Comparison of Multi-Purpose Cores of Keccak and AES

Panasayya Yalla Ekawat Homsirikamol **Jens-Peter Kaps**

Cryptographic Engineering Research Group (CERG)
http://cryptography.gmu.edu
Department of ECE, Volgenau School of Engineering,
George Mason University, Fairfax, VA, USA

Design, Automation & Test in Europe – DATE 2015
March 11th, 2015

Comparison of Multi-Purpose Cores of Keccak and AES

- Security protocols (IPSec, SSL, TLS, etc.) provide several cryptographic services requiring multiple dedicated algorithms.
- Alternative: using a single cryptographic primitive in various modes for all secret key functions.
- We investigated AES and Keccak f-function.
- Typically AES is smaller and has better throughput over area ratio (TP/Area) then Keccak.
- High-speed and low area implementations each.
- Multi-purpose Keccak outperforms AES by a factor of 4 (TP/Area) on average across devices and modes.
- Keccak in AE-mode (Keyak) achieves a TP of 23.2 Gbps on Xilinx Virtex-7 and 28.7 Gbps on Altera Stratix-IV.
- Dedicated Keyak outperforms AES-GCM by a factor of 6 on average across all devices.