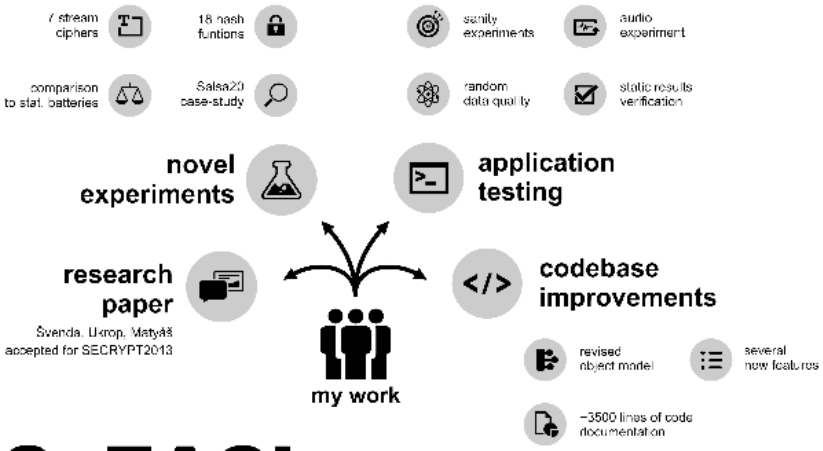
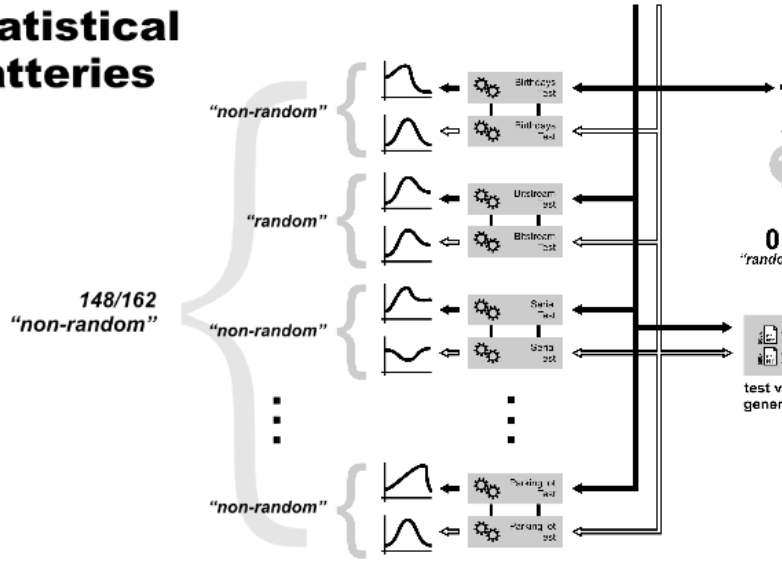
Martin Ukrop
(bachelor thesis)

icons from
The Noun Project

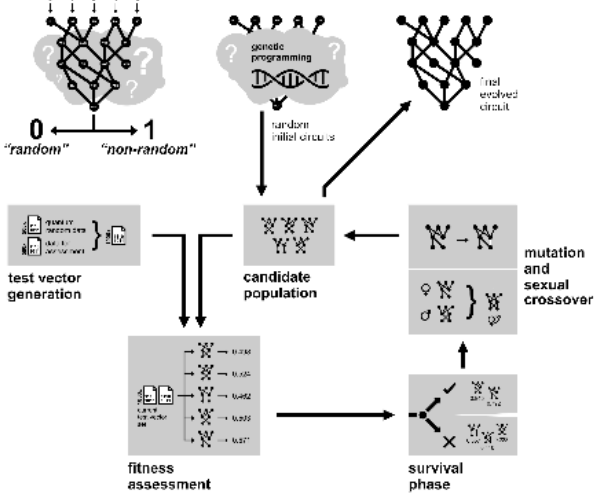
How to distinguish random and non-random data?



1. statistical batteries

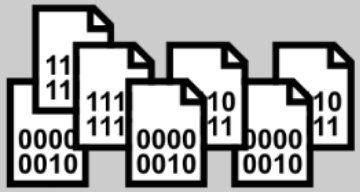


2. EACirc



How to distinguish random and non-random data?

