Evolutionary Computation Techniques for Constructing SAT-based Attacks in Algebraic Cryptanalysis

Artem Pavlenko[1], Alexander Semenov[2] and Vladimir Ulyantsev[1]

[1] ITMO University, St. Petersburg, Russia
[2] Matrosov Institute for System Dynamics and Control Theory SB RAS, Irkutsk, Russia
{alpavlenko, ulyantsev}@corp.ifmo.ru

Introduction

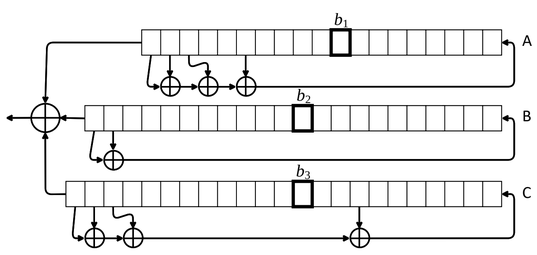
- Algebraic cryptanalysis is a way of breaking ciphers through solving systems of **algebraic equations** over finite fields. This system of equations can be simplified by guessing the values of some of its variables.
- An algebraic attack that uses some **guessed bit set** to simplify the system of cryptanalysis equations is called a guess-and-determine attack.
- Previously tabu search and simulated annealing have been used to construct a guess-and-determine attack [Semenov et al. 2018].
- We propose to apply **evolutionary algorithms** with additional heuristics for this purpose.

Highlights

- We use **(1+1)-EA** and **GA** to construct SAT-based guess-and-determine attacks on cryptographic ciphers.
- We propose a sample size **adaptation strategy** to increase the number of individuals that the algorithm processes during a fixed time budget.
- **Backdoors** have been found, some of them are better than those found earlier, but estimation of breaking time is still very long.

Translate Cipher to SAT Using Transalg

Cipher A5/1



b_1, b_2, b_3 – clocking bits
$X = X_A \cup X_B \cup X_C$
$X = \{x_1, x_2, \ldots, x_{64}\}$ – secret key
$Y = \{y_1, y_2, \ldots, y_{128}\}$ – key stream

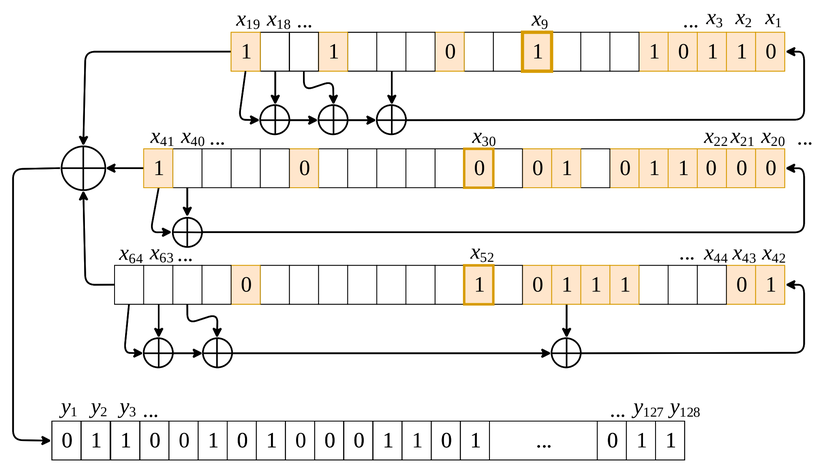
Transalg program

```
__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];
  }
}
```

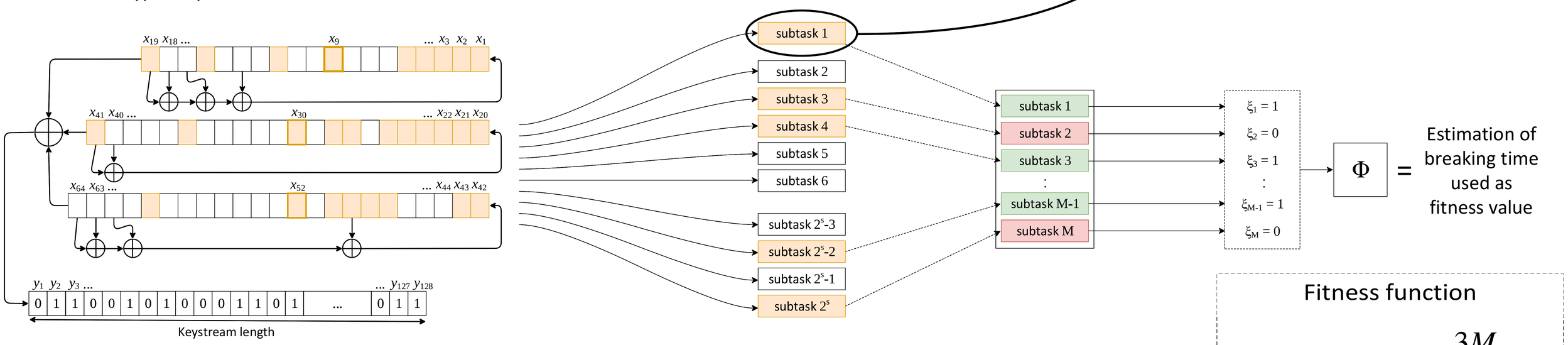
SAT-formula

```
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
...
-8425 -8293 8295 -8297 0
-8425 -8293 -8295 8297 0
```

