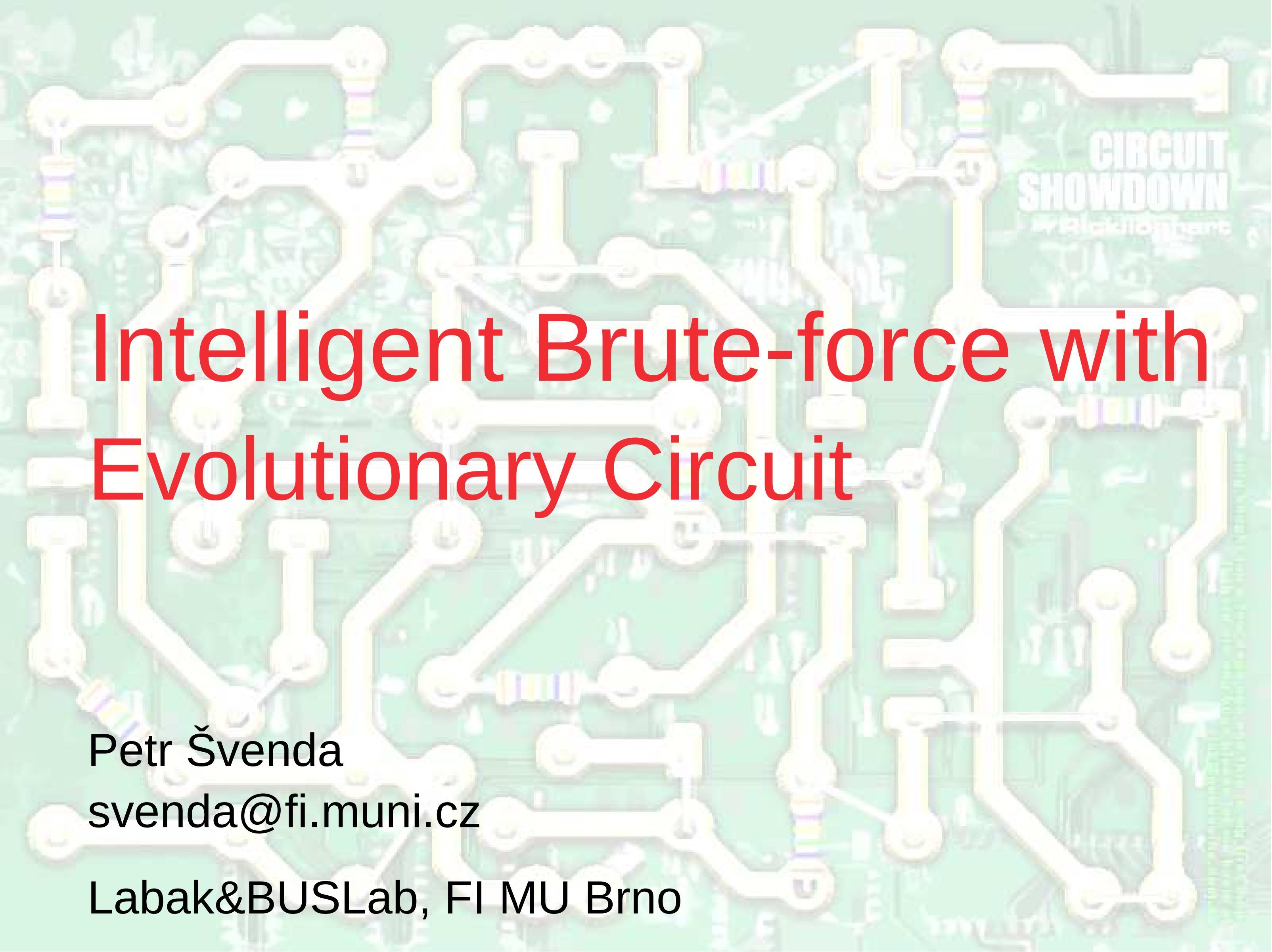
