Faculty of Mathematics and Information Science
Warsaw University of Technology

# A Generic Metaheuristic Approach to Sequential Security Games

**Adam Żychowski, Jacek Mańdziuk**

{a.zychowski, j.mandziuk}@mini.pw.edu.pl

**AAMAS 2020**

# Problem definition

Sequential Security Games with Stackelberg Equilibrium
Defender (D) commits strategy first, then Attacker (A) chooses strategy
Goal: maximize Defender's payoff

$$BR(\pi^D) = \arg\max_{\pi^A \in \Pi^A} U^A(\pi^D, \pi^A)$$

$$\arg\max_{\pi^D \in \Pi^D} U^A(\pi^D, BR(\pi^D))$$

$\pi^D, \pi^A$ – Defender's/Attacker's strategy
$U^D, U^A$ - Defender's/Attacker's payoff

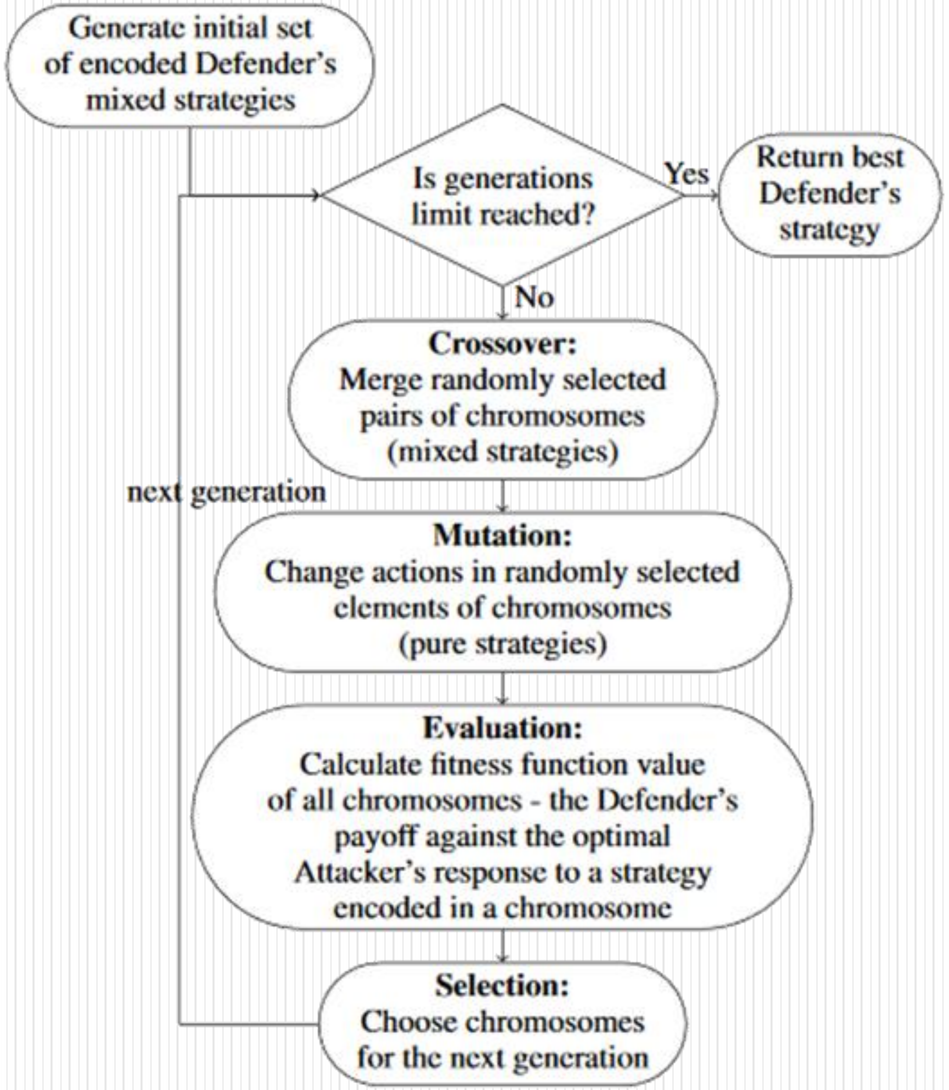
# Motivation and contribution

Finding Stackelberg Equilibrium is a kind of optimization problem – **evolutionary algorithms** is one of the most promising optimization methods

