2008 Математические методы криптографии № 1(1)
DOI 10.17223/20710410/1/10
УДК 621.394

КОМБИНАТОРНО-ГЕОМЕТРИЧЕСКИЕ ПОДХОДЫ К ПОСТРОЕНИЮ СХЕМ ПРЕДВАРИТЕЛЬНОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ (ОБЗОР)[1]

А.В. Черемушкин

Институт криптографии, связи и информатики Академии ФСБ России, г. Москва

E-mail: avc238@mail.ru

В обзоре рассматривается одна из схем предварительного распределения ключей, называемая схемой на основе пресечений множеств или схемой на основе шаблонов. Приводятся известные результаты об их свойствах и указываются способы построения таких схем.

Ключевые слова: *блок-схема, схема предварительного распределения ключей, схема пересечений множеств.*

Схемы предварительного распределения ключей на основе пресечений множеств являются очень простыми в использовании, не требующими реализации сложных алгебраических операций. Вместе с тем задача их построения оказывается достаточно трудной комбинаторной задачей. Примечательно, что конструкция таких схем явилась источником для применения целого ряда комбинаторных и геометрических понятий. Ниже будут приведены различные известные подходы к построению таких схем.

1. Основные определения

Под схемой предварительного распределения ключей обычно понимают два алгоритма. Первый определяет значения распределяемых между n участниками некоторых значений, которые будем называть ключевыми материалами, а второй позволяет каждой паре (или группе) 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.

При $n = 2$ достаточно передать каждому участнику один и тот же общий ключ. Поэтому далее предполагаем, что $n > 2$.

Приведем более точные определения.

Пусть $\boldsymbol{U} = \{1, \dots, n\}$ – множество участников; $\boldsymbol{P}, \boldsymbol{F} \subseteq 2^{\boldsymbol{U}}$, $\boldsymbol{P} \cap \boldsymbol{F} = \emptyset$, K – множество ключей.

Определение. *Схема предварительного распределения ключей* (*key predistribution scheme*) ($\boldsymbol{P}, \boldsymbol{F}$)-KPS – это пара множеств, называемых группами привилегированных – $\boldsymbol{P}$ и непривилегированных участников – $\boldsymbol{F}$, такая, что для любой группы $P \in \boldsymbol{P}$ каждый участник i, входящий в эту группу, может вычислить ключ $k_P \in K$, но никакая группа непривилегированных участников не сможет не только восстановить значение k_P, но не сможет получить никакой информации об этом ключе.

Если $\boldsymbol{P}$ состоит из всех подмножеств множества $\boldsymbol{U}$ мощности g, а $\boldsymbol{F}$ – из всех подмножеств мощности w, то будем использовать обозначение (g, w)-KPS. Это такие схемы предварительного распределения ключей, в которых каждая группа из g участников является привилегированной и может сформировать ключ k_P, но ни одна группа F из w участников, отличная от P, не может получить никакой информации об этом ключе. Понятно, что должно выполняться неравенство $g \geq w$.

Эффективность (g, w)-KPS оценивается величиной, которая называется *информационная скорость* и определяется как

$$\rho = \min\left\{\frac{\log|K|}{H(U_i)} : 1 \leq i \leq n\right\},$$

где U_i – случайная величина, принимающая значения из множества возможных значений ключевых материалов, распределяемых i-му участнику, $1 \leq i \leq n$, H – энтропия.

Так как основным назначением схем KPS является минимизация объема памяти, необходимого для хранения ключей, то представляют интерес также следующие параметры, измеряемые числом бит, необходимых для хранения ключей в центре и у каждого участника. Стойкость схемы можно оценивать суммарным количеством неизвестных бит, необходимых для восстановления ключа k_P. Обычно схема считается стойкой, если число бит, которые остаются неизвестными для непривилегированных групп участников, не

[1] Работа выполнена при поддержке гранта Президента РФ НШ № 8564.2006.10.

меньше некоторого заданного числа m. Пусть β_i – суммарная длина ключевых материалов, предоставленных i-му участнику, $1 \le i \le n$, то есть суммарное число бит в их записи (*объем памяти для узла*). *Средний объем памяти схемы* KPS $\overline{\beta}$ – это среднее арифметическое объемов памяти всех узлов схемы. *Общий объем памяти схемы* KPS – это суммарная длина всех различных ключевых элементов, хранящихся в центре.

Например, схема KPS с полной матрицей, в которой каждая пара участников обладает одним общим ключом, причем длины всех ключей одинаковы и равны m, имеет параметры

$$\rho = \frac{1}{n-1}, \quad \overline{\beta} = \beta_i = (n-1)m, \quad \beta = \frac{n(n-1)m}{2}.$$

Данная схема является эталоном, с которым можно сравнивать другие схемы. Ее называют тривиальной, так как ее использование, фактически, равносильно отсутствию какой-либо KPS.

2. Схемы распределения ключей, основанные на схемах пересечений множеств

Определение. Пусть $n > 2$. *Схема распределения ключей на основе шаблонов* KDP(n, k) (*key distribution patterns*) [1], или *схема пересечений множеств* SIS (*set intersection scheme*) [3] в простейшем случае определяется как набор множеств $\{S_1, ..., S_n\}$, являющихся подмножествами множества $\{1, \ldots, k\}$ и удовлетворяющих условию:

(1) если при $i, j, r \in \{1, ..., n\}$ выполнено включение $S_i \cap S_j \subseteq S_r$, то либо $i = r$, либо $j = r$.

