Optimizing Cryptographic Circuits

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

Boolean Circuits

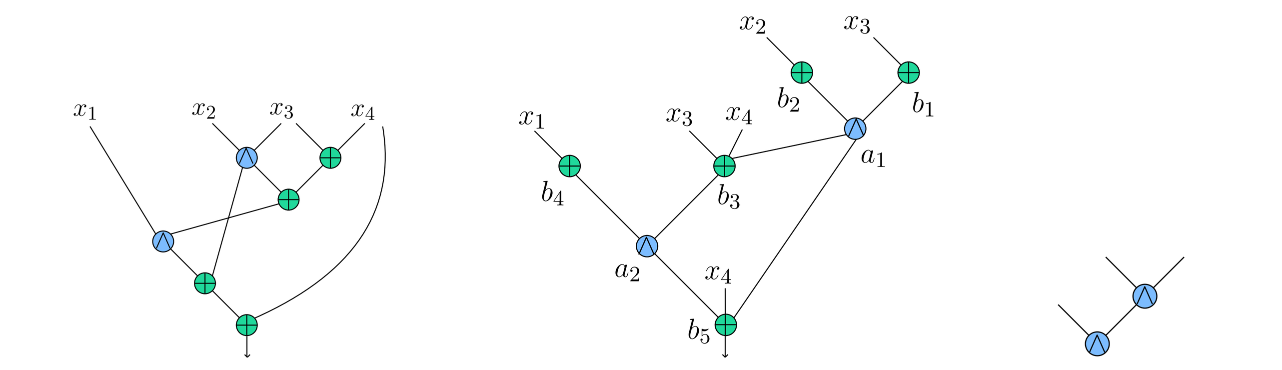
A Boolean circuit is a *directed acyclic graph*, where the inputs and the gates are the nodes, and the edges are the Boolean-valued *wires*.

A Boolean circuit with n inputs and m outputs computes a function of the form $f : \{0,1\}^n \to \{0,1\}^m$.

Basic Boolean operators: `AND`, `NAND`, `OR`, `NOT`, `XOR`, `XNOR`, ...

The *canonical form* of a circuit is a standard representation based on `AND` and `XOR` gates. The *topology* of a circuit is an abstraction that shows the relative positions of the `AND` gates.

Example. Let $f = x_1x_2x_3 + x_1x_3 + x_1x_4 + x_2x_3 + x_4$.



Circuit C to compute f · Canonical form of C · Topology of C

Complexity Measures

- *Size complexity*: The number of gates in the circuit.
- *Depth complexity:* The length of the longest path from an input gate to the output gate.
- *Multiplicative complexity* (MC): Number of *non-linear* gates used in a circuit, or (the minimum) required to implement a function.

Target metric depends on the application.

- Circuits with small number of gates use less energy and occupy smaller area, and are desired for *lightweight cryptography applications* running on constrained devices.
- Circuits with small number of AND gates are desired for *secure multi-party computation*, *zero-knowledge proofs* and *side channel protection*.
- Circuits with small AND-depth are desired for homomorphic encryption schemes.

Circuit Complexity Challenge

Given a Boolean function and a set of gates, construct a circuit which computes the function and is optimal according to a complexity measure.

Contact: `circuit_complexity@nist.gov`
Webpage: `https://csrc.nist.gov/Projects/Circuit-Complexity`
Data repository: `https://github.com/usnistgov/Circuits`

Low-MC Circuits for Sets of Quadratic Forms

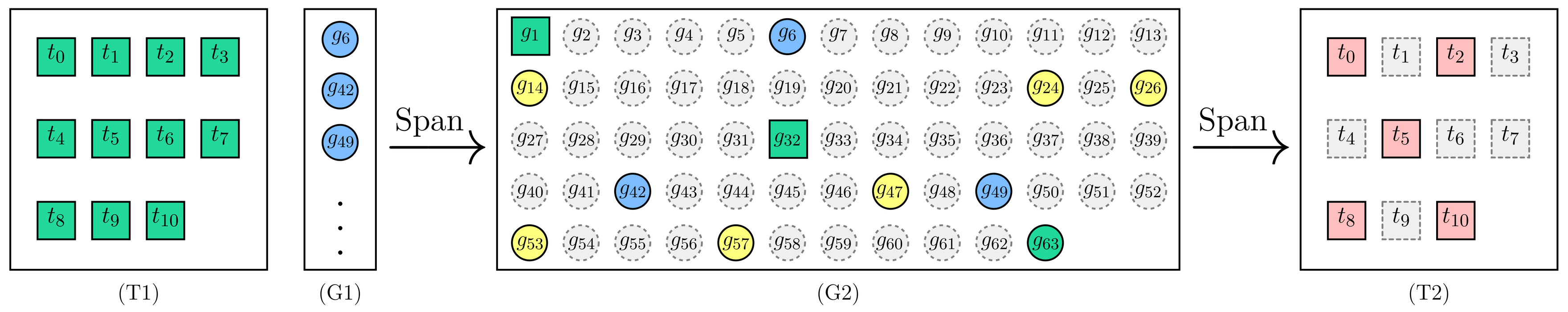
Goal: To design smaller circuits for computing sets of quadratic "forms". Example applications:

