The Evolution of EACirc

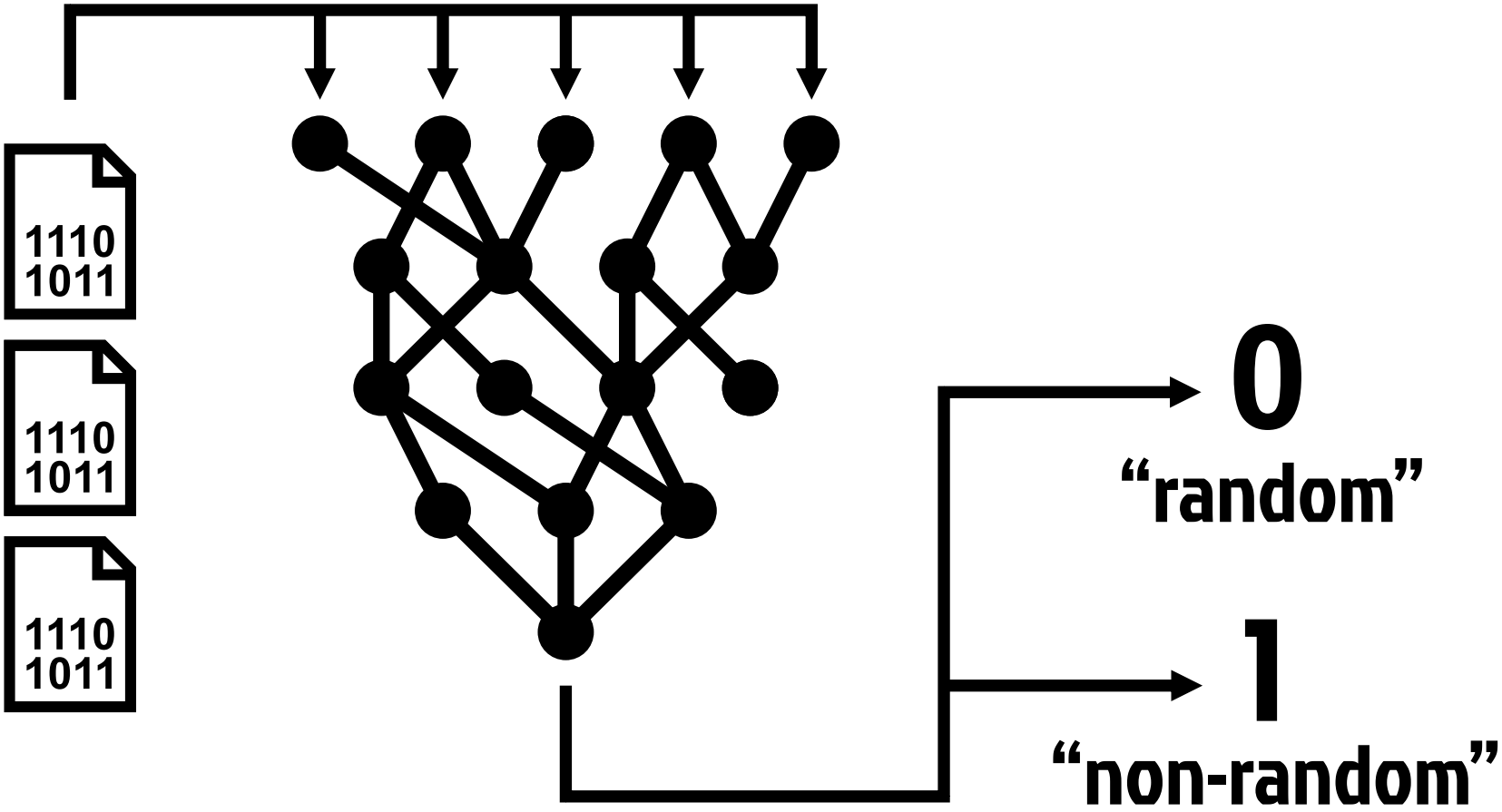
Martin Ukrop, Petr Švenda,
Marek Sýs et alii