По KDP(n, k)-схеме легко построить схему (2,1)-KPS. Для этого надо сформировать множество из k секретных ключей и присвоить им номера 1, …, k. Распределение ключевых материалов осуществляется путем передачи заранее секретным образом каждому абоненту P_i всех ключей с номерами из множества S_i. Теперь для формирования общего ключа участники i и j выбирают ключи, номера которых лежат в пересечении $S_i \cap S_j$, а затем вычисляют общий ключ как сумму или как значение хеш-функции от строки, составленной из этих ключей.

Заметим, что при таком подходе информация о номерах ключей каждого участника не является секретной и может передаваться по сети открытым способом.

Определение [1]. Пусть $w \ge 1$. *Устойчивая к сговору w участников*, или *устойчивая к w-кратной компрометации* схема w-CRKDP(n, k) (*collusion-resistant KDP*) определяется как набор множеств $\{S_1, ..., S_n\}$, являющихся подмножествами множества $\{1, \ldots, k\}$ и удовлетворяющих условию:

(2) если при $i, j, r_1, \ldots, r_w \in \{1, ..., n\}$ выполнено включение $S_i \cap S_j \subseteq \bigcup_{t=1}^{w} S_t$, то либо $i \in \{r_1, \ldots, r_w\}$, либо $j \in \{r_1, \ldots, r_w\}$.

Пусть $g \ge 2$. Определим теперь групповую схему предварительного распределения ключей.

Определение [1]. *w-Устойчивая к сговору схема для групп из g участников* (g, w)-CRKDP(n, k) определяется как набор множеств $\{S_1, ..., S_n\}$, являющихся подмножествами множества $\{1, \ldots, k\}$ и удовлетворяющих условию:

(3) если при $i_1, ..., i_g, p_1, ..., p_w \in \{1, ..., n\}$ выполнено включение $\bigcap_{j=1}^{g} S_{i_j} \subseteq \bigcup_{j=1}^{w} S_{p_j}$, то $\{i_1, ..., i_g\} \cap \{p_1, ..., p_w\} \ne \varnothing$.

3. Связь схем KDP и KPS

Пусть $\boldsymbol{B} = \{B_1, \ldots, B_b\}$ – множество подмножеств множества $\boldsymbol{U}$, называемых блоками, $\boldsymbol{P}, \boldsymbol{F} \subseteq 2^{\boldsymbol{U}}$, $\boldsymbol{P} \cap \boldsymbol{F} = \varnothing$. Схему предварительного распределения ключей на основе пересечений множеств ($\boldsymbol{P}$, $\boldsymbol{F}$)-KDP можно также определить как систему инцидентности ($\boldsymbol{U}$, $\boldsymbol{B}$), удовлетворяющую условию: для всех $F \in \boldsymbol{F}$, таких, что $\boldsymbol{P} \cap F = \varnothing$, выполнено

$$\{B_j : P \subseteq B_j \wedge F \cap B_j = \varnothing\} \ne \varnothing .$$

Последнее условие означает, что для каждой непривилегированной группы участников F найдется блок B_j, включающий всех участников привилегированной группы P, не пересекающийся с F. Данное определение является дуальным к приведенному выше определению KDP(n,q)-схемы. Множество S_j номеров ключей каждого участника в данном случае совпадает с множеством номеров блоков, в которые входит участник j.

Для каждого участника $i \in \boldsymbol{U}$ обозначим $r_i = \left| \{ B_j : i \in B_j \} \right|$, $1 \le i \le n$.

Теорема [6]. Пусть ($\boldsymbol{U}$, $\boldsymbol{B}$) – ($\boldsymbol{P}$, $\boldsymbol{F}$)-KDP и q – степень простого числа. Тогда существует ($\boldsymbol{P}$, $\boldsymbol{F}$)-KPS с ключевым множеством $K = GF(q)$ и информационной скоростью

$$\rho = \frac{1}{\max \{ r_i : 1 \le i \le n \}} .$$

В данном случае ключ k_P для каждой группы P привилегированных участников вычисляется по формуле $k_P = \sum_{i:P\subseteq B_i} s_i$, где $s_i \in GF(q)$ – случайное число, распределяемое каждому участнику, входящему в блок B_i (поэтому каждый участник получает r_i случайных чисел в качестве своих ключевых материалов).

Можно построить (***P***, ***F***)-KPS с более высоким значением информационной скорости. Для каждого $P \in \boldsymbol{P}$ обозначим

$$C_P = \left|\left\{ B_j : P \subseteq B_j \right\}\right| \quad \text{и} \quad D_P = \max\left\{\left|\left\{B_j : P \subseteq B_j \wedge F \cap B_j \neq \varnothing\right\}\right| : F \cap P = \varnothing\right\}.$$

В результате каждый участник группы P имеет C_P общих секретных значений, из которых каждой группе непривилегированных участников известно не более D_P.

