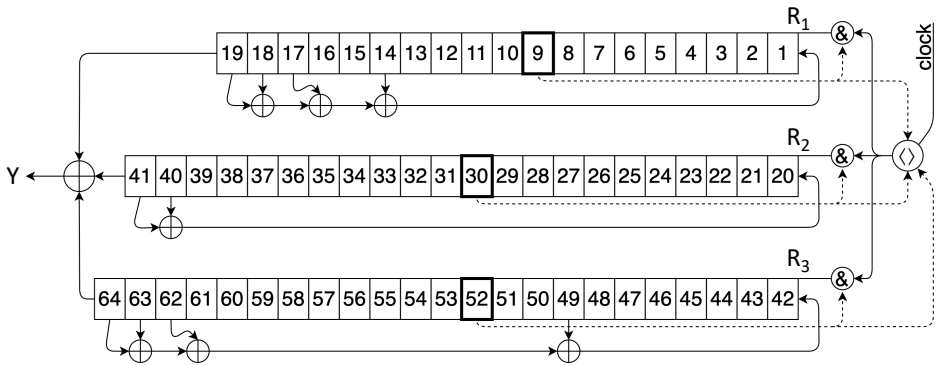
УНИВЕРСИТЕТ ИТМО

Разработка эволюционных методов декомпозиции задач обращения криптографических функций с использованием статистических тестов и инкрементальных SAT-решателей

Павленко Артём, M42391
Научный руководитель: Ульянцев В.И., к.т.н., доцент ФИТиП

Криптографические алгоритмы и криптоанализ

Алгоритм A5/1
(технология 2G)



$X = R_1 \cup R_2 \cup R_3$

$X = \{x_1, x_2, \ldots, x_{64}\}$ – секретный ключ

$Y = \{y_1, y_2, \ldots, y_{128}\}$ – ключевой поток

$$f_{A5/1}: \{0,1\}^{64} \rightarrow \{0,1\}^{128}$$

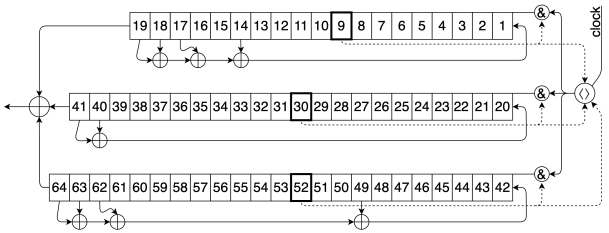
$$f_{A5/1}(x) = y$$

Задача **криптоанализа**:
зная y, найти x

$$f_{A5/1}^{-1}(x) = y$$

Сведение к SAT с помощью Transalg*

Алгоритм A5/1



$X = R_1 \cup R_2 \cup R_3$

$X = \{x_1, x_2, \ldots, x_{64}\}$

$Y = \{y_1, y_2, \ldots, y_{128}\}$

вручную ⇒

Программа для Transalg

```
__in bit XA[19];
__in bit XB[22];
__in bit XC[23];
__out bit Y[128];

bit shift_rslosA() {
  bit x0 = XA[18]^XA[17]^XA[16]^XA[13];
  for(int j = 18; j > 0; j=j-1) {
    XA[j] = XA[j-1];
  }
  XA[0] = x0;
}
...

bit majority(bit A, bit B, bit C) {
    return A&B|A&C|B&C;
}

void main() {
  int b1 = 8;
  int b2 = 10;
  int b3 = 10;
  bit maj;
  for(int i = 0; i < 128; i=i+1) {
    maj = majority(XA[b1], XB[b2], XC[b3]);
    if(!(maj^XA[b1])) shift_rslosA();
    if(!(maj^XB[b2])) shift_rslosB();
    if(!(maj^XC[b3])) shift_rslosC();
    Y[i] = XA[18]^XB[21]^XC[22];
  }
}
```

