Данильченко Анна группа КС-38

Тема: Квантовая криптография

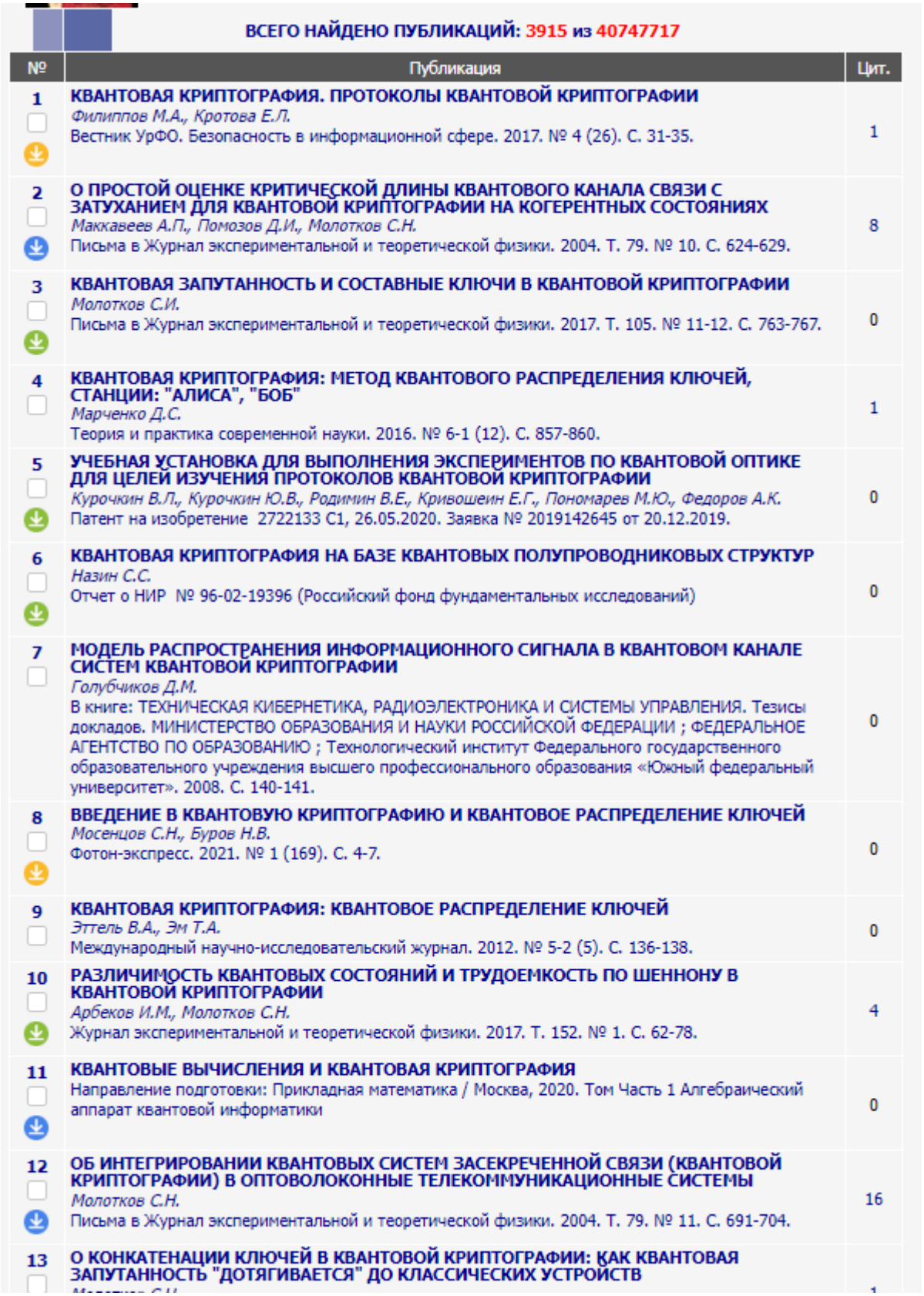
Ключевые слова

1.Криптография

ВСЕГО НАЙДЕНО ПУБЛИКАЦИЙ: 12530 из 40747717

№	Публикация	Цит.
1	**КРИПТОГРАФИЯ БУДУЩЕГО - ЭТО КВАНТОВАЯ КРИПТОГРАФИЯ** Фотоника. 2020. Т. 14. № 5. С. 412-413.	1
2	**КВАНТОВАЯ КРИПТОГРАФИЯ КАК ЭФФЕКТИВНАЯ СОСТАВЛЯЮЩАЯ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ** *Алиев Ф.К., Масленников О.В., Бардаев Э.А., Киселенко В.А., Орлов С.С., Матвеев Е.А., Шеремет И.А.* Информационная безопасность - актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности. 2018. № 1 (9). С. 3-8.	0
3	**ПРОФЕССИОНАЛЬНЫЙ СОПЕРНИК КРИПТОГРАФИИ (ПСК): МОДЕЛЬ РАЗРАБОТКИ ИГР ДЛЯ ИЗУЧЕНИЯ КРИПТОГРАФИИ** *Иванов С.Г., Доротскар З.* Международная конференция по мягким вычислениям и измерениям. 2021. Т. 1. С. 312-315.	2
4	**КВАНТОВАЯ КРИПТОГРАФИЯ - КРИПТОГРАФИЯ БУДУЩЕГО** *Смирнов М.М., Макарец А.Б.* В сборнике: Математика и математическое моделирование. Сборник материалов XV Всероссийской молодёжной научно-инновационной школы. Саров, 2021. С. 209-210.	1
5	**СИММЕТРИЧНАЯ И АСИММЕТРИЧНАЯ КРИПТОГРАФИЯ И ИХ ЗНАЧЕНИЕ ДЛЯ РАЗВИТИЯ КРИПТОГРАФИИ КАК НАУКИ** *Пониделко И.Н., Бандур К.А.* Академия педагогических идей Новация. Серия: Студенческий научный вестник. 2017. № 6. С. 224-229.	0
6	**КВАНТОВАЯ КРИПТОГРАФИЯ. ПРОТОКОЛЫ КВАНТОВОЙ КРИПТОГРАФИИ** *Филиппов М.А., Кротова Е.Л.* Вестник УрФО. Безопасность в информационной сфере. 2017. № 4 (26). С. 31-35.	1
