Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики

Эволюционные алгоритмы для криптоанализа генераторов ключевого потока с использованием программных средств решения задачи выполнимости

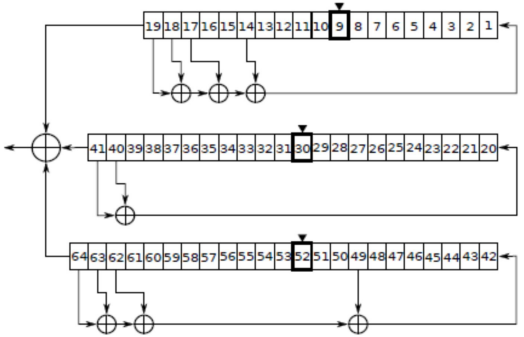
Автор: Павленко А.Л.
Научный руководитель: Ульянцев В.И.
Научный консультант: Семенов А.А.

Введение. Криптографические генераторы

Потоковые шифры, типовая схема

F – нелинейная функция

Шифр A5/1



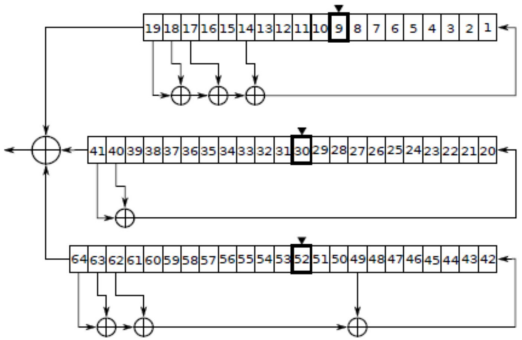
χ_j – функция сдвига

j – номер регистра

χ_j: $b_j \equiv majority(b_1, b_2, b_3)$

Введение. Сведение к SAT с помощью Transalg

Шифр A5/1



χ_j – функция сдвига

j – номер регистра

χ_j: $b_j \equiv majority(b_1, b_2, b_3)$

TA-программа

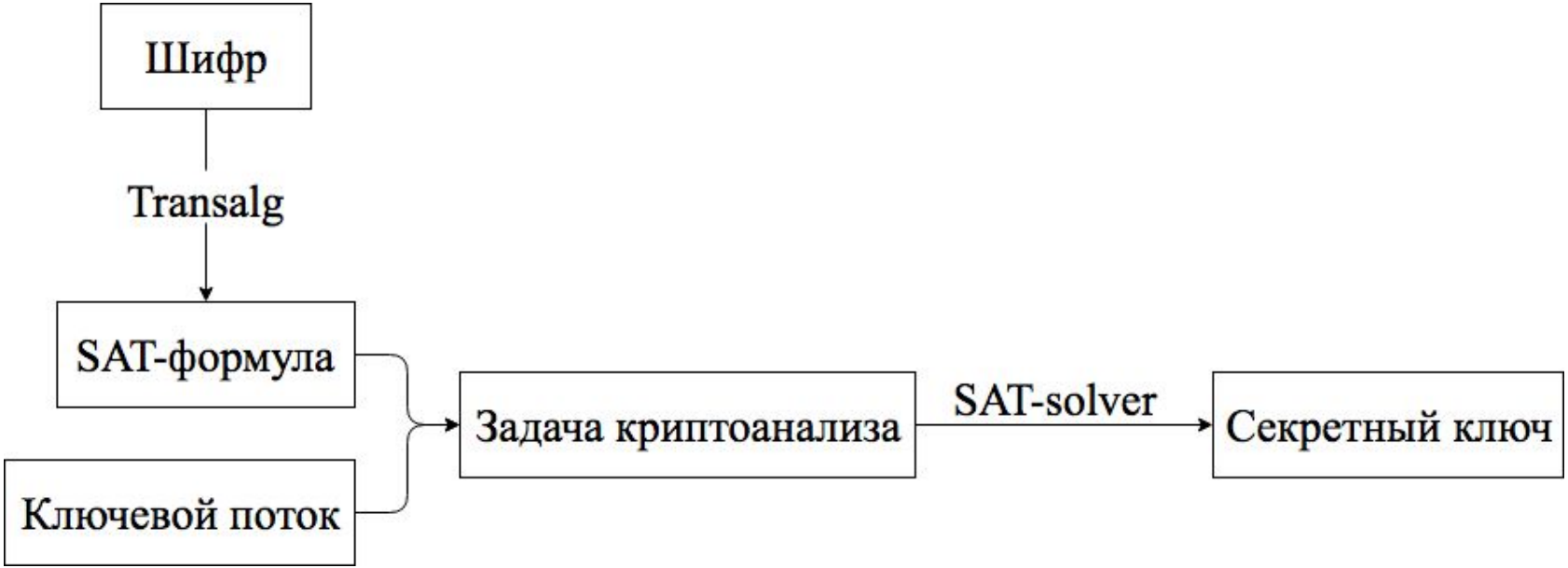
```
__in bit regB[22];
__in bit regC[23];
__out bit result[len];

bit shift_rslosA() {
  bit x = regA[18];
  bit y = regA[18]^regA[17]^regA[16]^regA[13];
  for(int j = 18; j > 0; j=j-1) {
    regA[j] = regA[j-1];
  }
  regA[0] = y;
  return x;
}
...

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

void main() {
  int midA = 8;
  int midB = 10;
  int midC = 10;
  bit maj;
  for(int i = 0; i < len; i= i + 1) {
    maj = majority(regA[midA],regB[midB],regC[midC]);
    if(!(maj^regA[midA])) shift_rslosA();
    if(!(maj^regB[midB])) shift_rslosB();
    if(!(maj^regC[midC])) shift_rslosC();
    result[i] = regA[18]^regB[21]^regC[22];
  }
}
```

