advances in Cryptology. EUROCRYPT-2004 (Lecture Notes in Computer Science). Berlin: Springer-Verlag, 2004. Vol. 3027. P. 323–341.

[3] Aumann Y., Ding Y.Z., Rabin M.O. Everlasting security in the bounded storage model // IEEE Trans. on Inform. Theory. 2002. Vol. 48. P. 1668–1676.

[4] Bennett C.H., Brassard G., Crepeau C., Maurer U. Generalized privacy amplification // Ibid. 1995. Vol. 41. P. 1915–1923.

[5] Bloch M., Barros J., Rodrigues M., McLaughlin S. Wireless information-theoretic security // Ibid. 2008. Vol. 54, No. 6. P. 2515–2534.

[6] Cachin C., Maurer U. Unconditional security against memory bounded adversaries // Advances in Cryptology — CRYPTO-97. 1997. P. 292–306.

[7] Cachin C. An information-theoretic model for steganography // 2nd Intern. Workshop on Information Hiding IH-98 (Lecture Notes in Compute Science). Berlin: Springer-Verlag, 1998. Vol. 1525. P. 306–318.

[8] Cachin C. An information-theoretic model for steganography // Inform. and Comput. 2004. Vol. 192, No. 1. P. 41–56.

[9] Chen B., Wornell G.W. Quantization index modulation methods: A class of provably good methods for digital watermarking and information embedding // IEEE Trans. Inform. Theory. 2001. Vol. 47, No. 5. P. 1423–1443.

[10] Cohen A.S., Lapidoth A. The Gaussian watermarking game // Ibid. (Special Issue on Shannon Theory). 2002. Vol. 48, No. 6. P. 1639–1667.

[11] Costa M.H.M. Writing on dirty paper // IEEE Trans. on Inform. Theory. 1983. Vol. 29, No. 3. P. 439–441.

[12] Cox I.J., Killian J., Leighton F.T., Shamoon T. Secure spread spectrum watermarking for multimedia // IEEE Trans. Image Proc. 1997. Vol. 6. P. 1673–1687.

[13] Csiszár I., Narayan P. Secrecy capacities for multiple terminals // IEEE Trans. Inform. Theory. 2004. Vol. 50, No. 12. P. 3047–3061.

[14] Dedic N., Itkis G., Reyzin L., Russell S. Upper and lower bounds on black box steganography // 2nd Theory of Cryptography Conf. Berlin, Germany: Springer-Verlag, 2005. P. 227–244.

[15] Desmedt Y., Wang Y., Burmester M. A complete characterization of tolerable adversary structures for secure point-to-point transmissions without feedback // ISAAC-05. 2005. P. 277–287.

[16] Fionov A. Universal homophonic coding // IEEE Intern. Symp. on Information Theory. Washington, DC, 2001. P. 116.

[17] Fionov A., Ryabko B. Simple ideal steganographic system for containers with known statistics // XI Intern. Symp. on Problems of Redundancy in Information and Control Systems. St.-Peterburg, 2007. P. 184–188.

[18] Gopala P.K., Lai L., Gamal H. On the secrecy capacity of fading channels // IEEE Trans. on Inform. Theory. 2008. Vol. 54, No. 10. P. 4687–4698.

[19] Hayashi M. General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel // Ibid. 2006. Vol. 52, No. 4. P. 1562–1575.

[20] Hayashi Y., Yamamoto H. Coding theorems for the Shannon cipher system with a guessing wiretapper and correlated source outputs // Ibid. 2008. Vol. 54, No. 6. P. 2808–2817.

[21] Hellman M.E. An extension of the Shannon theory approach to cryptography // Ibid. 1977. Vol. 23. P. 289–294.

[22] Hero A. O. Secure space-time communication // Ibid. 2003. Vol. 49, No. 12. P. 3235–3249.

[23] Hopper N., Langford J., von Ahn L. Provably secure steganography // Advances in Cryptology. CRYPTO-2002. Berlin, Germany: Springer-Verlag, 2002. Vol. 2442. P 18–22.

[24] Johnson M., Ishwar P., Prabhakan V. et al. On compressing encrypted data // IEEE Trans. on Signal Proc. 2004. Vol. 52, No. 10. P. 2992–3006.

[25] Khisti A., Wornell G., Wiesel A., Eldar Y. On the Gaussian MIMO wiretap channel // IEEE Intern. Symp. on Inform. Theory. Nice, France, 2007. P. 2471–2475.

[26] Kurosawa K., Suzuki K. Truly efficient 2-round perfectly secure message transmission scheme // IEEE Trans. on Inform. Theory. 2009. Vol. 55, No. 10. P. 5223–5232.

[27] Le T.V., Kurosawa K. Efficient public key steganography secure against adaptively chosen stegotext attacks // Tech. Rep. 2003/244. Cryptology ePrint Archive, IACR.

[28] Leung-Yan-Cheong S.K., Hellman M.E. The Gaussian wire-tap channel // IEEE Trans. on Inform. Theory. 1978. Vol. 24, No. 4. P. 451–456.

[29] Liang Y., Poor H.V., Shamai S. (Shitz) Secure communication over fading channels // Ibid. 2008. Vol. 54, No. 6. P. 2470–2492.

[30] Marvel L., Boncelet C.G. Jr., Retter C.T. Spread-spectrum image steganography // IEEE Trans. on Image Proc. 1999. Vol. 8. P. 1075–1083.

