УДК 004-514.144.25 Вестник УрФО № 1(31) / 2019, с. 23–30

Ведунова М. В., Игнатова А. О., Титов С.С.

DOI: 10.14529/secur190104

ЗАДАЧА БЛОКИРОВКИ ТРОЕК ШТЕЙНЕРА

В статье рассматриваются задачи блокировки многообразий как проблема информационной безопасности, применимая в схемах разделения секрета, совершенных шифрах и теории кодирования. Излагается подход к решению этой проблемы, основанный на блокировке двумерных аффинных многообразий над полем GF(2), связанной с блокировкой троек Штейнера. В работе рассмотрены блокирующие множества на тринадцати, пятнадцати, тридцати одном и шестидесяти трех элементах, а также предложены конструкции рекуррентного построения блокирующих множеств. Для них найдены максимальные и минимальные мощности.

Ключевые слова: *NSUCRYPTO, разделение секрета, системы троек Штейнера, плоскость Фано, проективное пространство.*

Vedunova M., Ignatova A., Titov S.

THE PROBLEM OF BLOCKING STEINER TRIPLES

This article considering the problem of blocking varieties as a problem of information security, applicable in secret separation schemes, perfect ciphers and coding theory. We present an approach to solving this problem based on the blocking of two-dimensional affine varieties over the field GF(2) associated with the blocking of Steiner triples. The paper considers blocking sets on thirteen, fifteen, thirty-one and sixty-three elements, and also proposes recurrent constructions of blocking sets. The maximum and minimum cardinalities are found for them.

Keywords: *NSUCRYPTO, secret sharing, system of Steiner triples, Fano plane, projective space.*

Во втором раунде международной Интернет-олимпиады по криптографии NSUCRYPTO-2015 [1] была предложена задача на специальный приз программного комитета «A secret sharing», в ноябре 2016 г. отмеченная как все еще не решенная. Постановка задачи требует предложить для каждого натурального $n \in \mathbf{N}$ явную конструкцию подмножества M множества F_2^n всех битовых строк длины n, удовлетворяющего следующим двум условиям:

1) каждый элемент $u \in M$ может быть представлен в виде $u=x \oplus y \oplus z$, где x, y, z – различные элементы множества $L=\bar{M}=F_2^n \setminus M$;

2) для любых трех различных $x, y, z \in \bar{M}$ справедливо $x \oplus y \oplus z \in M$.

Надо пояснить, что на специальный приз программного комитета этой Олимпиады предлагаются проблемы, решение которых неизвестно.

Данная проблема была частично решена для четных размерностей в публикации [О явных конструкциях для решения задачи «A secret Sharing»] на конференции Сиб-

Крипт-2017 командой Уральского государственного университета путей сообщения: К. Л. Геут, К. А. Кириенко, П. О. Садков, Р. И. Таскин, С. С. Титов [2]. Именно поэтому проблема требует продолжения усилий по ее окончательному решению.

В данной работе рассмотрены подходы к такого типа задачам как задачам блокировки и, в частности, изложены методы решения задачи блокировки троек Штейнера. При этом исходная задача «A Secret Sharing» трактуется как задача блокировки двумерных аффинных многообразий над полем GF(2). Поскольку каждое такое многообразие является сдвигом однозначно определенного двумерного линейного многообразия, соответствующего линейной тройке Штейнера, т.е. трёхэлементному множеству{x,y,z} ненулевых битовых строк x, y, z такому, что $x \oplus y \oplus z = 0$, то задача блокировки троек Штейнера может трактоваться как вспомогательный этап при решении исходной задачи, а её результаты и конструкции могут быть полезны в более общих проблемах [3].

Цель работы – выявление закономерности между мощностями блокирующих множеств. Данная закономерность позволит быстро находить мощность блокирующего множества. Так как в работе будут рассматриваться как линейные, так и нелинейные множества, то закономерности будут разные. Требуется найти максимальные и минимальные мощности блокирующего множества в системах троек Штейнера, построенных на разных количествах v элементов. Существуют линейные системы (с $v=2^n-1$ элементами, где $n \geq 3$) и нелинейные. Эти системы троек применимы, например, для построения совершенных кодов [4].

