EasyChair Preprint

№ 782

Improved heuristic for multiplicative depth minimization of boolean circuits

Pascal Aubry, Sergiu Carpov and Renaud Sirdey

February 20, 2019

Improved heuristic for multiplicative depth minimization of boolean circuits

Pascal Aubry, Sergiu Carpov, Renaud Sirdey

CEA, LIST

Point Courrier 172, 91191 Gif-sur-Yvette Cedex, France

Mots-clés : *homomorphic encryption, multiplicative depth, boolean circuits*

1 Introduction

In somewhat homomorphic encryption schemes (e.g. B/FV, BGV) the size of ciphertexts and the execution performance of homomorphic operations depend heavily on the multiplicative depth. In this work we propose an improved multiplicative depth minimization heuristic. In particular, a new circuit rewriting operator is introduced, the so called cone rewrite operator. The results we obtain using the new method are relevant in terms of accuracy and performance compared to previous works. Smaller multiplicative depths for a benchmark of boolean circuits are obtained when compared to previous work. In average, the multiplicative depth is lowered by approximatively 5 times and heuristic execution performance is significantly improved.

2 Improved heuristic

A boolean circuit is a directed acyclic graph $C = (V, E)$ with a set of nodes V and a set of edges E. Circuit nodes represent boolean functions (gates) and circuit edges are connections between nodes. In this work we suppose that the boolean circuits use AND and XOR operators only. The set $\{\mathrm{AND}, \mathrm{XOR}\}$ together with the constant "1" is functionally complete. In a boolean circuit the maximal number of successively executed AND operators is called circuit *multiplicative depth* and it influences the parameterization of HE schemes. The minimization of the multiplicative depth allows not only to obtain smaller ciphertext sizes but also to minimize the overall execution time of the boolean circuit.

2.1 Multiplicative cone rewrite operators

We call the *critical circuit* (or critical part of a circuit) the set of nodes of a boolean circuit which influence circuit multiplicative depth. Decreasing the multiplicative depth of the critical part will necessarily decrease the overall circuit multiplicative depth. In the litterature, a multi-start heurisitic based on a rewrite operator for multiplicative depth-2 paths exists. In this work, we extend this operator introducing a depth-2 cone rewrite operator. A multiplicative depth-2 critical cone δ^2 is a boolean structure ending by an AND gate v_t and beginning with AND gates $v_1, \ldots, v_n$, such that $v_i \in \mathrm{anc}(v_t)$ and $l(v_i) = l(v_t) - 1$, for any $i = 1, \ldots, n$. The left-hand side of illustrates such a cone. The outputs of $v_1, \ldots, v_n$ are combined by a XOR gate U_y and connected to one input of node v_t. Let a_t be the input of v_t other than U_y. We denote $a_1^{(i)}$ and $a_2^{(i)}$ the 2 inputs of v_i such that $l\left(a_1^{(i)}\right) \geq l\left(a_2^{(i)}\right)$ and by $y_1, \ldots, y_m$ the inputs of XOR gate U_y which are not critical. Let

$$\left(\bigoplus_{i=1}^{n}\left(a_1^{(i)} \cdot a_2^{(i)}\right) \oplus \bigoplus_{i=1}^{m} y_i\right) \cdot a_t.$$

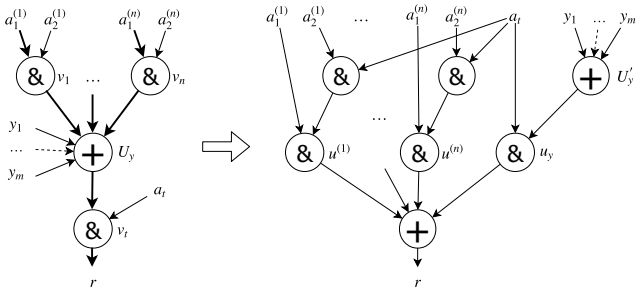

FIG. 1 – Critical depth-2 cone rewrite operator. Thick edges represent the critical paths.

It can be rewritten as

$$\left(\bigoplus_{i=1}^{n}\left(a_t \cdot a_2^{(i)}\right) \cdot a_1^{(i)}\right) \oplus \left(a_t \cdot \bigoplus_{i=1}^{m} y_i\right).$$

We obtain a new boolean structure (right-hand side of illustration) which minimizes the multiplicative depth of r by one. Depth-2 cone rewrite operators can also be extented to depth-K cone.

2.2 Improved heuristic

We propose a heuristic aiming to minimize the multiplicative depth of boolean circuits. At each iteration a minimal set Δ^{min} of depth-K cones is computed. Then the cones of this set are transformed and the multiplicative depth of circuit nodes is updated. We aim at finding a minimum sized set Δ^{min} of multiplicative depth-K cones such that each critical path in C contains the terminal gate of at least one cone δ^K from this set. This problem is related to the DVD (DAG vertex deletion) problem.The DVD problem is $\mathcal{UG}$-hard. A heuristic is used to find solution to the DVD problem.

As we have observed empirically, the decrease of circuit multiplicative depth makes the new critical circuit wider and wide. Respectively, the number of newly added gates (due to rewrite operators) increase in a non-linear way in the worst-case scenarios.

2.3 Experimental results

Boolean circuits from the EPFL Combinational Benchmark Suite were used for experimentations. In our experiments we have used only the first two types of circuits from this benchmark : 10 arithmetic and 10 random/control circuits. The number of gates varies from several hundreds to hundred of thousands.

The heuristic described in the previous section was implemented in C language. An Intel Core i7-7600U CPU @2.80GHz×4 was used as execution platform. Comparing to previous works, this improved heuristic gives better results for almost every benchmark. When multiplicative depth obtained is equal, the number of AND nodes is lower. In average the multiplicative depth decreases by more than 4.5 times. In term a computational performance the new heuristice is clearly faster (10 times faster for certain benchmarks).

3 Conclusions and perspectives

The heuristic uses advanced rewrite operators for boolean circuit for minimizing multiplicative depth.This depth is reduced by searching for a set of reducible cones and then rewriting them. In majority of benchmarks we have obtained smaller multiplicative depth circuits within a much lighter computational budget than in previous works. Some improvements of the heuristic can be envisaged. For example, the trade-off between reduction of multiplicative depth and the number of newly created AND gates must be considered better in the context HE execution.