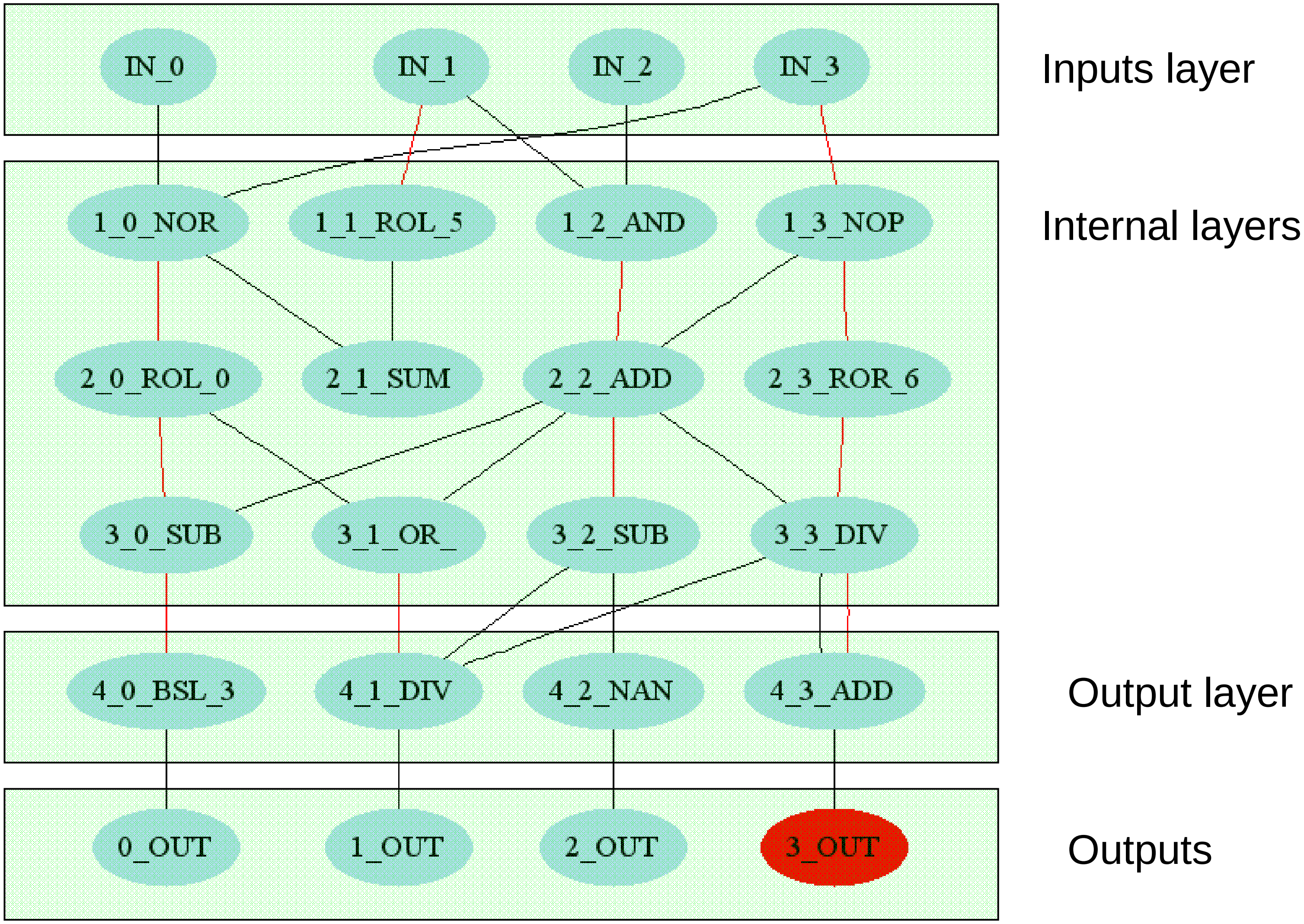


