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

ПОСТРОЕНИЕ АЛГОРИТМА ПЕРЕДАЧИ СООБЩЕНИЙ С «ОБЩЕЙ ПАМЯТЬЮ» НА ОСНОВЕ SMT LSS. ОРГАНИЗАЦИЯ СТЕГАНОКАНАЛА В SMT / CONSTRUCTION TRANSMISSION'S ALGORITHM WITH "MEMORY" BASED ON SMT LSS. ORGANIZATION OF THE SG-CHANNEL AT SMT

Собрана и проанализирована информация о схеме практически безопасной передачи сообщений, теории SMT и задаче об укладке рюкзака. Произведено теоретическое рассмотрение схемы практически безопасной передачи сообщений - LSS (1-раунд, n-каналов) на основе работ К. Куросавы и К. Сузуки в данной области. Предложена математическая реализация вариации алгоритма безопасной передачи сообщений на основе схемы SMT и задачи об укладке рюкзака. Приведено три различных математических примера реализации данного алгоритма. Произведено теоретическое рассмотрение стеганографических методов сокрытия информации. Произведено теоретическое рассмотрение модели TCP-стегосистемы.

Ключевые слова: СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА, СТЕГАНОГРАФИЯ, АЛГОРИТМ ПЕРЕДАЧИ, СОКРЫТИЕ ИНФОРМАЦИИ, ОБЩАЯ ПАМЯТЬ, ЗАДАЧА ОБ УКЛАДКЕ РЮКЗАКА, SMT.
17 источников.

Collected and analyzed information about the scheme is almost secure messaging SMT theory and the problem of packing a backpack. Performed a theoretical analysis schemes almost Message Security - LSS (1-round, n-channel) based on work of K. Kurosawa and K. Suzuki in this field. Proposed a mathematical algorithm realization of variations of secure messaging scheme based on SMT and the problem of packing a backpack. Given three different mathematical example of realization of this algorithm. Performed a theoretical analysis of steganographic techniques for hiding information. Performed a theoretical analysis model TCP-stegosystem.

Keywords: SECRET SHARING SCHEMES, STEGANOGRAPHY, TRANSMISSION'S ALGORITHM, INFORMATION'S HIDING, SHARED MEMORY, THE PROBLEM OF PACKING A BACKPACK, SMT.
17 sources.

Объектами исследования данной работы являются математический алгоритм передачи сообщений с «общей памятью» на основе схемы SMT LSS и процесс организации стеганоканала в SMT.

Цели работы – теоретическое рассмотрение схемы практически безопасной передачи сообщений (1-раунд, n-каналов) на основе работ в данной области К. Куросавы и К. Сузуки; теоретическое рассмотрение SMT; теоретическое рассмотрение задачи об укладке рюкзака и ее модификаций; построение вариации алгоритма безопасной передачи сообщений на основе схемы SMT и задачи об укладке рюкзака; приведение математических примеров реализации данного алгоритма; теоретическое рассмотрение стеганографических методов сокрытия информации и теоретическое рассмотрение модели TCP-стегосистемы.

В процессе разработки темы проводилось теоретическое рассмотрение отдельных модификаций задач об укладке рюкзака, работ Лагариаса и Одлыжко по реализации атак на рюкзачные криптосистемы, работ по влиянию коэффициента

плотности укладки рюкзака на успех проведения атаки на рюкзачную криптосистему, стеганографических методов сокрытия информации.

В конечном итоге приведены алгоритм математической реализации передачи сообщений с «общей памятью» на основе схемы SMT LSS, математические примеры реализации данного алгоритма, выявлена зависимость успеха проведения L^3-атаки на рюкзачную криптосистему от коэффициента плотности укладки рюкзака, рассмотрены стеганографические методы сокрытия информации.

На первом этапе выполнения данной работы была рассмотрена общая теория практически безопасной передачи сообщений – SMT. Известно, что схема абсолютно безопасной (1-раунд, n-каналов) передачи сообщений (MT) существует только тогда, когда $n \geq 2t + 1$, где t – число каналов, который контролирует противник.

Модель схемы (r-раундов, n-каналов) передачи сообщений была введена Долевым. В этой модели, где n – число каналов между отправителем и получателем. Отправитель хочет послать секрет s получателю за r-раундов, причем быть уверенным в безопасности и надежности s. Противник A может перехватывать сообщения, посылаемые через t каналов из n. Можно сказать, что схема (r-раундов, n-каналов) передачи сообщений абсолютно t-безопасна, если A не имеет никакой информации о секрете s (абсолютная безопасность) и получатель может корректно восстановить $s' = s$ (абсолютная надежность), при наличии любого противника A, который имеет бесконечные ресурсы и может влиять на работу t-каналов.

Под надежностью SMT LSS понимается, что получатель всегда при декодировании получит корректное значение секрета. Под абсолютной безопасностью понимается, что противник не может получить и не получает никакой информации о секрете s.