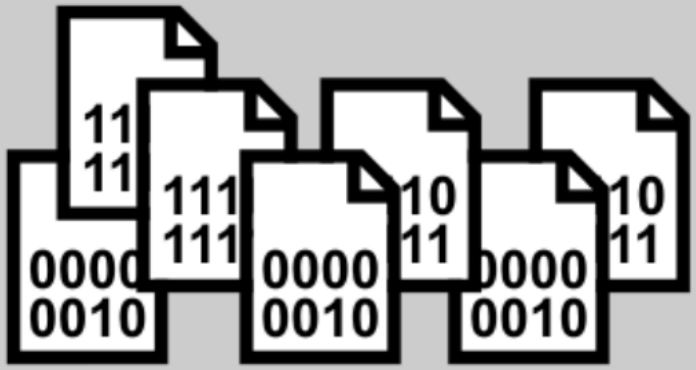
assessed data



referential truly random data

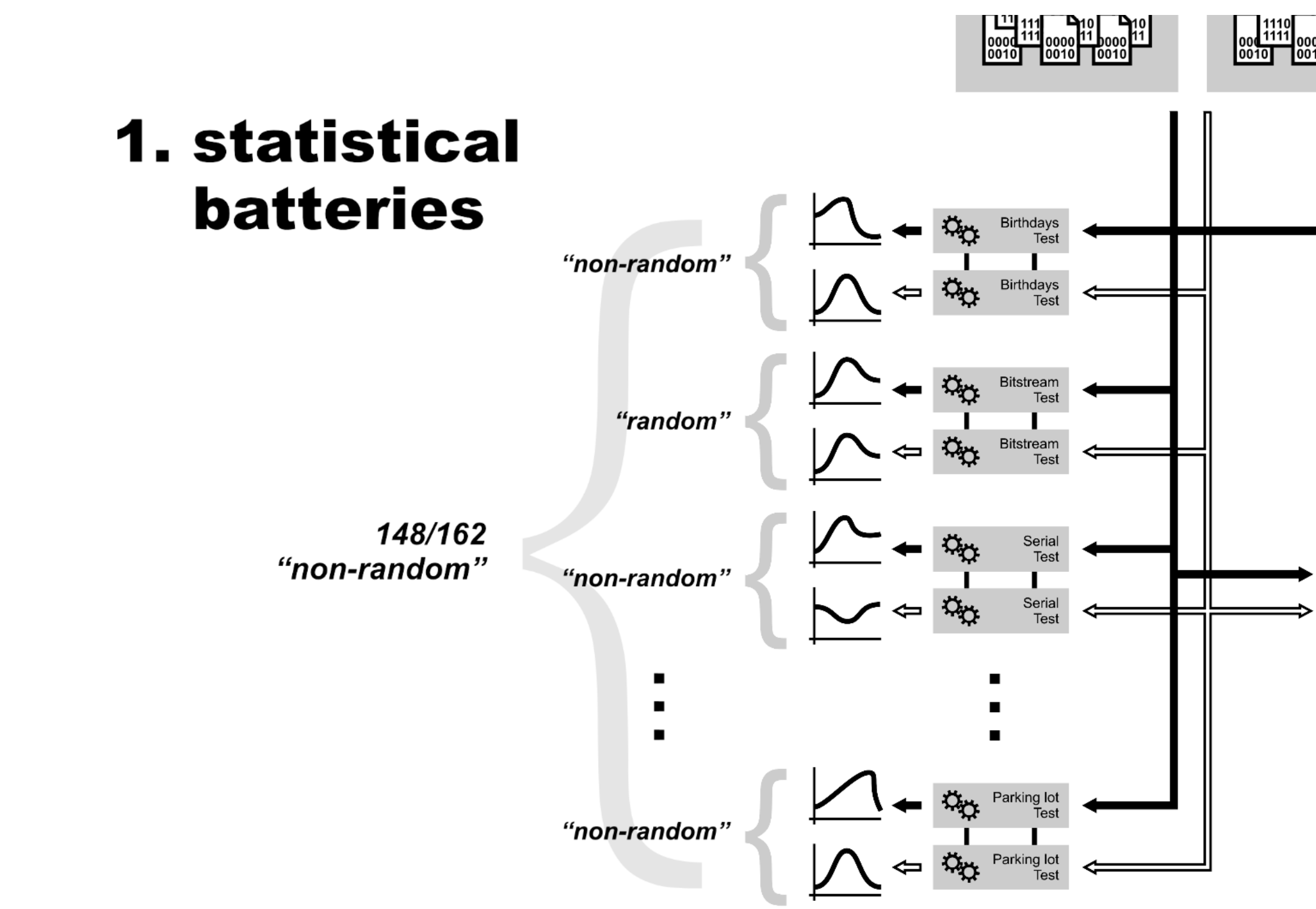
random

assessed data

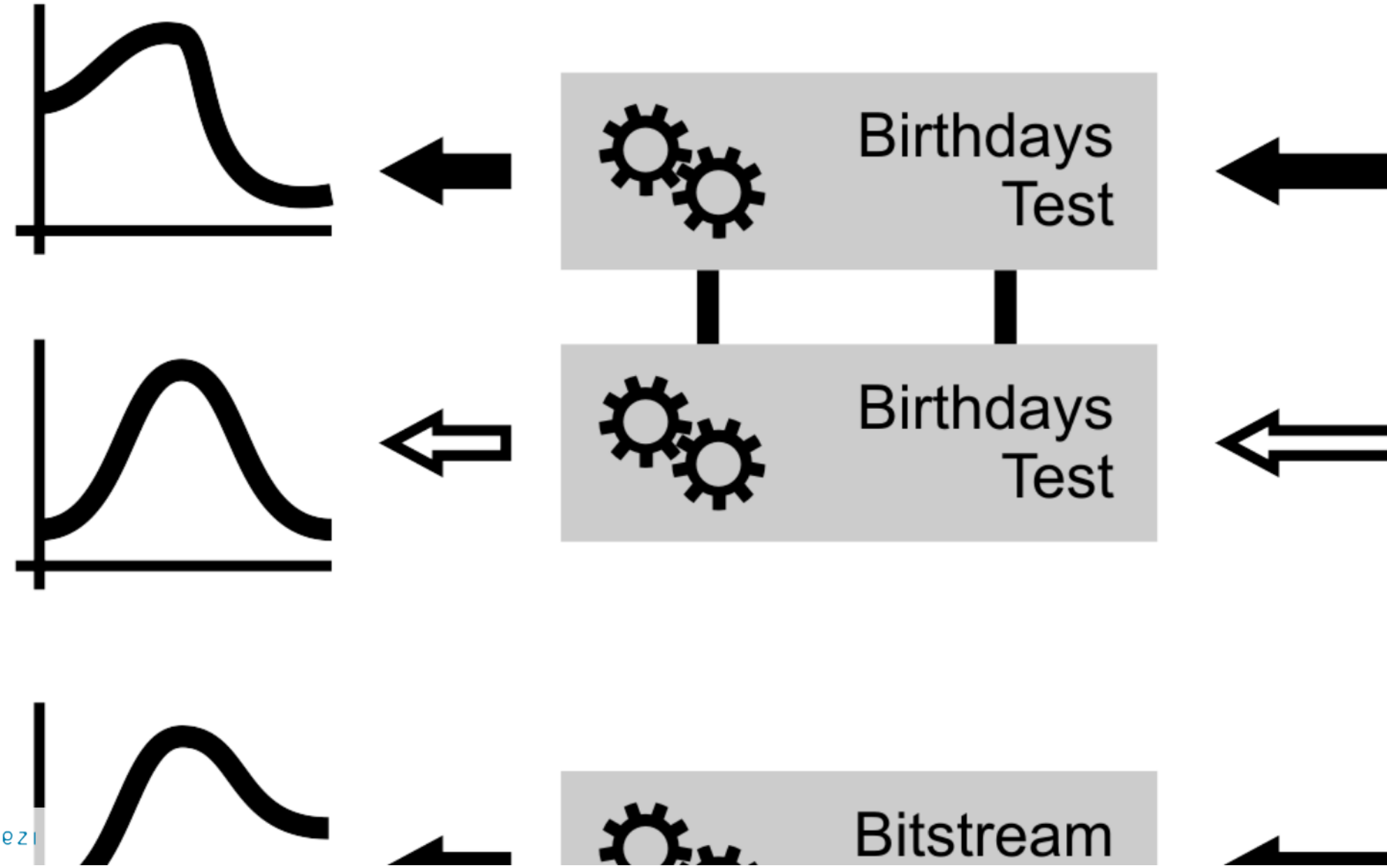


referential truly random data

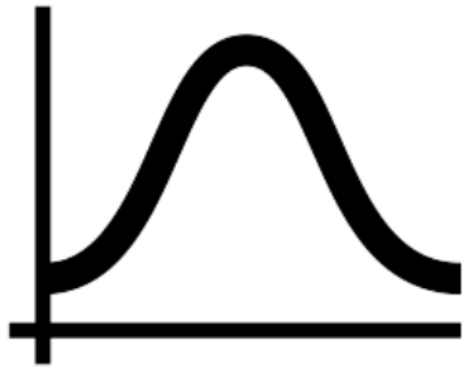
1. statistical batteries

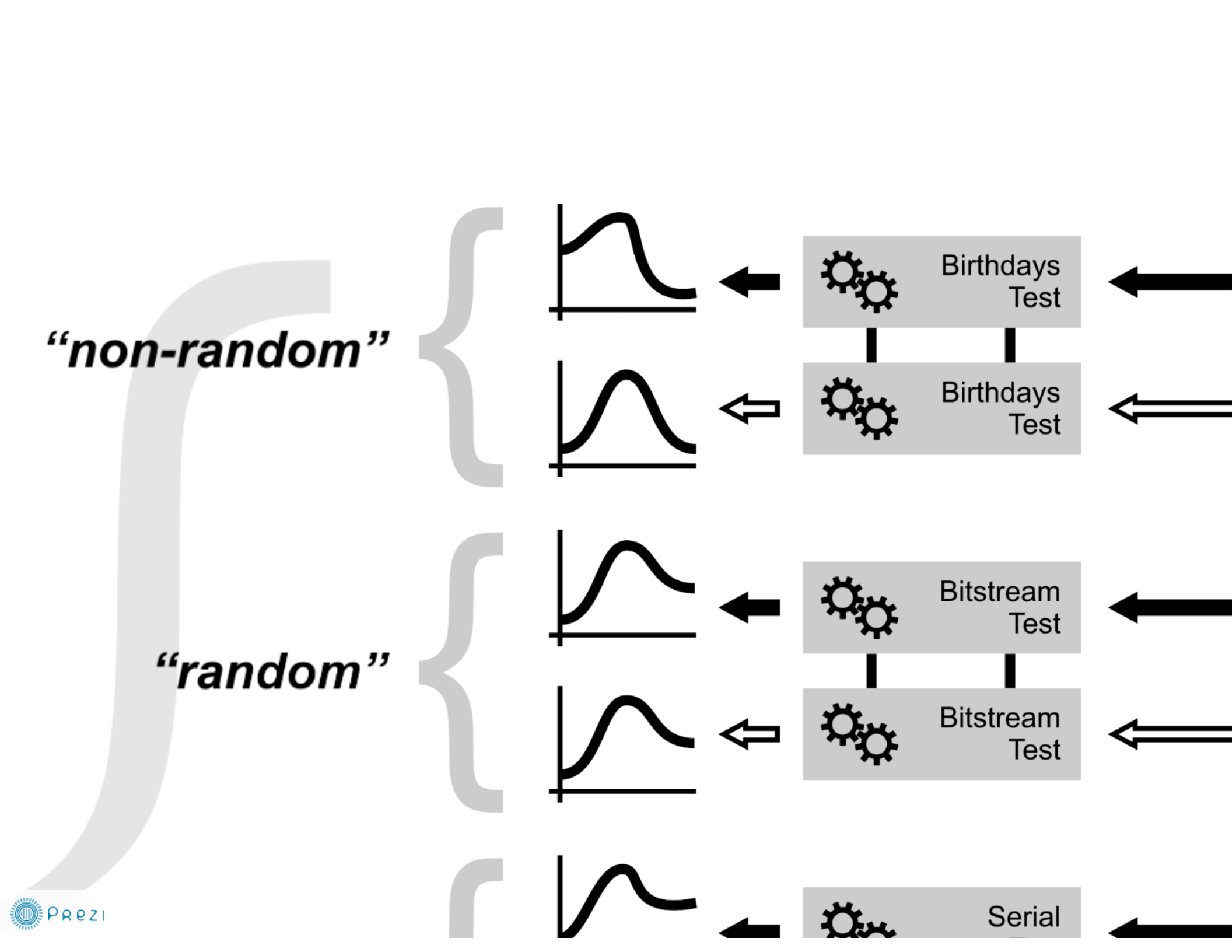


148/162
"non-random"

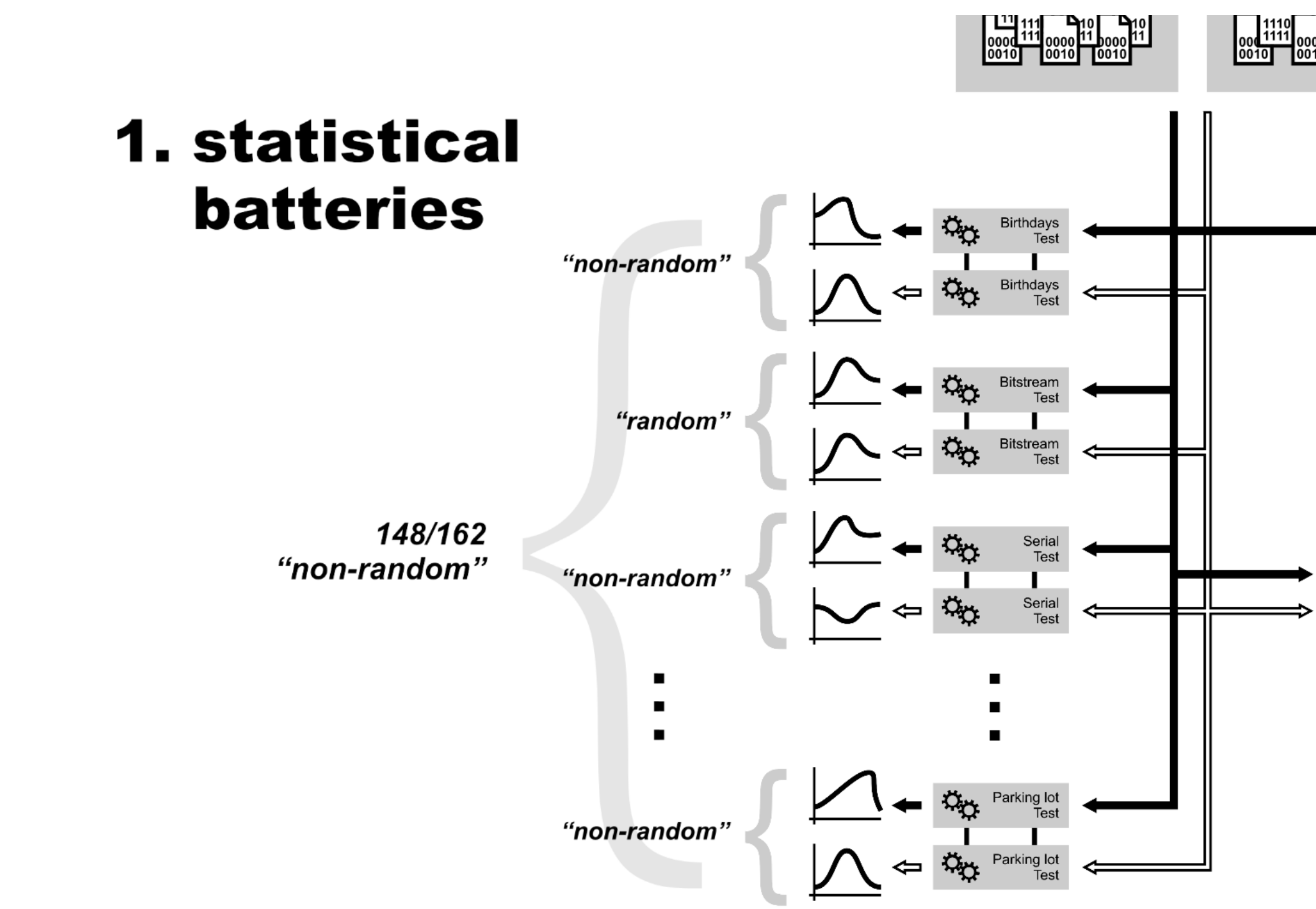

Birthdays
Test
Birthdays
Test
Bitstream

“non-random”



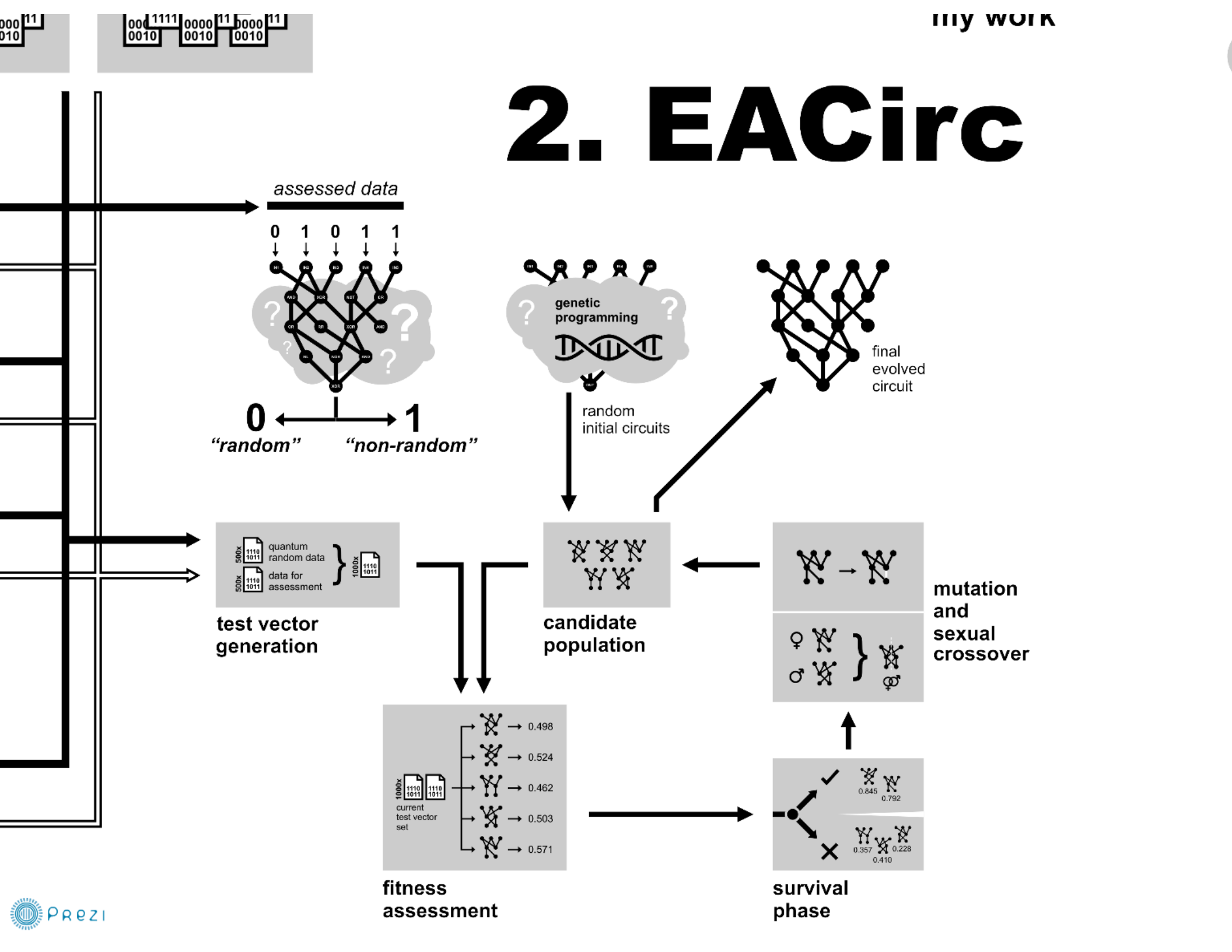

"non-random"
"random"
Birthdays Test
Birthdays Test
Bitstream Test
Bitstream Test
Serial