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
-69 15 -65 0
70 -15 65 0
70 -14 -65 0
-70 15 65 0
-70 14 -65 0
71 -14 65 0
71 -13 -65 0
-71 14 65 0
-71 13 -65 0
```

Transalg: [*Отпущенников И. В., Семенов А. А.* Технология трансляции комбинаторных проблем в SAT // Прикладная дискретная математика. – 2011. – Т. 11. – No. 1. – С. 96-115]

Введение. SAT-based криптоанализ



Введение. Пример взлома криптоалгоритмов

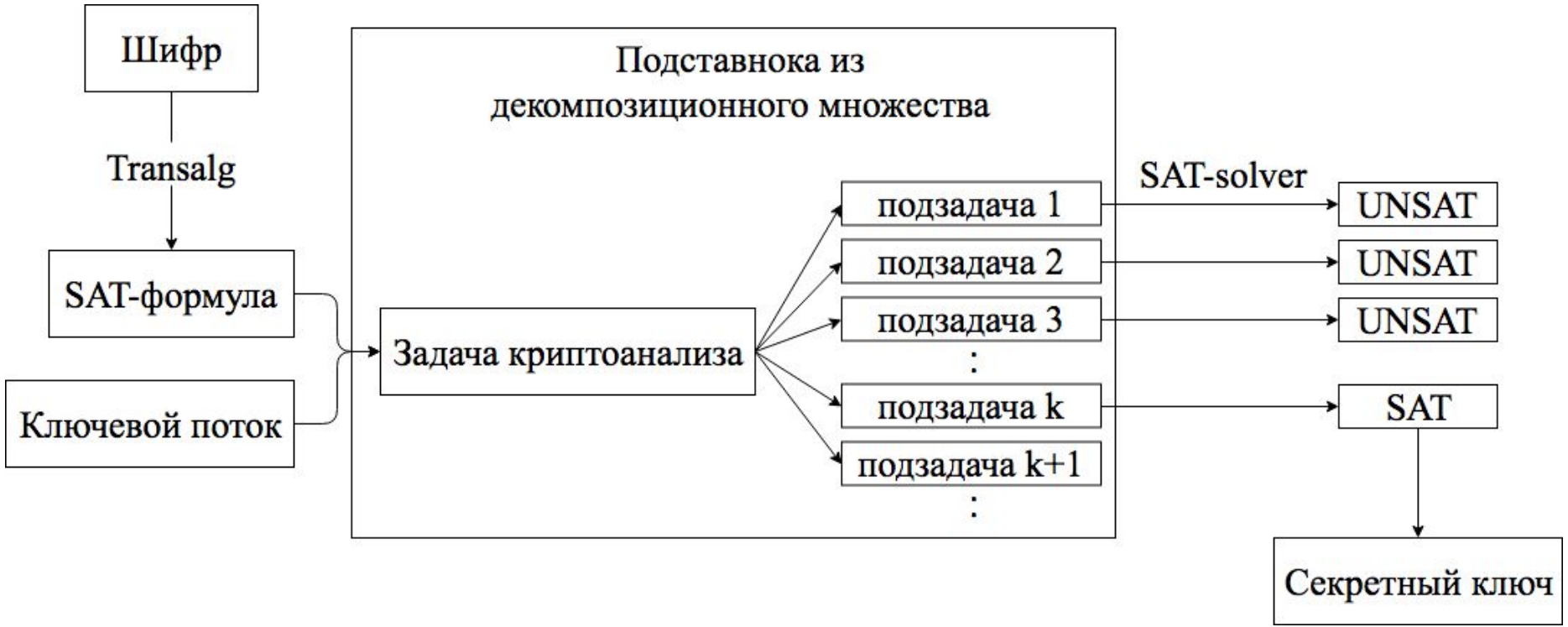
CPU: 2 core i5-6267U @ 2,9 GHz			
	Treengeling	PLingeling	Guess-and-determine атака
Volfram (128)	7м 13с	5м 50с	-
Geffe (64)	0.51с	0.38с	-

CPU: 32 core AMD Opteron 6378 @ 2.4 GHz			
	Treengeling	PLingeling	Guess-and-determine атака
Volfram (128)	6м 51с	4м 30с	-
Geffe (64)	0.53с	0.88с	-

Введение. Пример взлома криптоалгоритма

CPU: 32 core AMD Opteron 6276 @ 2.3 GHz			
Криптографический алгоритм: Trivium-64			
Ограничение по времени: 7 дней			