Теорема [6]. Пусть (***U***, ***B***) – (***P***, ***F***)-KDP и $m = \min\{ C_P - D_P \}$, $P \in \boldsymbol{P}$. Пусть q – степень простого числа, $q \geq \max\{C_P\} - 1$, $P \in \boldsymbol{P}$. Тогда существует (***P***, ***F***)-KPS с ключевым множеством $K = GF(q)^m$ и информационной скоростью

$$\rho = \frac{m}{\max\{ r_i : 1 \leq i \leq n \}}.$$

Доказательство этой теоремы использует понятие (n, m, t, q)-устойчивой (*resilent*) функции $f : GF(q)^n \to GF(q)^m$, которая остается сбалансированной при фиксации t аргументов, и основано на следующем факте: для любого примарного числа q, $q \geq n - 1$, существует (n, $m - t$, t, q)-устойчивая функция.

4. Построение схем KDP на основе блок-схем

Приведенные выше определения удобно интерпретировать в терминах схем отношений. Напомним, что *конечной структурой инцидентности* (***P***, ***B***, ***I***) называется пара конечных множеств ***P*** и ***B*** (элементы которых называются точками и блоками), связанных некоторым бинарным отношением инцидентности $\boldsymbol{I} \subseteq \boldsymbol{P} \times \boldsymbol{B}$. Определим t-(v, k, λ)-*схему* (или t-*схему*) как структуру инцидентности (***P***, ***B***, ***I***) с $|\boldsymbol{P}| = v$, $|\boldsymbol{B}| = b$, в которой каждый блок имеет мощность k и каждые t точек инцидентны λ блокам [14]. Если при $1 \leq i \leq t$ символом λ_i обозначить число блоков, инцидентных произвольным i точкам, то для таких схем выполняются соотношения

$$bk = vr, \qquad (r = \lambda_1),$$
$$\lambda_i \binom{k-i}{t-i} = \binom{v-i}{t-i}\lambda, \quad 1 \leq i \leq t.$$

В случае схем KDP можно положить $\boldsymbol{P} = \boldsymbol{U} = \{1, \ldots, n\}$ и $\boldsymbol{B} = \{1, \ldots, k\}$ либо рассматривать дуальное представление, рассматривая номера ключей $1, \ldots, k$ как точки, а множества $S_1, \ldots, S_n$ – как блоки. Рассмотрим примеры.

Пример 1. Схема распределения ключей с полной матрицей является KDP(v, b) при $v = n$ и $b = \binom{n}{2} = \frac{n(n-1)}{2}$. Это случай 2-($v$, 2, 1)-схемы, соответствующий тривиальной KPS.

Пример 2. KDP(n, n) получается при выборе в качестве $S_1, \ldots, S_n$ всех подмножеств мощности $n - 1$. Это случай тривиальной 2-(n, $n - 1$, $n - 2$)-схемы.

Более сложный пример можно получить на основе биплоскостей. Напомним, что *биплоскостью* называется симметричная (т. е. $b = v$ и $r = k$) 2-(v, k, 2)-*схема*.

Пример 3 [1]. Каждой биплоскости с $b = v = \frac{1}{2}(r^2 - r + 2)$ блоками соответствует симметричная схема KDP(n, k) с $n = k = \frac{1}{2}(r^2 - r + 2)$, в которой каждое из множеств $S_1, \ldots, S_n$ имеет мощность r. Действительно, каждым двум блокам инцидентны ровно $\lambda = 2$ точки, а каждым двум точкам инцидентны ровно два блока. Поэтому пересечение каждых двух множеств S_i и S_j содержит два номера ключа, причем эта пара номеров ключей лежит только в двух множествах, а именно S_i и S_j.

5. Связь с семействами Шпернера

Множество подмножеств множества $\boldsymbol{U} = \{1, \ldots, n\}$ называется *семейством Шпернера*, если ни одно из них не является подмножеством другого. Легко доказывается следующая

Лемма [1]. Семейство $\{S_1, \ldots, S_n\}$ подмножеств множества $\boldsymbol{U}$, $|\boldsymbol{U}| = k$, образует KDP(n, k)-схему в том и только в том случае, если множество $\{S_i \cap S_j \mid 1 \leq i < j \leq n\}$ образует семейство Шпернера.

Воспользуемся известным результатом Шпернера для доказательства нижней оценки на объем ключевых материалов.

Теорема (*Sperner*, 1928). Если подмножества $S_1, ..., S_n$ множества $\boldsymbol{U}$, $|\boldsymbol{U}| = k$, образуют семейство Шпернера, то $n \le \binom{k}{\lfloor k/2 \rfloor}$. Равенство достигается только в случаях, если $S_1, ..., S_n$ – все m-элементные подмножества множества $\boldsymbol{U}$, где $m = k/2$ при четном k и $m = (k + 1)/2$ или $(k – 1)/2$ при нечетном k.

Следствие 1 [1]. Для любой схемы KDP(n, k) выполняется неравенство $\binom{n}{2} \le \binom{k}{\lfloor k/2 \rfloor}$.

Следствие 2 [1]. Для любой схемы KDP(n, k) каждый абонент должен иметь менее $\log_2 n$ ключей. Если $n \ge 4$, то $k \ge 2 \log_2 n$.

Следствие 3 [1]. Для любой схемы KDP(n, k) и любого i выполняется неравенство $n - 1 \le \binom{r_i}{\lfloor r_i/2 \rfloor}$, где $r_i = |S_i|$, $1 \le i \le n$.

