РАЗРАБОТКА КРИПТОСИСТЕМЫ С РАЗДЕЛЯЕМЫМ СЕКРЕТОМ НА ОТКРЫТОМ КАНАЛЕ СВЯЗИ

Лысяк Александр Сергеевич

Российская Федерация, Новосибирская область, г. Новосибирск

2022

АННОТАЦИЯ

Настоящая исследовательская работа посвящена разработке криптосистемы разделения секрета на открытом канале связи, решающей проблему эффективного (т.е. за квазилинейное время) криптостойкого (k,n)-доступа (т.е. доступа по кворуму) к информации произвольной длины в незащищённом канале связи.

В процессе исследования проведён анализ существующих методов генерации общего ключа на открытом канале связи, а также анализ методов разделения секрета через кворум, учтены их плюсы и минусы. В работе использованы теоретические методы исследования с применением аппарата дискретной математики и мат. статистики, а также с приведением практический приложений приводимых теоретических исследований.

В работе предложено алгоритмическое обобщения метода Диффи-Хеллмана, решающее проблему генерации общего ключа между произвольным числом участников в незащищённом канале связи. Кроме того, предложен метод разделения секрета, работающий за квази-логарифмическое время относительно порядка поля на основе интерполяционных многочленов Лагранжа. При этом доказана криптостойкость предложенного метода. В конце работы, предложено полное описание всей криптосистемы с наглядными схемами.

В работе содержится подробное описание процесса сравнительного анализа существующих методов решения поставленных задач, а также описание разработки собственных алгоритмов. Все описываемые алгоритмические свойства содержат строгие доказательства.

Структура работы обусловлена предметом, целью и задачами исследования.

Работа состоит из введения, четырёх глав и заключения. Список литературы включает в себя 8 печатных изданий.

Содержание

Введение

Актуальность исследования

Представленная работа посвящена исследованию двух проблем: защищенной передачи данных между произвольными участниками без общего секрета по открытому каналу, а также проблеме разделения доступа к защищенным данным посредством кворума от произвольного числа участников.

Первая проблема особо актуальна в современном мире в связи с широким распространением открытых электронных каналов передачи информации и всемирной информатизацией. Таким каналом является Интернет: между передающим и принимающим участниками стоит множество посредников в виде интернет-провайдеров, владельцев интернет-ресурсов и многих других, кто участвует в передаче: все они могут беспрепятственно читать и подменять передаваемые данные. Задача защищенной передачи информации по открытому каналу возникает как в военных отраслях, так и в среде государственного и коммерческого документооборота, а также даже среди частных лиц, заинтересованных в приватности передаваемых данных.

Если у участников передачи есть некий общий секрет, то проблема решается посредством использования симметричных криптографических алгоритмов, однако если его нет, то возникает задача создания общего ключа для данных алгоритмов. Именно её решение и рассматривается в данной работе для случая произвольного числа участников передачи. Данная задача имеет решение для двух участников в виде известной схемы Диффи-Хеллмана: в данной работе предлагается её расширение на более общий случай произвольного числа участников.

Вторая проблема представляет интерес в задачах многопользовательской авторизации, т.е. когда требуется аутентифицировать и предоставить доступ к информации только при наличии кворума из участников [1]. Кроме того, данная задача, называемая в криптографии также пороговой схемой, активно решается в рамках разработки стеганографических алгоритмов для скрытой передачи информации в цифровых изображениях, а также в задачах выполнения критических транзакций (например, крупные банковских операции, требующие подтверждения несколькими участниками) [2, 3]. Представленная проблема имеет несколько узкоспециализированных решений, которые были проанализированы в рамках данной работы: схема Блэкли [4], схема Миньотта [5] и схема Асмута-Блума [6]. Все указанные алгоритмы имеют либо достаточно высокую сложность реализации, либо высокую вычислительную трудоемкость. В представленной работе предлагается более простой в реализации алгоритм пороговой схемы, имеющий квази-линейную вычислительную сложность (что будет показано далее), однако обладающий свойствами криптостойкости не ниже представленных выше методов.

Существующие алгоритмы решения проблемы разделения секрета и доступа к нему по кворуму обладают еще одним недостатком: все они предполагают обмен данными в защищенном канале, что в реальной практике, как было указано выше, далеко не всегда так. По этой причине конечной целью данной работы является создание алгоритмической криптографической схемы разделения секрета по кворуму среди произвольного числа участников с использованием открытого канала связи. Решение данной задачи представляет

собой разработку схемы с использованием некоторой комбинации первой и второй указанных схем.

Постоянно растущее число публикаций по указанным тематикам подтверждает актуальность выбранной темы исследований. На них же основаны предложенные в данной работе алгоритмы.

Цель исследования

Пусть имеется n ($n > 2$) участников обмена данными, которые имеют некоторую общую секретную информацию SS достаточно большого размера ($2^{10} < ||SS|| < 2^{45}$, где $||SS||$ - битовый размер информации) и могут обмениваться данными, используя только открытый канал связи.

Целью данной работы является разработка криптографического протокола обмена данными, при котором любые k участников из n, собравшись в кворум, могут получить доступ к SS, но никакое подмножество участников в количестве $t < k$ не может получить доступ к SS. При этом для обмена данными между участниками используется открытый незащищённый канал связи, который может прослушиваться злоумышленником, а у участников исходно нет общего секрета (ключа).

Основным объектом данного исследования является защищаемая секретная информация (SS), доступ к которой требуется разделить. Предметом исследования являются алгоритмы множественного разделения доступа к секретной информации, а также алгоритма множественной генерации общего секрета.

