НЕМАТЕМАТИЧЕСКИЕ МЕТОДЫ В КРИПТОГРАФИИ
(ЗАЩИЩЕННАЯ СВЯЗЬ НА ОСНОВЕ ОДНОРАНГОВОЙ MESH-СЕТИ)

Черепнёв М. А.[1]

DOI:10.21681/3034-4050-2026-1-72-77

Ключевые слова: *шифрование, защита информации, одноранговые сети, децентрализованные системы, цифровая подпись, распределение ключей, аутентификация.*

Аннотация

Цель работы *в анализе слабостей протоколов защиты информации в ТЗУ ВС РФ и разработке предложений по её усовершенствованию.*

Метод исследования *состоит в предложении использовать децентрализованную криптографию.*

Результаты исследования: *предложены некоторые новые методы защиты информации в условиях (временного) отсутствия удостоверяющего центра. Предлагаемые методы не используют трудно решаемые математические задачи (дискретное логарифмирование, факторизация, поиск наименьшего вектора в решетке и пр.). Предлагаются способы, похожие на физическую аутентификацию пользователя, но в цифровом варианте. Современные индивидуальные средства коммуникации позволяют это сделать. Кроме того предлагается использовать величину меш-сети в качестве фактора усиления стойкости связи составляющих её абонентов.*

Научная новизна *состоит в разработке новых протоколов децентрализованной криптографии, позволяющих понизить нагрузку на центральный узел и повысить функциональность и стойкость в работе сети в целом.*

Введение

Для сетей связи тактического звена предложена система защищенной связи на основе одноранговой mesh-сети. В этом случае совокупная цена оборудования становится значительно меньше, а сама сеть надежнее. При этом уничтожение узлов связи одноранговой сети становится неэффективным с точки зрения противника, так как не наносит ущерба работе связи. Кроме того, современные средства военной связи используют спутники связи, количество которых в нашей стране не велико, а кроме того, эти спутники являются уязвимыми для средств поражения противника. Как будет показано дальше, предложенная система способна самостоятельно определять переход абонентов в режим работы под контролем (захват противником).

Важным свойством надежных систем защиты информации является теоретико-информационный характер стойкости. Подобный характер стойкости можно получить и с помощью децентрализованной криптографии. Одна из первых работ на эту тему [3] дала толчок к построению крипто протоколов с совершенно новыми свойствами. Мы будем использовать эти идеи и некоторое их развитие совместно с более старыми [4] методами защиты информации.

Решение поставленной задачи

Рассмотрим схему децентрализованного шифрования на основе разделения открытого текста на пороговой схеме с последующей рассылкой разными маршрутами через списки доверия. Проверка совпадения на получателе исключает возможность подделки. Значит чем больше сеть, тем такая схема более стойкая. Она позволяет повысить стойкость до теоретико-информационного уровня. Упрощая пороговую схему до генерации случайных строк и их XOR-а со строкой передаваемого открытого текста, получим новый протокол сетевого шифрования. Поскольку выбор из некоторого набора строк половины этих строк может быть осуществлен перебором экспоненциального объема, то фиксированный такой выбор может быть взят в качестве общего ключа шифрования. При этом открытый текст будет XOR-ом выбранных строк. Конечно, если атакующий может читать весь трафик отправителя или получателя, или узла сети, где возможно собрать все необходимые строки, то дешифровка сводится к экспоненциальному перебору общего ключа шифрования.

1 Черепнёв Михаил Алексеевич, доктор физико-математических наук, профессор кафедры информационной безопасности факультета ВМК МГУ имени М. В. Ломоносова. г. Москва, Россия. E-mail: cherepniov@gmail.com

Однако, если коммутация в сети устроена так, что траектории пересылки выбранных строк не пересекаются, то для сбора всех таких строк потребуется контроль над частью всех таких траекторий. Если эти траектории выбираются с некоторой долей случайности, то это, фактически, потребует контроля над всей сетью. Однако, чем больше сеть, тем сложнее ее полностью контролировать.

