2009 Теоретические основы прикладной дискретной математики №4(6)

DOI 10.17223/20710410/6/4

УДК 621.394

РЕКУРСИВНЫЙ СПОСОБ ПОСТРОЕНИЯ СЕМЕЙСТВ БЕЗ ПЕРЕКРЫТИЙ[1]

А. В. Черемушкин

Институт криптографии, связи и информатики, г. Москва, Россия

E-mail: avc238@mail.ru

Предлагается модификация рекурсивного способа построения семейств множеств без перекрытий, основанная на использовании ортогональных массивов. Показано, как с их помощью можно построить схемы предварительного распределения ключей на основе пересечений множеств.

Ключевые слова: *семейство множеств без перекрытий, схема предварительного распределения ключей.*

1. Семейства множеств без перекрытий

Если X — множество из v элементов, $|X| = v$, а $\mathcal{F}$ — множество его подмножеств (блоков), $|\mathcal{F}| = b$, то $(X, \mathcal{F})$ называется (i, j)-*семейством без перекрытий* (*cover-free family*) и обозначается (i, j)-CFF(v, b), если для любых блоков $B_1, ..., B_u \in \mathcal{F}$, $u \leqslant i$, и любых не совпадающих с ними блоков $A_1, ..., A_w \in \mathcal{F}$, $w \leqslant j$, выполняется условие

$$\bigcap_{k=1}^{u} B_k \not\subseteq \bigcup_{s=1}^{w} A_s.$$

Матрица инцидентности системы множеств $(X, \mathcal{F})$ — это (0,1)-матрица размера $b \times v$, в которой столбцы соответствуют элементам множества X, а строки — подмножествам из $\mathcal{F}$, причем единицы стоят на пересечении со столбцами, помеченными элементами подмножества, соответствующего строке.

Непосредственно из определения вытекает следующий критерий.

Лемма 1 [1]. Система множеств $(X, \mathcal{F})$ является семейством без перекрытий (i, j)-CFF(v, b) в том и только в том случае, когда в ее матрице инцидентности для любых двух непересекающихся наборов, состоящих из i и j строк, найдется столбец, на пересечении которого с первым набором строк стоят единицы, а на пересечении со вторым — нули.

Следствие. Для параметров семейства (i, j)-CFF(v, b) выполняются неравенства $b \geqslant i + j$ и $v \geqslant \binom{i+j}{i}$.

Действительно, в матрице инцидентности для любого набора из $i+j$ строк должны найтись столбцы, содержащие всевозможные расположения из i единиц и j нулей.

2. Основная теорема

Ортогональным массивом OA$(n, k, 1)$ называется $n^2 \times k$-матрица с элементами из множества $\{1, \ldots, n\}$, каждые два столбца которой содержат все различные пары элементов.

[1]Работа выполнена при поддержке гранта Президента РФ НШ № 4.2008.10.

Лемма 2. Пусть $i \geqslant 1$, $j \geqslant 1$. В таблице ортогонального массива $\mathrm{OA}(n, ij+1, 1)$ для любых двух непересекающихся наборов, состоящих из i и j строк, найдется столбец, на пересечении с которым ни один из элементов, стоящих в строках из первого набора, не совпадает ни с одним из элементов, стоящих в строках из второго набора.

Доказательство. Рассмотрим два произвольных непересекающихся набора из i и j строк. Рассмотрим подтаблицу, состоящую из первой строки первого набора и всех строк второго набора. В каждом столбце этой подтаблицы выделим элементы первой строки, совпадающие с элементами этого же столбца, принадлежащими строкам второго набора. Из свойства ортогональности следует, что в строках второго набора совпадающие элементы не могут находиться в одинаковых строках, иначе найдутся два столбца с совпадающими парами элементов. Отсюда следует, что максимальное число столбцов с такими совпадениями равно j. Теперь в оставшихся столбцах элементы первой строки из первого набора не совпадают ни с одним из элементов строк второго набора. Удаляем в исходной таблице столбцы, в которых произошло совпадение элементов, и рассматриваем ортогональный массив из оставшихся столбцов. Повторяя рассуждения для оставшихся $i-1$ строк из первого набора, получаем, что совпадения элементов, стоящих на пересечении со строками из первого набора, с элементами из строк второго набора могут быть не более чем в ij столбцах. Теперь в оставшихся неудаленными столбцах элементы, стоящие в строках из первого набора, не совпадают с элементами из строк второго набора. ■

Теорема 1. Пусть $i \geqslant 2$, $j \geqslant 1$. Если существуют семейство без перекрытий (i,j)-$\mathrm{CFF}(v,b)$ и ортогональный массив $\mathrm{OA}(b, ij+1, 1)$, то существует и семейство (i,j)-$\mathrm{CFF}((ij+1)v, b^2)$.

