# Optimizing Cryptographic Strength of Substitution Layers in Symmetric-Key Cryptographic Algorithms

Christopher A. Wood

May 17, 2012

# Agenda

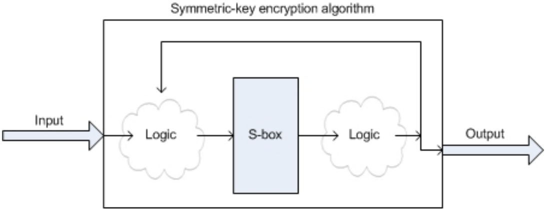
# Elements of Cryptographic Security

Cryptographic algorithm security is measured by:

- Levels of confusion and diffusion
- Resilience to common cryptanalytic attacks

# The substitution layer

A S-box is a common source for nonlinearity in symmetric-key cryptographic algorithms. It can be defined as function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$, where $n$ is the number of bits needed to represent each element in the field.



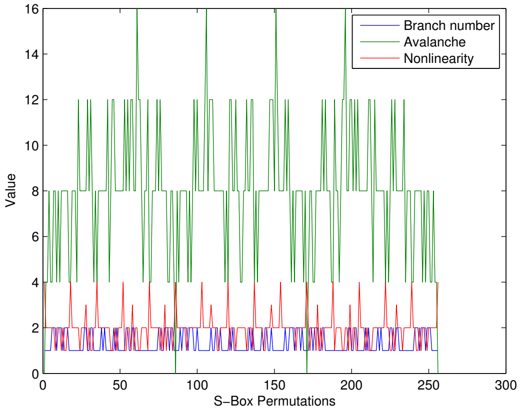
# Security Measurements

- Branch number
  - Measures the number of "active" S-box bits that are touched for every input $x \in$
- Avalanche number
  - Measures the total number of bit changes for a single bit change in the input to the S-box
- Nonlinearity degree
  - Measures how much nonlinear "behavior" the S-box exhibits

# Algorithm Design Goals

- High branch number
- Avalanche number of exactly $n^2 2^{n-1}$
- High degree of nonlinearity

# Exhaustive search for 2-bit S-box



# Branch number problem formulation

**Branch Number - Minimize**

$$B'_N(X) = -B_N(X) = -\min_{i,j \neq i}(\mathrm{wt}(i \oplus j) + \mathrm{wt}(X(i) \oplus X(j))),$$

subject to the constraints

$$0 \leq X(i) \quad \leq \quad 2^n - 1$$

where $n$ is the number of bits needed to represent the design variables.

# Avalanche number problem formulation

**Avalanche Number - Minimize**

$$A'_N(X) = -A_N(X) = -\sum_{i=0}^{n-1} \sum_{x \in \mathbb{F}_2^n} \mathrm{wt}(f(x) \oplus f(x \oplus 2^i))$$

subject to the constraints

$$\begin{aligned} 0 \leq X(i) &\leq 2^n - 1 \\ \min_{i,j \neq i}(\mathrm{wt}(i \oplus j) + \mathrm{wt}(X(i) \oplus X(j))) - n2^{n-1} &\leq 0 \end{aligned}$$

where $n$ is the number of bits needed to represent the design variables.

# Nonlinearity degree problem formulation

**Degree of Nonlinearity - Minimize**

$$P_S(X) = \max_{0 \neq a,b} |\{x \in \mathbb{F}_2^n : S(x+a) - S(x) = b\}|,$$

subject to the constraints

$$0 \leq X(i) \leq 2^n - 1,$$

where $n$ is the number of bits needed to represent the design variables.

**Joint MINLP Problem - Minimize**

$$f(X) = w_1 A'_N(X) + w_2 B'_N(X) + w_3 P_S(X),$$

subject to the constraints

$$\begin{aligned} 0 \leq X(i) &\leq 2^n - 1 \\ \min_{i,j \neq i}(\mathrm{wt}(i \oplus j) + \mathrm{wt}(X(i) \oplus X(j))) - n2^{n-1} &\leq 0, \end{aligned}$$

where $n$ is the number of bits needed to represent the design variables and $w_i$, where $1 \leq i \leq 3$, are *not* design variables.

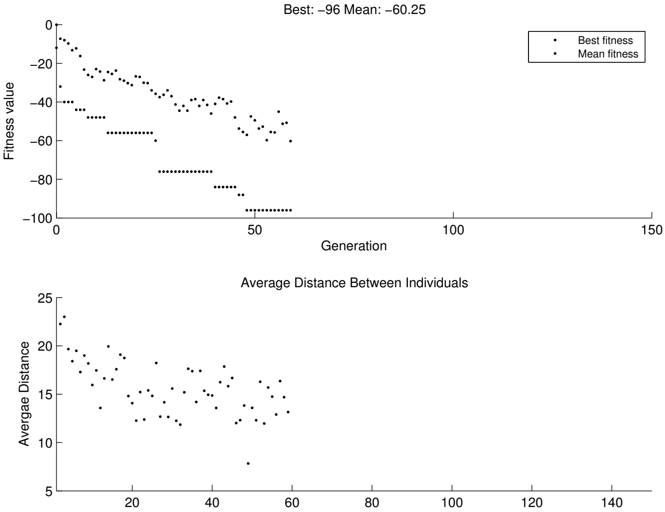
# MINLP algorithms

- Traditional MINLP algorithms (e.g. Branch and Bound)
    - 
- Evolutionary algorithms (e.g. genetic algorithms)
    - 

