Система классификации методов распределения ключей

System of Key Distribution Methods Classification

Синюк / Sinyuk A.
Александр Демьянович
(eentrop@rambler.ru)
доктор технических наук, доцент.
ФГКВОУ ВО «Военная академия связи имени Маршала Советского Союза С. М. Буденного» (ВАС им. С. М. Буденного) МО РФ,
доцент.
г. Санкт-Петербург

Остроумов / Ostroumov O.
Олег Александрович
(oleg-26stav@mail.ru)
ВАС им. С. М. Буденного,
адъюнкт.
г. Санкт-Петербург

Ключевые слова: криптографическая система защиты информации – cryptographic information protection system; ключ – key; классификация – classification; корреспондент связи – communication correspondent; канал связи – communication channel; защищенный канал связи – secure communication channel; открытый канал связи – open communication channel; метод распределения ключей – key distribution method; нарушитель – offender; канал перехвата – interception channel; протокол формирования ключа – key generation protocol.

Показатель эффективности криптографических систем защиты информации определяется их стойкостью в соответствии с принципом Керкхоффа, когда нарушителю из описания криптосистемы не известен только ключ. Криптосистема включает подсистему управления ключами, обеспечивающую генерацию, распределение, использование, замену ключей и другие функции.
Предлагается система классификации известных методов распределения ключей, обеспечивающих выполнение одной из основных функций жизненного цикла ключей.

Performance indicator of cryptographic information protection systems is determined by their resistance in accordance with the principle of Kerckhoff when only the key is unknown to the offender from the cryptosystem description. A cryptosystem includes key management subsystem, providing generation, distribution, use and replacement of keys and other functions. A system for classification of known key distribution methods, ensuring performance of one of the keys' lifecycle main functions, is proposed.

Введение

В современных телекоммуникационных сетях и информационных системах криптографические методы защиты информации считаются наиболее эффективными, а зачастую и единственно возможными среди известных методов защиты информации. Принципиальным моментом является использование криптографического ключа, под которым понимается некоторая секретная информация, известная законному собственнику информации и неизвестная нарушителю.

Основная часть

Основным вопросом синтеза и анализа криптографической системы защиты информации является оценка ее стойкости, определяющей ее способность противостоять атакам нарушителя на защищаемую информацию с использованием принципа Керкхоффа, в соответствии с которым стойкость криптосистемы должна быть обеспечена при условии, когда нарушителю известно полное описание криптосистемы и не известен только криптографический ключ [1].

Порядок использования криптографической системы определяется реализацией систем установки и управления ключами, которые выполняют задачи генерации, распределения (и передачи), проверки ключей и определяют порядок использования, смены, хранения и архивирования, резервного копирования, восстановления, замены, уничтожения старых, изъятия из обращения скомпрометированных ключей, соответственно [2, 3].