Доказательство. Рассмотрим матрицу инцидентности A семейства (i,j)-$\mathrm{CFF}(v,b)$. Построим (0,1)-матрицу B размера $b^2 \times (ij+1)v$ путем замены каждого элемента a, $1 \leqslant a \leqslant v$, в матрице ортогонального массива $\mathrm{OA}(b, ij+1, 1)$ на строку матрицы A с номером a. В силу леммы 2 для любых двух непересекающихся наборов, состоящих из i и j строк ортогонального массива, найдется столбец, на пересечении с которым ни один из элементов, стоящих в строках из первого набора, не совпадает ни с одним из элементов, стоящих в строках из второго набора. Поэтому после замены всех элементов этого столбца на соответствующие строки матрицы A в построенной матрице B в силу леммы 1 найдется столбец, в котором на пересечении со строками из первого набора стоят единицы, а на пересечении со строками из второго набора — нули. По лемме 1 матрица B является матрицей инцидентности семейства (i,j)-$\mathrm{CFF}((ij+1)v, b^2)$. ■

3. Построение ортогональных массивов на основе разностных матриц

$(n,k;\lambda)$-*Разностной матрицей* называется матрица (d_{st}) размера $k \times n\lambda$ над кольцом вычетов $\mathbf{Z}_n$, в которой при всех x, y, $1 \leqslant x < y \leqslant k$, в мультимножестве

$$\{d_{xz} - d_{yz} \mod n : 1 \leqslant z \leqslant n\lambda\}$$

каждый из элементов $\mathbf{Z}_n$ встречается ровно λ раз.

В работе [1] разностные матрицы использовались для построения семейств без перекрытий. Предложенная там основная конструкция взята из работы [2]. Заметим, что она может быть интерпретирована в терминах ортогональных массивов. Для этого следует воспользоваться следующим способом построения ортогональных массивов

на основе разностных матриц. Если выполнено условие $(n,(k-1)!)=1$, то $(n,k;1)$-разностную матрицу $D=(d_{xz})$ можно построить, полагая при $1\leqslant x\leqslant n$ и $1\leqslant z\leqslant k$

$$d_{xz}=xz \bmod n.$$

По уже построенной $(n,k;1)$-разностной матрице $D=(d_{xz})$ ортогональный массив $\mathrm{OA}(n,k,1)$ с матрицей $B=(b_{(x,y),z})$ размера $n^2\times k$ строится следующим образом: при $1\leqslant x,y\leqslant n$ и $1\leqslant z\leqslant k$ полагают

$$b_{(x,y),z}=d_{xz}+y \mod n.$$

Разностные матрицы над произвольными абелевыми группами и способ построения на их основе ортогональных массивов описаны, например, в [3].

4. Рекурсивное построение семейств без перекрытий

В работе [1] предложен рекурсивный способ, позволяющий из семейств без перекрытий (i,j)-$\mathrm{CFF}(v,b)$ и $(b^{2^t},ij+1,1)$-разностных матриц, $t=0,1,2,\ldots$, которые существуют при условии $(b,(ij)!)=1$ [2], строить новые семейства (i,j)-$\mathrm{CFF}((ij+1)^t v_0, b_0^{2^t})$. Вместе с тем условие $(b,(ij)!)=1$ ограничивает возможность его применения.

Рассмотрим естественную модификацию этого способа, основанную на использовании теоремы 1 и позволяющую строить такие семейства для более широкого класса значений (i,j,v,b).

Выберем b_0 так, чтобы при каждом $t=0,1,2,\ldots$ выполнялось условие существования ортогонального массива $\mathrm{OA}(b^{2^t},ij+1,1)$. Теперь, начиная с семейства (i,j)-$\mathrm{CFF}(v_0,b_0)$, будем последовательно применять теорему 1. В результате будет построена последовательность семейств

$$\{\ (i,j)\text{−}\mathrm{CFF}((ij+1)^t v_0, b_0^{2^t})\ :\quad t=1,2,\ldots\ \},$$

параметры v,b каждого из которых удовлетворяют условию

$$v=v_0(\log_{b_0} b)^{\log_2(ij+1)}.$$

Заметим, что результат из работы [1] получается как частный случай теоремы 1. Хотя использование разностных матриц существенно упрощает саму процедуру построения, теорема 1 позволяет расширить по сравнению с [1] множество допустимых значений параметров (i,j,v,b), для которых можно построить семейство без перекрытий.

В работе [1] для заданных (i,j) выбиралось такое минимальное число $b_0\geqslant i+j$, что выполнялось условие $(b_0,(ij)!)=1$, причем из него автоматически вытекало равенство $(b_0^{2^t},(ij)!)=1$ при всех $t=1,2,\ldots$ При этом число b_0 не могло иметь малых делителей.

В то же время ортогональные массивы существуют и при других значениях параметров (i,j,v,b). Например, так как при любых $p\geqslant 2$ и $m\geqslant 1$ ортогональные массивы $\mathrm{OA}(p^m,p^m+1,1)$ легко строятся на основе поля из p^m элементов, то можно строить семейства без перекрытий (i,j)-$\mathrm{CFF}(v,b)$ при $i+j\leqslant p^m=b_0$.

