Improving the security and the scalability of the AES algorithm

Alessandro A. Nacci, *Politecnico di Milano*
Vincenzo Rana, *Politecnico di Milano*
Marco D. Santambrogio, *Politecnico di Milano*
Donatella Sciuto, *Politecnico di Milano*

Although the reliability and robustness of the AES protocol have been deeply proved through the years, recent research results and technology advancements are rising serious concerns about its solidity in the (quite near) future. In fact, smarter brute force attacks and new computing systems are expected to drastically decrease the security of the AES protocol in the coming years (e.g., quantum computing will enable the development of search algorithms able to perform a brute force attack of a 2n-bit key in the same time required by a conventional algorithm for a n-bit key). In this context, we are proposing an extension of the AES algorithm in order to support longer encryption keys (thus increasing the security of the algorithm itself). In addition to this, we are proposing a set of parametric implementations of this novel extended protocols. These architectures can be optimized either to minimize the area usage or to maximize their performance. Experimental results show that, while the proposed implementations achieve a throughput higher than most of the state-of-the-art approaches and the highest value of the *Performance/Area* metric when working with 128-bit encryption keys, they can achieve a 84× throughput speedup when compared to the approaches that can be found in literature working with 512-bit encryption keys.

ACM Categories & Descriptors: E.3 Data Encryption;

Keywords: cryptography; AES; Advanced Ecryption Standard; security; FPGA