	PLingeling	Treengeling	Guess-and-determine атака
задача 1	прервано	прервано	2д 6ч
задача 2	прервано	3д 2ч	3д 19ч
задача 3	прервано	4д 10ч	15ч
задача 4	прервано	прервано	1д 21ч
задача 5	прервано	прервано	4д 3ч

Введение. Guess-and-determine атака



Цель

- Разработать и реализовать новые автоматизированные методы построения декомпозиционных представлений трудных вариантов задачи о булевой выполнимости и применить эти методы для построения атак на ряд криптографических генераторов ключевого потока

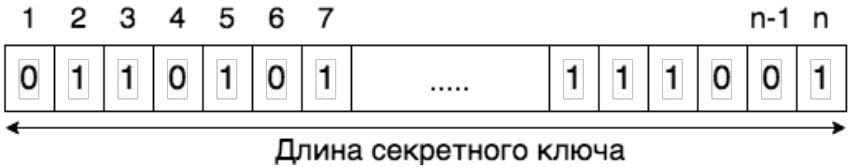
Задачи

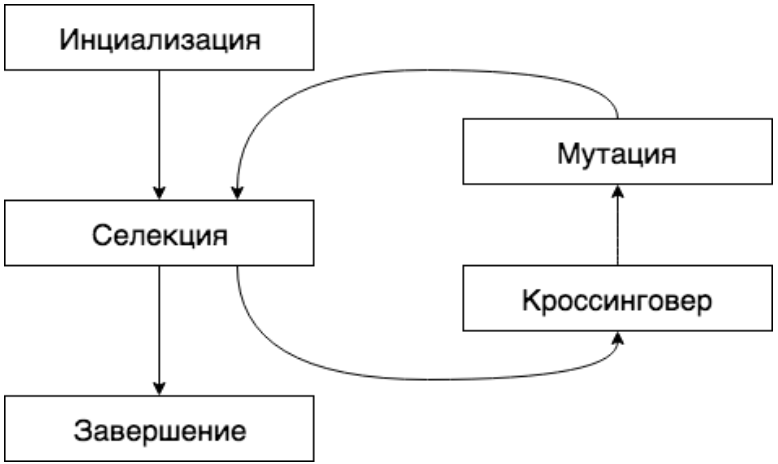
- Разработать и реализовать эволюционный алгоритм для автоматизированного построения guess-and-determine атак на генераторы ключевого потока
- Разработать новые эвристики для уменьшения временных затрат на их построение
- Применить полученный алгоритм к задачам криптоанализа ряда современных шифров