Из этих оценок получаются следующие минимальные значения min b и min r_i для маленьких значений n:

n	3	4	5	6	7	8	9
min b	3	4	5	6	7	7	8
min r_i	2	3	4	4	4	5	5

Еще один тип оценок вытекает из известных комбинаторных соотношений на параметры конфигураций в случае, когда схеме KDP(n, k) соответствует 1-схема, то есть все множества S_i имеют одинаковую мощность, и каждый элемент j, $1 \le j \le n$, входит в одинаковое число r множеств S_i, $1 \le i \le n$. Так, например, из обобщенного неравенства Фишера вытекает оценка $k \ge n$, а также можно показать, что для нетривиальной схемы KDP(n, k) выполняются неравенства $r \ge 3$, $|S_i| \ge 3$ и $|S_i \cap S_j| \ge 2$, $1 \le i, j \le n$.

6. Вероятностный алгоритм построения KDP

Теорема [3]. Существуют KDP(n, k)-схемы с $k \le [13 \log_2 n]$.

Доказательство проводится с помощью вероятностного метода в комбинаторике. В нем множество S_i строится поэлементно в результате реализации последовательности независимых случайных испытаний по схеме Бернулли с вероятностью успеха p. При таком подходе, в общем случае, множества S_i имеют различную мощность. При выборе значения $p = 2/3$ и $k = 13 \log_2 n$ получаем вероятность успеха не менее 1/2.

Если изменить вероятностную схему и потребовать, чтобы множества S_i выбирались случайным образом из множества всех подмножеств фиксированной мощности $|S_i| = t$, то в результате получаются, как правило, более эффективные схемы, содержащие меньшее число ключей. В качестве значения t нужно выбирать то, которое минимизирует вероятность появления «плохих» троек в смысле предыдущей теоремы. В табл. 1 из работы [3] приведены практически вычисленные значения числа ключей для обеих схем.

Таблица 1

Число участников	Число ключей (k)	
(n)	1 способ	2 способ
50	73	48
75	80	53
100	86	56
200	99	64
500	116	75
Число участников	Число ключей (k)	
(n)	1 способ	2 способ
10^3	129	83
10^4	172	111
10^5	215	138
10^6	258	165
10^8	344	220

Поскольку алгоритм построения схемы KDP(n, k) носит вероятностный характер, то после построения требуется проверить, выполняется ли условие (1). Для этого требуется не более $O(n^3k)$ операций. В то же время при очень больших значениях n можно отказаться от этой проверки, так как вероятность построения такой схемы очень мала. Например, при $n = 10^8$ и $k = 399$ она не превышает 10^{-20}. В табл. 2 приведены зна-

чения k, при которых выполняются заданные ограничения на величину β вероятности риска построения первым способом схемы с невыполненным условием (1).

Таблица 2

Число абонентов	Число ключей (k)	
(n)	$\beta \le 10^{-10}$	$\beta \le 10^{-20}$
500	163	254
10^3	171	262
10^4	199	290
10^5	226	317
10^6	253	344
10^8	308	399

Вероятностный алгоритм из предыдущей теоремы можно преобразовать в детерминированный.

Теорема [3]. Схема KDP(n, k) с $k \le 2 \log_2 n$ может быть построена детерминированным алгоритмом за $O(n^3k)$ операций при использовании памяти объема $O(n^3)$.

Как отмечают авторы, полученный детерминированный алгоритм имеет такую же трудоемкость, как и вероятностный, но он не может быть эффективно распараллелен.

7. Схемы KDP, устойчивые к сговору

Рассмотрим теперь примеры схем w-CRKDP(n, k).

Схема из примера 1, очевидно, является w-CRKDP при всех w, $1 \le w \le n$.

Пример 4 [1]. Предположим, имеется 3-(v, k, λ)-схема, параметры которой удовлетворяют неравенству $\lambda_2 > w\lambda_3$ (здесь $\lambda = \lambda_3$). Тогда ей соответствует w-CRKDP(b, v). Действительно, если при $i, j \in \{1, ..., n\}$ и $r_1, ..., r_w \in \{1, ..., n\} \setminus \{i, j\}$ выполнено включение $S_i \cap S_j \subseteq \bigcup_{t=1}^{w} S_t$, то в силу равенств $|S_i \cap S_j| = \lambda_2$ и $|S_i \cap S_j \cap S_{r_t}| = \lambda_3$ при всех $1 \le r_t \le w$ получаем противоречие с неравенством $\lambda_2 > w\lambda_3$.

Лемма [1]. Пусть $w \ge 1$. Семейство $\{S_1, ..., S_n\}$ подмножеств множества $\boldsymbol{U}$, $|\boldsymbol{U}| = k$, образует (w+1)-CRKDP(n, k)-схему в том и только в том случае, если для любой точки j остаточная KDP($n1$, $k - 1$)-схема, полученная из нее удалением одной точки j и оставлением только тех множеств $S_1, ..., S_{n1}$, которые содержат эту точку, является w-CRKDP-схемой.

Так как остаточная схема любой t-схемы является ($t - 1$)-схемой, то из этой леммы вытекает

Следствие [1]. Пусть $w \ge 1$. Любая ($w + 2$)-схема является схемой w-CRKDP.

В качестве общих результатов можно привести следующие оценки.

Теорема [3]. Для любой схемы w-KDP(n, k) выполняется неравенство $k \ge w(\log_2 n - \log_2 w - 1)$.

