УДК 004.056

РАЗРАБОТКА КРИПТОСИСТЕМЫ С РАЗДЕЛЯЕМЫМ СЕКРЕТОМ НА ОТКРЫТОМ КАНАЛЕ СВЯЗИ

Немойкина Ева Владиславовна
Ханты-Мансийский автономный округ-Югра, г. Сургут, МБОУ СОШ № 26, 11 класс
Научный руководитель: Лысяк Наталья Николаевна, ХМАО-Югра, г. Сургут, МБОУ СОШ № 26, учитель математики

Введение

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

Обе проблемы особо актуальны в современном мире в связи с широким распространением открытых электронных каналов передачи информации, всемирной информатизацией и распространением задачах многопользовательской авторизации [1], также стеганографии [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], однако сушествующие алгоритмы имеют либо достаточно высокую сложность реализации, либо высокую вычислительную трудоемкость.

Целью данной работы является разработка криптографического протокола обмена данными, при котором любые k участников из n ($n > 2$), собравшись в кворум, могут получить доступ к “большому” секрету SS ($2^{10} < ||□□|| < 2^{45}$, где $||□□||$ – битовый размер информации), 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).

Протокол безопасного обмена между произвольным числом участников на незащищенном канале связи

Пусть имеется n ($□ > 2$) участников обмена данными, не имеющие общего секретного ключа, и могут обмениваться данными, используя только открытый канал связи.

Требуется организовать обмен большими 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.

Для организации обмена данными первым создания общего секретного ключа возьмем за основу классический протокол создания общего секрета Диффи-Хеллмана для 2 участников и доработаем его таким образом, чтобы он работал для произвольного числа участников $n > 2$ 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 (для i-го участника создаётся общий секрет на текущем этапе) мы пропускаем промежуточные ключи последовательно от первого до последнего участника, кроме i-го, 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 ($= □_□$), участнику i, который у себя внутри (без пересылки кому-либо далее) возводит полученный промежуточный ключ в степень своего секретного показателя $□_□$.

Сложность разработанного обобщенного алгоритма равна $□(□ * □) * □_1$, где $□_1$ – сложность операции возведения в степень основания g в конечном поле порядка p (квази-логарифмическая относительно порядка поля).

Для обмена данными между участниками с использованием полученного общего секрета K следует использовать какой-либо криптостойкий симметричный алгоритм шифрования с использованием полученного ключа K длиной 256 бит. Схема обмена показана на рисунке 1.

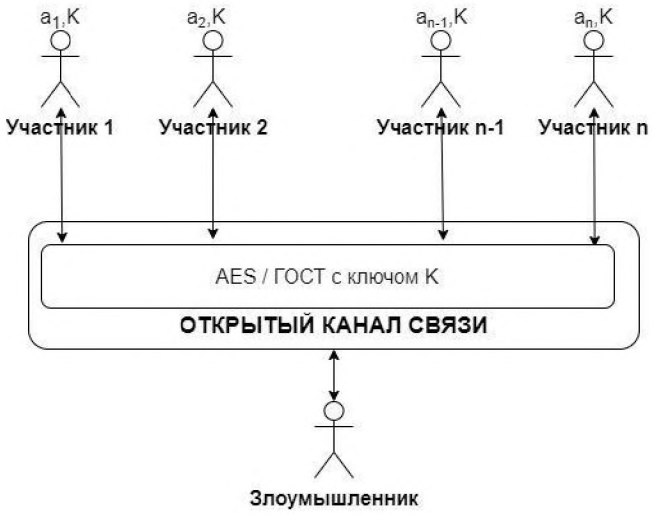

Рис. 1. Общая схема алгоритма защищённого обмена по открытому каналу связи

Таким образом, 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 и производительностью симметричных криптоалгоритмов, что решает первую из поставленных задач.

Схема быстрого разделения секрета и доступа по кворуму

Пусть имеется n ($\square > 2$) 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 качестве основы для разработки алгоритма разделения секрета возьмем идею интерполяционных многочленов Лагранжа. Для того, чтобы разделить секрет между n участниками таким образом, чтобы восстановить его могли любые k участников, мы "прячем" его в многочлен степени (k-1). Восстановить этот многочлен и исходный секрет можно по произвольным k различным точкам.

