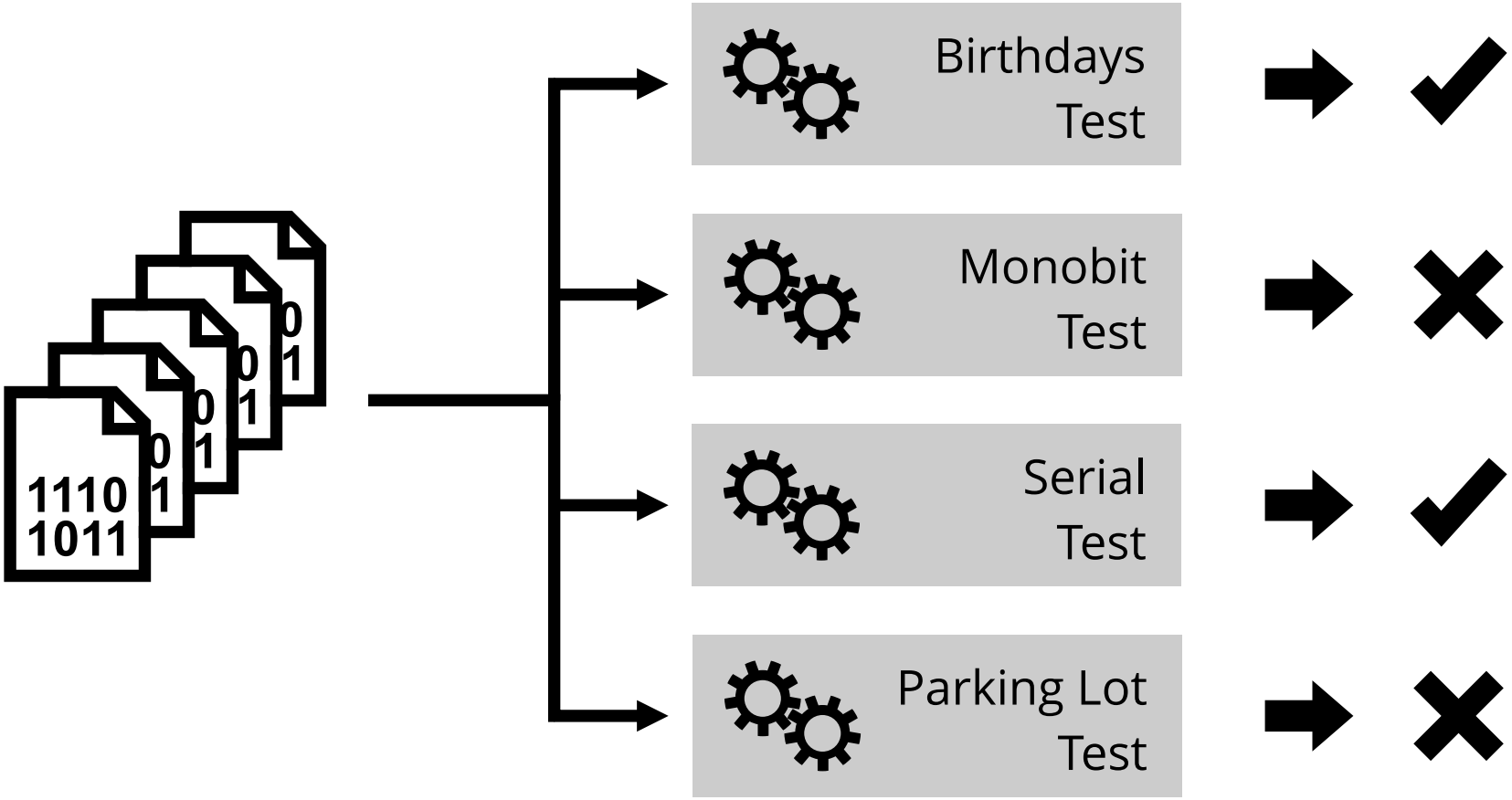
The Evolution of Randomness Testing

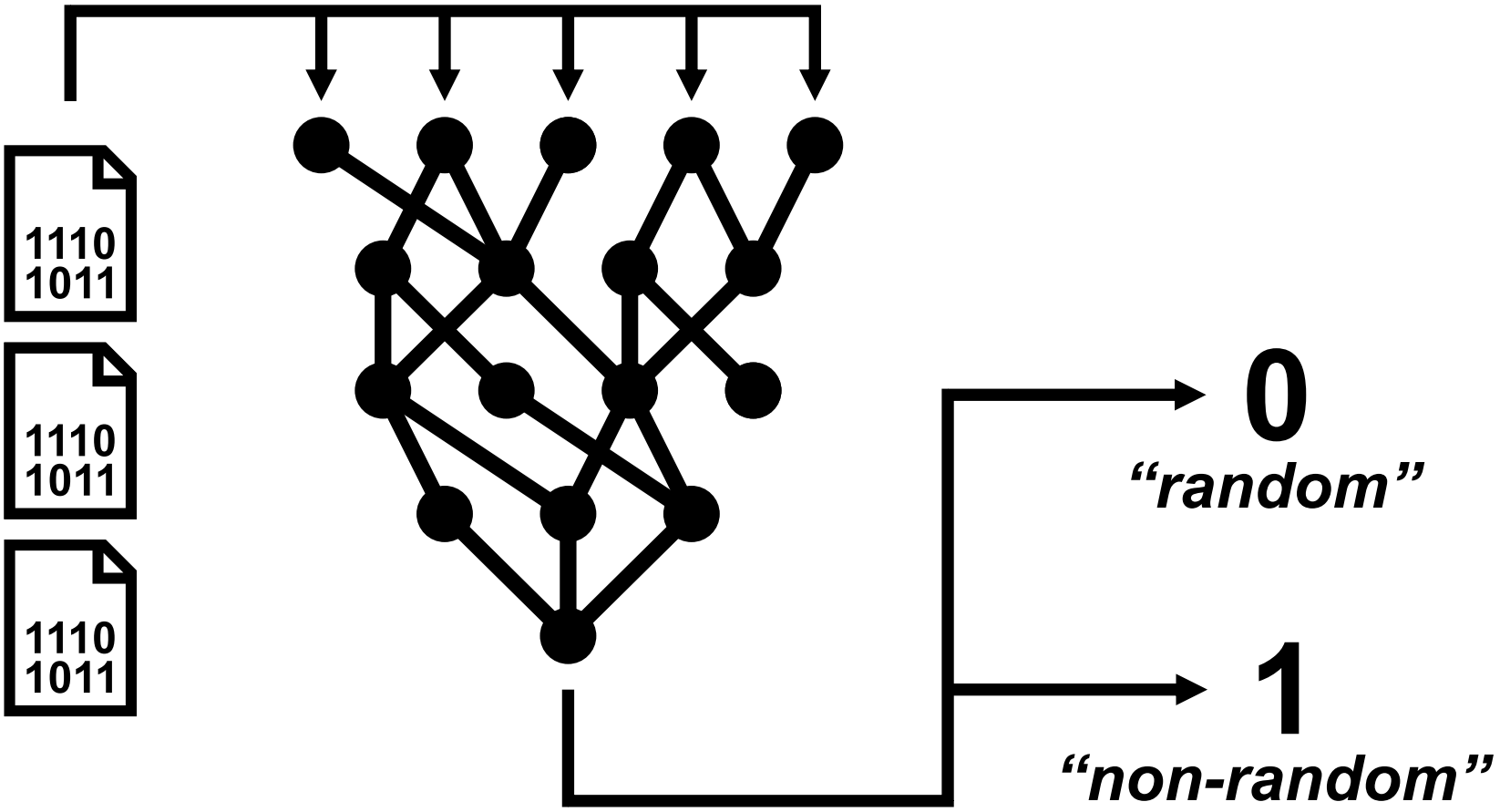
Martin Ukrop,
Petr Švenda, Vashek Matyáš