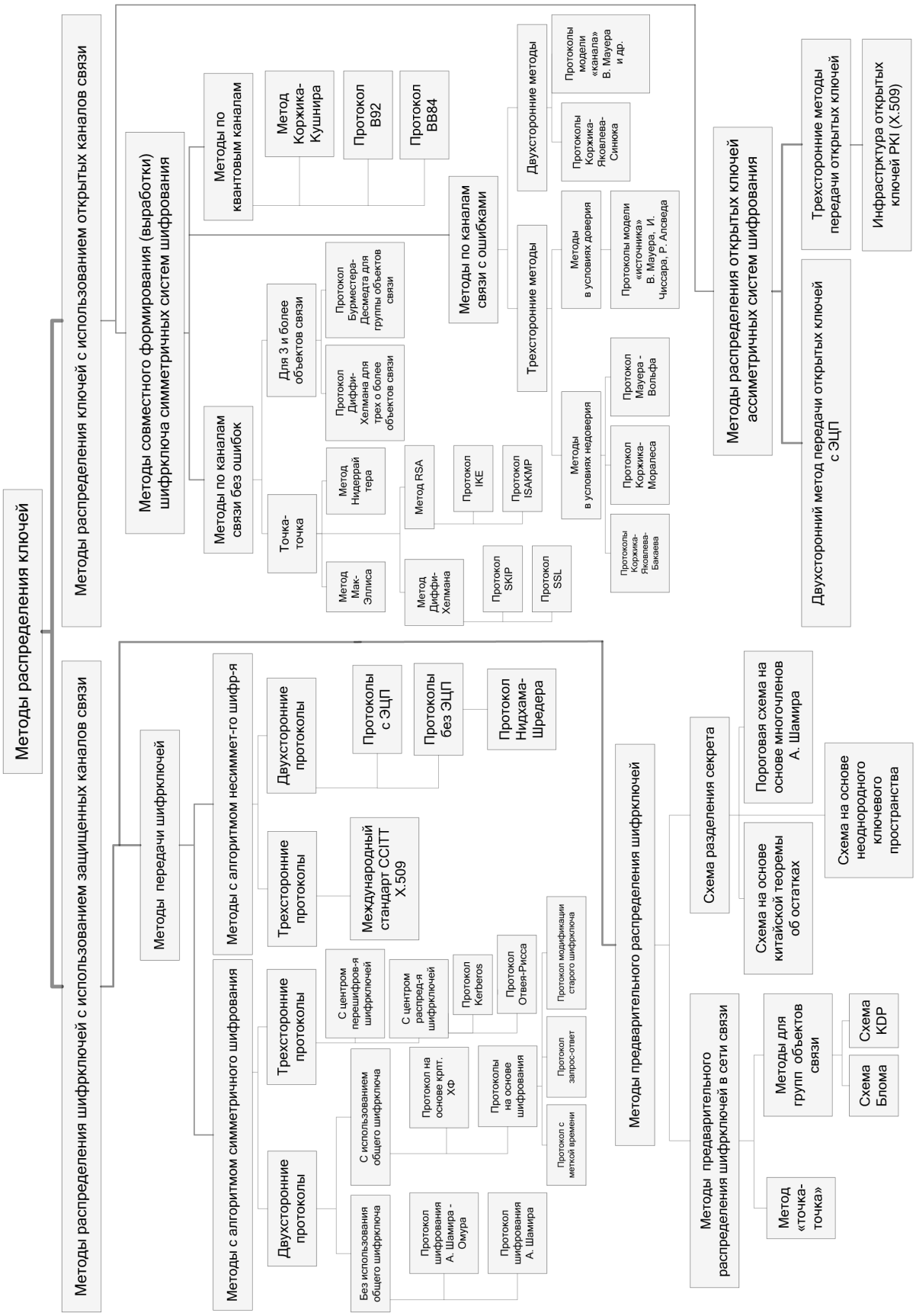

Рис. 1. Система классификации методов распределения ключей

Построим систему классификации известных методов распределения ключей в соответствии с основными классификационными признаками. Предлагаемая система классификации показана на рисунке.

Методы распределения ключей по виду используемого канала связи можно классифицировать на 2 больших класса: методы с использованием защищенных каналов связи и методы с использованием открытых каналов связи.

Охарактеризуем первый класс. Известно, что проблема распределения ключей по защищенным каналам является фундаментальной [1, 3, 4, 5]. При ее решении одновременно решаются задачи обеспечения секретности и аутентификации распределяемых ключей. Самый надежный способ первоначального распределения ключей – личная встреча взаимодействующих сторон (корреспондентов). Можно использовать специальных курьеров, которые будут развозить ключи. В этом случае дополнительно решается задача аутентификации ключей на основе доверия корреспондентов друг другу или опечатанному пакету, доставленного курьером.

Методы первого класса по способу формирования ключа подразделяются на два подкласса методов: предварительного распределения ключей и передачи ключей. Рассмотрим первый подкласс. Для двух взаимодействующих сторон и при большом их числе требуется предварительная рассылка по защищенному каналу(ам) значительного объема ключевой информации и последующее ее хранение [1, 3]. Поэтому применяют методы предварительного распределения ключей, предусматривающие распределение и хранение не самих ключей, а некоторой меньшей по объему исходной информации, на основе которой каждая сторона может вычислить ключ для взаимодействия с другой стороной. Последние включают две группы методов для сетей связи и системы разделения секрета.

Система предварительного распределения ключей реализует алгоритмы: генерации исходной информации (общая открытая и секретная части каждой стороны); вычисления ключа для абонентов по исходной информации.

Необходимо определиться с терминами «система распределения ключей» и «протокол распределения ключей». Первый определяет структурную организацию системы установки ключей [2]. Второй термин определяет совокупность действий, выполняемых в заданной последовательности двумя или более субъектами (корреспондентами) с целью формирования общих секретных ключей. Корректность выполнения протокола зависит от действий каждого субъекта криптосистемы. Субъекты действуют по предписанным алгоритмам [2].

Для двухсторонних задач известен метод «точка-точка» при непосредственном взаимодействии [3]. В качестве примера системы предварительного распределения ключей для групп корреспондентов связи можно привести систему Блома [6]. Кроме этого, известна система KDP (key distribution patterns), которая основана на системе пересечений множеств [7].

Для многих практически важных приложений, связанных с запуском критических процессов или определяющих порядок получения доступа к значимым данным, ответственное лицо должно ввести секретный ключ. Чтобы обезопасить процедуру принятия решения и не отдавать все на волю одного человека, являющегося обладателем ключа, используют метод разделения секрета [3]. Он состоит в назначении определенной группы лиц, которая имеет право принимать решение. Каждый член группы владеет определенной долей секрета (специально выбранным набором данных), полная совокупность которых позволяет восстановить секретный ключ. При этом для восстановления секретного ключа требуется обязательное присутствие всех членов группы. Примером системы разделения секрета выступает пороговая система Шамира [8]. Дополнительно известны системы на основе китайской теоремы об остатках и на основе неоднородного ключевого пространства [2].

