# Вычислительные машины, комплексы и компьютерные сети (05.13.15)

УДК 51.37
DOI: 10.24160/1993-6982-2021-2-108-118

## Алгоритмические аспекты создания и использования ключевых пространств беспроводных сенсорных сетей на основе комбинаторных блок-схем

А.Б. Фролов, Н.П. Кочетова, А.О. Клягин, Д.Ю. Темников

На основе анализа особенностей управления ключами в беспроводных сенсорных сетях (БСС) сформулирован ряд отвечающих определенным требованиям к ключевым пространствам БСС положений алгоритмического подхода к их созданию и использованию в предположении, что их структура соответствует одной из разновидностей комбинаторных блок-схем — циклической или ациклической проективной плоскости, линейной или квадратичной трансверсальной блок-схеме. Распределенный характер БСС позволяет избежать построения комбинаторной блок-схемы в полном объеме и вычислять необходимые блоки по мере необходимости при масштабировании сети (добавлении новых узлов) или нецентрализованном определении параметров коммутации конкретных узлов. Для этого необходимы алгоритмы вычисления блоков комбинаторной блок-схемы (как множеств номеров ключей, распределяемых данному узлу) и дуальных блоков (как множеств номеров узлов, которым распределены ключи с номерами, сов-падающими с номерами дуальных блоков), а также алгоритмы решения производных задач: вычисления номеров общих ключей двух узлов и номера узла, имеющего общий ключ с одним из двух узлов и, возможно, другой ключ с другим узлом. Указанные задачи решены на основе использования нумерации элементов, блоков и дуальных блоков в соответствии с предложенным правилом двойственности: множества элементов и дуальных блоков находятся во взаимно-однозначном соответствии по нумерации, дуальный блок с заданным номером содержит номера блоков, содержащих элементы с его же номером. Распределенное (независимое) вычисление блоков осуществляется на основе алгебраических идентификаторов, вычисляемых по номерам блоков. Помимо возможного отсутствия физической связи между узлами учтены недопустимость использования отдельных (скомпрометированных) ключей, а также возможная неполнота комплектования узлов сети ключами, как и неполнота реализации системы в целом. Приведены алгоритмы вычисления параметров коммутации двух узлов при проектировании БСС и алгоритм компьютерного моделирования вычисления таких параметров при функционировании БСС при указанных ограничениях и использовании любого из перечисленных выше типов комбинаторных блок-схем.

*Ключевые слова:* беспроводная сенсорная сеть, ключевое пространство, проективная плоскость, комбинаторная и трансверсальная комбинаторная блок-схемы, алгебраический идентификатор блока, правило двойственности нумерации блоков и дуальных блоков, компрометация ключа, неполнота комплектации узла ключами, незавершенность системы.

*Для цитирования:* Фролов А.Б., Кочетова Н.П., Клягин А.О., Темников Д.Ю. Алгоритмические аспекты создания и использования ключевых пространств беспроводных сенсорных сетей на основе комбинаторных блок-схем // Вестник МЭИ. 2021. № 2. С. 108—118. DOI: 10.24160/1993-6982-2021-2-108-118.

## The Algorithmic Aspects of Creating and Using Wireless Sensor Network Key Spaces Based on Combinatorial Block Diagrams

A.B. Frolov, N.P. Kochetova, A.O. Klyagin, D.Yu. Temnikov

Algorithmic approach principles relating to development and use of wireless sensor network (WSS) key spaces are formulated based on an analysis of the keys management peculiarities. The formulated principles, which meet certain requirements for the WSS key spaces, have been elaborated proceeding from the assumption that their structure corresponds to one of the varieties of combinatorial block diagrams: cyclic or acyclic projective plane, linear or quadratic transversal block diagrams. Owing to the WSS having a distributed configuration, it becomes possible to avoid the need to construct a combinatorial block diagram in full scope, and the required blocks are computed, whenever

necessary, in scaling the network (in adding new nodes) or when determining, in a decentralized manner, the switching parameters of specific nodes. To do so, it is necessary to have algorithms for computing the blocks of the combinatorial block diagram (as the sets of key numbers allocated to a given node) and dual blocks (as the sets of the numbers of nodes to which keys are assigned with the numbers coinciding with the numbers of dual blocks), as well as algorithms for solving derived problems: computing of the key number common to two nodes and the number of the node that has a common key with one of two nodes and, possibly, another key with the other one. These problems are solved by using the numbering of elements, blocks and dual blocks in accordance with the proposed duality rule: sets of elements and dual blocks are in one-to-one correspondence by numbering; the dual block with a specified number contains the numbers of blocks containing elements with this number. Distributed (independent) calculation of blocks is carried out on the basis of algebraic identifiers computed by block numbers. In addition to the possible absence of a physical connection between the nodes, the inadmissibility of using separate (compromised) keys is taken into account, and the incomplete furnishing of the network nodes with keys, as well as the incompleteness of the system implementation as a whole. Algorithms for computing the switching parameters of two nodes in designing the WSS and an algorithm for computer modeling of the calculation of such parameters during the WSS operation subject to the specified constraints and in using any of the above types of combinatorial block diagrams are presented.

*Key words:* wireless sensor network, key space, projective plane, combinatorial block diagram, transversal combinatorial block diagram, algebraic block identifier, duality rule for blocks and dual blocks numbering, key compromising, incompleteness of furnishing a node with keys, incompleteness of the system.

*For citation:* Frolov A.B., Kochetova N.P., Klyagin A.O., Temnikov D.Yu. The Algorithmic Aspects of Creating and Using Wireless Sensor Network Key Spaces Based on Combinatorial Block Diagrams. Bulletin of MPEI. 2021;2:108—118. (in Russian). DOI: 10.24160/1993-6982-2021-2-108-118.

**Введение**

Беспроводные сенсорные сети (БСС) обеспечивают информационный обмен в системах, создаваемых, в частности, по принципам Industry 4.0, включающим требование безопасности. Безопасность реализуется криптографическими методами, что предполагает установку в узлах сети ключей и последующее их использование для зашифрования, расшифрования, аутентификации и исполнения других криптографических протоколов. Такие сети содержат от нескольких сотен до нескольких тысяч узлов. Управление ключами включает их генерацию, установку, использование и аннулирование скомпрометированных ключей.

Генерация и установка ключей проходят по следующей общей схеме пересечения множеств: генерируется упорядоченный ключевой пул $\boldsymbol{K}$, состоящий из большого числа $v$ единиц ключевой информации с идентификаторами, например, номерами $s$ векторов в наборе $\boldsymbol{K}$. Для каждого узла $U_i$ сети на основе $\boldsymbol{K}$ вычисляются и устанавливаются в узел предварительные ключи $\boldsymbol{K}_i$, $\boldsymbol{K}_i \subseteq \boldsymbol{K}$. После этого в любых двух узлах $U_i$ и $U_j$ сети по известным идентификаторам ключевых единиц в каждом из них и ключевым единицам собственных предварительных ключей $\boldsymbol{K}_i$ и $\boldsymbol{K}_j$ по пересечению $\boldsymbol{K}_{i,j} = \boldsymbol{K}_i \cap \boldsymbol{K}_j$ может быть вычислен общий ключ $k_{i,j}$ для взаимной коммуникации. Чтобы пары узлов не имели доступа к ключевой информации другой пары узлов, необходимо выполнение следующего условия Шпернера:

$$\boldsymbol{K}_i \cap \boldsymbol{K}_j \subseteq \boldsymbol{K}_r \rightarrow r \in \{i, j\}. \qquad (1)$$

Удовлетворяющее условию (1) ключевое пространство образует так называемую KDP-схему. В основе этой теории лежат публикации [1 — 5].