Гипотезы данного исследования:

1. Существуют алгоритмы создания защищённого канала связи между произвольным числом участников, не имеющих общего секрета, на открытом канале связи.
2. Существует метод реализации (k, n)-пороговой схемы для секретной информации между произвольными участниками с квази-линейной сложностью относительно порядка поля, не имеющих общего секрета, на базе открытого канала связи.

Задачи исследования

1. Исследовать существующие методы генерации общего ключа и разработать на их основе протокол создания защищённого канала связи на базе открытого канала с высокой скоростью обмена данными.
2. Разработать схему разделения малого секрета (битовый размер не превосходит 1024, чего достаточно для ключа к некоторому симметричному алгоритму шифрования, используемого для шифрования секрета SS).
3. Объединить протоколы из пунктов выше в единый алгоритм (протокол) с минимизацией вычислительной сложности.

Научная новизна работы заключается в следующем:

1. Проведено исследование существующих методов генерации общего ключа, выбран наиболее вычислительно легковесный алгоритм и на базе него разработано обобщение алгоритма создания общего секрета Диффи-Хеллмана на случай

произвольного числа участников обмена с линейным ростом сложности относительно числа участников, доказана криптостойкость предложенного алгоритма.

2. Разработан алгоритм решения задачи (k,n)-пороговой схемы разделения секрета с применением для решения данной задачи интерполяционных полиномов Лагранжа.
3. Разработан с использованием решений двух первых задач криптопротокол *(k,n)*-доступа к большим (с позиции битового размера) данным с использованием открытого канала связи с доказанной криптостойкостью и трудоёмкостью, не превышающей сложности алгоритмов симметричного шифрования.

Применяемые методы исследования:

1. Анализ литературы по теме исследования (конечные поля, арифметика в них, методы разделения секрета, методы генерации общего ключа, методы интерполяции).
2. Сбор и обобщение сведений, а также сравнительный анализ имеющихся методов генерации общего ключа, а также о решениях задачи (k, n)-пороговой схемы, их достоинствах и недостатках.
3. Индукция (при обобщении метода Диффи-Хеллмана), дедукция и синтез гипотез (при разработке метода восстановления секрета при помощи многочленов Лагранжа).

Глава 1. Арифметика над полями Галуа

Определим основные теоретические понятия, а также их свойства, в рамках которых будет строиться наше исследование.

Поле - это множество элементов, для которых определены операции сложения, взятия противоположного значения, умножения и деления с выполнением следующих аксиом:

- Коммутативность сложения.
- Ассоциативность сложения.
- Существование нулевого элемента.
- Существование противоположного элемента.
- Коммутативность умножения.
- Ассоциативность умножения.
- Существование единичного элемента.
- Существование обратного элемента для ненулевых элементов.
- Дистрибутивность умножения относительно сложения.

Простейшим полем является поле рациональных чисел (дробей), однако множество натуральных или целых чисел полями не являются (т.к. не выполняется аксиома о существовании обратных элементов). Хотя названия операций и взяты из арифметики, в общем случае элементы поля не обязательно являются числами, и определения операций не всегда привычные нам арифметические.

Поле, содержащее конечное число элементов, называется конечным полем или полем Галуа и обозначается как *GF(q)*. Для такого поля актуальны понятия порядка и характеристики. Порядок поля - это число его элементов, которое в случае полей Галуа всегда должны являться степенью некоторого простого числа p, т.е. $q = p^n$, где n - произвольное натуральное число (в ином случае не будут выполняться аксиомы поля). Характеристика поля - это наименьшее положительное целое число p, такое, что сумма p

копий единицы равна нулю:$\sum_{i=1}^{n} 1 = n \cdot 1 = 0$. Для полей Галуа порядка p^n характеристикой поля является число p, что показано в [7]. Для задач криптографии, в том числе рассмотренных далее в данной работе, интерес представляют простые поля Галуа, т.е. с порядком, являющимся простым числом, а значит, совпадающим с характеристикой поля. Такие поля также называют полями вычетов или кольцами вычетов по модулю. Далее будем говорить именно о таких полях.

Арифметика над простыми конечными полями представима в виде традиционной арифметики (т.е. арифметических операций сложения и умножения) над множеством натуральных чисел, которая выполняется по модулю порядка поля, т.е. после любой операции мы берем остаток от деления на порядок поля. Приведем пример.

Пусть у нас есть конечное поле *GF*(13). Оно состоит из 13 элементов: от 0 до 12. У него также есть нулевой и единичный элемент: 0 и 1, соответственно. Приведем примеры операций в поле:

- 3+5 *(mod 13)* = 8 *(mod 13)* - всё типично, "*(mod 13)*" означает взятие остатка от деления на 13.
- 7 + 8 *(mod 13)* = 15 *(mod 13)* = 2 *(mod 13)*.
- $5^3 (mod\ 13) = 125\ (mod\ 13) = 8\ (mod\ 13)$.

Поля Галуа чрезвычайно популярны в криптографии и теории кодирования в целом в силу ограниченности числа элементов в реальной работе современных систем передачи информации (включая IT-системы). Это стало возможным благодаря арифметике конечного поля, а также вычислительной простоте операций внутри конечных полей: они выполняются быстрее, чем традиционные арифметические (это частично будет показано далее). Кроме того, в простых полях Галуа выполняется ряд удобных свойств, наподобие малой теоремы Ферма: $\forall a \in GF(p): a^{p-1} = 1\ (mod\ p)$, что позволяет возводить числа в высокие степени чрезвычайно быстро: в работе [8] показано, что вычислительная сложность возведения в степень в конечных полях равна $T_1 = O((log(a))^3)$, где a - показатель степени.