# Intelligent Brute-force with Evolutionary Circuit

Petr Švenda
svenda@fi.muni.cz

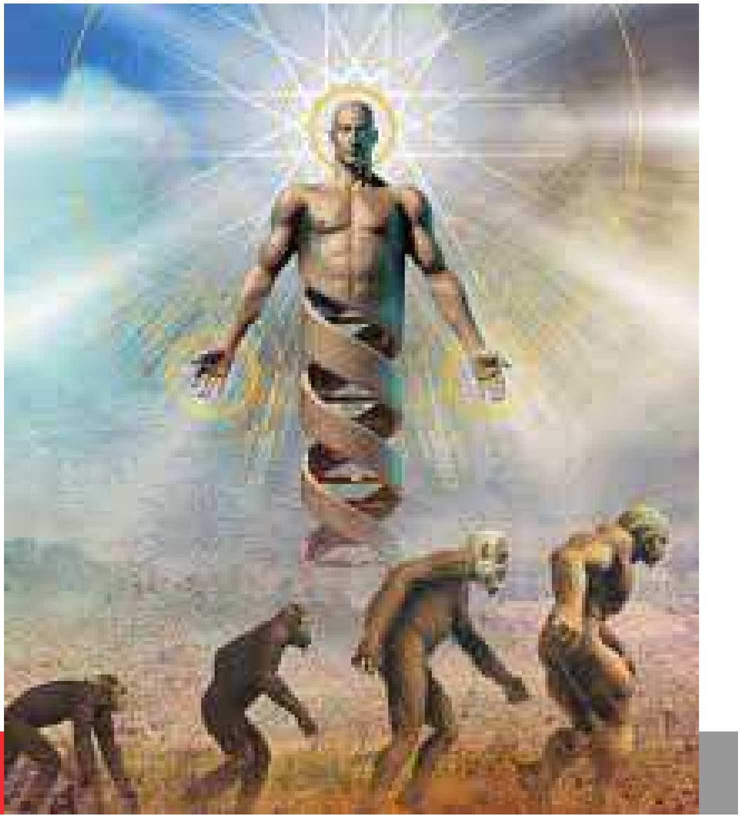
Labak&BUSLab, FI MU Brno

# Why Circuit?


IN_0
IN_1
IN_2
IN_3
1_0_NOR
1_1_ROL_5
1_2_AND
1_3_NOP
2_0_ROL_0
2_1_SUM
2_2_ADD
2_3_ROR_6
3_0_SUB
3_1_OR_
3_2_SUB
3_3_DIV
4_0_BSL_3
4_1_DIV
4_2_NAN
4_3_ADD
0_OUT
1_OUT
2_OUT
3_OUT
Inputs layer
Internal layers
Output layer
Outputs

# Why intelligent?

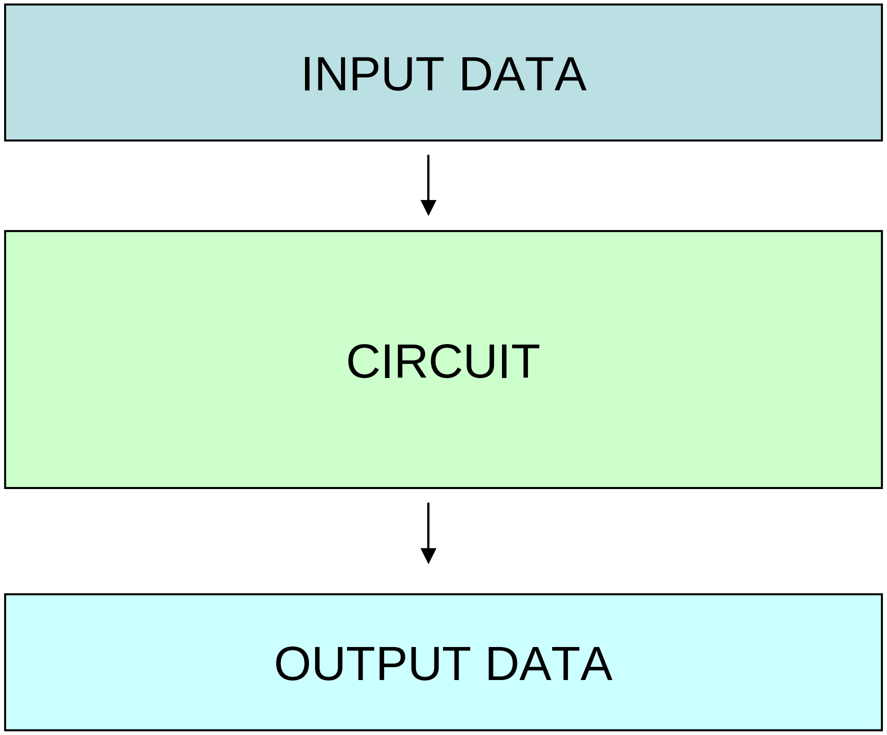
- Someone has to design the circuit
- We use genetic algorithms
  - usually better then random search
  - (not really intelligent)