Рассмотрим другой подкласс методов распределения ключей с использованием защищенных каналов связи – методы передачи ключей, которые по типу используемого алгоритма шифрования подразделяются на группы методов с использованием симметричного и ассимметричного шифрования. К первой группе методов относятся протоколы, в которых стороны осуществляют передачу ключей при непосредственном взаимодействии, и в протоколах которых предусмотрена третья сторона, играющая роль доверенного центра [3].

Различают двусторонние протоколы, в которых стороны заранее располагают какой-либо известной им обоим секретной информацией, и протоколы, не требующие выполнения этого условия. В рамках первой подгруппы протоколов с общим ключом должна решаться задача обеспечения подлинности сеанса связи, включающая подтверждение подлинности субъектов сеанса связи [2]. Проверку подлинности сеанса связи можно осуществить, используя механизмы запроса-ответа и отметки времени [3]. Протокол распределения ключей должен обеспечить выполнение требований: взаимную аутентификацию субъектов сеанса связи; подтверждение целостности сеанса связи; минимальное число сообщений, необходимых для обмена ключами.

В некоторых системах используется механизм модификации ключа, когда новый сеансовый ключ формируется из предыдущего значения ключа с помощью некоторой заранее оговоренной односторонней функции преобразования блоков данных. Известны методы, использующие стойкую однонаправленную хеш-функцию для формирования нового ключа.

В протоколах с общей секретной информацией вместо шифрования возможно использование криптографической хэш-функции [3].

Известны протоколы, в которых стороны заранее не располагают какой-либо известной им секретной информацией. Примером служит «бесключевой» протокол А. Шамира [2]. Независимо друг от друга А. Шамир и Дж. Омура описали алгоритм шифрования, позволяющий передать ключ без использования какой-либо общей секретной информации [3].

Методы с использованием симметричного шифрования имеют другую ветвь классификации – протоколы передачи ключей при централизованном распределении ключей с доверенным центром. Для выполнения трехсторонних протоколов [3] создаются доверенные центры, выполняющие функции центров распределения или перешифрования ключей. Различие между ними заключается в том, что в первом случае генерация ключей осуществляется в центре распределения, а во втором случае – самими абонентами. Один из первых протоколов такого типа был предложен в работе [9, 10]. Слабость протокола заключается в возможности повторной передачи абоненту В сообщения, когда последний не имеет возможности установить были ли полученный ключ использован. В случае компрометации этого ключа нарушитель может аутентифицироваться и передавать сообщения от имени А. Недостаток этого протокола устранен в известном протоколе Kerberos [1, 5, 10, 11]. К этой подгруппе относится протокол распределения ключей с использованием сервера Отвея-Рисса, описанный в [12].

Способы передачи ключей с использованием асимметричного шифрования образуют другую группу методов передачи ключей. К ней относятся двухсторонние протоколы без использования электронной цифровой подписи (ЭЦП), например протокол Нидхэма-Шредера [9]. Аутентифицированный протокол передачи ключей с использованием цифровой подписи содержит одно сообщение [3]. В трехстороннем протоколе по международному стандарту CCITT X.509 [3] передача ключей производится с использованием сертификатов открытых ключей. Сертификат представляет собой набор данных, состоящий из идентификатора абонента, его открытого ключа и дополнительной информации, например времени выдачи сертификата и срока его действия, заверенных цифровой подписью доверенного центра или заслуживающего доверия лица. Он предназначен для исключения возможности подмены открытого ключа при его хранении или пересылке. Получив сертификат и проверив цифровую подпись, можно убедиться в том, что открытый ключ действительно принадлежит данному абоненту.

Рассмотрим второй класс методов по типу используемого для распределения ключей канала связи – методы распределения ключей с использованием открытых каналов связи. Второй класс по виду распределяемого ключа подразделяется на подклассы методов распределения открытых ключей ассиметричных систем шифрования и совместного формирования (выработки) ключа симметричных систем шифрования. Первый подкласс по наличию третьей стороны декомпозируется на группы двухсторонних методов передачи открытых ключей с ЭЦП и трехсторонних методов. Первая группа по своему описанию и реализации одинакова с двухсторонними методами передачи ключей с ЭЦП, которые рассмотрены выше. Различие заключается в том, что теперь открытые ключи передаются по открытому каналу связи вместо зашифрованных ключей. Стандарт CCITT X.509 определяет подобный протокол [3, 11].