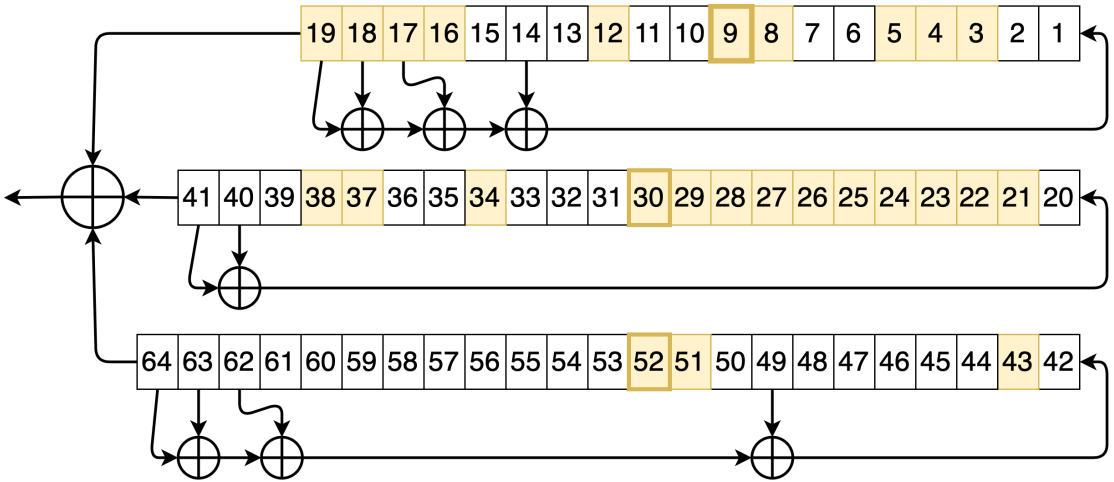
автоматически ⇒

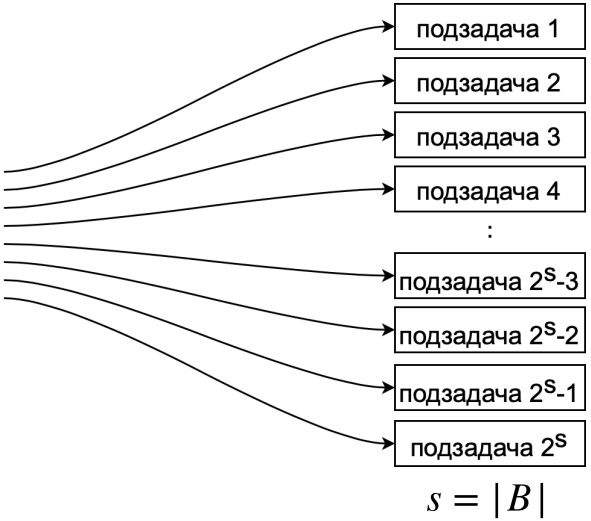
SAT-формула

```
p cnf 8425 38262
c input variables 64
c literals count 128374
65 9 30 0
65 9 52 0
-65 9 -30 -52 0
65 -9 -52 0
-65 -9 30 52 0
65 -9 -30 0
66 -19 65 0
66 -18 -65 0
-66 19 65 0
-66 18 -65 0
67 -18 65 0
67 -17 -65 0
-67 18 65 0
-67 17 -65 0
68 -17 65 0
68 -16 -65 0
-68 17 65 0
-68 16 -65 0
69 -16 65 0
69 -15 -65 0
-69 16 65 0
... ...
38264 -8425 -8293 8295 -8297 0
38265 -8425 -8293 -8295 8297 0
```

*Transalg: [Otpuschennikov, I., Semenov, A., Gribanova, I., Zaikin, O., Kochemazov, S.: Encoding Cryptographic Functions to SAT Using TRANSALG System. In: ECAI 2016. FAIA, vol. 285, pp. 1594–1595 (2016)]