Теорема [3]. Существует схема w-KDP(n, k), у которой $k \le \lceil ((w+2)^{w+3}/\, 4w^w \log_2 n) \rceil$.

Следствие [3]. Существует схема w-KDP(n, k), имеющая $\lceil 2(w+2)^3 \ln n \rceil$ ключей.

Аналогично рассмотренным выше алгоритмам построения схем KDP может быть предложен алгоритм построения схем w-KDP.

Теорема [3]. Схема w-KDP(n, k) с $k \le \lceil w^3 \ln k \rceil$ может быть построена детерминированным алгоритмом за $O(n^3k)$ операций.

Заметим, что семейства множеств, в которых ни одно из множеств не содержится в объединении w других, подробно изучались в комбинаторике (см., например, работы [11, 13]).

В работе [5] описаны примеры использования циклических геометрий для построения w-KDP-схем. Ниже будут построены w-KDP-схемы, полученные из инверсных плоскостей и плоскостей Минковского. Отметим, что имеются и другие примеры построения w-KDP-схем, например, на основе плоскостей Лагерра (Laguerre) [4].

Напомним, что *инверсная плоскость* (*плоскость Мебиуса*) является 3-($s^2 + 1$, $s + 1$, 1)-схемой с параметрами $v = s^2 + 1$, $k = s + 1$, $b = s(s^2 + 1)$, $r = s(s + 1)$, $\lambda = s + 1$ и представляет собой структуру инцидентности, имеющую точки и блоки, называемые окружностями, такую, что выполняются аксиомы:

C1: любая окружность содержит по крайней мере три точки;

C2: для каждых трех различных точек существует единственная окружность, им инцидентная;

C3: если p и q точки, а C – окружность, содержащая p, но не содержащая q, то существует только одна окружность C', содержащая p и q и имеющая с окружностью C одну общую точку p;

C3: существует четыре точки, не принадлежащие одной окружности.

Пример 5 [5]. Рассмотрим структуру инцидентности ($\boldsymbol{P}$, $\boldsymbol{B}$, $\boldsymbol{I}$) на основе инверсной плоскости порядка s, которая определяется так: множеством точек $\boldsymbol{P}$ (участников) служит множество всех $s^2 + 1$ точек инверсной

плоскости, а множеством блоков ***B*** (ключей) – множество всех $s(s^2+1)$ окружностей. Пусть (i) обозначает множество блоков, инцидентных точке i. Тогда каждой паре абонентов i и j соответствует множество $(i) \cap (j)$, состоящее из окружностей, проходящих через две точки i и j. Если при этом выполнено включение

$$(i) \cap (j) \subseteq \bigcup_{t=1}^{w} (r_t) \ ,$$

то так как через три различные точки проходит не более одной окружности, в объединении справа должно быть, по крайней мере, $|(i) \cap (j)| = s+1$ окружностей. Значит, данная структура образует w-KDP-схему при всех $w \le s$. Для этой схемы $\beta_i = (s^2+1)\,l$, где длину ключевого материала l можно положить равной $\left\lceil \frac{m}{s-w+1} \right\rceil$. В этом случае будет выполнено условие стойкости w-KDP-схемы, которое означает, что после того, как w участников $\{r_1, \ldots, r_w\}$ объединят свои ключевые материалы с целью восстановления общего ключа участников i и j, неизвестными останутся по крайней мере m бит. Средний и общий объем памяти схемы будут равны соответственно

$$\overline{\beta} = (s^2+1)\left\lceil \frac{m}{s-w+1} \right\rceil \qquad \text{и} \qquad \beta = \sum_{x \in B} l(x) = (s^3+s)\left\lceil \frac{m}{s-w+1} \right\rceil .$$

Пример 6 [5]. Рассмотрим остаточную структуру инцидентности (***P′***, ***B′***, ***I***), полученную из инверсной плоскости порядка s удалением одной точки и всех окружностей, содержащих эту точку. Тогда, очевидно, она также будет w-KDP-схемой при всех $w \le s-1$. Для этой схемы $\beta_i = (s^2-1)\,l$, где в качестве длины ключевого материала l можно выбрать величину $\lceil m / (s-w) \rceil$. В этом случае также будет выполнено условие стойкости w-KDP-схемы. Средний и общий объем памяти схемы будут равны соответственно

$$\overline{\beta} = (s^2-1)\left\lceil \frac{m}{s-w} \right\rceil \qquad \text{и} \qquad \beta = \sum_{i=1}^{|B|} \beta_i = (s^3-s^2)\left\lceil \frac{m}{s-w} \right\rceil ,$$

так как число слагаемых в последней сумме равно $(s^3+s)-(s^2+s) = s^3-s^2$.

Конечной плоскостью Минковского ([14]) называется структура инцидентности с точками, прямыми и окружностями, в которой множество всех прямых разбивается на два класса L_1 и L_2 так, что выполняются аксиомы:

M1: каждая точка лежит на единственной прямой из каждого класса L_1 и L_2, каждая прямая класса L_1 пересекается с каждой прямой класса L_2 в единственной точке и прямые и окружности пересекаются в единственной общей точке;

M2: любые три точки, из которых никакие две не коллинеарны, инцидентны одной единственной окружности;

M3: если p и q – неколлинеарные точки и если C – окружность, содержащая p, но не содержащая q, то существует только одна окружность C', содержащая p и q и имеющая с окружностью C одну общую точку p;

M4: существует окружность, содержащая по крайней мере три точки.