Изначально мы должны провести т.н. фазу разделения секрета, на которой мы генерируем наш многочлен и прячем наш малый секрет s в его свободный член. После этого для каждого участника генерируется уникальная точка на базе данного многочлена.

Для восстановления секрета произвольные k участников собирают свои k точек и строят многочлен по классической схеме интерполяции Лагранжа (1).

$$\square(\square) = \sum_{\square=1}^{\square} \square_{\square} \cdot \square_{\square}(\square), \text{ где } \square_{\square}(\square) = \prod_{\square=1,\square\neq\square}^{\square} \frac{(\square-\square_{\square})}{(\square_{\square}-\square_{\square})} = \frac{(\square-\square_1)}{(\square_{\square}-\square_1)}\frac{(\square-\square_2)}{(\square_{\square}-\square_2)}\dots\frac{(\square-\square_{\square})}{(\square_{\square}-\square_{\square})} \quad (1)$$

Значение полученного многочлена в точке 0 будет равняться малому секрету s.

В результате исследований криптостойкости в работе показано, что если у нас есть кворум из (k-1) участника и (k-1) точки, соответственно, то секретом s может быть любой элемент поля $GF(p)$ с равной вероятностью и у нас не будет дополнительной информации, позволяющий вычислить секрет s.

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: $2^{10} < ||\square\square|| < 2^{45}$ и открытый канал связи. Тогда изобразим общую схему следующим образом (рисунок 2).

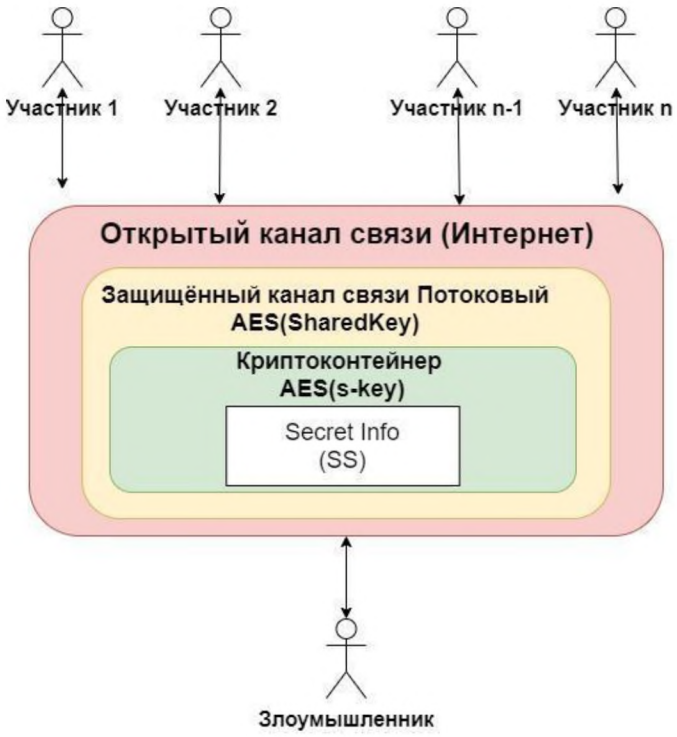

Рис. 2. Общая схема криптосистемы с разделяемым секретом на открытом канале связи

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: $□_1$ и $□_2$ (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 $□_1$ и $□_2$ по “Схеме восстановления секрета” из раздела 3.2.
   d. Лидер восстанавливает ключ *s-key*= $□_1|□_2$.
   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 работы – исследованиям, анализу существующих и полученных результатов, разработаны:

1. алгоритм создания защищённого канала связи между произвольным числом участников, не имеющих общего секрета, на открытом канале связи с высокой криптостойкостью;

2. 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. 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.

Список литературы:

1. Luo P., Yu-Lun Lin A., Wang Z., Karpovsky M. Hardware Implementation of Secure Shamir's Secret Sharing Scheme // 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. 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 // J. Syst. Software.Elsevier, 2011. Vol. 84, Iss. 3. P. 341-353.doi:10.1016/J.JSS.2010.11.928
3. Salim S., Suresh S., Gokul R., Reshma S. Application of Shamir Secret Sharing Scheme for Secret Data Hiding and Authentication // International Journal of Advanced Research in Computer Science & Technology: Journal. 2014. Vol. 2, no. 2. P. 220-224.
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. M.: Триумф, 2002. С. 589.
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. M.: Триумф, 2002. С. 589-590.