SantaCrypt 2013, 28. 11. 2013

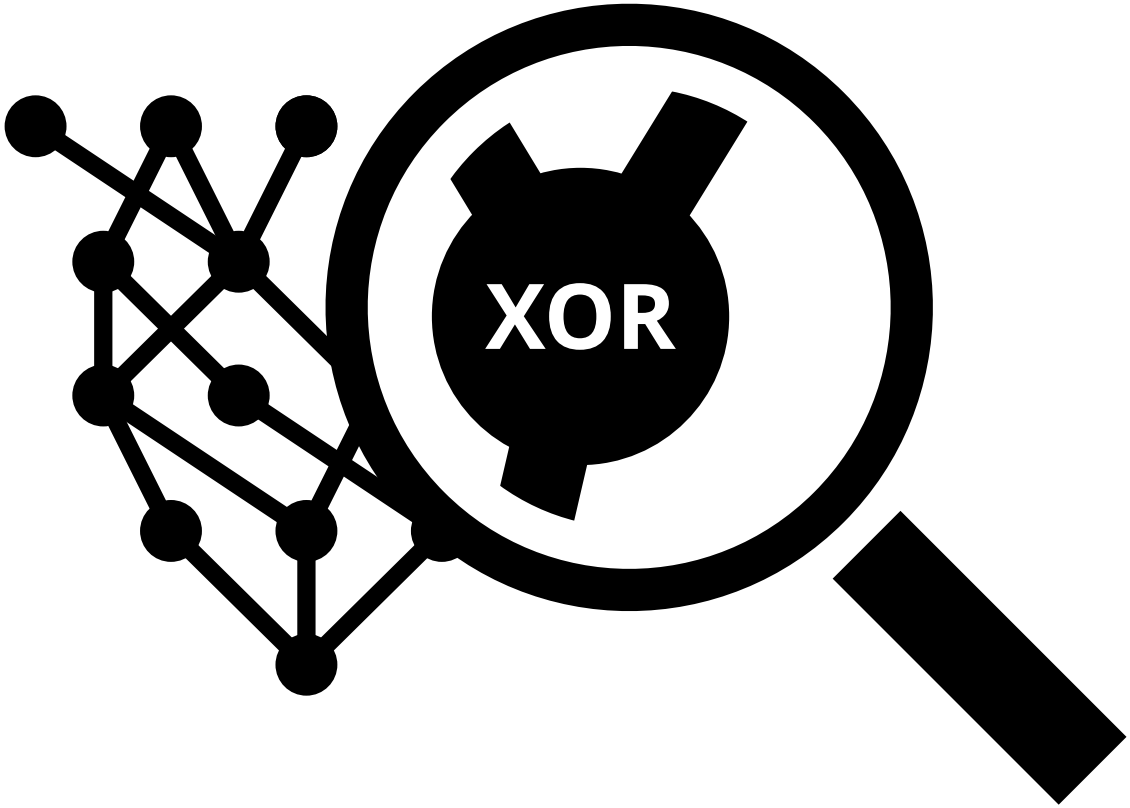
Statistical randomness tests



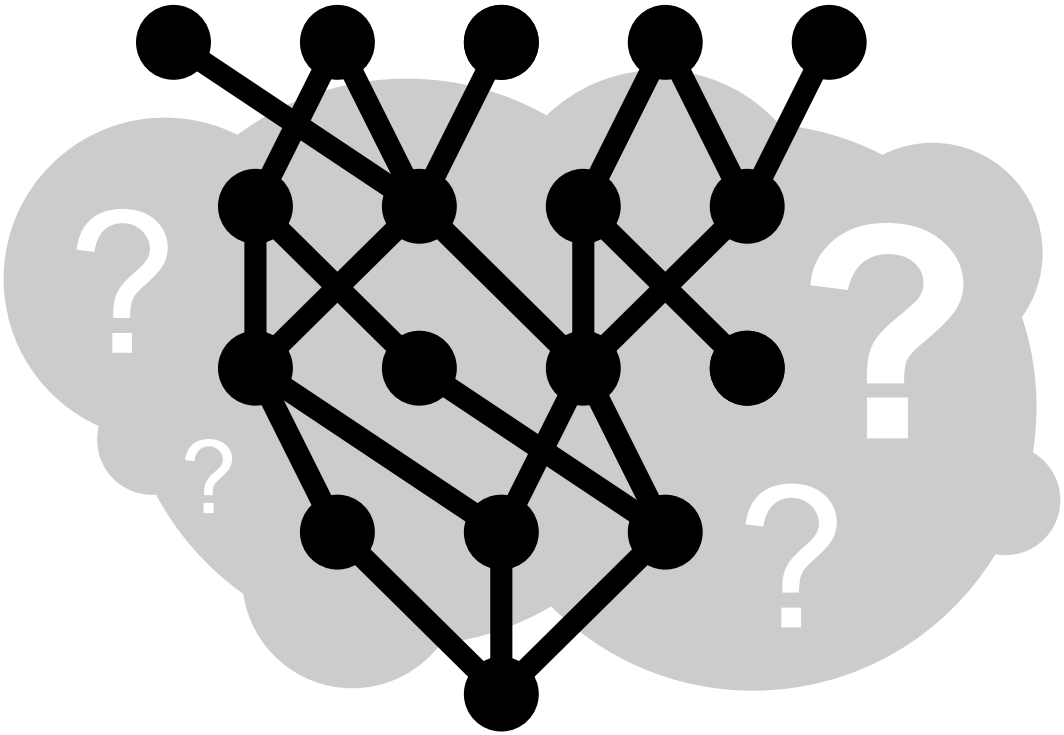
Distinguisher construction I.