Общая постановка задачи блокировки и её применение в информационной безопасности состоит в следующем. Имеется некоторое множество F (элементов), в котором дано семейство подмножеств J (блоков), покрывающих F. Изучается задача построения такого подмножества M или его дополнения L=F\M, что в каждом блоке B семейства J окажется хотя бы один элемент подмножества M. Естественно рассматривать минимальные (по включению) подмножества M и называть их *блокирующими множествами*. Если пользоваться метафорой блоков как контролируемых пространств или траекторий движения злоумышленника, то блокирующие множества представляют собой в этой метафоре блок-посты или контролирующие устройства [5]. Двойственным образом, естественно рассматривать дополнения L блокирующих множеств, характеризующиеся как максимальные (по включению) подмножества множества F, не включающие в себя целиком ни одного блока B из семейства блоков J. В нашей метафоре это – пространство для маневра (с точки зрения противника, стремящегося сделать его наибольшим). Если рассматриваемые семейства и множества имеют конкретную математическую природу, то получаются конкретные математические задачи блокировки. Так, если F – множество элементов некоторого матроида, а J – семейство его циклов, то L – его максимальное независимое подмножество, т.е. база. Матроиды естественным образом возникают в теории идеальных схем разделения секрета [6]. В этом случае, как известно, решение задачи дается жадным алгоритмом. В задаче «A Secret Sharing» дано F – множество битовых строк длины n, а J – семейство двумерных аффинных многообразий над полем GF(2) в этом пространстве.

Классические версии задачи блокировки имеются в теории блок-схем, в том числе задача Киркмана [7, 8].

Примером задачи блокировки является и блокировка прямых на конечной плоскости. Блокирующие множества в проективной плоскости – это множество точек, пересекающих множество линий. Блокирующее множество называется тривиальным, если он содержит прямую линию и минимальным, если никакое из его собственных подмножеств не является блокирующим множеством. Блокирующее множество минимально, если удаление от любой точки оставляет множество, которое не является блокирующим множеством. Эта задача актуальна и для разделения секрета, и для теории совершенных шифров [12, 6, 13, 14, 15]. В теории совершенных шифров [12] блокировка троек {x,y,k}, где x – открытый текст, y – закрытый текст, k – ключ в уравнении зашифрования y=x*k означает атаку по шифртексту или атаку на ключ, что для троек Штейнера {x,y,k} равносильно блокировке в квазигруппе Штейнера с умножением y=x*k.

Задача данного исследования заключается в поиске максимальной и минимальной мощностей блокирующего множества для нескольких множеств. Применяется метод жадного алгоритма. Главный принцип жадного алгоритма заключается в принятии локально оптимальных решений на каждом этапе, до-

пуская, что конечное решение также окажется оптимальным. В условиях поставленной классической задачи структура задается матроидом – семейством подмножеств некоторого множества, представляющая собой обобщение идеи независимости элементов, аналогично независимости элементов линейного пространства, на произвольное множество. Результат применения этого алгоритма в общем случае зависит от упорядочивания элементов, входящих в систему троек Штейнера. Так как мы будем рассматривать неизоморфные системы троек Штейнера и различные упорядочения элементов, результат может быть неодинаковым. Задача состоит в построении блокирующих множеств и выяснении возможных значений, который может принимать их мощность (в том числе особенно важны максимальная и минимальная мощности).

Рассмотрев блокирующее множество для v=7, сможем убедиться в том, что результат получения мощностей будет одинаков. Это произойдет потому, что данное блокирующее множество относится к полю Фано и система, в конечном итоге, будет представлять из себя матроид Фано – матроид ранга три [16] Это векторный матроид, связанный с семью ненулевыми векторами в трехмерном векторном пространстве (над полем из двух элементов). Из общей теории следует, что все базы матроида всегда имеют одинаковую мощность.

Система троек, построенная на тринадцати элементах, не относится к линейным. Так как при v=13 мы будем рассматривать неизоморфные системы троек (их две) и различные упорядочения элементов, то результат может быть неодинаковым.

Применение жадного алгоритма к задаче блокировки заключается в выполнении двух его этапов: некоторое линейное упорядочивание элементов множества и, затем, построение множества L путём поочерёдного добавления к нему каждого нового наименьшего (в смысле этого упорядочения) элемента при условии, что это не приводит к появлению блока в L. Очевидно, что в случае, когда блоки – это циклы некоторого матроида, то результатом такого построения L оказывается база этого матроида, а M – его кобаза.