Для каждой плоскости Минковского существует целое число s, которое называется порядком плоскости (в этом случае саму плоскость обозначают через $M(s)$), такое, что:

1) каждая окружность имеет $(s+1)$ точку;

2) плоскость $M(s)$ имеет $(s+1)^2$ точек, $(s+1)$ прямую в каждом из двух классов и $s(s^2-1)$ окружностей;

3) каждая прямая имеет $(s+1)$ точку;

4) каждая точка лежит на двух прямых и $s(s-1)$ окружностях;

5) каждые две неколлинеарные точки лежат на $(s-1)$ окружностях.

Пример 7 [5]. Пусть $2 \le u \le s$. Рассмотрим структуру инцидентности (***P***, ***B***, ***I***) на основе инверсной плоскости Минковского порядка s. Для этого зафиксируем u точек $R_1, \ldots, R_u$, лежащих на одной прямой. Пусть множеством точек P (абонентов) служит множество всех точек плоскости Минковского, не лежащих на прямой, содержащих данные точки, а множеством блоков B (ключей) – множество всех окружностей, проходящих через точки $\{r_1, \ldots, r_u\}$, и некоторую пару точек i и j, лежащих на одной прямой. Тогда паре абонентов i и j соответствует множество окружностей, проходящих через точки i, j и $r_1, \ldots, r_u$. Данная структура имеет s^2+s точек и $u(s^3+s)+(s^2+s)(2s-1)/2$ блоков (ключей). При этом имеется us точек, инцидентных $(u-1)(s-1)+2s-1$ ключам, и s^2+s-us точек, инцидентных $u(s-1)+2s-1$ ключам. Полагаем длину ключевого материала равной $l = \lceil m / (u-w-2) \rceil$, если блок является окружностью, и m в противном случае. При таком выборе будет выполнено условие стойкости w-KDP-схемы, и она будет иметь следующие параметры:

$$\bar{\beta} = \frac{u(m-1)s(s-1)+(s^2+s+us)u(s-1)}{s^2+s}\left\lceil \frac{m}{u-w-2} \right\rceil + (2s-1)m\,,$$

$$\beta = u(s^2-s)\left\lceil \frac{m}{u-w} \right\rceil + \frac{(s^2+s)(2s-1)m}{2}\,.$$

8. Групповые схемы KDP, устойчивые к сговору

Для групповых схем известны следующие примеры.

Лемма [1]. Пусть $g \geq 1$, $w \geq 1$. Семейство $\{S_1, ..., S_n\}$ подмножеств множества $\boldsymbol{U}$, $|\boldsymbol{U}| = k$, образует (g, w+1)-CRKDP(n, k)-схему в том и только в том случае, если для любой точки j остаточная KDP(n_1, $k-1$)-схема, полученная из нее удалением одной точки j и оставлением только тех множеств S_1, ..., S_{n1}, которые содержат эту точку, является (g, w)-CRKDP-схемой.

Следствие [1]. Пусть $g \geq 1$, $w \geq 1$. Любая ($g + w$)-схема является схемой (g, w)-CRKDP.

Теорема [1]. Число ключей любой (g, w)-KDP(n, k)-схемы удовлетворяет неравенству

$$k \geq w(g \log_2 n - \log_2 w - g \log_2 g).$$

Теорема [1]. Существует (g, w)-KDP(n, k)-схема, у которой $k \leq \lceil ((w+g)^{w+g+1}/\, g^g w^w \log_2 n\,) \rceil$.

Заметим, что изучаемый в комбинаторике тип (i, j)-семейств без перекрытий, по сути, совпадает с понятием схемы (g, w)-KDP.

Определение. Если $\boldsymbol{X}$ – множество из v элементов, $|\boldsymbol{X}| = v$, а $\boldsymbol{F}$ – множество его подмножеств (блоков), $|\boldsymbol{F}| = b$, то ($\boldsymbol{X}$, $\boldsymbol{F}$) называется (i, j)-*семейством без перекрытий* (*cover-free family*) и обозначается (i, j)-CFF(v, b), если для любых i блоков $B_1, ..., B_i \in \boldsymbol{F}$ и любых j блоков $A_1, ..., A_j \in \boldsymbol{F}$ выполняется условие

$$\bigcap_{k=1}^{i} B_k \not\subset \bigcup_{s=1}^{j} A_s\,.$$

Такие семейства были введены в рамках теории кодирования в [9] (см. также [10]).

В работе [8] для построения семейств (i, j)-CFF(v, b) используются системы (i, j)-SS(v,b).

Определение [13]. (i, j)-*разделенная система* (*separating system*) – это пара множеств ($\boldsymbol{X}$, $\boldsymbol{B}$), такая, что для всех P, $Q \subseteq \boldsymbol{X}$ с условием $|P| \leq i$, $|Q| \leq j$ и $P \cap Q = \varnothing$, существует блок $B \in \boldsymbol{B}$, такой, что либо $P \subseteq B$ *и* $Q \cap B = \varnothing$, либо $Q \subseteq B$ *и* $P \cap B = \varnothing$. Если $|X| = v$ и $|\boldsymbol{B}| = b$, то используется обозначение (i, j)-SS(v, b).