1. statistical batteries

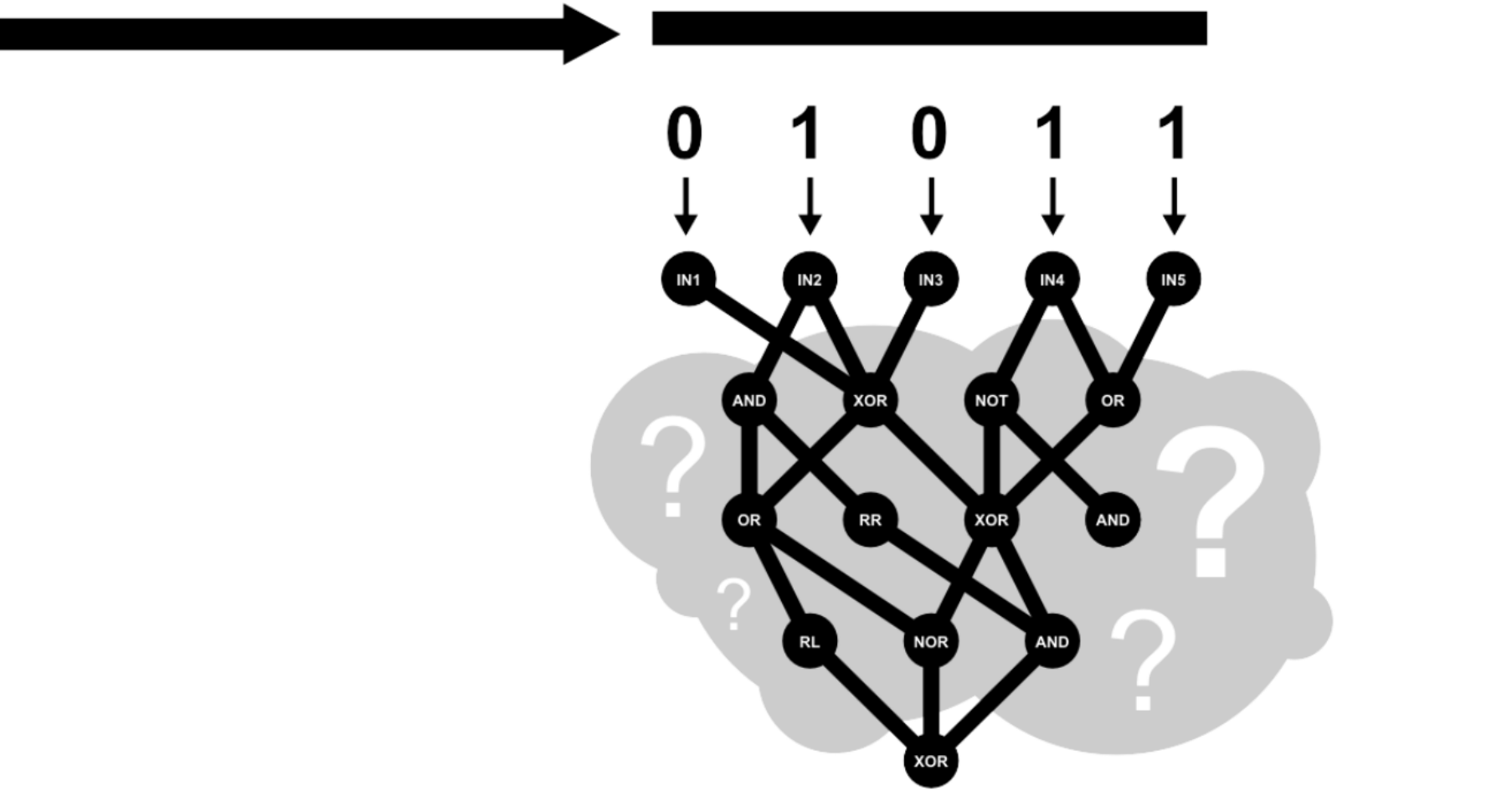


148/162
"non-random"