Обобщая, классический набор арифметических операций в конечных полях имеет существенно более низкую вычислительную сложность, чем в классических полях целых или вещественных чисел.

Одновременно с этим, в [8] показано, что задача вычисления дискретных логарифмов в конечных полях вычислительно сложная и решается за время $T_2 = O(p \cdot (log(a))$, т.е. пропорционально порядку поля p.

На этом факте основан ряд криптографических алгоритмов, в том числе протокол Диффи-Хеллмана, рассмотренный ниже.

Основные выводы:

- С использованием теории конечных полей Галуа можно снизить вычислительную сложность ряда операций до квази-логарифмической, что гораздо ниже традиционной арифметики.
- С использованием особенностей операций в конечных полях можно решать ряд криптографических задач, не имеющих решения в традиционной арифметике (на базе этого свойства основан ряд известных криптографических протоколов).
- Все исследования по разработке целевого крипто-протокола будем проводить в полях Галуа в силу их гибкости и вычислительно низкой сложности.

Глава 2. Протокол безопасного обмена на незащищенном канале связи

2.1. Постановка задачи

Пусть имеется n ($n >= 3$) участников обмена данными, не имеющих исходно общего секрета (секретного ключа), а также некоторый незащищенный канал связи, который может быть прослушан потенциальным злоумышленником. Требуется организовать обмен большими ($\sim 2^{10} - 2^{40}$ *бит*) данными между участниками таким образом, чтобы злоумышленник не мог перехватить передаваемые по открытому каналу данные, при условии, что злоумышленник может только читать передаваемые данные, но не может их модифицировать.

Рис. 1. Схема обмена данными по незащищенному каналу связи.

Общая схема протокола защищенного обмена данными между произвольным числом участников:

1. Создание общего секрета, известного всем n участникам, но неизвестного злоумышленнику.
2. Использование симметричного алгоритма шифрования с общим секретным ключом из п.1.

2.2. Базовая схема создания общего ключа

Для организации обмена данными первым создания общего секретного ключа возьмем за основу классический протокол создания общего секрета Диффи-Хеллмана. Он показывает способ создания общего секретного ключа для двух участников и выглядит следующим образом.

Пусть даны два участника A1 и A2.

1. Оба участника договариваются о некоторых двух числах p и g, где p - произвольное простое число высокого порядка. g - некоторое простое натуральное число порядка $\sqrt[2]{p}$ и может быть подобрано также случайным образом. Для максимальной криптостойкости протокола g подбирается, как первообразный корень от p. p и g - несекретные и свободно передаются сторонами, известны злоумышленнику.
2. A1 генерирует случайное простое число a, вычисляет $A = g^a \ (mod\ p)$ и пересылает число A участнику A2.
3. A2 генерирует случайное простое число b, вычисляет $B = g^b \ (mod\ p)$ и пересылает число B участнику A1.
4. A1 получает число B и вычисляет $K = B^a \ (mod\ p) = (g^b)^a \ (mod\ p) = g^{ba} \ (mod\ p)$
5. A2 получает число A и вычисляет $K = A^b \ (mod\ p) = (g^a)^b \ (mod\ p) = g^{ab} \ (mod\ p)$

В итоге, оба участника получили один и тот секретный ключ K, основанный на свойстве коммутативности произведения (в данном случае - показателей степени). При этом операция возведения в степень в конечном поле выполняется за время, линейное относительно показателя степени, в силу чего процесс создания общего ключа является вычислительно быстрой операцией. Одновременно с этим, злоумышленник, обладая числами A и B, не может получить ни общий секретный ключ, ни показатели a и b, т.к. операция вычисления дискретного логарифма в конечном поле имеет экспоненциальную сложность и неразрешима за разумное время (если числа p, a и b выбраны достаточно большими).

Данный известный протокол создания общего ключа применяется в криптопротоколах SSL и TLS при создании защищенного соединения между сайтом и клиентом, на этот сайт заходящим, при условии использования сайтом https протокола. Однако он хорошо работает для схему с двумя участниками обмена. Что же делать, если участников - произвольное количество? К тому же, протокол не описывает однозначно схему генерации чисел p и g.

2.3. Обобщенный алгоритм создания общего ключа

Доработаем алгоритм Диффи-Хеллмана таким образом, чтобы он работал для произвольного числа участников n без потери криптостойкости. Для этого сделаем некоторое обобщение схемы возведения промежуточных ключей в степень и схему пересылки сообщений. Общая идея заключается в том, что на каждом этапе создания секретного ключа i мы пропускаем промежуточные ключи последовательно от первого до последнего участника, кроме i-го (для кого создаётся общий секрет на текущем этапе) с тем, чтобы получить все показатели степени числа g в произведении, кроме i-го, и на последнем шаге - передаём g в степенях секретных показателей всех участников, кроме показателя i $(= a_i)$, участнику i, который у себя внутри (без пересылки кому-либо далее) возводит полученный промежуточный ключ в степень своего секретного показателя a_i.