Новыми проблемами в криптографии являются: сетевая работа per-to-per протоколов, перегрузки узлов в централизованных сетях. Поэтому модель нарушителя при получении доказательства сетевой стойкости должна рассматривать атаку сети на выделенного клиента. Принцип децентрализованной стойкости всей сети должен содержать требование: для несанкционированного доступа к информации нужно сломать защиту каждого. Кроме того, должна быть обеспечена независимость от транспорта (сети) и клиентского программного обеспечения. При этом известные трудно решаемые задачи (факторизация, дискретное логарифмирование, решение нелинейных систем алгебраических уравнений от многих переменных и т.д.) остаются основой криптографической стойкости.

Ускоренное решение криптографических задач (обращение односторонних функций) может быть получено не только с помощью квантового компьютера, но и с помощью конвейерных, векторных и других специальных вычислителей. Поэтому одной из важных задач является построение и использование теоретически (а не вычислительно) стойких методов. В том числе не дешифруемых протоколов.

Децентрализованное шифрование на основе разделения шифр текста на пороговой схеме с последующей рассылкой разными маршрутами через списки доверия. Проверка совпадения на получателе.

Данный протокол использует сетевую структуру сети для поднятия уровня стойкости до теоретико-информационного уровня. А именно, упрощаем пороговую схему до генерации n случайных строк и XOR-а половины из них со строкой зашифрованного текста.

Количество выборов без учета порядка из n строк половины равно

$$C_n^{n/2} \approx 2^n \sqrt{\frac{2}{\pi n}}$$

(данная оценка получена с помощью формулы Стирлинга). Поэтому, если номера использованных в суммировании строк считать секретным ключом, то угадать их среди всех передаваемых строк экспоненциально трудно. В тоже время если противнику удается перехватить не все используемые строки, то он получает лишь случайную строку. То есть в этом случае имеется теоретически не дешифруемый протокол.

Оценки на трудоемкость метода «грубой силы» – экспоненциальные. Значит, чем больше сеть, тем такое шифрование более стойкое.

Для повышения стойкости с помощью программно-конфигурируемых сетей можно предусмотреть, чтобы указанные выше маршруты передачи отдельных строк не пересекались, а также распределить пересылку по времени, по частотным диапазонам, по различным сетям, с использованием ранее пересланных кому-то случайных строк или зашифрованных строк секретной информации; псевдослучайных строк, полученных на основе общего секретного ключа и т.д. То есть часть строк может вообще не передаваться, а быть общим секретом.

Другой способ увеличить стойкость криптопротоколов, не прибегая к трудно решаемым математическим задачам – это оцифровка физической аутентификации. При этом для получения объективной оцифрованной информации можно эффективно использовать клавиатуру, микрофон, а также квантовые сенсоры [1] (датчики движения, анализаторы химических событий, точечные термометры, атомные часы и т.д.). Данные с этих устройств (см. например [2]), подписанные секретным ключом абонента и снабженные меткой времени (которую нельзя модифицировать незаметно) и открытым ключом, могут составить портрет абонента, достаточный для его (или его открытого ключа) автоматической аутентификации (динамическая аутентификация). Естественно, чем больше различных способов анализа состояния абонента, тем более стойкая аутентификация может быть построена с их использованием. Повторному использованию аутентифицирующей информации помешают метки времени, которые нельзя модифицировать незаметно (защищенные метки времени).

Доверие в сети может распространяться и с помощью непосредственно физической аутентификации, поддержанной в течение некоторого периода метками времени. Распространение информации в сети при помощи

правила «рукопожатий» позволит охватить всех.

Объективное наблюдение за абонентом со стороны нескольких «доверенных» абонентов. Одиночного абонента труднее аутентифицировать. А вот если у него имеется доверенное окружение (например, имеющее с ним общие секретные ключи, находящееся с ним в постоянном контакте, на прямой видимости и т.д.) то подтверждающая информация от разных членов окружения подтверждает аутентификацию абонента (коллективная аутентификация).

