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

АЛГОРИТМ SMT LSS BROADCAST. ПЛОТНОСТЬ УКЛАДКИ РЮКЗАКА И ЕДИНСТВЕННОСТЬ РАЗЛОЖЕНИЯ СЕКРЕТА / SMT LSS BROADCAST ALGORITHM. DENSITY OF PACKING OF THE BACKPACK AND UNIQUE EXPANSION OF THE SECRET

Произведено рассмотрение влияния плотности укладки рюкзака на стойкость всей рюкзачной криптосистемы к L3-атаке. Аналогично осуществлено изучение влияния данного коэффициента укладки на единственность решения аддитивной задачи при разложении заданного секрета. Реализована модификация алгоритма SMT LSS. Предложена вариация алгоритма безопасной передачи сообщений на основе схемы SMT и задачи об укладке рюкзака с использованием широковещательной рассылки всех исходных данных, где засекречивается только ключевая последовательность. Произведена полная программная реализация заданного алгоритма и приведены результаты тестирования работы вышеописанного алгоритма в конкретном поле Галуа.

Ключевые слова: АЛГОРИТМ SMT LSS, ПЛОТНОСТЬ УКЛАДКИ, ЕДИНСТВЕННОСТЬ РАЗЛОЖЕНИЯ, ВОЗРАСТАЮЩАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ, ЗАДАЧА ОБ УКЛАДКЕ РЮКЗАКА, SMT.
15 источников.

Performed analysis of the influence of packing density of the backpack for stability all knapsack cryptosystem to L3-attack. Similarly performed to study the influence of this factor on the packing problem that the solution of the additive decomposition of the secret. Modification of the SMT LSS algorithm was realized. Proposed of the algorithm variation of the safe transfer of messages based on SMT circuit and problems on installation backpack with all the original broadcast data, where only the key sequence is secret. Perform a full software realization a given algorithm and the results of testing of the above of the algorithm in a particular field.

Keywords: SMT LSS ALGORITHM, DENSITY OF PACKING, UNIQUENESS OF EXPANSION, GROWING SEQUENCE, THE PROBLEM OF PACKING A BACKPACK, SMT.
15 sources.

Объектами исследования данной работы являются математический алгоритм передачи сообщений с «общей памятью» на основе схемы SMT LSS с использованием широковещательной рассылки всех исходных данных, где засекречивается только ключевая последовательность, проблема влияния плотности укладки рюкзака на стойкость всей рюкзачной криптосистемы к L^3-атаке и проблема влияния плотности укладки рюкзака на единственность решения аддитивной задачи при разложении заданного секрета.

Цели работы – теоретическое рассмотрение влияния плотности укладки рюкзака на стойкость всей рюкзачной криптосистемы к L^3-атаке; теоретическое рассмотрение влияния плотности укладки рюкзака на единственность решения аддитивной задачи при разложении заданного секрета; построение вариации алгоритма безопасной передачи сообщений на основе схемы SMT и задачи об укладке рюкзака с использованием широковещательной рассылки всех исходных данных, где засекречивается только ключевая последовательность; практическая реализация алгоритма SMT LSS в виде программного обеспечения; тестирование работы практически реализованного алгоритма в конкретном поле Галуа.

В процессе разработки темы проводилось теоретическое рассмотрение отдельных работ Костера и Одлыжко по влиянию коэффициента плотности укладки рюкзака на успех проведения L^3-атаки на рюкзачную криптосистему.

В конечном итоге приведены алгоритм математической реализации передачи сообщений на основе схемы SMT LSS broadcast, выделены ключевые отличия от предыдущей вариации данного алгоритма, выявлены зависимости успеха проведения L^3-атаки на рюкзачную криптосистему и единственности разложения секрета от коэффициента плотности укладки рюкзака, практически реализован алгоритм в виде программного обеспечения.