7	**ALGORITHMS AND METHODS OF CRYPTOGRAPHY** *Bobylev Ya.O.* В сборнике: Languages in professional communication. 2021. С. 370-375.	0
8	**ӘР ТҮРЛІ IOT ҚҰРЫЛҒЫЛАРЫНА ҚОЛДАНЫЛАТЫН ЖЕҢІЛ САЛМАҚТЫ КРИПТОГРАФИЯ** *Әбілбек А.М., Муханова А.А., Оспанов Р.М.* Интернаука. 2021. № 12-3 (188). С. 40-42.	0
9	**ЭТАПЫ РАЗВИТИЯ КРИПТОГРАФИИ И СТЕГАНОГРАФИИ** *Умарзода С.У.* В сборнике: Права человека в современном мире: концепции, реальность и перспективы. Материалы международной научно-практический конференции, посвящённой Дню прав человека и международному дню борьбы с коррупцией. Душанбе, 2022. С. 404-414.	2
10	**БАҢК ЖҮЙЕСІНДЕ АҚПАРАТТЫ ҚОРҒАУДА КРИПТОГРАФИЯ ТЕХНОЛОГИЯСЫН ПАЙДАЛАНУ** *Жұбатқанов А.Б., Дәуітбаева А.О.* В сборнике: Integration of the Scientific Community to the Global Challenges of Our Time. Materials of the II international scientific-practical conference. In 3 volumes. 2017. С. 402-405.	0
11	**MODELS OF INTERACTION OF CRYPTOGRAPHY AND CHAOTIC DYNAMICS** *Shayakhmetova B.K., Ten T.L., Kogay G.D., Omarova Sh.E.* Bulletin of the Karaganda University. Mathematics Series. 2019. № 2 (94). С. 141-148.	0
12	**CRYPTOGRAPHY AND LAW: THE CASE OF BRAZIL** *Cardoso O.V.* Digital Law Journal. 2022. Т. 3. № 3. С. 8-19.	0
13	**ИНТЕРАКТИВНЫЙ ИНТЕРНЕТ-ТРЕНАЖЕР ПО КВАНТОВОЙ КРИПТОГРАФИИ** *Слонкина И.С., Пестунов А.И.* В сборнике: АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. труды Межвузовской научно-практической конференции. 2017. С. 182-185.	1