Эволюционный алгоритм

Особь: декомпозиционное множество, в виде битового вектора

$$X = \{x_2, x_3, x_5, x_7, \ldots, x_n\}$$





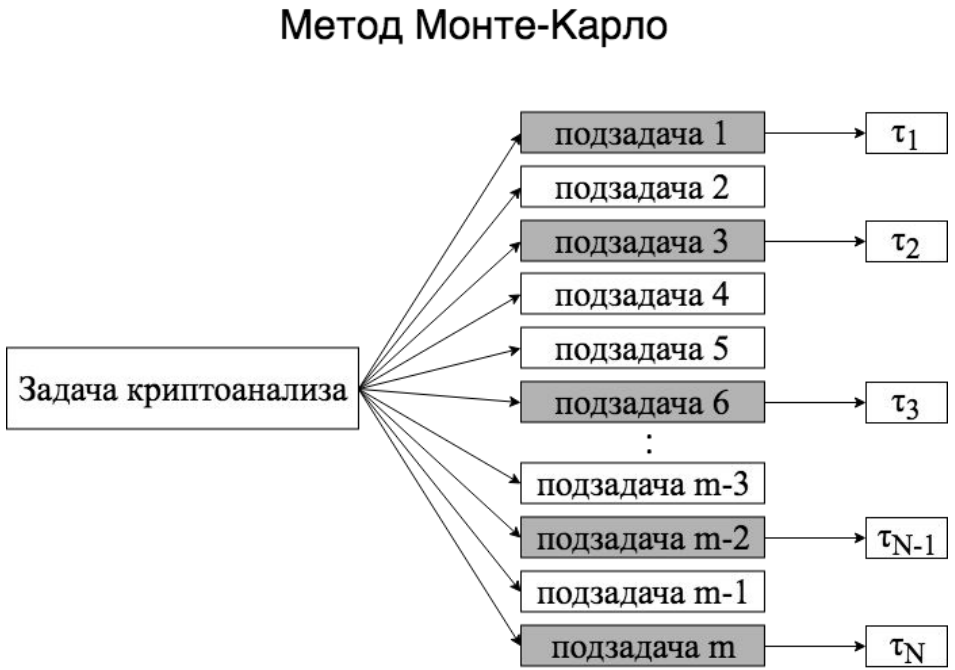
Функция приспособленности. Inverse Backdoor Set (1)

$$s = |X|$$

$$P_X = \frac{\#\{i = 1 \ldots 2^s : \tau_i < tl\}}{2^s}$$

Оцениваем:

$$P_X = \frac{1}{N} \cdot \sum_{i=1}^{N} \xi_i \text{, где } \xi_i = \begin{cases} 1, & \tau_i \le tl \\ 0, & \tau_i > tl \end{cases}$$



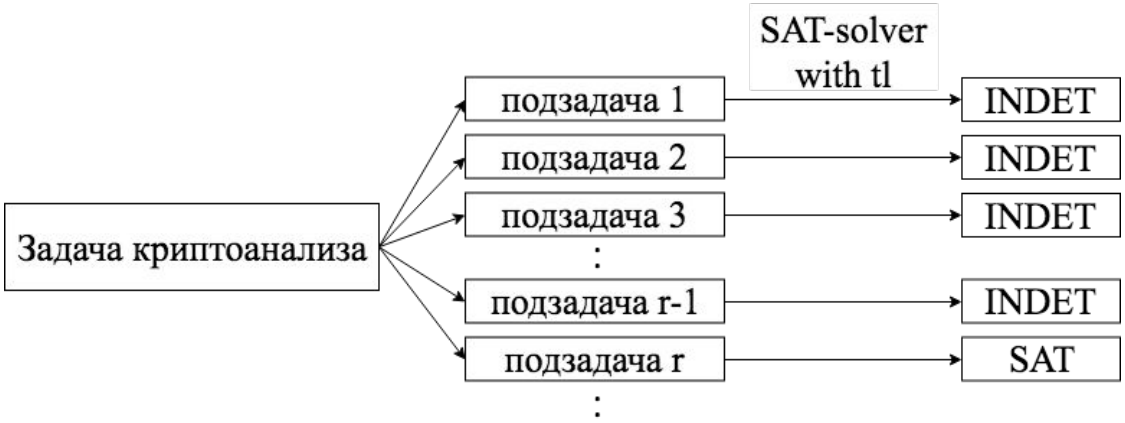
Inverse Backdoor Set: [*Semenov A., Zaikin O., Otpuschennikov I., Kochemazov S., Ignatiev A.* On cryptographic attacks using backdoors for SAT // The Thirty-Second AAAI Conference on Artificial Intelligence. – IEEE, 2018. – P. 6641-6648]

Функция приспособленности. Inverse Backdoor Set (1)

$$s = |X|$$

$$P^* = 1 - (1 - P_X)^r$$

$$P^* > 0.95 \text{ при } r \geq \frac{3}{P_X}$$

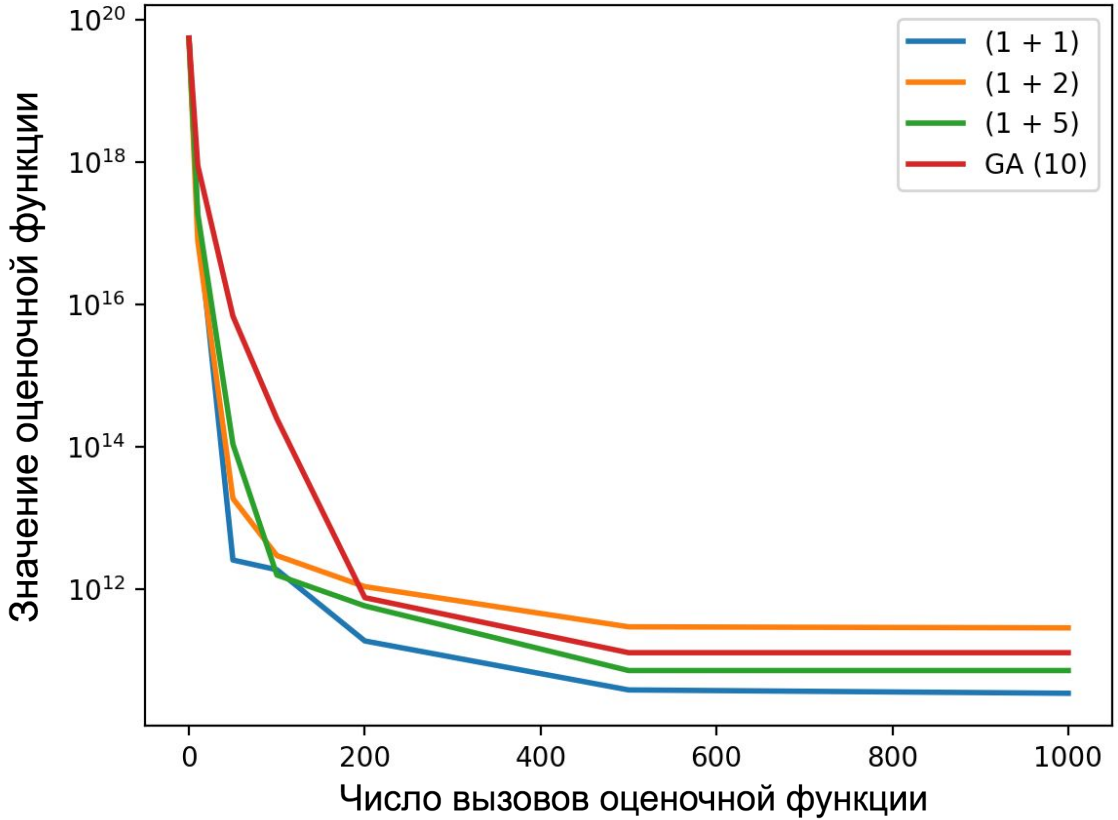