Creating a **general** Stackelberg Games solution framework based on evolutionary algorithms, easily **adaptable to various types of games**

An **anytime** approximation method for **time-critical** applications

# EASG Overview



# Chromosome representation

Each chromosome represents Defender's mixed strategy – a set of pure strategies with their probabilities

Initially chromosomes contain random pure strategies

$$CH_q = \{(\pi_1^q, p_1^q), \ldots, (\pi_{l_q}^q, p_{l_q}^q)\}, \ \sum_{i=1}^{l_q} p_{l_q}^q = 1$$

$\pi_i^q$ - pure strategy (e.g. list of Defender's actions in consecutive time steps)

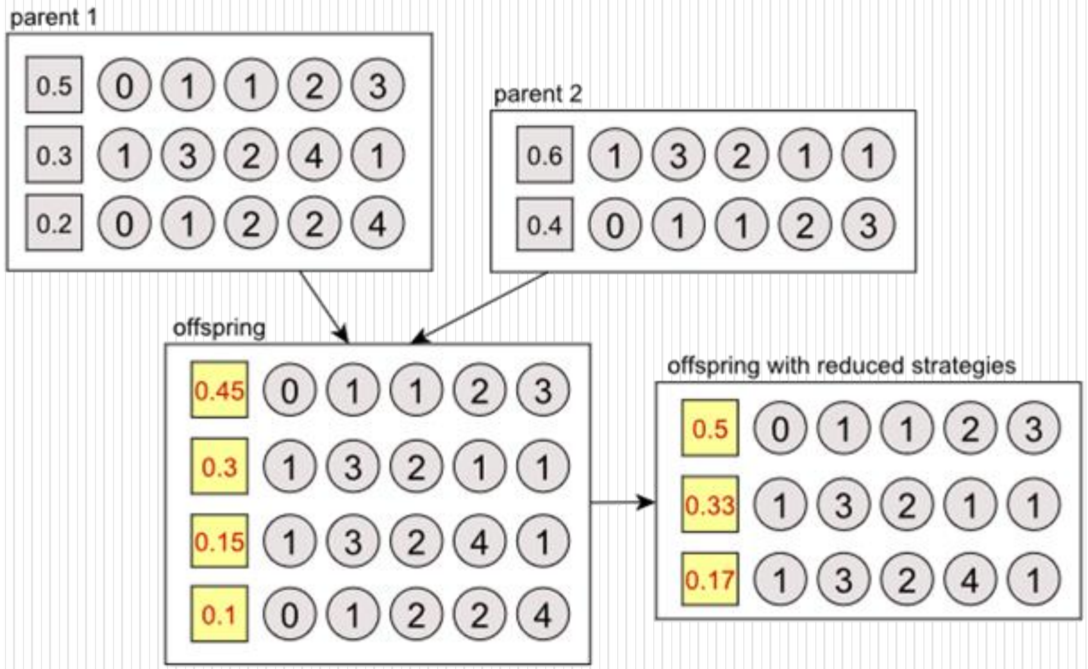
$p_i^q$ - probability of strategy $\pi_i^q$

$l_q$ – length of chromosome $CH_q$ (the number of pure strategies included in the mixed strategy represented by that chromosome)

# Crossover

Crossover operation combines two chromosomes by merging their sets of pure strategies and halving their probabilities

After crossover each pure strategy $(\pi_j^q)$ may be deleted with probability $1 - \frac{p_j^q}{2}$