CROCS
Centre for Research on
Cryptography and Security

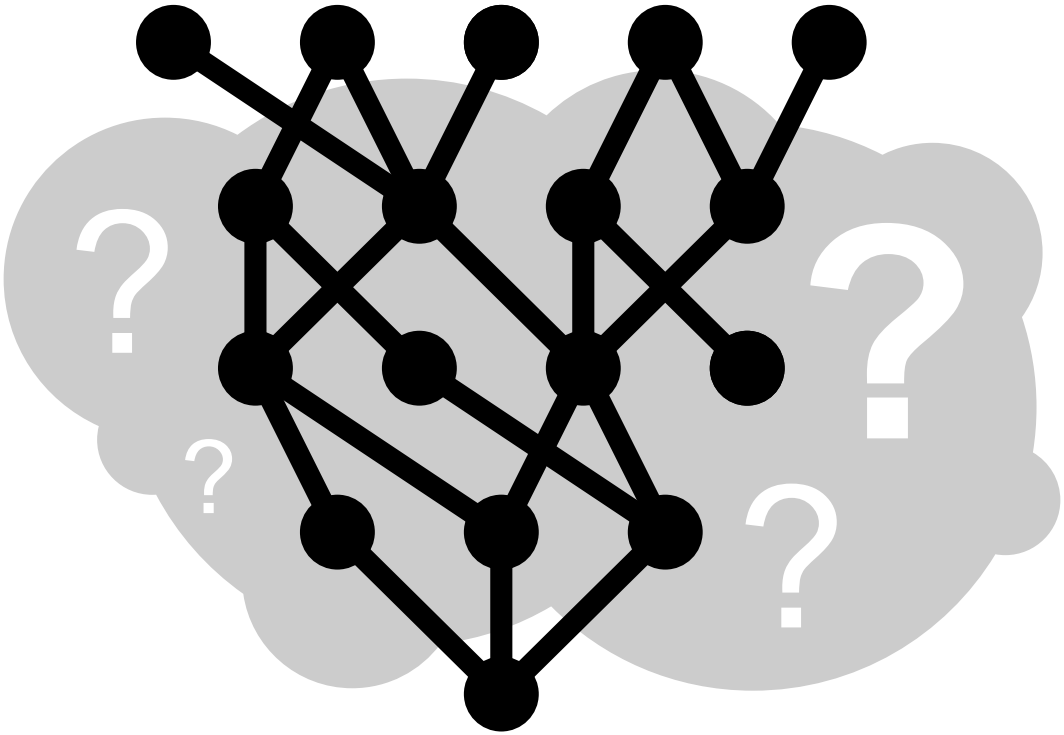
GAČR presentation, 5. 2. 2016

icons from The Noun Project

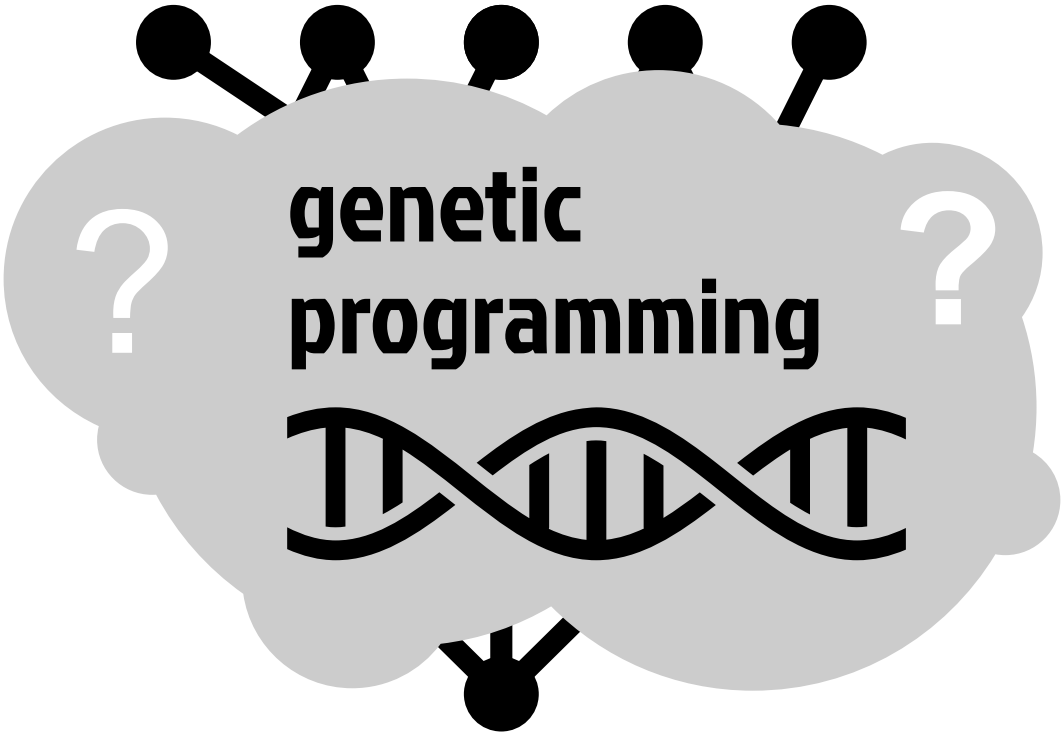
Software circuit distinguishers



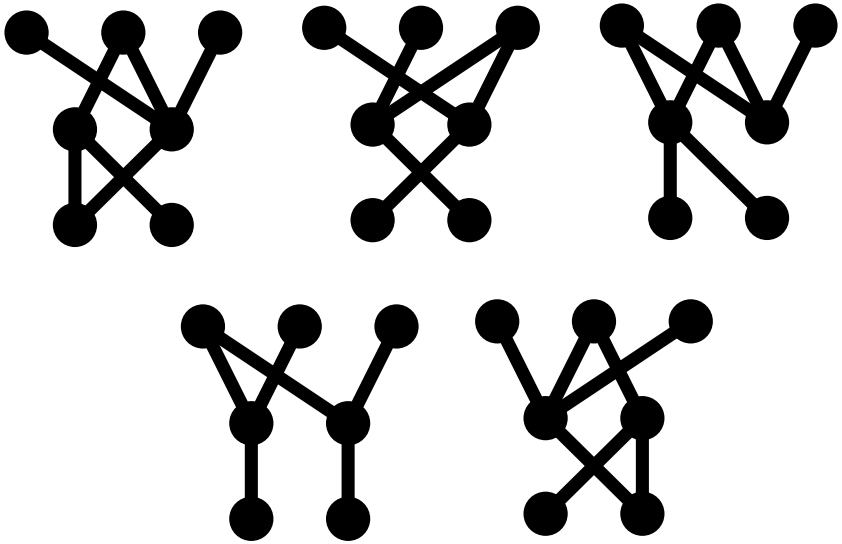
Distinguisher construction...



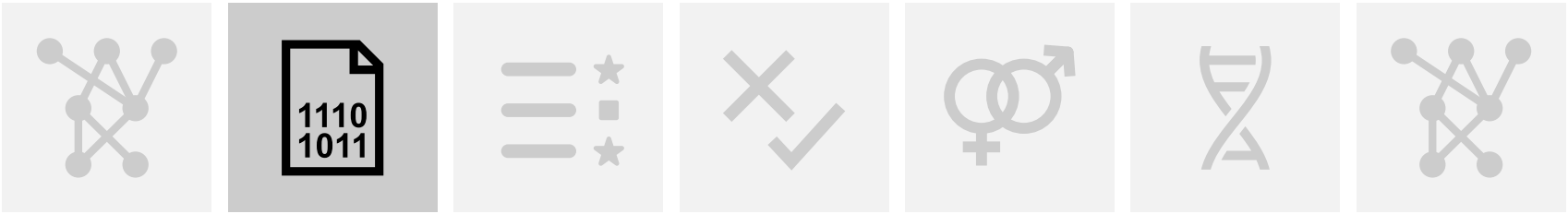
...with the use of Evolutionary Algorithms

