УДК 004.056 + 519.151 + 004.072.4 Вестник УрФО № 4(14)/2014. Стр. 36–39

Сорокина С. В., Титов С. С.

МАТРОИДЫ, ДВОЙСТВЕННЫЕ К БИНАРНЫМ, И ИХ СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА

Необходимость защиты информации от хищения или несанкционированной модификации порождает необходимость распределения прав доступа к ней. Грамотное разграничение доступа к информации подразумевает, что неразрешённая группа участников не получает никакой информации о секрете, а любая разрешённая – может его однозначно восстановить. В данной статье высказана гипотеза, которая в этой статье будет проверяться на примере матроида Фано, а затем в ходе дальнейших исследований и на других матроидах.

Ключевые слова: *информационная безопасность, матроиды, цикл матроида, базис матроида, идеальная схема разделения секрета, структура доступа.*

Sorokina S. V., Titov S. S.

MATROIDS DUAL TO BINARY ONES AND THEIR SECRET SEPARATION SCHEMES

The need to protect information from theft or unauthorized modification necessitates the sharing of rights of access to it. Proper differentiation of access to information means that the group of unpermitted participants gets no information about the secret, and any permitted one can restore it. The article dwells on the hypothesis which is going to be proved on the example of Fano matroid, as well as in the course of further research and other matroids.

Keywords: *information security, matroids, matroid cycle, matroid basis, ideal secret separation scheme, access structure.*

Реализация структур доступа на основе схем разделения секрета в настоящее время осуществляется на основе матроидов. Другими словами, по идеальной схеме разделения секрета можно построить матроид. Вопрос, можно ли, имея матроид, построить по нему схему разделения секрета, остаётся открытым до сих пор.

Мы предполагаем, что это возможно, и для этих целей рассматриваем матроид Фано, представимый как векторный над конечным полем GF(2), иначе говоря, бинарный матро-

ид. По нашей гипотезе, матрица идеальной схемы разделения секрета будет представлять собой матрицу циклов двойственного матроида. Для подтверждения этой гипотезы построим схему разделения секрета по матроиду Фано.

Матроид – это такая пара (X, I), где X – конечное множество, называемое **носителем матроида**, а I – некоторое множество подмножеств X, называемое семейством **независимых множеств**, то есть $I \in 2^X$. При этом должны выполняться следующие условия:

1) $\varnothing \in I$;

2) если $A \in I$ и $B \subset A$, то $B \in I$;

3) если $A, B \in I$ и $|A| > |B|$,
то $\exists x \in A \setminus B : B \cup \{x\} \in I$.

База матроида — максимальное по включению независимое множество.

Зависимое множество — подмножество носителя матроида, не являющееся независимым.

Матроид представим над полем F, если он изоморфен некоторому векторному матроиду над этим полем. Если матроид представим над любым полем, его называют регулярным. Матроид, который является представимым над двухэлементным полем $GF(2)=\{0,1\}$ (полем называют множество элементов, на котором определены две операции: сложение и умножение, даже если эти операции не являются обычными операциями сложения и умножения, а также вычитание и деление – на любой ненулевой элемент), называется бинарным матроидом. Матроид, представимый над полем $GF(3)=\{0,1,2\}$ из трёх элементов, называется тернарным матроидом.

Цикл матроида — минимальное по включению зависимое множество. Семейство циклов часто обозначается буквой C.

Двойственным матроидом называется матроид, носитель которого совпадает с носителем данного матроида, а базы – дополнения баз данного матроида до носителя, т. е. $X^*=X$, а множество баз двойственного матроида – это множество таких B^*, что $B^*=X\setminus B$, где B – база данного матроида.

Предположим, что матрица G идеальной схемы разделения секрета с матроидом M определяется двойственным матроидом M^* через список его циклов как список его зависимых множеств. Следовательно, если матроид M представим над конечным полем F, то M^* задаёт порождающую матрицу G линейного над полем F кода с проверочной матрицей H, задаваемой циклами матроида M, этот код и есть код этой СРС.