На первом этапе выполнения данной работы была произведена модификация существующего алгоритма, в результате чего был получен алгоритм SMT LSS broadcast. Можно выделить следующие его ключевые особенности по отношению к первому варианту алгоритма:

- использование широковещательной рассылки (по всем каналам между отправителем и получателем) исходных данных, используемых в алгоритме;
- решение полностью отказаться от попыток засекретить начальную совокупность документов $S_1 \ldots S_n$ (с помощью которой организовывается «общая память»), так как она не несет какой-либо информации о передаваемом секрете S, то есть при таком раскладе условие безопасности передачи сообщений не нарушается (злоумышленник, контролирующий каналы передачи все также не имеет никакой информации о секрете S);
- изменение алгоритма формирования необходимой возрастающей последовательности $\{f_1, f_2, \ldots f_n\}$ «типа Фибоначчи», где $f_1 = 1$, $f_2 = d_1 * e_1$, $f_3 = d_2 * e_2 + f_2 + f_1$, $f_4 = d_3 * e_3 + f_3 + f_2 + f_1$, … , $f_n = d_{n-1} * e_{n-1} + f_{n-1} + \sum f_i$, $\{e_1 \ldots e_n\}$ – ключ формирования $\{f_1 \ldots f_n\}$, где $e_i = 1$ – элемент d_i участвует в формировании последовательности или $e_i = 0$ – не участвует;
- формирование ключевой последовательности $E = \{e_1, e_2 \ldots e_n\}$, где $e_i = 0$, либо $e_i = 1$ и $E \neq \{0, 0, \ldots 0\}$ – ключ не существует. Данная ключевая последовательность будет использоваться непосредственно для передачи

по каналам связи секрета S. Длина ключевой последовательности равна длине сформированной возрастающей последовательности «типа Фибоначчи» - |F| = |E| = n;

- сам секрет S формируется следующим образом: если элемент e_i ключевой последовательности {E} равен единице, то соответствующий элемент f_i возрастающей последовательности входит в разложение секрета S, если элемент e_i ключевой последовательности {E} равен нулю, то соответствующий элемент f_i возрастающей последовательности не входит в разложение секрета S. Например, если $e_4 = 1$, то элемент f_4 возрастающей последовательности участвует в формировании секрета S, если $e_5 = 0$, то f_5 не участвует в формировании секрета S.

На втором этапе данного исследования осуществлено изучение влияния коэффициента плотности укладки на возможность успешного проведения L^3-атаки на рюкзачную криптосистему и на единственность разложения секрета при решении аддитивной задачи.

Плотность (величина была введена Лагариасом и Одлыжко при проектировании ими алгоритма 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 $\{1, 2^1, 2^2, \dots 2^k\}$ плотность будет равна $d = k / \log_2(2^k) = 1$. Для последовательности «типа Фибоначчи», которая используется в данном разрабатываемом алгоритме, плотность будет равна $d = i+1 / \log_2(\max(f_i))$, либо $d = \frac{n}{log_2 f_n}$ в общем случае.

В соответствии с теорией Костера и Одлыжко – чем больше величина плотности укладки рюкзака, тем меньше вероятность успеха осуществления L^3-атаки на данную рюкзачную криптосистему. При значении плотности $d > 0.9408$ проведение L^3-атаки на рюкзачную криптосистему затруднено. Однако существует и другая особенность (зависимость), связанная с плотностью укладки рюкзака. Чем больше значение плотности укладки рюкзака, тем больше вероятность того, что заданная криптологическая задача потеряет свою единственность в решении аддитивной задачи при разложении секрета S.

Одной из основных задач, на данном этапе проектирования алгоритма является оценка этой границы, в пределах которой следует выбирать значение плотности рюкзака такой, чтобы отсутствовала возможность проведения L^3-атаки и одновременно существовала единственность в решении рюкзачной задачи при разложении заданного секрета. С математической (теоретической) точки зрения обозначить и доказать данную границу очень сложно. Однако, в ходе конкретных практических экспериментов (с помощью реализованного программного приложения) по разложению чисел (секретов) в заданной последовательности (поле GF_p), была выявлена необходимость того, чтобы значение плотности варьировалось в пределах $1{,}0 \leq d \leq 2{,}5$. При значении плотности укладки $d > 2.5$ постоянно нарушается условие единственности решения задачи при разложении секрета. Как указывалось выше, данные значения были выявлены лишь экспериментальным путем, но существует большая вероятность полагать, что если и истинные значения немного другие, то они все равно близки к этому интервалу.