Задача данной работы — алгоритмизация этапов создания и использования ключевого пространства БСС на основе определенных типов комбинаторных блок-схем, отличающаяся возможностью независимого (распределенного) вычисления блоков (идентификаторов ключей узлов) в процессе масштабирования в пределах заданного его объема, нецентрализованного вычисления параметров коммутации узлов для конфиденциального обмена при отсутствии некоторых физических связей, запрете использования некоторых ключей, а также неполноте комплектации узлов ключами, как и незавершенности масштабирования ключевого пространства.

На основе анализа особенностей БСС сформулированы отвечающие определенным требованиям к ключевым пространствам БСС основные положения алгоритмического подхода к их созданию и использованию.

Рассмотрены алгоритмы вычисления блоков и дуальных блоков комбинаторной блок-схемы, а также алгоритмы решения производных задач: вычисления идентификаторов общих элементов двух блоков, и идентификатора блока, имеющего общий элемент с одним из двух блоков и, возможно, другой элемент с другим.

Приведен возможный вариант реализации предложенного алгоритмического подхода к созданию и использованию ключевого пространства БСС: даны способы инициализации и масштабирования ключевого пространства и вычисления параметров коммутации между двумя узлами при проектировании БСС. Учтены возможное отсутствие физической связи между узлами, недопустимость использования отдельных (скомпрометированных) ключей, а также возможная неполнота комплектования узлов сети ключами, как и неполнота реализации системы в целом.

Предложен алгоритм компьютерного моделирования вычисления указанных параметров при функционировании БСС. Охарактеризованы полученные алгоритмические приемы создания и использования ключевого пространства БСС и возможности их применения при проектировании и компьютерном моделировании БСС.

**Особенности создания и использования ключевого пространства беспроводной сенсорной сети и положения алгоритмического подхода**

Задача настоящего параграфа — анализ особенностей БСС с целью выявления основных положений алгоритмического подхода к созданию и использованию ключевого пространства БСС, отвечающих определенным требованиям к БСС.

Управление ключами в сенсорных сетях включает следующие этапы [6, 7].

*Предварительное распределение ключей (Key Predistribution).* Имеются система блоков ключей ($\boldsymbol{K}$; $\boldsymbol{K}_1$, $\boldsymbol{K}_2$, …, $\boldsymbol{K}_b$) и изоморфная ей система идентификаторов ($\boldsymbol{S}$; $\boldsymbol{S}_1$, $\boldsymbol{S}_2$, …, $\boldsymbol{S}_b$). Узлам $U_i$ сети соответствуют множества $\boldsymbol{S}_i$ идентификаторов ключей из множества $\boldsymbol{K}_i$, $i = 1, \ldots, b$. Одновременно идентификаторам $s_j$ ключей соответствуют множества $\boldsymbol{U}_j$, $j = 1, \ldots, n$ узлов, содержащих ключи $k_j$. Эти системы образуют ключевое пространство БСС, и данный этап является этапом его создания.

*Обнаружение общего ключа (Shared Key Discovery).* Соответствие $\boldsymbol{S}\times\boldsymbol{U}$ на множествах $\boldsymbol{S}$ идентификаторов ключей и $\boldsymbol{U}$ узлов общеизвестно. Это позволяет находить общие ключи двух узлов $U_i$ и $U_j$ среди распределенных им ключей, если общие ключи имеются. Хранить данное соответствие заранее в каждом узле нецелесообразно по затратам памяти, поэтому соответствие $\boldsymbol{S}\times\boldsymbol{U}$ должно иметь определенные структурные свойства.

*Определение пути доставки ключа (Path-key Establishment).* В больших сенсорных сетях возникают ситуации, когда у некоторых пар узлов нет общих ключей, но имеется возможность передачи ключа одного узла другому по цепочке секретных каналов с использованием общих ключей узлов, являющихся вершинами этой цепочки. Как правило, возможны цепочки из двух шагов (двухшаговые цепочки). В схемах распределения ключей, допускающих использование таких цепочек, число ключей, распределяемых узлам, можно уменьшить.

Описанные два этапа являются этапами использования ключевого пространства БСС.

Таким образом, в качестве математической модели ключевого пространства в БСС выступает система множеств ($\boldsymbol{K}$, $\boldsymbol{B}$), где $\boldsymbol{K}$ — множество единиц ключевой информации, а $\boldsymbol{B}$ — множество блоков, являющихся подмножествами множества $\boldsymbol{K}$. Данная модель является моделью, анализируемой в теории комбинаторных блок-схем.

Начальными работами по изучению схем пересечения множеств на основе комбинаторных блок-схем для предварительного распределения ключей можно считать [7 — 9].

Для распределения ключей в беспроводных сенсорных сетях (БСС) в [10, 11] были применены проективные плоскости. Их использование оказалось проблематичным из-за необходимости размещения в узлах сети большого числа ключей, превышающего квадратный корень из числа узлов в сети, что в условиях ограниченных ресурсов узлов беспроводных сенсорных сетей считается неприемлемым. В связи с этим были применены трансверсальные блок-схемы [6, 12]. В них число размещаемых в узлах БСС ключей стало удовлетворительным, но утрачивалась локальная связность сети, что компенсировалось возможностью соединений узлов из различных блоков при использовании единственного посредника — узла, в котором проходили расшифрование и зашифрование при передаче из одного узла в другой или вычисление нового ключа и передача его узлам по защищенным каналам.

Ключевое пространство создается с учетом ряда ограничений, определяемых спецификой узлов сети. Узлами являются сенсорные датчики со встроенными компьютерами для приема, обработки и передачи данных. В [13] приведен пример характерной аппаратной конфигурации сенсорных узлов Bercley Mica Motes с 8-битным процессором Atmel ATmega 128L тактовой частотой 4 МГц и 128 Кбайт, а также 4 Кбайт SRAM. Процессор поддерживает только минимальный RISC-подобный набор команд, без поддержки умножения. Передатчик платформы UC Berkeley Mica обладает полосой пропускания 10 Кбит/с и размером пакета около 30 байтов при низкой надежности передачи данных. Радиоприемник диапазона ISM поддерживает связь с максимальной скоростью 40 Кбит/с на дальность до 100 футов.

