визуализацией медиаданных на графических акселераторах // Программирование. — 2014. — Т. 40, № 4, С. 55–63.
[2] Оборудование для автоматизации телевизионного вещания. Адрес доступа: http://www.softlab.tv/rus/forward/hardware_all.html (дата обращения 21.05.2017).

2.16. *Грибанова И.* Несбалансированные приближения булевых функций в применении к обращению криптографических хеш-функций

Хеш-функция MD4 [1] — одна из первых криптографических хеш-функций, построенных на основе конструкции Меркля — Дамгарда. Несмотря на то, что данная функция уязвима к атаке поиска коллизий, до сих пор не предложено эффективных алгоритмов для решения задачи ее обращения.

В докладе будут представлены результаты по обращению неполнораундой версий MD4 с использованием новой техники, которая включает в себя: замену некоторых раундовых подфункций MD4 несбалансированными булевыми функциями; решение полученной изменённой (интереполированной) задачи; переход к решению исходной задачи. Данная техника комбинируется с дополнительными условиями на переменные сцепления хеш-функции MD4, которые были предложены Г. Доббертином в [2].

Напомним, что в MD4 вычисление переменной сцепления на i-м шаге описывается формулой

$$Q_i = (Q_{i-4} + \Phi_i(Q_{i-1}, Q_{i-2}, Q_{i-3}) + m_{p(i)} + k_i) <<< s_i,$$

где $i \in \{0, ..., 47\}$, Φ_i — раундовая функция i-го шага, $m_{p(i)}$ — 32-битный вектор, часть хешируемого сообщения, k_i, s_i — константы i-го шага. Заметим, что Q_i — это 32-битный булев вектор, операции над которым выполняются побитово. Переход от исходной сбалансированной булевой функции к несбалансированной будем называть модификацией.

Для решения задачи обращения MD4-39 (39-шаговой версии хеш-функции MD4) осуществлялась модификация функций, задающих вектор Q_{34}. Соответствующие пропозициональные кодировки были построены с помощью системы Transalg [3], в которой процесс вычисления сложной булевой функции представляется в виде суперпозиции функций меньшей арности. Далее в пропозициональную кодировку исходной задачи была подставлена часть данных из решения интерполированной задачи, а именно 256 бит найденного хешируемого сообщения. Стоит отметить, что среднее время решения задачи обращения с использованием этих данных оказалось меньше, чем среднее время решения исходной задачи без интерполяции.

Проведённые вычислительные эксперименты с использованием многопоточных SAT-решателей, которые запускались на одном рабочем узле кластера «Академик В.М. Матросов» [4], демонстрируют работоспособность предлагаемого подхода в применении к задаче обращения MD4-39.

Список литературы

[1] Rivest R. L. The MD4 message digest algorithm // Lecture Notes in Computer Science. — 1990. — Vol. 537, P. 303–311.
[2] Dobbertin H. The first two rounds of md4 are not one-way // Lecture Notes in Computer Science. — 1998. — Vol. 1372. P. 284–292.
[3] Otpuschennikov I., Semenov A., Gribanova I. et al. Encoding Cryptographic Functions to SAT Using TRANSALG System // Proc. of the «22nd European Conference on Artificial Intelligence». — 2016. — Vol. 285, P. 1594–1595.
[4] Иркутский суперкомпьютерный центр СО РАН. Адрес доступа: http://hpc.icc.ru.

2.17. *Долгая А.А., Герус А.И., Фереферов К.А.* Разработка web-интерфейса базы данных катастрофических событий

В целях исследования закономерностей распределения природных катастроф и социальных явлений авторским коллективом была создана информационно-вычислительная система, позволяющая осуществлять просмотр, пополнение и редактирование базы данных природных и социальных катастроф [1].

Помимо ведения базы данных в информационно-вычислительной системе доступны функции фильтрации, визуализации данных на карте и экспорта данных в формат Excel, а также реализовано исследование временных закономерностей катастрофических событий с помощью спектрального анализа временных рядов.

Разработанная информационно-вычислительная система создавалась как однопользовательское приложение для апробации различных методов анализа нового массива данных. Полученные результаты показали, что база данных катастрофических событий является мощным инструментом исследования закономерностей геосоциального процесса [2], поэтому следует сделать ее доступной для широкого круга пользователей. В связи с этим принято решение создать web-интерфейс для рассматриваемого массива данных, который наследует большую часть функций однопользовательской версии (просмотр, фильтрация, сортировка, экспорт, статистическая обработка данных).

Доступ к ресурсу будет осуществляться через сайт Института вулканологии и сейсмологии ДВО РАН. В качестве СУБД используется MariaDB 5.5. Для создания интерфейса используется язык Python версии 3.4. В дополнении к перечисленным функциям разрабатываемый ресурс будет содержать форму отправки запроса на пополнение данных (добавление или редактирование сведений о катастрофах будет осуществлять модератор), а также спра-