В итоге, предлагаемый обобщённый алгоритм создания общего секрета будет выглядеть следующим образом:

1. Участник 1 генерирует числа p и g с учётом следующих требований.
    a. $p \in (2^{1023}, 2^{1024} - 1]$ и является простым, другими словами p должно быть 1024-битным простым числом, что в переводе в десятичную систему счисления означает 308-значное число.
    b. $g \in (\sqrt{p}/2;\ \sqrt{p} * 2)$ и тоже является простым (в идеале - первообразный корень по модулю p).
2. Участник 1 передаёт числа p и g оставшимся (n-1) участникам.
3. Каждый участник генерирует собственные случайные числа $a_1, a_2, \ldots, a_n$, при этом порядок данных чисел должен быть не более, чем на 1 порядок ниже p (иначе сложность вычисления дискретного логарифма злоумышленником снижается), но не превосходит p (иначе сложность вычислений участников повышается без роста криптостойкости).
4. Последовательная генерация общего ключа: для каждого i = 1,…, n выполняем следующие шаги:
    a. Генерация общего секрета для участника i: для каждого j = 1,...,n И $j \neq i$ выполняем следующие шаги:
        i. Если j - первый участник вычислений, т.е. ((j = 1) И (i > 1)) ИЛИ ((j = 2) И (i = 1)): участник j вычисляет $A_i^j = g^{a_j} \ (mod\ p)$ и пересылает его участнику (j+1), если $j + 1 \neq i$ и (j+2), если $j + 1 = i$.
        ii. Если j - не первый участник вычислений: участник j получает A_i^{j-1} или A_i^{j-2} (в зависимости от значения i) и вычисляет $A_i^j = (A_i^{j-1})^{a_j} \ (mod\ p)$ и пересылает число A_i^j, в зависимости от условий:
            1. Участнику (j+1), если $(j + 1 \neq i)$ *И* $(j + 1 \leq n)$и переход на шаг 4.a.ii.
            2. Участнику (j+2), если $(j + 1 = i)$ И $(j + 2 \leq n)$и переход на шаг 4.a.ii.
            3. Участнику i, если $(j + 1 > n)$ *ИЛИ* $((j + 1 = i)$ *И* $(i = n))$ - конец всех итераций j и переход на шаг 4.b.
    b. Участник i получает $A_i^n = g^{a_1 \cdot a_2 \cdot \ldots a_{i-1} \cdot a_{i+1} \cdot \ldots \cdot a_n} \ (mod\ p)$и выполняет операцию $K = (A_i^n)^{a_i} = g^{a_1 \cdot a_2 \cdot \ldots a_{i-1} \cdot a_i \cdot a_{i+1} \cdot \ldots \cdot a_n} \ (mod\ p)$, что является общим секретом.
    c. Повторяем этапы 4.a-4.b для всех оставшихся участников i = 1,…, n.

2.4. Общая схема протокола защищенного обмена между произвольным числом участников

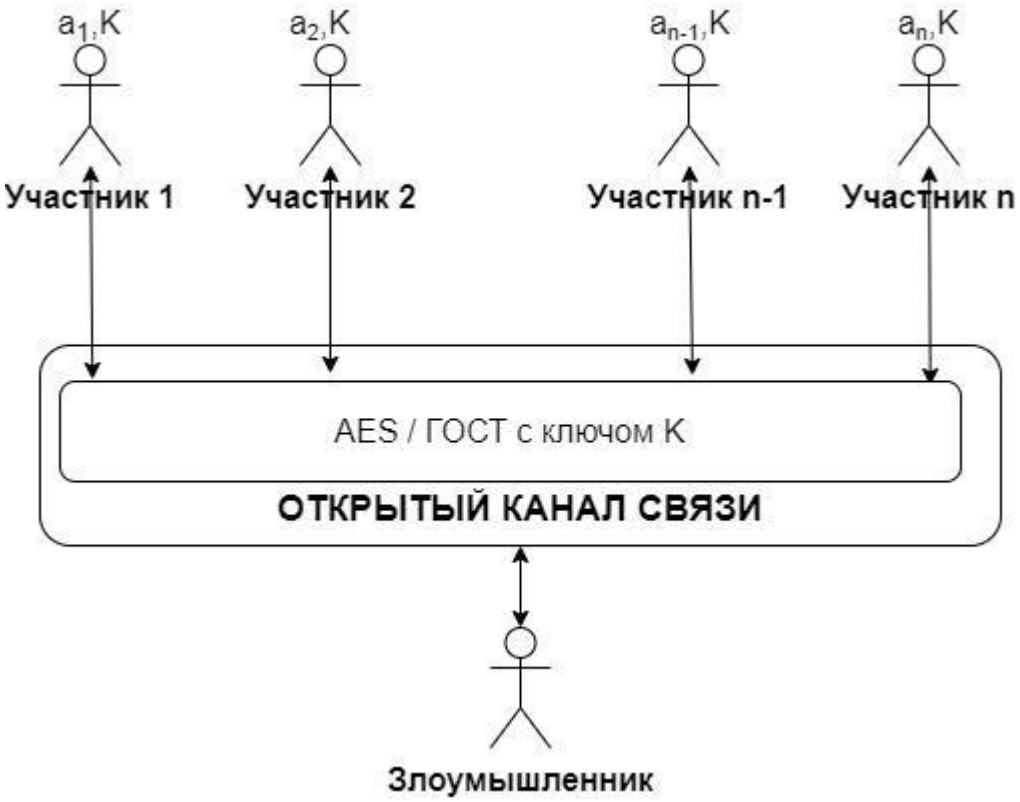

Рис. 2. Общая схема алгоритма защищённого обмена по открытому каналу связи.