Для обеспечения информационной безопасности используют блоки криптографических систем с заложенными в них ключами. Для хранения ключей требуется память, объем которой в сенсорных узлах весьма ограничен.

Применение ключевого пространства предполагает вычисление рабочих, разделяемых узлами ключей (Shared Keys), а это связано с затратой времени и электрической энергии при ограниченности энергетического ресурса сенсорного узла. Наконец, условия размещения узлов и небольшой радиус действия их передающих устройств ограничивают возможность организации защищенного информационного обмена непосредственно одного узла с другим на основе имеющейся в них ключевой информации.

В [13, 14] перечислены особенности сенсорных сетей, принимаемые во внимание при разработке безопасных протоколов этапа начальной загрузки:

- ограниченные вычислительные и энергетические ресурсы узла практически исключают использование алгоритмов с открытым ключом, например, по схеме согласования ключей Диффи–Хеллмана, требующих при реализации на встроенном компьютере десятки минут, что позволяет выводить узлы из строя атаками на истощение ресурса (DoS-Denial of Service);

● ограниченный объем памяти сенсорного узла не позволяет применять системы пересечения множеств, удовлетворяющие условию (1), т. е. узлы доверяют один другому, что создает понижение устойчивости к их компрометации;

● уязвимость узлов к физическому захвату и атакам раскрытия ключей;

● отсутствие априорных знаний о конфигурации после развертывания: протокол безопасности не должен предполагать предварительное знание, какие узлы будут соседями в сети;

● ограниченный объем памяти для хранения ключей в данном узле не допускает установки уникальных ключей с каждым другим узлом в сети;

● типичные платформы сенсорных сетей имеют очень низкую пропускную способность;

● зависимость от базовых станций порождает новые уязвимости атаками на базовую станцию.

В настоящей работе обоснован алгоритмический подход к созданию и использованию ключевых пространств БСС с учетом этих особенностей. Перечислим его основные положения, а также обусловленные ими необходимые по [13, 14] свойства проектируемой сети.

Схема предварительного распределения ключей является распределенной системой, структура которой соответствует определенной комбинаторной блок-схеме — циклической или ациклической проективной плоскости, линейной или квадратичной трансверсальной блок-схеме, поэтому *она функциональна без привлечения базовой станции в качестве арбитра или верификатора*.

Инициализация и масштабирование системы заключаются в изготовлении физического узла, вычислении номеров его ключей, установке этих ключей в узел и подключении узла к системе. Номер общего ключа для коммутации двух узлов определяется по их номерам или идентификаторам, он используется, если общий ключ имеется и есть физическая связь между узлами. Если общего ключа нет или нет физической связи между узлами, то по номерам двух узлов вычисляется (возможно, при нарушениях физических связей за несколько итераций) номер узла, имеющего общий ключ и физическую связь с одним из них и, возможно, другой общий ключ и физическую связь с ним. Таким образом, *развернутые узлы позволяют устанавливать безопасную связь друг с другом*.

Блоки комбинаторной блок-схемы вычисляются по мере масштабирования системы. Число блоков комбинаторной схемы не меньше числа узлов предельно масштабированной системы, при масштабировании дополнительные узлы устанавливаются и комплектуются ключами из единого источника. *Дополнительные легитимные узлы, развернутые позднее, могут образовывать защищенные соединения с уже развернутыми узлами. Это означает, что информация о начальной загрузке всегда должна присутствовать и не может просто удаляться после развертывания. В то же время неавторизованные узлы не могут устанавливать связь с сетевыми узлами и, таким образом, получать доступ к сети. Любая сенсорная сеть развертывается только одной стороной, т. е. сенсорные узлы, развертываемые несколькими независимыми ненадежными сторонами, не являются частью одной сети.*

Имеется возможность определения в процессе функционирования наличия физической связи между двумя узлами системы, ключа с данным номером, ключа с данным номером в узле с данным номером (ключи могут отсутствовать по условиям безопасности) и узла с данным номером. *Схема может работать без предварительной информации о том, какие узлы вступают в связь с другими в пределах дальности действия после развертывания.*

Реализованная система содержит физические узлы, соответствующие некоторым блокам комбинаторной блок-схемы. Применяются алгебраические структуры, определяемые над полями малой характеристики, при этом используются только аддитивные операции или табличные реализации мультипликативных операций. Поэтому *требования к вычислительным ресурсам и памяти для схемы могут быть низкими, а схема будет устойчивой к DoS-атакам из внешних источников.*

### Алгоритмы вычисления блоков и дуальных блоков комбинаторных блок-схем и алгоритмы решения производных задач

Теория и подходы к построению комбинаторных блок-схем изложены в монографиях [15, 16].

Приведем основные используемые понятия этой теории и авторские алгоритмические решения [17], позволившие создать систему указанных алгоритмов и решить поставленную задачу.

Комбинаторная блок-схема — это пара ($\boldsymbol{X}$, $\boldsymbol{A}$), где $\boldsymbol{X}$ — конечное множество элементов, а $\boldsymbol{A}$ — конечное множество подмножеств множества $\mathbf{X}$, называемых блоками. Используются также двойственные относительно схемы ($\boldsymbol{X}$, $\boldsymbol{A}$) комбинаторные схемы. В роли множества элементов двойственной блок-схемы выступает множество идентификаторов блоков из множества $\boldsymbol{A}$, множество ее блоков находится во взаимно однозначном соответствии с множеством элементов $\boldsymbol{X}$, при этом блоки являются множествами идентификаторов блоков из $\boldsymbol{A}$, содержащих элементы, соответствующие этим блокам.

Применительно к распределению ключей, множество $\boldsymbol{X}$ — множество идентификаторов ключей. Блоки из множества $\boldsymbol{A}$ соответствуют узлам сети и состоят из идентификаторов ключей, размещенных в данном узле. Блоки двойственной блок-схемы состоят из идентификаторов блоков множества $\boldsymbol{A}$, содержащих идентификатор ключа, соответствующий идентификатору данного блока двойственной блок-схемы.

Для применения комбинаторных блок-схем при управлении ключами требуются алгоритмы вычисления блоков (множеств идентификаторов ключей, распределяемых данному узлу) по заданным идентификаторам и дуальных блоков (множеств идентификаторов узлов, которым распределен ключ с идентификатором, совпадающим с идентификатором дуального блока), а также алгоритмы решения производных задач: вычисления идентификаторов общих ключей двух узлов, для двух заданных идентификаторами узлов определения идентификатора узла, имеющего общий ключ с одним из этих узлов и, возможно, другой ключ с другим и др.

Для идентификации элементов, блоков и дуальных блоков использована их нумерация начальными неотрицательными целыми числами по правилу двойственности: множества элементов и дуальных блоков находятся во взаимно однозначном соответствии по нумерации, дуальный блок с заданным номером содержит номера блоков, содержащих элементы с тем же номером. Таким образом, основными являются задачи вычисления блока и дуального блока по их номерам.