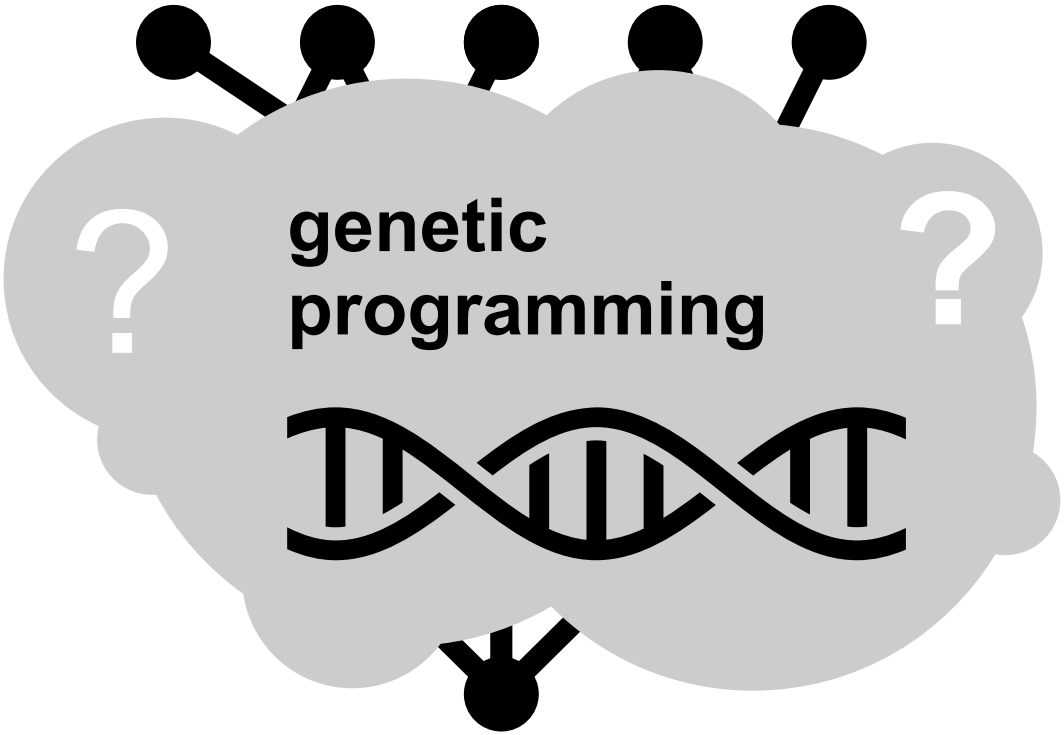
Distinguisher construction II.



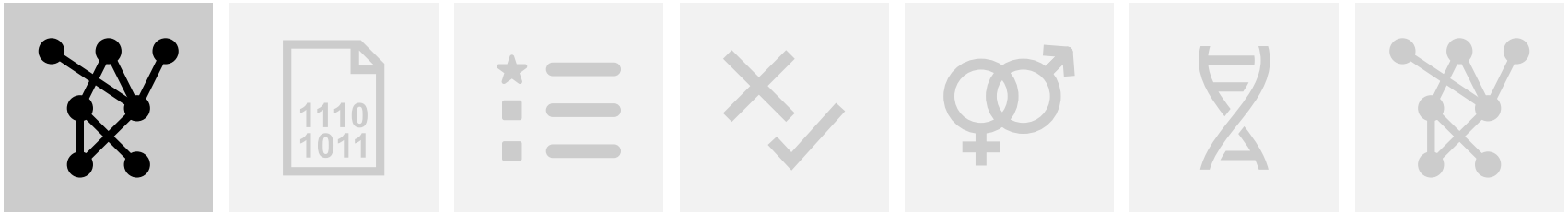
Distinguisher construction III.

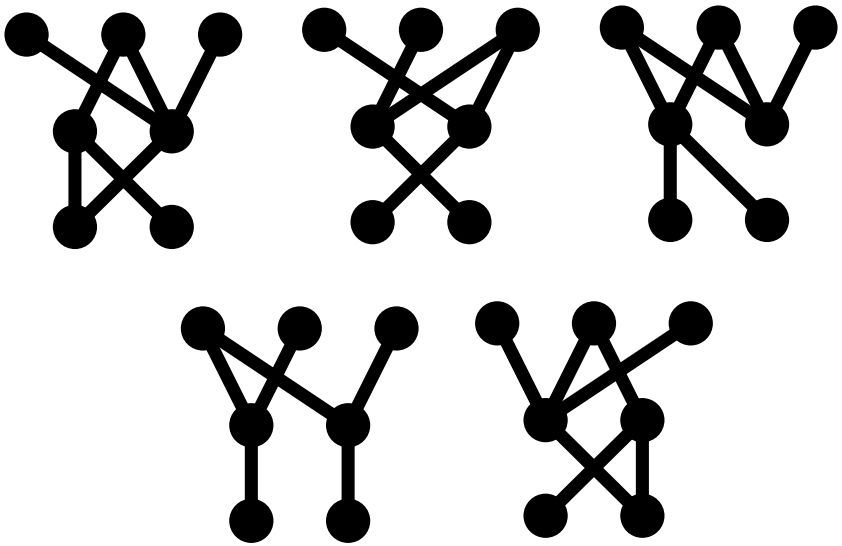


Distinguisher construction IV.