# Why brute-force?

280 CPUs, 140 GPUs

# What for? (Ideal scenario)



*AES in&out data*

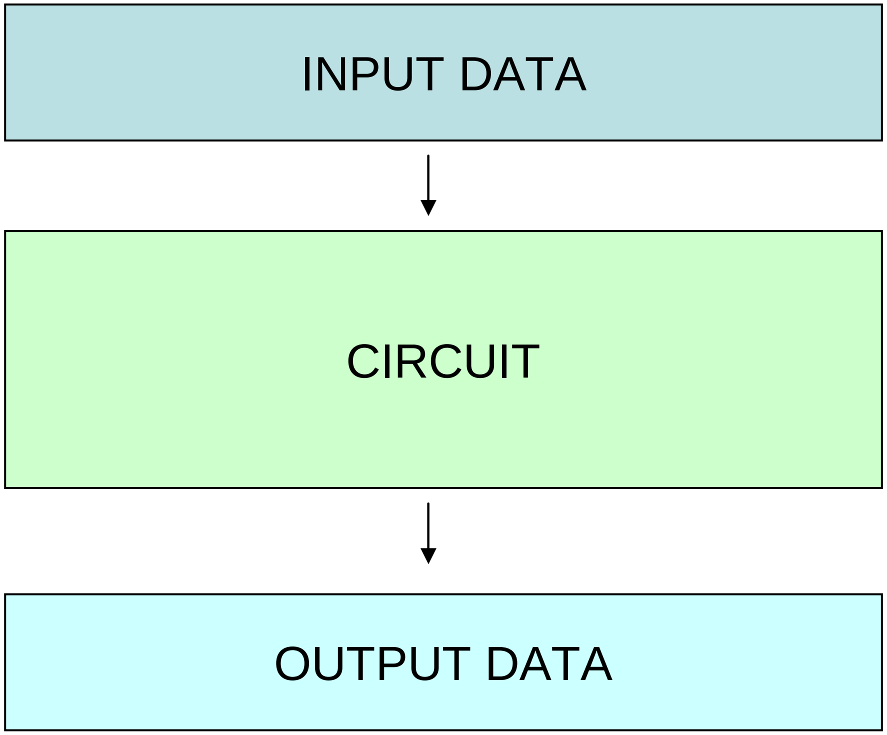
*Circuit execution*

*Used key*

# What for? (More realistic scenarios)

- Any weakness in any function
  - SHA-3 & eStream candidates
- Weaknesses for functions with reduced number of rounds
- Probabilistic approach
  - 100% success not required