Оценка времени взлома шифра:

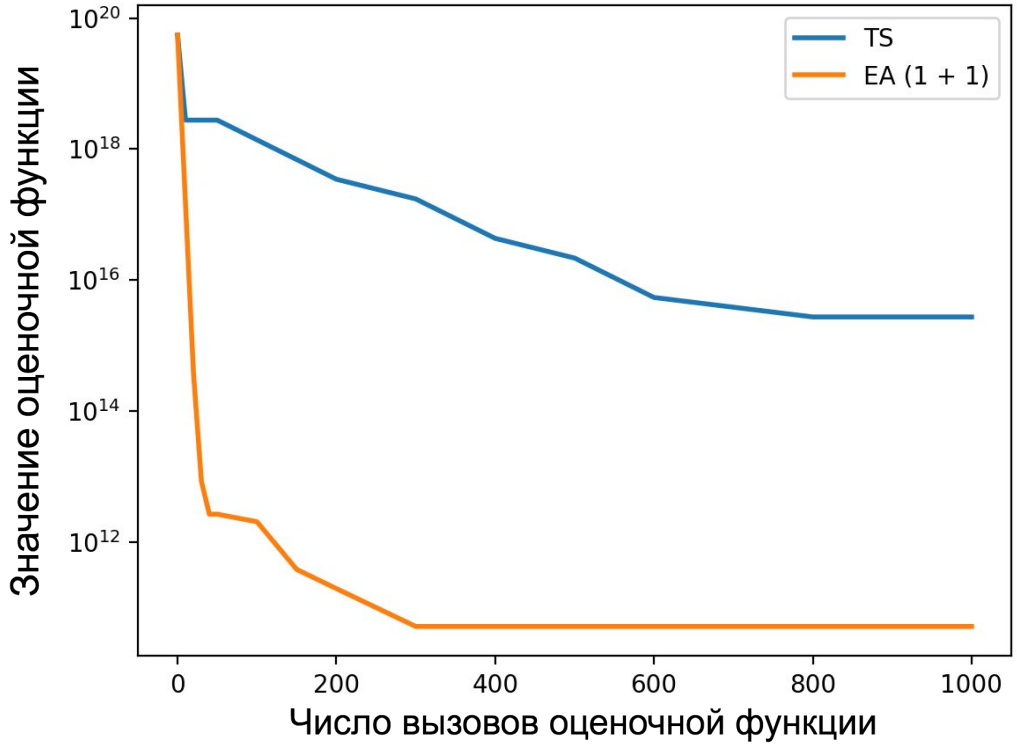
$$F(X) = 2^s \cdot t \cdot r$$

Inverse Backdoor Set: [*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]

Сравнение Стратегий



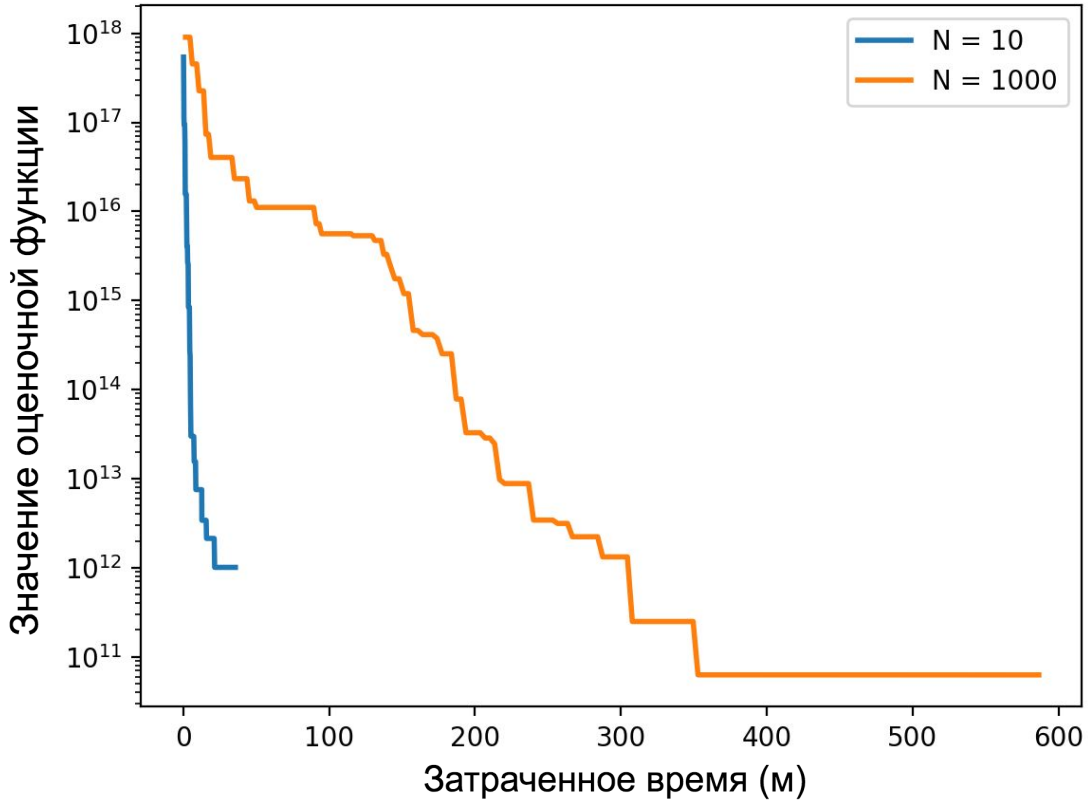
Сравнение Evolutionary Algorithm и Tabu Search*



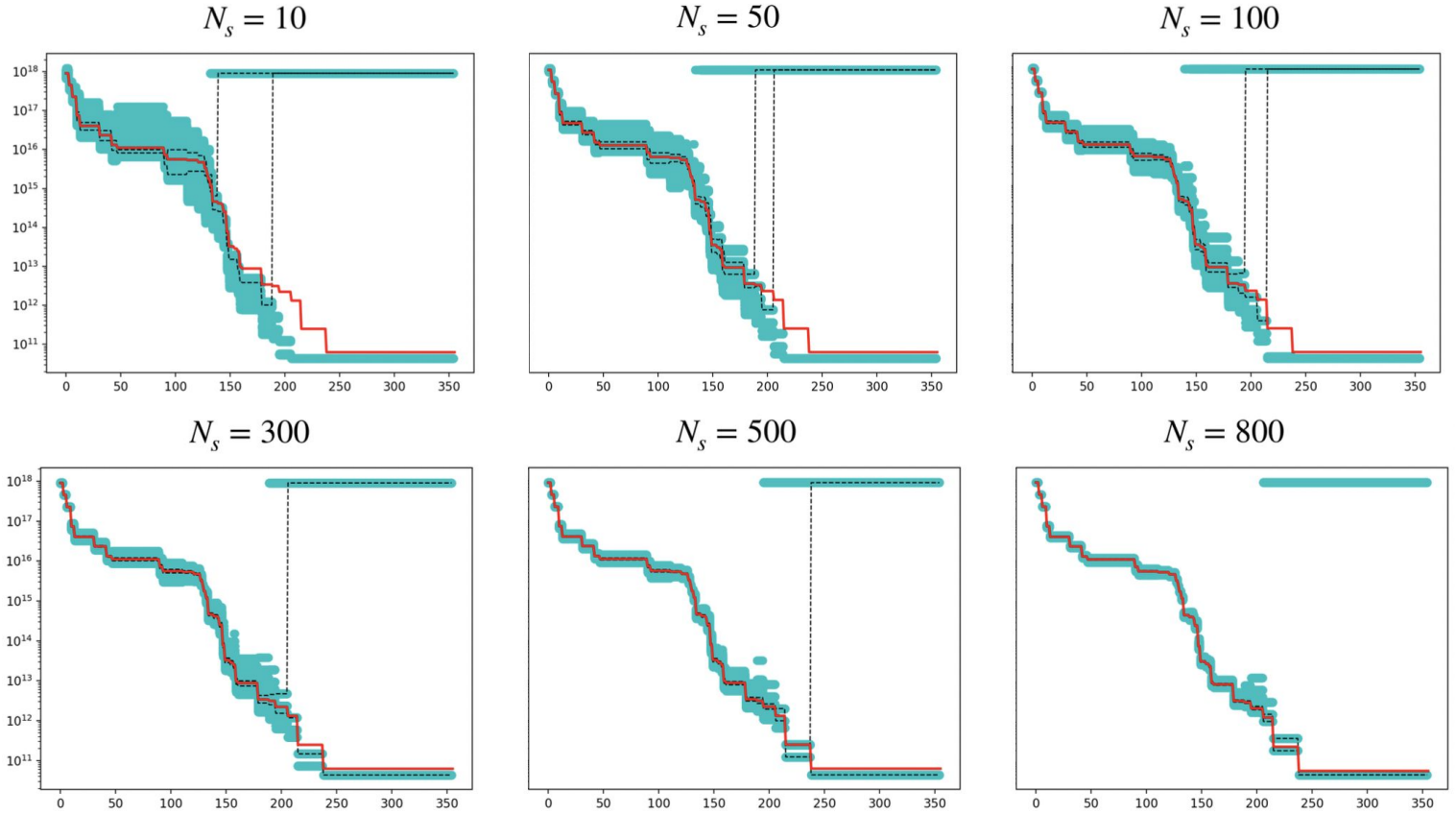
* [*Semenov A., Zaikin O.* Algorithm for Finding Partitionings of Hard Variants of Boolean Satisfiability Problem with Application to Inversion of Some Cryptographic Functions // SpringerPlus. – 2016. – Vol. 5. – P. 554-554.]

Адаптивное изменение объема выборки. Идея.

Шифр: A5/1
Стратегия: (1+1)

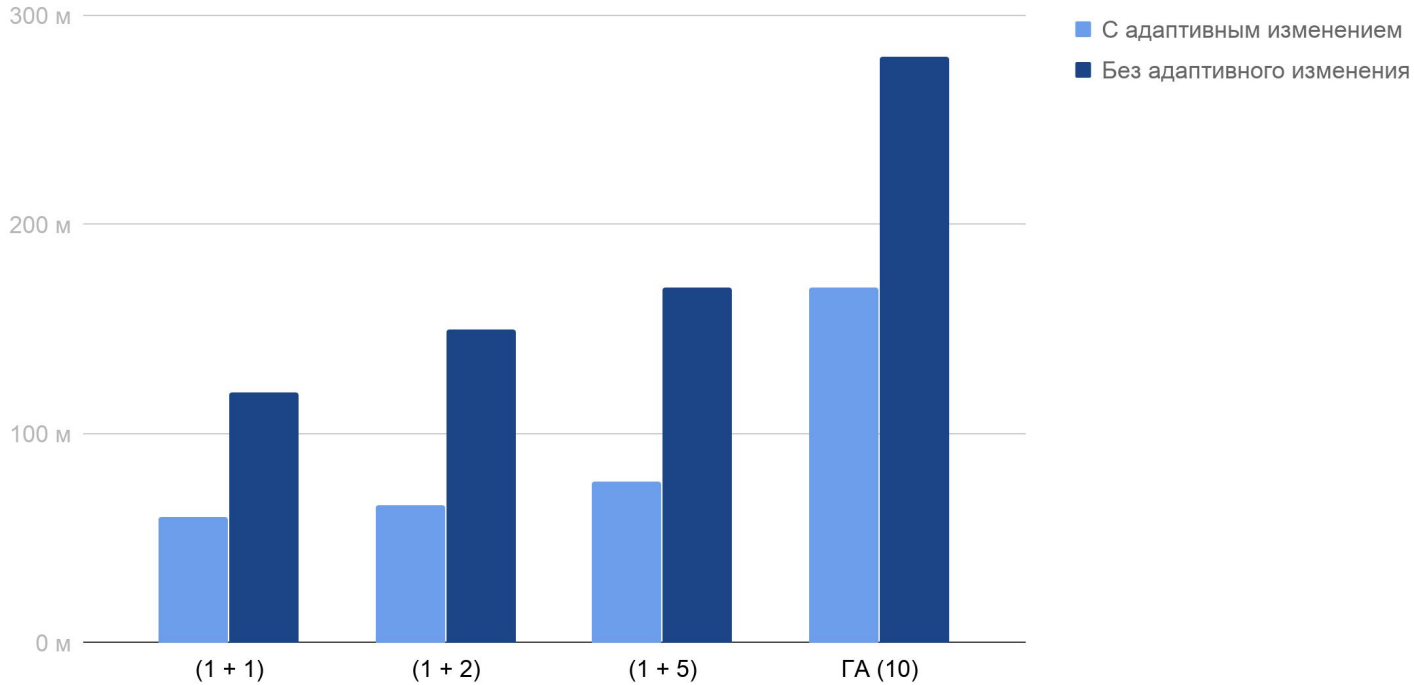


Адаптивное изменение объема выборки. Анализ



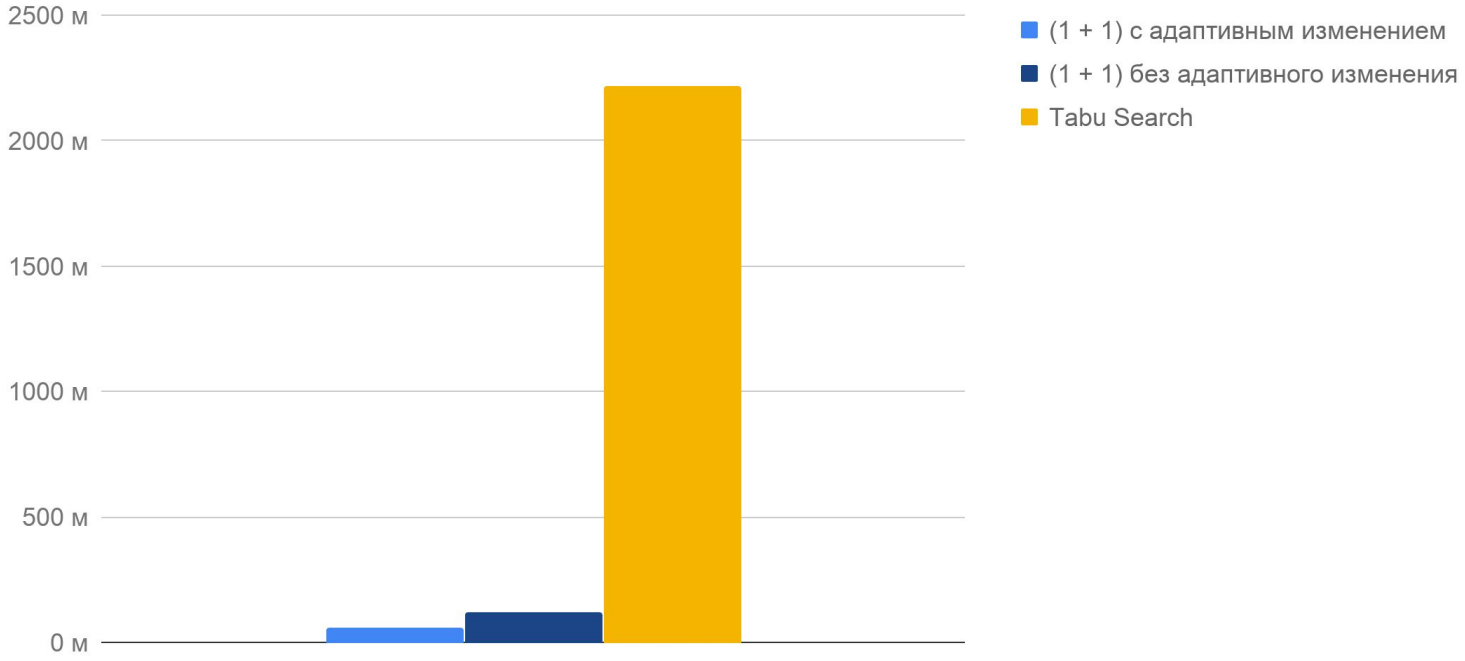
Адаптивное изменение объема выборки. Результат

Сравнение временных затрат на достижение граничного значения $6.7 \cdot 10^{12}$.