Рассматриваемые комбинаторные блок-схемы характеризуются порядком $n$, являющимся простым числом или степенью простого числа (что считается достаточным условием их существования). Проективная и двойственная проективная плоскости имеют по $n^2 + n + 1$ элементов и блоков. Каждый блок и каждый дуальный блок содержат $n + 1$ элементов. Любые два элемента встречаются в одном блоке, и идентификаторы любых двух блоков встречаются в одном дуальном блоке. При этом любые два блока и любые два дуальных блока имеют по одному общему элементу. Проективная и двойственная проективные плоскости в теории комбинаторных блок-схем являются ($n^2 + n + 1$, $n + 1$,1) уравновешенными неполными блок-схемами (УНБС).

При построении циклической проективной плоскости используется ($n^2 + n + 1$, $n + 1$,1)-разностное множество. Это множество $n + 1$ неотрицательных целых чисел. Разностью по модулю $n^2 + n + 1$ некоторых двух из них можно представить любое неотрицательное целое число, не превышающее $n^2 + n$. Алгоритмы построения разностных множеств, порядок $n$ которых есть простое число или степень простого числа, известны [15, 16].

Линейная трансверсальная комбинаторная блок-схема $TD(k, n)$ имеет $kn$ элементов и $n^2$ блоков, содержащих по $k$ элементов. При этом у двух блоков не более одного общего элемента, но для любых двух блоков имеется третий блок, имеющий с каждым из них общий элемент.

Квадратичная комбинаторная блок-схема $TD(3, k, n)$ формируется из $kn$ элементов и $n^3$ блоков, содержащих по $k$ элементов. При этом два блока имеют не более двух общих элементов, но для любых двух блоков есть третий блок, имеющий с каждым из них общий элемент.

Распределенное (независимое) вычисление блоков проходит на основе их алгебраических идентификаторов, в роли которых выступают [17]:

- разностное множество и номер блока или дуального блока (для циклических проективных плоскостей);
- пары или тройки элементов конечного поля (для линейных и квадратичных трансверсальных плоскостей);
- нормированные базисы двухмерных подпространств трехмерного векторного пространства над конечным полем (для ациклических проективных плоскостей). Номера $n_1(j)$ первого $e_1(j)$ и $n_2(j)$ второго $e_2(j)$ элементов базиса блока определяются по номеру $j$ блока [17]:

$$n_1(j) = \begin{cases} 0, \text{ если } j \le n; \\ \left\lfloor \dfrac{j-1}{n} \right\rfloor, \text{ если } j > n; \end{cases}$$

$$n_2(j) = \begin{cases} 1 + nj, \text{ если } j \le n; \\ j - (n_1(j) - 1)n, \text{ если } j > n. \end{cases}$$

Здесь $e_1 = e_1(j) = \psi^{-1}(n_1(j))$, $e_2(j) = \psi^{-1}(n_2(j))$, где $\psi(\cdot)$ — функция нумерации блоков.

Эти же алгебраические идентификаторы работают и при решении некоторых производных задач.

В [17] получены алгоритмы вычисления блоков $B_c(j)$ и дуальных блоков $B_c^*(j)$ циклических проективных плоскостей по номеру $j$ блока и соответствующие аналитические решения: при заданном разностном множестве $D$ блок с номером $j$ циклической проективной плоскости и дуальный блок с номером $j$ выглядят как множество вычетов:

$$B_c(j) = \{b : b = (j + d)_{n^2+n+1}, d \in D\};$$

$$B_c^*(j) = \{b : b = (j - d)_{n^2+n+1}, d \in D\}.$$

Также в [17] приведены аналитические решения задач вычисления блоков $B_{ac}(j)$ и дуальных блоков $B_{ac}^*(j)$ применительно к ациклическим проективным плоскостям, блоков $B_{a,b}$ и $B_{a,b,c}$ и множеств номеров таких блоков, имеющих заданный элемент $t$, применительно к линейным и квадратичным трансверсальным комбинаторным блок-схемам по их алгебраическим идентификаторам.

Алгоритмические решения данных задач оформлены Свидетельствами о государственной регистрации программы для ЭВМ[1].

[1]Свид. № 2020618211 РФ. Программа для вычисления блоков циклической проективной геометрии и совокупностей номеров ее блоков, содержащих заданное множество элементов / А.Б. Фролов, А.М. Винников, Н.П. Кочетова // Реестр программ для ЭВМ. 2020. Бюл. № 8.

Свид. № 2020618352 РФ. Программа для вычисления блоков линейной или квадратичной трансверсальной комбинаторной блок-схемы и совокупностей номеров их блоков, содержащих данный элемент или пересекающихся с двумя данными блоками / А.Б. Фролов, А.М. Винников, Д.Ю. Темников // Там же.

Свид. 2020619591 РФ. Программа для вычисления блоков ациклической проективной геометрии и совокупностей номеров ее блоков, содержащих один или два элемента / А.Б. Фролов, А.М. Винников, А.О. Клягин // Там же.

Рассмотрим две производные задачи.

Общий элемент двух блоков, если он существует, вычислим как пересечение двух блоков, рассчитанных по описанным алгоритмам для любой рассматриваемой комбинаторной блок-схемы.

Однако для трансверсальных блок-схем можно использовать алгоритмы с алгебраическими идентификаторами блоков [6].

Для трансверсальной блок-схемы $TD(k, n)$ при задании блоков $b_1$ и $b_2$ двумя идентификаторами — $id(j_1) = (a, b)$ и $id(j_2) = (a', b')$ [6] общий элемент получается по программе:

if $a! = a'$:
$x = (b' - b)(a - a')^{-1} \bmod p$
if $x \le k - 1$:
    return $\varphi([x, ax + b])$
return []

Здесь $\varphi(\cdot)$ — функция нумерации элементов векторного пространства [17], а программа — алгоритм решения линейных уравнений $ax + b = a'x + b'$ или $(a - a')x + (b - b') = 0$ над конечным полем или расширением конечного поля.

Для трансверсальной блок-схемы $TD(3, k, n)$ при задании блоков $b_1$ и $b_2$ двумя идентификаторами $id(j_1) = (a, b, c)$ и $id(j_2) = (a', b', c')$ [17]:

if $a! = a'$:
return $\varphi([x, ax^2 + bx + c])$:

$$x = \left(b + b' \pm \sqrt{(b - b')^2 - 4(a - a')(c - c')}\right)\left(2(a - a')\right)^{-1},$$

$x \le k - 1]$
return [].

Это алгоритм решения квадратного уравнения $ax^2 + bx + c = a'x^2 + b'x + c'$, или $(a - a')x^2 + (b - b')x + (c - c') = 0$ над конечным полем или расширением конечного поля. В нем использована операция извлечения квадратного корня. Алгоритмы подобной операции в конечных полях, как и оценки сложности, рассмотрены в [18 — 21].

Выходом указаных функций является (возможно, пустое) множество номеров общих ключей узлов, соответствующих блокам с номерами $j_1, j_2$.