Для проверки этой гипотезы рассмотрим бинарный матроид на примере матроида Фано.

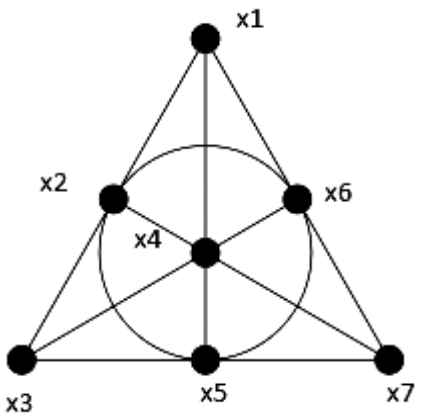


Рис. 1. Матроид Фано

Для матроида Фано носителем матроида является семиэлементное множество $X=\{x_1, \ldots, x_7\}$, элементы которого можно параметризовать битами (элементами поля $GF(2)=\{0,1\}$):

1) $\vec{i} = (1,0,0) = x_1$;
2) $\vec{j} = (0,1,0) = x_3$;
3) $\vec{k} = (0,0,1) = x_7$;
4) $\vec{i} + \vec{j} = (1,1,0) = x_2$;
5) $\vec{j} + \vec{k} = (0,1,1) = x_5$;
6) $\vec{i} + \vec{k} = (1,0,1) = x_6$;
7) $\vec{i} + \vec{j} + \vec{k} = (1,1,1) = x_4$.

Выпишем циклы матроида Фано, состоящие из 3 элементов (см. рис. 1, на котором трёхэлементные циклы соответствуют отрезкам и окружности):

1) x_1, x_2, x_3;
2) x_3, x_5, x_7;
3) x_1, x_6, x_7;
4) x_2, x_4, x_7;
5) x_6, x_4, x_3;
6) x_5, x_4, x_1;
7) x_2, x_5, x_6.

и циклы, состоящие из четырёх элементов:

1) x_2, x_3, x_6, x_7;
2) x_1, x_3, x_7, x_4;
3) x_1, x_2, x_5, x_7;
4) x_1, x_2, x_4, x_6;
5) x_1, x_3, x_5, x_6;
6) x_4, x_5, x_6, x_7;
7) x_2, x_3, x_4, x_5.

Если записать все вершины ($x_1, x_2, x_3, x_4, x_5, x_6, x_7$) матроида Фано в строчку, а под ними записывать все циклы, ставя единицу напротив вершины, через которую данный цикл проходит, и нуль в противном случае, то получится таблица циклов матроида Фано.

Таблица 1

№ строки	x_1	x_2	x_3	x_4	x_5	x_6	x_7
1	1	1	1	0	0	0	0
2	0	0	1	0	1	0	1
3	1	0	0	0	0	1	1
4	0	1	0	1	0	0	1
5	0	0	1	1	0	1	0
6	1	0	0	1	1	0	0
7	0	1	0	0	1	1	0
8	0	1	1	0	0	1	1
9	1	0	1	1	0	0	1
10	1	1	0	0	1	0	1
11	1	1	0	1	0	1	0
12	1	0	1	0	1	1	0
13	0	0	0	1	1	1	1
14	0	1	1	1	1	0	0

Данная таблица представляет собой матрицу H, в которой строка 1 дополняется строкой 13; строка 2–11; строка 3–14; строка 4–12; строка 5–10; строка 6–8 и строка 7–9.

Мы выбираем в качестве базиса множество (x_1, x_3, x_7), поскольку элементы x_1, x_3, x_7 образуют знакомый всем базис $\{i, j, k\}$ векторного пространства. И если добавить к базису элемент x_2, то увидим, что во множестве $\{x_1, x_2, x_3, x_7\}$ содержится единственный трёхэлементный цикл $\{x_1, x_2, x_3\}$, а цикла в цикле быть не может. Если мы добавим к базе элемент x_4, то получим $\{x_1, x_3, x_4, x_7\}$ – цикл, который уже есть в таблице циклов, а цикл не может быть базисом. Если мы добавим к базе элемент x_5, то получим $\{x_1, x_3, x_5, x_7\}$, где содержится единственный трёхэлементный цикл $\{x_7, x_5, x_3\}$, а если добавим x_6, то получим $\{x_1, x_3, x_6, x_7\}$, где содержится единственный трёхэлементный цикл $\{x_1, x_6, x_7\}$, а цикла в цикле быть не должно. Таким образом, $\{x_1, x_3, x_7\}$ – базис матроида Фано, следовательно, ранг матроида Фано равен трём. Составим таблицу схемы разделения секрета по нашему базису.