# Degraded avalanche affect circuit



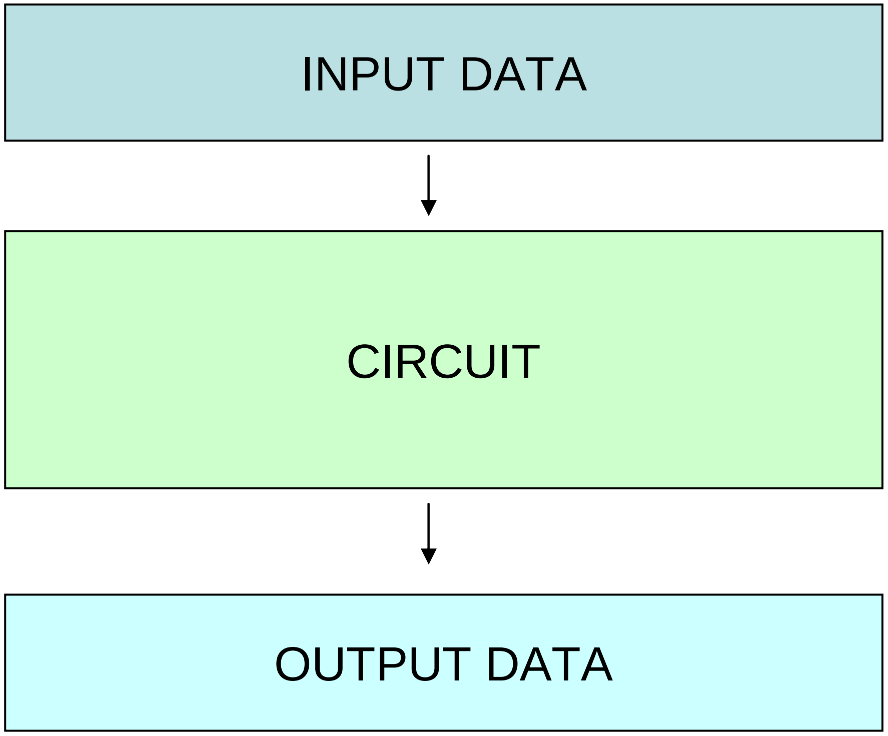
*input block M*

*Circuit execution*

*bits_to_invert*

H = hash(M),
M’ = bits_to_invert(M),
H’ = hash(M’)
Hamming distance(H, H’)