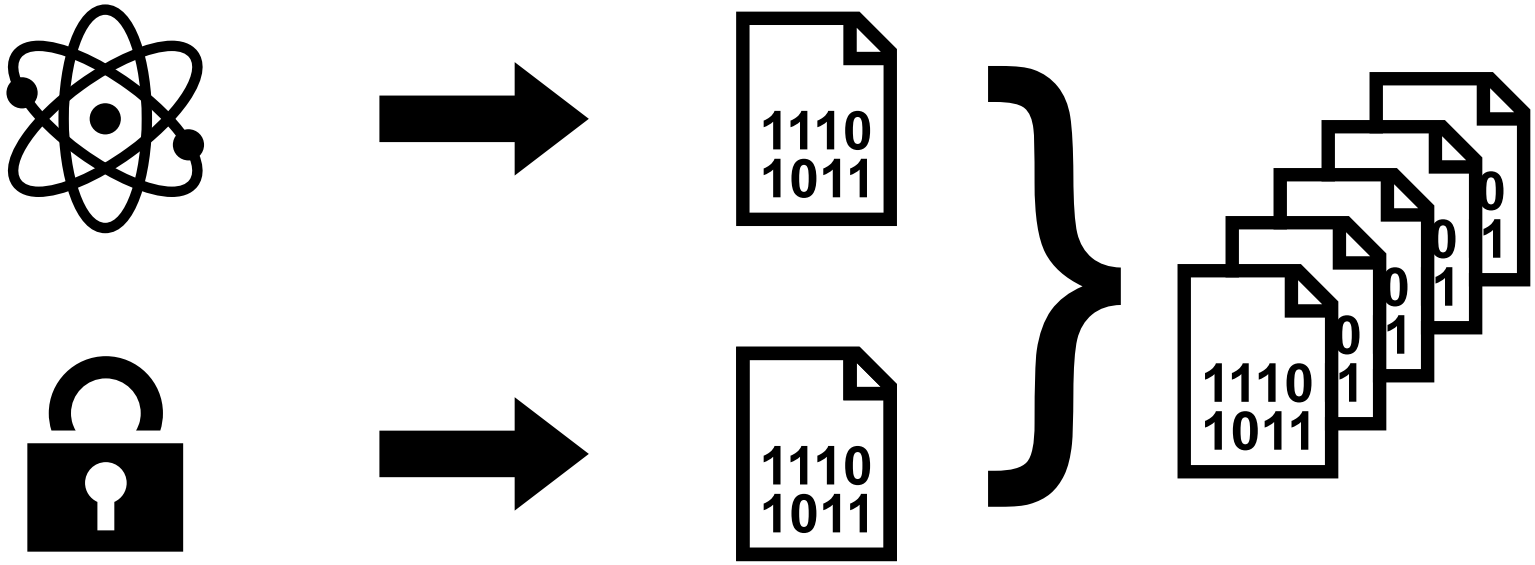


1. Initialization

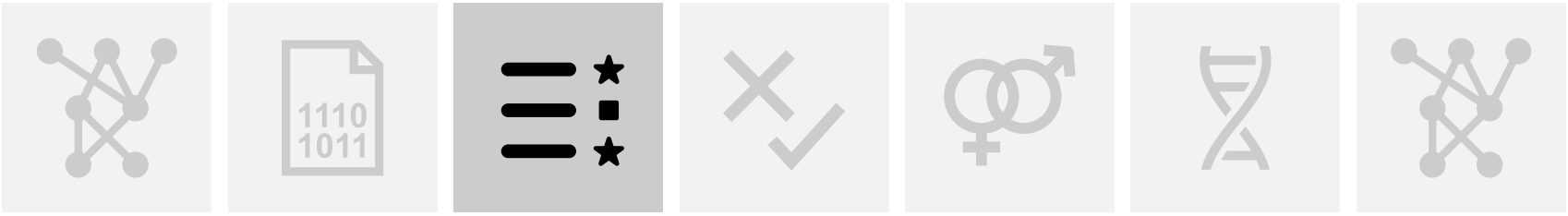


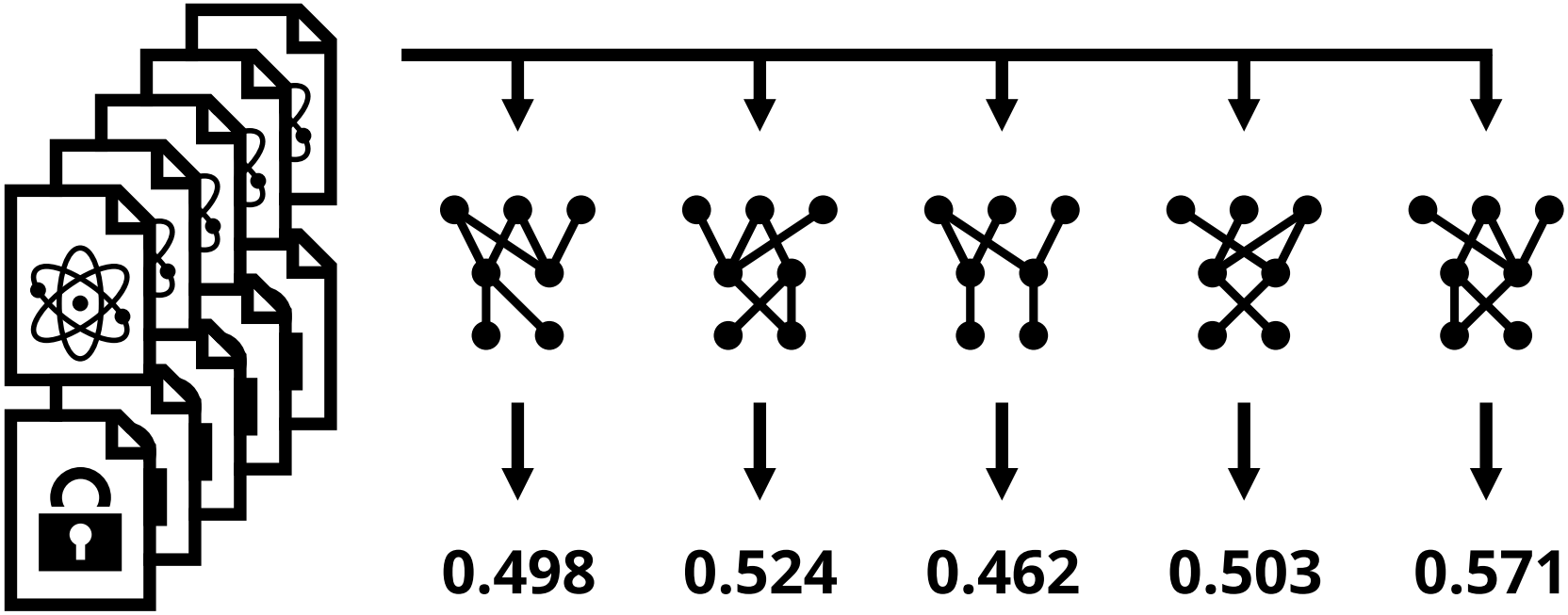
2. Test vector generation



