New Directions in AI-based Cryptography

Luca Mariot
https://lucamariot.org

Dagstuhl Seminar – Intelligent Security
11 October 2022
Symmetric ciphers require several low-level primitives, such as:

(a) Pseudorandom Generators

(b) Boolean functions and S-boxes

(c) Latin Squares and Orthogonal Arrays
AI approach for symmetric crypto

- "Traditional" approach: ad-hoc and algebraic constructions
- "AI" approach: support the designer using AI methods:
  - Optimization (Evolutionary algorithms, swarm intelligence...)
  - Computational models (cellular automata, neural networks...)

\[ \chi \text{ point} \]

\[ \Downarrow \quad F: \{0, 1\}^n \rightarrow \{0, 1\}^m \]

Luca Mariot  
New Directions in AI-based Cryptography
Genetic Algorithms (GA) & Genetic Programming (GP)

- **Black-box optimization** of a fitness function [L15]
- Work on a **coding** of the solutions

- **GA Encoding**: bitstrings
  \[ f(x_1, x_2, x_3) = x_1 \cdot x_2 \oplus x_1 \oplus x_2 \oplus x_3 \]  
  
- **GP Encoding**: trees
  \[ f(x_1, x_2, x_3, x_4) = (x_1 \text{ AND } x_2) \text{ OR } (x_3 \text{ XOR } x_4) \]  
  
Luca Mariot  
New Directions in AI-based Cryptography
Use of EA in symmetric cryptography

Design of primitives as combinatorial optimization problems, examples [C21, M22]:

- **Boolean functions** $f : \mathbb{F}_2^n \to \mathbb{F}_2$ for stream ciphers
  
  ![Diagram of stream cipher](image)

- **S-Boxes** $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ for block ciphers

Possible advantages of using EA for this search [P16, M19b]:

- **Diversity** of solutions, due to the "blindness" of EA
- **Flexibility** of EA (optimizing several properties at once)
One-dimensional Cellular Automata (CA):

Example: \( n = 6, \ d = 3, \ f(s_i, s_{i+1}, s_{i+2}) = s_i \oplus s_{i+1} \oplus s_{i+2} \)

- No Boundary CA:
  - \( f(1,0,0) = 1 \)
  - \( f(1,1,0) = 0 \)
- Periodic Boundary CA:
  - \( f(1,0,0) = 1 \)
  - \( f(1,1,0) = 0 \)

Each cell updates its state \( s \in \{0, 1\} \) by applying a local rule \( f : \{0, 1\}^d \rightarrow \{0, 1\} \) to itself and the \( d - 1 \) cells on its right.
**Goal:** investigate how CA can be used in the design of cryptographic primitives [W86, L13]

Why CA?

1. **Security from Complexity**
2. **Efficient Implementation**
Real world CA-Based Crypto: Keccak $\chi$ S-box

- Local rule: $\chi(x_1, x_2, x_3) = x_1 \oplus (1 \oplus (x_2 \cdot x_3))$ (rule 210)
- Invertible for every odd size $n$ of the CA

Used as a PBCA with $n = 5$ in Keccak [B11]

Luca Mariot
New Directions in AI-based Cryptography
CA S-boxes found by GP

**Idea:** evolve a CA rule that defines an S-box, optimizing:

- **crypto** properties (nonlinearity, differential uniformity) [M19a]
- **implementation** properties (area, latency)

- Up to size $7 \times 7$: results on par or slightly better than the state of the art (Keccak, PRESENT, Piccolo, ...) [P17]
New Direction 1:
Evolve constructions of crypto primitives
Evolving Constructions of Boolean functions with GP

Predefined functions:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$f_0$</td>
<td>1001</td>
</tr>
<tr>
<td>$f_1$</td>
<td>1010</td>
</tr>
</tbody>
</table>

Independent variables:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$v_0$</td>
<td>0101</td>
</tr>
<tr>
<td>$v_1$</td>
<td>0011</td>
</tr>
</tbody>
</table>

GP Boolean construction function

IF

$v_0$ $f_0$ XOR

$f_1$ $v_1$

Output:

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1010</td>
<td>1001</td>
<td>0101</td>
<td>1001</td>
</tr>
</tbody>
</table>

**Idea:** Do not evolve primitives directly, but rather their mathematical constructions [C22]

**Use Boolean minimizers to interpret the constructions**

**Research Question:** Does GP obtain previously known constructions or new ones?
New Direction 2: Evolutionary-based distinguishers
Differential Cryptanalysis

- **Idea**: chosen plaintext attack, see how differences propagate to the ciphertext

\[ x, x': x \oplus x' = \Delta \]

- **Goal**: Compute differential probability of \( \Delta \rightarrow \Delta^* \)

- **Distinguishing attack**: given \((x, x')\), classify if it is a *random* or *real* pair

- **Tool**: Difference Distribution Table (DDT)
Deep learning-based differential distinguishers

- A. Gohr (CRYPTO 2019): train a CNN as a differential distinguisher
- Better accuracy than pure distinguishers on SPECK32/64

Problem: learned models are hardly interpretable!

---

1 Image credits: A. Benamira et al., A Deeper Look at Machine Learning-Based Cryptanalysis, EUROCRYPT 2021
New Direction 2: GP-based distinguishers

▶ **Idea:** Replace convolutional layers with convolutional GP [J21]

▶ **Research Question:** Is "convolutional" GP able to reach CNN performances, and yield models easier to interpret?
New Direction 3:
Evolutionary approach to adversarial examples
**Adversarial Examples in DNN**

- **DNN known to be vulnerable to adversarial examples (AE)**
- **Idea**: perturb a valid example to mess the DNN’s classification

Classification: Panda

Noise perturbation

Classification: Gibbon

> Perturbation moves the example beyond the decision boundary of a DNN

---


Luca Mariot

New Directions in AI-based Cryptography
Evolutionary Construction of AE

- Perturbations for AE can be **minimal**
- **One-pixel attack**: Modify just one pixel in a valid example

![Images of perturbed images](3)

- Pixel selection done with **Evolutionary Algorithms**

---

New Direction 2: LON Analysis of Loss Landscapes

- **Idea**: use fitness landscape analysis on the space of AE
- **Approach**: continuous variant of Local Optima Networks

Research Questions:
- Is it possible to improve EA-based one-pixel attacks?
- Gain insights to build more robust DNN?

---

Where we arrived so far:

▶ Evolutionary algorithms and CA give interesting alternatives for the design of symmetric primitives
▶ Flexibility of optimization objectives

Looking at the future:

▶ Plenty of open problems in the design research thread, but... ... mainly of mathematical interest
▶ Leverage on the interpretability of evolutionary models for cybersecurity applications
References