2.Квантовая криптография



ВСЕГО НАЙДЕНО ПУБЛИКАЦИЙ: 3915 из 40747717

№	Публикация	Цит.
1	**КВАНТОВАЯ КРИПТОГРАФИЯ. ПРОТОКОЛЫ КВАНТОВОЙ КРИПТОГРАФИИ** *Филиппов М.А., Кротова Е.Л.* Вестник УрФО. Безопасность в информационной сфере. 2017. № 4 (26). С. 31-35.	1
2	**О ПРОСТОЙ ОЦЕНКЕ КРИТИЧЕСКОЙ ДЛИНЫ КВАНТОВОГО КАНАЛА СВЯЗИ С ЗАТУХАНИЕМ ДЛЯ КВАНТОВОЙ КРИПТОГРАФИИ НА КОГЕРЕНТНЫХ СОСТОЯНИЯХ** *Маккавеев А.П., Помозов Д.И., Молотков С.Н.* Письма в Журнал экспериментальной и теоретической физики. 2004. Т. 79. № 10. С. 624-629.	8
3	**КВАНТОВАЯ ЗАПУТАННОСТЬ И СОСТАВНЫЕ КЛЮЧИ В КВАНТОВОЙ КРИПТОГРАФИИ** *Молотков С.И.* Письма в Журнал экспериментальной и теоретической физики. 2017. Т. 105. № 11-12. С. 763-767.	0
4	**КВАНТОВАЯ КРИПТОГРАФИЯ: МЕТОД КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ, СТАНЦИИ: "АЛИСА", "БОБ"** *Марченко Д.С.* Теория и практика современной науки. 2016. № 6-1 (12). С. 857-860.	1
5	**УЧЕБНАЯ УСТАНОВКА ДЛЯ ВЫПОЛНЕНИЯ ЭКСПЕРИМЕНТОВ ПО КВАНТОВОЙ ОПТИКЕ ДЛЯ ЦЕЛЕЙ ИЗУЧЕНИЯ ПРОТОКОЛОВ КВАНТОВОЙ КРИПТОГРАФИИ** *Курочкин В.Л., Курочкин Ю.В., Родимин В.Е., Кривошеин Е.Г., Пономарев М.Ю., Федоров А.К.* Патент на изобретение 2722133 C1, 26.05.2020. Заявка № 2019142645 от 20.12.2019.	0
6	**КВАНТОВАЯ КРИПТОГРАФИЯ НА БАЗЕ КВАНТОВЫХ ПОЛУПРОВОДНИКОВЫХ СТРУКТУР** *Назин С.С.* Отчет о НИР № 96-02-19396 (Российский фонд фундаментальных исследований)	0
7	**МОДЕЛЬ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИОННОГО СИГНАЛА В КВАНТОВОМ КАНАЛЕ СИСТЕМ КВАНТОВОЙ КРИПТОГРАФИИ** *Голубчиков Д.М.* В книге: ТЕХНИЧЕСКАЯ КИБЕРНЕТИКА, РАДИОЭЛЕКТРОНИКА И СИСТЕМЫ УПРАВЛЕНИЯ. Тезисы докладов. МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ ; ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ ; Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет». 2008. С. 140-141.	0
8	**ВВЕДЕНИЕ В КВАНТОВУЮ КРИПТОГРАФИЮ И КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ** *Мосенцов С.Н., Буров Н.В.* Фотон-экспресс. 2021. № 1 (169). С. 4-7.	0
9	**КВАНТОВАЯ КРИПТОГРАФИЯ: КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ** *Эттель В.А., Эм Т.А.* Международный научно-исследовательский журнал. 2012. № 5-2 (5). С. 136-138.	0
10	**РАЗЛИЧИМОСТЬ КВАНТОВЫХ СОСТОЯНИЙ И ТРУДОЕМКОСТЬ ПО ШЕННОНУ В КВАНТОВОЙ КРИПТОГРАФИИ** *Арбеков И.М., Молотков С.Н.* Журнал экспериментальной и теоретической физики. 2017. Т. 152. № 1. С. 62-78.	4
11	**КВАНТОВЫЕ ВЫЧИСЛЕНИЯ И КВАНТОВАЯ КРИПТОГРАФИЯ** Направление подготовки: Прикладная математика / Москва, 2020. Том Часть 1 Алгебраический аппарат квантовой информатики	0
12	**ОБ ИНТЕГРИРОВАНИИ КВАНТОВЫХ СИСТЕМ ЗАСЕКРЕЧЕННОЙ СВЯЗИ (КВАНТОВОЙ КРИПТОГРАФИИ) В ОПТОВОЛОКОННЫЕ ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ** *Молотков С.Н.* Письма в Журнал экспериментальной и теоретической физики. 2004. Т. 79. № 11. С. 691-704.	16
13	**О КОНКАТЕНАЦИИ КЛЮЧЕЙ В КВАНТОВОЙ КРИПТОГРАФИИ: КАК КВАНТОВАЯ ЗАПУТАННОСТЬ "ДОТЯГИВАЕТСЯ" ДО КЛАССИЧЕСКИХ УСТРОЙСТВ**	1