2. EACirc

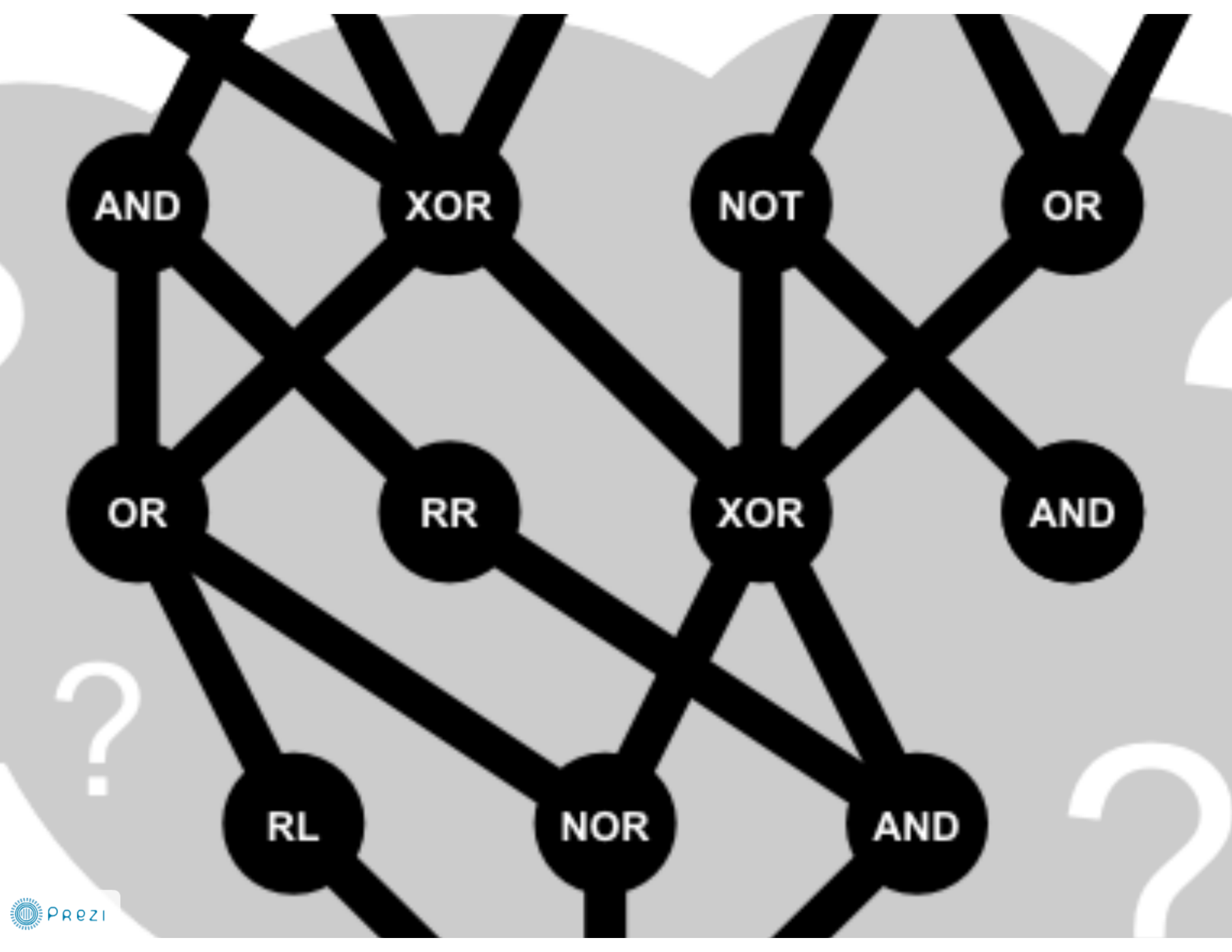


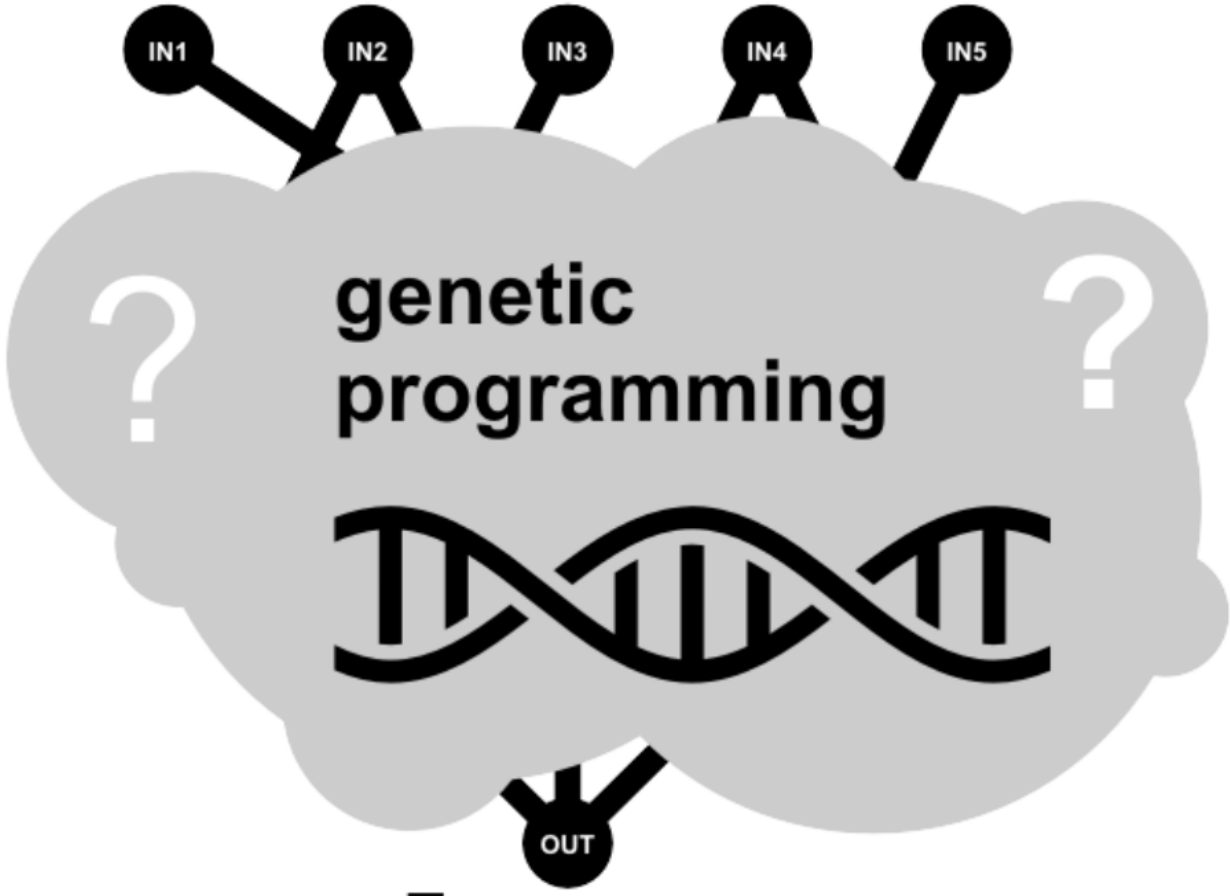
assessed data



0 **1**

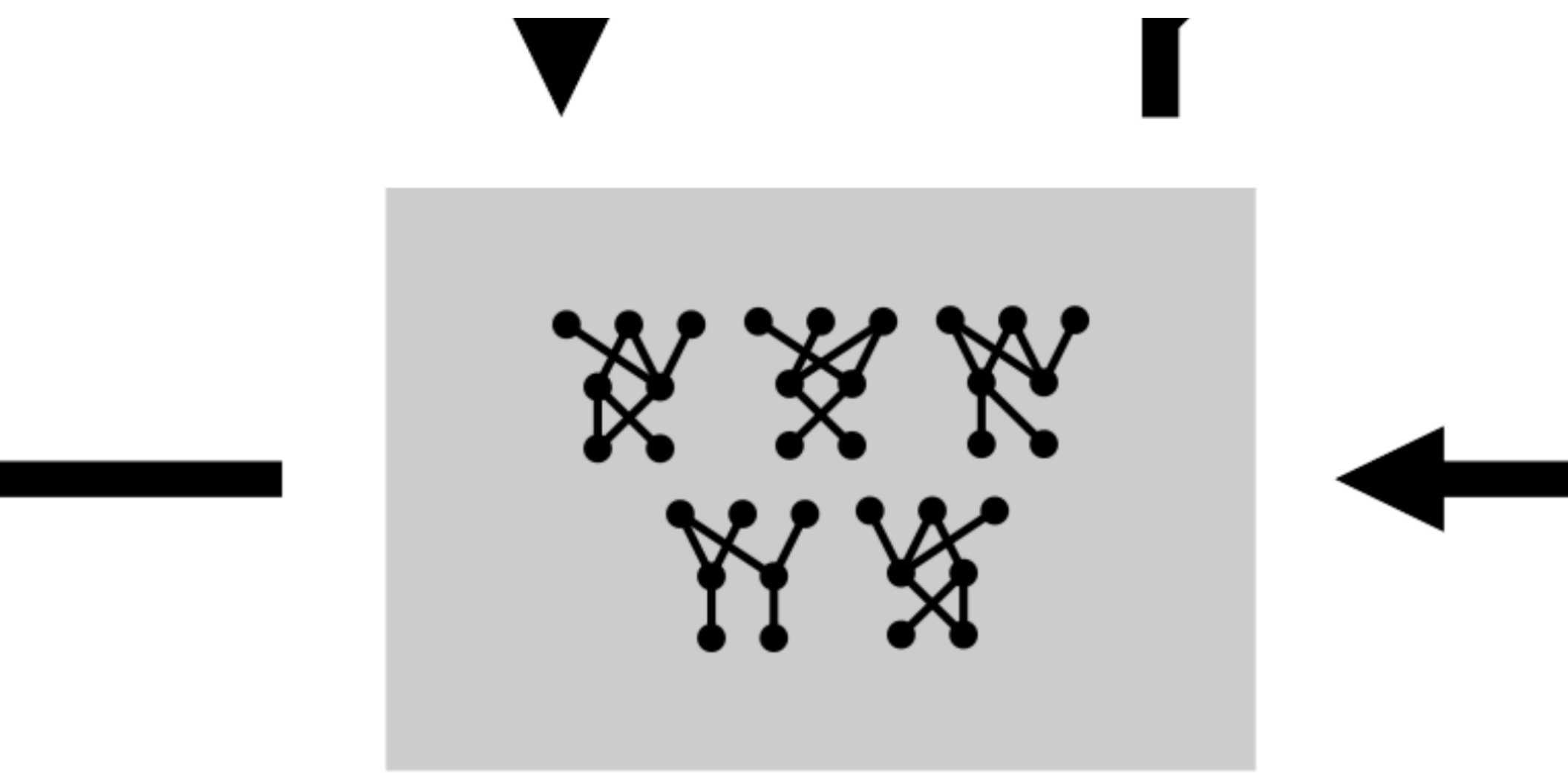
"random" ***"non-random"***


AND
XOR
NOT
OR
OR
RR
XOR
AND
RL
NOR
AND

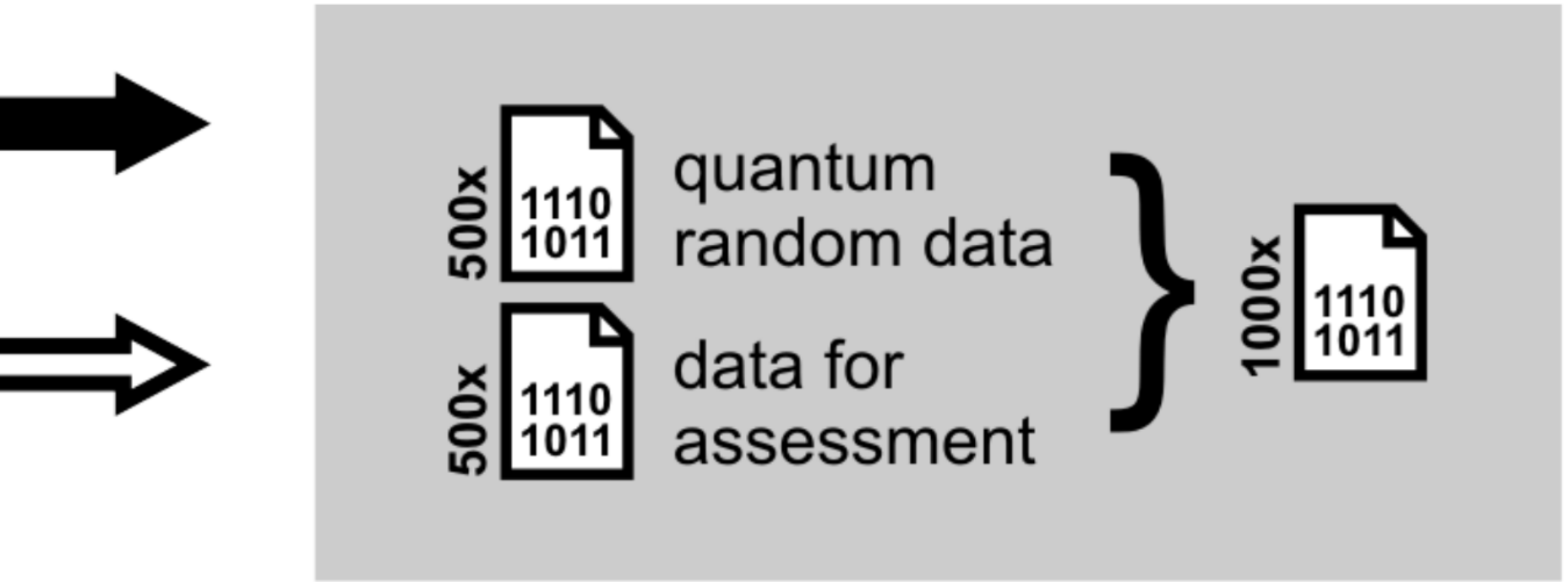


random
initial circuits

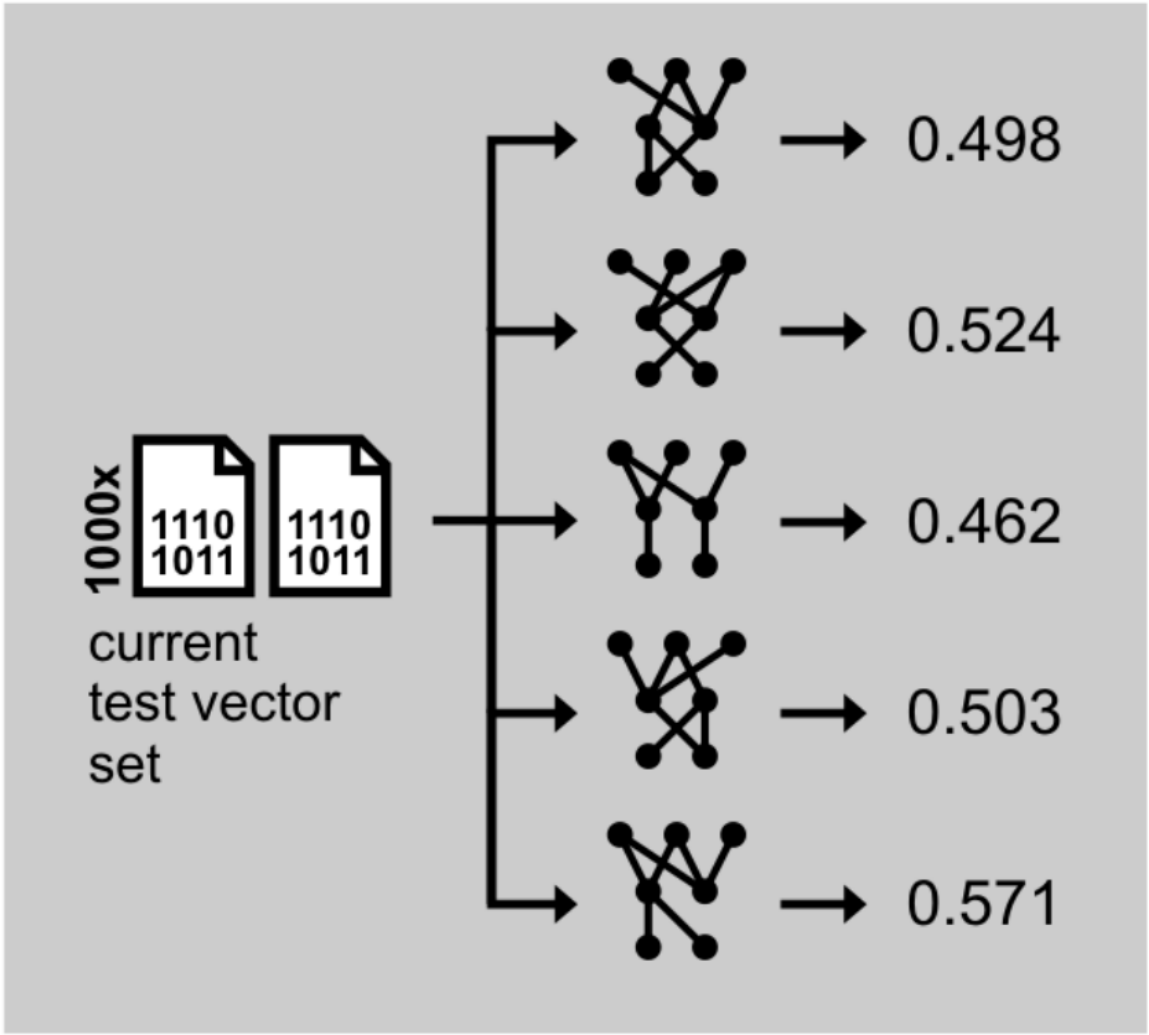
om”