Постоянный автоконтакт, обеспечивающий поддержку непрерывной аутентификации, также повышает стойкость. Эта оцифровка обычного протокола переклички на поверке в воинских частях или переклички «Ау» в условиях ограниченной видимости. В этом случае по голосу (а в нашем случае могут быть использованы и другие, в том числе квантовые и нано датчики [1]) можно не только аутентифицировать абонента, но и узнать его статус.

Отметим еще важную особенность рассматриваемого подхода. Если абонент пересылает (и получает) передающему устройству информацию в зашифрованном виде, то такая система остается стойкой при использовании любого иностранного оборудования и программного обеспечения с единственным условием выполнения транспортной функции. Поэтому, использование для пересылки зашифрованных сообщений оборудования разных производителей одновременно, с проверкой совпадения передаваемого сообщения на получателе, повышает стойкость. Предварительное зашифрование и расшифрование должно производиться на отечественном доверенном оборудовании (индивидуальном шифраторе).

Рассмотрим конкретный пример. Пусть имеется подразделение из 50 бойцов, которые отправляются на боевое задание. Первоначально у каждой пары есть свой симметричный ключ для шифрованной связи. Всего 2500 различных ключей. Пусть, для простоты, у каждого имеется однотипная рация, устройство которой позволяет в каждый момент времени связаться с 10 бойцами своей группы. При этом возможен захват каждой рации в работающем состоянии в течение периода времени (такт, например 2–4 минуты) противником с вероятностью p.

Задача состоит в обеспечении секретной связи, стойкой с некоторой вероятностью, достаточной для безопасной передачи координат объектов на линии боевого соприкосновения.

Средства для решения указанной задачи следующие:

1. Целенаправленный аутентифицирующий запрос, состоящий в анализе статических и динамических персональных данных. Статические (неизменяемые) персональные данные включают секретный ключ. Динамические – это результаты наблюдения за бойцом со стороны его окружения, результаты работы квантовых и наносенсоров, аудио, SMS, фото; все с метками времени (простановка этих меток – это отдельная задача, которая в данной статье не рассматривается). Анализу может подвергаться почерк бойца при наборе с клавиатуры, характер его движений (это по своей природе тоже симметричные ключи, которые, однако, трудно «отделить от человека», воспроизвести). Пусть анализатор (например искусственный интеллект) определяет по этим признакам «свой-чужой» с вероятностью p_1.
2. Запрос-перекличка осуществляется один раз в 2–4 минуты. Опрашивает случайного доступного абонента (равновероятно) на предмет адекватности отклика. Адекватность понимается в смысле «небольшого» отличия от предыдущего отклика того же абонента. Это можно реализовать, например, при помощи вычисления хеша от кода сообщения. Опуская подробности, имеем, что «небольшое» отличие в сообщениях дает для них одно и то же кодовое слово. Например, если кодовое расстояние вдвое больше «небольшого», а расстояние от сообщений до соответствующих кодовых слов в четыре раза меньше кодового расстояния. Пусть вероятность определить своего в результате такого запроса неверно равна p_2.
3. Целенаправленный запрос окружения передающего абонента на результаты запросов-переклички и физической аутентификации. Вероятность реализации (возможность) опросить хотя бы одного из окружения за 2–4 минуты равна p_3.
4. Построение нового секретного ключа:
   а) с использованием старых ключей;

б) с использованием запросов п. 1–3;
в) с использованием посредников в сети.

5. Режим теоретически не дешифруемой передачи (при возможности создания большого числа непересекающихся маршрутов).

Пункты 1–3 выбраны так, чтобы не допустить перегрузки сети. Пункты 1 и 3 описывают вызовы по мере необходимости конкретной связи и, поэтому, не сильно увеличивают трафик. Для реализации пункта 2, при условии, что перекличка двусторонняя, достаточно задействовать каждый из 2500 двусторонних каналов с вероятностью 0,1. То есть в среднем, нагрузка на сеть оценивается в 250 пересылок за такт.

Оценим вероятность как функцию времени. Пусть T – количество прошедших интервалов (тактов) между перекличками.