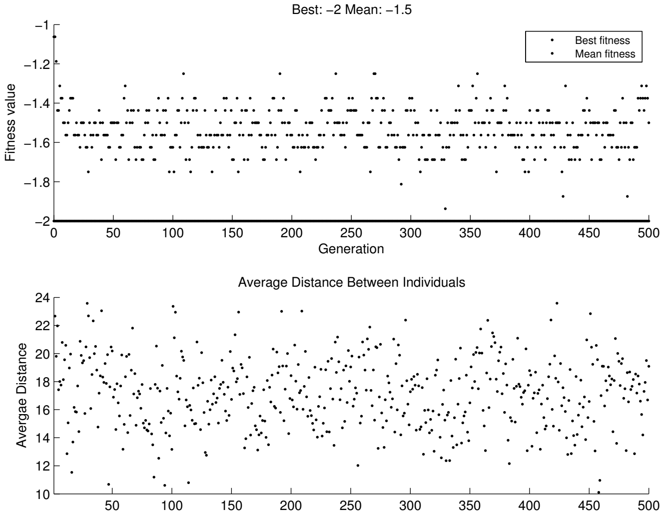
# Genetic algorithm configuration

| **Algorithm Option** | **Configuration Description** |
|---|---|
| Population mutation function | Randomly scaled children generations |
| Generations | 500 |
| Tolerance Function limit | $1 \times 10^{-6}$ from last function value change |
| Stall generation limit | $2^{n^n}$ identical function values |
| Initial population | S-box configuration $\langle 0, 1, ..., n \rangle$ |

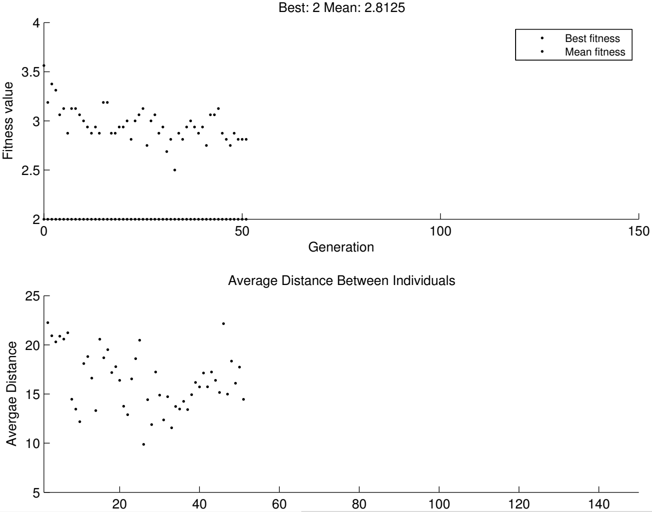
# Avalanche number for 4-bit S-box



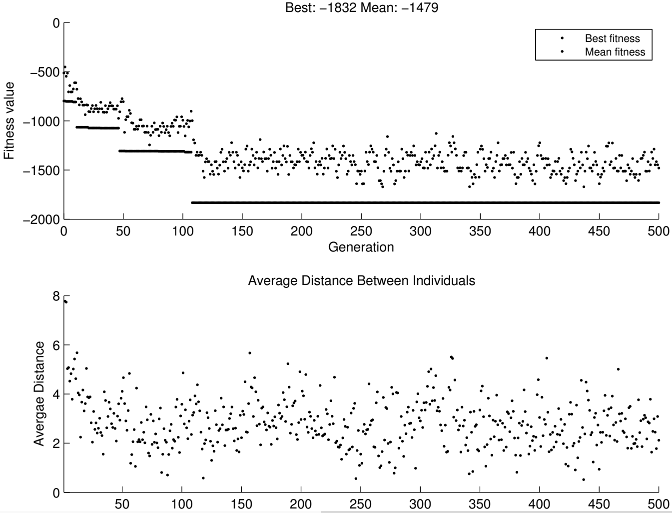
# Branch number for 4-bit S-box



# Nonlinearity degree for 4-bit S-box



# Multi-objective MINLP solution for 4-bit S-box



# Solution Analysis

| **Measurement** | **Results** |
|---|---|
| Branch number | BAD |
| Avalanche number | OKAY |
| Nonlinearity degree | GOOD |

# Conclusion

- Evolutionary optimization algorithms are the most appropriate for cryptographic applications
  - Effectively finds solutions for some discontinuous and instable functions
  - Not very effective at finding solution for multi-objective problems due to WHAT?
- TODO: what else?