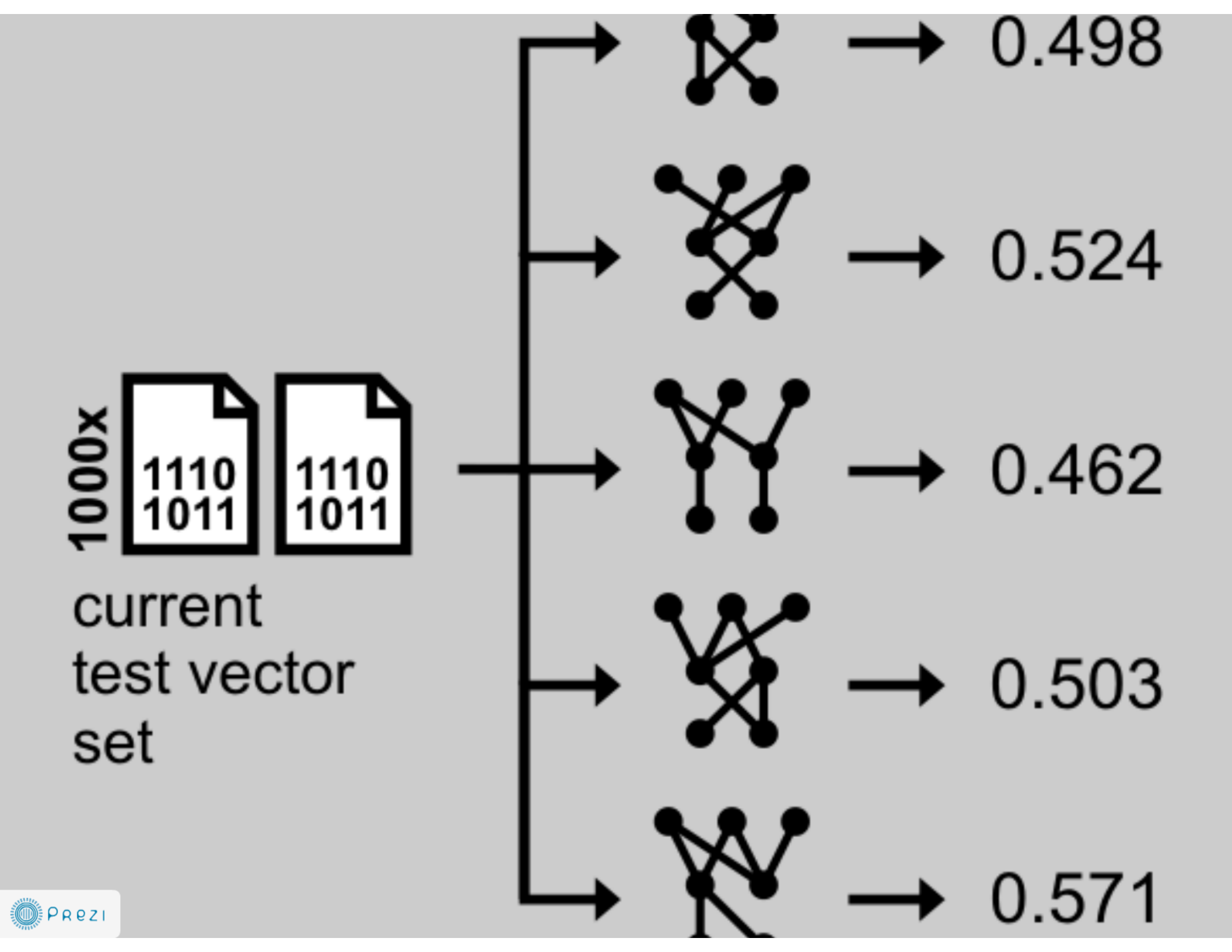
candidate population

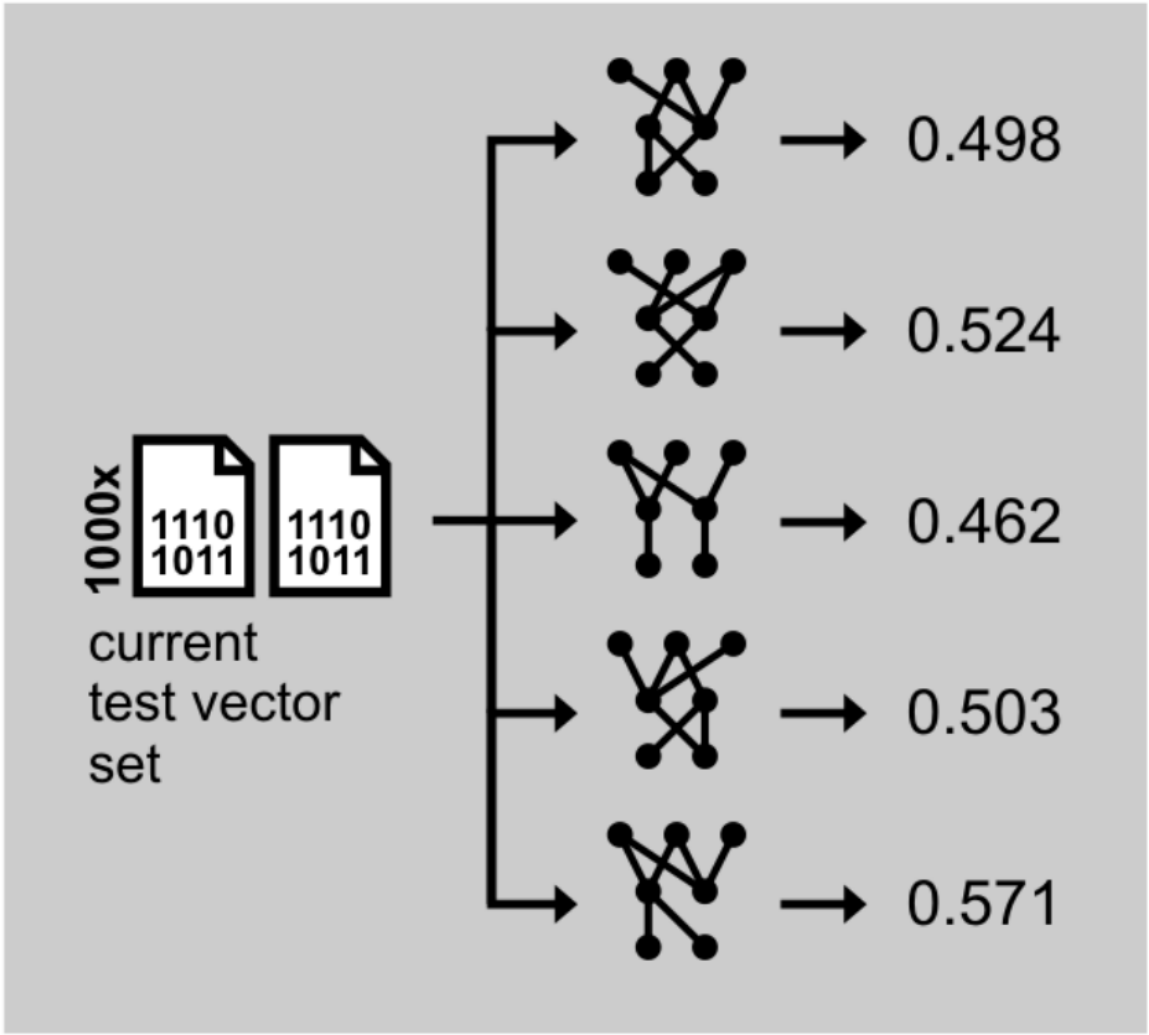


test vector generation

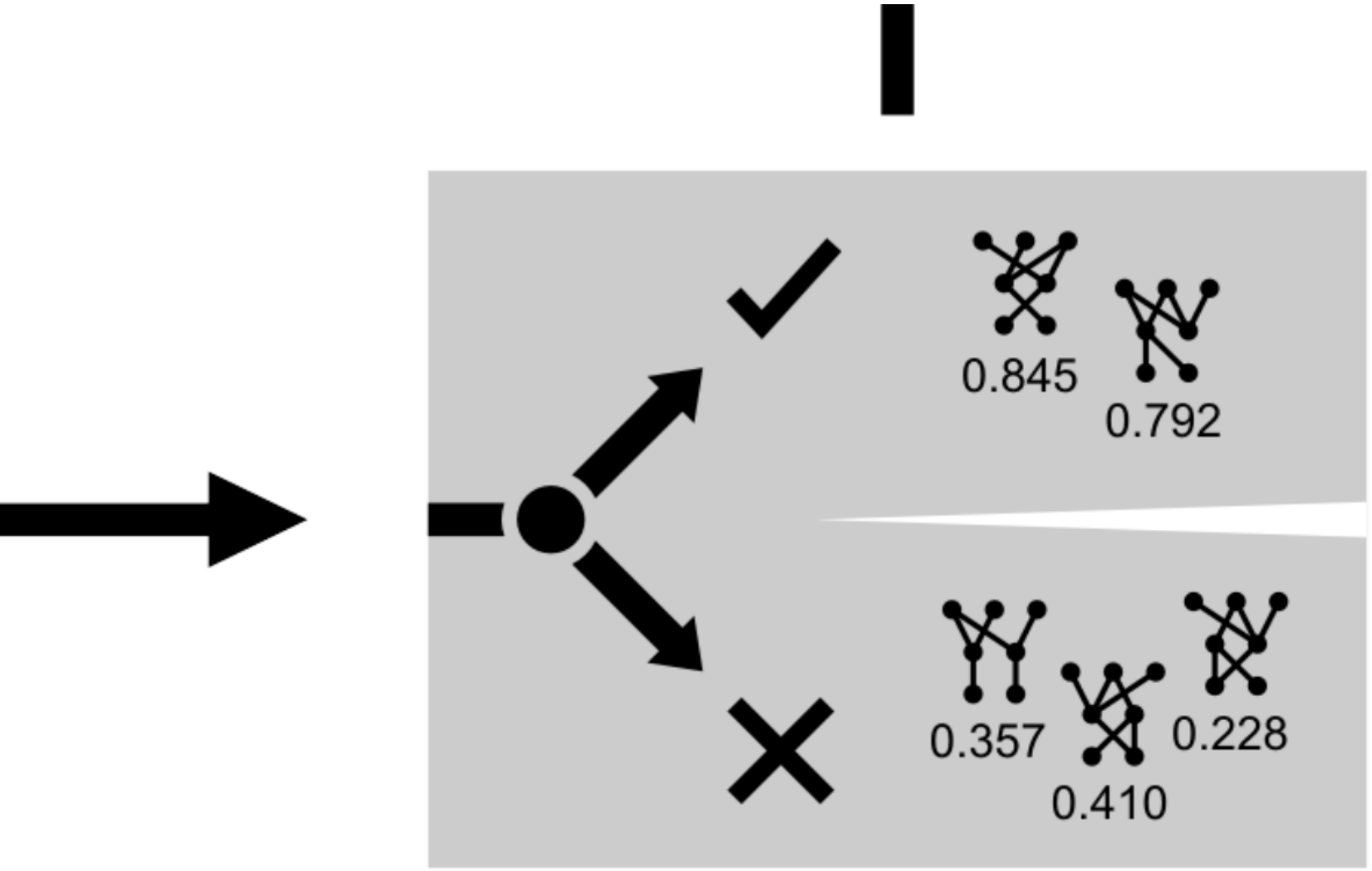


fitness assessment

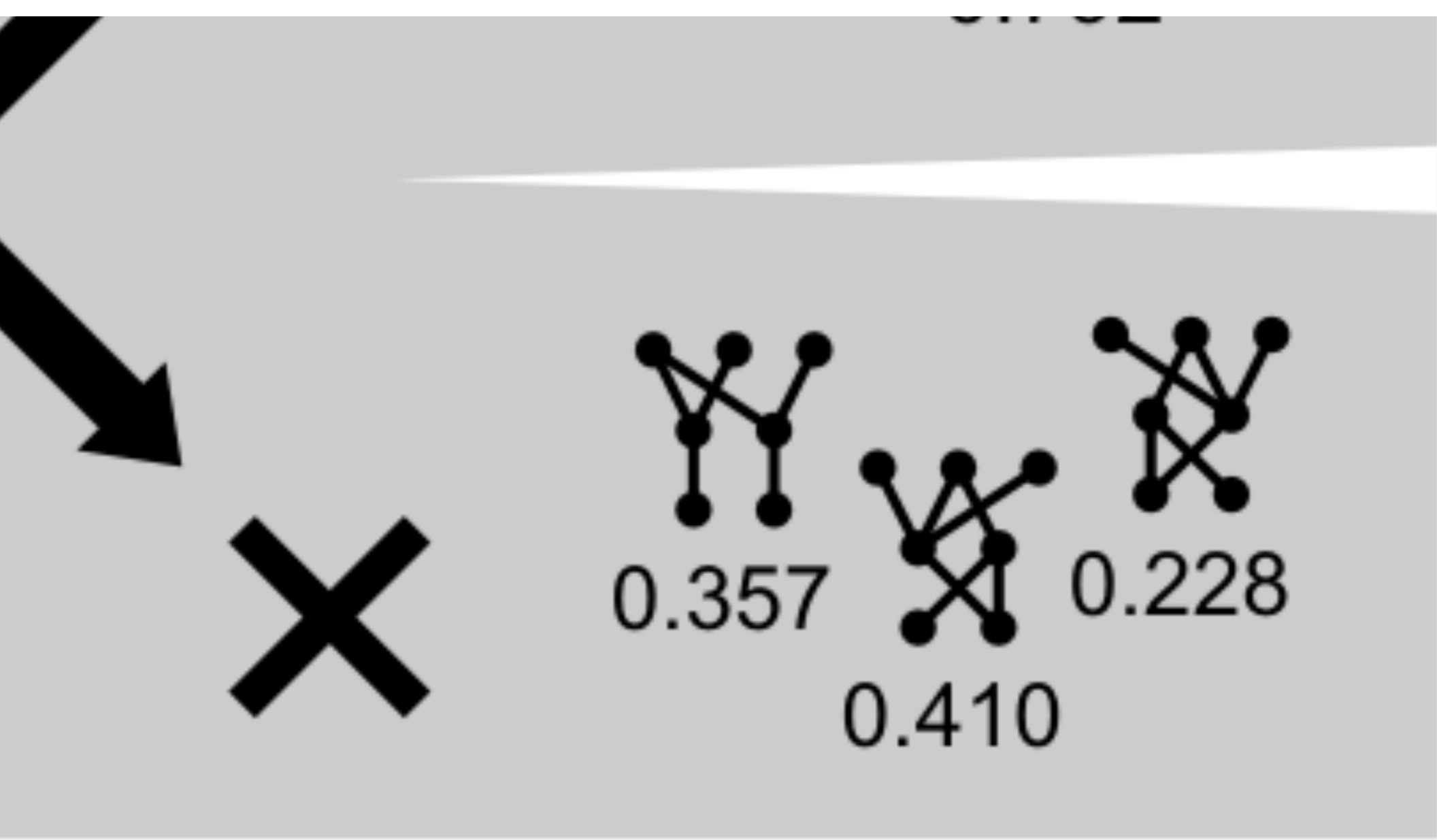

1000x
1110
1011
1110
1011
current
test vector
set
0.498
0.524
0.462
0.503
0.571



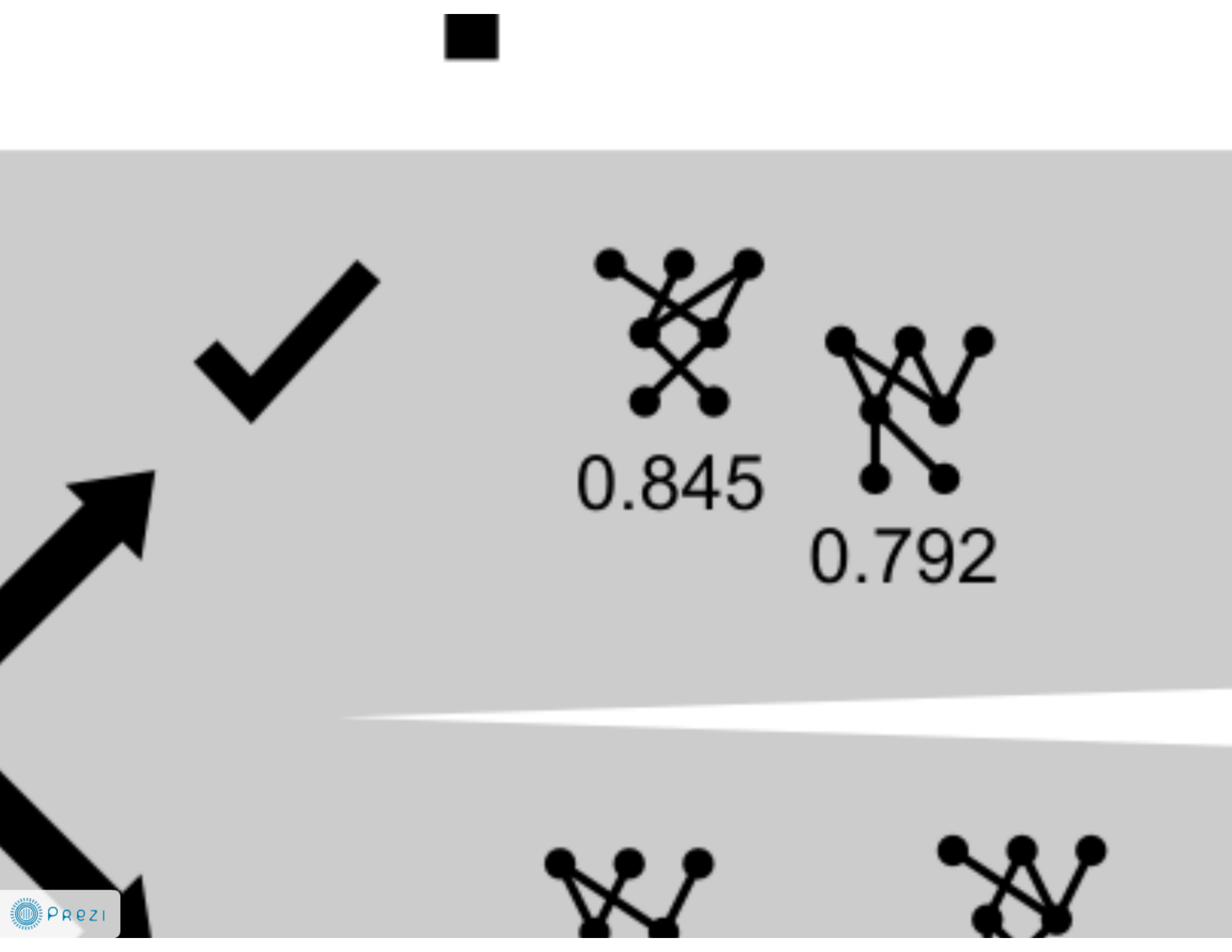
fitness assessment

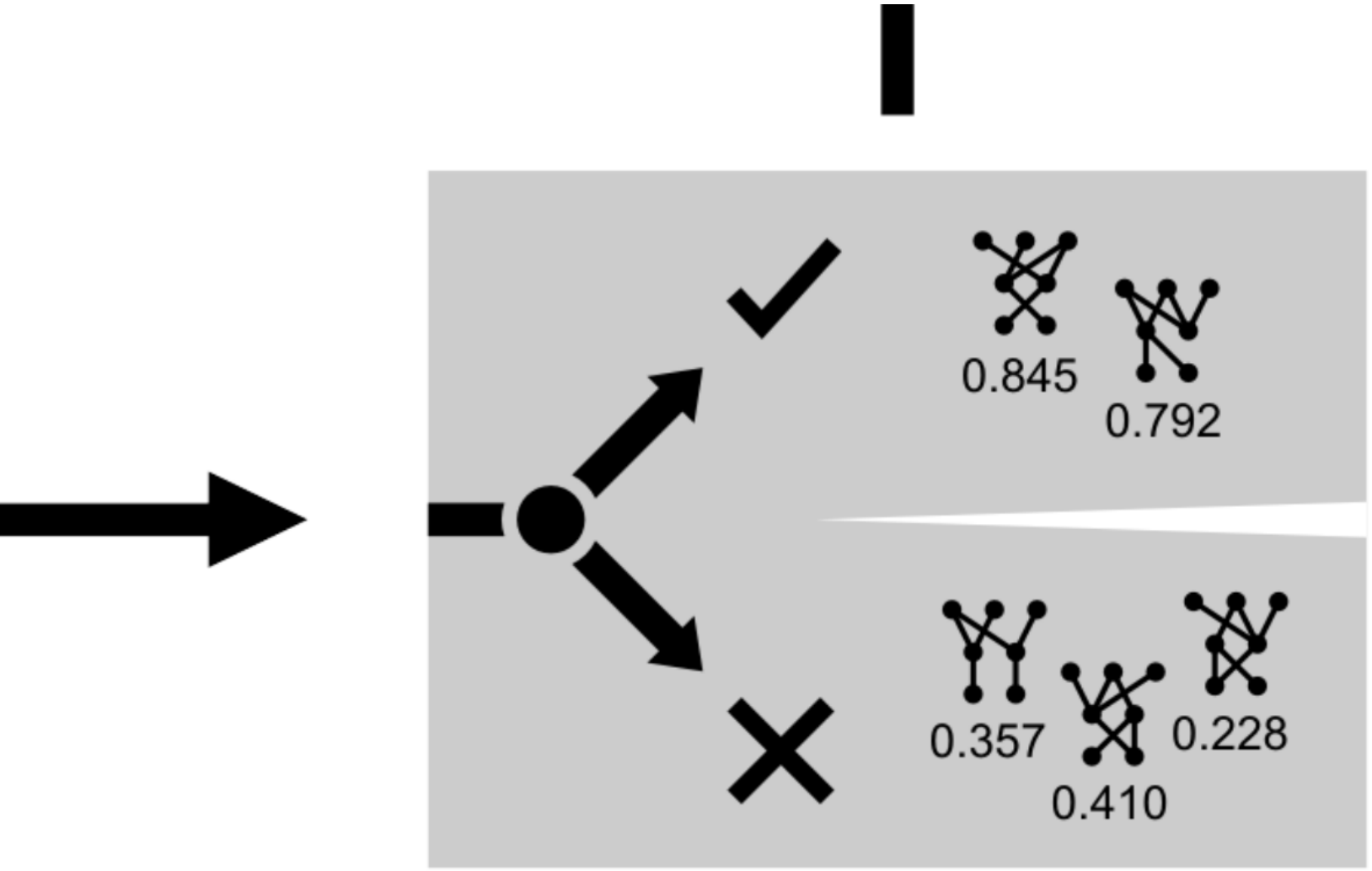


survival phase

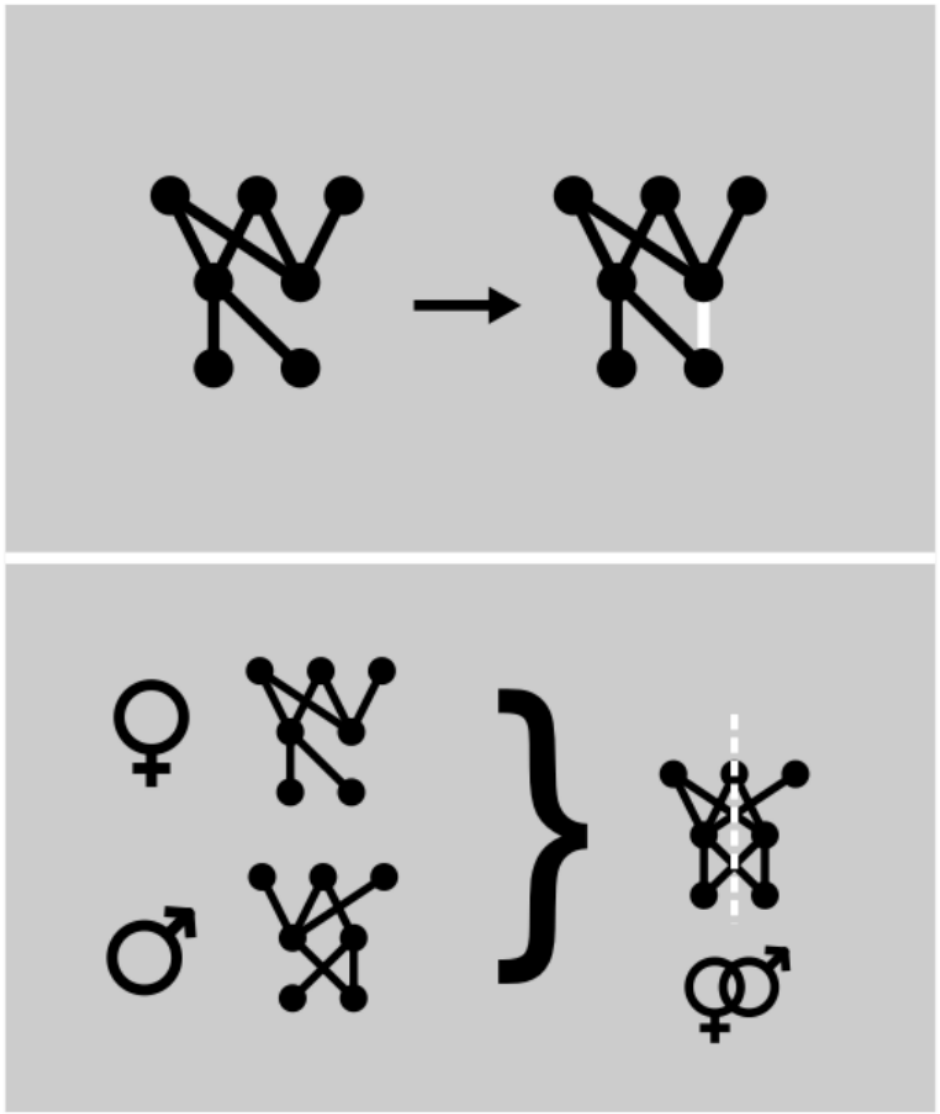


rvival

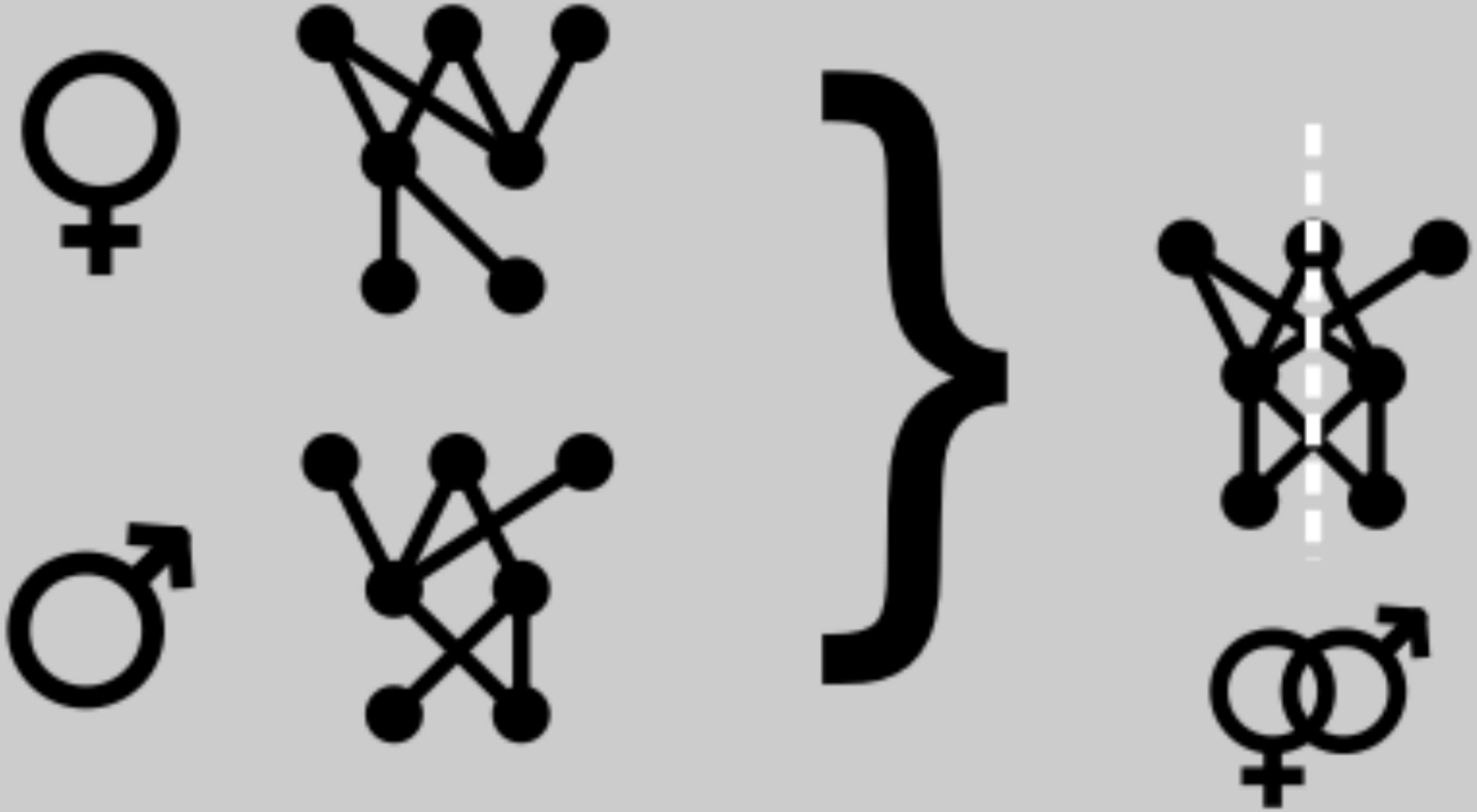

0.845
0.792

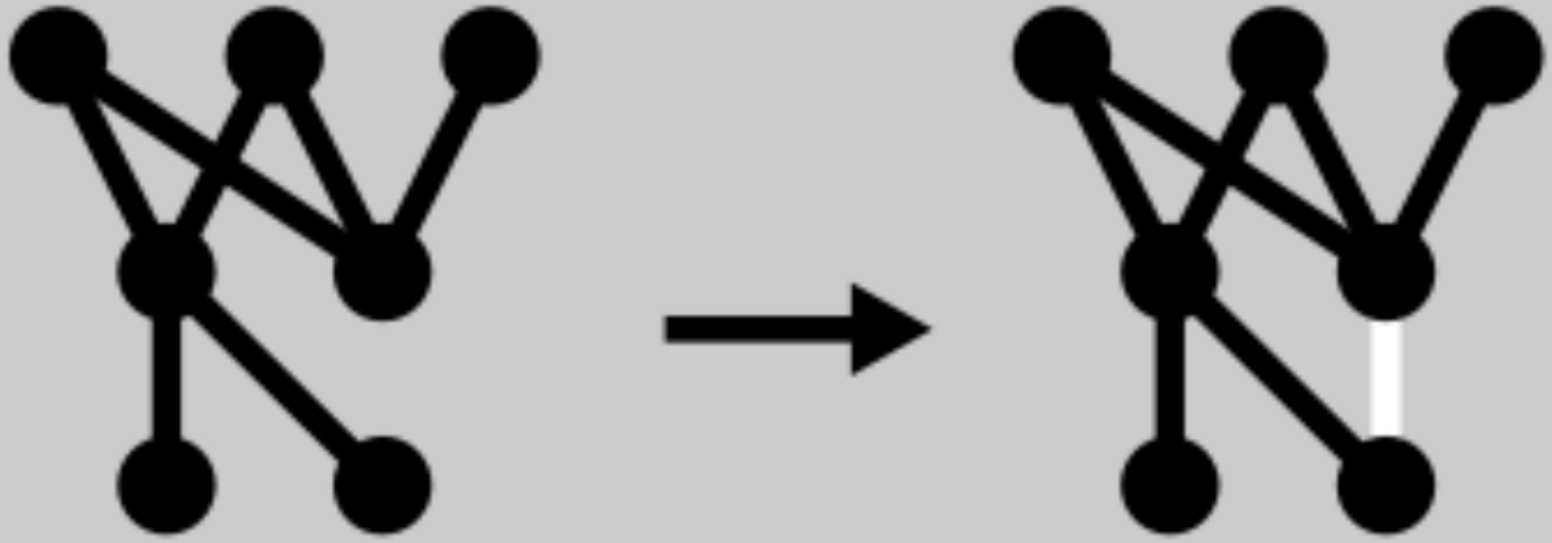


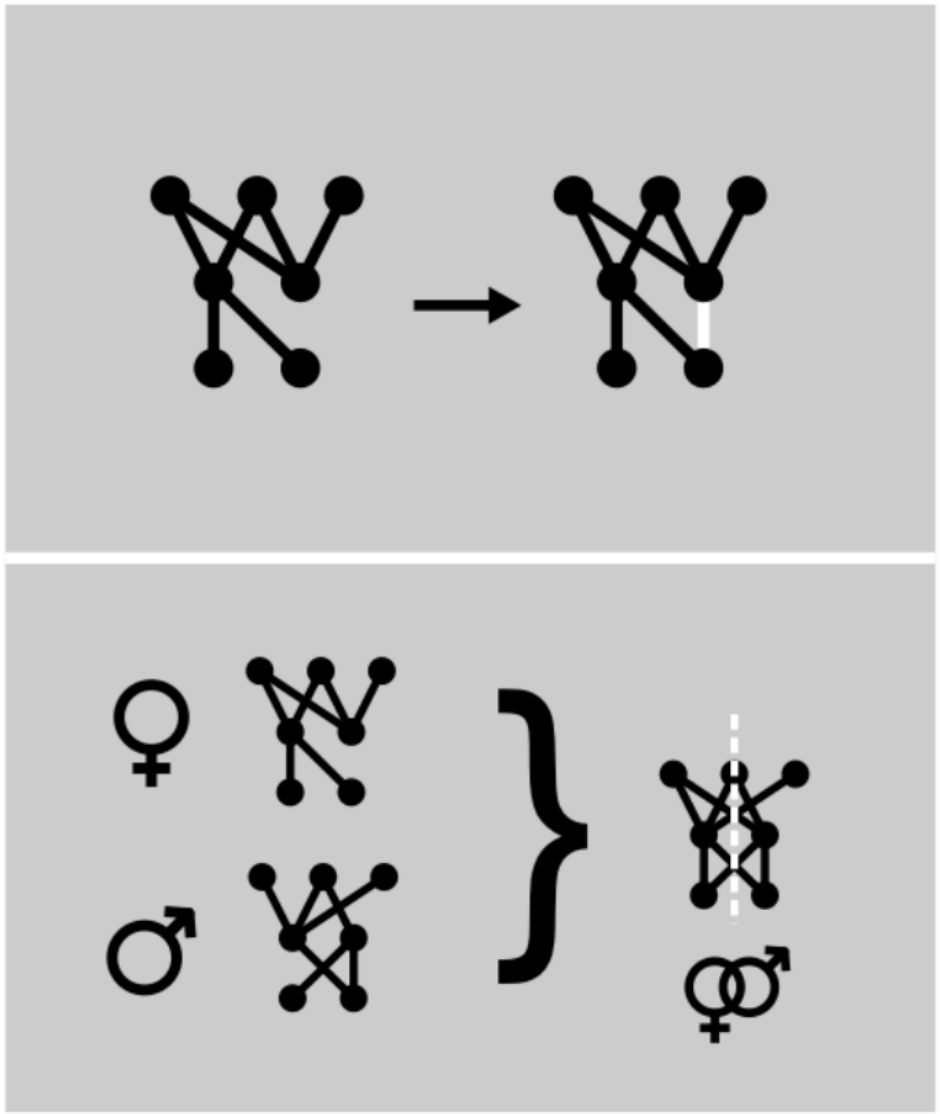
survival phase



