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

ЛЯПУНОВСКИЕ ЧТЕНИЯ

21 ноября – 23 ноября 2016 года

Материалы конференции

Иркутск – 2016

ПОСТРОЕНИЕ НОВЫХ ДИФФЕРЕНЦИАЛЬНЫХ ПУТЕЙ ДЛЯ ЗАДАЧИ ПОИСКА КОЛЛИЗИЙ ХЕШ-ФУНКЦИИ MD4*

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

Криптографические хеш-функции нашли широкое применение в различных протоколах защиты данных, а также в системах электронно-цифровой подписи. Одним из примеров таких хеш-функций являются хеш-функции семейства MD, построенные на базе конструкции Меркля-Дамгарда.

В работах [1, 2] коллективом китайских криптографов во главе с К. Ванг (X. Wang) был предложен алгоритм поиска коллизий для хеш-функций MD4 и MD5. Основу данного алгоритма составляют дополнительные ограничения, накладываемые на промежуточные значения хеш-функций в виде целочисленных разностей по модулю 2^{32}. Ограничения такого вида формируют «дифференциальный путь», который значительно сужает пространство поиска. Далее рассматривается задача поиска одноблоковых коллизий хеш-функции MD4.

Рассмотрим процесс вычисления хеш-значений MD4 для двух 512-битных сообщений M и M'. На каждом шаге в хеш-регистрах H и H' записаны 32-х битные слова, представляющие собой промежуточные хеш-значения для сообщений M и M'. На эти слова накладываются дополнительные ограничения из дифференциального пути, обозначаемые через δ_k, где k – номер шага. Разность между значениями хеш-регистров на последнем шаге должна быть равна 0, что означает существование коллизии.

Кратко опишем идею построения новых дифференциальных путей для задачи поиска коллизий при помощи SAT-подхода. Пусть $\tilde{C}$ – КНФ, кодирующая задачу поиска одноблоковой коллизии MD4, $C_{\Delta\setminus\delta_k=c}$ – КНФ, кодирующая условия из некоторого дифференциального пути Δ (например, пути Ванг) без учета соотношения на k-шаг, а $C_{\delta_k=c}$ – КНФ, которая выполнима тогда и только тогда, когда переменная δ_k принимает значение c. Осуществим перебор всех возможных значений 32-х битной константы c и рассмотрим проблемы выполнимости соответствующих КНФ вида $\tilde{C} \wedge C_{\Delta\setminus\delta_k=c} \wedge C_{\delta_k=c}$.

В ходе вычислительных экспериментов было установлено, что для большинства значений c современные SAT-решатели быстро доказывают невыполнимость КНФ вида $\tilde{C} \wedge C_{\Delta\setminus\delta_k=c} \wedge C_{\delta_k=c}$. Все остальные значения константы c, для которых решение не было найдено за несколько секунд, рассматривались в качестве возможных значений δ_k в новом дифференциальном пути. С помощью данного подхода удалось построить новый дифференциальный путь, отличный от пути Wang. Для сравнительной оценки скорости нахождения коллизий использовался SAT-решатель Cryptominisat [3], имеющий функцию перечисления решений.

1. Wang X., Lai X., Feng D., et.al. Cryptanalysis of the hash functions MD4 and RIPEMD // Lecture Notes in Computer Science. 2005. Vol. 3494. P. 1–18.
2. Wang X., Yu H. How to break MD5 and other hash functions // Lecture Notes in Computer Science. 2005. Vol. 3494. P. 19–35.
3. Soos M., Nohl K., Castelluccia C. Extending SAT Solvers to Cryptographic Problems // Lecture Notes in Computer Science. 2009. Vol. 5584. P. 244–257.

*Работа выполнена при частичной поддержке гранта РФФИ № 14-07-00403.