Вторая производная функция — поиск блока, пересекающегося с двумя данными блоками, решается построением пересечения дуальных блоков, номера которых являются номерами ключей, один из которых принадлежит одному блоку, а другой — второму.

### О реализации алгоритмического подхода по созданию и использованию ключевого пространства беспроводной сенсорной сети

Как было отмечено, инициирование и масштабирование системы заключаются в изготовлении физического узла, вычислении номеров его ключей, установке этих ключей в узел и подключении узла к системе. Имеется потенциально пополняемый секретный пул $\boldsymbol{K}$ ключей, пронумерованных начальными неотрицательными числами. Исходя из предела $v$ масштабирования системы (максимально возможного числа узлов в ней), и допустимого числа $k$ ключей в блоке, выбирается комбинаторная блок-схема и ее параметры.

Для проективной плоскости:

$$n = \min(k, \{m{:}m^2 + m + 1 \ge v\}).$$

Для линейной трансверсальной блок-схемы $TD(k, n)$:

$$n = \min(m{:}m^2 \ge v);$$

Для квадратичной трансверсальной блок-схемы $TD(3, k, n)$:

$$n = \min(m{:}m^3 \ge v).$$

При инициализации вычисляется начальный блок с заданным номером $j$ и определяются номера входящих в него элементов. По ним заполняется ключами секретный сегмент памяти узла. При масштабировании создается блок с новым номером, также устанавливаются номера входящих в него элементов и заполняется секретный сегмент его памяти. Одновременно при инициализации или масштабировании в постоянную память узла, соответствующего блоку с номером $j$, записываются идентификаторы $id(j)$.

Для проективной плоскости:

$$\text{базис блока } id(j) = (e_1(j), e_2(j)).$$

Для линейной трансверсальной блок-схемы $TD(k, n)$:

$$id(j) = \varphi^{-1}(j) = (a, b).$$

Для квадратичной трансверсальной блок-схемы $TD(3, k, n)$:

$$id(j) = \varphi^{-1}(j) = \varphi^{-1}(j) = (a, b, c) \text{ блока } A_{a,b,c}.$$

Для характеристики ограничений применения рассмотренных комбинаторных блок-схем используем ряд списков:

- $L_{key}$ — номеров исключенных (скомпрометированных) ключей;
- $L_{blockkey}$ — исключенных пар [<номер узла>, <номер ключа>] (отражение неполноты укомплектования узла ключами);
- $L_{blockblock}$ — пар [<номер узла>, <номер узла >] (характеристика наличия физической связи между узлами) ;
- $L_{block}$ — номеров реализованных узлов <номер узла> (характеристика уровня масштабирования системы).

По ним определяются значения предикатов (в аббревиатурах имен предикатов el — elimination, k — key, b — block, n — number):

— kel(kn):kn $\in L_{key}$;
— bkel([bn,kn]):[bn,kn] $\in L_{blockkey}$;
— bbel([bn,bn]):[bn,bn] $\in L_{blockblock}$;
— blockexistence(bn):bn $\in L_{block}$.

При описании алгоритмов применим функции:

— psi($e$) — нумерации элементов $e$ комбинаторной блок-схемы;

— psiinv($n$) — вычисления элемента комбинаторной блок-схемы по его номеру $n$;

— dualhiinv($N$) — вычисления блока двойственной комбинаторной блок-схемы по его номеру (набора номеров блоков комбинаторной блок-схемы, содержащих элемент с заданным номером $N$).

— id($j_1$) — вычисления идентификатора блока с номером $j_1$;

— cens($id(j_1)$, $id(j_2)$) — вычисления множества номеров общих элементов блоков с номерами $j_1, j_2$ по их идентификаторам.

С использованием указанных функций и представленных предикатов в табл. 1 дан алгоритм вычисления условий защищенной коммуникации между двумя узлами при заданных предикатами ограничениях. Он предназначен для проектирования защищенных коммуникаций в компьютерной сети, структура которой потенциально (т. е. при максимально возможном масштабировании) соответствует одной из рассмотренных комбинаторных схем при заданных ограничениях (включающих определенный уровень масштабирования системы, недопустимость использования отдельных ключей, неполноту комплектации узлов ключами, отсутствие некоторых двусторонних технических соединений) в предположении стабильности последних. Для пар узлов, между которыми необходимы защищенные коммуникации, вычисляются номера ключей для возможной непосредственной связи или двухшаговой связи через узел-посредник. При этом выявляются ситуации, при которых ни один из указанных видов коммуникации невозможен.

*Таблица 1*

**Алгоритм коммуникации в БСС**

ВХОД: Пара номеров узлов $j_1, j_2$.
ВЫХОД: Описание наиболее простой защищенной коммуникации между заданными двумя узлами указанием:
— номера ключа для возможной непосредственно коммутации на нем,
— номера ключа и номера узла-посредника для возможной коммутации на нем при невозможности непосредственной коммутации на этом ключе,
— номеров двух ключей и номера узла-посредника для возможной коммутации с вычислением в узле-посреднике общего ключа для непосредственной коммуникации между узлами или через узел-посредник, если непосредственная связь между двумя узлами невозможна, или сообщения о невозможности коммутации при заданных ограничениях.

```
keys = cens(id(j1), id(j2))
for it in keys:
    if not kel(it) and not bkel (j1, it) and not bkel (j2, it) and not bbel(j1,j2):
       print "Номер ключа непосредственной связи узлов с номерам j1 =", psi(id(j1)),"и j2 =", psi(id(j2)), ":",it
       return [it]
keysofj1= psiinv(j1)
keysofj2= psiinv(j2)
for it1 in keysofj1:
    for it2 in keysofj21:
       if it1==it2:
         if  not kel(it1) and not bkel(j1, it1) and not bkel(j2, it1):
              ckey=it1
              commonblocks= dualhiinv(ckey)
              for it3 in commonblocks:
                   if not bkel(it3,ckey) and not it3==j1 and not it3==j2:
                      print "Номер ключа связи узлов с номерами j1=",j1,"и j2=" ,j1, "через узел с номером “, it3,” :", ckey
                      return [ckey,it3]
for it1 in keysofj1:
    for it2 in keysofj2:
       if it1!=it2 and not bkel([j1,it1]) and not bkel([j2,it2]) and not kel(it1) and not kel (it2):
         commonblocks=sorted(set(dualhiinv ([it1]))&set(dualhiinv ([it2])))
         if commonblocks !=[]:
              for it3 in commonblocks:
                   if not bkel([it3,it1]) and not bkel([it3,it2]) and not bbel([it3,j2]) and not it3==j1 and not it3==j2 and not bbel[bn1,it3]:
                      print "узел с номером j1=",j1,"по ключу с номером", it1,"связан с узлом с номером", it3,"связанным  по ключу", it2,"с узлом с номером",j2),"
                      return [j1, it1, it3, it2, j2]
print "Связи (непосредственной или через одного посредника) между узлами с номерами j1=",j1,"и j2=" ,j2,"нет !"
return []
```

Примечания.
1. Применяются функции id($j$), cens(id($j_1$), id($j_2$)) и dualhiinv($t$) для определенных типов комбинаторных схем (проективная плоскость, линейная или квадратичная трансверсальная блок-схемы).
2. По умолчанию для всех используемых в алгоритме номеров блоков bn выполняется blockexistence(bn).