Известно, что к трехсторонним методам передачи открытых ключей относится инфраструктура открытых ключей (Public-Key Infrastructure – PKI), представляющая собой систему, определяющую, кому принадлежит тот или иной открытый ключ. Международный стандарт ISO X.509 определяет общую структуру PKI и протоколы их использования [3]. В соответствии со стандартом существует центральный орган, который называется центром сертификации (ЦС), который обладает парой «открытый ключ-закрытый ключ» и публикует свой открытый ключ. Открытый ключ центра сертификации известен всем. Чтобы присоединиться к инфраструктуре открытого ключа, пользователь А генерирует собственную пару «открытый ключ-закрытый ключ». Закрытый ключ он сохраняет в секрете, а открытый ключ передает центру сертификации. Центр сертификации проверяет, действительно ли пользователь А является тем, за кого себя выдает, а затем подписывает цифровое утверждение примерно следующего содержания: «Ключ принадлежит пользователю А». Это утверждение называется сертификатом и удостоверяет, что данный ключ принадлежит пользователю А. Теперь, если пользователь А захочет пообщаться с пользователем Б, он может отослать ему свой открытый ключ и сертификат. У пользователя Б есть открытый ключ центра сертификации, с помощью которого он может проверить цифровую подпись последнего. Если пользователь Б доверяет центру сертификации, он может довериться и тому, что ключ действительно принадлежит пользователю А. Выполнив описанные действия, пользователь Б может заверить в центре сертификации свой открытый ключ, после чего отослать открытый ключ и сертификат пользователю А. Теперь пользователи А и Б знают открытые ключи друг друга. Последние, могут быть использованы для запуска протокола согласования ключей, который сгенерирует ключ сеанса для безопасного общения. Основная концепция инфраструктуры открытого ключа страдает от ряда фундаментальных проблем, среди которых: косвенная авторизация, связанная с проблемой имен пользователей; зависимость безопасности от степени доверия к центру сертификации; отзыв сертификата.

Рассмотрим второй подкласс методов распределения ключей с использованием открытых каналов связи – методы совместного формирования ключа симметричных систем шифрования. Последние по

свойствам используемого открытого канала связи подразделяются на группы методов по квантовым каналам, по каналам связи без ошибок, по каналам связи с ошибками. Исследуем первую подгруппу. В последнее десятилетие XX века в ряде работ авторов Ч. Беннета и Ж. Брассара [13, 14, 15] освещались исследования методов квантовой криптографии. Среди отечественных специалистов работы в данной области вели С. Л. Галкин, А. Ю. Юркина, М. Б. Кокосийска, Б. И. Минков, Д. В. Кушнир под руководством профессора В. И. Коржика [16, 17, 18, 19]. Применение принципа неопределенности Гейзенберга [20] в системах передачи информации с поляризованными фотонами, позволяет получить новый криптографический эффект: построить канал связи, в котором невозможно прослушивание без обнаружения с очень большой вероятностью.

Цель известного протокола открытого распределения ключей BB84 [13] заключается в том, чтобы, используя квантовый канал, обеспечить передачу последовательности случайных битов между двумя пользователями, которые до этого не имели никакой совместной секретной информации. Если квантовая передача не нарушалась, то пользователи могут с уверенностью применять согласованную секретную последовательность в качестве секретного ключа в любой традиционной криптосистеме. Если обнаружится, что передача была нарушена, то пользователи могут не принимать во внимание полученную двоичную последовательность и должны попытаться произвести квантовую передачу еще раз.

Другой протокол B92 предложен Беннеттом в 1992 году [14], в котором для кодирования «0» и «1» использованы не четыре, как в протоколе BB84, а любые два неортогональных поляризованных состояния. Среди отечественных протоколов известен протокол Коржика-Кушнира, где для исправления ошибок канала применен интерактивный протокол исправления ошибок [18, 19].

Далее рассмотрим группу методов совместного формирования ключа по каналам связи без ошибок, которые основаны на идее шифрования с открытым ключом [2, 3, 18, 21] по числу объектов связи (корреспондентов), участвующих в процессе формирования (выработки) ключа декомпозируются на подгруппы методов для двух объектов связи («точка-точка») и для трех и более объектов связи (ключи для конференц-связи). К подгруппе методов «точка-точка» относится известный протокол Диффи-Хеллмана [22, 23], который включает независимое генерирование каждым из пары связывающихся корреспондентов своего случайного числа, преобразование его посредством некоторой процедуры, обмен преобразованными числами по открытому каналу связи и вычисление общего секретного ключа. Таким образом, открытое распределение ключей позволяет каждой паре корреспондентов системы выработать общий секретный ключ. Важным преимуществом является то, что ни один из абонентов заранее не может определить значения ключа, так как ключ зависит от сообщений, передаваемых в процессе обмена. Стойкость протокола основана на сложности известной экспоненциально трудной задачи вычисления дискретных логарифмов.