Рассмотрим первую систему [7]:

1,2,3 1,4,5 1,6,7 1,8,9 1,10,11 1,12,13 2,4,6 2,5,7 2,8,10 2,9,12
2,11,13 4,3,8 4,7,9 4,10,13 4,11,12 7,3,11 7,8,13
7,10,12 8,5,11 8,6,12 6,9,11 3,5,12 3,6,10
3,9,13 5,6,13 5,9,10

При переборе элементов в прямой последовательности найдем мощности множеств L и M, где M – блокирующее множество, L= – дополнение к M.

L={1,2,4,7,8,11} – отсюда следует, что мощность дополнения L=6, из этого следует, что мощность блокирующего множества |M|=7.

Найдем мощности множеств L и M при других порядках перебора элементов:

В обратной последовательности: 13,12,…,2,1; L={13,12,11,10,9,8} – получим мощность дополнения |L|=6, тогда |M|=7.

В иной последовательности получим: L={13,1,2,4,8} – отсюда следует, что мощность дополнения |L|=5, тогда мощность блокирующего множества |M|=8.

Рассмотрим вторую систему троек [7]:

1,2,3 1,4,5 1,6,7 1,8,9 1,10,11 1,12,13 2,4,6 2,5,7 2,8,10 2,9,12
2,11 13 4,3,8 4,7,9 4,10,13 4,11,12 7,3,11 7,8,13
7,10,12 8,5,11 8,6,12 6,9,11 3,5,12 6,9,13
3,9,10 5,6,10 5,9,13

При переборе элементов в прямой последовательности найдем мощности множеств L и M:

L={1,2,4,7,8,11} – тогда мощность дополнения |L|=6, отсюда мощность блокирующего множества |M|=7.

Найдем мощности множеств L и M при других порядках перебора элементов:

В обратной последовательности 13,12,…,2,1; L={13,12,11,10,9,8} – отсюда получим мощность дополнения |L|=6, тогда мощность |M|=7.

В иной последовательности:

13,1,2,4,8,3,6,12,11,9,5,10,7; L={13,1,2,4,8} – получим мощность дополнения |L|=5, отсюда следует, что мощность блокирующего множества |M|=8.

В обеих системах, состоящих из 26 троек, мощности блокирующего множества получились равными 7 и 8, где |M|=8 – это максимальная мощность и |M|=7 – это минимальная мощность блокирующего множества.

Соответственно, если |M|=7 – это минимальная мощность M, тогда |L|=6 C_6^3 это максимальная мощность множества L.

Аналогично, если максимальная мощность блокирующего множества равна восьми, то минимальная мощность дополнения равна семи.

При M<7 троек будет недоставать. Это видно если посчитать сочетания, например при M= 6, из 6 элементов по 3: =6!/(3!*(6-3)!)=20 троек.

При v=7, получаем трехбитные строки, где побитовая сумма строк равна нулю. Блокирующее множество для данной системы показано на плоскости Фано, представляющей из себя конечную проективную плоскость второго порядка, имеющую наименьшее возможное число точек и прямых (7 точек и 7 прямых), с тремя точками на каждой прямой и с тремя прямыми, проходящими через каждую точку.

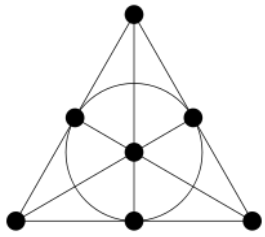

Рис. 1. Плоскость Фано

Здесь очевидно, что единственным решением является |M|=3, |L|=4, и в качестве блокирующего множества M выступает любая прямая, так как на проективной плоскости любые две прямые пересекаются.

Перейдем к рассмотрению множества на пятнадцати элементах (т.е. при v=15). Система, представленная ниже, относится к линейным, так как ее умножение * в квазигруппе Штейнера сводится к побитовому сложению:

u*v=u⊕v, если u≠v, иначе u*u=u, хотя u⊕u=0.

Система, представленная ниже, относится к линейным.

1,2,3	1,4,5	1,6,7	1,8,9	1,10,11	1,12,13	1,14,15	2,4,6	3,4,7	4,8,12
	5,8,13		6,8,14	7,8,15	2,7,5	3,5,6	4,9,13		5,9,12
	6,9,15		7,9,14	2,8,10	3,8,11		4,10,14		5,10,15
	6,10,12		7,10,13	2,9,11	3,9,10		4,11,15		5,11,14
	6,11,13		7,11,12	2,12,14	3,12,15		2,13,15		3,13,14

Для данной системы найдено два решения.