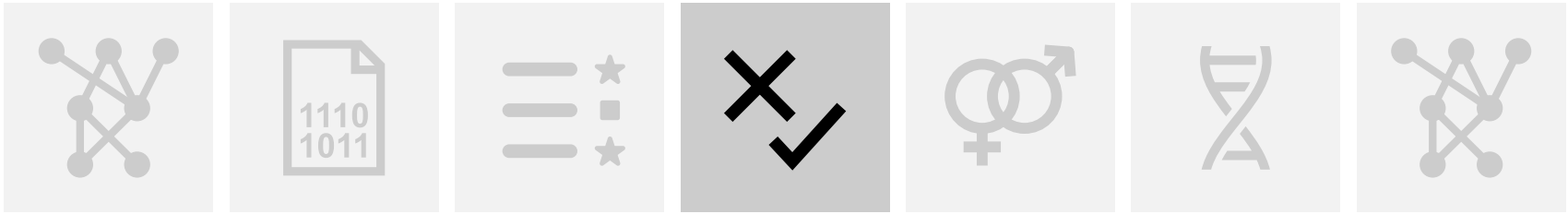


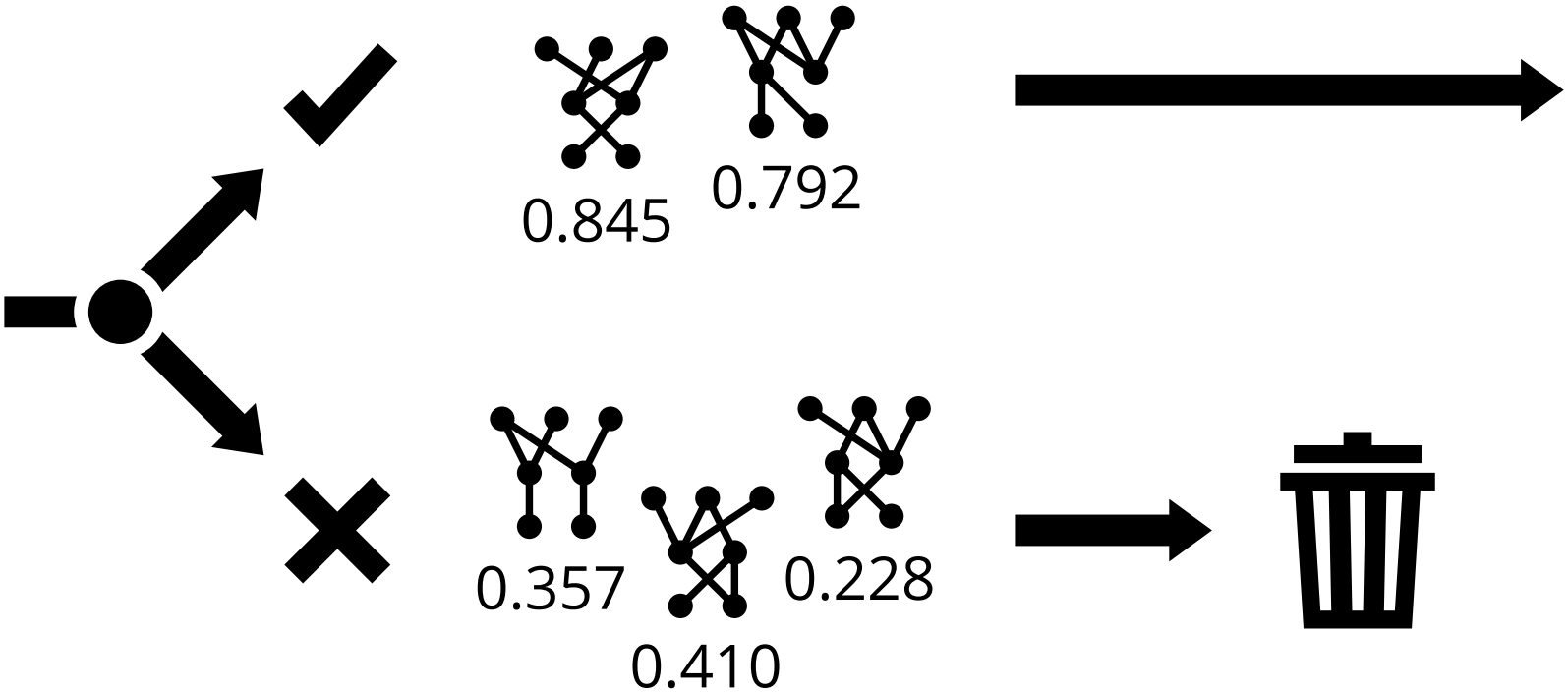
3. Evaluation



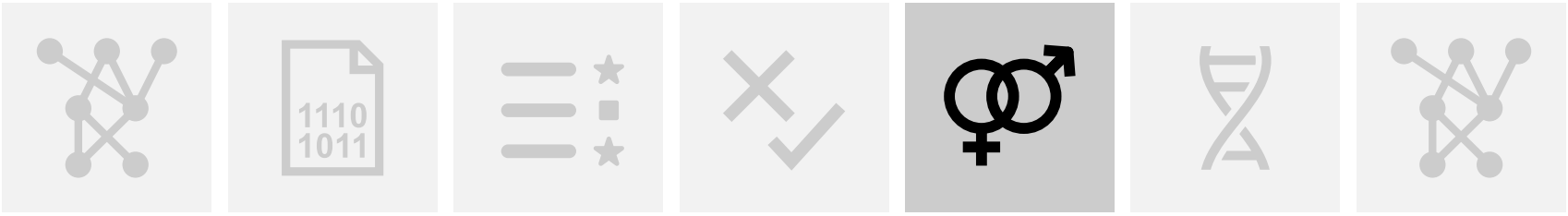