Декомпозиция. Guess-and-determine атака



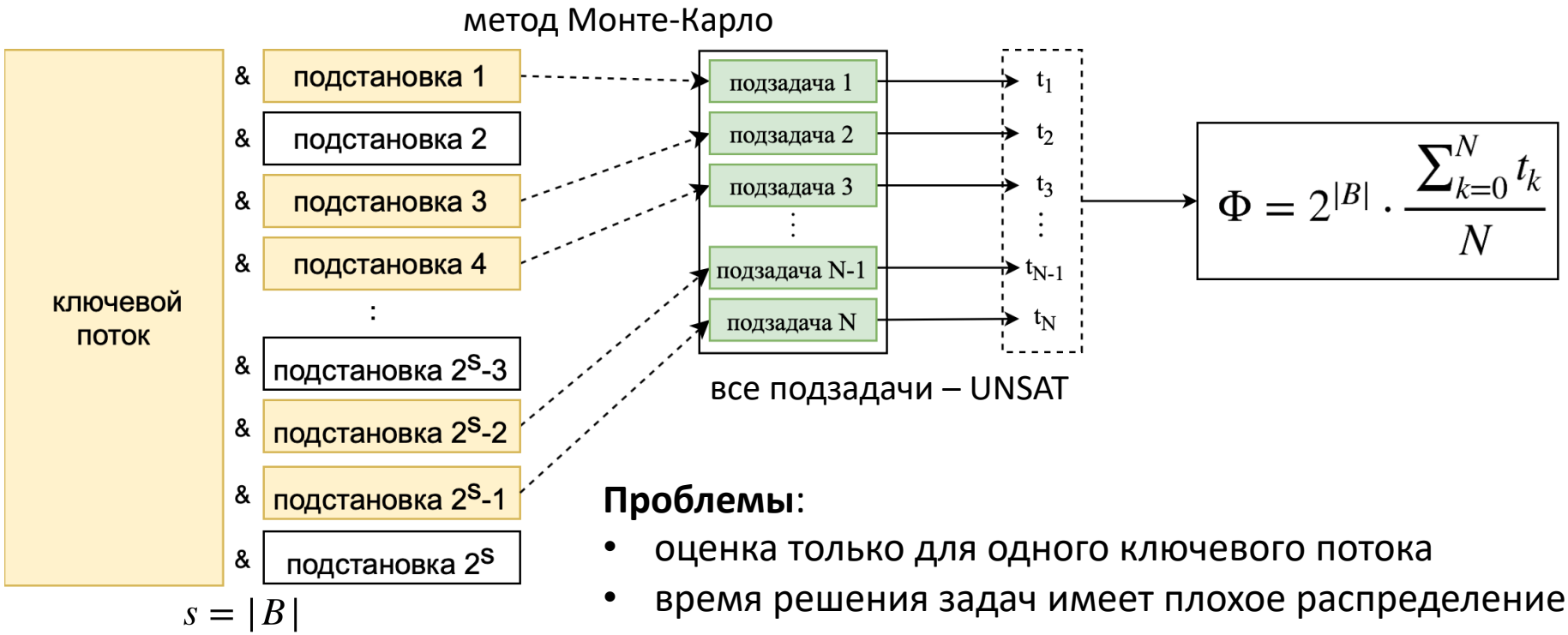


$s = |B|$

$$B = \{ x_3, x_4, x_5, x_8, x_9, x_{12}, x_{16}, x_{17}, x_{18}, x_{19}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{34}, x_{37}, x_{38}, x_{43}, x_{51}, x_{52} \}$$