Для обмена данными между участниками с использованием полученного общего секрета K следует использовать какой-либо криптостойкий симметричный алгоритм шифрования, основанный на полученном по обобщенному алгоритму Диффи-Хеллмана ключе K длиной 256 бит. Симметричные алгоритмы хороши своей высокой скоростью работы (порядка 4 Гбит/с на современном среднестатистическом 2-ядерном процессоре) и, следовательно, - передачи данных между участниками. Предлагаемые алгоритмы: AES (стандарт симметричного шифрования в США с доказанной криптостойкостью), ГОСТ 28147-89 (стандарт симметричного шифрования в РФ с доказанной криптостойкостью).

Итоги и результаты исследования.

1. Мы обобщили схему Диффи-Хеллмана для получения общего секрета для всех n участников, используя открытый канал связи без компрометации ключа на базе сложности задачи дискретного логарифмирования в конечных полях.
2. Сложность полученного обобщенного алгоритма будет равняться $O(n * n) * T_1$, где T_1 - сложность операции возведения в степень основания g в конечном поле порядка p (приведена в Главе 1 и соответствует квази-логарифмической относительно порядка поля сложности). Таким образом, сложность создания общего секрета квадратично зависит от числа участников n.
3. Мы разработали общую схему протокола защищённого обмена между произвольным числом участников на базе обобщения метода Диффи-Хеллмана с квази-

логарифмической по порядку поля (размеру ключа) сложностью, что решает первую из поставленных задач.

Глава 3. Схема быстрого разделения секрета

3.1. Постановка задачи

Пусть имеется n ($n \geq 3$) участников, которые имеют некоторый общий разделяемый секрет s, где $||s|| < 1024$ бит. Требуется разработать криптографический протокол, для которого верно следующее:

- Любые k участников из n могут получить доступ к s, обмениваясь сообщениями по защищенному каналу связи.
- Никакое подмножество участников в количестве $t < k$ не может восстановить секрет s в том смысле, что для его восстановления потребуется решить вычислительно сложную задачу, не решаемую на современных суперкомпьютерах за разумное время (в том числе это означает, что данное подмножество участников не может получить никакой дополнительной информации, существенно упрощающей поиск s).

При этом мы предполагаем, что среди участников нет злоумышленников, пытающихся саботировать работу протокола (все отправляют друг другу корректные данные).

3.2. Алгоритм разделения малого секрета

В качестве основы для разработки алгоритма разделения секрета возьмем идею интерполяционных многочленов. Идея предлагаемой схемы заключается в том, что для интерполяции многочлена степени (k-1) требуется k точек. К примеру, для задания прямой (многочлен степени 1) достаточно двух точек, для задания параболы (многочлен степени 2) - трех точек, и так далее. Основа криптостойкости данной схемы состоит в том, что интерполяция многочлена степени (k-1) невозможна, если известно число точек, меньшее, чем k.

Для того, чтобы разделить секрет между n участниками таким образом, чтобы восстановить его могли любые k участников, где $k \leq n$, мы “прячем” его в многочлен степени (k-1). Восстановить этот многочлен и исходный секрет можно только по k различным точкам. При этом совершенно неважно, по какому именно подмножеству точек из всего бесконечно возможного их числа. Данная схема основана на следующем утверждении:

Утверждение (гипотеза). По любым k различным точкам всегда можно построить многочлен степени не выше (k-1) и при том только один. Докажем это утверждение.

Существование.

Существование основано на интерполяционных полиномах Лагранжа, которые выглядят следующим образом:

$L(x) = \sum_{i=1}^{k} \quad y_i \cdot l_i(x)$, где $l_i(x)$ - так называемые базисные полиномы, определяемые следующим образом $l_i(x) = \prod_{j=1, j\neq i}^{k} \quad \frac{(x-x_j)}{(x_i-x_j)} = \frac{(x-x_1)}{(x_i-x_1)}\frac{(x-x_2)}{(x_i-x_2)}\ldots\frac{(x-x_k)}{(x_i-x_k)}$. Видим, что порядок $L(x)$равен порядку $l_i(x)$и равен (k-1). При этом $L(x)$ после упрощения и приведения слагаемых может иметь в конечном итоге порядок ниже (k-1).

Действительно, $\forall i: l_i(x_i) = 1$, однако $\forall i\ \forall j \neq i: l_i(x_j) = 0$. Откуда имеем, что для любого i только один базисный многочлен не будет обращаться в 0 в точке x_i и будет в ней равен 1. Получаем, что $\forall i: L(x_i) = y_i l(x_i) = y_i$. Таким образом, мы построили многочлен, удовлетворяющий нашим условиям. Существование доказано.

Единственность.

Предположим существует некоторый отличный от $L(x)$ многочлен $P(x)$ степени (k-1), также проходящий через все точки (x_i, y_i). Тогда рассмотрим многочлен $Q(x) = L(x) - P(x)$. Заметим, что $\forall i = 1,\ldots,k: Q(x_i) = L(x_i) - P(x_i) = y_i - y_i = 0$. Тогда все различные точки x_i будут являться корнями многочлена $Q(x)$ степени (k-1), всего таких точек k. Однако, как известно, ненулевой многочлен степени n может иметь не более n различных корней, откуда следует, что $Q(x)$ является нулевым многочленом. Имеем $Q(x) = L(x) - P(x) = 0 \ => \ L(x) = P(x)$. Единственность доказана.