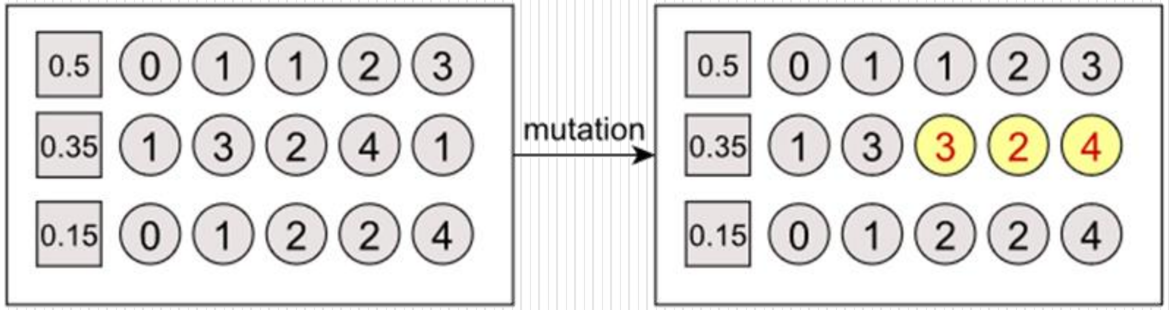


# Mutation

Mutation randomly changes one Defender's action in one of pure strategies starting from a randomly chosen time step

Each chromosome is mutated with *mutation rate* probability

Exploration of new areas of the search space



# Selection

Fitness function - Defender's payoff in case of playing a mixed strategy encoded in the chromosome

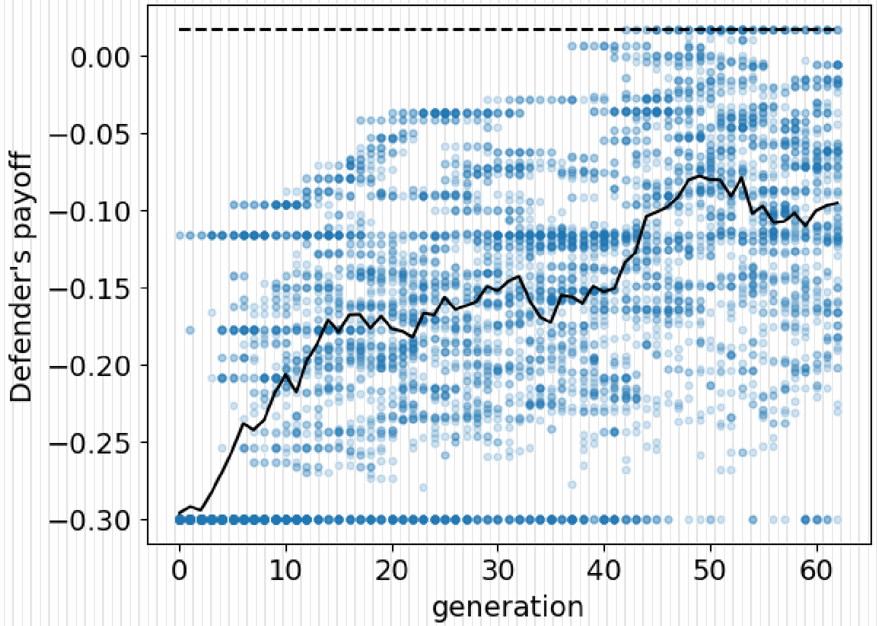
Binary tournament - two chromosomes are randomly chosen and the one with a higher fitness value is promoted to the next generation with probability $p_s > 0.5$, otherwise the lower-fitted one is promoted

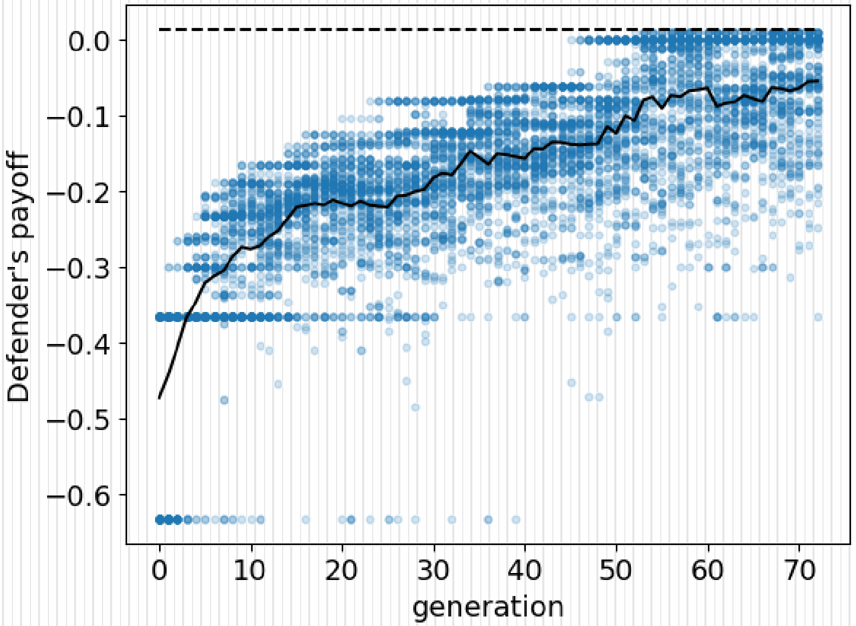
Some number of *elite* chromosomes (with the greatest fitness function value) ➔ unconditionally promoted to the next generation population