Вероятность ошибки в определении своего целенаправленными запросами вида 1 и 3 в первом такте, при условии, что все опрашиваемые рации не захвачены, не больше, чем

$$P = p \sum_{i=0,\dots,10)} C_{10}^{i} \left(\frac{9}{10}\right)^{i} \left(\frac{p_2}{10}\right)^{10-i} (1-p_1)(1-p_3) =$$

$$= p(1-p_1)(1-p_3)\left(\frac{9+p_2}{10}\right)^{10} =$$

$$= p(1-p_1)(1-p_3)(1-\left(\frac{1-p_2}{10}\right)^{10} \approx$$

$$\approx (1-p_1)(1-p_3)e^{-(1-p_2)}.$$

В общем случае получаем примерно тоже, умноженное на

$$\sum_{i=0,\dots,10)} C_{10}^{i} p^{10-i}(1-p)^{i} = 1.$$

Для двух тактов аналогично получим

$$p(1-p)P + p(1-p_1)(1-p_3)^2 e^{-2(1-p_2)} \approx$$

$$\approx p(1-p_1)(x+x^2)(1-p)^2,$$

$$x = \frac{(1-p_3)e^{-(1-p_2)}}{1-p}.$$

В общем случае для T тактов имеем:

$$p(1-p_1)\frac{1-x^T}{1-x}(1-p)^T,$$

что дает величину, пропорциональную $(1-p)^T$ при растущем T, так как в нетривиальном случае всегда выполнено: $(1-p_3)e^{-(1-p_2)} < 1$. Заметим, что множитель $(1-p)^T$ при растущем T пропорционален вероятности того, что никто из бойцов не будет захвачен, что в нашей модели происходит с вероятностью, стремящейся к нулю. Таким образом, вероятность того, что захваченный воин будет принят за своего в нашей модели незначительно отличается от вероятности того, что он вообще будет захвачен.

Для оценки эффективности п. 4 достаточно потребовать, чтобы граф двусторонней связи был двусвязным. Двусвязный граф – это связный и неделимый граф, то есть удаление любой вершины не приведёт к потере связности. Теорема Уитни утверждает, что граф двусвязен тогда и только тогда, когда между любыми двумя его вершинами есть как минимум два непересекающихся пути.

Для п. 5 заметим следующее: данный протокол использует сетевую структуру коммутации для поднятия уровня стойкости с теоретико-сложностного (для вскрытия требуются большие вычисления) до теоретико-информационного (вычислительная мощность не облегчает вскрытия) уровня. А именно, генерируем n случайных строк и XOR-сумму их со строкой зашифрованного текста.

Генерируем еще $n-1$ случайных строк. Перемешиваем получившиеся строки и посылаем адресату по сети разными маршрутами в разное время. При этом, некоторые пересылки могут быть заменены на ссылки на ранее переданные кому-то строки секретной или открытой информации. Количество выборов без учета порядка из $2n$ строк $n+1$ нужной для получения шифртекста, равно

$$C_{2n}^{n+1} \approx \frac{2^{2n}}{\sqrt{\pi n}}.$$

Поэтому, если номера использованных в суммировании строк считать секретным ключом, то угадать их среди всех передаваемых строк экспоненциально трудно. В то же время, если противнику удается перехватить не все используемые в суммировании строки, то он получает лишь случайную строку. То есть в этом случае имеется теоретически не дешифруемый протокол.

Заключение

Децентрализованная криптография во многом приходит на смену криптографии двусторонних протоколов. Новые направления в криптографии, используемые в таких технологиях как «Блокчейн», могут быть расширены для применения в системах защиты сетевого взаимодействия. При этом стойкость может возрастать с ростом количества абонентов в сети и выходить на теоретико-информационный уровень. Эта стойкость может не зависеть от оборудования, используемого для работы в сети. Перегрузки

центральных узлов и атаки на них в децентрализованных сетях отсутствуют. Кроме того, такие решения позволяют получить доселе невозможные свойства: противодействие атакам типа «человек посередине», удаленная аутентификация незнакомых абонентов, невозможность блокировки отдельных абонентов, определение статуса «доверенный свой», определение режима «работа под контролем» и т.д.

