2. *Коренева А. М., Фомичев В. М.* Криптографические свойства блочных шифров, построенных на основе регистров сдвига // Прикладная дискретная математика. Приложение. 2012. № 5. С. 49–51.

УДК 519.151, 519.725, 519.165

КОНСТРУКЦИИ ИДЕАЛЬНЫХ СХЕМ РАЗДЕЛЕНИЯ СЕКРЕТА

Н. В. Медведев, С. С. Титов

Работа посвящена исследованию вопросов разграничения доступа к информации при помощи линейных идеальных однородных схем разделения секрета. Приведена конструкция таких схем над любым полем $\mathrm{GF}(q)$. Путём добавления участников показано, что такие схемы сводятся к схемам на проективных пространствах.

Ключевые слова: *однородные схемы разделения секрета, структуры доступа, матроиды, код Рида — Маллера, идеальные схемы.*

Неотъемлемыми атрибутами современных компьютерных систем и сетей передачи данных являются криптографические протоколы защиты информации. На этом пути часто возникают сложные проблемы, требующие привлечения серьёзного математического аппарата. Одна из таких актуальных и активно исследуемых западными специалистами областей — разграничение доступа [1] при помощи протоколов (схем) разделения секрета (СРС) [2, 3].

Механизм работы СРС заключается в предоставлении участникам долей секрета таким образом, чтобы заранее заданные коалиции участников (разрешённые коалиции) могли однозначно восстановить секрет [4]. Особый интерес вызывают однородные СРС [5 – 7], которые допускают идеальную реализацию. При этом ограничиваются рассмотрением разделяющих СРС, т. е. таких, где нет незаменимых участников [6].

Разрешённые коалиции идеальной совершенной схемы разделения секрета определяются циклами некоторого связного матроида, изучение которого и даёт структуру доступа [8]. В терминах циклов аксиом всего две. Представляется естественным рассмотреть двойственный вариант аксиоматизации матроида, а именно использовать не циклы C матроида M, а его нуль-множества Z, т. е. $Z = M \setminus C$, которые можно назвать «антициклами». Тогда аксиомы матроида в терминах антициклов имеют следующий вид: 1) нет антицикла в антицикле, т. е. если Z_1, Z_2 — антициклы и $Z_1 \subset Z_2$, то $Z_1 = Z_2$; 2) если $e \in M$, $e \notin Z_1 \cup Z_2$ и Z_1, Z_2 — антициклы, причём $Z_1 \neq Z_2$, то существует такой антицикл Z, что $(\{e\} \cup (Z_1 \cap Z_2)) \subset Z$.

Перейдём к рассмотрению матроидов в проективном m-мерном пространстве M над $\mathrm{GF}(q)$. Возьмём в качестве нуль-множеств Z гиперпространства в M. Как известно [9], $|M| = (q^{m+1} - 1)/(q - 1)$ и $|Z| = (q^m - 1)/(q - 1)$. Поскольку любые два гиперпространства Z_i и Z_j всегда пересекаются, т. е. $(Z_i \cap Z_j) \neq \varnothing$, причём $\dim Z = m - 1$, $\dim(Z_i \cap Z_j) = m - 2$, то для любой точки $e \notin (Z_i \cap Z_j)$ существует единственное гиперпространство Z, натянутое на $\{e\}$ и на пересечение гиперпространств Z_i и Z_j, так что $Z = \langle \{e\}, Z_i \cap Z_j \rangle$. А это — не что иное, как вторая аксиома матроида в терминах антициклов, которую можно назвать усиленной, так как существует единственное такое гиперпространство. Следовательно, вторая аксиома матроида выполняется. Первая аксиома матроида с очевидностью выполняется, так как размерности гиперпространств одинаковы и антицикла в антицикле быть не может.

Далее рассмотрим матроиды в аффинном m-мерном пространстве M над $\mathrm{GF}(q)$. Как известно [9], $|M| = q^m$ и $|Z| = q^{m-1}$. В аффинном пространстве может быть два случая пересечения гиперпространств Z_i и Z_j: 1) либо пересекаются, т. е. $Z_i \cap Z_j \neq \varnothing$, тогда вторая аксиома матроида выполняется, как в проективном пространстве; 2) либо параллельны, т. е. $Z_i \cap Z_j = \varnothing$, тогда это тривиальный случай и вторая аксиома матроида также выполняется, так как объединение двух соответствующих гиперпространствам циклов образует всё пространство M. Первая аксиома матроида выполняется в обоих случаях, как и в проективном пространстве.

При реализации идеальной однородной совершенной СРС гиперпространства соответствуют линейным функциям. На основе обобщённых кодов Рида — Маллера получена

Теорема 1. Аффинное и проективное пространства над $\mathrm{GF}(q)$ являются однородными матроидами с гиперпространствами в качестве антициклов.

При этом возникает естественный и сложный вопрос полного описания класса однородных СРС над $\mathrm{GF}(q)$. Для решения этого вопроса рассмотрена возможность добавления участников СРС однородного матроида. Путём комбинаторных рассуждений доказано

Утверждение 1. Линейные однородные разделяющие СРС над $\mathrm{GF}(q)$ сводятся к подсхемам схемы некоторого проективного пространства над $\mathrm{GF}(q)$ с гиперпространствами в качестве антициклов.

ЛИТЕРАТУРА

1. *Гайдамакин Н. А.* Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд-во Урал. ун-та, 2003.
2. *Shamir A.* How to share a secret // Comm. ACM. NY, USA: ACM, 1979. V. 22. No. 11. P. 612–613.
3. *Черемушкин А. В.* Криптографические протоколы: основные свойства и уязвимости // Прикладная дискретная математика. Приложение. 2009. № 2. С. 115–150.
4. Введение в криптографию / под общ. ред. В. В. Ященко. СПб.: Питер, 2001.
5. *Marti-Farre J. and Padro C.* Secret sharing schemes on sparse homogeneous access structures with rank three // Electronic J. Combinatorics. 2004. No. 11(1). Research Paper 72. 16 p.
6. *Медведев Н. В., Титов С. С.* Бинарные почти пороговые матроиды // Научно-технический вестник Поволжья. 2012. № 4. С. 136–142.
7. *Медведев Н. В., Титов С. С.* Почти пороговые схемы разделения секрета на эллиптических кривых // Доклады ТУСУРа. 2011. № 1(23). Ч. 1. С. 91–96.
8. *Блейкли Г. Р., Кабатянский Г. А.* Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Проблемы передачи информации. 1997. Т. 33. № 3. С. 102–110.
9. *Холл М.* Комбинаторика. М.: Мир, 1970. 424 с.

УДК 519.723

О НЕМИНИМАЛЬНЫХ СОВЕРШЕННЫХ ШИФРАХ

Н. В. Медведева, С. С. Титов

Рассмотрены свойства неминимальных совершенных шифров. Показано, что неминимальный совершенный шифр вкладывается в максимальный совершенный шифр. Доказан аналог теоремы К. Шеннона для неэндоморфных совершенных шифров.