**Компьютерное моделирование системы предварительного распределения ключей**

В таблице 2 продемонстрирован алгоритм, моделирующий функционирование компьютерной сети, использующей схему предварительного распределения ключей комбинаторно-блочного типа, при котором защищенные коммуникации заранее не планируются, а организуются при взаимодействии узлов. Узлы транслируют пары идентификаторов (id($j_1$), id($j_2$)), один из которых — идентификатор узла с номером $j_1$, являющегося инициатором коммуникации, а второй — идентификатор вызываемого узла с номером $j_2$.

Предполагается, что узлы периодически воспринимают сообщения при наличии технических связей. Тогда узел $j_2$ определяет, что необходима связь с узлом $j_1$ и транслирует пару идентификаторов (id($j_1$), id($j_2$)), в итоге оба узла вычисляют номер ключа cens(id($j_1$), id($j_2$)). Узел $j_3$, принимая сообщение (id($j_1$), id($j_2$)), при котором cens(id($j_1$), id($j_3$)) ≠ [] и cens(id($j_2$), id($j_3$)) ≠ [], транслирует тройку идентификаторов ((id($j_2$), id($j_1$) id($j_3$)). По ней узлы $j_1$ и $j_2$ вычисляют номера ключей cens(id($j_1$), id($j_3$)) и cens(id($j_2$), id($j_3$)) двухшаговой коммуникации и номер $j_3$ узла-посредника. Ясно, что последовательная организация алгоритма допускает распараллеливание, что и соответствует анализируемой модели функционирования.

Указанный алгоритм моделирует также коммуникацию узла $j_1$ и вызываемого им узла $j_2$, который, в отличии от узла $j_1$, не публикует, а принимает набор [$j_1$, $j_2$].

На примере схемы предварительного распределения ключей на основе квадратичной трансверсальной блок-схемы покажем возможность реализации объявленных во введении положений алгоритмического подхода к построению и использованию систем комбинаторно-блочной структуры.

Пусть схема предварительного распределения ключей построена по квадратичной трансверсальной блок-схеме ***TD***(3, 3, 4). По умолчанию, ее элементами, т. е. номерами ключей, являются числа 0, …, 11, номерами блоков — числа 0, …, 63, а блоками, т. е. множествами номеров ключей, назначенных узлам сети, — тройки элементов:

0. [0, 4, 8], 1. [0, 7, 10], 2. [0, 5, 11], 3. [0, 6, 9], 4. [0, 6, 11], 5. [0, 5, 9],
6. [0, 7, 8], 7. [0, 4, 10], 8. [0, 7, 9], 9. [0, 4, 11], 10. [0, 6, 10], 11. [0, 5, 8],
12. [0, 5, 10], 13. [0, 6, 8], 14. [0, 4, 9], 15. [0, 7, 11], 16. [1, 5, 9], 17. [1, 6, 11],
18. [1, 4, 10], 19. [1, 7, 8], 20. [1, 7, 10], 21. [1, 4, 8], 22. [1, 6, 9], 23. [1, 5, 11],
24. [1, 6, 8], 25. [1, 5, 10], 26. [1, 7, 11], 27. [1, 4, 9], 28. [1, 4, 11], 29. [1, 7, 9],
30. [1, 5, 8], 31. [1, 6, 10], 32. [2, 6, 10], 33. [2, 5, 8], 34. [2, 7, 9], 35. [2, 4, 11],
36. [2, 4, 9], 37. [2, 7, 11], 38. [2, 5, 10], 39. [2, 6, 8], 40. [2, 5, 11], 41. [2, 6, 9],
42. [2, 4, 8], 43. [2, 7, 10], 44. [2, 7, 8], 45. [2, 4, 10], 46. [2, 6, 11], 47. [2, 5, 9],

*Таблица 2*

**Алгоритм моделирования коммуникации в сети комбинаторно-блочного типа вызывающего узла, имеющего номер $j_1$, и опубликовавшего набор [$j_1$, $j_2$]**

```
ВХОД: 1. Набор [j1, j2];
ВЫХОД: Отклик сети [L_j^(1), L_j^(2), L_j^(3)] ∈ {[[],[],[]], [[j1], [j2], []],[[j1], [j2], [j3]]}.
id1= id(j1),
id2= id(j2),
comelementnumbers = cens(id1, id2),
for it in comelementnumbers:
    if not kel(it) and not bkel (j1, it) and not bkel (j2, it) and not bbel(j1, j2):
        return [[id1],[id2],[]]
for j  in range (0, v):
    if (j!= j1 and j!= j2):
        id3=id(j)
        cens1=cens(id1, id3)
        cens2=cens(id2, id3)
        if(cens1!=[] and cens2!=[]):
           for k1 in cens1:
             if(not bkel(j, k1) and not bkel(j1, k1)):
                for k2 in cens2:
                   if(not bkel(j, k2) and not bkel(j2, k2)):
                       return [[id1], [id2], [id3]]
print "Связи (непосредственной или через одного посредника) между узлами с номерами ", j1,"и", j2,"нет !"
return [[],[],[]]
```

Примечания.

1. Функции cens() для определенных типов комбинаторных схем (проективная плоскость, линейная или квадратичная трансверсальная блок-схемы).

2. По умолчанию, для всех используемых в алгоритме номеров bn блоков выполняется blockexistence(bn).

48. [3, 7, 11], 49. [3, 4, 9], 50. [3, 6, 8], 51. [3, 5, 10], 52. [3, 5, 8], 53. [3, 6, 10],
54. [3, 4, 11], 55. [3, 7, 9], 56. [3, 4, 10], 57. [3, 7, 8], 58. [3, 5, 9], 59. [3, 6, 11],
60. [3, 6, 9], 61. [3, 5, 11], 62. [3, 7, 10], 63. [3, 4, 8].

Блоками двойственной трансверсальной блок-схемы *DTD*(3, *k*, *n*) являются следующие числовые наборы (номера узлов сети, в которых имеется ключ с заданным номером):

0. [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15],
1. [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31],
2. [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47],
3. [48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63],
4. [0, 7, 9, 14, 18, 21, 27, 28, 35, 36, 42, 45, 49, 54, 56, 63],
5. [2, 5, 11, 12, 16, 23, 25, 30, 33, 38, 40, 47, 51, 52, 58, 61],
6. [3, 4, 10, 13, 17, 22, 24, 31, 32, 39, 41, 46, 50, 53, 59, 60],
7. [1, 6, 8, 15, 19, 20, 26, 29, 34, 37, 43, 44, 48, 55, 57, 62],
8. [0, 6, 11, 13, 19, 21, 24, 30, 33, 39, 42, 44, 50, 52, 57, 63],
9. [3, 5, 8, 14, 16, 22, 27, 29, 34, 36, 41, 47, 49, 55, 58, 60],
10. [1, 7, 10, 12, 18, 20, 25, 31, 32, 38, 43, 45, 51, 53, 56, 62],
11. [2, 4, 9, 15, 17, 23, 26, 28, 35, 37, 40, 46, 48, 54, 59, 61].