1) Молотков, С. Н. Об интегрировании квантовых систем засекреченной связи (квантовой криптографии) в оптоволоконные телекоммуникационные системы / С. Н. Молотков // Письма в Журнал экспериментальной и теоретической физики. – 2004. – Т. 79. – № 11. – С. 691-704. – EDN OOFMVX.

ОБ ИНТЕГРИРОВАНИИ КВАНТОВЫХ СИСТЕМ ЗАСЕКРЕЧЕННОЙ СВЯЗИ (КВАНТОВОЙ КРИПТОГРАФИИ) В ОПТОВОЛОКОННЫЕ ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ

МОЛОТКОВ С.Н. [1,2]

[1] Институт физики твердого тела РАН, 142432 Черноголовка, Московская обл., Россия
[2] МГУ им. М. В. Ломоносова, 142432 Черноголовка, Московская обл., Россия

Тип: статья в журнале - научная статья Язык: русский

Том: 79 Номер: 11 Год: 2004 Страницы: 691-704

ЖУРНАЛ:

ПИСЬМА В ЖУРНАЛ ЭКСПЕРИМЕНТАЛЬНОЙ И ТЕОРЕТИЧЕСКОЙ ФИЗИКИ
Учредители: Институт физических проблем им. П.Л. Капицы РАН, Российская академия наук
ISSN: 0370-274X

АННОТАЦИЯ:

Описан прототип новой системы квантовой криптографии. Подобные криптосистемы естественно называть квантовой криптографией на временных сдвигах. Схема реализует все базовые квантовые криптографические протоколы (BB84, B92, BB84(4+2)) в рамках единой оптоволоконной системы. Схема не использует оптоволоконных интерферометров типа Маха-Цандера, что позволяет естественным образом реализовать мультиплексный режим передачи секретного ключа, а также естественным образом интегрировать данную квантовую криптографическую схему в традиционные оптоволоконные телекоммуникационные системы. Предлагаемый метод временного кодирования в квантовой криптографии позволяет принципиально упростить экспериментальные схемы и вообще избавиться от наиболее тонкой оптоволоконной части - интерферометра. По сути, принципиальное отличие метода временного кодирования от метода фазового кодирования состоит в том, что из метода фазового кодирования выброшена та часть, которая использует фазовые соотношения в суперпозиции между "частями" квантового состояния, и оставлена лишь часть, использующая принцип разделения по времени. Принцип разделения по времени - общий для обоих методов и является минимально необходимым, в отличие от принципа фазового кодирования, который может быть вообще исключен. Проведено краткое сравнение нашей схемы с двумя наиболее развитыми схемами с фазовым кодированием (без самокомпенсации и с пассивной самокомпенсацией).

