***А.В. АЛЕКСАНДРОВ***, к.ф-м.н. доцент каф. ИЗИ;
***А.Д. МЕТЛИНОВ***, студент гр. КЗИ-108.

# ПОСТРОЕНИЕ ПРОТОКОЛА С «ОБЩЕЙ ПАМЯТЬЮ» НА ОСНОВЕ SMT / SMT LSS WITH MEMORY

Рассмотрена предметная область поставленной задачи, произведен сбор необходимой информации для получения нужных навыков в данной разработке. Собрана и проанализирована информация о схеме разделения с возможностью восстановления секрета при поврежденных долях, эффективной раундовой схеме абсолютно безопасной передачи сообщений, теории SMT и задаче об укладке рюкзака. Произведено рассмотрение схемы практически безопасной передачи сообщений - LSS (1-раунд, n-каналов) на основе работ К. Куросавы и К. Сузуки в данной области. Даны полные ее теоретическое и математическое описания. Произведена реализация программного обеспечения для поиска наименьшего пути между двумя вершинами произвольного графа.

Ключевые слова: СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА, ПРОТИВОДЕЙСТВИЕ ЗЛОУМЫШЛЕННИКАМ, НЕЗАЩИЩЕННЫЕ КАНАЛЫ, ЭФФЕКТИВНОСТЬ СХЕМ РАЗДЕЛЕНИЯ, ЗАЩИЩЕННАЯ ПЕРЕДАЧА, ЗАДАЧА ОБ УКЛАДКЕ РЮКЗАКА, SMT.

1 табл., 11 источников.

Considered the subject area of the task made gathering the necessary information to get the necessary skills in this development. Collected and analyzed information about general error decodable secret sharing scheme, round-efficient perfectly secure message transmission scheme against general adversary, SMT theory and the problem of packing a backpack. Performed considered almost secure - LSS (1-round, n-channel) message transmission scheme based on work of K. Kurosawa and K. Suzuki in the field. Given its full theoretical and mathematical description. Made realization of software to find the smallest path between two vertices of a graph.

Keywords: SECRET SHARING SCHEMES, COUNTERING AN ADVERSARY, UNPROTECTED CHANNELS, EFFICIENCY SEPARATION SCHEMES, SECURE TRANSMISSION, THE PROBLEM OF PACKING A BACKPACK, SMT.

1 table, 11 sources.

Объектами исследования данной работы являются схемы безопасной передачи сообщений, теория безопасной передачи сообщений – SMT (secure message transmission), современная модель безопасности Долева-Яо и задача об укладке рюкзака.

Цель работы – теоретическое рассмотрение схемы практически безопасной передачи сообщений (1-раунд, n-каналов) на основе работ К. Куросавы и К. Сузуки в данной области; разработка программного обеспечения, осуществляющего поиск минимального пути между двумя вершинами произвольного графа (необходимо для дальнейших наработок – реализации протокола обмена сообщениями на основе исследуемой практически безопасной схемы передачи сообщений); теоретическое рассмотрение SMT, современной модели безопасности Долева-Яо и задачи об укладке рюкзака.

В процессе разработки темы проводилось теоретическое рассмотрение отдельных криптостойких схем разделения секрета (модификации задачи об укладке рюкзака, схема разделения с возможностью восстановления при поврежденных

долях, эффективная раундовая схема абсолютно безопасной передачи сообщений и т.п.).

В конечном итоге рассмотрены криптостойкие схемы разделения секрета, переведены и изучены наиболее значимые работы в данной области К. Куросавы и К. Сузуки, реализовано небольшое программное обеспечение, рассмотрена теория SMT, современной модели безопасности Долева-Яо и задачи об укладке рюкзака.

Эффективность схем разделения секрета определяется алгоритмом работы дилера, количеством всех долей, используемых в схеме разделения, количеством долей и участников, необходимых для восстановления секрета и т.п. Эффективность алгоритма формирования долей определяется высоким быстродействием, низкими требованиями к ресурсам системы и криптостойкостью. Эффективность задачи об укладке рюкзака определяется возможностью разделения секрета на доли и их упаковки с помощью заданных «весов» и количеством «весов» и дополнительных переменных, передаваемых по каналам связи.

На первом этапе выполнения данной работы была рассмотрена общая теория практически безопасной передачи сообщений – SMT. Произведено сравнение процесса передачи сообщений при использовании небезопасного протокола обмена информацией - SMTP и протокола практически безопасной передачи сообщений - SMT. SMT в первую очередь заботиться о безопасности процесса самой передачи, с учетом того, что каналы, по которым она происходит, надежными не являются. По сути SMT используется для реализации конфиденциальной передачи сообщений. Подобная передача реализуется в рамках абсолютной и практически абсолютной секретности.

Предположим, что мы имеем секрет S (поделенный на определенное количество долей) определенный в поле F (поле Галуа GFp, где p>>1). Сам злоумышленник имеет возможность и контролирует каналы передачи для перехвата долей секрета. Тогда при использовании SMT получаем:

- в случае абсолютной секретности – перехват одной (любой) из долей не дает никакой дополнительной информации о значении секрета S. При этом все варианты значений $p(Si) = 1/p$ – равновероятны для всех долей секрета.

- в случае практически абсолютной секретности – перехват одной (любой) из долей дает некоторую (незначительную) информацию. При этом все варианты значений p(Si) > 1/p – практические равновероятны для всех долей секрета (в числителе вместо единицы могут появляться другие коэффициенты – 3, 5, 7, 10, но само p принимает огромные значение).

На втором этапе были разработаны приблизительные алгоритмы шифрования и дешифрования, которые в дальнейшем будут усовершенствованы и использованы при реализации протокола SMT LSS с общей памятью.