В силу леммы 1 минимальным семейством без перекрытий для заданных значений i и j будет семейство (i,j)-$\mathrm{CFF}(v,b)$ при $i+j=b$, в матрице инцидентности которого каждый столбец имеет ровно i единиц. Если при данном значении b не найдется соответствующего ортогонального массива, то выбираем значение $b_0\geqslant i+j$ так, чтобы при каждом $t=0,1,2,\ldots$ выполнялось условие существования ортогонального

массива $\mathrm{OA}(b^{2^t}, ij+1, 1)$. Теперь в качестве семейства (i,j)-CFF(v_0, b_0) берем то, у которого $v_0 = \min\left\{\binom{b}{i}, \binom{b}{j}\right\}$ и в матрице инцидентности каждый столбец имеет ровно i единиц при $i \leqslant j$ и $n-j$ единиц при $i > j$ соответственно.

В данном случае $v \geqslant b$. Применяя теорему, можно построить семейства с условием $v < b$. Например, при $b = 4$, последовательно применяя теорему 1, получаем семейства (2, 2)-CFF(6, 4), (2, 2)-CFF(30, 16), (2, 2)-CFF(150, 256), (2, 2)-CFF(750, 65536), (2, 2)-CFF(3750, 4294967296) и т. д.

5. Схемы предварительного распределения ключей

Пусть $g \geqslant 2$. Под схемой предварительного распределения ключей для групп, состоящих не более чем из g участников, понимают два алгоритма: первый определяет значения распределяемых между n участниками наборов данных, которые будем называть ключевыми материалами, а второй позволяет каждой группе, состоящей не более чем из g участников, вычислить значение ключа для организации закрытого сеанса. При этом должно выполняться условие, гарантирующее, что никакая другая группа участников, не включающая первую в качестве подмножества, объединив свои ключевые материалы, не сможет получить никакой информации о ключе. Более подробно см. обзор [4].

Пусть $w \geqslant 1$. Схема предварительного распределения ключей для групп участников называется устойчивой к сговору w участников, если любая группа, состоящая не более чем из w участников, объединив свои ключевые материалы, не сможет определить ключи, применяемые группами из оставшихся участников.

Определение [5]. *Устойчивая к сговору w участников схема распределения ключей на основе шаблонов для групп из g участников* (g,w)-CRKDP(n,k) (*collusion-resistant key distribution patterns*) определяется набором подмножеств $\{S_1, ..., S_n\}$ множества $\{1, \ldots, k\}$, удовлетворяющим условию: если $i_1, \ldots, i_g, p_1, \ldots, p_w \in \{1, \ldots, n\}$ и выполнено включение

$$\bigcap_{j=1}^{g} S_{i_j} \subseteq \bigcup_{j=1}^{w} S_{p_j},$$

то $\{i_1, \ldots, i_g\} \cap \{p_1, \ldots, p_w\} \neq \varnothing$.

Для ее применения надо сформировать множество из k секретных ключей и присвоить им номера $1, \ldots, k$. Распределение ключевых материалов осуществляется путем передачи заранее по защищенному каналу каждому абоненту P_i всех ключей с номерами из множества S_i. Теперь для формирования общего ключа каждый участник из группы участников $\{P_{i_1}, \ldots, P_{i_g}\}$ выбирает ключи, номера которых лежат в пересечении $S_{i_1} \cap \ldots \cap S_{i_g}$, а затем вычисляет общий ключ как значение хеш-функции от строки, составленной из этих ключей.

Так как данное определение по сути совпадает с определением семейства без перекрытий (g,w)-CFF(k,n), то, переформулируя теорему 1, получаем следующий результат для схем распределения ключей на основе шаблонов.

Теорема 2. Пусть $g \geqslant 2$, $w \geqslant 1$. Если существует (g,w)-CRKDP(n,k)-схема и ортогональный массив $\mathrm{OA}(n, gw+1, 1)$, то существует и (g,w)-CRKDP$(n^2, (gw+1)k)$-схема.

Используя данный подход в сочетании с [1], можно строить различные схемы предварительного распределения ключей на основе шаблонов. Например, при $g = w = 2$

можно в зависимости от условий применять следующие схемы:

n	256	625	2401	4096	65536
k	150	250	525	700	750

ЛИТЕРАТУРА

1. *Stinson D. R., van Trung T, Wei R.* Secure frameproof codes, key distribution patterns, group testing algorithms and related structures // J. Statist. Plan. Infer. 2000. V. 86. No. 2. P. 595–617.
2. *Atici M., Magliveras M. M., Stinson D. R., Wei W.-D.* Some recursive constructions for perfect hash families // J. Combinat. Designs. 1996. V. 44. P. 353–363.
3. *Beth T., Jungnickel D., Lenz H.* Design theory. Cambridge Univ. Press, 1989. 688 p.
4. *Черемушкин А. В.* Комбинаторно-геометрические подходы к построению схем предварительного распределения ключей (обзор публикаций) // Прикладная дискретная математика. 2008. № 1(1). С. 55–63.
5. *Mitchell C. J., Piper C.* Key storage in Secure Networks // Discr. Appl. Math. 1988. V. 21. P. 215–228.