При переборе элементов в прямой последовательности получим:

L={1,2,4,7,8,11,13,14} – отсюда следует, что мощность дополнения |L|=8, тогда мощность блокирующего множества |M|=7.

При переборе элементов в другой последовательности, например, при (1,2,4,8,15,3,8,5,6,9,10,12,14,13,11,7), получим:

L={1,2,4,8,15}, то есть мощность дополнения равна |L|=5, тогда мощность блокирующего множества равна |M|=10.

Итог: если мощность дополнения равная пяти – это минимальная мощность дополнения, то мощность блокирующего множества равная десяти – это максимальная мощность блокирующего множества. И аналогично получим: если мощность дополнения равная восьми – это максимальная мощность дополнения, то мощность блокирующего множества равная семи – это минимальная мощность блокирующего множества.

При рассмотрении блокирующего множества v=15 получили, аналогичные трехбитным, четырехбитные строки. На данном множестве также определяется система линейных троек Штейнера, где побитовая сумма строк будет равна нулю.

Рассмотрим систему Штейнера на тридцати одном элементе (т.е. при v=31), которая также является линейной на множестве ненулевых пятибитных строк. Для троек на данном множестве были найдены следующие решения.

При переборе элементов в прямой последовательности получим:

L=1,2,4,7,8,11,13,14,16,19,21,22,25,26,28,31, тогда получим мощность дополнения равную |L|=16, отсюда получим мощность блокирующего множества |M|=15.

При переборе элементов в другой последовательности, например, при (17,29,14,26,3, 30,20,1,22,2,12,16,24,5,31,8,13,18,4,6,7,9,23,15,2 8,21,25,11,19,10) получим:

L={4,26,3,1,22,5,8,10} тогда мощность дополнения |L|=10, получим мощность блокирующего множества |M|=21.

При переборе элементов в другой последовательности, например, при (29,18,13,30,28 ,21,16,18,9,20,6,15,24,14,10,26,12,5,22,25,31,23, 17,11,19,3,4, 7,2,27) получим: L={29,18,13,30,28,21,20,26,5} – отсюда получим мощность дополнения |L|=9, тогда мощность блокирующего множества |M|=22.

Таким образом, для множества v=31 максимальная мощность M равна 22, средняя – 21 и минимальная – 15. При рассмотрении данного множества получили пятибитовые строки, где сумма побитовых строк равна нулю.

Рассмотрим множество на шестидесяти трех элементах.

При рассмотрении данного множества получили следующие мощности блокирующего множества:

При переборе элементов в прямой последовательности получили следующий результат:

L={1,2,4,7,8,11,13,14,16,19,21,22,25,26,28,3 2,35,37,38,41,42,44,47,49,50,52,55,56,59,61,62} – мощность дополнения |L|=31, тогда мощность блокирующего множества |M|=32.

При переборе элементов в другой последовательности, например, при 1,2,4,8,15,16,32 ,51,21,42,30,57,27,3,5,6,9,10,12,7,11,13,14,17,18, 20,24,31,33,36,40,47,48,34,50,49,55,59,60,35,19, 23,29,26,53,38,43,46,37,58,63,25,28,22,62,52,45, 56,61,54,41,44,39, получим: L={1,2,4,8,15,16,32, 51,21,42,30,57,27} – мощность дополнения |L|=13, тогда мощность блокирующего множества |M|=50.

При переборе элементов в другой последовательности, например, при 17,57,53,14,60, 36,50,4,49,25,58,15,27,59,38,47,41,29,21,20,28,1 ,39,46,44,40,34,9,

52,16,45,43,35,51,63,54,12,23,5,19,61,6,22,5 6,7,48,11,13,2,10,24,26,31,8,32,62,3,

37,42,33,30,18,59, получим:

L={17,57,53,14,60,4,25,58,27,38,47,41,20,1,5 1,7,11,24,14} – тогда мощность дополнения |L|=19; отсюда следует, что мощность блокирующего множества |M|=44.

Таким образом, при рассмотрении данного множества результаты получились следующие: максимальная получившаяся мощность блокирующего множества равна 50, средняя - 44, и минимальная равна 32. Получены шестибитовые строки, побитовая сумма которых равна нулю.