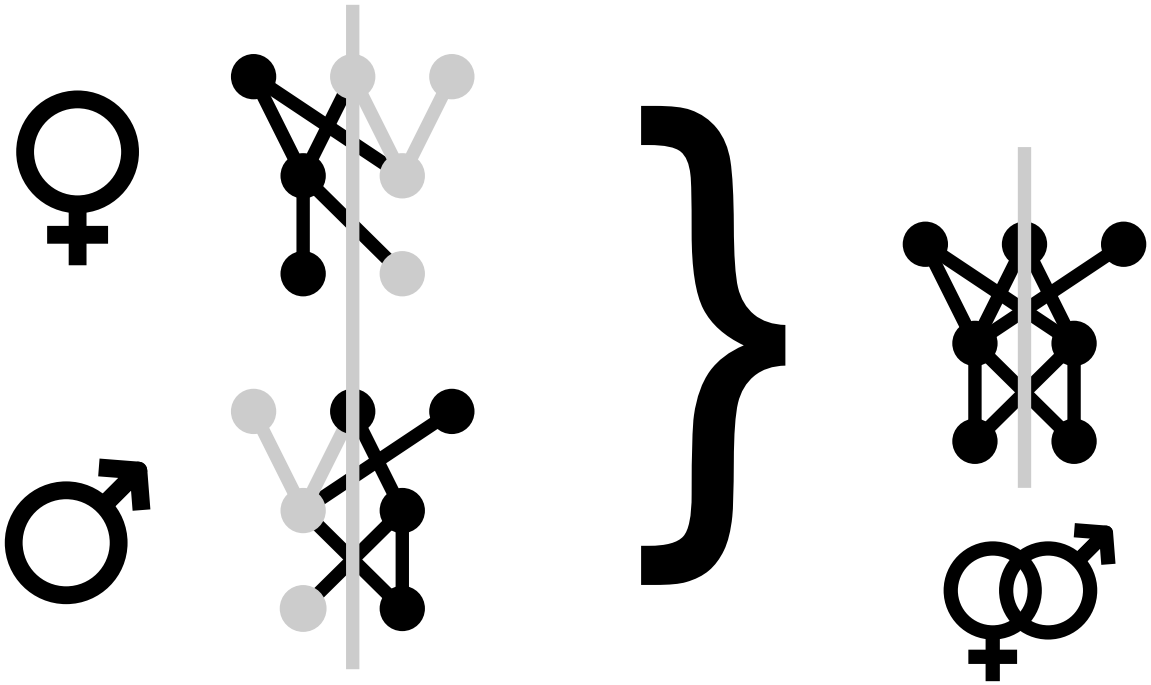
4. Survival of the fittest



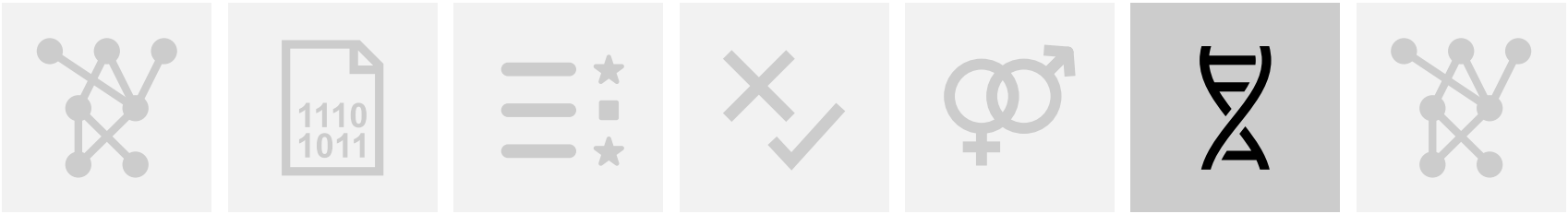


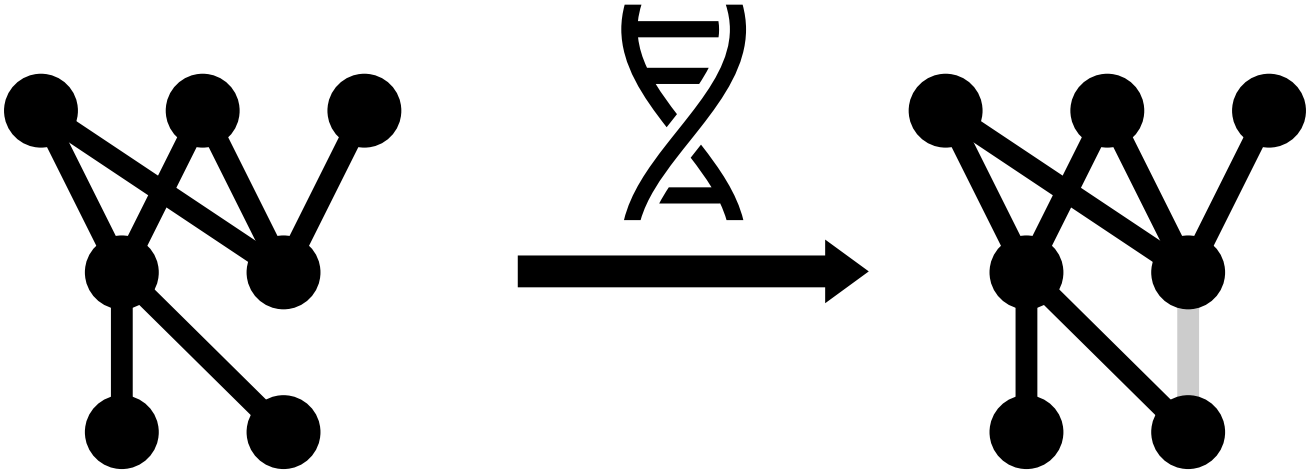
5. Sexual crossover (breeding)