Количество же различных точек многочлена не ограничено, поэтому мы спокойно можем создать различные точки для всех n участников и любое их подмножество в количестве k сможет однозначно восстановить искомый многочлен $Q(x)$.

Опишем данную схему более формально. Имеется n участников, желающих разделить некоторый малый секрет s, состоящий из двух частей $s = s_1|s_2, где\ ||s_i|| \leq 512$, с доступом по произвольному кворуму k.

Примечание (гипотеза). Благодаря разделению малого секрета s на два (s_1и s_2), мы сокращаем порядок нашего поля Галуа p с 1024 бит до 512 бит, что существенно снижает сложность дальнейших вычислений в данном поле.

Выделим одного особого участника D и назовём его лидером. Схема состоит из двух фаз: фаза разделения секрета и фаза восстановления. На фазе разделения секрета лидер, знающий s, генерирует n долей секрета и посылает их участникам (кроме себя) по защищенному каналу связи, забывая их после. На фазе восстановления секрета любое подмножество из не менее чем k участников, где k - параметр протокола, однозначно восстанавливает секрет, обмениваясь сообщениями по защищенному каналу связи.

Схема фазы разделения секрета:

1. Лидер выбирает некоторое случайное большое простое число p, где $p > max(s_1, s_2)$. Лидер выбирает случайным образом произвольные целые числа $a_1,\ldots,a_{k-2}$, такие что $-p < a_i < p, a_i \neq 0$.
2. Лидер строит многочлен в конечном поле порядка p вида $Q(x) = s_1 + a_1x + \ldots + a_{k-1}x^{k-1}\ (mod\ p)$, где $a_{k-1} = s_2 - s_1 - \sum_{i=1}^{k-2} \quad a_i$.

3. Лидер выбирает случайным образом произвольные целые числа $g_1, \ldots, g_n$, такие что $-p < g_i < p, g_i \neq 0, g_i \neq 1$ и все g_i попарно различны - это аргументы точек каждого участника.
4. Лидер вычисляет значения точек $h_i = Q(g_i)$ и передает каждому участнику i соответствующие точки (g_i, h_i) по защищенному каналу связи, где $i = 1, \ldots, n$.
5. Лидер "забывает" s, все точки (g_i, h_i), кроме своей, а также все a_i, $i = 1, \ldots, n$ и более их не использует.

Схема фазы восстановления секрета:

1. Среди кворума из k участников $i_1, \ldots, i_k$ каким-либо образом выбирается лидер D. Примечание: для простоты дальнейших объяснений переупорядочим участников таким образом, чтобы лидеру соответствовал номер i_k.
2. Оставшиеся (k-1) участников отправляют лидеру свои точки $(g_{i_1}, h_{i_1}), \ldots, (g_{i_{k-1}}, h_{i_{k-1}})$.
3. Лидер, имея k точек на плоскости $(g_{i_1}, h_{i_1}), \ldots, (g_{i_k}, h_{i_k})$, может однозначно восстановить многочлен $Q(x)$, что следует из доказанной выше теоремы. В качестве базовой схемы построения многочлена выберем показанный выше в доказательстве существования интерполяционный многочлен Лагранжа.
4. Лидер вычисляет $Q(0) = s_1 + \sum_{i=1}^{k-1} a_i \cdot 0 = s_1$, а также $Q(1) = s_1 + \sum_{i=1}^{k-2} a_i \cdot 1^i + a_{k-1} \cdot 1^{k-1} == s_1 + \sum_{i=1}^{k-2} a_i + s_2 - s_1 - \sum_{i=1}^{k-2} a_i = s_2$ и пересылает всем участникам секрет $s = s_1 | s_2$.

3.3. Криптостойкость предложенного алгоритма (результаты и выводы).

Подведем итоги проведенного исследования и проанализируем криптостойкость разработанного алгоритма.

Гипотеза. Пусть у нас есть кворум из (k-1) участника и (k-1) точки, соответственно. Тогда секретом s может быть любой элемент поля $GF(p)$ с равной вероятностью и у нас не будет дополнительной информации, позволяющий вычислить секрет s.

Допустим у нас есть кворум из (k-1) участника. Мы имеем (k-1) точек, однако многочлен степени (k-2), построенный по ним, не даст возможность вычислить секрет s, т.к. нам неизвестен ни один из коэффициентов искомого многочлена $a_0, \ldots, a_{k-1}$, и значения данного многочлена в точках 0 и 1 (равные нашим s_1 и s_2, соответственно) не будут совпадать со значениями в этих же точках корректного многочлена $Q(x)$.

Одновременно, для построения многочлена степени k, имея (k-1) корректных точек, нам нужна ещё одна точка. Пусть это будет точка с аргументом $x_k = 0$. В силу утверждения выше о возможности построения по любым k различным точкам единственного многочлена степени (k-1), значение y_k может принимать любое значение в поле $GF(p)$ и при этом мы не сможем проверить корректность построенного многочлена. Таким образом, вероятность построения корректного многочлена и раскрытия секрета в случае наличия произвольных (k-1) корректных точек, равна $1/p$, т.е. есть в результате интерполяции по (k-1) точке секретом может быть любой элемент поля с равной вероятностью. При этом попытка полного перебора

всех возможных точек не позволит злоумышленнику получить дополнительную информацию о секрете *s*, что и доказывает нашу гипотезу.