ПЕРЕВОДНАЯ ВЕРСИЯ:

INTEGRATION OF QUANTUM CRYPTOGRAPHY INTO FIBER-OPTIC TELECOMMUNICATION SYSTEMS
Molotkov S.N.
JETP Letters. 2004. Т. 79. № 11. С. 559-570.

2) Филиппов, М. А. Квантовая криптография. Протоколы квантовой криптографии / М. А. Филиппов, Е. Л. Кротова // Вестник УрФО. Безопасность в

информационной сфере. – 2017. – № 4(26). – С. 31-35. – EDN YMOXJU.

eLIBRARY ID: 32322067 EDN: YMOXJU

КВАНТОВАЯ КРИПТОГРАФИЯ. ПРОТОКОЛЫ КВАНТОВОЙ КРИПТОГРАФИИ

ФИЛИППОВ М.А.[1], **КРОТОВА Е.Л.**[1]

[1] Пермский национальный исследовательский политехнический университет

Тип: статья в журнале - научная статья Язык: русский

Номер: 4 (26) Год: 2017 Страницы: 31-35

УДК: 003.26 + 004.056.55 + 004.22

ЖУРНАЛ:

ВЕСТНИК УРФО. БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ
Учредители: Южно-Уральский государственный университет (национальный исследовательский университет)
ISSN: 2225-5435

КЛЮЧЕВЫЕ СЛОВА:

КРИПТОГРАФИЯ, КВАНТОВАЯ КРИПТОГРАФИЯ, ПРОТОКОЛ, ШИФРОВАНИЕ

АННОТАЦИЯ:

В этой статье представлен обзор распределения квантовых ключей, ориентированного на сферу информационных технологий. В частности, в этой статье описывается протокол BB84 и его многочисленные варианты, а также произведён их сравнительный анализ. Привлекательность идеи квантовой криптографии состоит в разработке новейшего способа генерирования полностью случайных скрытых ключей между пользователями квантовой линии связи, которые раньше никогда не встречались и не имеют общей скрытой информации. Секретность способа и невозможность незаметного съема информации с линии связи основаны на законах квантовой физики - в противоположность используемым в настоящее время способам криптографии, которые основаны на математических закономерностях и поддаются расшифровке.

3) Молотков, С. И. Квантовая запутанность и составные ключи в квантовой криптографии / С. И. Молотков // Письма в Журнал экспериментальной и теоретической физики. – 2017. – Т. 105. – № 11-12. – С. 763-767. – DOI 10.7868/S0370274X17120116. – EDN YSMGNV.

eLIBRARY ID: 29359392 EDN: YSMGNV DOI: 10.7868/S0370274X17120116

КВАНТОВАЯ ЗАПУТАННОСТЬ И СОСТАВНЫЕ КЛЮЧИ В КВАНТОВОЙ КРИПТОГРАФИИ

МОЛОТКОВ С.И. [1,2,3]

[1] Институт физики твердого тела РАН
[2] Россия Академия Криптографии Российской Федерации
[3] МГУ им. М.В. Ломоносова

Тип: статья в журнале - научная статья Язык: русский

Том: 105 Номер: 11-12 Год: 2017 Страницы: 763-767

ЖУРНАЛ:

ПИСЬМА В ЖУРНАЛ ЭКСПЕРИМЕНТАЛЬНОЙ И ТЕОРЕТИЧЕСКОЙ ФИЗИКИ
Учредители: Институт физических проблем им. П.Л. Капицы РАН, Российская академия наук
ISSN: 0370-274X

АННОТАЦИЯ:

Секретность протоколов квантовой криптографии после сеанса квантового распределения ключей (КРК) формулируется в терминах близости двух ситуаций - квантовых состояний, отвечающих реальной и идеальной ситуациям после КРК. Мерой близости является следовое расстояние. Более естественно формулировать секретность непосредственно в терминах малости вероятности успеха угадывания ключей подслушивателем после произвольного числа сеансов КРК. Возникает принципиальный вопрос, ответ на который заранее крайне неочевиден - достаточно ли критерия секретности в смысле близости реальной и идеальной ситуаций для одного сеанса КРК для того, чтобы гарантировать секретность ключей в смысле малости вероятности угадывания ключей подслушивателем для произвольного числа сеансов КРК? Показано, что ответ на данный вопрос оказывается положительным.

