# A Low-Power Parallel Architecture for Linear Feedback Shift Registers

# Abstract:

Linear feedback shift registers (LFSRs) are used to implement BCH encoders and cyclic redundancy check (CRC), which are broadly used in digital communication systems. Previous parallel LFSR designs adopt a state-space transformation that shortens the feedback data path and reduces the gate count. Transformations have been designed to minimize the total gate count of the three involved matrix multiplications. However, the transformation matrix multiplication is only active for one clock cycle at the end. In this brief, we propose an alternative transformation matrix construction that effectively shifts the complexity from the other two matrices, which are active in every clock cycle, to the transformation matrix without increasing the critical path or the total gate count. For an example CRC-32, the proposed design achieves 33% power and 8% gate count reductions without compromising the achievable clock frequency.

**Tools used:**

**Xilinx13.2**