Под **разделением секрета** понимают любой метод распределения секрета среди группы участников, каждому из которых достается доля секрета. Секрет потом может воссоздать только разрешённая коалиция участников, а неразрешённая коалиция никакой информации о секрете не получает.

Сопоставим $x_1 \to S_1$, $x_2 \to S_2$, $x_3 \to S_3$ и так далее и выразим через базис остальные элементы, получив $S_2=S_1+S_3$, $S_5=S_3+S_7$, $S_6=S_1+S_7$, $S_4=S_1+S_3+S_7$.

Построим таблицу схемы разделения секрета (СРС), перебрав все возможные сочетания базиса (в левой части таблицы), т.е. элементов S_1, S_3, S_7. Поскольку поле двоичное, а базис состоит из 3 элементов, то вариантов сочетаний будет всего 8. Заполним правую часть таблицы для всех элементов матроида: S_1 берём из левой части таблицы; S_2 вычисляем как S_1+S_3; S_3 снова берём из левой части таблицы; S_4 вычисляется как $S_1+S_3+S_7$; S_5 – это S_3+S_7; S_6 – S_1+S_7; S_7 берём из левой части таблицы. Все операции сложения выполняются по модулю 2.

Таблица 2

S_1	S_3	S_7	S_1	S_2	S_3	S_4	S_5	S_6	S_7
0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	1	1	1
0	1	0	0	1	1	1	1	0	0
0	1	1	0	1	1	0	0	1	1
1	0	0	1	1	0	1	0	1	0
1	0	1	1	1	0	0	1	0	1
1	1	0	1	0	1	0	1	1	0
1	1	1	1	0	1	1	0	0	1

Для подтверждения того, что таблица СРС матроида Фано является матрицей циклов матроида, двойственного матроиду Фано, построим таблицу, в которой перечислим все базы и кобазы матроида Фано.

Таблица 3

Базы	Кобазы	Базы	Кобазы	Базы	Кобазы
$\{x_1, x_2, x_4\}$	$\{x_3, x_5, x_6, x_7\}$	$\{x_5, x_6, x_1\}$	$\{x_2, x_3, x_4, x_7\}$	$\{x_2, x_3, x_6\}$	$\{x_1, x_4, x_5, x_7\}$
$\{x_1, x_2, x_5\}$	$\{x_3, x_4, x_6, x_7\}$	$\{x_1, x_3, x_5\}$	$\{x_2, x_4, x_6, x_7\}$	$\{x_2, x_3, x_7\}$	$\{x_1, x_4, x_5, x_6\}$
$\{x_1, x_2, x_6\}$	$\{x_3, x_4, x_5, x_7\}$	$\{x_1, x_3, x_7\}$	$\{x_2, x_4, x_5, x_6\}$	$\{x_3, x_4, x_5\}$	$\{x_1, x_2, x_6, x_7\}$
$\{x_1, x_2, x_7\}$	$\{x_3, x_4, x_5, x_6\}$	$\{x_2, x_4, x_6\}$	$\{x_1, x_3, x_5, x_7\}$	$\{x_3, x_4, x_7\}$	$\{x_1, x_2, x_5, x_6\}$
$\{x_2, x_3, x_4\}$	$\{x_1, x_5, x_6, x_7\}$	$\{x_1, x_4, x_7\}$	$\{x_2, x_3, x_5, x_6\}$	$\{x_3, x_4, x_1\}$	$\{x_2, x_5, x_6, x_7\}$
$\{x_2, x_3, x_5\}$	$\{x_1, x_4, x_6, x_7\}$	$\{x_1, x_5, x_6\}$	$\{x_2, x_3, x_4, x_7\}$	$\{x_1, x_5, x_7\}$	$\{x_2, x_3, x_4, x_6\}$
$\{x_2, x_4, x_6\}$	$\{x_1, x_2, x_3, x_7\}$	$\{x_3, x_5, x_6\}$	$\{x_1, x_2, x_4, x_7\}$	$\{x_4, x_5, x_7\}$	$\{x_6, x_1, x_2, x3\}$
$\{x_4, x_5, x_6\}$	$\{x_7, x_1, x_2, x_3\}$				