1) Молотков, С. Н.

ОБЩИЕ ПОКАЗАТЕЛИ

Название показателя	Значение
Число публикаций на elibrary.ru	315
Число публикаций в РИНЦ	315
Число публикаций, входящих в ядро РИНЦ	284
Число цитирований из публикаций на elibrary.ru	1259
Число цитирований из публикаций, входящих в РИНЦ	1247
Число цитирований из публикаций, входящих в ядро РИНЦ	1063
Индекс Хирша по всем публикациям на elibrary.ru	13
Индекс Хирша по публикациям в РИНЦ	13
Индекс Хирша по ядру РИНЦ	11
Число публикаций, процитировавших работы автора	710
Число ссылок на самую цитируемую публикацию	35
Число публикаций автора, процитированных хотя бы один раз	242 (76,8%)
Среднее число цитирований в расчете на одну публикацию	3,70
Индекс Хирша без учета самоцитирований	11
Индекс Хирша с учетом только статей в журналах	13
Год первой публикации	1978
Число самоцитирований	509 (40,8%)
Число цитирований соавторами	664 (53,2%)
Число соавторов	102
Число статей в зарубежных журналах	26 (8,3%)
Число статей в российских журналах	258 (81,9%)
Число статей в российских журналах из перечня ВАК	253 (80,3%)
Число статей в российских переводных журналах	133 (42,2%)
Число статей в журналах с ненулевым импакт-фактором	273 (86,7%)
Число цитирований из зарубежных журналов	350 (28,1%)
Число цитирований из российских журналов	774 (62,1%)
Число цитирований из российских журналов из перечня ВАК	742 (59,5%)
Число цитирований из российских переводных журналов	470 (37,7%)
Число цитирований из журналов с ненулевым импакт-фактором	1004 (80,5%)

