Федеральное государственное бюджетное учреждение науки
ИНСТИТУТ ДИНАМИКИ СИСТЕМ И ТЕОРИИ УПРАВЛЕНИЯ
имени В.М. Матросова
Сибирского отделения Российской академии наук

ЛЯПУНОВСКИЕ ЧТЕНИЯ

30 ноября – 2 декабря 2015 года

Материалы конференции

Иркутск – 2015

ИССЛЕДОВАНИЕ ЗАДАЧИ ОБРАЩЕНИЯ ХЕШ-ФУНКЦИИ MD4 ПРИ ПОМОЩИ SAT-ПОДХОДА*

И.А. Грибанова
Институт динамики систем и теории управления имени В.М. Матросова СО РАН
the42dimension@gmail.com

Хеш-функциями называются отображения вида $\chi: \{0,1\}^* \to \{0,1\}^c$, где c – некоторая константа. Для того чтобы хеш-функция считалась криптографически стойкой необходимо, чтобы она удовлетворяла ряду требований, напрямую связанных с применением такой хеш-функции на практике. Одним из таких требований является стойкость хеш-функции к восстановлению прообраза. Это означает, что для заданного значения y задача поиска такого x, что $\chi(x) = y$, должна быть вычислительно сложной.

Основой большинства современных хэш-функций является конструкция Меркля-Дамгарда [1, 2]. Наиболее известными представителями таких хэш-функций являются функции семейств MD и SHA. Несмотря на то, что некоторые из этих хеш-функций были признаны уязвимыми к атакам построения коллизий [3, 4], задачу обращения не удается эффективно решить даже для MD4 (самой простой из семейства MD).

В работе [5] удалось осуществить обращение 39 шагов алгоритма MD4 с помощью SAT-подхода. Атака, описанная в [5], потребовала около 8 часов работы SAT-решателя minisat, при этом в соответствующую SAT-кодировку были добавлены дополнительные ограничения на промежуточные значения хеш-функции. Такого рода ограничения впервые были представлены в работе [6].

В настоящем докладе будет представлен автоматический метод поиска ограничений типа представленных в [6], использующий SAT-подход. Пусть C – КНФ, кодирующая задачу обращения некоторой функции χ, и X – множество переменных, фигурирующих в C. Предположим, что к C требуется добавить ограничения, задающие некоторый предикат над переменными из множества $\tilde{X}$, $\tilde{X} \subseteq X$, а $R(\tilde{X})$ – формула, задающая данный предикат. Введем новую переменную $u, u \notin X$, и рассмотрим формулу $C \wedge (u \vee R(\tilde{X}))$. Очевидно, что ограничение $R(\tilde{X})$ будет активно при $u = 1$ и неактивно при $u = 0$. Переменные вида u будем называть переменными переключения. В результате варьирования значений переменных переключения можно найти набор дополнительных ограничений, учет которых повысит скорость решения SAT-задачи, кодирующей обращение рассматриваемой функции. На данном этапе реализован простой механизм перебора значений переменных переключения, который тем не менее позволил синтезировать ограничения из [6] в автоматическом режиме.

1. Merkle R. A. Certified digital signature // LNCS. 1990. Vol. 435. P. 218–238.
2. Damgard I. A. A design principle for hash functions // LNCS. 1990. Vol. 435. P. 416–427.
3. Wang X., Lai X., Feng D., Chen H., Yu X. Cryptanalysis of the Hash Functions MD4 and RIPEMD // LNCS. 2005. Vol. 3494. P. 1-18.
4. Wang X., Yu H. How to Break MD5 and Other Hash Functions // LNCS. 2005. Vol. 3494. P. 19-35.
5. De D., Kumarasubramanian A., and Venkatesan R. Inversion attacks on secure hash functions using SAT solvers // LNCS. 2007. Vol. 4501. P. 377–382.
6. Dobbertin H. The first two rounds of MD4 are not One-Way // Proc. 5th Intern. Workshop Fast Software Encryption. London, UK: Springer Verlag, 1998. P. 284–292.

*Исследование выполнено при частичной поддержке РФФИ, гранты: 14-07-31172 мол_а, 15-07-07891 а.