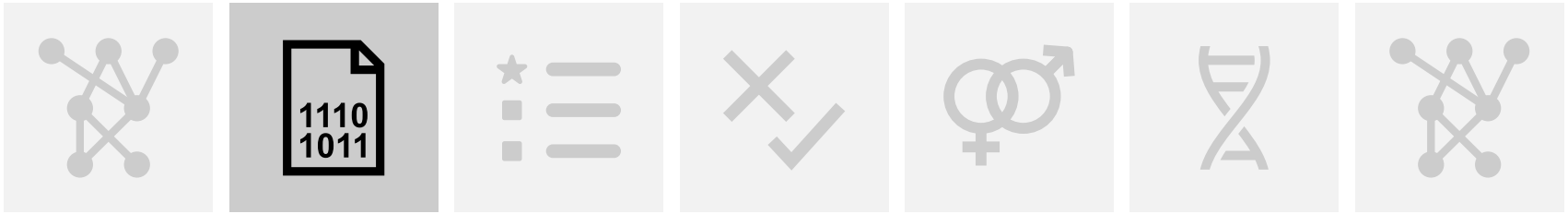


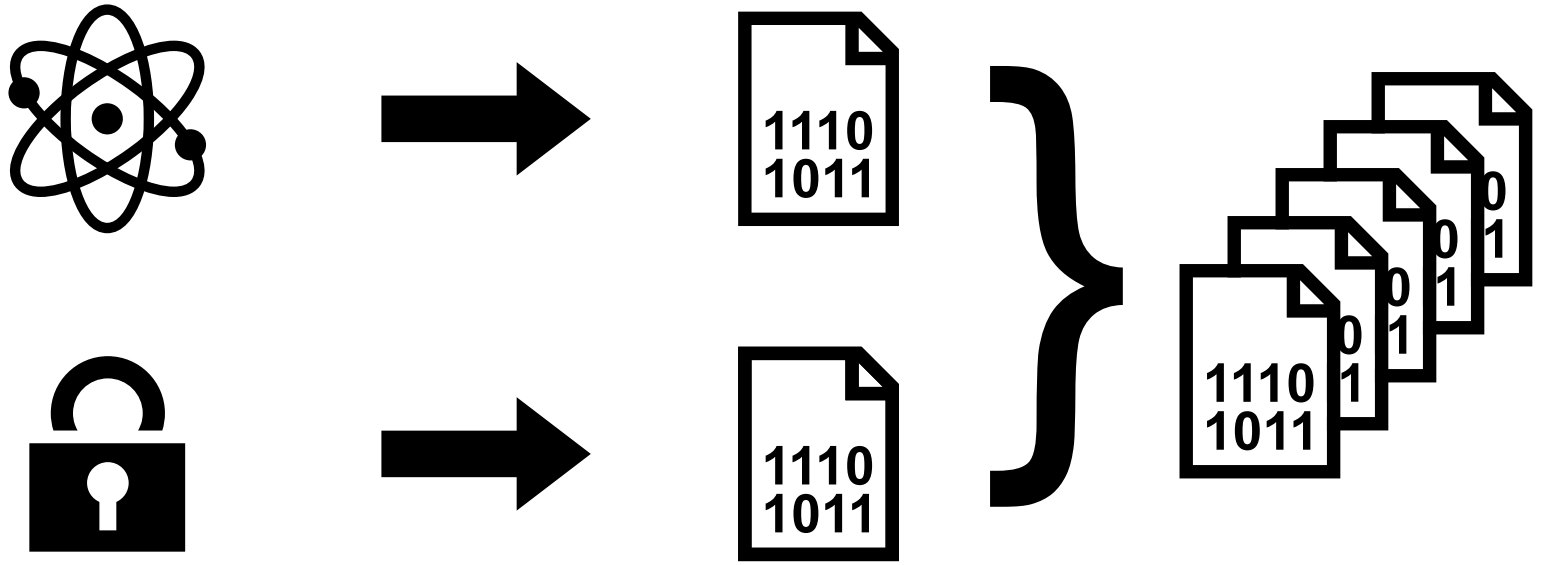
EACirc – initialization



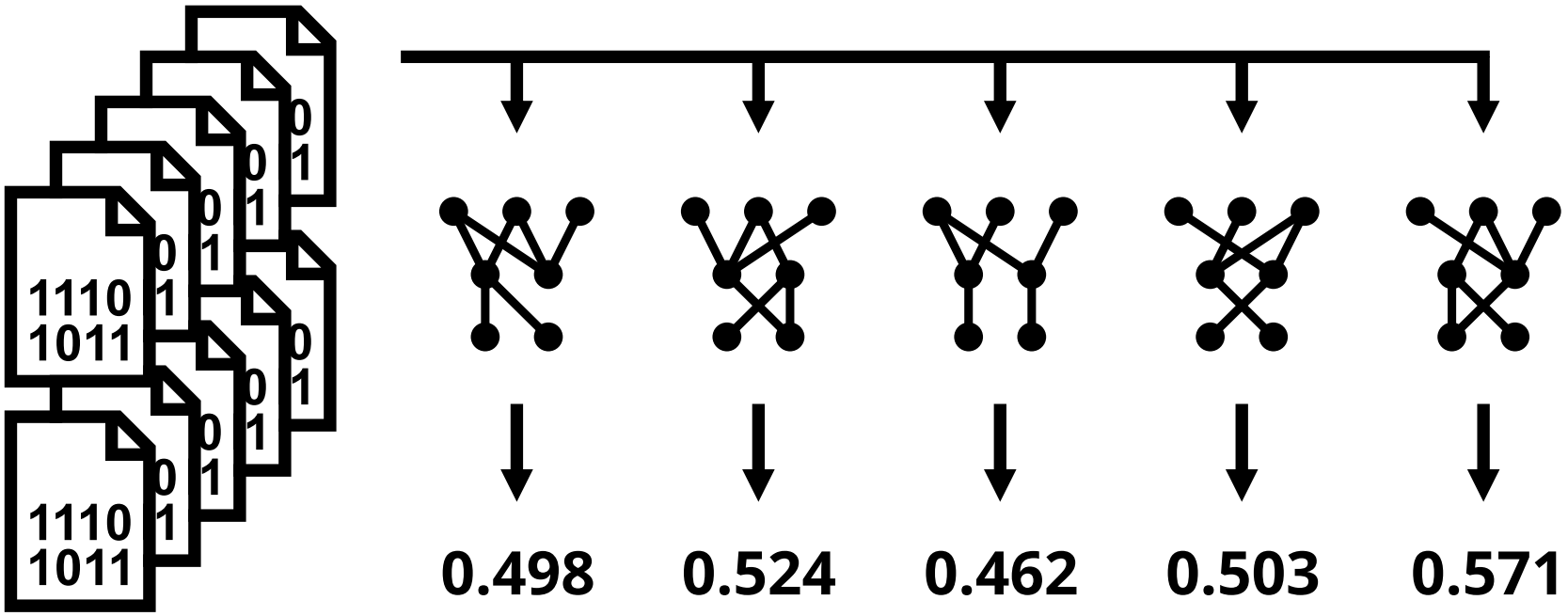


EACirc – test vector generation

