Math-Net.Ru

Общероссийский математический портал

Г. В. Балакин, С. М. Буравлев, С. П. Горшков, А. М. Зубков, Г. И. Ивченко, А. В. Князев, А. П. Коваленко, О. А. Козлитин, В. А. Копытцев, А. В. Лапшин, Д. В. Матюхин, Ю. И. Медведев, В. Г. Михайлов, А. В. Михайлев, Ю. В. Нестеренко, А. Б. Пичкур, Б. А. Погорелов, В. Н. Сачков, А. В. Тарасов, И. Г. Шапошников, В. А. Шишкин, А. М. Шойтов, Памяти Игоря Александровича Круглова, *Матем. вопр. криптогр.*, 2020, том 11, выпуск 4, 5–6

DOI: <https://doi.org/10.4213/mvk336>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.172.240.79

26 апреля 2023 г., 17:37:00

Памяти Игоря Александровича Круглова 1961 – 2020

6 октября 2020 года после тяжелой болезни умер Игорь Александрович Круглов, член-корреспондент Академии криптографии Российской Федерации, профессор Института криптографии, связи и информатики, доктор физико-математических наук.

Игорь Александрович Круглов родился 31 марта 1961 года в Москве в семье военнослужащего. В 1983 году с золотой медалью окончил технический факультет Высшей школы КГБ СССР им. Ф.Э. Дзержинского, после чего связал свою жизнь с научной и преподавательской деятельностью. Прошел путь от адъюнкта до профессора кафедры.

Одним из важных научных результатов И.А. Круглова является математическое обоснование свойств схемы электронной подписи, введенной ЦБ РФ в 1993 году. Результаты данного исследования впоследствии легли в основу разработки российского стандарта электронной подписи ГОСТ Р 34.10-94 и обоснования его криптографических характеристик.

Хорошо известны результаты И.А. Круглова в области вероятностных распределений на группах и полугруппах. Это направление, находящееся на стыке алгебры и теории вероятностей, является актуальным для ряда задач в области защиты информации. И.А. Круглов продолжил исследования М.М. Глухова, Ю.А. Горчинского, Б.М. Клосса, В.Я. Козлова, В.Н. Сачкова. В частности, им доказан принцип сходимости Б.М. Клосса для произведений случайных элементов со значениями в конечных простых полугруппах в случае, когда распределения сомножителей определяются цепью Маркова.

И.А. Круглов внес значительный вклад в решение задач комбинаторного анализа, имеющих приложения в криптографии. В соавторстве с В.Н. Сачковым им были получены важные результаты о свойствах распределения весового дефицита случайных инволюций и алгоритмах построения семейств разностных инволюций. Они позволяют строить подстановки для S-боксов блочных шифров, устойчивые к дифференциальному методу криптографического анализа.

Список научных трудов И.А. Круглова насчитывает свыше 100 работ, опубликованных в "Трудах по дискретной математике", журналах "Математические вопросы криптографии", "Дискретная математика", "Фундаментальная и прикладная математика" и в других изданиях. Глубокие научные результаты И.А. Круглов получил в рамках научно-исследовательских работ Академии криптографии Российской Федерации.

Игорь Александрович был замечательным педагогом, читал лекции по алгебре, комбинаторному анализу, математической логике, дискретной математике и их приложениям в Институте криптографии, связи и информатики, разработал несколько оригинальных спецкурсов. Является автором ряда учебных пособий и монографий. Он более 20 лет исполнял обязанности ученого секретаря двух диссертационных советов. Светлая память об Игоре Александровиче Круглове навсегда сохранится в сердцах его коллег.

<i>Г.В. Балакин</i>	<i>С.М. Буравлев</i>	<i>С.П. Горшков</i>
<i>А.М. Зубков</i>	<i>Г.И. Ивченко</i>	<i>А.В. Князев</i>
<i>А.П. Коваленко</i>	<i>О.А. Козлитин</i>	<i>В.А. Копытцев</i>
<i>А.В. Лапшин</i>	<i>Д.В. Матюхин</i>	<i>Ю.И. Медведев</i>
<i>В.Г. Михайлов</i>	<i>А.В. Михалев</i>	<i>Ю.В. Нестеренко</i>
<i>А.Б. Пичкур</i>	<i>Б.А. Погорелов</i>	<i>В.Н. Сачков</i>
<i>А.В. Тарасов</i>	<i>И.Г. Шапошников</i>	<i>В.А. Шиликин</i>
<i>А.М. Шойтов</i>		