Далее были отмечены существующие (выявленные Куросавой и Сузуки) в данной схеме проблемы отправителя, безопасности и надежности.

На втором этапе работы было определено общее описание модели SMT LSS. Любая схема SMT всегда состоит из пары алгоритмов (кодирование и декодирование) определенных следующим образом. Пусть S – множество секретов.

Алгоритм кодирования - это вероятностный алгоритм шифрования, который получает секрет s ∈ S на входе, а не выходе получается шифрованный текст (x1…xn), где xi – сообщение переданной через i-ый канал.

Алгоритм декодирования - это детерминированный алгоритм расшифровки, который берет принимаемый шифрованный текст (x'1…x'n) и на выходе получает s' ∈ S или ошибку декодирования.

На третьем этапе работы было разработано само математическое описание вышеупомянутого алгоритма передачи сообщений с «общей памятью» на основе схемы SMT LSS:

1. Первым делом между отправителем и получателем необходимо организовать (создать) ту самую «общую память», путем информационного обмена между ними определенными документами с использованием схемы разделения секрета – SMT LSS.

2. При организации передачи этих документов между отправителем и получателем для начала необходимо понимать, нужна ли их секретность при передаче. Ответ на этот вопрос зависит от факта наличия (отсутствия) контролирования злоумышленником каналов передачи сообщений между отправителем и получателем. Если есть полная уверенность, что каналы безопасны - разумно не применять лишних алгоритмов для передачи данных документов. Но такой случай исключительная редкость, так как злоумышленник постоянно старается контролировать как можно большее число доступных каналов связи. В другом случае, когда секретность передачи сообщений нужна, необходимо использовать схему разделения, в данном случае – SMT LSS. Однако можно обойтись и менее сложным алгоритмом передачи – методом голосования – опять же, когда полная секретность передачи не нужна.

В подобных системах для повышения верности приема используется многократная передача кодовых комбинаций – метод голосования.

Многократная передача кодовых комбинаций является наиболее просто реализуемым способом повышения достоверности при передаче сообщений между отправителем и получателем, когда $n > 3t + 1$ (n-общее число каналов связи, t-число

каналов, которые контролирует злоумышленник). Пусть передается буква А, число повторений возьмем равным пяти. Если на приемном конце имеем АБААС (буква А исказилась 2 раза, превратившись соответственно в Б и С), то выносится решение о том, что передавалась буква А, поскольку в последовательности из пяти букв она встречалась наиболее часто. Если в принятой последовательности ни одна из букв не повторяется, то принятое сообщение ликвидируется (стирается).

Главный недостаток такого способа - существенное уменьшение скорости передачи. В вышеописанном примере скорость передачи информации уменьшается в 5 раз по сравнению со случаем однократной передачи кодовых комбинаций.

Также возможна одновременная передача кодовых комбинаций по нескольким параллельным каналам (обычно число каналов нечетное) решение о том, какая кодовая комбинация передавалась, выносится методом голосования (т.е. так же, как и при многократной передаче кодовых комбинаций).

При передаче сообщений по N параллельным каналам скорость передачи информации не зависит от числа каналов. Однако при этом существенно возрастают (в N раз!) расходы на аренду каналов.

При использовании SMT LSS - пусть у отправителя и получателя имеются несколько документов $S_1 \ldots S_n$, которыми они хотят обменяться («создать общую память»). Каждый из документов S_i передается между ними с использованием схемы разделения секрета, то есть каждый S_i делится на доли $s_1 \ldots s_k$. Каждая из долей передается по каналам связи получателю (для гарантии безопасности одна из них передается по надежному каналу), с учетом того, что любой из каналов (все сразу) может прослушивать и контролировать злоумышленник. У получателя каждый документ собирается из полученных долей. Подобный процесс соответственно осуществляется n-раз.

3. Из вышеописанного информационного обмена между отправителем и получателем создается общая база документов («общая память») $\{d_1 \ldots d_n\}$, где $S_1 = d_1, \ldots, S_n = d_n$. Отсюда отправитель и получатель имеют совокупность документов $\{d_1 \ldots d_n\}$, причем $d_i \neq d_j$ (нет смысла передавать один и тот же документ два раза и более).

4. Для передачи секрета S будет использоваться криптографическая задача об укладке рюкзака. С помощью документов из «общей памяти» формируется супервозрастающая (в поле Галуа GF_p, где p-простое) последовательность «типа Фибоначчи».

Условие супервозрастания: для любого i, $f_{i+1} \geq \sum f_i$. Примеры пригодных к использованию супервозрастающих последовательностей: $\{1, 2^1, 2^2, \ldots 2^n\}$, {1, 1, 2, 3, 5, 8…n}, $\{1, d_1 + d_2 + d_3, 1 + \sum d_i, \ldots d_{i-3} + d_{i-2} + d_{i-1} + (1 + \sum d_i)\ (1)^*\}$ и т.п.