В 1978 году Р. Райвест, А. Шамир и Л. Адлеман предложили систему шифрования RSA [24] со своим способом формирования ключа, которая использовала однонаправленную функцию с потайным ходом. Эта система широко используется в настоящее время на практике.

Известна система Мак-Элиса [25, 26], построенная на основе теории алгебраического кодирования кода Гоппы [27], для которого проблема поиска кодового слова по данному весу в линейном двоичном коде является NP-полной. К достоинствам способа можно отнести высокую стойкость к компрометации. Однако рекомендуемые в [1, 25] параметры приводят к увеличению открытого ключа до 2^{19} бит и при шифровании длина сообщения увеличивается в 1,6 раза.

Протокол Нидеррайтера [28] очень близок к алгоритму Мак-Элиса, где открытый ключ – это случайная матрица проверки четности кода, исправляющего ошибки. Закрытым ключом служит эффективный алгоритм декодирования этой матрицы. В криптосистеме Нидеррайтера, в отличие от криптосистемы Мак-Элиса, используется обобщенный код Рида-Соломона.

Протокол Simple Key Management for Internet Protocol (SKIP) [2, 4] предназначен для обеспечения защиты трафика пользователей и прикладных систем при прозрачности средств защиты. В нем используется система открытого распределения ключей Диффи-Хеллмана. При распределении открытых ключей должен быть решен вопрос об их аутентификации. Разделяемый секретный ключ используется только для шифрования пакетных ключей. Протокол SKIP устанавливается непосредственно над пакетным драйвером, что обеспечивает высокую совместимость с прикладными программами.

На сетевом и сеансовом уровнях модели OSI в протоколе распределения временных ключей Secure Sockets Layer (SSL) применяются асимметричные криптосистемы [3], в которых временные ключи по алгоритму Диффи-Хеллмана распределяются с помощью основных открытых ключей. На сеансовом уровне ключи распределяются с помощью асимметричных систем RSA и Эль-Гамаля.

Для согласования параметров и управления ключами при формировании общего защищенного канала и создании в его рамках отдельных защищенных соединений наибольшее распространение получил протокол ISAKMP (Internet Security Association Key Management Protocol – протокол управления ключами и контекстами безопасности в Internet) [3]. Данный протокол разработан организацией Internet Engineering Task Force (IETF) и определен в качестве обязательного стандарта по управлению ключами в спецификации IPSec протокола IPv6. В сравнении с протоколом SKIP протокол ISAKMP более сложен в реализации, но

обеспечивает повышенную безопасность информационного взаимодействия.

Для автоматического обмена ключами используется протокол управления ключами в Интернете Internet Key Exchange (IKE) [3]. Дополнительно могут быть применены другие протоколы, такие как Kerberos или SKIP. IKE совмещает в себе три отдельных протокола: ISAKMP – протокол ассоциаций безопасности и управления ключами в интернете; Oakley (Oakley key determination protocol) – протокол определения ключей Окли; SKEMI (Secure Key Exchange Mechanism for Internet) – механизм безопасного обмена ключами в Интернете.

Известны разработанные протоколы на основе независимого формирования коррелированных последовательностей с неравномерным законом распределения вероятностей [29–33]. В процессе формирования ключа корреспонденты генерируют последовательности, отбрасывают несовпадающие символы с использованием кода в режиме обнаружения ошибок, сжимают оставшиеся последовательности в ключ.

Рассмотрим другую ветвь классификации методов совместного формирования ключа по каналам связи без ошибок по числу объектов связи – подгруппу методов для трех и более объектов связи [3]. Простейший пример протокола для группы из трех участников можно получить, слегка модифицировав протокол открытого распределения ключей Диффи-Хеллмана [3]. Анализ протокола показывает, что для формирования единого ключа необходима полносвязная модель канальной связности и протоколу присущи все недостатки описанного ранее протокола Диффи-Хеллмана. Известный протокол Бурместера и Десмедта для формирования ключа для конференц-связи группы описан в статье [34].

Опишем группу методов совместного формирования ключа симметричных систем шифрования по открытым каналам связи с ошибками, в которых для формирования ключа используется случайный фактор возникновения ошибок в каналах связи. Группа по наличию доверенной стороны подразделяются на подгруппы методов с доверенной стороной и без нее. Первая подгруппа методов декомпозируется на множества методов формирования ключа в условиях полного доверия и в условиях частичного доверия.

К первому множеству относится известная модель «источника с перехватом», описанная в источниках [35–37]. Существенным ограничением модели является условие, определяющее обеспечение лучшего качества каналов корреспондентов по сравнению с каналом перехвата нарушителя [37, 38].