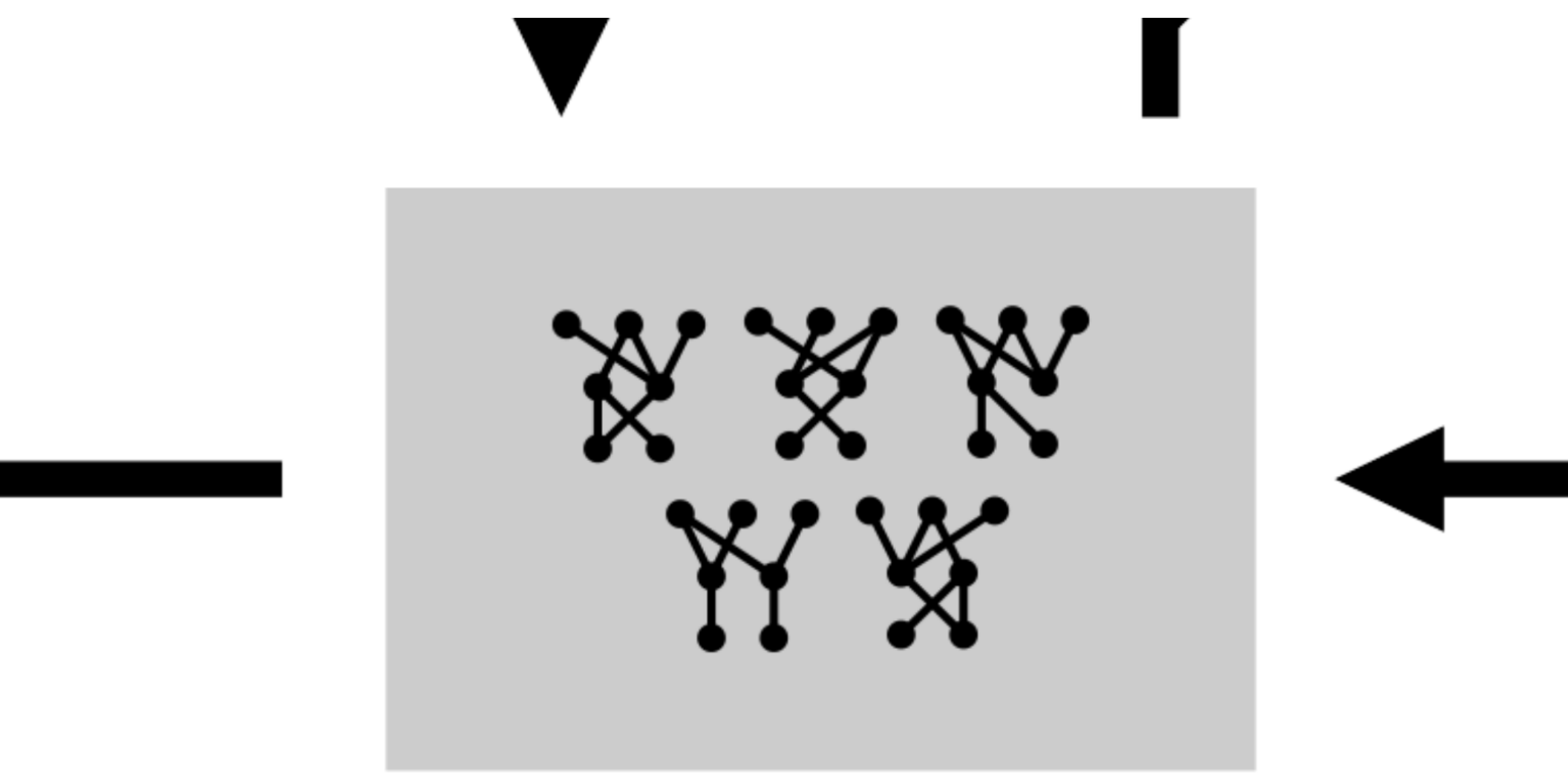
mutation and sexual crossover



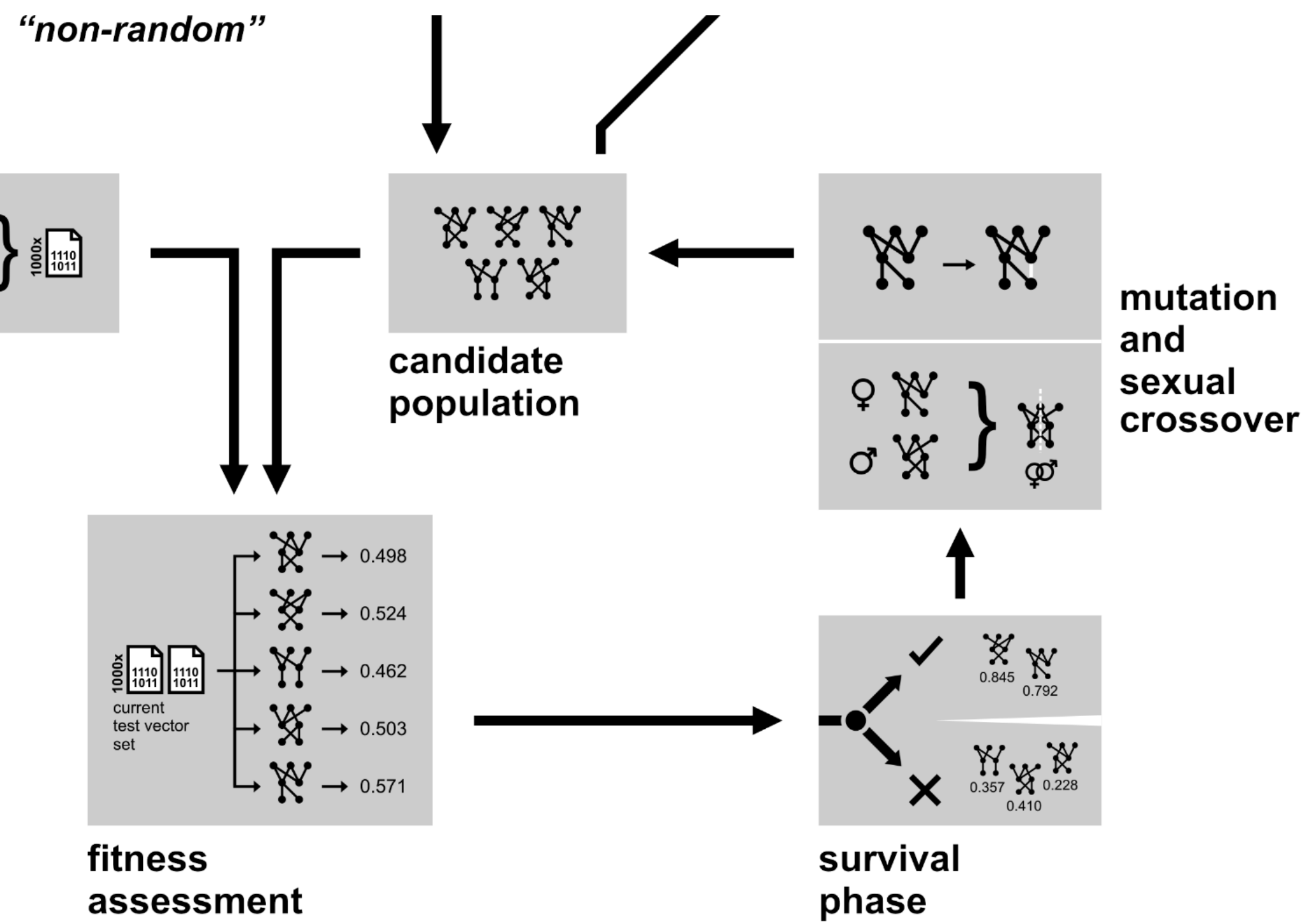


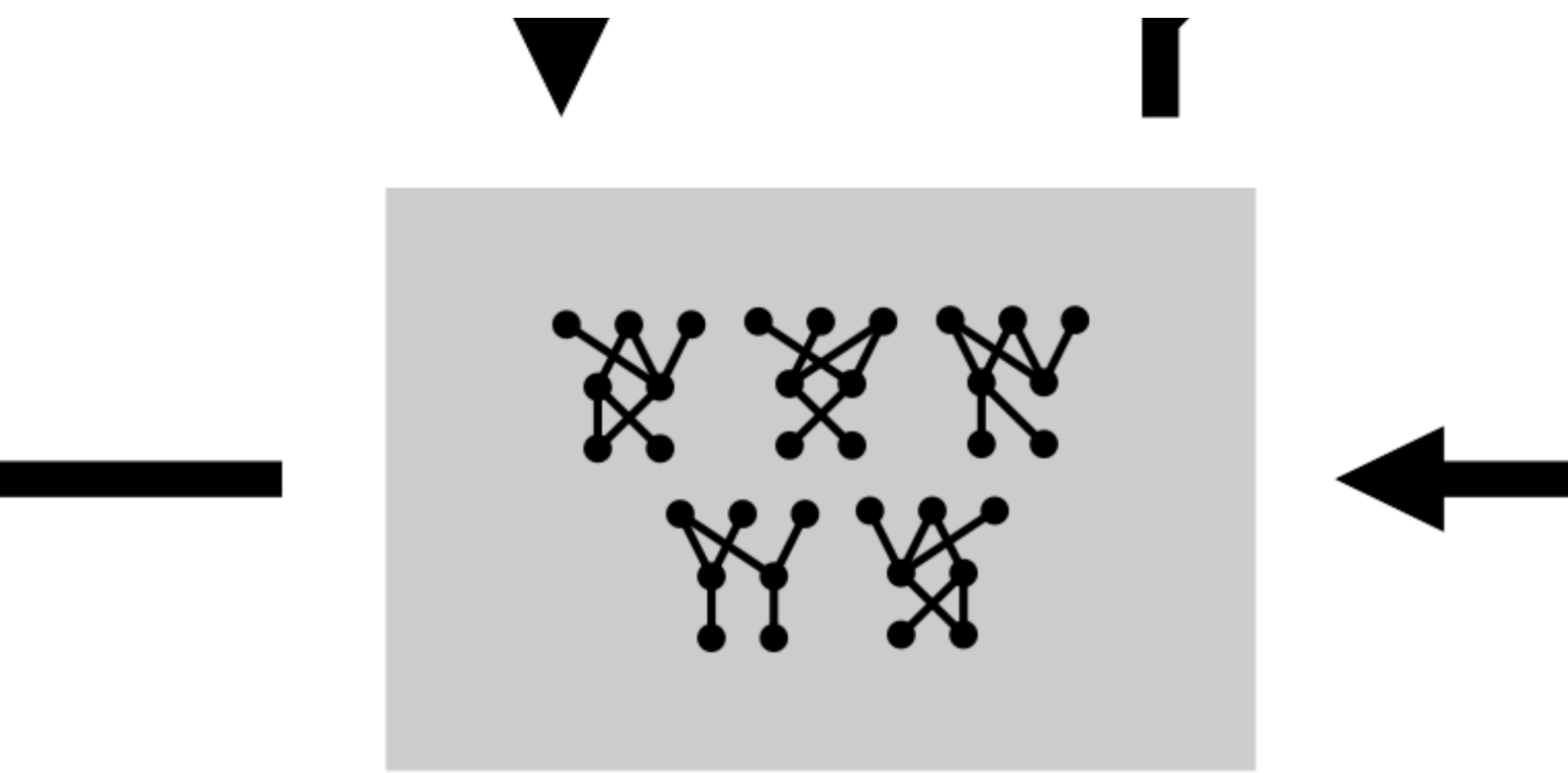


mutation and sexual crossover

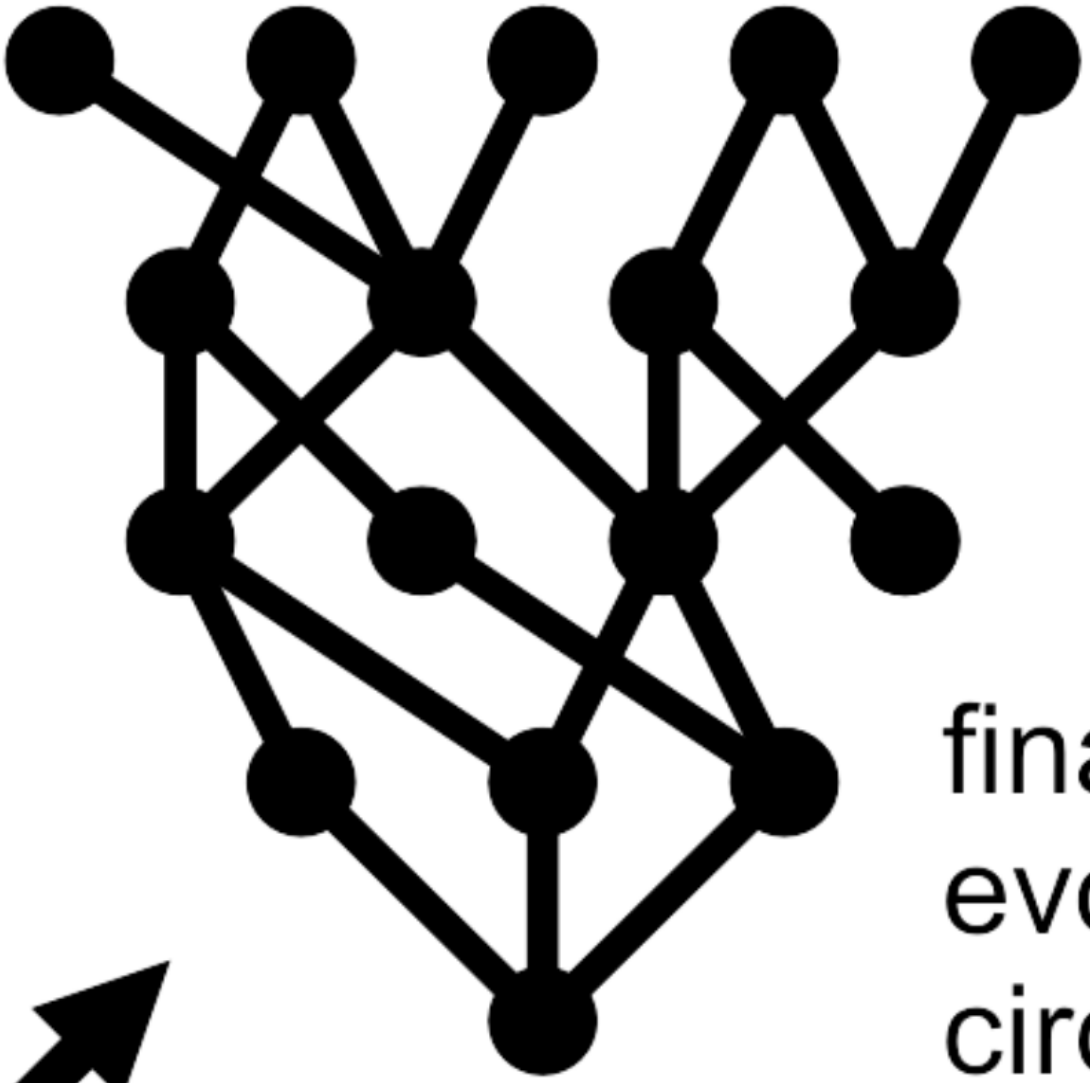


candidate population


"non-random"
1000x
1110
1011
candidate
population
mutation
and
sexual
crossover
1000x
1110
1011
1110
1011
current
test vector
set
0.498
0.524
0.462
0.503
0.571
0.845
0.792
0.357
0.228
0.410
fitness
assessment
survival
phase



candidate population



final
evolved
circuit

7 stream ciphers

18 hash funtions

sanity experiments

audio experiment

comparison to stat. batteries