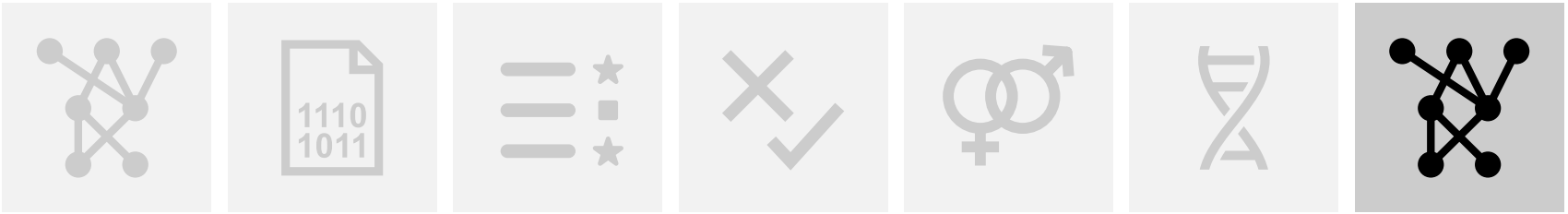


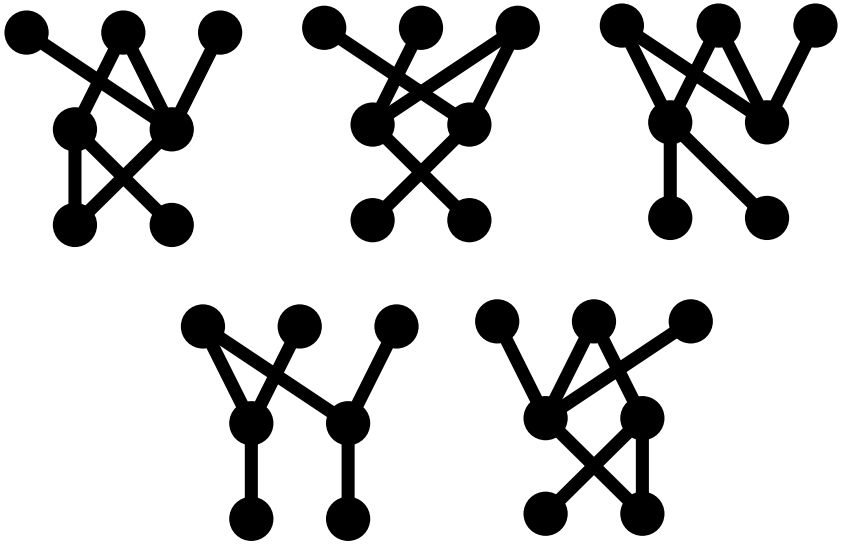
6. Mutation



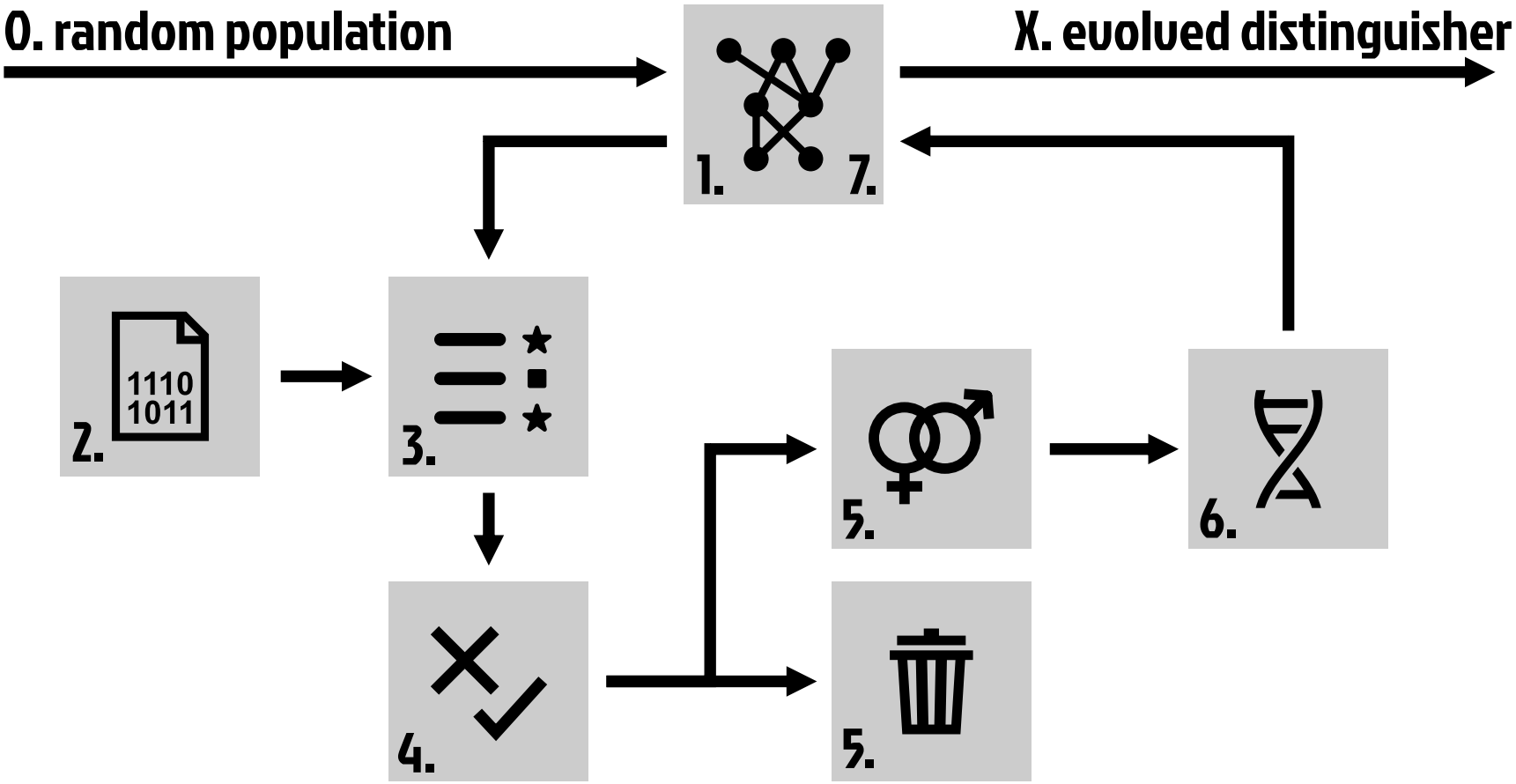


7. Repeat for another generation

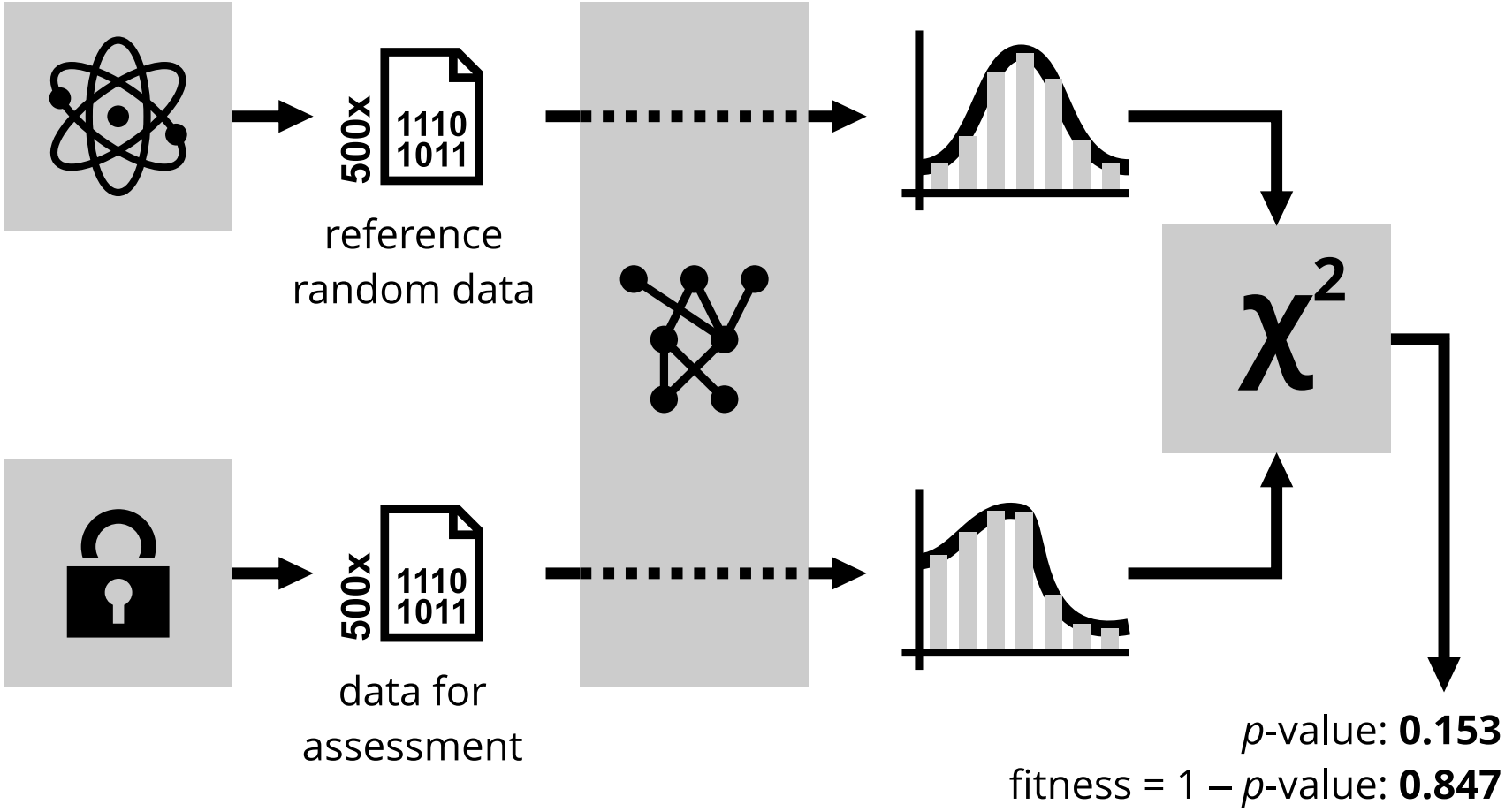




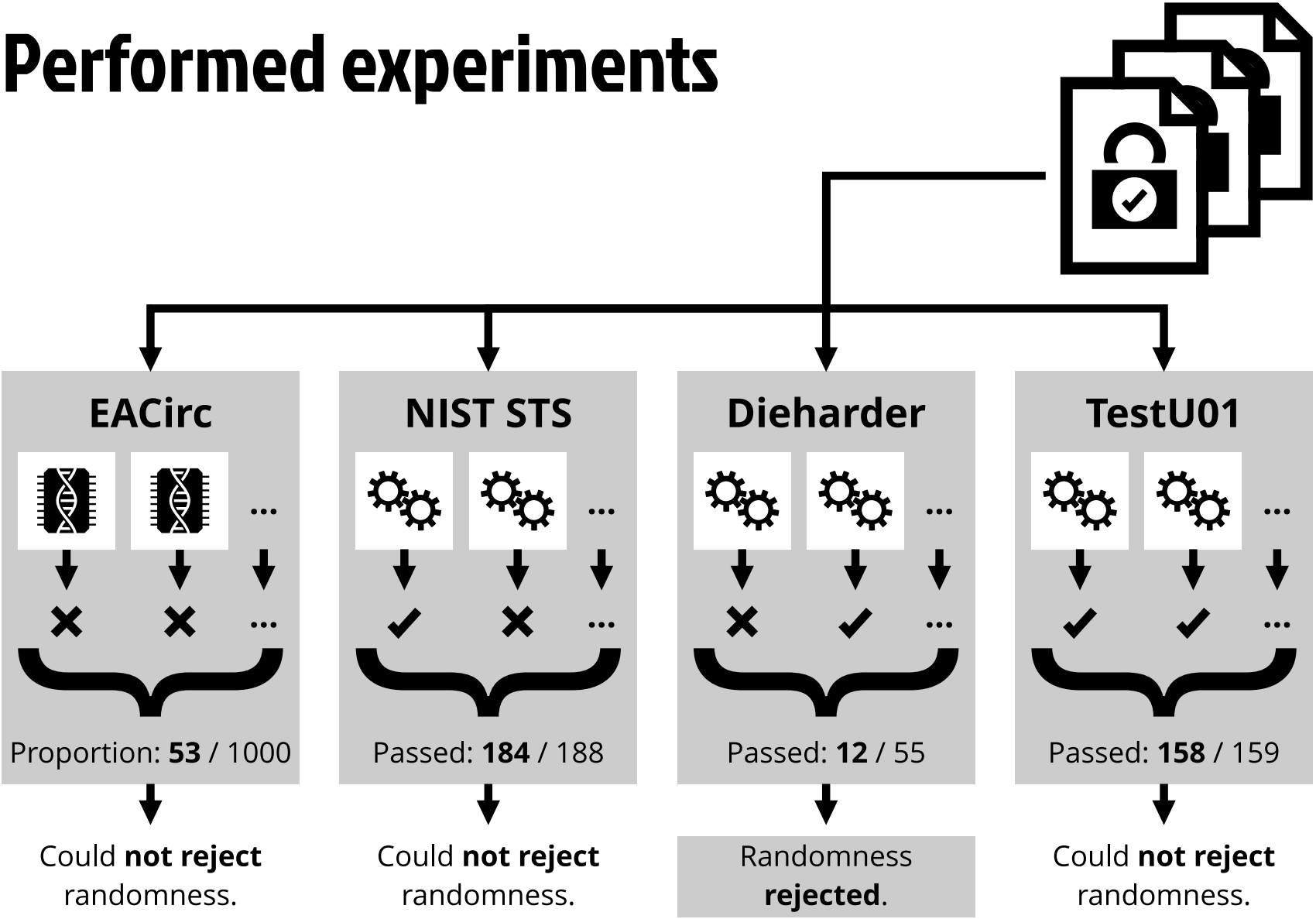
EACirc workflow summary



Fitness evaluation



Performed experiments



EACirc results interpretation

EACirc (run 1)

gen 1: fitness 0.495
gen 101: fitness 0.551
gen 201: fitness 0.601
... ... : ...
gen 30 001: fitness 0.998

Kologorov-Smirnov uniformity test
p-value: **0.008**

→ uniformity **rejected** (*p*-value < α)

EACirc (run 2)

K-S test
p-value: **0.267**

→ uniformity **not rejected**

...

...

...

