# An Algorithm for Reversible Logic Circuit Synthesis Based on Tensor Decomposition

**Panjin Kim**
Hochang Lee, Kyung Chul Jeong, Daewan Han

*The Affiliated Institute of ETRI, Daejeon, Republic of Korea*

pansics@hotmail.com

An algorithm for reversible logic synthesis is proposed. The task is, for given $n$-bit substitution map $P_n : \{0,1\}^n \rightarrow \{0,1\}^n$, to find a sequence of reversible logic gates that implements the map. The gate library adopted in this work consists of multiple-controlled Toffoli gates denoted by $C^mX$, where $m$ is the number of control bits that ranges from 0 to $n - 1$.

The main idea is to view an $n$-bit substitution map as a rank-$2n$ tensor and to transform it such that the resulting map can be written as a tensor product of a rank-$(2n - 2)$ tensor and the $2 \times 2$ identity matrix. The process is iteratively applied until it reaches tensor product of only $2 \times 2$ matrices.

Time complexity of the algorithm is exponential in $n$ as most previously known algorithms for reversible logic synthesis also are, but it terminates within reasonable time for not too large $n$ which may find practical uses. Our primary target is to reduce the number of Toffoli gates in the output circuit. Benchmark results show that the algorithm works well for hard benchmark functions, but it does not seem to be advantageous when the function is structured. A working code written in Python is publicly available from GitHub. The algorithm is applied to find reversible circuits for cryptographic substitution boxes which are being used in some block ciphers.