Сведем результаты в одну таблицу:

Таблица 1

$v= F_n^2-1$	n	$\|L\|$	$\|M\|$
7	3	3	4
15	4	5; 8	10; 7
31	5	9; 20; 16	22; 21; 15
63	6	13; 19; 31	50; 44; 32

При n=4 представлены максимальная и минимальная мощность блокирующего множества. При n>4 могут быть и другие значения мощности блокирующего множества.

Перейдем к рассмотрению **рекуррентного построения** блокирующего множества для линейных систем битовых строк, что как раз и требуется для проблемы «A secret sharing».

Пусть во множестве $S_n= \overline{F_n^2} \backslash 0$ блокирующее множество M и его дополнение L построены. Предлагается использовать эти множества для решения задачи блокировки (линейных) троек Штейнера во множестве $S_k= F_2^k \backslash 0$ при k>n.

Множество L удовлетворяет, как максимальное подмножество в S_n, не содержащее ни одной тройки, следующим двум условиям:

Для любых трех различных элементов $x_1,x_2,x_3 \in L$ справедливо x1+x2+x3≠0; (отсутствие троек);

Для любого $u \in M=Sn \backslash L$ существуют так же $x_1,x_2 \in L$, что u=x1+x2; (максимальность такого L).

Рассмотрим множество $L_k \subset S_k$ вида $L_k=L_n \oplus M_{k-n}$, где $L_n=L$, а $M_{k-n} \subset F_2^k$ есть множество битовых строк длины k, в которых первые n битов равны нулю.

Проверка выполнения L_k выписанных двух условий:

Пусть l_1,l_2,l_3 – различные элементы множества S_k. Их можно считать заданными в виде пар $l_i=(x_i,y_i)$ (i=1,2,3), где $x_i \in L_n$ (а последние (n-k) битов равны нулю), $y_i \in M_{k-n}$ (а первые n битов равны нулю).

Если $x_1 \neq x_2 \neq x_3 \neq x_1$, то $l_1+l_2+l_3=x_1$, y_1+x_2,

$y_2+x_3, y_3=(x_1+x_2+x_3,\ y_1+y_2+y_3)\neq(0,0)$, так как $x_1+x_2+x_3\neq 0$ по первому условию для множества Ln.

Если $x_1=x_2$, то для выполнения равенства $l_1+l_2+l_3=0$ необходимо $x_1+x_2+x_3=0$, откуда $x_3=0$, что невозможно, так как $0\notin L_n$.

Следовательно, первому условию L_k удовлетворяет.

Пусть теперь $(u,v)\notin L_k$. Если $u\neq 0$, то $u\notin L_n$, и, значит, существуют такие $x_1, x_2\in L_n$, что $x_1+x_2=u$, $x_1\neq x_2$. Взяв произвольные $y_1, y_2\in M_{k-n}$ такие, что $y_1+y_2=v$ (например, $y_1=v$, $y_2=0$) и положив $l_1=(x_1, y_1)$, $l_2=(x_2, y_2)$, получим $l_1, l_2\in L_k$, $l_1\neq l_2$, $l_1+l_2=(u, v)$.

Если же u=0, то $v\neq 0$, и для произвольного $x\in L_n$ взяв $l_1=(x, 0)$, $l_2=(x, v)$, получим опять $l_1, l_2\in L_k$, $l_1\neq l_2$, $l_1+l_2=(u, v)$, то есть L_k удовлетворяет и второму условию. Получаем:

Утверждение. Для любого L в S_n, удовлетворяющего условиям (1) и (2), существует L_k в S_n (при k>n), удовлетворяющее этим условиям и имеющее мощность $|L_k| = |L| * 2^{k-n}$.

Это – обобщение конструкции удвоения (при k=n+1).

Как показывают примеры, имеются блокирующие множества, мощность которых отличается от выписанных в доказанном утверждении. Так, хотя максимальное значение мощности L_k получается из конструкции удвоения, построение минимального по мощности множества L_k требует продолжения исследований.

Заключение. В ходе данного исследования найдены мощности линейных (v=7, v=15, v=31, v=63) блокирующих множеств, а также мощности нелинейного блокирующего множества для v=13, предложен метод рекуррентного построения блокирующих множеств. С помощью данного метода можно находить мощность блокирующего множества при любых n.

