ФОНД НАУЧНИ ИЗСЛЕДВАНИЯ
Министерство на образованието и науката

# Информация за изпълнение на етап на проект

| |
|---|
| ***Наименование на конкурса:*** |
| *Конкурс за финансиране на научни изследвания – 2017 г.* |
| ***Основна научна област:*** |
| *Математически науки и информатика* |
| ***№ на договор:*** |
| *ДН 12/8 от 15.12.2017* |
| ***Начална и крайна дата на проекта:*** |
| *15.12.2017 – 15.12.2020* |
| ***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* |
| ***Общ размер на отпуснатото финансиране за първи етап:*** |
| *54000* |
| ***Интернет страница на проекта (ако има такава):*** |
| |
| ***Научни публикации по проекта:*** |
| **1. T. Baicheva** and S. Topalova, On Tight Optimal Conflict-avoiding Codes for 3, 4, 5 and 6 Active Users, *Cybernetics and Information Technologies*, Institute of Information and Communication Technologies - BAS, vol. 18, no. 5, pp. 5-11, 2018. **SJR: 0.203** **https://content.sciendo.com/view/journals/cait/18/5/article-p5.xml** |
| **2. T. Baicheva** and S. Topalova, Classification of strongly conflict-avoiding codes, *IEEE Communications Letters*, vol. 22, issue 12, pp. 2415 - 2418, 2018. **ISI IF: 2.723** **https://ieeexplore.ieee.org/document/8488490** |
| **3. T. Baicheva** and S. Topalova, Classification of optimal (v, k, 1) binary cyclically permutable constant weight codes with k=5, 6 and 7 and small lengths, *Designs, Codes and Cryptography*, vol. 87 (2-3), pp. 365-374, 2019. **ISI IF: 1.114** **https://link.springer.com/article/10.1007/s10623-018-0534-x** |
| **4. T. Baicheva**, **V. Dutcheva** and **N. Nikolov**, Simulation model for the investigation of the efficiency of an artificial immune algorithm for generation of S-boxes with good cryptographic |

| |
|---|
| properties, **presented** at *13th Annual Meeting of the Bulgarian Section of SIAM,* December 18 - 20, 2018, Sofia, Bulgaria, **to appear** in *Studies in Computational Intelligence*. **SJR (2018): 0.18** |
| **5.** P. Çomak, **S. Nikova** and V. Rijmen, On decomposition of permutations, **presented** at *BalkanCryptSec,* Iasi, Romania, September 20-21, 2018, **to appear** in *Communications in Computer and Information Science*. **SJR (2018): 0.17** |
| **6. T. Baicheva** and S. Topalova, On the diffusion property of the Improved Generalized Feistel with different permutations for each round, **presented** at *8th International Conference on Algebraic Informatics*, Niš, Serbia, June 30 – July 4, 2019, **to appear** in *Lecture Notes in Computer Science 11545*, **SJR (2018): 0.28** https://www.springer.com/gp/book/9783030213626 |
| **7. T. Baicheva** and P. Kazakov, CRC selection for decoding of CRC-polar concatenated codes, **will be presented** at *9th Balkan Conference in Informatics*, September 26-28, 2019, Sofia, Bulgaria, to **appear** in *ACM ICPS Proceedings*. **SJR (2018): 0.17** |
| **8.** V. Arribas , B. Bilgin, G. Petrides, **S. Nikova**, V. Rijmen, Rhythmic Keccak: SCA Security and Low Latency in HW, **presented** at *Conference on Cryptographic Hardware and Embedded Systems*, Amsterdam, The Netherlands, September 9–12, 2018, **available** at *Cryptology ePrint Archive*: Report 1193, https://eprint.iacr.org/2017/1193 |
| **9.** S. Dhooghe and **S. Nikova**, My Gadget Just Cares For Me - How NINA Can Prove Security Against Combined Attacks, **available** at *Cryptology ePrint Archive*: Report 2019/615, https://eprint.iacr.org/2019/615 |
| **10. M. Dimitrov**, **T. Baicheva** and **G. Ivanov**, Implementation of RSA attack using 2-dimensional lattices by constructing hypotheses of keys with low Hamming weight, **presented** at *Training School on Cryptanalysis of Ubiquitous Computing Systems*, 16-20 April 2018, Azores, Portugal , *EXTENDED ABSTRACTS, Paper 21* https://www.cryptacus.eu/en/events/training-school-2018/pitches-and-posters/ |
| **11. M. Dimitrov**, **T. Baicheva** and B. Esslinger, Efficient generation of cryptographically strong S-boxes with high nonlinearity, **submitted** to *Cryptography and Communications*. **ISI IF: 1.213** |

***Описание на очакваните резултати по проекта (до 1 стр. в рамките на полето по-долу):***

Очакваните резултати от този проект са свързани с конкретните цели, които той си поставя, а именно:

- Ще бъдат разработени нови методи за изучаване на разностни множества и свързаните с тях редици с добри корелационни свойства и кодове за асинхронно предаване; булеви функции като градивни елементи на субституционни кутии; графи, матрици и декомпозиционни функции за създаване на сигурни криптографски алгоритми и протоколи. Тези методи ще използват и комбинират резултатите и подходите от различни области на чистата или приложната математика и могат да бъдат приложени за по-нататъшни изследвания на изучаваните в проекта комбинаторни структури, както и на други, свързани с тях, структури.
- Ще бъдат конструирани и класифицирани нови редици с добри корелациионни свойства, оптимални кодове за асинхронно предаване, субституционни кутии с добри криптографски свойства и ще бъдат предоставени за ползване от всеки, който се интересува от тях. По този начин крайните потребители ще имат директен достъп до обектите, без да е необходимо да прилагат сложни конструктивни методи, използващи тежки математически апарати.
- Ще бъдат разработени нови алгоритми и техни имплентации като компютърни програми, които ще бъдат използвани за решаването на задачите, поставени в рамките на настоящия проект. Тези алгоритми ще бъдат публикувани и на свой ред могат да бъдат използвани от всеки, който се интересува от решаването на подобни задачи.
- Разработеният инструментариум за апостериорен автоматичен криптоанализ на публични ключове генерирани с RSA и на RSA съобщения и библиотеката за тестове на протоколи, изискващи ОТ, ще бъдат достъпни за всички, заинтересовани от тематиката. Те могат да бъдат използвани в научните изследвания на други изследователи, работещи в областта на криптологията.

## 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<br>Д-р Светла Йорданова Никова<br>Д-р Николай Русев Николов<br>Д-р Георги Велков Иванов<br>Виолета Андреева Дъчева<br>Любомир Георгиев Филипов | ДО ИМИ, ДАНС<br>УЧ, КУ Льовен<br>ДАНС<br>ДАНС<br>ДАНС<br>ДО ВТУ |
| ***Партньорска организация:*** | |
| | |
| ***Участници:*** | |
| | |
| ***Партньорска организация:*** | |
| | |
| ***Участници:*** | |
| | |

[1] Отбележете академичната длъжност, научната степен, име и фамилия на всеки участник като включите и участниците, които са работили по проекта не през целия период за изпълнение на проекта

[2] Отбележете дали участникът в колектива е млад учен (МУ), постдокторант (ПД), докторанти (ДО) или студенти (СТ), или учен от чужбина (УЧ).

***Постигнати резултати от изпълнението на проекта и кратък анализ на тяхната приложимост (до 1 стр. в рамките на полето по-долу)***

**Резултати:**

- Класифицирани са оптимални плътни избягващи конфликти кодове (tCAC) с тегла 3, 4, 5 и 6 и оптимални силни избягващи конфликти кодове (SCAC) с тегла 3, 4 и 5 и с малки дължини. Разработените класификационни алгоритми позволиха да се класифицират кодове, за които до момента не съществуваха резултати.
- Класифицирани са оптимални двоични (v,k,1) циклично-пермутационни константно тегловни кодове (CPCW) за малки v и k=5, 6 и 7. Чрез прилагане на каскадни конструкции от тези кодове могат да се получат нови с по-големи дължини. Показано е несъществуването на (127,7,1) циклично разностно множество.
- Определени са най-добрите по отношение на контрол на грешки за всяка дължина, до която могат да бъдат използвани, скъсени циклични кодове (CRC) имащи от 11 до 19 проверочни бита. Изследването показва, че има по-добри кодове от тези предложени за разработвания 5G стандарт.
- Създаден е симулационен модел за оценка на поведението и коректността на изкуствен имунен алгоритъм за генериране на субституционни кутии с добри криптографски свойства и са конструирани такива с минимален брой спектрални Уолш коефициенти с максимална абсолютна стойност.
- Показано е кога една пермутация над $F_2^n$ може да се разложи на пермутации от втора и/или трета степен за всяко $3 \leq n \leq 31$.
- Намерени са последователности от различни пермутации за блокови шифри от тип Feistel с 10, 12, 14 и 16 подблока, които осигуряват по-добра дифузия в сравнение с тези, които използват една и съща пермутация на всички рундове.
- Предложени са изисквания (Non-Interference, Non-Accumulation – NINA), които да позволяват да се оцени сигурността на криптографски алгоритъм срещу комбинирани диференциален анализ на консумацията и диференциален анализ на дефектите атаки.
- Представена е атака на RSA криптосистемата, която използва двумерна решетка и предположението, че достатъчно дълга последователност от двоичното представяне на частаната експонента има малко тегло по Хеминг.

**Приложения:**

- CAC и CPCW кодовете се използват за разпределяне на трафика между потребителите на асинхронни комуникационни канали с множествен достъп без обратна връзка.
- Предложените CRC кодове могат да бъдат използвани във всяка кодова схема с променлива дължина на информационния блок.
- Субституционните кутии са основен градивен елемент на блоковите шифри като маскират връзката между ключа и шифрования текст.
- Пермутациите, които имат квадратично разлагане позволяват ефективно, по отношение на нужния ресурс, имплементиране на маскиране срещу side-channel криптографски атаки.
- Последователностите от пермутации с оптимална дифузия се използват за изграждане на блокови шифри от тип Feistel, които имат висока устойчивост срещу .
- Предложената атака на RSA криптосистемата е използвана за реконструиране на частен ключ само като е известно, че частната експонента е с дължина 400 бита и теглото по Хеминг на първите 310 бита е 4.