Литература

1. Букашкин С. А., Черепнёв М. А. Квантовые устройства в криптографии INJOIT, Vol. 11, No 1 (2023), p. 104–108
2. Букашкин С. А., Черепнёв М. А. Принцип децентрализации в системах защищенной связи. Сборник материалов XIII межведомственной научной конференции «Актуальные направления развития систем обеспечения безопасности объектов государственной охраны и охраняемых объектов, специальной связи для нужд органов государственной власти и специального информационного обеспечения государственных органов.» февраль 2023г., Орел.
3. Nakamoto, Satoshi[2]: «Bitcoin: A Peer-to-Peer Electronic Cash System» Available: www.bitcoin.org/bitcoin.pdf.
4. Черепнев М. А. Криптографические протоколы / М. А. Черепнев; Московский государственный университет имени М. В. Ломоносова, Факультет вычислительной математики и кибернетики. – Москва: МАКС Пресс, 2018. – 2, 125 с. – ISBN 978-5-89407-592-1. – Текст: непосредственный.

NON-MATHEMATICAL METHODS IN CRYPTOGRAPHY
(SECURE COMMUNICATION BASED ON A PEER-TO-PEER MESH NETWORK)

Cherepnev M. A.[3]

Keywords: *encryption, information protection, peer-to-peer networks, decentralized systems, digital signature, key distribution, authentication.*

Abstract

The purpose of the work *is to analyze the weaknesses of information security protocols in the technical intelligence of the Armed Forces of the Russian Federation and to develop proposals for its improvement.*

The research method *consists in proposing the use of decentralized cryptography.*

Results: *some new methods of information protection in the (temporary) absence of certification authority have been proposed. The proposed methods do not use mathematical problems that are difficult to solve (discrete logarithm, factorization, search for the smallest vector in a lattice, etc.). Methods similar to physical user authentication are proposed, but in a digital version. Modern individual means of communication allows you to do this. It is proposed to use the value of the network mesh as a factor in strengthening the communication stability of its subscribers.*

The scientific novelty *lies in the development of new protocols of decentralized cryptography, which reduce the load on the central node and increase the functionality and stability of the network as a whole.*

References

1. Bukashkin S. A., Cherepnyov M. A. Kvantovy`e ustrojstva v kriptografii INJOIT, Vol. 11, No 1 (2023), p. 104–108
2. Bukashkin S. A., Cherepnyov M. A. Princip decentralizacii v sistemax zashhishhennoj svyazi. Sbornik materialov XIII mezhvedomstvennoj nauchnoj konferencii «Aktual'ny'e napravleniya razvitiya sistem obespecheniya bezopasnosti ob'ektov gosudarstvennoj oxrany' i oxranyaemy'x ob'ektov, special`noj svyazi dlya nuzhd organov gosudarstvennoj vlasti i special'nogo informacionnogo obespecheniya gosudarstveny'x organov.» fevral' 2023 g., Orel.

2 Сатóси Накамóто (англ. Satoshi Nakamoto) — псевдоним человека или группы людей, разработавших протокол криптовалюты биткойн и создавших первую версию программного обеспечения, в котором этот протокол был реализован. Было предпринято несколько попыток раскрыть реальную личность или группу, стоящую за этим именем, но ни одна из них не была успешной.

3 Mikhail A. Cherepnev, Doctor of Physical and Mathematical Sciences, Professor, Department of Information Security, Faculty of Computer Science, Lomonosov Moscow State University, Moscow, Russia. E-mail: cherepniov@gmail.com

3. Nakamoto, Satoshi: «Bitcoin: A Peer-to-Peer Electronic Cash System». Available: www.bitcoin.org/bitcoin.pdf
4. Cherepnev, M. A. Kriptograficheskie protokoly` / M. A. Cherepnev; Moskovskij gosudarstvenny`j universitet imeni M. V. Lomonosova, Fakul'tet vy'chislitel'noj matematiki i kibernetiki. - Moskva: MAKS Press, 2018. – 2, 125 s. – ISBN 978-5-89407-592-1. – Tekst : neposredstvenny'j.