EACirc (run 1000)

K-S test
p-value: **0.003**

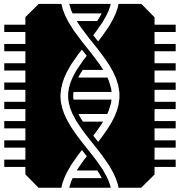
→ uniformity **rejected**

proportion of rejected runs: **13/1000**

↓

experiment outcome: **randomness not rejected**

Results summary



EACirc (vs. statistical batteries)

- adaptable tests
- inspecting short independent subsequences

Published results

- 7 round-limited eStream candidates

  better than NIST STS: Hermes(2), Fubuki (1)

  promising cases: LEX (4), TSC-4 (12)

- 18 round-limited SHA-3 candidates

  comparable to NIST STS

- 52 CAESAR candidates (168 variants)

  falling behind NIST STS

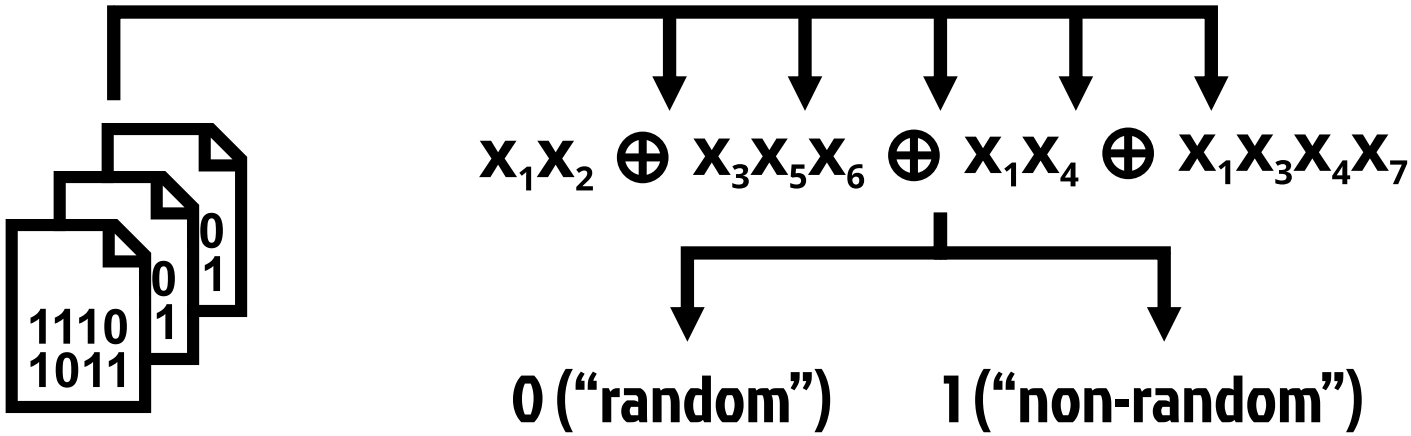
CAESAR candidates assesment

CAESAR candidates	randomness tests				
	NIST STS	Diehard	Dieharder	TestU01	EACirc
Keyak	✓	✓	✗	✓	✓
Prøst	✓	✓	✓	✓	✓
π-Cipher	✗	✓	✗	✓	✗
TriviA-ck	✓	✓	✓	✓	✓
...	...	...	...	...	...

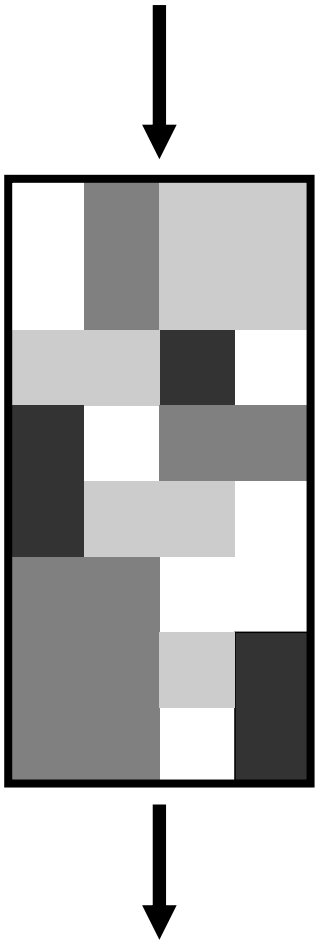
Alternative representation (ANF)

Individuals in Algebraic normal form

- exclusive or of multiple terms (XOR of ANDs)
- simpler form than software-emulated circuits
- easier interpretation, faster
- may limit expressivity



Function decomposition (”heatmap”)



Motivation

- better interpretation of results
- give function designers feedback on their design

Realization

- try “turning off” different parts of the function
- test each version (What blocks are essential?)
- preliminary results on Tangle, Decim, DSHA-2

GAČR grant MU & BUT [2016-2018]

WP I. [Q1–Q3/2016]

- tweak EACirc
- tweak evolution (operators & parameters)

WP II. [Q3/2016–Q3/2017]

- alternative representation (ANF)
- function decomposition (”heatmap”)

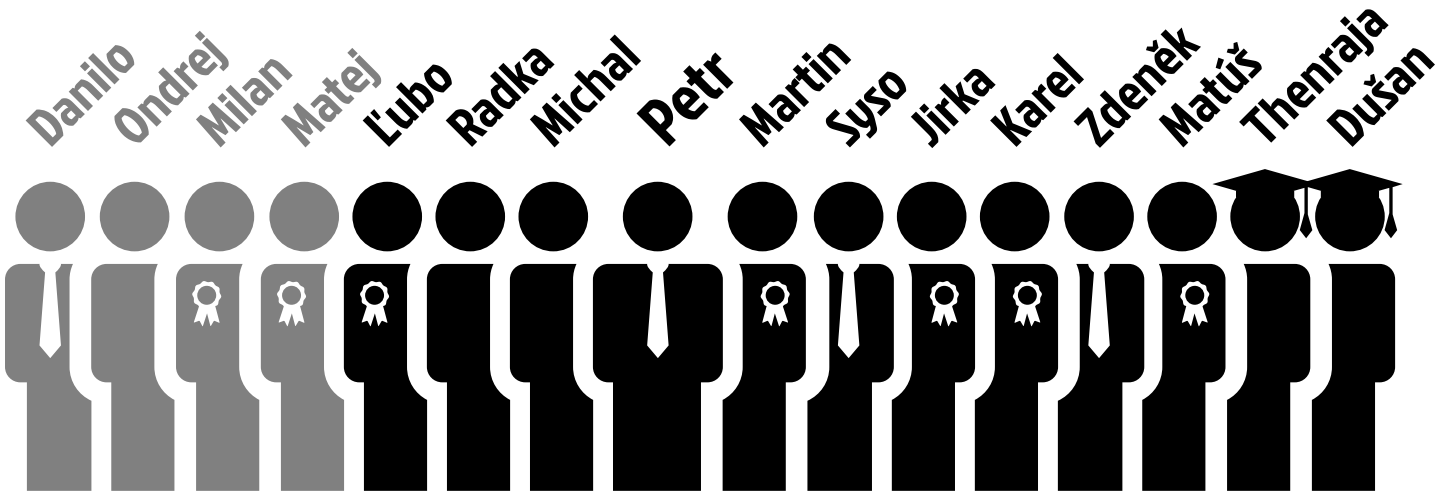
WP III. [Q3/2017–Q4/2018]

- custom FPGA accelerator
- application to cryptoprimitives

The EACirc project

Published results so far

- 4 conference papers, 1 book chapter
- 2 master theses, 4 bachelor theses
- 2 SantaCrypt presentations, EGI brochure feature



Thank you!

Questions are welcome.

EACirc

Fork me on GitHub!
github.com/crocs-muni/EACirc