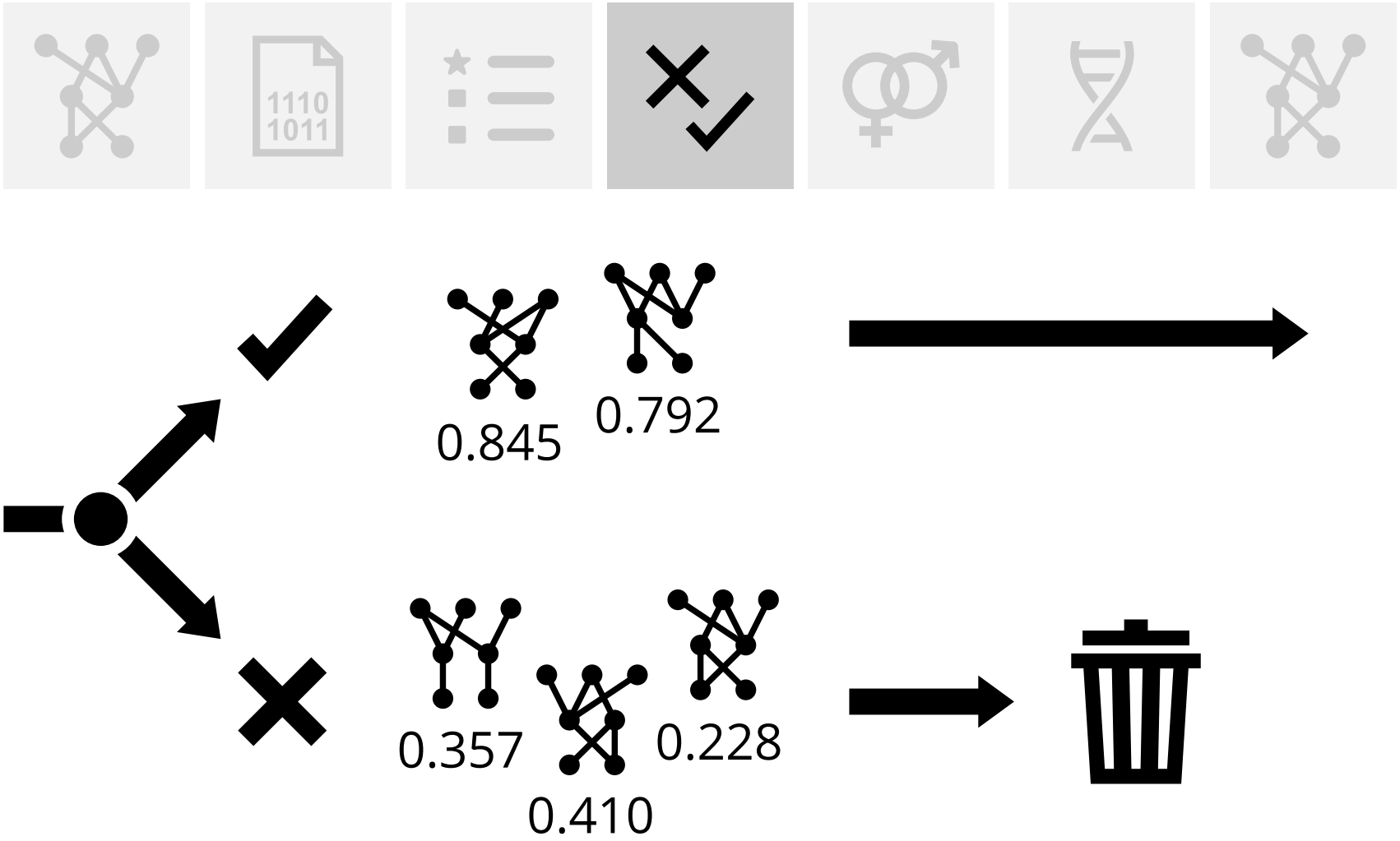




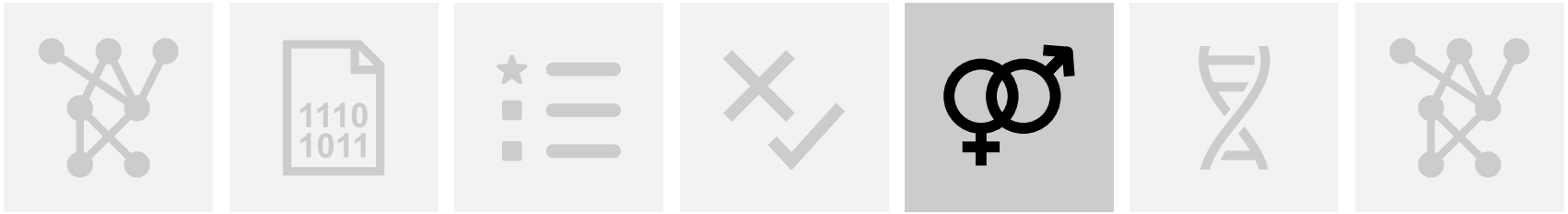
EACirc – evaluation

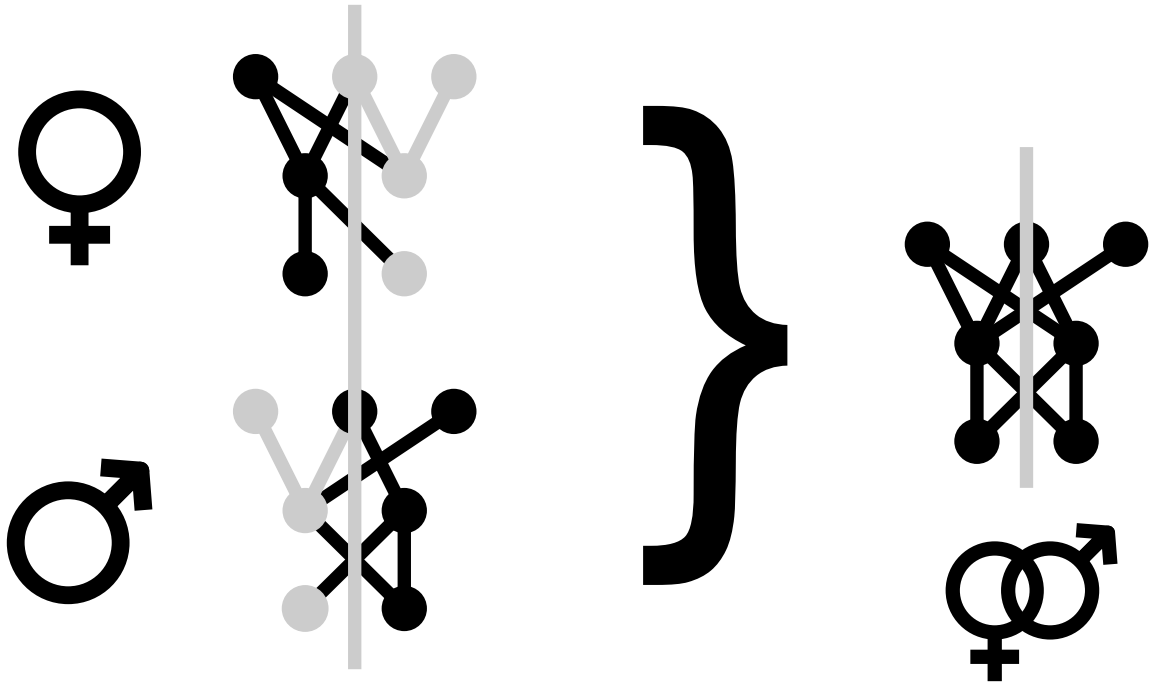


EACirc – survival

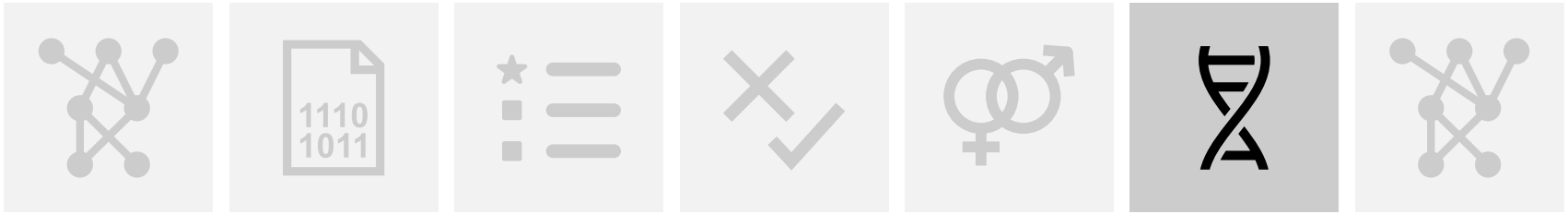


