ФОНД НАУЧНИ ИЗСЛЕДВАНИЯ

„КОНКУРС ЗА ФИНАНСИРАНЕ НА НАУЧНИ ИЗСЛЕДВАНИЯ – 2017 г.”

Наименование на конкурса:
Конкурс за финансиране на научни изследвания – 2017 г.
Основна научна област/тематично направление, в което проектът кандидатства:
Математически науки и информатика
Допълнителни научни области/тематични направления при интердисциплинарни проекти:
Заглавие на проекта:
Съвременни компютърни методи за изследване на комбинаторни структури осигуряващи цялостност и сигурност на информацията.
Базова организация:
Институт по математика и информатика, БАН
Партньорски организации:
Ръководител на научния колектив (академична длъжност, научна степен, име):
Проф. дмн Цонка Стефанова Байчева

Сума за изпълнение на проекта:
120 000 лева

Резюме на проекта:

Целта на проекта са изследвания на комбинаторни структури осигуряващи цялостност и сигурност на информацията. Изследването ще се основава на фундаментални математически методи, допълнени с разработването и използването на ефективни компютърни алгоритми и софтуер, за да се получат интересни нови резултати. Ще бъдат използвани съвременни компютърни подходи, за да се изследват, конструират и класифицират различни комбинаторни структури, което ще доведе до решаване на конкретни, с доказана изчислителна трудност, задачи. Изследователските задачи, върху които възнамеряваме да работим в рамките на този проект, се основават на изследвания на класически комбинаторни структури, които имат директни приложения в кодирането и криптологията, а именно разностни множества, булеви функции, графи, декомпозиционни функции и др. Планираме да подобрим вече съществуващи методи и да предложим нови, като приложим интердисциплинарен подход и използваме резултати от различни области на математиката като алгебра, теория на числата, комбинаторика, теория на кодирането и теория на вероятностите в комбинация с ефиктивни съвременни алгоритми като евристично търсене чрез еволюционни алгоритми. Получените резултати от класификацията на изследваните комбинаторни структури ще доведат до конструирането на нови редици с добри корелационни свойства, кодове за асинхронна комуникация и субституционни кутии с добри криптографски свойства. Натрупаният опит в разработването на методи и алгоритми за изследване на комбинаторни обекти ще бъде използван за създаване на методи и инструменти за криптоанализ на криптографски алгоритми и протоколи. Тези методи и инструменти ще бъдат приложени за криптоанализ на конкретни алгоритми и протоколи като, например, протокол за биометрични данни.

Научният екип на проекта се състои от утвърдени експерти с множество публикации в горепосочените области, както и от докторанти. Екипът включва изследователи от Института по математика и информатика, БАН, KU Leuven, Белгия, Държавна агенция национална сигурност и Великотърновския университет. Предимството на научния екип е, че неговите членове вече са работили заедно в предишни проекти (включително проект финансиран от ФНИ) и имат съвместни публикации. Това е доказателство за способността им да получат нови научни резултати в темите на проекта. По време на предишното ни сътрудничество постигнахме значителен напредък както в теоретичните изследвания, така и в конкретни практически приложения. Въз основа на гореизложеното, сме уверени, че екипът на проекта има необходимия опит и силна мотивация, за да гарантира успешното изпълнение на проекта.

Разпределение на сумата по проекта между базовата организация и партньорите

Организация:

Институт по математика и информатика, БАН

Сума: 120 000 лева

Обща сума за изпълнение на проекта:

120 000 лева

Членове на научния колектив

Организации/участници[1]	***Бележка***[2]
Базова организация:	
Институт по математика и информатика, БАН	
Ръководител на научния колектив	
Проф. дмн Цонка Стефанова Байчева	
Участници:	
Мирослав Маринов Димитров	ДО ИМИ, ДАНС
Д-р Светла Йорданова Никова	УЧ, КУ Льовен
Д-р Николай Русев Николов	ДАНС
Д-р Георги Велков Иванов	ДАНС
Виолета Андреева Дъчева	ДАНС
Любомир Георгиев Филипов	ДО ВТУ