Другая ветвь классификации методов с доверенной стороной определяется в условиях частичного доверия, т.е. когда объекты связи доверяют полученной от третьей стороны последовательности символов [39, 40]. Применение подобных методов формирования ключа возможно в условиях имитовоздействия. Третья сторона используется только для предварительного распределения ключевой информации, причем она в формировании ключа не участвует. Первым представляется протокол Маурера-Вольфа [39], включающий фазы инициализации выработки исходных данных случайных последовательностей и формирования ключа с использованием открытых каналов обсуждения в условиях имитовоздействия. Известный протокол Коржика-Моралиса характеризуется получением ключа небольшого размера, который затем используется для реализации разных типов аутентификации [40].

В работах [41, 42] на основе анализа протокола Мауэра-Вольфа разработан протокол Коржика-Яковлева-Бакаева без передачи параметров хэш-функции. Суть протокола заключается в том, что в качестве параметров хэш-функции корреспонденты выбирают соответствующие части из распределенных в фазе инициализации случайных последовательностей, а затем обмениваются проверочными символами к этим частям. Вследствие этого уменьшается длина аутентифицируемого сообщения по сравнению с протоколом Мауэра-Вольфа.

Подгруппа методов формирования ключа по открытым каналам связи с ошибками без доверенной стороны декомпозируется на множества двухсторонних методов и методов формирования сетевого ключа. Рассмотрим двухсторонние методы. Первым представителем выступает концепция подслушивающего канала А. Вайнера [43], в которой рассмотрен случай, когда канал связи между корреспондентами (основной канал) является менее зашумленным, чем канал противника (канал перехвата). Развитием концепции было исследование и получение ситуации, когда формировались «виртуальные» основной канал (ОК) и канал перехвата (КП), где качество первого превосходило качество второго. Представителями этого направления считаются протоколы модели «канала» В. Мауера [35, 36], способ формирования ключей из предварительно распределенных последовательностей [44], протоколы Коржика-Яковлева-Синюка [45–52].

Второе множество методов без выделения доверенной стороны называется – методы формирования сетевого ключа и объединяет протоколы формирования ключа для трех и более корреспондентов по открытым каналам связи с ошибками. Актуальность исследований этого направления определяется самой низкой стойкостью сетевого ключа к компрометации нарушителя. Методы формирования трехсторонненего ключа описаны в [52–57], а описание протокола открытого сетевого ключевого согласования приведено в [58–60].

Заключение

В заключении необходимо отметить, что в работе сделана попытка систематизированного представления методов распределения ключей путем построения

системы классификации. Предлагаемая система может быть полезна исследователям предметной области, связанной с разработкой современных систем установки и управления ключами, с точки зрения представления проблемы распределения ключей с системных позиций и определения актуальных направлений научных исследований.

Литература

1. Menezes, A. J. Handbook of applied cryptography / A.J. Menezes, P.C. Oorschot, S.A. Vanstone. – CRC Press, N.Y. 1996. – 780 p.

2. Молдовян, Н. А. Введение в криптосистемы с открытым ключом / Н.А. Молдовян, А.А. Молдовян. – СПб.: БХВ-Петербург, 2005. – 288 с.

3. Основы криптографии: Учебное пособие / А.П. Алферов [и др.]. – 3-е изд., испр. и доп. – М.: Гелиос АРВ, 2005. – 480 с.

4. Молдовян, Н. А. Криптография: от примитивов к синтезу алгоритмов / Н.А. Молдовян, А.А. Молдовян, М.А. Еремеев. – СПб.: БХВ-Петербург, 2004. – 448 с.

5. Фергюсон, Н. Практическая криптография : [пер. с англ.] / Н. Фергюсон, Б. Шнайер. – М. : Издательский дом «Вильямс»,2005. – 424 с.

6. Blom, R. Nonpublic key distribution / R. Blom // Advances in Cryptology.— Proceedings of EUROCRYPT'82. Plenum. New York. – 1983. – P. 231–236.

7. On key storage in secure networks / M. Dyer [et al.] // Cryptology. – 1995. – No. 8. – P. 189–200.

8. Shamir, A. How to share a secret / A. Shamir // Commun. ACM. – 1979. – Vol. 22. – No. 11. – P. 612–613.

9. Needham, R. M. Using encryption for authentication in large networks of computers / R.M. Needham, M.D. Schroeder // Communications of the ACM. – 1978. – Vol. 21. – P. 993–999.

10. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М.А. Иванов. – М.:КУДИЦ-ОБРАЗ, 2001 – 368 с.

11. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С : [пер. с англ.] / Б. Шнайер. – М. : Издательский дом «Вильямс», 2003. – 568 с.

12. Otway, D. Efficient and timely mutual authentication / D. Otway, O. Rees // Operating Systems Review. – 1987. – Vol. 21. – P. 8–10.

