**Теорема 2.** Построенное бинарное отношение на множестве булевых функций при каждом зафиксированном значении циклического сдвига $s$ совпадает с отношением порядка, построенным в работе [3].

В [3] показано, что наименьшим элементом для этого отношения является функция XOR. Поэтому имеет место

**Следствие 2.** Использование булевой функции XOR в хэш-функции MD5 является оптимальным с точки зрения устойчивости MD5 к дифференциальному криптоанализу.

**Теорема 3.** В построенном бинарном отношении на множестве значений циклических сдвигов для каждой булевой функции все значения циклических сдвигов эквивалентны.

ЛИТЕРАТУРА

1. *Rivest R.* The MD4 message digest algorithm // LNCS. 1991. V. 537. P. 303–311.
2. *Rivest R.* The MD5 message digest algorithm // RFC 1321, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992.
3. *Нгуен Т. Х., Карпунин Г. А.* Оптимальность выбора функции xor в одной модели дифференциального криптоанализа хэш-функций семейства MDx // Материалы IV Междунар. научн. конф. по проблемам безопасности и противодействия терроризму и VII Общерос. научн. конф. «Математика и безопасность информационных технологий» (МАБиТ–2008), Москва, МГУ, 30 октября – 1 ноября 2008 г. М.: МЦНМО, 2009. С. 65–70.

УДК 519.151,519.725, 519.165

## ПРОБЛЕМЫ ПОЧТИ ПОРОГОВЫХ СХЕМ РАЗДЕЛЕНИЯ СЕКРЕТА

Н. В. Медведев, С. С. Титов

В настоящее время вопросы, связанные с криптографическими методами защиты информации и математическими задачами криптологии, являются чрезвычайно важными [1]. Такими, например, являются задачи делегирования прав, разграничения доступа к информации и разделения секрета. Одними из основных криптографических примитивов в теории и практике защиты информации являются схемы разделения секрета (СРС).

Основная идея СРС состоит в предоставлении участникам долей секрета таким образом, чтобы только заранее заданные разрешённые коалиции участников могли однозначно восстановить секрет, а неразрешённые не получали никакой дополнительной к имеющейся априорной информации о возможном значении секрета [2].

В работе [3] описаны идеальные почти пороговые СРС, основанные на эллиптических кривых и позволяющие реализовать более сложную, чем у пороговых СРС, структуру доступа [4], при которой не все $n$-элементные множества участников могут однозначно восстановить секрет. Эллиптическая кривая и точки на ней используются для параметризации участников. В работе [5] доказано, что можно реализовать такую СРС с бесконечным количеством участников, где всюду плотность расположения рациональных точек на эллиптической кривой выступает аналогом совершенности.

Разрешённые коалиции идеальной совершенной схемы разделения секрета определяются циклами некоторого связного матроида, изучение которого и даёт структуру доступа [2], в данном случае матроиды будут почти пороговыми [3].

Если в структуре доступа СРС есть незаменимые участники, т. е. те, которые входят во все разрешённые коалиции, то основная идея СРС — восстановление секрета в отсутствие каких-либо участников — не работает. Незаменимость участника означает, что, какова бы ни была доля секрета, выдаваемая этому участнику, без его участия в восстановлении секрета не обойтись. Незаменимые участники фактически обладают теми же правами, что и дилер, хранитель секрета, и ассоциируются с ним. Они обладают «правом вето», т. е. без них ничего не решится. Итак, для разделения незаменимых участников необходимо, чтобы был цикл, содержащий по отдельности каждого из этих двух участников. Этим доказано

**Утверждение 1.** В матроиде, соответствующем СРС, нет незаменимых участников тогда и только тогда, когда для любых $x \neq y$ существует разделяющий их цикл $C$, т. е. $x \notin C$, $y \in C$.

Назовём такие матроиды разделяющими.

Матроид назовем почти пороговым, если все его циклы имеют мощность $n$, но, возможно, не все его $n$-элементные подмножества — циклы. Путём комбинаторных рассуждений доказано

**Утверждение 2.** Для мощностей цикла 1, 2 и 3 связного почти порогового непорогового матроида не существует.

Разграничение доступа к информации в компьютерных системах естественным образом, путём рассмотрения битовых строк, приводит к бинарным матроидам, т. е. матроидам, реализующимся как векторные над полями характеристики два. На этом пути удаётся построить связный почти пороговый непороговый матроид с мощностью цикла 4. Рассмотрением фактор-групп группы кода СРС получена обобщающая

**Теорема 1.** Бинарные связные разделяющие почти пороговые матроиды исчерпываются матроидами, соответствующими кодам Рида — Маллера первого порядка.

ЛИТЕРАТУРА

1. Доктрина информационной безопасности [Электронный ресурс]. `http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm`.
2. Введение в криптографию / под общ. ред. В. В. Ященко. СПб.: Питер, 2001. 288 с.
3. *Медведев Н. В., Титов С. С.* Почти пороговые схемы разделения секрета на эллиптических кривых // Доклады ТУСУРа. 2011. №1(23). С. 91–96.
4. *Гайдамакин Н. А.* Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд-во Урал. ун-та, 2003. 328 с.
5. *Медведев Н. В., Титов С. С.* О топологии эллиптических кривых // Тр. Ин-та математики и механики УрО РАН. 2012. Т. 18. №1. С. 242–250.
6. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.

УДК 681.326; 531.19

## МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ ТРЁХЗНАЧНОЙ ЛОГИКИ

Е. Л. Столов

В последнее время созданы простые физические устройства, реализующие трёхзначную логику [1], что стимулирует разработку физических схем, работающих