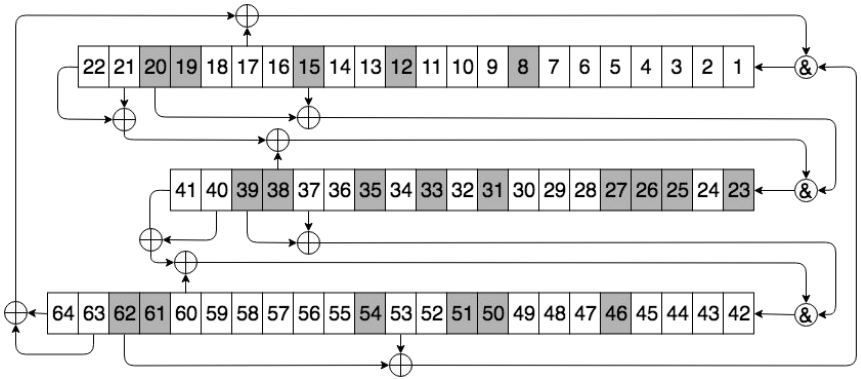


Адаптивное изменение объема выборки и TS

Сравнение временных затрат на достижение граничного значения $6.7 \cdot 10^{12}$.

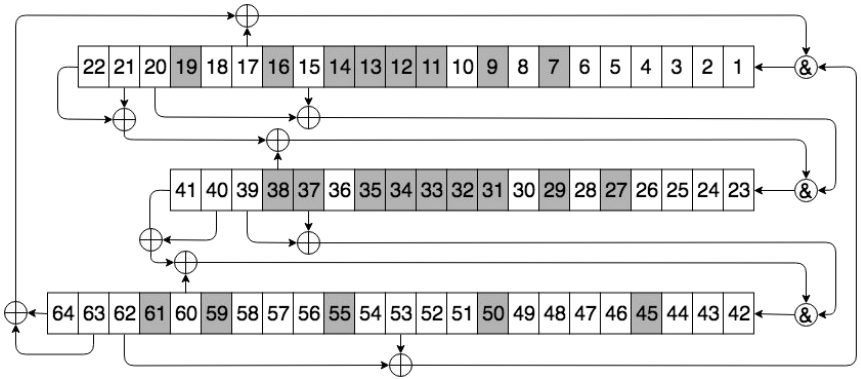


Новое декомпозиционное множество для Trivium 64



Оценка времени взлома: ~317 дней*

Результат наших коллег из лаборатории ИДСТУ СО РАН



Оценка времени взлома: ~184 дня*

Результат, полученный в ходе исследования

*из расчета на одно ядро процессора AMD Opteron 6378 @ 2.4 GHz

Дальнейшие задачи и пути исследования

- Рассмотреть другие потоковые шифры: E0, Grain, Trivium
- Разработать методы подбора оптимальных параметров для SAT-решателей
- Исследовать переменные Цейтина на предмет возможности их включения в декомпозионное множество

Заключение

- Разработан и реализован эволюционных алгоритм для автоматизированного построения guess-and-determine атак на криптографические алгоритмы