Третьим этапом в проектировании данного алгоритма является необходимость оценки средней длины блока - *l*, который будет формироваться алгоритмом и передаваться за один раз. Предполагается, что передаваемый секрет (документ) состоит из большого количества символов и делится на блоки одинаковой длины *l*, последний блок при необходимости заполняется нулями до заданной длины.

Для удобства работы в любой IDE (использование стандартных типов данных), при выборе длины блока передаваемой информации разумно остановится на величине $l = 64$, либо $l = 32$, если длину блока брать меньше – очень сильно падает плотность укладки, что в нашем случае неприемлемо. Все элементы сформированной возрастающей последовательности будут находиться в диапазоне $1 \leq f_i \leq 2^l\text{-}1$.

Плотность вышеописанной последовательности будет находиться в пределах $1.00 \leq d \leq 1.15$, что соответствует заданным требованиям усложнения возможности осуществления L^3-атаки на данную криптологическую рюкзачную систему. Также при таких значениях плотности укладки заданной исходной возрастающей

последовательности выполняется условие единственности (в общем случае) решения криптологической задачи об укладке рюкзака.

В соответствие с заданным размером блока подбирается поле Галуа, в пределах которого будут происходить все последующие вычисления, которому будут принадлежать все элементы заданной возрастающей последовательности. Для блока длины $l = 64$ необходимо взять поле Галуа – GF_p, где $p \sim 2^{64}$. Плотность укладки для такого рюкзака, где его исходная возрастающая последовательность находиться в поле GF_p, где $p \sim 2^{64}$, равна $d = 1.0747$. Полученная плотность удовлетворяет вышеописанным условиям.

На четвертом этапе осуществлена практическая реализация вышеописанного алгоритма в виде программного обеспечения. Основные возможности реализованного ПО:

- считывание исходной последовательности документов $\{d_1, d_2, \dots d_n\}$ и ключа формирования $\{e_1, e_2, \dots e_n\}$ необходимых для формирования возрастающей последовательности $\{f_1, f_2, \dots f_n\}$;
- формирование $\{f_1, f_2, \dots f_n\}$ в соответствии с вышеописанным алгоритмом и заданным ключом (если $\{E\} = 0$, то формируется классический ряд Фибоначчи);
- подсчет плотности укладки полученной последовательности $\{f_1, f_2, \dots f_n\}$;
- разложение введенного числа (документа, секрета) с помощью «жадного алгоритма»;
- вывод результатов о возможности разложения данного секрета без дополнительного коэффициента Δ, вывод значения Δ, если без него секрет разложить невозможно;
- формирование ключа разложения секрета S.

На последнем этапе проектирования для заданного поля и данной возрастающей последовательности была проведена серия экспериментов по разложению случайных чисел (секретов), что, в общем, дало положительные результаты – плотность укладки рюкзака для разных последовательностей в заданном поле GF_p всегда больше единицы, что удовлетворяет поставленному

условию, условие единственности решения криптологической задачи об укладке в общем случае выполняется.

В итоге, формирование возрастающей последовательности $\{f_1, f_2 \ldots f_n\}$ необходимо и возможно подчинить следующим условиям:

- плотность укладки рюкзака $d \geq 1$ ($d \sim 1$);
- значения элементов последовательности в пределах $1 \leq f_i \leq 2^l-1$.

В дальнейшем планируется работа над еще большим совершенствованием данного алгоритма передачи сообщений (окончательный выбор поля Галуа, в котором будут происходить вычисления; точный выбор длины блока l; решение вопроса о единственности разложения секрета при решении аддитивной задачи; выбор способа передачи ключевой последовательности и т.п.).

Литература

1. *Coster M. J., Joux A., LaMacchia B. A.*, et al. Improved low-density subset sum algorithms // Computational Complexity. 1992. No. 2. P. 111–128.

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

3. *Karp R. M.* Reducibility among combinatorial problems // Complexity of Computer Computations: Proc. of a Symp. on the Complexity of Computer Computations, the IBM Research Symposia Series. NY: Plenum Press, 1972. P. 85–103.

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

5. *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.

6. *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.

7. *Odlyzko A. M. and Lagarias J. C.* Solving Low-Density Subset Sum Problems // J. Association Computing Machinery. 1985. V. 32. No.1. P. 229–246.

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

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

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

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

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

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

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

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