Ограничения предложенной схемы:

1. **Надежность лидера:** по умолчанию в схеме предполагается, что тот, кто генерирует и раздаёт точки, надежен, что не всегда верно.
2. **Честность участников:** в схеме нет проверки корректности точек, полученных от участников: участвующий в фазе восстановления участник не может достоверно сказать, что его точка подлинна (лидер передал верную точку, или же она не была искажена злоумышленником при передаче): многочлен $Q(x)$ строится на любом множестве точек: нет механизма проверки достоверности ни точек, ни полученного с их использованием секрета *s*.

Решение данных проблем выходит за рамки данной работы.

Таким образом, нам удалось решить вторую из поставленных задач и разработать алгоритм решения *(k,n)*-пороговой схемы, работающий за квази-линейное время и обладающий необходимой криптостойкостью.

Глава 4. Общий алгоритм протокола разделения большого секрета на открытом канале связи

На основе разработанного обобщенного алгоритма Диффи-Хеллмана, а также предложенного алгоритма (*k,n*)-пороговой схемы на базе интерполяционных многочленов Лагранжа синтезируем общую общую схему целевого криптопротокола с “большим” секретом.

Пусть у нас имеется *n* участников с порогом доступа *k* без общего секрета, некоторая секретная информация *SS*, для которой верно: $2^{10} < ||SS|| < 2^{45}$ и открытый канал связи. Тогда изобразим общую схему следующим образом (рис. 3).

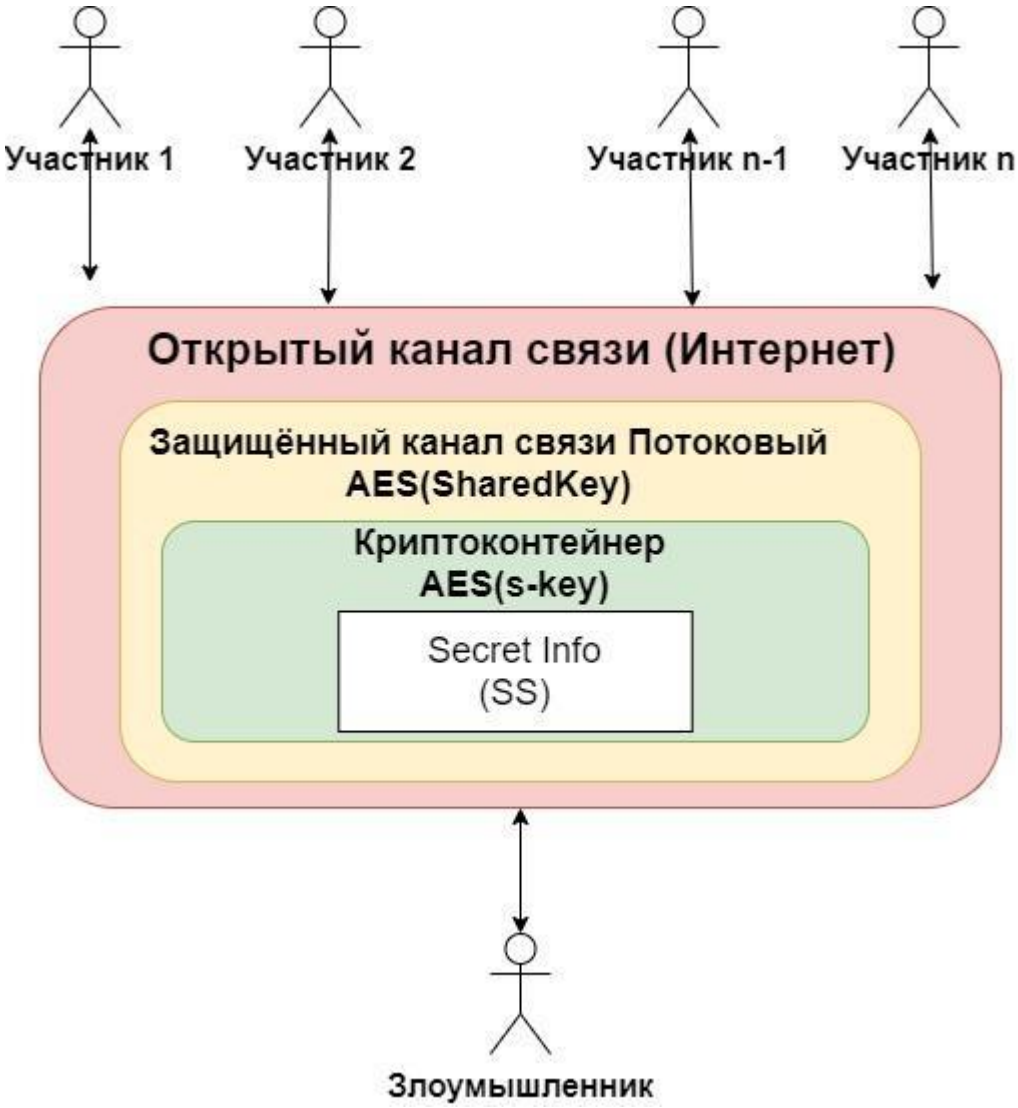

Рис. 3. Общая схема криптосистемы с разделяемым секретом на открытом канале связи.

Схема работы алгоритма / криптопротокола выглядит следующим образом:

1. Метод создания защищенного канала связи:
   a. Собираются все n (для разделения секрета) / k (для восстановления секрета) участников, между которыми разделяется секрет.
   b. Участники генерируют общий ключ SharedKey длиной 256 бит на основе обобщенного алгоритма создания общего секрета из раздела 2.3.
   c. Участники создают между собой защищенный канал связи на основе симметричного блокового алгоритма шифрования AES с ключом SharedKey. (раздел 2.4).