# Bit prediction circuit

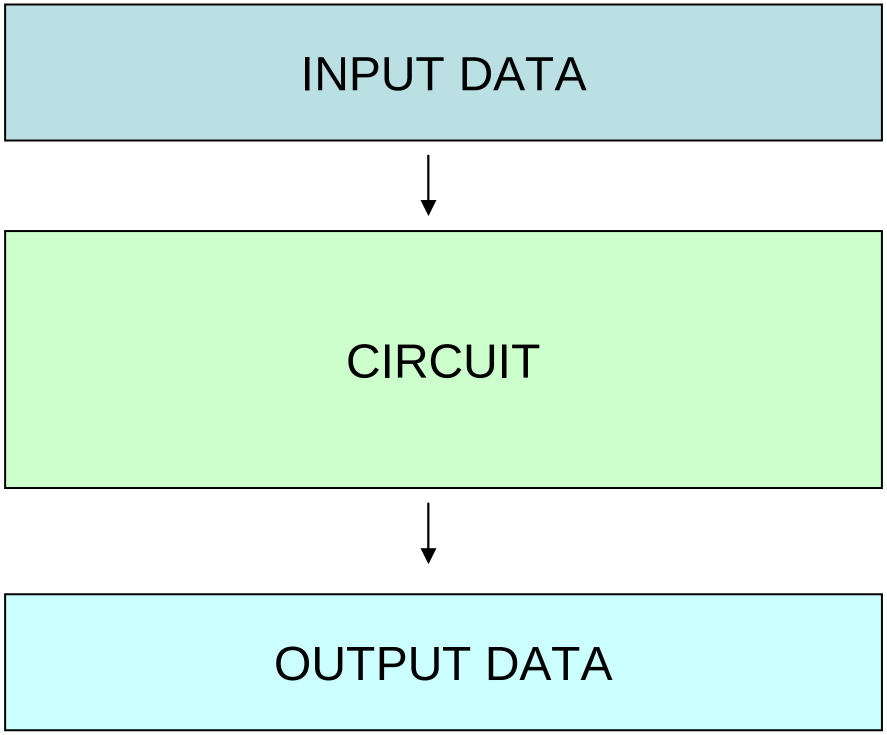


*key stream / hash stream*

*Circuit execution*

*bit position, bit value*

# Distinguisher from random stream circuit



INPUT DATA

*hash OR random*

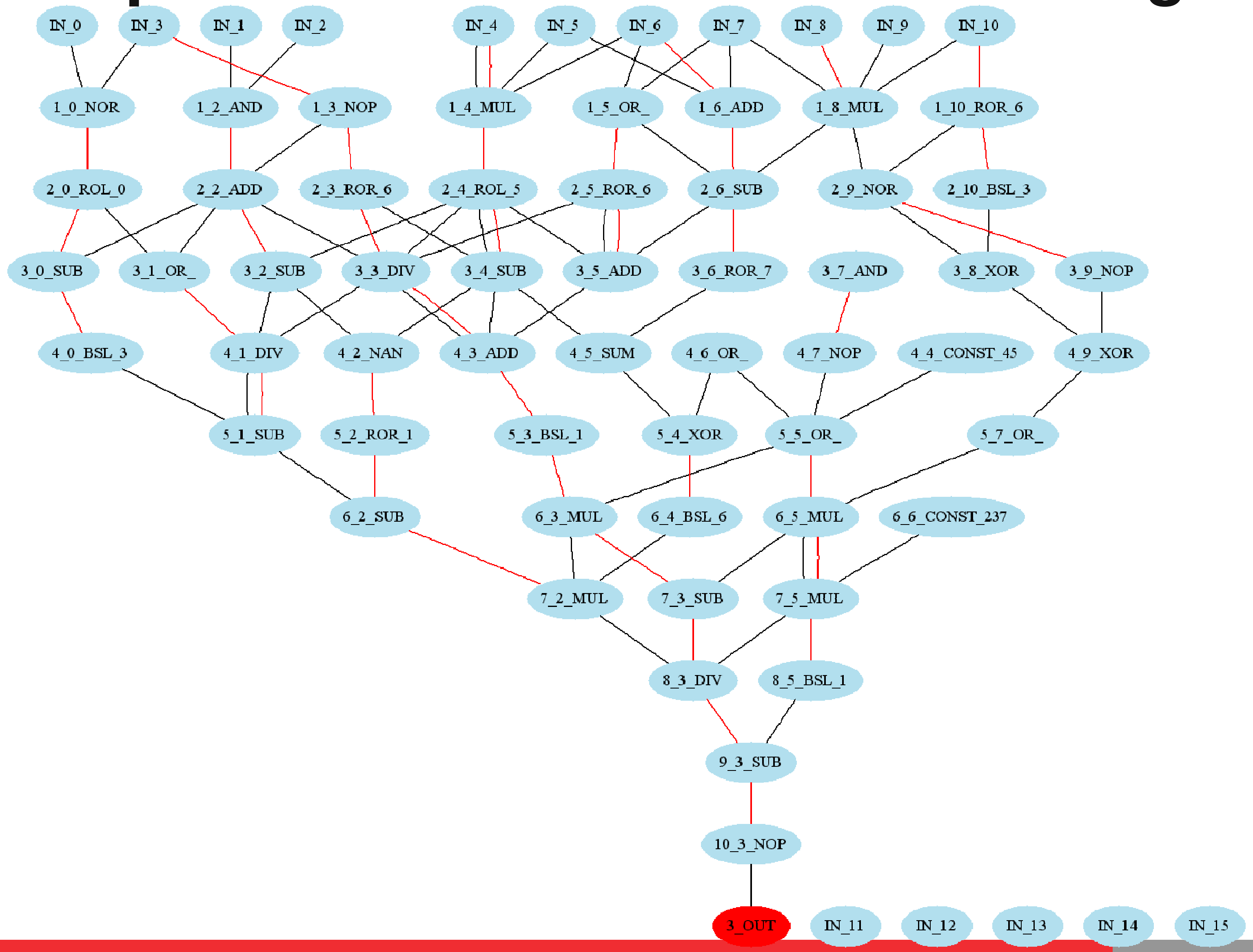
CIRCUIT

*Circuit execution*

OUTPUT DATA

*1if hash, 0 if random*

# Example: 10 rounds MD5/RNG distinguisher



## Any suggestions are welcomed!

# Practical results – random distinguisher

- Random stream distinguisher
  - circuit try to differentiate between completely random stream and stream generated by target function with unknown input
  - QRGBS http://random.irb.hr/index.php
  - input data are either random stream or hash of structured data
    - two random bytes repeated to form 16B input
  - output data is 0x00 for hash function, 0xff for random stream
  - tested on MD5 and SHA1
- Best results so far
  - around 68% success of distinguishing for 10-round MD5 (from 64)
  - around 70% success of distinguishing for 8-round SHA1 (from 80)
  - circuit: 10 layers, 4 connectors