Литература

1. Сайт олимпиады NSUCRYPTO [Электронный ресурс]. – Режим доступа: http://nsucrypto.nsu.ru/, свободный (дата обращения 31.01.2019)

2. Geut K., Kirienko K., Sadkov P., Taskin R., Titov S. On explicit constructions for solving the problem «A secret sharing» // Prikladnaya Diskretnaya Matematika. Prilozhenie. 2017. №10. P.68–70. (in Russian).

3. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: Изд-во. Урал. ун-та, 2003. – 328 с.

4. Ковалевская Д.И., Соловьева Ф.И., Филимонова Е.С. О системах троек Штейнера малого ранга, вложимые в совершенные двоичные коды // Дискретный анализ и исследование операций. 2013. Т. 20. №3(111). С. 3-25.

5. Башуров В.В. Математические модели безопасности / В.В. Башуров, Т.И. Филимоненкова. – Новосибирск: Наука, 2009. – 87 с. ISBN 978-5-02-023288-4.

6. Введение в криптографию // под общ. ред. В. В. Ященко. СПб.: Питер, 2001.

7. Холл М. Комбинаторика, Пер. с англ. – М.: Издательство «Мир», Москва. – 1970. – 424 с.

8. Медведев Н.В., Титов С.С. Об однородных идеальных схемах разделения секрета и матроидах коранга три // Вестник УрФО. Безопасность в информационной сфере. – 2015. – №4 (18) – С. 21 – 26.

9. Tama´s SzoUnyi. Blocking Sets in Desarguesian Affine and Projective Planes. FINITE FIELDS AND THEIR APPLICATIONS 3, 187–202 (1997) article No. FF960176.

10. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988.

11. Olga Polverino. Linear sets in finite projective spaces. Discrete Mathematics 310 (2010) 3096–3107.

12. Зубов А.Ю. Совершенные шифры. – М.: Гелиос АРВ, 2003. – 160 с.

13. Медведев Н.В., Титов С.С. О почти пороговых матроидах и схемах разделения секрета // Вестник УрФО. Безопасность в информационной сфере. 2012. № 1(3). С. 31–36.

14. Парватов Н.Г. Совершенные схемы разделения секрета // Прикладная дискретная математика. 2008. № 2(2). С. 50–57.

15. Болотова Е.А., Коновалова С. С., Титов С.С. Свойства решеток разграничения доступа, совершенные шифры и схемы разделения секрета // Проблемы безопасности и противодействия терроризму: материалы IV Междунар. науч. конф. М.: МЦНМО, 2009. Т. 2. С. 71–86.

16. Медведев Н.В., Титов С.С. Об однородных матроидах и блок-схемах. Прикладная дискретная математика. Приложение. №10. 2017. Труды 16-й Всероссийской конференции [Сибирская научная школа-семинар с международным участием «компьютерная безопасность и криптография»] – SIBECRYPT'17.

17. Геут К.Л., Титов С.С. О рекуррентных соотношениях в информационной безопасности. Вестник УрФО. Безопасность в информационной сфере. 2017. №1(23). С. 24-27.

18. Сайт Википедии [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Плоскость_Фано, свободный (дата обращения 31.01.2019)

References

1. Sajt olimpiady NSUCRYPTO [Jelektronnyj resurs]. – Rezhim dostupa: http://nsucrypto.nsu.ru/, svobodnyj (data obrashhenija 31.01.2019)

2. Geut K., Kirienko K., Sadkov P., Taskin R., Titov S. On explicit constructions for solving the problem «A secret sharing» // Prikladnaya Diskretnaya Matematika. Prilozhenie. 2017. №10. P.68–70. (in Russian)

3. Gajdamakin N.A. Razgranichenie dostupa k informacii v komp'juternyh sistemah. – Ekaterinburg: Izd-vo. Ural. un-ta, 2003. – 328 s.

4. Kovalevskaja D.I., Solov'eva F.I., Filimonova E.S. O sistemah troek Shtejnera malogo ranga, vlozhimye v sovershennye dvoichnye kody // Diskretnyj analiz i issledovanie operacij. 2013. T. 20. №3(111). S. 3-25.

5. Bashurov V.V. Matematicheskie modeli bezopasnosti / Bashurov V.V., Filimonenkova T.I. – Novosibirsk: Nauka, 2009. – 87 s. ISBN 978-5-02-023288-4.