В качестве алгоритма алгоритмов шифрования и дешифрования могут использоваться самые различные алгоритмы. При построении протокола безопасной передачи сообщений с «обшей памятью» будет использоваться алгоритм шифрования, в основе которого будет лежать криптографическая задача об укладке рюкзака и ее модификации. Теоретический пример с ее использованием:

- имеются отправитель сообщения, его получатель и каналы связи (один из них надежный – для передачи ключевой последовательности e1,e2…ek);
- отправитель особым образом разбивает сообщение (секрет) S на определенное количество долей – S1, S2…Sk;
- выбираются коэффициенты e1,e2…ek – их значения либо 0 – доля не включена в значение S, либо 1 – доля секрета включена в значение S;
- вычисляется значение S как сумма произведений всех Si и ei, если секрет невозможно представить данной суммой – в конце к общей сумме добавляют переменную Δ для приведения ее к необходимому значению;
- получателю отправляется значения Si и значения всех ei, при необходимости Δ.

На третьем этапе произведено теоретическое рассмотрение современной модели безопасности Долева-Яо. Описаны возможности злоумышленника, который непосредственно имеет доступ к каналам передачи сообщений и может их все контролировать (за исключением абсолютно надежных). Аналогично в рамках данной теории рассмотрены ограничения, которые накладываются на злоумышленника, так как он не является всемогущим.

Работа Долева-Яо является первой значительной работой в области анализа криптографических протоколов. Применение формальных методов означает введение некоторых абстракций для описания рассматриваемых свойств системы. Модель Dolev-Yao является абстракцией криптографических операций протокола защиты. Фактически эта модель явилась первой формализацией модели злоумышленника.

Работа является значительной в том смысле, что она была первой формальной моделью, в которой допускалось параллельное выполнение анализируемого протокола, криптографические алгоритмы рассматривались как черные ящики, подчиняющиеся ограниченному набору алгебраических свойств (например, операции кодирования и декодирования сводят друг друга на нет), и которая включала злоумышленника, способного читать, модифицировать и уничтожать информацию и, возможно, также управлять некоторыми легальными участниками системы.

На четвертом этапе работы было произведено теоретическое рассмотрение криптографической задачи об укладке рюкзака (ее модификаций). Алгоритм рюкзака — первый алгоритм для обобщённого шифрования с открытым ключом. Разработан Ральфом Мерклом и Мартином Хеллманом. Идея в том, что сообщение шифруется как решения набора задачи о ранце. Предметы выбираются с помощью блока открытого текста, длина блока равна количеству предметов. Биты открытого текста соответствую ценности предметов.

Для шифрования текст разбивают на блоки, по длине равные числу предметов. Считается, что единица указывает на наличие предмета в рюкзаке, а ноль на его отсутствие. Суммируя вес предметов, получаем шифр для каждого отдельного блока.

Таблица 1. Пример получения шифротекста.

| Открытый текст | 1 1 1 1 1 0 | 0 0 1 1 0 0 | 0 0 0 0 0 0 | 0 0 0 0 0 1 |
|---|---|---|---|---|
| Вещи в рюкзаке | 3 4 6 7 10 11 | 3 4 6 7 10 11 | 3 4 6 7 10 11 | 3 4 6 7 10 11 |
| Шифротекст | 3 + 4 + 6 + 7 + 10 = 30 | 6 + 7 = 13 | 0 | 11 |

На пятом, заключительном этапе было реализовано программное обеспечение для поиска наименьшего пути между двумя вершинами произвольного графа. В

дальнейшем планируется работа над практической реализацией полноценного протокола обмена информацией с «общей памятью» на основе схемы практически безопасной передачи сообщений (1-раунд, n-каналов) - SMT и задачи об укладке рюкзака. Выбор платформы для реализации осуществлялся из возможности работы с очень длинными числами, работы с сетью, из личных предпочтений и т.п.

## Литература


1. *Kurosawa Kaoru*, General Error Decodable Secret Sharing Scheme and Its Application, IEEE Trans. Inf. Theory, vol. IT-57, pp. 6304-6309, Sept. 2011.

2. *Kurosawa Kaoru, Suzuki Kazuhiro*, Almost Secure (1-Round, n-Channel) Message Transmission Scheme, Information Theoretic Security, Lecture Notes in Computer Science, Volume 4883. Springer-Verlag Berlin Heidel-berg, 2009, p. 99.

3. *D.Dolev, C.Dwork, O.Waarts, M.Yung*: Perfectly Secure Message Transmission. J. ACM 40(1): pp.17- 47 (1993).

4. *W. Ogata, K. Kurosawa, D. Stinson*: Optimum Secret Sharing Scheme Secure against Cheating. SIAM J. Discrete Math. 20(1): 79-95 (2006).

5. *K. Srinathan, A. Narayanan, C. Pandu Rangan*: Optimal Perfectly Secure Message Transmission. CRYPTO 2004: 545-561.

6. *Ананий В. Левитин* Глава 3. Метод грубой силы: Задача о рюкзаке // Алгоритмы: введение в разработку и анализ. — М.: «Вильямс», 2006. — С. 160-163.

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

8. *Черемушкин А.В.* Криптографические протоколы: основные свойства и уязвимости. М.: 2009, 36с.

9. *К. Шеннон.* Работы по теории информации и кибернетике. // ИИЛ, Москва 1963, 829с.

10. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си // М.: "Триумф", 2002.

11. *Под редакцией Ященко.* Введение в криптографию. Новые математические дисциплины. // МЦНМО Санкт-Петербург, 2001, 288с.