[31] Maurer U.M. Conditionally-perfect-secrecy and a provably-secure randomized cipher // J. Cryptol. 1992. Vol. 5. P. 53–66.

[32] Maurer U., Wolf S. Information-theoretic key agreement: From weak to strong secrecy for free // Advances in Cryptology — EUROCRYPT-2000. P. 351–368.

[33] Merhav N. On random coding error exponents of watermarking codes // IEEE Trans. on Inform Theory. 2000. Vol. 46, No. 3. P. 420–430.

[34] Merhav N. A large-deviations notion of perfect secrecy // Ibid. 2003. Vol. 49, No. 2. P. 506–508.

[35] Merhav N. On the Shannon cipher system with a capacity-limited key-distribution channel // Ibid. 2006. Vol. 52, No. 3. P. 1269–1273.

[36] Merhav N. On joint coding for watermarking and encryption // Ibid. 2006. Vol. 52, No. 1. P. 190–205.

[37] Merhav N. Shannon's secrecy system with informed receivers and its application to systematic coding for wiretappered channels // Ibid. 2008. Vol. 54, No. 6. P. 2723–2734.

[38] Mittelholzer T. An information-theoretic approach to steganography and watermarking // 3nd Intern. Workshop on Information Hiding (IH-99). Berlin: Springer-Verlag, 2000. Vol. 1768. P. 1–16.

[39] Moulin P., O'Sullivan J. Information-theoretic analysis of information hiding // IEEE Trans. on Inform. Theory. 2003. Vol. 49, No. 3. P. 563–593.

[40] Moulin P., Goteti A.K. Block QIM watermarking games // IEEE Trans. on Inform. Forensics and Security. 2006. Vol. 1, No. 3. P. 293–310.

[41] Negi R., Goel S. Secret communication using artificial noise // IEEE Vehicular Technology Conf. Toulouse, France, 2006.

[42] Ozarow L.H., Wyner A.D. Wire-tap channel II // EUROCRYPT-84. Workshop on Advances in Cryptology: Theory and Applications of Cryptographic Techniques. Paris, France, 1985. P. 33–51.

[43] Parada P., Blahut R. Secrecy capacity of SIMO and slow fading channels // IEEE Intern. Symp. Inform. Theory. Adelaide, Australia, 2005. P. 2152–2155.

[44] Ryabko B., Fionov A. Efficient homophonic coding // IEEE Trans. Inform. Theory. 1999. Vol. 45, No. 6. P. 2083–2091.

[45] Ryabko B., Ryabko D. Information-theoretic approach to steganographic systems // IEEE Intern. Symp. on Information Theory. Nice, France, 2007. P. 2461–2464.

[46] Shafiee S., Liu N., Ulukus S. Towards the secrecy of the Gaussian MIMO wire-tap channel: The 2-2-1 channel // IEEE Trans. on Inform. Theory. 2009. Vol. 55, No. 9. P. 4033–4039.

[47] Shannon C.E. Communication theory of secrecy systems // Bell Syst. Tech. J. 1949. Vol. 28, No. 3. P. 565–715.

[48] Shikata J., Matsumoto T. Unconditionally secure steganography against active attacks // IEEE Trans. Inform. Theory. 2008. Vol. 54, No. 6. P. 2690–2705.

[49] Srinathan K., Narayanan A., Rangan C. P. Optimal perfectly secure message transmission // CRYPTO-04. 2004. P. 545–561.

[50] Tekin E., Yener A. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming // IEEE Trans. Inform. Theory. 2008. Vol. 54, No. 6. P. 2735–2751.

[51] Thangaraj A., Dihidar S., Calderbank A. R. et al. Applications of LDPC codes to the wiretap channel // Ibid. 2007. Vol. 53. P. 2933–2945.

[52] Wang Y., Moulin P. Steganalysis of block-structured stegotext // SPIE. 2004. Vol. 5306: Security, Steganography, and Watermarking of Multimedia Contents VI. P. 477–488.

[53] Wyner A.D. The wire-tap channel // Bell Syst. Tech. J. 1975. Vol. 54, No. 8. P. 1355–1387.

[54] Yamamoto H. Coding theorem for secret sharing communication systems with two noisy channels // IEEE Trans. on Inform. Theory. 1989. Vol. 35, No. 3. P. 572–578.

[55] Yamamoto H. Coding theorem for secret sharing communication systems with two Gaussian wiretap channels // Ibid. 1991. Vol. 37, No. 3. P. 634–638.

[56] Yamamoto H. Rate–distortion theory for the Shannon cipher system // Ibid. 1997. Vol. 43, No. 3. P. 827–835.

[57] Zhang W., Li S. Security measurements of steganographic systems // ACNS 2004 (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2004. Vol. 3089. P. 194–204.

[58] Елтышева Е.Ю., Фионов А.Н. Построение стегосистемы на базе растровых изображений с учетом статистики младших бит // Вестник СибГУТИ. 2009. № 1. С. 67–84.

[59] Рябко Б.Я. Просто реализуемая идеальная криптографическая система // Проблемы передачи информации. 2000. Т. 36, № 1. С. 90–104.

[60] Рябко Б.Я., Фионов А.Н. Алгоритмы кодирования для идеальных стеганографических систем // Вестник НГУ. Информ. технологии. 2008. № 2. С. 88–93.

[61] Рябко Б.Я., Фионов А.Н. Идеальные стеганографические системы // Докл. ТУСУРа. 2008. № 2, ч. 1. С. 61–62.

Поступила в редакцию 26 января 2010 г.