- multiplication of binary polynomials,
- Galois field multiplication in characteristic 2, used in elliptic curve cryptography, and
- binary matrix multiplication.

Problem: Consider a set $\{g_1, \ldots, g_m\}$ of generators g_j, each requiring one `AND` gate. How many such generators are needed to calculate a particular set $\{t_0, \ldots, t_{k-1}\}$ of k target functions t_i?

Approach: We enhance the search method of Barbulescu et al. by expanding subspaces incrementally, scoring intermediate results, and applying "genetic" mutations.

An intermediate state of the algorithm (example):



Legend: T1 is a set of 11 targets; G1 is an incremental expansion to T1; G2 is the set of generators in the span of T1 ∪ G1; T2 is the set of targets spanned by G2; the greyed out elements with dashed border are not in span.

The figure shows 11 targets t_i, together with 3 selected generators g_j, spanning 12 generators:

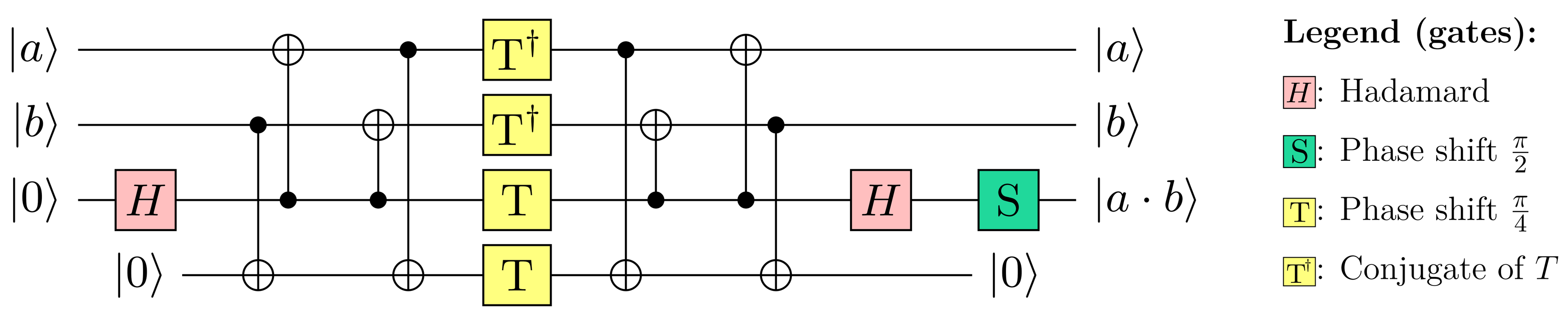
- 2 are targets t_i, and 1 other is a linear combination g_j of targets;
- 3 are the expansion generators; g_j
- **6 are new generators** g_j (1st score), which are in the span of T1 ∪ G1.

The set of 12 generators spans **5 targets** t_i (2nd score). We terminate when T2 equals T1, i.e., the 2nd score is k. The solution is derived from the subset G2 of generators.

Results: We have found circuits with small number of `AND` gates for many instances of binary polynomial multiplication.

Boolean Circuits for Post-Quantum Cryptography

Quantum Circuits: Quantum computation will trigger a revision of all our cryptosystems. NIST is currently working to standardize post-quantum public-key cryptography. Because of Grover's algorithm, symmetric key cryptography will also be impacted. In quantum circuits, the gates corresponding to `AND`, such as the one below (by Mathias Soeken — see ia.cr/2019/1146), are much more expensive than those corresponding to `XOR`.