$$\sum_{i=1}^{2^s} t_i \ll T_{BruteForce},$$

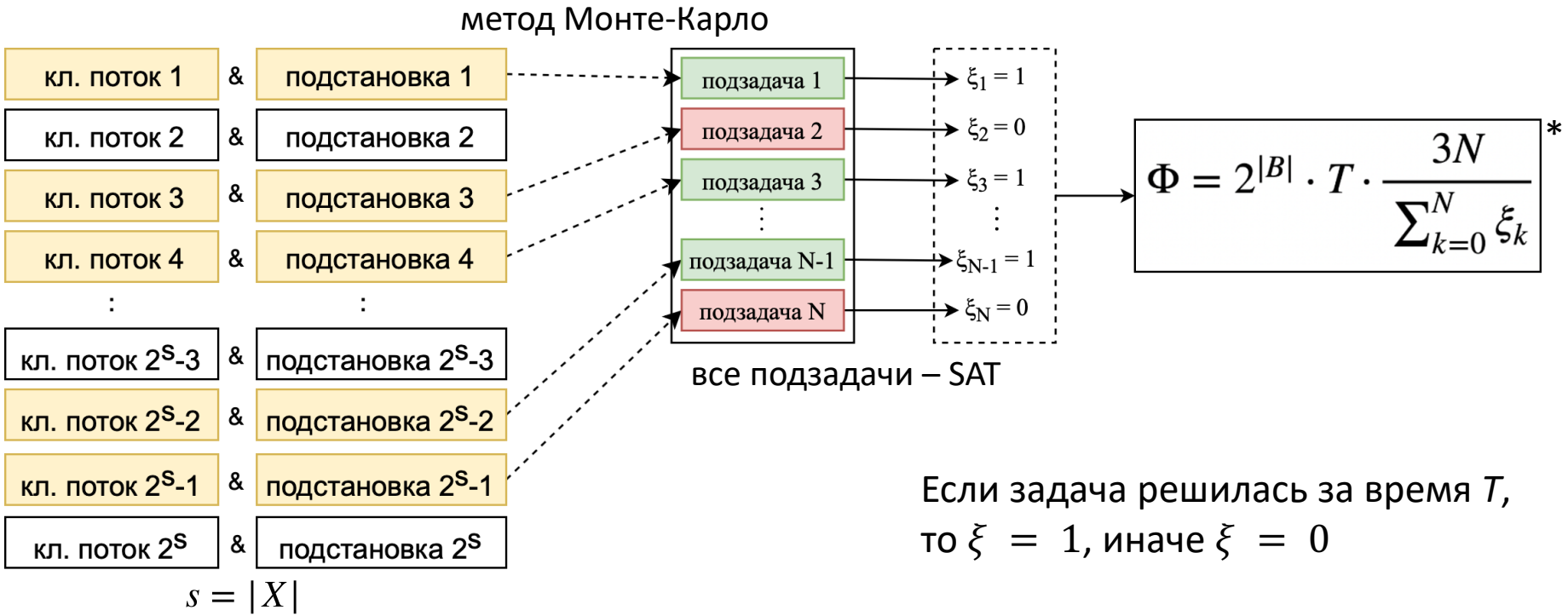
Оценивание декомпозиции. UNSAT-иммунность



Проблемы:

- оценка только для одного ключевого потока
- время решения задач имеет плохое распределение

Оценивание декомпозиции. SAT-иммунность



Если задача решилась за время T, то $\xi = 1$, иначе $\xi = 0$

*IBS resistant function: [*Semenov A., Zaikin O., Otpuschennikov I., Kochemazov S., Ignatiev A.* On cryptographic attacks using backdoors for SAT // The Thirty-Second AAAI Conference on Artificial Intelligence. – IEEE, 2018. – P. 6641-6648]

Автоматизированные методы декомпозиции

1. Поиск с запретами (Tabu search)
2. Имитация отжига (Simulated annealing)
3. GBFS (Greedy best-first search)

1 & 2: [*Semenov A., Zaikin O.* Algorithm for finding partitionings of hard variants of boolean satisfiability problem with application to inversion of some crypto- graphic functions // SpringerPlus. — 2016. — Vol. 5, no. 1. — P. 554.]
1 & 2: [*Semenov A., Zaikin O., Otpuschennikov I., Kochemazov S., Ignatiev A.* On cryptographic attacks using backdoors for SAT // The Thirty-Second AAAI Conference on Artificial Intelligence. – IEEE, 2018. – P. 6641-6648.]
3: [*Zaikin O., Kochemazov S.* Pseudo-boolean black-box optimization methods in the context of divide-and-conquer approach to solving hard SAT instances // DEStech Transactions on Computer Science and Engineering. — 2018. — Optim.]