- Разработана новая эвристика для уменьшения временных затрат на их построение
- Найдено декомпозиционное множество для шифра Trivium 64 с меньшим значением оценочной функции

Достижения

- дипломант Конгресса Молодых Ученых VII “Диплом за лучший научно-исследовательский доклад студента”

Поданные заявки

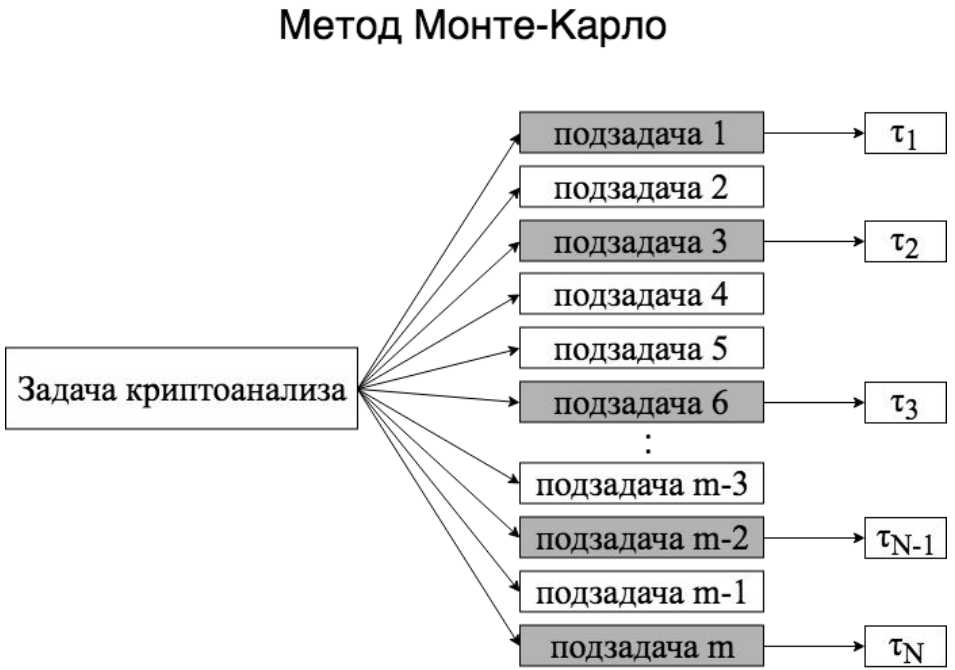
- Российский Научный Фонд. “Разработка эволюционных стратегий поиска декомпозиций трудных вариантов задачи о булевой выполнимости с применением к обращению криптографических функций” в качестве исполнителя
- Российский Фонд Фундаментальных Исследований. “Разработка методов машинного обучения для NP-трудных задач построения графовых моделей на основе SAT-решателей” в качестве исполнителя

Функция приспособленности. SAT Partitioning

Оценка времени взлома шифра:

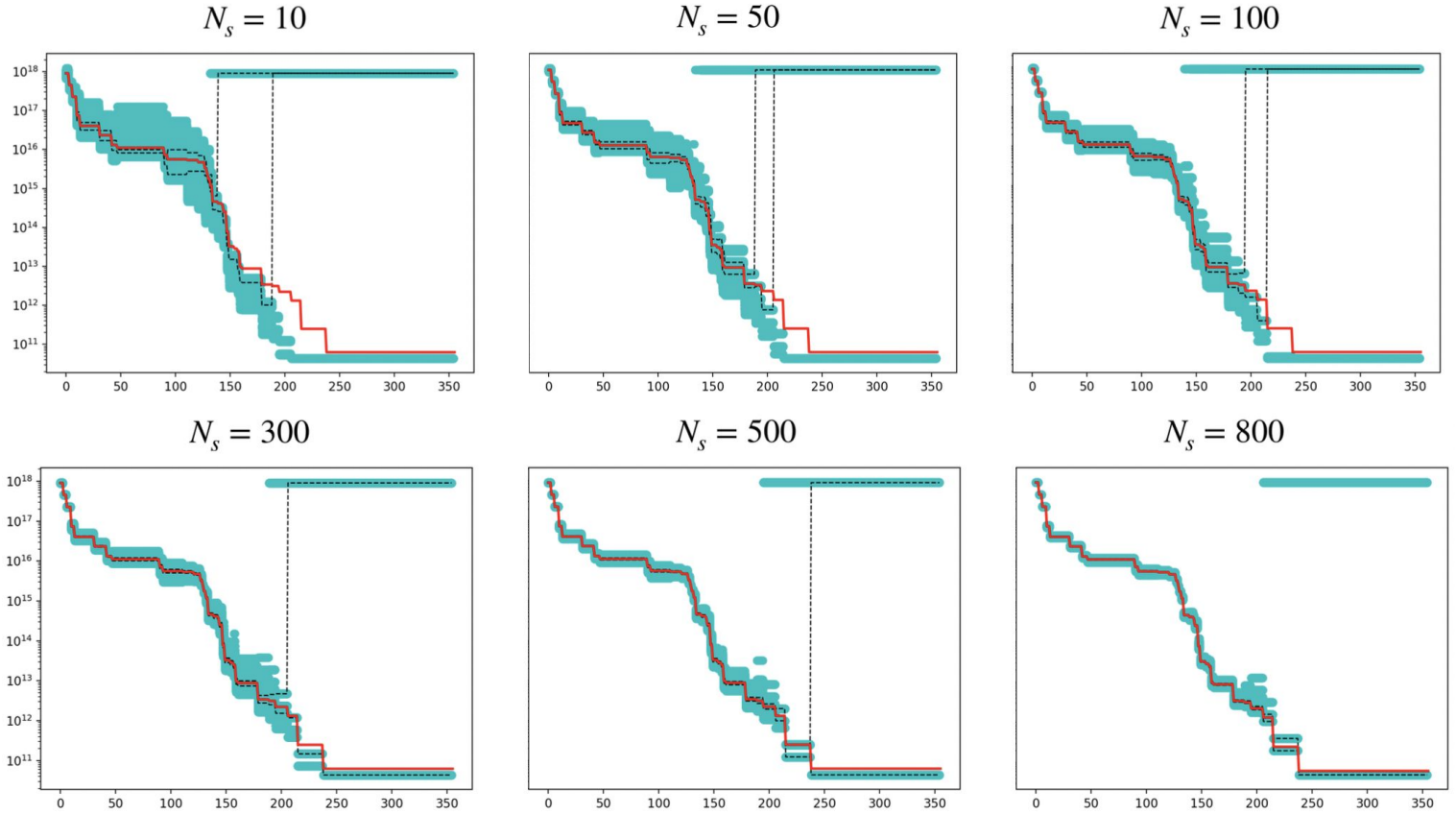
$$s = |X|$$

