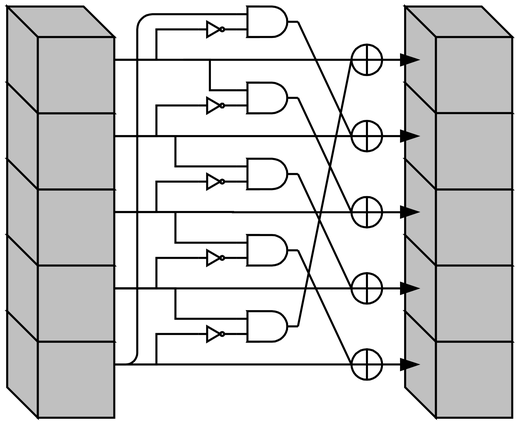
NIST Circuit Complexity Benchmarking

Luís T. A. N. Brandão · Çağdaş Çalık · Morris Dworkin · René Peralta · Meltem Sönmez Turan

Cryptographic Technology Group, Computer Security Division, National Institute of Standards and Technology

Circuit Complexity Challenge

A Boolean circuit is a *directed acyclic graph* that computes a function using basic Boolean operators such as `AND`, `NOT`, `XOR`, `XNOR`.



Circuit for SHA-3 S-Box (from https://keccak.team/figures.html)

Challenge: Given a function and a set of gates, construct a circuit that optimally computes it according to some *logical metric*.

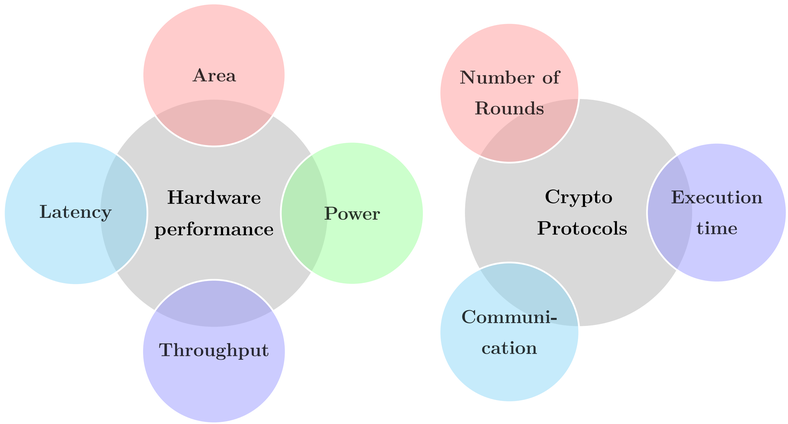
Aim:

- Improve our understanding of circuit complexity.
- Develop techniques for better circuits for academia and industry.
- Evaluate and compare the performance of new heuristics.

Logical & Performance Metrics

- **Circuit size:**
  - Smaller gate count ⇒ smaller hardware area, less energy
  - Lower number of nonlinear gates (e.g., `AND`) ⇒ less communication for crypto lower cost for side-channel resistance.
- **Circuit depth:**
  - Smaller circuit depth ⇒ lower latency
  - Lower AND-depth ⇒ fewer interaction rounds in multiparty computation; more efficient homomorphic encryption

Performance metrics for real-world apps relate to **logical** metrics.



Public Benchmarking

We represent circuits using Straight Line Programs (SLPs).

```
begin CIRCUIT MAJ3
# Description: The majority of x1,x2,x3
Inputs: x1:x3;
Outputs: y1;
GateSyntax: GateName Output Inputs
begin SLP
  XOR t1 x1 x2;
  XOR t2 x1 x3;
  AND t3 t1 t2;
  XOR y1 t3 x1
end SLP end CIRCUIT
```

Method:

- Select functions of varying difficulties and sizes
- Determine evaluation criteria and publish best known circuits

Circuit	Gate count					Depth	
	All	AND	XOR	XNOR	NOT	All	AND
AES S-Box	113	32	77	4	0	27	6
AES S-Box^{-1}	121	34	83	4	0	21	4
AES-128(k,m)	28 600	6400	21 356	844	0	326	60
SHA-256(m)	115 882	22 385	89 248	3894	355	5403	1604

k: AES key; m: message (128-bit for AES; 512-bit for SHA-256)

Webpage: https://csrc.nist.gov/Projects/Circuit-Complexity **Email:** circuit_complexity@nist.gov **GitHub:** https://github.com/usnistgov/Circuits

Poster produced for the NIST-ITL Virtual Science Day 2020

Luís is a Foreign Guest Researcher at NIST (Contractor via Strativia); Çağdaş is a Foreign Guest Researcher at NIST.