2. Метод разделения секрета (если секрет еще не “спрятан”):
   a. Участники создают защищенный канал связи между собой (см. шаги п.1).
   b. Участники среди всех выбирают лидера.
   c. Лидер генерирует случайным образом ключ *s-key* длиной 256 бит и разделяет его на 2 равные по длине части: s_1 и s_2 (128 бит каждый).

d. Лидер шифрует алгоритмом AES секретную информацию *SS* (произвольной длины), используя сгенерированный в п.2.c ключ *s-key*.
e. Лидер, используя защищенный канал связи, разделяет ключ *s-key* по “Схеме разделения секрета” из раздела 3.2 и пересылает доли участникам.

3. Метод восстановления секрета (если секрет уже “спрятан”):
   a. Участники создают защищенный канал связи между собой (см. шаги п.1).
   b. Участники среди всех выбирают лидера.
   c. Лидер совместно с участниками восстанавливает секретные доли s_1 и s_2 по “Схеме восстановления секрета” из раздела 3.2.
   d. Лидер восстанавливает ключ *s-key*$= s_1|s_2$.
   e. Лидер дешифрует алгоритмом AES секретную информацию *SS* (произвольной длины), используя восстановленный ключ *s-key* и использует её по назначению.

Таким образом, мы построили искомый криптопротокол (криптосистему), позволяющий получить доступ к секрету произвольной длины доступ при наличии кворума *k* из *n* участников и базирующийся на открытом канале связи. Данный криптопротокол основан на разработанных в предыдущих разделах алгоритмах, где доказана их высокая криптостойкость и квази-логарифмическая сложность.

Заключение

В результате проведённого исследования, анализа существующих и полученных результатов имеем следующее (выводы):

1. Разработан алгоритм создания защищённого канала связи между произвольным числом участников, не имеющих общего секрета, на открытом канале связи с высокой криптостойкостью.
2. Разработан инновационный с научной точки зрения вычислительно эффективный метод реализации (*k,n*)-пороговой схемы для секретной информации между произвольными участниками (с квази-логарифмической сложностью относительно порядка поля).
3. Разработан полноценный криптографической протокол реализации пороговой схемы доступа на базе открытого канала связи с высокой криптостойкостью и квази-логарифмической сложностью, однако обладающих ограничениями, связанными с доверием участников друг другу.
4. Искомая цель построения целевой криптосистемы достигнута, поставленные задачи выполнены.

<u>Разработанный криптопротокол может применяться в следующих областях:</u>

1. Информационный крипто-сейф с мультидоступом - когда нужно “быстро” получить доступ к защищенной информации произвольного размера с использованием кворума из участников.

2. Информационные системы с многопользовательской авторизацией - когда для получения доступа к какой-либо части системы требуется подтверждения от кворума из участников. Разделяемый секрет в этом случае будет являться ключом к доступу в нужную часть системы (в частности, это удобно, если он является приватным ключом с проверкой по публичному сертификату).
3. Методы стеганографии, когда нужно “незаметно” спрятать какую-либо информацию в существующем контейнере (например, в изображении).

Перспективы дальнейших исследований заключаются в доработке алгоритма для случая, когда среди участников имеются злоумышленники, желающие скомпрометировать работу криптосистемы путём подмены передаваемых данных в процессе восстановления секрета, а также для случая, когда внешний злоумышленник может подменять передаваемую информацию.

Литература

1. P. Luo, A. Yu-Lun Lin, Z. Wang, M. Karpovsky. Hardware Implementation of Secure Shamir's Secret Sharing Scheme (англ.) // HASE '14 Proceedings of the 2014 IEEE 15th International Symposium on High-Assurance Systems Engineering : Proceeding. — Washington, DC, USA: IEEE Computer Society, 2014. — P. 193—200. — ISSN 978-1-4799-3466-9. — doi:10.1109/HASE.2014.34.
2. Ulutas M., Ulutaş G., Nabiyev V. V. Medical image security and EPR hiding using Shamir's secret sharing scheme (англ.) // J. Syst. Software — Elsevier, 2011. — Vol. 84, Iss. 3. — P. 341–353. — ISSN 0164-1212; 1873-1228 — doi:10.1016/J.JSS.2010.11.928
3. S. Salim, S. Suresh, R. Gokul, Reshma S. Application of Shamir Secret Sharing Scheme for Secret Data Hiding and Authentication (англ.) // International Journal of Advanced Research in Computer Science & Technology : Journal. — 2014. — Vol. 2, no. 2. — P. 220—224. — ISSN 2347-8446.
4. Шнайер Б. 23.2 Алгоритмы разделения секрета. Векторная схема // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — С. 589. — 816 с. — 3000 экз. — ISBN 5-89392-055-4.
5. A generalization of Mignotte’s secret sharing scheme. Proceedings of the 6th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (2004).
6. Шнайер Б. Схема Асмута-Блума // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — С. 589—590. — 816 с. — 3000 экз. — ISBN 5-89392-055-4.
7. Лидл, Нидеррайтер, 1988, с. 66.
8. Крэндалл Ричард, Померанс Карл. Простые числа: Криптографические и вычислительные аспекты / Под ред. и с предисл. В. Н. Чубарикова.. — М.: УРСС:: Книжный Дом «ЛИБРОКОМ», 2011. — 664 с. — ISBN 978-5-453-00016-6, 978-5-397-03060-2.