# Performance

Mean Defender's payoff increases in time - the entire population moves towards the areas with higher payoff

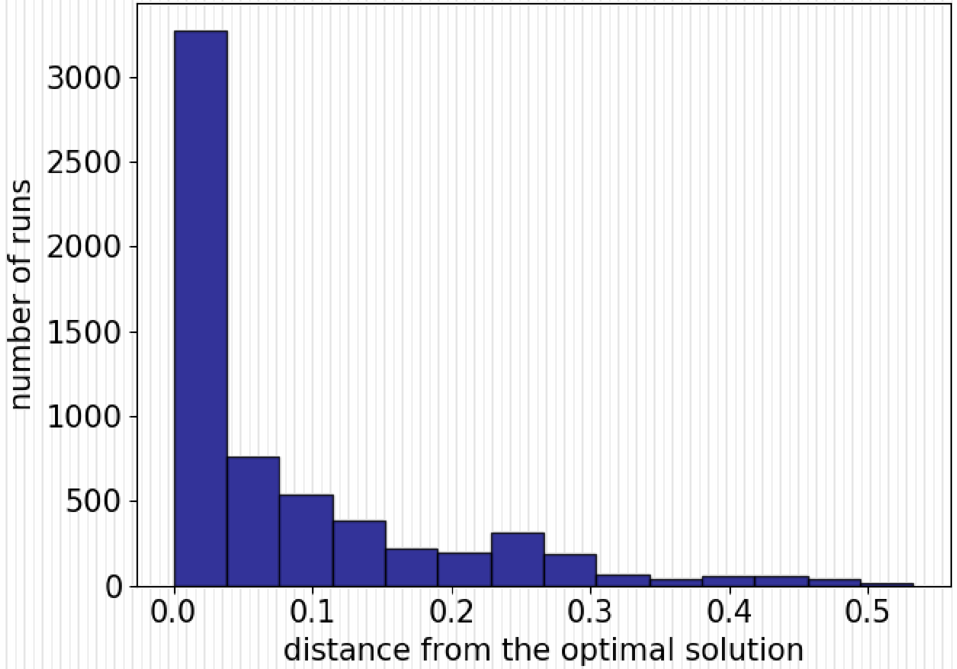
Low-payoff individuals exist in all generations - exploration of new strategies



# Results quality

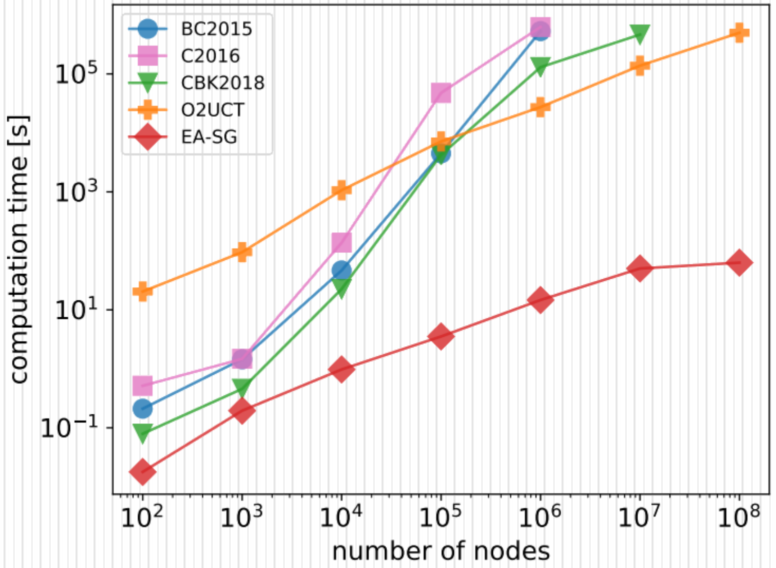
| Games type | Fraction of games with optimal solution found | Mean difference between the optimal and EASG | The highest difference between the optimal and EASG |
|---|---|---|---|
| Warehouse Games | 72% | 0.0013 | 0.0127 |
| Search Games | 47% | 0.0253 | 0.0955 |
| FlipIt Games | 73% | 0.0087 | 0.0321 |