Блоки комбинаторных блок схем *TD*(3, 3, 4) и *DTD*(3, 3, 4) вычисляются независимо один от другого, например:

psiinv (48) = [3, 7, 11],

dualhiinv (7) = [1, 6, 8, 15, 19, 20, 26, 29, 34, 37, 43, 44, 48, 55, 57, 62].

Необходимые блоки вычисляются по мере масштабирования системы. Даже если система соответствует полной комбинаторной блок-схеме, ее использование может быть ограничено рядом условий, которые определим списками исключений $L_{key}$, $L_{blockkey,}$ $L_{blockblock}$, полагая, что список $L_{block}$ содержит все используемые в эксперименте блоки.

Параметры (используемые ключи и узлы) конфиденциальной коммуникации между узлами сети вычисляются с учетом такого рода ограничений по алгоритму, приведенному в табл. 2.

Применительно к компьютерной сети, проектируемая структура которой должна соответствовать квадратичной трансверсальной блок-схеме над полем GF(2^2) при длине блоков $k = 3$, даны примеры вычислений по данному алгоритму параметров коммуникации между блоками 55 и 57 с двумя общими ключами и непересекающимися блоками 30 и 41.

**Пример 1.** Ограничений нет:

Номер ключа непосредственной связи узлов 55 и 57:3.

**Пример 2.** Исключен ключ номер 3:

$L_{key} = [3]$.

Номер ключа непосредственной связи узлов 55 и 57:7.

**Пример 3.** Исключены ключ номер 3 и связь между блоками 55 и 57:

$L_{key} = [3]$; $L_{blockblock} = [[55, 57]]$

Номер ключа связи узлов 55 и 57 через узел 1:7

**Пример 4.** Исключены ключ номер 7 из узла 57 и ключ номер 3 из узла 55:

$L_{blockkey} = [[57, 7],[55, 3]]$.

Узел 55 по ключу 7 связан с узлом 48, связанным по ключу 3 с узлом 57

**Пример 5.** Исключены связи между узлами с номерами из ряда пар:

$L_{blockblock}$ = [[55, 57], [55, 48], [55, 49], [55, 50], [55, 51], [55, 52], [55, 53], [55, 54], [55, 56], [55, 58], [55, 59], [55, 60], [55, 61], [55, 62], [55, 63], [55, 1], [55, 6], [55, 8], [55, 15], [55, 19], [55, 20], [55, 26], [55, 29], [55, 34], [55, 37], [55, 43], [55, 44]].

Непосредственная или через одного посредника связь между узлами 55 и 57 невозможна.

**Пример 6.** Исключены ключи с номерами 3 и 7 из узлов 55 и 57:

$L_{blockkey}$ = [[55, 3], [55, 7], [57, 3], [57, 7]].

Непосредственная или через одного посредника связь между узлами 5 и 57 невозможна.

**Пример 7.** Связь между узлами, не имеющими общих ключей при отсутствии ограничений:

Узел 30 по ключу 1 связан с узлом 17, связанным по ключу 6 с узлом 1.

Нетрудно убедиться в справедливости результатов эксперимента путем сопоставления с приведенным полным описанием квадратичной трансверсальной блок-схемы *TD*(3, 3, 4), и двойственной трансверсальной блок-схемы *DTD*(3, 3, 4). Компьютерные эксперименты выполнены с использованафием системы компьютерной алгебры Sage [22] посредством алгебраического процессора МЭИ [23].

**Заключение**

На основе анализа особенностей БСС сформулированы и реализованы согласующиеся с требованиями к ключевым пространствам положения алгоритмического подхода к созданию и использованию подобных ключевых пространств.

Применительно к определенным типам комбинаторных блок-схем сформулировано и алгебраически обосновано правило двойственности нумерации элементов, блоков и дуальных блоков комбинаторной блок-схемы.

Использованы авторские алгоритмы распределенного вычисления блоков и дуальных блоков по алгебраическим идентификаторам, вычисляемым по номерам блоков. Приведены алгоритмы вычисления общих элементов блоков и дуальных блоков по их номерам, а также алгоритмы вычисления параметров защищенной коммутации узлов в условиях ограничений по физической связи или использованию ключей.

Результаты могут быть применены при проектировании или компьютерном моделировании функционирования БСС.

**Литература**

1. **Mitchell C.J., Piper C.** Key Storage in Secure Networks // Discrete and Appl. Math. 1988. V. 21. Pp. 215—228.

2. **Mitchell C.J.** Combinatorial Techniques for Key Storage Reduction in Secure Networks // Technical Memo. Bristol: Hewlett-Packard Laboratories, 1988.

3. **Dyer M., Fenner T., Frieze A., Thomason A.** On Key Storage in Secure Networks // J. Cryptology. 1995. V. 8(4). Pp. 189—200.

4. **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. Pp. 158—166.

5. **Erdösh P., Frankl P., Füredi Z.** Families of Finite Sets in Which no Set is Covered by the Union of *r* Others // Israel J. Math. 1985. V. 51. Pp. 75—89.

6. **Lee J., Stinson D.R.** On the Construction of Practical Key Predistribution Schemes for Distributed Sensor Networks Using Combinatorial Designs // ACM Trans. Information and Syst. Security. 2008. V. 11. No. 2. Pp. 1—35.

7. **Stinson D.R., Van Trung T**. Some New Results on Key Distribution Patterns and Broadcast Encryption // Designs, Codes and Cryptography. 1998. V. 14. Pp. 261—279

8. **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. Pp. 595—617

9. **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. Pp. 189—200.

10. **Camtepe S., Yener B.** Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks // Lecture Notes in Computer Sci. 2004. V. 3193. Pp. 293—308.

11. **Lee J., Stinson D.R.** Deterministic Key Predistribution Schemes for Distributed Sensor Networks // Lecture Notes in Computer Sci. 2005. V. 3357. Pp. 294—307.

12. **Paterson M.B., Stinson D.R.** A Unified Approach to Combinatorial Key Predistribution Schemes for Sensor Networks // Designs Codes and Cryptography.·2014. V. 71. Pp. 433—457.

13. **Chan H., Perrig A., Song D.** Random Key Predistribution Schemes for Sensor Networks // Proc. Symp. Security and Privacy. 2003. Pp. 197—213.

14. **Eschenauer L., Gligor V.** A Key-management Scheme for Distributed Sensor Networks // Proc. IX ACM Conf. Computer and Communications Security. ACM Press, 2002. Pp. 41—47.

15. **Холл М.** Комбинаторика. М: Мир, 1970.

16. **Stinson D.** Combinatorial Designs: Constructions and Analysis. Berlin: Springer, 2003.