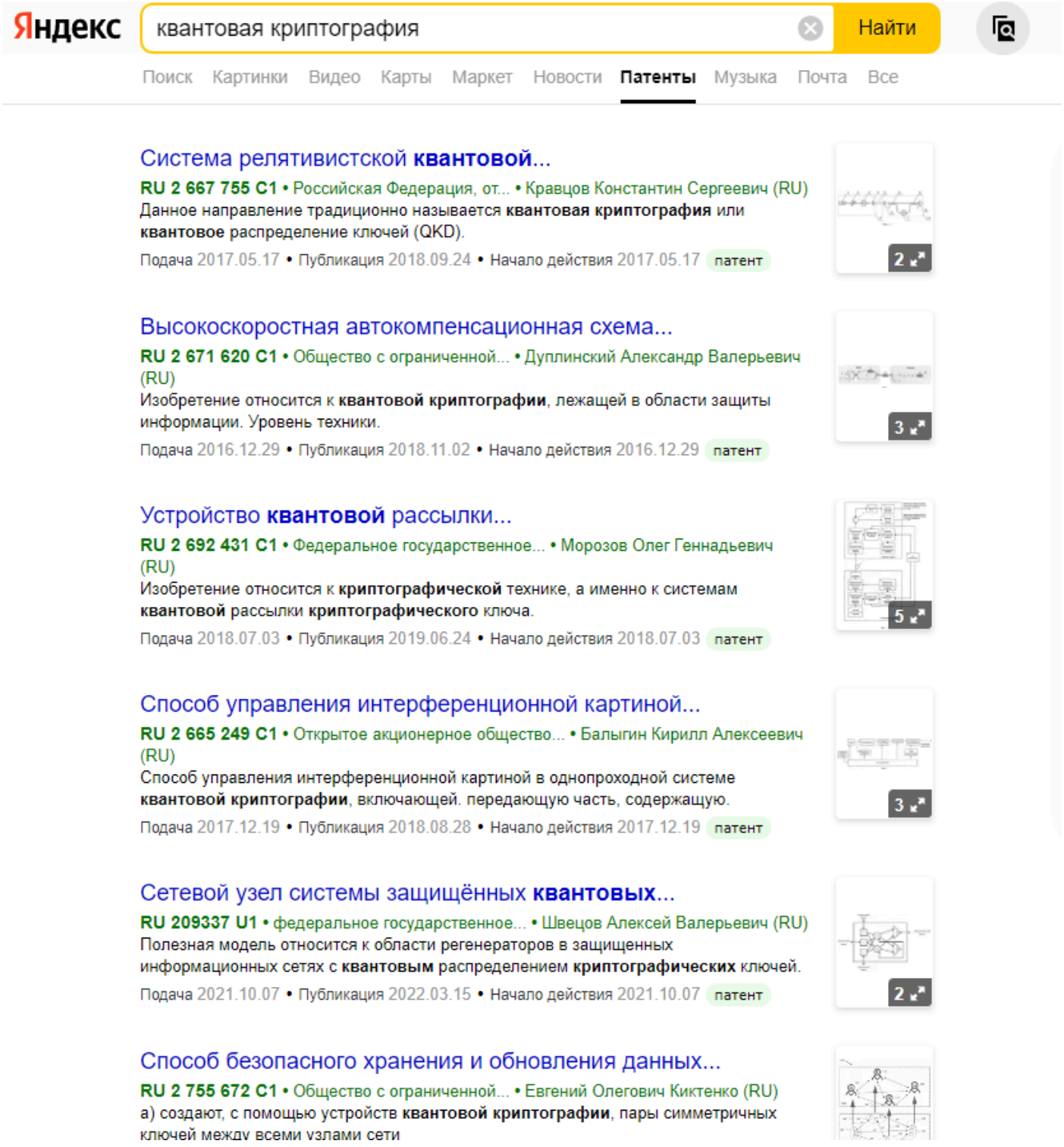
2) Е. Л. Кротова

ОБЩИЕ ПОКАЗАТЕЛИ

Название показателя	Значение
Число публикаций на elibrary.ru	104
Число публикаций в РИНЦ	83
Число публикаций, входящих в ядро РИНЦ	8
Число цитирований из публикаций на elibrary.ru	404
Число цитирований из публикаций, входящих в РИНЦ	387
Число цитирований из публикаций, входящих в ядро РИНЦ	59
Индекс Хирша по всем публикациям на elibrary.ru	7
Индекс Хирша по публикациям в РИНЦ	7
Индекс Хирша по ядру РИНЦ	2
Число публикаций, процитировавших работы автора	351
Число ссылок на самую цитируемую публикацию	152
Число публикаций автора, процитированных хотя бы один раз	35 (42,2%)
Среднее число цитирований в расчете на одну публикацию	3,93
Индекс Хирша без учета самоцитирований	7
Индекс Хирша с учетом только статей в журналах	4
Год первой публикации	1996
Число самоцитирований	35 (9,0%)
Число цитирований соавторами	100 (25,8%)
Число соавторов	307
Число статей в зарубежных журналах	3 (3,6%)
Число статей в российских журналах	57 (68,7%)
Число статей в российских журналах из перечня ВАК	47 (56,6%)
Число статей в российских переводных журналах	4 (4,8%)
Число статей в журналах с ненулевым импакт-фактором	49 (59,0%)
Число цитирований из зарубежных журналов	38 (9,8%)
Число цитирований из российских журналов	137 (35,4%)
Число цитирований из российских журналов из перечня ВАК	90 (23,3%)
Число цитирований из российских переводных журналов	3 (0,8%)
Число цитирований из журналов с ненулевым импакт-фактором	138 (35,7%)

3)МОЛОТКОВ С.И. – нет SCIENCE INDEX

Патенты на данную тему:



Вывод

Изучение данной темы важно для нашего информационного будущего, его защиты. Как мы видим данная тема с каждым годом становится актуальнее, но специалистов в этой сфере довольно мало.