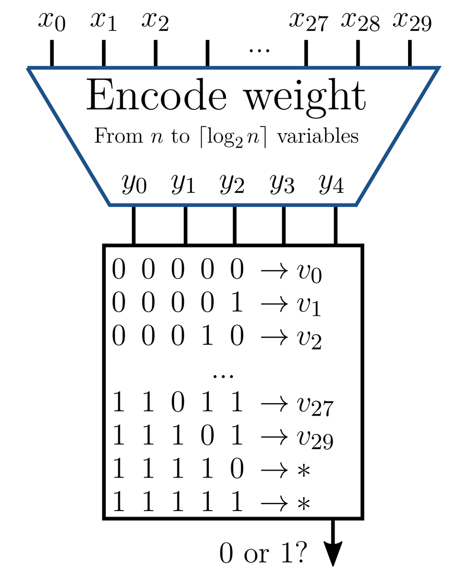
Example quantum-circuit implementation of an `AND` gate

Challenges

- Improve quantum circuits for symmetric encryption functions.
- Design cryptographic primitives with low MC for use in the post-quantum world. An example is the post-quantum signature candidate *PICNIC*.
- Design a standard format for describing quantum circuits.

MC of Symmetric Boolean Functions

Goal: To find efficient circuits with low number of `AND` gates for symmetric Boolean functions, in which the output is determined by the number of ones of the input.



Method: There are two parts:

1. Encode the weight using *full adders* and *half headers*.
2. Build the symmetric function using the weight encoding.

Results:

- Proposed technique constructs circuits for all symmetric functions with up to 25 variables.
- Upper bounds on maximum MC of class of n-variable Boolean functions for $n \leq 132$.

Boolean Functions with MC 3 and 4

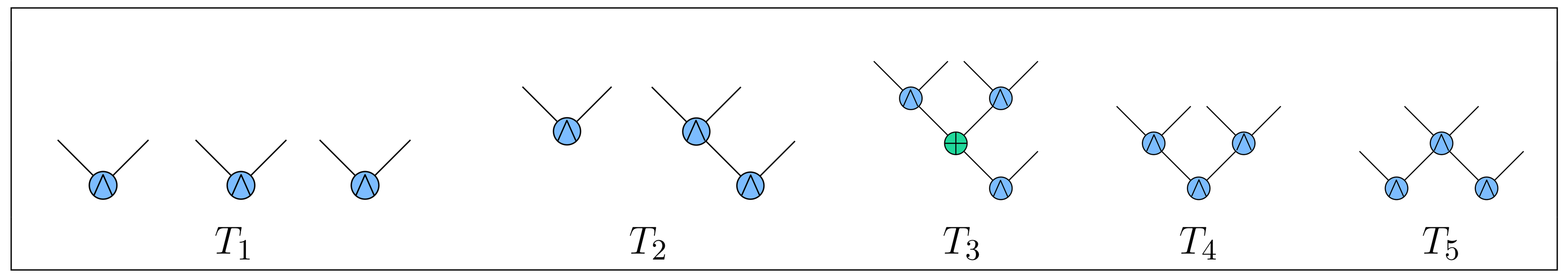
Goal: To identify the Boolean functions having MC 3 and 4.

Method: MC is affine invariant, it is enough to find the exhaustive list of affine equivalence classes that can be generated with 3, and 4 `AND` gates. Method has two parts:

- *Part I:* Identify the topologies having $k = 3, 4$ `AND` gates.
- *Part II:* Evaluate topologies to find unique representative from each affine equivalence class.

Results

- There are 24 equivalence classes with MC 3. They can be generated using at least one of the following topologies.



- The number of n-variable Boolean functions with MC 3 is

$$\sum_{d=4}^{6} \left(2^{n-d} \prod_{i=0}^{d-1} \frac{2^n - 2^i}{2^d - 2^i} \beta_d \right)$$

where $\beta_4 = 32\,768, \beta_5 = 775\,728\,128, \beta_6 = 183\,894\,007\,808$.

- There are 1277 equivalence classes with MC 4. They can be generated using one of the 84 topologies with 4 AND gates.

References

- Ç. Çalık, M. Sönmez Turan, R. Peralta, *Boolean Functions with Multiplicative Complexity 3 and 4*, submitted to Cryptography and Communications, Special Issue on Boolean Functions and Their Applications, 2019
- L.T.A.N. Brandão, Ç. Çalık, M. Sönmez Turan, R. Peralta. *Upper Bounds on the Multiplicative Complexity of Symmetric Boolean Functions*, Cryptogr. Commun., 2019. https://doi.org/10.1007/s12095-019-00377-3
- Ç. Çalık, M. Dworkin, N. Dykas, R. Peralta, *Searching for Best Karatsuba Recurrences*, To appear in Proceedings of Symposium on Experimental Algorithms, Springer 2019.

Poster produced for the NIST-ITL Science Day 2019 — November 06, 2019 (Gaithersburg MD, USA)