17. **Фролов А.Б., Клягин А О., Кочетова Н.П. Темников Д.Ю.** Распределенное вычисление комбинаторных блок-схем // Проблемы теоретической кибернетики: Материалы заочного семинара XIX Междунар. конф. Казань, 2020. С. 126—129.

**References**

1. **Mitchell C.J., Piper C.** Key Storage in Secure Networks. Discrete and Appl. Math. 1988;21:215—228.

2. **Mitchell C.J.** Combinatorial Techniques for Key Storage Reduction in Secure Networks. Technical Memo. Bristol: Hewlett-Packard Laboratories, 1988.

3. **Dyer M., Fenner T., Frieze A., Thomason A.** On Key Storage in Secure Networks. J. Cryptology. 1995;8(4): 189—200.

4. **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;A33:158—166.

5. **Erdösh P., Frankl P., Füredi Z.** Families of Finite Sets in Which no Set is Covered by the Union of *r* Others. Israel J. Math. 1985;51:75—89.

6. **Lee J., Stinson D.R.** On the Construction of Practical Key Predistribution Schemes for Distributed Sensor Networks Using Combinatorial Designs. ACM Trans. Information and Syst. Security. 2008;11;2: 1—35.

7. **Stinson D.R., Van Trung T.** Some New Results on Key Distribution Patterns and Broadcast Encryption. Designs, Codes and Cryptography. 1998;14:261—279

8. **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;86;2:595—617

9. **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;8;3:189—200.

10. **Camtepe S., Yener B.** Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks. Lecture Notes in Computer Sci. 2004;3193:293—308.

11. **Lee J., Stinson D.R.** Deterministic Key Predistribution Schemes for Distributed Sensor Networks. Lecture Notes in Computer Sci. 2005;3357:294—307.

12. **Paterson M.B., Stinson D.R.** A Unified Approach to Combinatorial Key Predistribution Schemes for Sensor Networks. Designs Codes and Cryptography.·2014;71:433—457.

13. **Chan H., Perrig A., Song D.** Random Key Predistribution Schemes for Sensor Networks. Proc. Symp. Security and Privacy. 2003:197—213.

14. **Eschenauer L., Gligor V.** A Key-management Scheme for Distributed Sensor Networks. Proc. IX ACM Conf. Computer and Communications Security. ACM Press, 2002:41—47.

15. **Kholl M.** Kombinatorika. M: Mir, 1970. (in Russian).

16. **Stinson D.** Combinatorial Designs: Constructions and Analysis. Berlin: Springer, 2003.

17. **Frolov A.B., Klyagin A O., Kochetova N.P. Temnikov D.Yu.** Raspredelennoe Vychislenie Kombinatornykh Blok-skhem. Problemy Teoreticheskoy Kibernetiki: Materialy Zaochnogo Seminara XIX Mezhdunar. Konf. Kazan', 2020:126—129. (in Russian).

18. **Gashkov S.B. Frolov A.B.** The Complexity of Solving Low Degree Equations over Ring of Integers and Residue Rings // Moscow University Mathematics Bull. 2019. V. 74. No. 1. Pp. 5—13.

19. **Гашков С.Б., Гашков И.Б.** Быстрый алгоритм извлечения квадратных корней в некоторых конечных полях нечетной характеристики // Вестник Московского университета. Серия 1: «Математика. Механика». 2018. Т. 73(5). С. 8—14.

20. **Волокитин М.В.** Алгебраические возможности пакета Mathematica и их расширение // Вестник МЭИ. 2010. № 2. С. 114—120.

21. **Гашков С.Б., Фролов А.Б., Попова Е.П.** Об оценках сложности алгоритмов извлечения квадратных корней в конечных полях и в кольцах вычетов // Вестник МЭИ. 2018. № 5. С. 79—88.

22. **Sage Web Site** [Офиц. сайт] www.sagemath.org (дата обращения 25.09.2020).

23. **Frolov A.B., Vinnikov A.M.** Modeling Cryptographic Protocols Using Computer Algebra Systems // Proc. V Intern. Conf. Information Technol. Engineering Education. Moscow, 2020. Pp. 1—4.

18. **Gashkov S.B. Frolov A.B.** The Complexity of Solving Low Degree Equations over Ring of Integers and Residue Rings. Moscow University Mathematics Bull. 2019;74;1:5—13.

19. **Gashkov S.B., Gashkov I.B.** Bystryy Algoritm Izvlecheniya Kvadratnykh Korney v Nekotorykh Konechnykh Polyakh Nechetnoy Kharakteristiki. Vestnik Moskovskogo Universiteta. Seriya 1: «Matematika. Mekhanika». 2018;73(5):8—14. (in Russian).

20. **Volokitin M.V.** Algebraicheskie Vozmozhnosti Paketa Mathematica i Ikh Rasshirenie. Vestnik MEI. 2010; 2:114—120. (in Russian).

21. **Gashkov S.B., Frolov A.B., Popova E.P.** Ob Otsenkakh Slozhnosti Algoritmov Izvlecheniya Kvadratnykh Korney v Konechnykh Polyakh i v Kol'tsakh Vychetov. Vestnik MEI. 2018;5:79—88. (in Russian).

22. **Sage Web Site** [Ofits. Sayt] www.sagemath.org (Data Obrashcheniya 25.09.2020).

23. **Frolov A.B., Vinnikov A.M.** Modeling Cryptographic Protocols Using Computer Algebra Systems. Proc. V Intern. Conf. Information Technol. Engineering Education. Moscow, 2020:1—4.

**Сведения об авторах:**

**Фролов Александр Борисович** — доктор технических наук, профессор кафедры математического и компьютерного моделирования НИУ «МЭИ», e-mail: abfrolov@mail.ru
**Кочетова Наталья Петровна** — студентка НИУ «МЭИ», e-mail: iNatashka99@yandex.ru
**Клягин Антон Олегович** — студент НИУ «МЭИ», e-mail: klyaginto@mail.ru
**Темников Дмитрий Юрьевич** — студент НИУ «МЭИ», e-mail: dnstnt@mail.ru

**Information about authors:**

**Frolov Aleksandr B.** — Dr.Sci. (Techn.), Professor of Mathematical and Computer Modeling Dept., NRU MPEI, e-mail: abfrolov@mail.ru
**Kochetova Natalia P.** — Student of NRU MPEI, e-mail: iNatashka99@yandex.ru
**Klyagin Anton O.** — Student of NRU MPEI, e-mail: klyaginto@mail.ru
**Temnikov Dmitriy Yu.** — Student of NRU MPEI, e-mail: dnstnt@mail.ru

**Работа выполнена при поддержке:** РФФИ (проект № 19-01-00294а)
**The work is executed at support:** RFBR (Project No. 19-01-00294a)

**Конфликт интересов:** авторы заявляют об отсутствии конфликта интересов
**Conflict of interests:** the authors declare no conflict of interest

**Статья поступила в редакцию:** *06.09.2020*
**The article received to the editor:** *06.09.2020*