13. Bennett, C. H. Quantum cryptography: Public key distribution and coin tossing / C.H. Bennett, G. Brassard // Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. – 1984. – P. 175–179.

14. Experimental Quantum Cryptography / C.H. Bennet [et al.] // Journal of Cryptography. – 1992. – No. 5.

15. Bennett, C. H. Quantum Cryptography Using Any Two Nonorthogonal States / C.H. Bennet // Phys. Rev. Letters. – 1992. – Vol. 68. – No. 21. – P. 3121–3124.

16. Балакирский, В. Б. Принципы квантовой криптографии / В.Б. Балакирский, В.И. Коржик, Д.В. Кушнир // Защита информации. – 1995. – Вып. 3/1. – С. 43–51.

17. Экспериментальное и теоретическое моделирование волоконно-оптического квантового канала связи / С.Л. Галкин [и др.] // 48-я НТК проф.-препод. состава Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича: Тез. докл. – СПб., 1995. – С. 7–9.

18. Практическая реализация передачи ключей по волоконно-оптическому каналу связи / В.И. Коржик [и др.] // 47-я НТК проф.-препод. состава Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича: Тез. докл. – СПб, 1994. – С. 2–6.

19. Кушнир, Д. В. Исследование и разработка методов передачи конфиденцальных данных по квантовому каналу : дис. ... канд. техн. наук : 05.12.20 / Д.В. Кушнир; СПбГУТ им. проф. М. А. Бонч-Бруевича. – СПб, 1996. – 157 с.

20. Experimental quantum cryptography / C.H. Bennet [et al.] // Journal of Cryptology. – 1992. – Vol. 5. – No. 1. – P. 3–28.

21. Оков, И. Н. Криптографические системы защиты информации / И.Н. Оков. – СПб.: ВУС, 2001. – 236 с.

22. Диффи, У. Первые десять лет криптографии с открытым ключом / У. Диффи // ТИИЭР. – 1988. – Т. 76. – № 5. – С. 54–72.

23. Патент US № 4200770 H04L9/04 от 02.04.80

24. Rivest, R. A method for obtaining digital signatures and public-key cryptosystems / R. Rivest, A. Shamir, L. Adleman // Communications ACM. – 1978. – Vol. 21. – P. 120–126.

25. McEIiece, R. J. A Public-Key Cryptosystem Based on Algebraic Coding Theory / R.J. McEIiece // Deep Space Network Progress Report 42–44. – Jet Propulsion Laboratory, California Institute of Technology, 1978. – P. 114–116.

26. Park, S. J. An Entrusted Undeniable Signature / S.J. Park, K.H. Lee., D.H. Won // Proceedings of the 1995 lapan-Korea Workshop on Information Secunty and Cryptography. Inuyama. Japan. 24–27 Jan 1995. – P. 120–126.

27. Мак-Вильямс, Ф. Теория кодов, исправляющих ошибки. / Ф. Мак-Вильямс, Н. Слоэн. – М.: Связь, 1979. – 744 с.

28. Niederreiter, H. Knapsack-Type Cryptosystems and Algebraic Coding Theory / H. Niederreiter // Problems of Control and Information Theory. – 1986. – Vol. 15. – No. 2. – P. 159–166.

29. Синюк, А. Д. Оценка потенциальных условий формирования ключа с использованием открытых каналов без ошибок / А.Д. Синюк // Проблемы информационной безопасности. Компьютерные системы. – 2007. – № 2. – С. 72–82.

30. Синюк, А. Д. Основные принципы формирования ключа с использованием открытых каналов связи без помех / А.Д. Синюк // Вопросы защиты информации. – 2008. – Вып. 2 (81). – С. 10–19.

31. Синюк А. Д. Синтез протокола формирования ключа с использованием открытых каналов связи без ошибок / А.Д. Синюк // Вопросы защиты информации. – 2009. – Вып. 1 (84). – С. 2–5.

32. Патент РФ № 2355116 от 10.05.2009.

33. Патент РФ № 2356168 от 20.05.2009.

34. Burmester, M. A secure and efficient conference key distribution system / M. Burmester, Y. Desmedt // Advances in Cryptology – EUROCRYPT '89. LNCS 434. – 1990. – P. 122–133.

35. Maurer, U. Protocols for Secret Key Agreement by Public Discussion Based on Common Information / U. Maurer // Advances in Cryptology CRYPTO '92, Lecture Notes in Computer Science. – 1993. – Vol. 740. – P. 461–470.

36. Maurer, U. Secret Key Agreement by Public Discussion Based on Common Information / U. Maurer // IEEE Trans. on IT. – 1993, May. – Vol. 39. – P. 733–742.