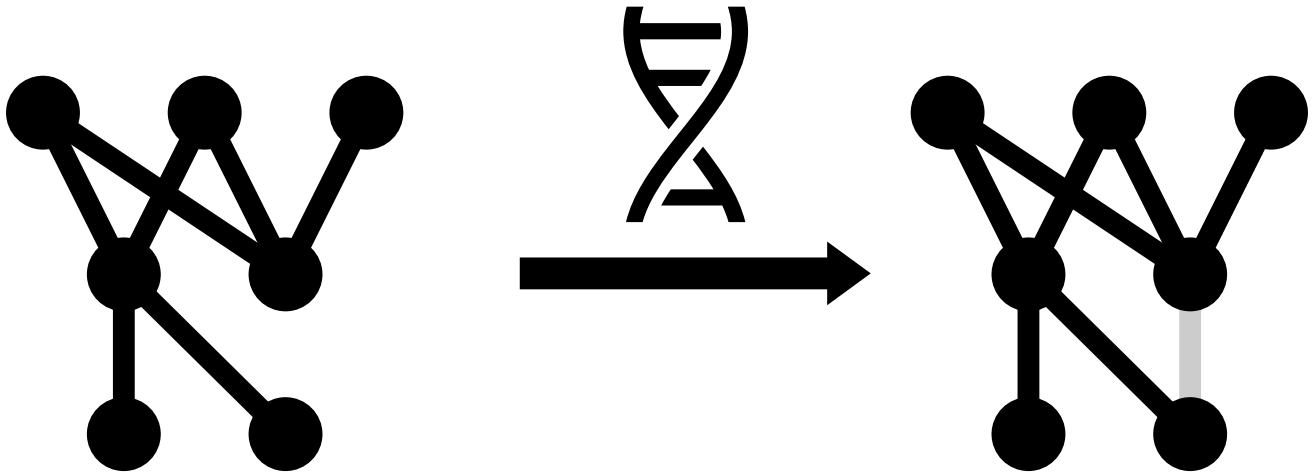
EACirc – sexual crossover



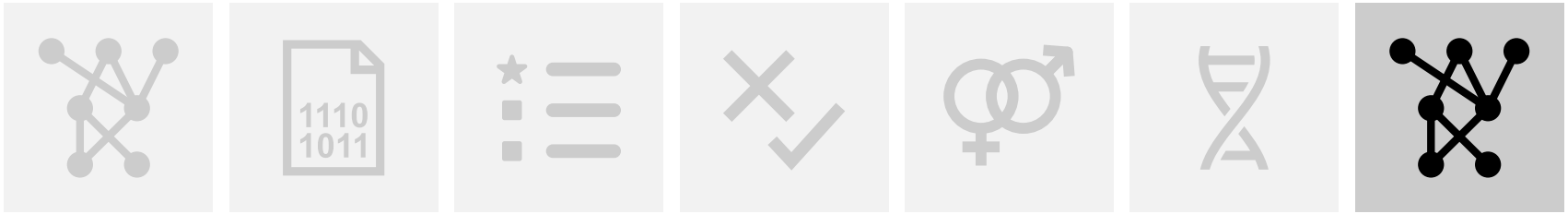


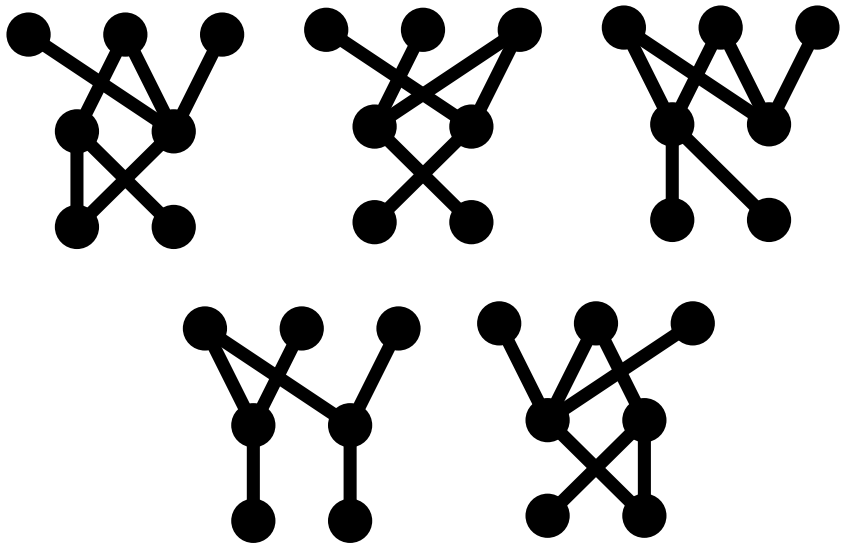
EACirc – mutation



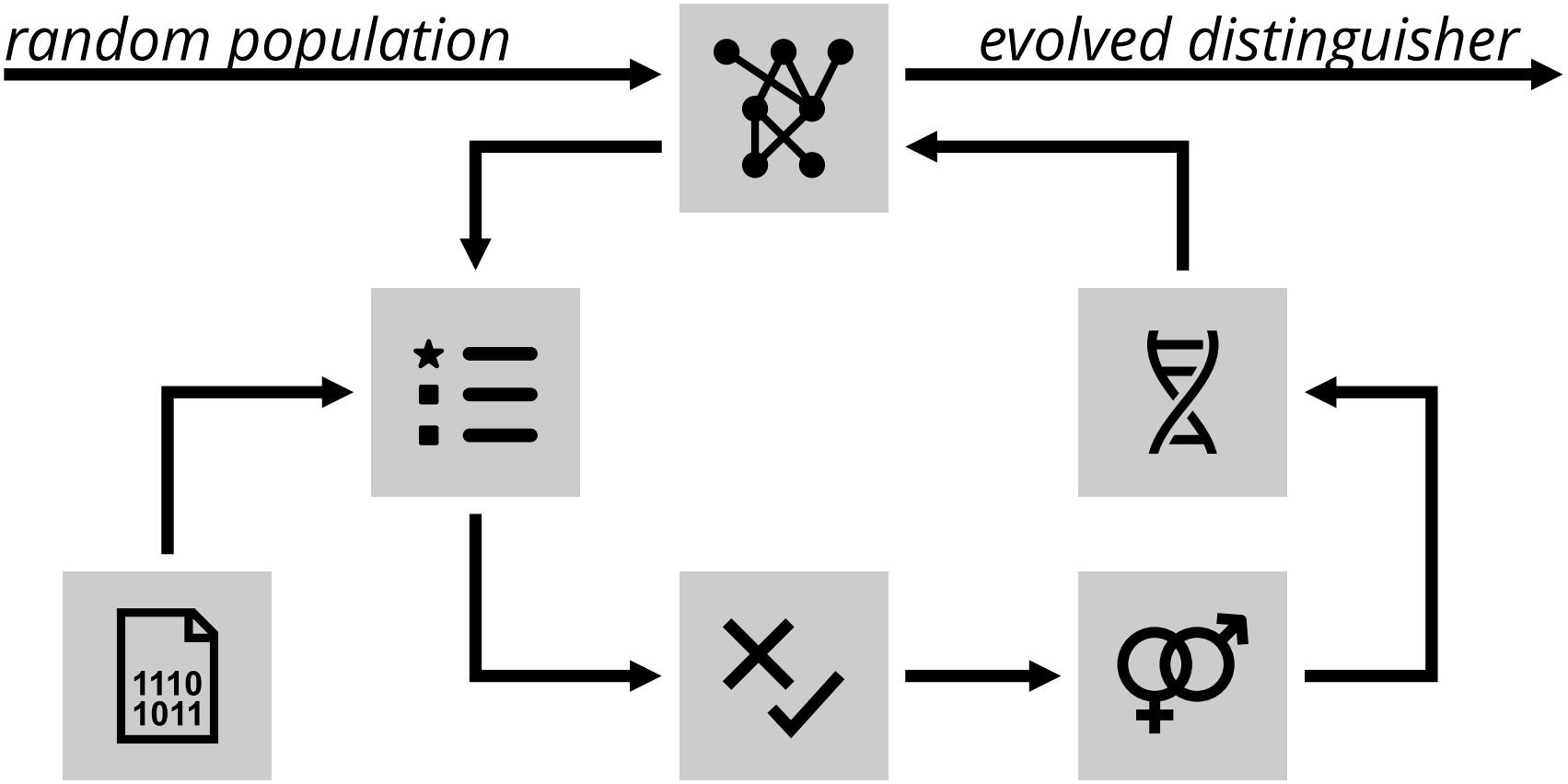


EACirc – iteration

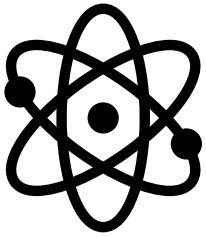




EACirc – overview



Performed experiments

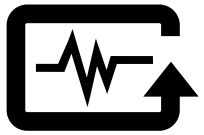


random data

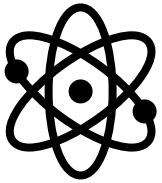
vs.

