

ПРОГРАММА РАБОТЫ СЕМИНАРА НА ОСЕНЬ 2021 г.

30.09.2021

Д.С. Сафиуллин (КАИ)

СПЕЦТЕМА

11.11. 2021

В.А. Райхлин, Р.Ф. Гибадуллин, И.С. Вершинин (КАИ)

СНИЖЕНИЕ РАЗМЕРОВ НОСИТЕЛЯ СТЕГОСООБЩЕНИЙ В АССОЦИАТИВНОЙ СТЕГАНОГРАФИИ

Ассоциативная стеганография воплощает в себе своеобразный симбиоз понятий стеганографии и криптографии. Размеры носителя стегосообщений были определены ранее условием, что объем битовых вкраплений не должен превышать 1% объема носителя, что характерно для стеганографии. Соответственно предыдущие исследования проведены при размерах бинарных матриц-эталонов кодовых символов $m \times n = 119 \times 60$. В докладе рассматривается значимость так называемой полноты покрытия для стойкости ассоциативной защиты к «лобовой» атаке перебором ключей. Формулируется критерий полноты при ограничении перебора временными рамками создания базы данных сцен с ассоциативной защитой и криптоанализа сообщений. Показывается, что полнота покрытия при таком переборе может быть установлена и в случаях $n < 60$, если соответственно увеличивать его объем. Даются оценки снижения размеров носителя при выборе $n = 40$ и 30 . Устанавливается сохранение стойкости к «лобовой» атаке, стегостойкости и помехоустойчивости сокрытых сообщений при таком выборе.

25.11.2021

И.А. Казанцев, Р.К. Классен (КАИ)

CALCITE КАК КЛЮЧ К ВЫПОЛНЕНИЮ SQL-ЗАПРОСОВ В ПРОИЗВОЛЬНЫХ СРЕДАХ

Представлен обзор фреймворка с открытым кодом Apache Calcite. Показан принцип его работы и место в системах управления базами данных. Демонстрируются возможности Apache Calcite в дисциплинах разбора SQL-запросов, построения планов выполнения, оптимизации полученных планов и доступа к данным. Фреймворк Apache Calcite не предоставляет готовых решений по оптимизации плана выполнения запроса и доступа к данным. Поэтому необходима их самостоятельная разработка. Прочие модули могут быть модифицированы или разработаны самостоятельно для наиболее эффективного решения задачи. Приводятся результаты натурных экспериментов в сравнении с популярными СУБД. Обсуждаются возможности применения Apache Calcite для реализации собственного движка выполнения запросов на GPU и для реализации более эффективного (по сравнению с MySQL) движка для выполнения операций соединения.

23.12.2021

А.Х. Рахматуллин (ОАО «СЕТЕВАЯ КОМПАНИЯ»)

УСКОРЕНИЕ ПОИСКА ЭКСТРЕМУМОВ СИСТЕМ НЕРАВЕНСТВ ПОСРЕДСТВОМ РЕКУРРЕНТНЫХ НЕЙРОННЫХ СЕТЕЙ НА ПРИМЕРЕ ПОИСКА ПСП С ЗАДАННОЙ АВТОКОРРЕЛЯЦИОННОЙ ФУНКЦИЕЙ.

Рассматриваемые вопросы:

1. Ускорение дискретных численных методов решения оптимизационных задач с использованием дифференциального нейронного компьютера для поиска псевдослучайных последовательностей с заданной автокорреляционной функцией.
2. Синтез алгоритма генерации начальных значений поиска решения системы неравенств для метода имитации отжига рекуррентной нейронной сетью с выделенной памятью.
3. Практическая реализация алгоритма.
4. Тестирование и анализ полученных результатов.