37. Maurer, U. Towards characterizing when information - theoretic secret key agreement is possible / U. Maurer, S. Wolf // Advances in Cryptology ASIACRYPT '96 , Lecture Notes in Computer Science – 1996. – Vol. 1163. – P. 145–158.

38. Ahlswede, R. Common Randomness in Information Theory and Cryptography–Part I: Secret Sharing / R. Ahlswede, I. Csiszar // IEEE Trans. on IT. – 1993, July. – Vol. 39. – No. 4. – P. 1121–1132.

39. Maurer, U. Information-theoretically secure secret-key agreement by NOT au-thenticated public discussion / U. Maurer // Advances in Cryptology – EUROCRYPT 97. – 1997. – Vol. 1233. – P. 209–225.

40. Korjik, V. Hybrid authentication based on noisy channels / V. Korjik, G. Moralis-Luna // International Journal of information security. – 2003. – Vol. 1. – No. 4. – P. 203–210.

41. Яковлев, В. Протоколы формирования ключа с использованием открытых каналов связи с шумом в условиях активного перехвата. Часть 2 / В. Яковлев, В. Коржик, М. Бакаев // Проблемы информационной безопасности. Компьютерные системы. – 2004 – № 4. – С. 60–75.

42. Яковлев, В. Протоколы формирования ключа на основе каналов связи с шумом в условиях активного перехвата с использованием экстракторов / В. Яковлев, В. Коржик, М. Бакаев // Проблемы информационной безопасности. Компьютерные системы. – 2006. – № 1. – С. 60–81.

43. Wyner, A. The wire – tap channel / A. Wyner // Bell Syst. Techn. J. – 1975. – Vol. 54. – No 8. – P. 1355–1387.

44. Патент ЕР № 0511420 А1 МПК6 Н04L9/08 от 04. 11. 92

45. Синюк, А. Д. Протокол выработки ключа в канале с помехами / А.Д. Синюк, В.И. Коржик, В.А. Яковлев // Проблемы информационной безопасности. Компьютерные системы. – 2000. – № 1. – С. 52–63.

46. Синюк, А. Д. Протокол выработки ключа, основанный на большем информационном различии последовательностей легального и нелегального пользователей / А.Д. Синюк, В.И. Коржик, В.А. Яковлев // Проблемы информационной безопасности. Компьютерные системы. – 2000. – № 2. – С. 37–48.

47. Yakovlev, V. Key Distribution Protocol Based on Noisy Channel and Error Detection Codes / V. Yakovlev, V. Korjik, A. Sinuk // International Workshop MMM–ACNS 2001. Lecture Notes in Computer Science. – 2001. – Vol. 2052. – P. 242–250.

48. Патент РФ № 2171012 от 20.07.2001.

49. Патент РФ № 2180469 от 10.03.2002.

50. Патент РФ № 2180770 от 20.04.2002.

51. Патент РФ № 2183051 от 27.05.2002.

52. Yakovlev, V. Achieveabiliti of the Key–Capacity in a Scenario of Key Sharing by Public Discussion and the presence of Passive Easvesdropper / V. Yakovlev, V. Korjik, A. Sinuk // International workshop. Mathematical metods, model and architectures for computer network security. Lecture Notes in computer science. – 2003. – No. 2776. – P. 308–315.

53. Синюк, А. Д. Формирование трехстороннего шифр-ключа по открытым каналам связи с ошибками : монография / А.Д. Синюк. – СПб: ВАС, 2009. – 360 с.

54. Синюк, А. Д. Постановка задачи формирования группового ключа по открытым каналам связи с ошибками / А.Д. Синюк // Информация и Космос. – 2011. – № 1. – С. 95–99.

55. Бушуев, С. Н. Математическая модель нарушителя открытого ключевого согласования сети с минимальным числом корреспондентов / С.Н. Бушуев, А.Д. Синюк // Вопросы радиоэлектроники. – 2013. – Вып. № 1. – С. 109–118.

56. Патент РФ № 2480923 от 27.04.2013.

57. Остроумов, О. А. Протокол открытого формирования трехстороннего ключа / О.А. Остроумов, А.Д. Синюк // Наукоемкие технологии в космических исследованиях Земли. – 2014. – Т. 6. – Вып. 2. – С. 48–52.

58. Синюк, А. Д. Установление криптографической связности между корреспондентами сети подвижной связи / А.Д. Синюк // Информация и Космос. – 2008. – № 2. – С. 95–99.

59. Синюк, А. Д. Теоретические аспекты построения протокола установления криптографической связности между корреспондентами сети подвижной связи / А.Д. Синюк // Информация и Космос. – 2008. – № 4. – С. 114–119.

60. Синюк, А. Д. Протокол формирования сетевого ключа по открытым каналам связи с ошибками / А.Д. Синюк // Труды СПИИРАН. – 2010. – Вып. 3(14). – С. 29–49.