Example of a subtask. Backdoor variables substituted with given values.



Cryptanalysis Task with Backdoor | Backdoor-based Decomposition | Monte-Carlo Sampling | Solving | Evaluating



Backdoor = Individual

$B = \{ x_1, x_2, x_3, x_4, x_5, x_9, x_{12}, x_{16}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{27}, x_{28}, x_{30}, x_{36}, x_{41}, x_{42}, x_{43}, x_{47}, x_{48}, x_{49}, x_{50}, x_{52}, x_{60} \}$

Fitness function

$$\Phi = 2^{|B|} \cdot T \cdot \frac{3M}{\sum_{k=1}^{M} \xi_k}$$

Evolutionary Algorithms Application to Backdoors Construction

Algorithms details

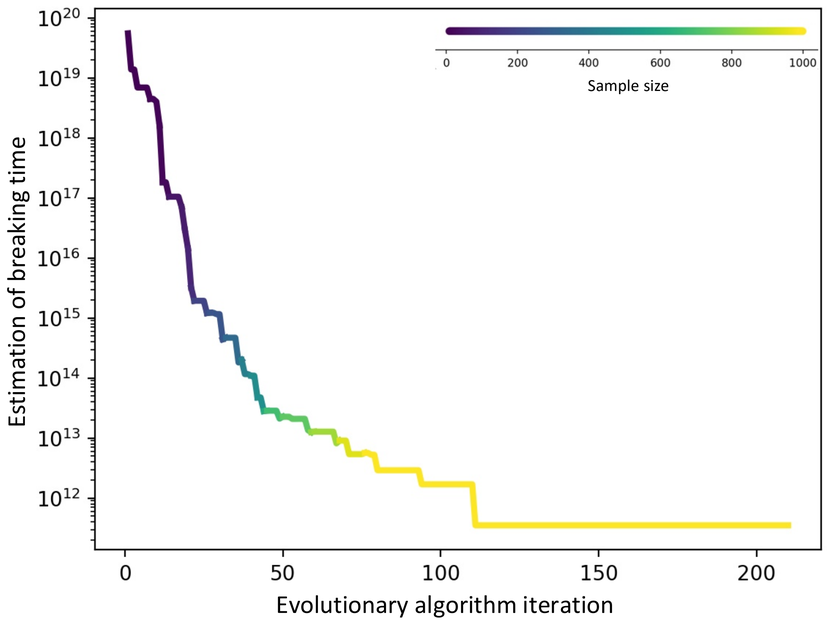
EA (1+1):
- standard bit mutation
- stagnation limit = 300

GA (Elitism):
- population size N = 10
- standard bit mutation
- uniform crossover with probability 0.2

Solver:
- SAT-solver – ROKK
- time limit – 10 seconds for one SAT-instance

Adaptation strategy:
- algorithm starts with Monte-Carlo sample size M = 10
- M is gradually increases to 1000 with the decrease of the fitness value

Dynamic adaptation of the sample size



Experimental results

	Tabu Search		EA (1+1)		GA (Elitism)	
	|B|	Estimation of breaking time (s)	|B|	Estimation of breaking time (s)	|B|	Estimation of breaking time (s)
Trivium-Toy 64/75	17	4.30e+07	21	**3.19e+07**	22	5.36e+07
Trivium-Toy 96/100	34	3.14e+12	33	1.28e+13	40	**2.09e+12**
Bivium 177/200	40	4.29e+12	32	2.60e+12	39	**1.49e+12**
ASG 72/76	8	**5601.33**	9	5604.8	8	6155.19
ASG 96/112	14	3.95e+06	13	6.76e+06	16	**3.72e+06**
ASG 192/200	47	**1.14e+16**	47	2.27e+18	44	2.84e+17

Supposed by the Russian Science Foundation (project No 18-71-00150)