5. Передаваемый секрет S должен удовлетворять условию $\sum e_i + d_i + \Delta = S$. Тут стоит пояснить насчет дополнительного коэффициента Δ. В общем случае, когда секрет S можно однозначно представить в виде вышеописанной суммы произведений - он равен нулю. Каких случаев больше? Когда дополнительный коэффициент нужен, либо когда он равен 0? На самом деле данный вопрос очень сложен с математической точки зрения и однозначного ответа на него дать невозможно. Однако существуют зависимости, которые помогают понять, когда данный коэффициент нужен, а когда соответственно нет.

Во-первых, наличие (отсутствие) данного коэффициента зависит от типа сверхвозрастающей последовательности. Например, для сверхвозрастающей последовательности степеней двойки он всегда будет отсутствовать, а для последовательности Фибоначчи (и многих других последовательностей, у которых первый член равен единице) он присутствовать будет.

Во-вторых, появление (отсутствие) данного коэффициента косвенно зависит от плотности укладки рюкзака - информационной меры избыточности рюкзачной криптосистемы. При стремлении данной величины к единице, можно с большой уверенностью говорить об отсутствии данного добавочного коэффициента, следовательно, о единственности решения данной криптографической задачи.

Когда же такое осуществить невозможно, то секрет S представляется в виде суммы произведений, в результате которой получается число S’, которое стремится к значению S. Чтобы компенсировать разницу этих значений (в общем случае) и вводится $\Delta = S - S'$. Отличий в алгоритмах шифрования и дешифрования при введении и использовании коэффициента Δ практически нет. При шифровании мы

добавляем Δ, чтобы привести S’ к S, а при дешифровании, перед решением аддитивной задачи об укладке рюкзака, мы должно просто вычесть Δ из полученного шифротекста.

Плотность (величина была введена Лагариасом и Одлыжко при проектировании ими L^3-атаки) рюкзака определяется как $d(a) = k / \max_{1 \le i \le k} \log_2(a_k)$. Плотность служит информационной мерой избыточности рюкзачной криптосистемы. Для сверхвозрастающей последовательности степеней двойки {1, 2^1, 2^2,… 2^k} плотность будет равна $d = k / \log_2(2^k) = 1$. Для последовательности «типа Фибоначчи» плотность будет равна $d = i+1 / \max(d_i)$.

На четвертом этапе были приведены математические примеры реализации вышеописанного алгоритма передачи сообщений между отправителем и получателем.

На пятом этапе был произведен обзор известных стеганографических систем, для каждого метода сокрытия информации приведено его описание. Заданы положения и требования, которыми необходимо руководствоваться при построении стегосистемы. Затем была рассмотрена модель TCP-стегосистемы, сформулирована ее концепция (возможности встраивания необходимой информации и получения подтверждения).

Потенциальный противник имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, которая остается неизвестной противнику, является ключ, с помощью которого его владелец может установить факт присутствия скрытого сообщения и его содержание. Если противник каким-то образом узнает о существовании скрытого сообщения, то это не должно позволить ему извлечь подобные сообщения из других контейнеров до тех пор, пока ключ хранится в тайне. Свойства контейнера должны быть модифицированы таким образом, чтобы стегоконтейнер беспрепятственно проходил по каналу связи, никоим образом не привлекая внимание потенциального противника. Стегосистема должна быть надежной. А именно предполагать защиту от потери, дублирования и нарушения очередности получения стегоконтейнеров и осуществлять контроль целостности сообщения.

В дальнейшем планируется работа над совершенствованием алгоритма передачи сообщений на основе протокола SMT (отказ от использования открытого и закрытого ключа, работа над формированием сверхвозрастающих последовательностей определенного типа и соответствующих определенным критериям, дальнейшее рассмотрение возможностей ухода от известных атак на рюкзачные криптосистемы и т.д.), над созданием алгоритма стегосистемы для организации стегоканала в SMT и реализации самой стегосистемы.

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. *Lagarias J. C., A. M. Odlyzko* – Solving low-density subset problems, Proc. 24th Annual IEEE Symp. on Found, of Corp. Science, pp. 1-10, 1983.

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

7. *M. Tompa and H. Woll*, How to share a secret with cheaters, Journal of Cryptology 1 (1988), 133-138.

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

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

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

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

12. *Слоэн Н. Дж. А.* «Коды, исправляющие ошибки, и криптография» - в сб. Математический цветник. – М.: Мир, 1983, с 432-472.

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

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

15. *Коханович Г.Ф., Пузыренко А.Ю.* «Компьютерная Стеганография» «МК-Пресс», Киев 2006, 278 стр.

16. Стеганография [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/wiki/Стеганография, 2012.

17. Построение стеганографической системы на базе протокола IPv4 [Электронный ресурс]. Режим доступа: http://www.securitylab.ru/contest/264960.php, 2006.