Если к каждой базе добавлять поочерёдно элементы из списка соответствующих кобаз, то получатся циклы матроида, двойственного матроиду Фано:

1) $\{x_1, x_2, x_5, x_7\}$;
2) $\{x_2, x_3, x_4, x_5\}$;
3) $\{x_1, x_3, x_5, x_6\}$;
4) $\{x_1, x_2, x_4, x_6\}$;
5) $\{x_2, x_3, x_6, x_7\}$;
6) $\{x_1, x_3, x_4, x_7\}$;
7) $\{x_4, x_5, x_6, x_7\}$.

Если выписать из правой части таблицы 2 те элементы, значение которых равно единице, и обозначить их не S_1, S_2 и т. д., а x_1, x_2 и т. д., то мы получим те же самые циклы матроида, двойственного матроиду Фано.

Таким образом получается, что таблица 2 представляет собой выколотый код Рида – Маллера схемы разделения секрета. В то же время эта таблица является матрицей G, т. е. матрицей циклов матроида, двойственного матроиду Фано.

Если дальнейшая проверка гипотезы на матроидах, представимых как векторные над $GF(3)$ и $GF(q)$, а также на других матроидах, о возможности построения идеальной схемы разделения секрета по циклам двойственного матроида подтвердит её справедливость, то задачу можно будет считать решённой.

References

1. Alekseichuk A.N., Boyarinova Yu.E. Modulyarnaya skhema razdeleniya sek-reta nad kol'tsom gaussovykh tselykh chisel [Modular Secret Separation Scheme over the Loop of Gaussian Integers]// Reestrashchya, zbershannya i obrobka danikh. - V. 9, No. 1, 2007. - p. 87-99.

2. Anikevich E.A., Eremeev M.A., Kornienko A.A. Vysokoskorostnye algoritmy i protokoly kriptograficheskoi zashchity informatsionnykh resursov zheleznodorozhnogo transporta [Highspeed Algorithms and Protocols of Cryptographic Security of Information Resources of railway Transport]// Izvestiya Peterburgskogo universiteta putei soobshcheniya. - Issue 2. – St. Petersburg: PGUPS Publ., 2004. - p. 85-88.

3. Asanov M.O., Baranskii V.A., Rasin V.V. Diskretnaya matematika: grafy, matroidy, algoritmy [Discrete Mathematics: Graphs, Matroids, and Algorithms]. - Izhevsk: research and development center 'Regular and Chaotic Dynamics', 2001. - 288 p.

4. Vvedenie v kriptografiyu / Pod obshch. red. V.V. Yashchenko [Introduction into Cryptography/Under the Editorship of V.V. Yaschenko]. - St. Petersburg: Piter Publ., 2001. - 288 p.

Сорокина Светлана Викторовна, аспирант УрГУПС, г. Екатеринбург. E-mail: sorokina@ifsusu.ru

Титов Сергей Сергеевич, д. ф.-м. н., профессор УрГУПС. E-mail: stitov@usaaa.ru

Svetlana Viktorovna Sorokina, PhD student of Ural State University of Railway Transport, Yekaterinburg. E-mail: sorokina@ifsusu.ru

Sergey Sergeevich Titov, PhD Physics and Mathematics, Professor of Ural State University of Railway Transport. E-mail: stitov@usaaa.ru