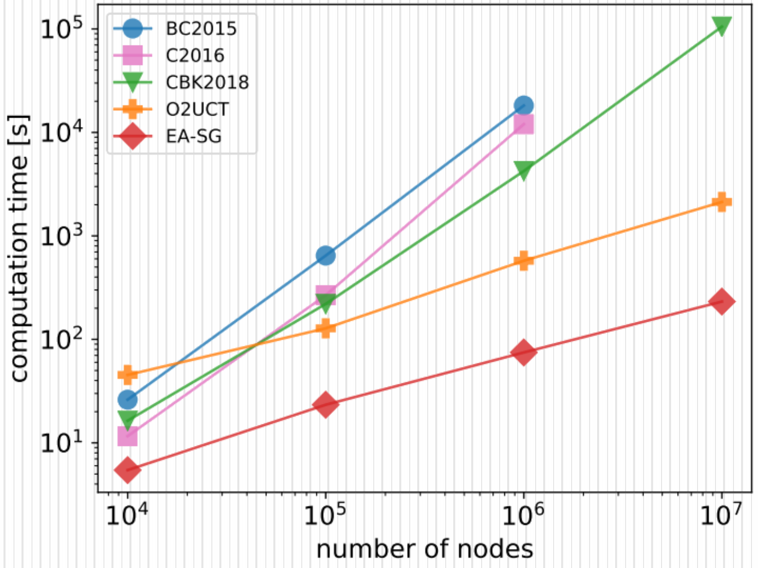
# Time scalability

Time performance strongly depends on selected steering parameters – the possibility of establishing the expected balance between computation time and quality of results

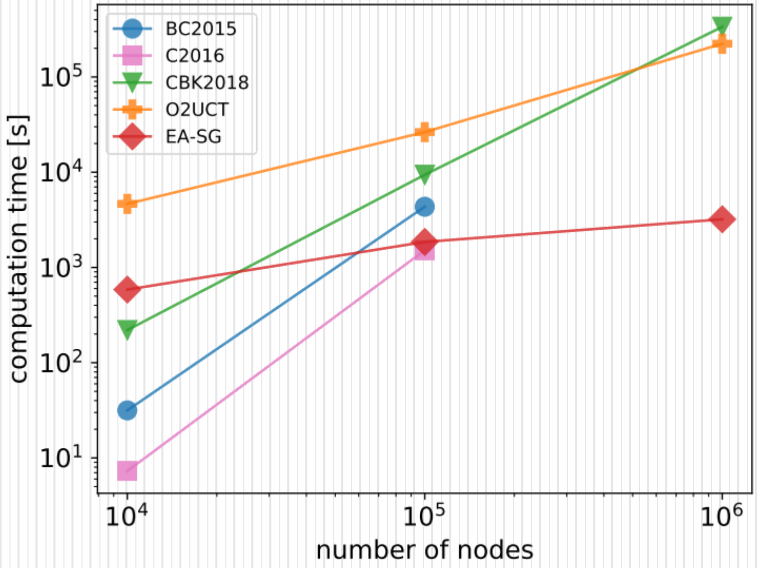
The highest time efficiency among the tested methods




Warehouse Games




Search Games




FlipIt Games

# Summary

**Evolutionary algorithm** which can be **easily adapted to various types of Security Games**

Efficient approximation method with **high stability** and **good results quality**

Capable of **solving larger and more complex sequential Security Games** than state-of-the-art methods

Iteration-based construction - **well suited for time-critical applications** (*anytime* method)