$$F(X) = 2^s \cdot \frac{1}{N} \cdot \sum_{i=1}^{N} \tau_i$$

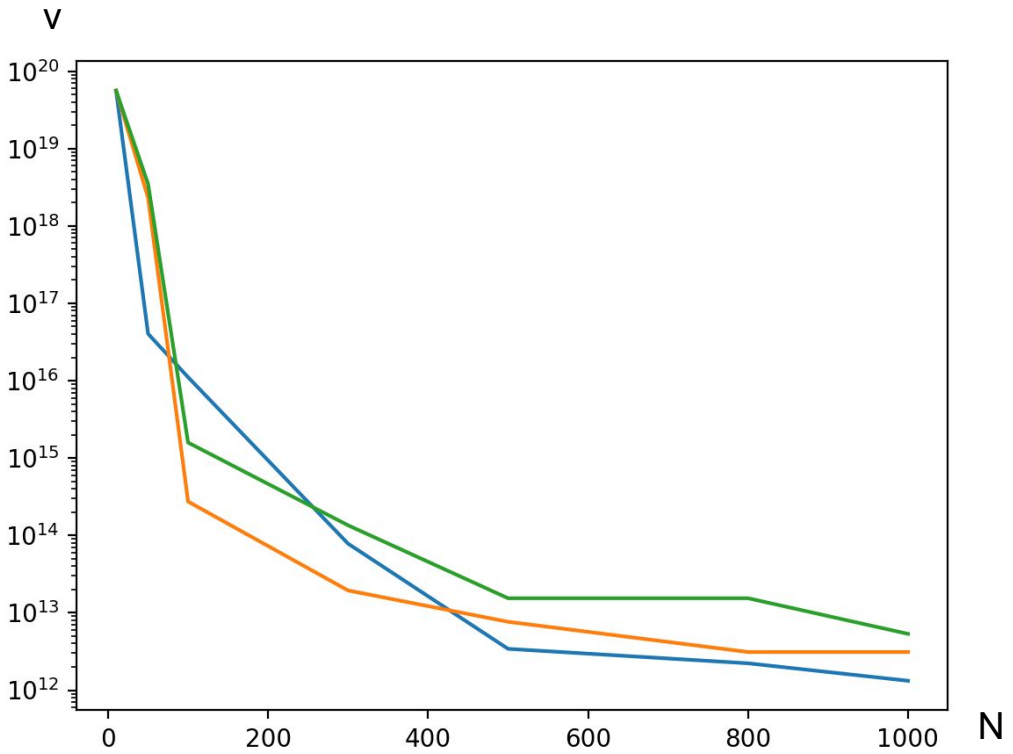


SAT Partitioning: [Semenov A., Zaikin O. Algorithm for Finding Partitionings of Hard Variants of Boolean Satisfiability Problem with Application to Inversion of Some Cryptographic Functions. In SpringerPlus, 2016]

Адаптивное изменение объема выборки. Анализ

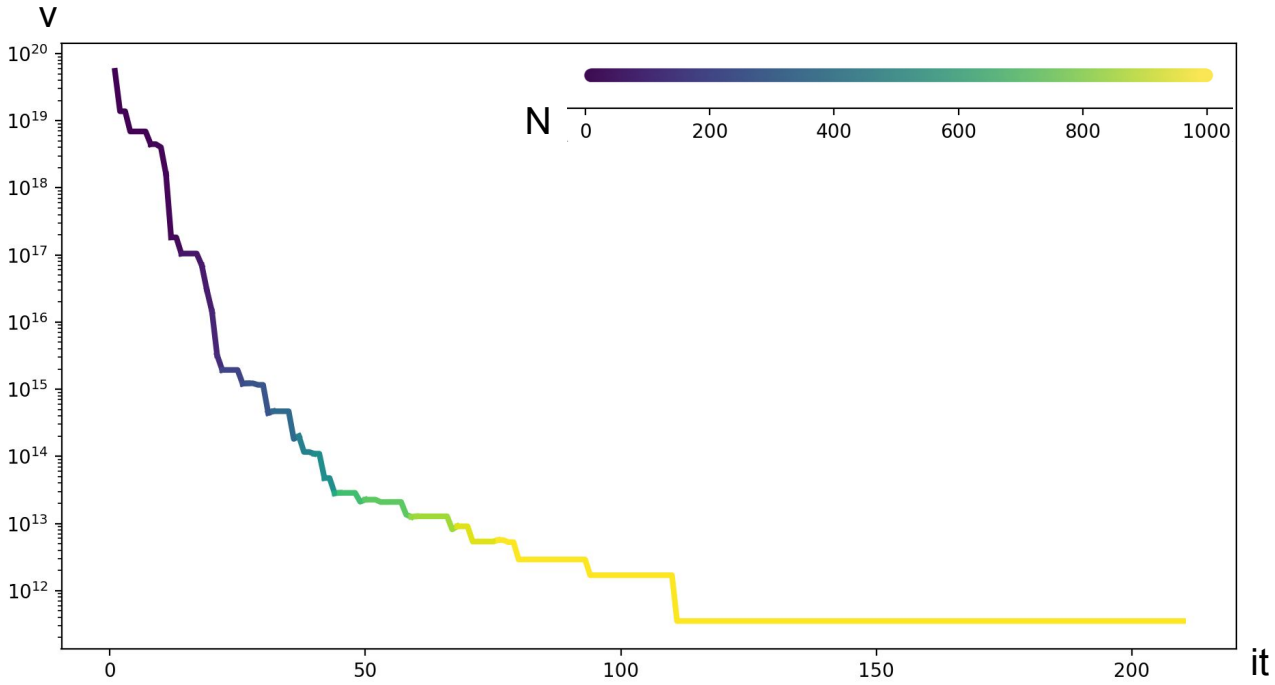


Адаптивное изменение объема выборки. Стратегия



N	v
10	до $5.5 \cdot 10^{17}$
50	до $4.9 \cdot 10^{16}$
100	до $8.1 \cdot 10^{14}$
300	до $1.1 \cdot 10^{14}$
500	до $1.7 \cdot 10^{13}$
800	до $6.7 \cdot 10^{12}$
1000	после $6.7 \cdot 10^{12}$

Адаптивное изменение объема выборки. Пример



Наращивание выборки

Пусть $N_1 < N_2$

$F_{N_1}(X)$? $F_{N_2}(X)$ корректно ли?

$$P_X = \frac{1}{N_2} \cdot \left(\sum_{i=1}^{N_1} \xi_i + \sum_{i=N_1+1}^{N_2} \xi_i \right)$$

подсчитанные ранее

свеже подсчитанные подзадачи