Salsa20 case-study

random data quality

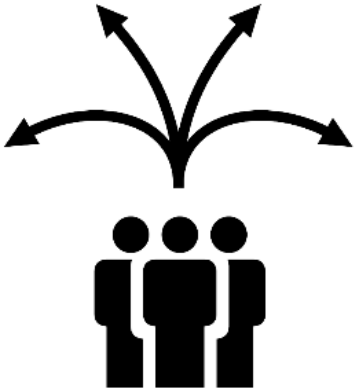
static results verification

novel experiments

application testing

research paper

Švenda, Ukrop, Matyáš
accepted for SECRYPT2013



my work

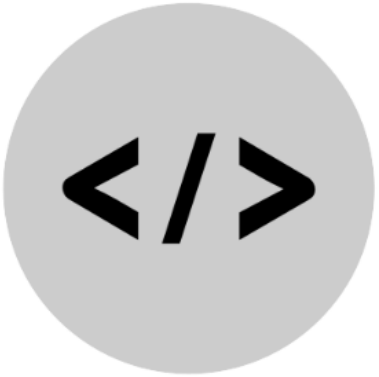
codebase improvements

revised object model

several new features

~3500 lines of code documentation

2. EACirc



codebase improvements

revised
object model

several
new features

~3500 lines of code
documentation

revised
object model

~3500 lines of

several
new features

object model

~3500 lines of code documentation

sanity
experiments

audio
experiment

random
