Применение графических ускорителей для поиска высоковероятностных линейных дифференциальных характеристик хэш-функции SHA-1

Абраменкова Марина Анатольевна

Студент

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: marimurony@gmail.com

Криптографические хэш-функции позволяют строить надежные и быстрые схемы электронной цифровой подписи. От криптографической стойкости хэш-функции зависит криптостойкость использующей ее схемы электронной цифровой подписи. SHA-1 является одной из наиболее популярных хэш-функций на данный момент.

Основным видом атак на хэш-функции является атака поиска коллизий. Атака поиска коллизий SHA-1 состоит из двух этапов:

- линеаризация хэш-функции и построение линейной дифференциальной характеристики
- построение полной дифференциальной характеристики и поиск коллизий

Данная работа посвящена первому этапу. Цель работы — нахождение оптимальной линейной дифференциальной характеристики для SHA-1 и обоснование минимальности ее веса.

В статье Прамсталлера, Рекбергера и Раймона [1] было предложено использовать теорию линейных кодов для поиска линейных дифференциальных характеристик. Авторы используют предположение, что чем меньше вес Хэмминга линейной дифференциальной характеристики, тем лучше соответствующая линейная дифференциальная характеристика. Таким образом, задача поиска оптимальных линейных дифференциальных характеристик сводится к задаче поиска слов минимального веса в линейном коде. В качестве наилучшего результата авторы опубликовали характеристику веса 237, однако вопрос о минимальности данного веса оставался открытым.

Для данной работы алгоритмы Шабо [3], Штерна [4] и Бернштейна, Ланг и Петерса [5] были адаптированы для задачи поиска слов минимального веса в линейном коде. Даже при том, что эти алгоритмы гораздо лучше полного перебора, сходятся они довольно медленно. Поэтому было решено использовать графические ускорители

для оптимизации их работы. Эти алгоритмы были реализованы на ГПУ с применением технологии параллельного программирования CUDA. С их помощью было найдено кодовое слово веса 237. С помощью формул из статьи Леона [2], а также с учетом особенностей исследуемого линейного кода была посчитана вероятность ошибки, которая составила $6.242 \cdot 10^{-14}$. Таким образом, была обоснована минимальность веса 237.

Литература

1. Pramstaller N., Rechberger C., Rijmen V. Exploiting coding theory for collision attacks on SHA-1 // In Cryptography and Coding 2005, Berlin, 2005, vol. 3796 of Lecture Notes in Computer Science, P. 78—95, Springer-Verlag.
2. Leon J. A probabilistic algorithm for computing minimum weights of large error correcting codes // In IEEE Transactions on Information Theory, 1988, vol. 34(5), P. 1354—1359.
3. Chabaud F. On the Security of Some Cryptosystems Based on Errorcorrecting Codes // In Proceedings of EUROCRYPT 1994, Springer, 1995, vol. 950 of Lecture Notes in Computer Science, P. 131–139.
4. Stern J. A method for finding codewords of small weight // In Proceedings of Coding Theory and Applications 1988, Springer, 1989, vol. 388 of Lecture Notes in Computer Science, P. 106—113.
5. Bernstein D.J., Lange T., Peters C. Attacking and Defending the McEliece Cryptosystem // In Post-Quantum Cryptography, vol. 5299 of Lecture Notes in Computer Science, P. 31–46, Springer, 2008.