a) 7 eStream cipher candidates

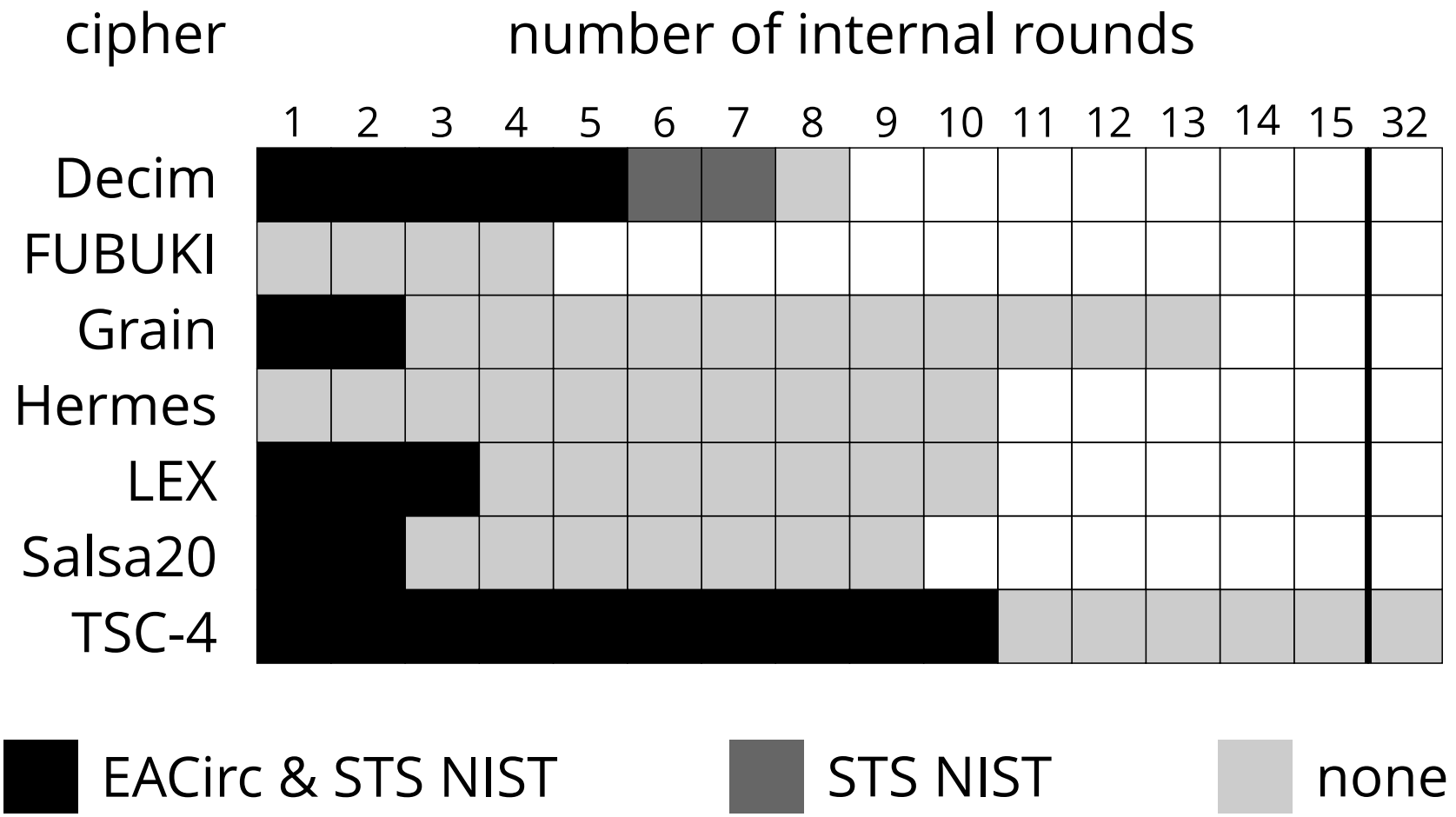
b) 18 SHA-3 hash function candidates



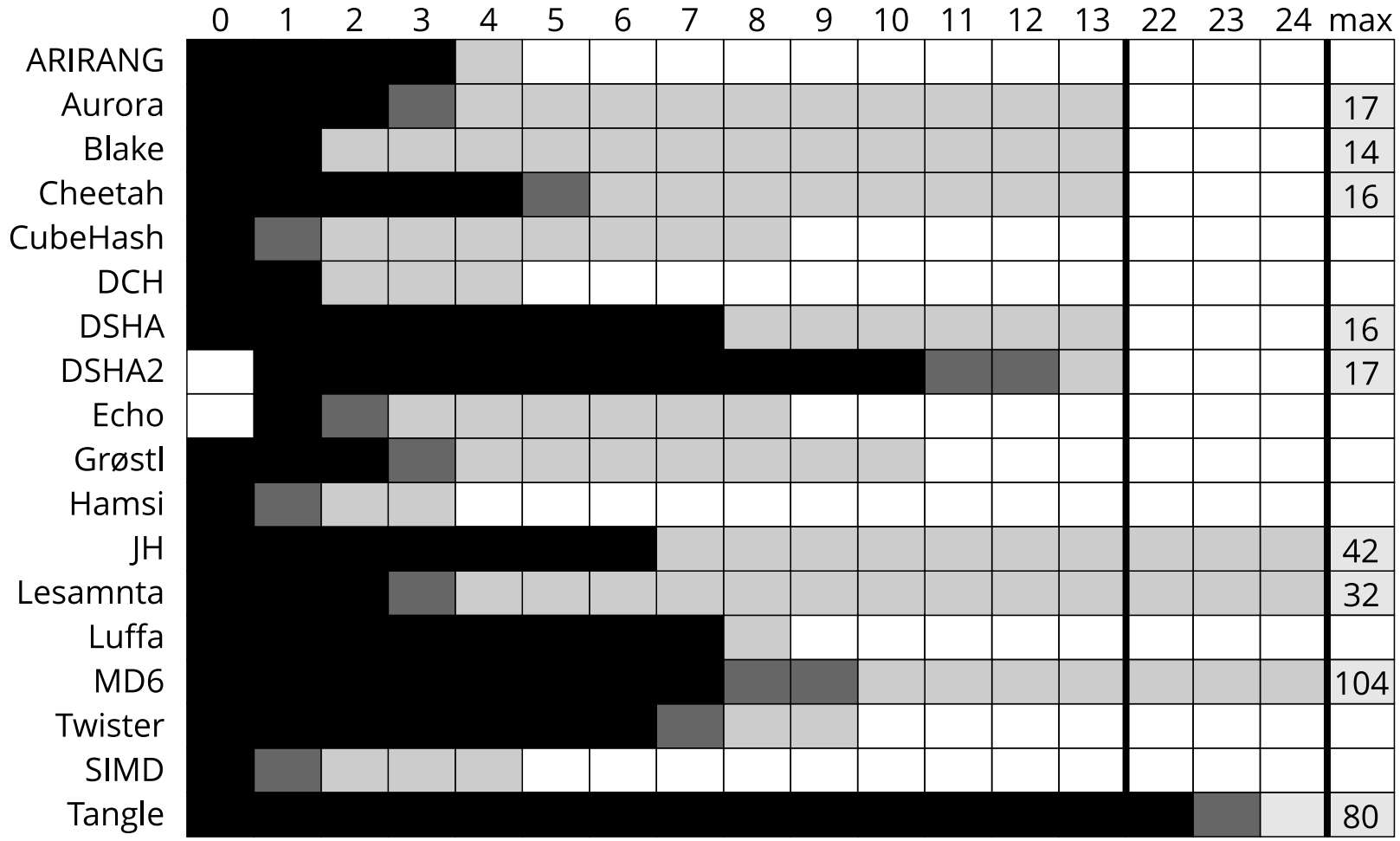
c) random data



eStream – achieved results



SHA-3 – achieved results



Future work

- precise statistical interpretation of results
- processing longer inputs
- byte-code dumps in nodes

EACirc – conclusions

automated

universal

less data needed

occasionally worse than statistical tests

local patterns only

comparably slower

Thank you!

Questions are welcome.