data quality

static results
verification

application testing

sanity
experiments

random
data quality

audio
experiment

static results verification

7 stream ciphers

18 hash funtions

comparison to stat. batteries

Salsa20 case-study

novel experiments

7 stream ciphers

18 hash funtions

ciphers

comparison
to stat. batteries

Salsa20 case-study

research paper

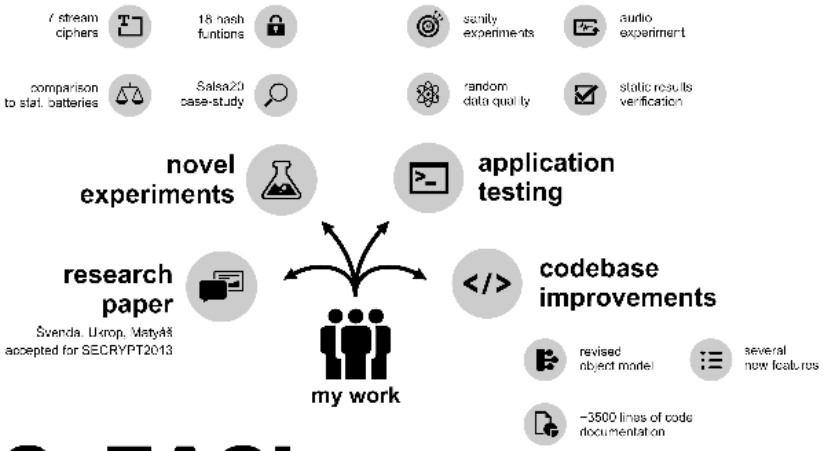
Švenda, Ukrop, Matyáš

accepted for SECRYPT2013

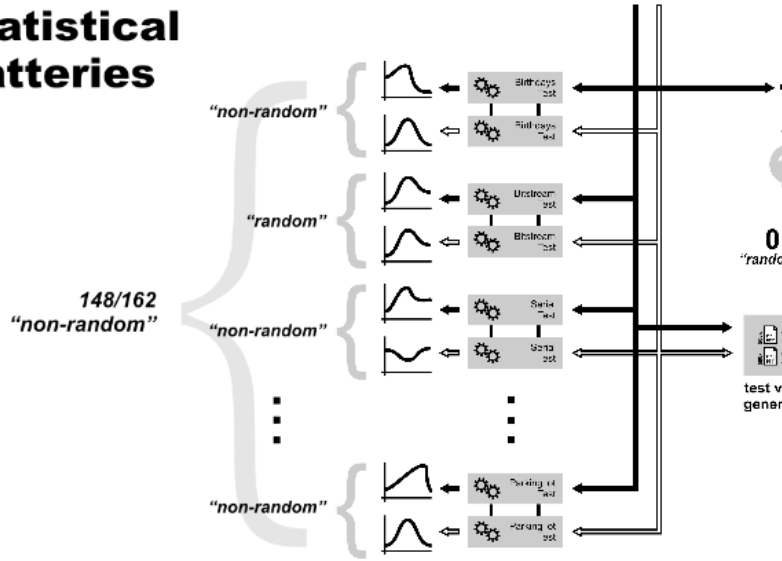
Martin Ukrop
(bachelor thesis)

icons from
The Noun Project

How to distinguish random and non-random data?



1. statistical batteries



2. EACirc