# Scalability of SHA-3 Finalists for Lightweight Implementations on FPGAs

Jens-Peter Kaps

## Abstract

The competition for the new cryptographic hash algorithm SHA-3 by the National Institute for Standards and Technology (NIST) in the US has entered its final round. One of several important criteria with which NIST will determine the winner amongst the final five candidates is the ability of the hash function to be scalable even for low resource devices [1]. Determining this scalability is difficult to achieve. Horizontal folding is a technique that reduces the size of a full-scale implementation by reducing the number of operations implemented in dedicated units. It is therefore limited by the regularity of the algorithm. Vertical folding reduces the datapath width and is limited by the symmetry of the datapath. A recent study by Homsirikamol et al. [2] shows that these simple scaling techniques reach their limit for the five finalists at implementation sizes on Xilinx Spartan-3 devices at 608 slices for BLAKE to 3369 slices for Keccak which could not be folded. We have recently completed our lightweight implementations of the SHA-3 finalists with the goal of fitting into 500 slices and one Block RAM on Spartan-3. In this presentation, we use our implementations to explore the design space of all candidates between our results and the simple scaling techniques of [2]. In particular we are trying to answer the question, how much additional area do we need to spend in order to achieve a disproportionate increase in the throughput over area ratio. This will give us an insight into the scalability of the SHA-3 finalists for lightweight implementations on FPGAs.

## References

[1] Announcing request for candidate algorithm nominations for a new cryptographic hash algorithm (SHA-3) family. Federal Register/ Vol. 72, No. 212, Nov 2007. Notices 62212.

[2] Ekawat Homsirikamol, Marcin Rogawski, and Kris Gaj. Comparing hardware performance of round 3 SHA-3 candidates using multiple hardware architectures in Xilinx and Altera FPGAs. ECRYPT II Hash Workshop 2011, May 2011.