Определение [8]. (N, n, m, $\{i, j\}$)-*разделенное семейство хеш-функций* (*separating hash family*) (обозначается как SHF(N; n, m, $\{i, j\}$)) – это множество из N функций f: $Y \to X$, $|Y| = n$, $|X| = m$, такое, что для всех f и для любых подмножеств C_1, $C_2 \subseteq \{1, 2, \ldots, n\}$, $|C_1| = i$, $|C_2| = j$ и $C_1 \cap C_2 = \varnothing$, существует функция f, такая, что

$$\{f(y):\ y \in C_1\} \cap \{f(y):\ y \in C_2\} = \varnothing.$$

Лемма [7]. Каждая схема (i, j)-SS(v, b) эквивалентна семейству SHF(b; v, 2, $\{i, j\}$).

Теорема [7]. Если существует система (i, j)-SS(v, b), то существует (i, j)-CFF(2v, b).

9. Построение больших схем KDP из малых

В работе [1] указано три способа построения новых KDP(n, k) на основе уже построенных ранее. Не углубляясь в детали, отметим только, что по двум схемам KDP(n_1, k_1) и KDP(n_2, k_2) можно построить схему KDP(n, k) с параметрами:

(a) $n = n_1 \times n_2$, $k = k_1 + k_2$;

(b) $n = n_1 + r_1(n_2 - 1)$, $k = k_1 + k_2 - 1$;

(c) $n = n_1 + n_2 + (r_1 - 1)(r_2 - 1) - 1$, $k = k_1 + k_2 - 2$,

где r_1 и r_2 – число множеств первой и второй схем соответственно, содержащих произвольную точку (номер ключа). Например, начиная с двух KDP(7, 7), соответствующих двум биплоскостям, каждая из которых является 2-(7, 4, 2)-схемой, с применением этих конструкций можно соответственно построить:

(a) KDP(49, 14), в которой множества S_i имеют мощность 8;

(b) KDP(31, 13), в которой множества S_i имеют мощность 9;

(c) KDP(22, 12), в которой множества S_i имеют мощность 10.

Утверждение [1]. Если схемы KDP(n_1, k_1) и KDP(n_2, k_2) являются w-CRKDP-схемами, то схема KDP(n, k), построенная из них с помощью конструкций (a), (b) и (c), также является w-CRKDP-схемой.

В заключение приведем еще один простой и эффективный индуктивный способ построения KDP(n, k)-схем, предложенный Д.Б. Тишуриным и Р.В. Шпаком. Определим *матрицу инцидентности* KDP(n, k)-схемы

как (0, 1)-матрицу размера $n \times k$, в которой столбцы соответствуют элементам множества S, а строки – подмножествам S_1, ..., S_n, причем единицы стоят на пересечении со столбцами, помеченными элементами подмножества, соответствующего строке. Например, KDP(n, n)-схеме из примера 2 соответствует матрица инцидентности

$$\begin{pmatrix} 11...10 \\ 11...01 \\ ... \\ 01...11 \end{pmatrix}.$$

Заметим, что любая перестановка строк и столбцов матрицы инцидентности KDP(n, q)-схемы преобразует ее в матрицу KDP(n, k)-схемы.

Лемма. (0, 1)-матрица размера $n \times q$ задает схему KDP(n, k) в том и только в том случае, если для любых трех ее строк найдутся три столбца, на пересечении которых стоит матрица инцидентности схемы KDP(3, 3).

Доказательство. Пусть строкам матрицы соответствуют множества S_1, ..., S_n. Тогда утверждение леммы вытекает из следующего очевидного замечания: для любых трех строк i, j, r существование столбца, на пересечении с которым в этих строках стоят элементы 1, 1 и 0 соответственно эквивалентно условию $S_i \cap S_j \not\subset S_r$.

Теорема. Если существует KDP(n, k)-схема, то существует и KDP(n^2, $3q$)-схема.

Доказательство. Пусть имеется KDP(n, k)-схема с матрицей инцидентности A. Для $1 \le i \le n$ определим матрицы A_i и B_i, первая из которых получается из A циклической перестановкой строк вверх на $i - 1$ шагов, а вторая составлена из одинаковых строк, каждая из которых совпадает с i-й строкой матрицы A. Рассмотрим матрицу

$$\left(\begin{array}{ccc} A & A & B \\ A & A_2 & B_2 \\ ... & ... & ... \\ A & A_n & B_n \end{array}\right) = \begin{pmatrix} C_1 \\ C_2 \\ ... \\ C_n \end{pmatrix}.$$

Покажем, что эта матрица является матрицей инцидентности KDP(n^2, $3q$)-схемы. В силу леммы достаточно показать, что для произвольных трех строк этой матрицы найдутся три столбца, на пересечении которых стоит матрица инцидентности KDP(3, 3)-схемы.

Если три строки лежат в одной подматрице $C_i = (A, A_i, B_i)$, то такие столбцы найдутся в ее первой подматрице, совпадающей с матрицей A. Если три строки лежат в разных подматрицах C_i, C_j, C_k, то такие столбцы найдутся в подматрицах B_i, B_j, B_k.