Актуальность

Информационная безопасность

- Криптографические методы для её обеспечения
- Обоснование **криптостойкости** используемых алгоритмов шифрования, посредством построения **криптографических атак**

Построение криптографических атак – **трудоемкая** задача

Большинство известных криптографических атак – **аналитические**

Автоматизированные методы позволяют **относительно быстро** получить первоначальную оценку криптостойкости алгоритма

Цель и задачи работы

Цель: Разработать новые методы автоматизированного построения декомпозиционных множеств для криптографических алгоритмов

Задачи:

- Применить эволюционные алгоритмы для построения декомпозиционных множеств
- Применить статистические тесты к вычислению функции приспособленности
- Использовать инкрементальное решение задач в процессе вычисления функции приспособленности.

Эволюционные алгоритмы

- Эволюционная Стратегия (1+1)
- Генетический алгоритм: Элитизм

Особь: декомпозиционное множество B
Функция приспособленности: для исследования SAT-иммунности

Сравнение особей

Выборка из N задач обращения криптографических функций, ослабленных оцениваемой декомпозицией *B*, которые делятся на 2 типа:

- Задача *i* была решена за время $t_i < T$
- Задача *i* не была решена за время *T*

Пусть было решено N_+ задач, тогда время на проведение атаки для *B* можно оценить следующей формулой: (функция приспособленности)

$$\Phi(\chi_B) = \frac{\sum_{i=1}^{N_+} t_i}{N_+} + \left(\frac{N}{N_+} - \frac{1}{2} \right) \cdot (2^{|B|} \cdot T)$$

Сравнение особей: Статистические тесты

Идея: Будем адаптивно подбирать размер выборки *N* **в процессе сравнения**
Нулевая гипотеза: Выборки не различаются

Пусть N_{max} – максимальный размер выборки, Q – шаг выборки

Процесс сравнения:

1. Решаем Q задач из выборки
2. Проводим статистическое тестирование двух особей
3. Пока статистический тест не различает особи наращиваем выборку с шагом Q не превышая N_{max}
4. Вычисляем значения приспособленности и выбираем лучшую особь

Выбор параметров

Самый лучший выбор значения для *Q*: *Q = 1*

Однако тогда эффективная реализация возможна только в однопоточном режиме

Для выбранных алгоритмов зададим следующие параметры:

- Эволюционная стратегия (1+1). $N_{max} = 500$. *Q = 50*
- Генетический алгоритм: Элитизм. $N_{max} = 500$. *Q = 100*

Выбор статистического теста

Накладываемые **ограничения**:

- Измерения ограничены сверху величиной *T*
- Измерения не подчиняются нормальному распределению

Был выбран: **U-критерий Манна-Уитни**

Также для сравнения тестов был выбран: **тест Барнарда**

Сравнение статистических тестов

Алгоритм	Разрешающая способность U-критерия Манна-Уитни		Разрешающая способность теста Барнарда	
	Число исходов	Доля исходов, %	Число исходов	Доля исходов, %
A5/1	**1397**	**18.99**	1328	18.06
Bivium	**13167**	**72.80**	10327	57.10
Trivium 64	**7894**	**46.63**	6511	38.46
Trivium 96	**4060**	**32.56**	3640	29.19

Для каждого криптографического алгоритма было сделано 5 независимых запусков генетического алгоритма

Число просмотренных точек

Алгоритм	Число точек		
	Со статистическим тестом	Без статистического теста	Во сколько раз больше
A5/1	**1471**	341	x4.31
Bivium	**3616**	2439	x1.48
Trivium 64	**3398**	1323	x2.57
Trivium 96	**2494**	1299	x1.92

На основе одного запуска для каждой комбинации криптографического алгоритма и метода

Инкрементальная функция приспособленности

В процессе вычисления:

- Инициализируется SAT-решатель на общей для всех подзадач формуле
- Каждая задача решается с соответствующей подстановкой значений в виде допущений

Таким образом SAT-решатель запоминает информацию о решенных подзадачах и использует её при решении последующих

В результате:

+ Снижение временных затрат на вычисление функции приспособленности
– Снижение эффективности построенных декомпозиционных множеств

Сравнение декомпозиционных множеств

Алгоритм	Статистические тесты		Адаптивная стратегия*	
	|B|	Оценка, сек	|B|	Оценка, сек
ASG 72	10	**4794.55**	9	5604.8
ASG 96	19	**1.56e+06**	16	3.72e+06
Bivium	27	**7.49e+11**	39	1.49e+12
Trivium 64	17	**2.03e+07**	21	3.17e+07
Trivium 96	35	**1.24e+12**	40	2.09e+12

*Adaptive strategy: [Pavlenko A.L., Semenov A., Ulyantsev V. Evolutionary Computation Techniques for Constructing SAT-Based Attacks in Algebraic Cryptanalysis//Lecture Notes in Computer Science, 2019, Vol. 11454, pp. 237-253]

Сравнение с другими автоматизированными методами

Работа*	Работа**	Работа***
A5/1	ASG 72	Trivium
Bivium	ASG 96	Mickey
Grain v0	ASG 192	Grain v1

В приведенных работах проводилось исследование UNSAT-иммунности

*: [*Semenov A., Zaikin O.* Algorithm for finding partitionings of hard variants of boolean satisfiability problem with application to inversion of some crypto- graphic functions // SpringerPlus. — 2016. — Vol. 5, no. 1. — P. 554.]

**: [*Zaikin O., Kochemazov S.* An improved SAT-based guess-and-determine attack on the alternating step generator // International Conference on Information Security. — Springer. 2017. — P. 21–38.]

***: [*Zaikin O., Kochemazov S.* Pseudo-boolean black-box optimization methods in the context of divide-and-conquer approach to solving hard SAT instances // DEStech Transactions on Computer Science and Engineering. — 2018. — Optim.]

Атака на Alternating Step Generator (ASG 72)

Полученная оценка: 4794.55 сек. Конкуренты: 1116 сек.

Число атак	Ограничение времени, сек.	Успешные атаки, %	Усредненное время, сек.	Отклонение времени, сек.
1000	1.0	64.8	1039.24	17.43
1000	2.0	100	1081.32	492.72
1000	3.0	100	1592.62	281.56
10000	**2.0**	**100**	**1084.26**	**486.00**

Из расчета на одно ядро процессора Intel®Xeon®E5-2695 v4

Заключение

- Разработаны эволюционные методы построения декомпозиционных множеств для криптографических алгоритмов с применением статистических тестов
- Разработанная функция приспособленности на основе статистических тестов может быть использована с любым другим алгоритмом оптимизации, а также для любой другой задачи использующей метод Монте-Карло для оценивания особей
- Были построены новые декомпозиционные множества для ряда криптографических алгоритмов
- Благодарность Александру Семенову и Максиму Буздалову за коллаборацию

Публикации и выступления

- Pavlenko A., Buzdalov M., Ulyantsev V. Fitness Comparison by Statistical Testing in Construction of SAT-Based Guess-and-Determine Cryptographic Attacks//GECCO 2019 - Proceedings of the 2019 Genetic and Evolutionary Computation Conference Companion. — 2019. — P. 312-320
- Pavlenko A., Semenov A., Ulyantsev V.I., Zaikin O. Parallel Framework for Evolutionary Black-box Optimization with Application to Algebraic Cryptanalysis//42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). — 2019. — P. 1144-1149
- *Павленко А., Ульянцев В.* Применимость статистических тестов к эволюционным методам декомпозиции экземпляров задачи о булевой выполнимости для криптоанализа генераторов ключевого потока. — 2019. — VIII Конгресс молодых ученых.
- *Павленко А., Ульянцев В.* Эволюционные алгоритмы построения декомпозиционных множеств для трудных вариантов задач о булевой выполнимости, позволяющих достичь сверхлинейного ускорения при решении. — 2020. — IX Конгресс молодых ученых.

Спасибо за внимание!

alpavlenko@itmo.ru

ITMO more than a UNIVERSITY