6. Vvedenie v kriptografiju / pod obshh. red. V.V. Jashhenko. SPb.: Piter, 2001.

7. Holl M. Kombinatorika, Per. s angl. – M.: Izdatel'stvo «Mir», Moskva. – 1970. – 424 s.

8. Medvedev N.V., Titov S.S. Ob odnorodnyh ideal'nyh shemah razdelenija sekreta i matroidah koranga tri // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. – 2015. – №4 (18) – C. 21 – 26.

9. Tama´s SzoUnyi. Blocking Sets in Desarguesian Affine and Projective Planes. FINITE FIELDS AND THEIR APPLICATIONS 3, 187–202 (1997) ARTICLE NO. FF960176

10. Lidl R., Niderrajter G. Konechnye polja. M.: Mir, 1988.

11. Olga Polverino. Linear sets in finite projective spaces. Discrete Mathematics 310 (2010) 3096–3107

12. Zubov A. Ju. Sovershennye shifry. – M.: Gelios ARV, 2003. – 160 s.

13. Medvedev N.V., Titov S.S. O pochti porogovyh matroidah i shemah razdelenija sekreta // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2012. № 1(3). C. 31–36.

14. Parvatov N.G. Sovershennye shemy razdelenija sekreta // Prikladnaja diskretnaja matematika. 2008. № 2(2). S. 50–57.

15. Bolotova E.A., Konovalova S.S., Titov S.S. Svojstva reshetok razgranichenija dostupa, sovershennye shifry i shemy razdelenija sekreta // Problemy bezopasnosti i protivodejstvija terrorizmu: materialy IV Mezhdunar. nauch. konf. M.: MCNMO, 2009. T. 2. S. 71–86.

16. Medvedev N.V., Titov S.S. Ob odnorodnyh matroidah i blok-shemah. Prikladnaja diskretnaja matematika. Prilozhenie. №10. 2017. Trudy 16-j Vserossijskoj konferencii [Sibirskaja nauchnaja shkola-seminar s mezhdunarodnym uchastiem «komp'juternaja bezopasnost' i kriptografija»] – SIBECRYPT'17.

17. Geut K.L., Titov S.S. O rekurrentnyh sootnoshenijah v informacionnoj bezopasnosti. Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2017. №1(23). S. 24-27.

18. Sajt Vikipedii [Jelektronnyj resurs]. – Rezhim dostupa: https://ru.wikipedia.org/wiki/Ploskost'_Fano, svobodnyj (data obrashhenija 31.01.2019)

ВЕДУНОВА Марина Викторовна, студентка второго курса на специальности «Информационная безопасность», Электротехнический факультет, ФГБОУ ВО Уральский государственный университет путей сообщения (УрГУПС). 620034, Россия, г. Екатеринбург, ул. Колмогорова, 66. E-mail: marina.vedunova.13.99@gmail.com

ИГНАТОВА Анастасия Олеговна, студентка второго курса на специальности «Информационная безопасность», Электротехнический факультет, ФГБОУ ВО Уральский государственный университет путей сообщения (УрГУПС), 620034, Россия, г. Екатеринбург, ул. Колмогорова, 66. E-mail: anastasiaignatova101@gmail.com

ТИТОВ Сергей Сергеев, профессор кафедры «Естественнонаучные дисциплины», ФГБОУ ВО Уральский государственный университет путей сообщения (УрГУПС), 620034, Россия, г. Екатеринбург, ул. Колмогорова, 66. E-mail: stitov@usaaa.ru

VEDUNOVA Marina, student of the second year on the «Information security» specialty, Electrical technical faculty, Ural State University of Railway Transport (USURT), 620034, Russia the city of Ekaterinburg Kolmogorov, 66,. E-mail: marina.vedunova.13.99@gmail.com

IGNATOVA Anastasia, student of the second year on the «Information security» specialty, Electrical technical faculty, Ural State University of Railway Transport (USURT), 620034, the city of Ekaterinburg Kolmogorov 66, Russia, E-mail: anastasiaignatova101@gmail.com

TITOV Sergey, Doctor of Physical and Mathematical sciences, Professor of the «Natural Sciences» chair, Ural State University of Railway Transport (USURT), 620034, the city of Ekaterinburg Kolmogorov 66. E-mail: stitov@usaaa.ru