Пусть теперь три строки лежат в двух подматрицах $C_i = (A, A_i, B_i)$ и $C_j = (A, A_i, B_j)$. Пусть две строки лежат в подматрице C_i, а одна в подматрице C_j. Покажем, что найдутся три столбца, на пересечении которых стоит одна из матриц вида

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad \text{или} \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Для удобства будем называть матрицы A, A_i и B_i первой, второй и третьей колонками матрицы C_i. Если в первой колонке все три строки разные, то такие столбцы найдутся уже в первой колонке. Пусть теперь среди двух строк первой колонки две совпадают. Аналогично, если во второй колонке строки различны, то такие столбцы найдутся во второй колонке. Поэтому предположим, что во второй колонке также две строки совпадают. При этом совпадать может только третья строка с одной из двух первых, причем в первой и второй колонках совпадают разные строки. В третьей колонке всегда совпадают первые две строки, так как они берутся из одной матрицы B_i.

Осталось заметить, что в силу основного свойства KDP-схемы в ее матрице инцидентности для любых трех строк, две из которых совпадают, всегда найдется столбец, на пересечении которого с совпадающими строками стоят единицы, а на пересечении с третьей строкой – ноль.

Следствие. Если существует KDP(n_0, k_0)-схема, то для любого натурального t существует KDP(n, k)-схема с параметрами $n = {n_0}^{2^t}$, $q = 3^t k_0$ и $k = k_0 \ (\log_{n_0} n)^{\log_2 3}$.

Доказательство получается применением теоремы t раз. В результате строится схема KDP(n,q) с $n = {n_0}^{2^t}$ и $k = 3^t k_0$. Выражая из этих равенств t и приравнивая выражения, получаем равенство $\ln k = \log_2 3 \ln \log_2 (\log_{n_0} n) + \ln k_0$, откуда и вытекает требуемое равенство.

Например, начиная со схем KDP(3, 3), KDP(4, 4) и KDP(5, 5), можно построить схемы со следующими параметрами:

n	k
81	27
256	36
625	45
6561	81
65536	108
390625	135
43046721	243
4294967296	324
152587890625	405

Оценим объем ключевых материалов, получаемых каждым участником. Если в исходной KDP(n, k)-схеме все множества S_1, ..., S_n имеют одинаковое число элементов, равное m, $2 < m < k$, то для схемы KDP(n^2, $3k$) имеем $\overline{\beta} = \beta_i = 3m, \quad \beta = 3k$.

Заметим также, что если к матрице инцидентности KDP(n^2, $3k$)-схемы, построенной из KDP(n, k)-схемы с использованием предыдущей теоремы, добавить три строки вида (0…01...11...1), (1...10...01...1) и (1...11...10...0), то получится KDP(n^2+3, $3k$)-схема. С использованием этого факта можно построить, например, KDP(n, k)-схемы с параметрами

n	k
147	27
364	36
787	45
21612	81
132499	108
619372	135
467078547	243
17555985004	324
383621674387	405

ЛИТЕРАТУРА

1. *Mitchell C.J.*, *Piper C.* Key storage in Secure Networks // Discrete and Applied Math. 1988. 21. P. 215 – 228.
2. *Mitchell C.J.* Combinatorial techniques for key storage reduction in secure networks // Technical memo. Hewlett-Packard Laboratories. Bristol, 1988.
3. *Dyer M.*, *Fenner T.*, *Frieze A.*, *Thomason A.* On key storage in secure networks // J. Cryptology. 1995. V. 8. P. 189 – 200.
4. *O'Keefe C.M.* Applications за finite geometries in information security // Australas. J. Combin. 1993. V. 7. P. 195 – 212.
5. *O'Keefe C.M.* Key distribution patterns using Minkowski planes // Design, Codes and Cryptography. 1995. V. 5. No. 3. P. 261 – 267.
6. *Stinson D.R.*, *van Trung T.* Some new results on key distribution patterns and broadcast encryption // Designs, Codes and Cryptography. 1998. V. 14. P. 261 – 279.
7. *Stinson D.R.*, *van Trung T*, *Wei R.* Secure frameproof codes, key distribution patterns, group testing algorithms and related structures // J. Statist. Plan. Infer. May 2000. V. 86. No. 2. P. 595 – 617.
8. *Stinson D.R.*, *Wei R.*, *Zhu L.* New constructions for perfect hash families and related structures using combinatorial designs and codes // J. Combinatorial Designs. 2000.V. 8. No. 3. P. 189 – 200.
9. *Kautz W.H.*, *Singleton R.S.* Nonrandom binary superimposed codes // IEEE Trans. Inform. Theory. 1964. V. 10. P. 363 – 377.
10. *Dyachkov A.G.*, *Rykov V.V.*, *Rashad A.M.* Superimposed distance codes // Problems of Control and Information Theory. 1989. V. 18. P. 237 – 250.
11. *Erdösh P.*, *Frankl P.*, *Füredi Z.* Families of finite sets in which no set is covered by the union of two others // J. Combinatorial Theory. 1982. V. A33. P. 158 – 166.
12. *Erdösh P.*, *Frankl P.*, *Füredi Z.* Families of finite sets in which no set is covered by the union of r others // Israel J. Mathematics. 1985. V. 51. P. 75 – 89.
13. *Friedeman A.D.*, *Graham R.L.*, *Ullman J.D.* Universal single transition time asynchronous state assignments // IEEE Trans. Comput. 1969. V. 18. P. 541 – 547.
14. *Dembovski P.* Finite geometries. Berlin; Heidelberg: Springer Verlag, 1968.