Toward a Universal High-Speed Interface for Authenticated Ciphers

Ekawat Homsirikamol, William Diehl, Ahmed Ferozpuri, Farnoud Farahmand,
Malik Umar Sharif, and Kris Gaj
George Mason University

Abstract

In this talk, we would like to propose a universal hardware interface and the related communication protocol to be used in all future implementations of authenticated ciphers submitted to the CAESAR competition. A common interface would help in reducing any potential biases, and would make the comparison in hardware more reliable and fair. By design, our proposed interface will be equally suitable for hardware implementations of authenticated ciphers developed manually (at the register-transfer level), and those obtained using high-level synthesis tools. Our implementation of the proposed interface and communication protocol includes universal, open-source pre-processing and post-processing units, common for all CAESAR candidates.

The main features of our interface, communication protocol, and the associated pre-processing and post-processing units include:

- support for inputs of arbitrary size (as long as the size is a multiple of a byte)
- full support for padding input blocks, and clearing any portions of output words not belonging to ciphertext or plaintext
- storing decrypted messages internally, until the result of authentication is known, and thus preventing the output of the decrypted messages if the tag is invalid
- an overlap among, processing the current input block, reading the next input block, and writing the previous output block (supporting maximum throughput for long messages)
- lack of influence on the maximum clock frequency (and thus throughput) of the entire cryptographic core
- simple high-level communication protocol (allowing the processing of inputs even if the full input's length is unknown at the time when the processing starts [as long as the algorithm itself supports this capability])
- ability to communicate with very simple, passive devices, such as FIFOs
- support for the burst transfer, characteristic for many high-speed communication bus protocols
- ease of extension to realistic lower-level interfaces/protocols, such as AMBA-AXI (emerging as a de-facto standard for Systems-on-Chip) and PCI Express (for high-bandwidth serial communication between PCs and hardware accelerator boards).

Apart from the full documentation, examples, and the source code of the pre-processing and post-processing uniits, we are planning to make available in public domain:

- a universal testbench to verify the functionality of any CAESAR candidate implemented using the GMU interface, and
- VHDL wrappers used to determine the maximum clock frequency and the resource utilization of all implementations.

We hope that the existence of these resources will substantially reduce the time necessary to develop hardware implementations of all CAESAR candidates for the purpose of evaluation, comparison, and future deployment in real products.

In particular, we will provide a clear path of extending designs based on the proposed interface to IP (Intellectual Property) cores supporting all basic variants of the de-facto industry standard for system-on-chip buses, developed by ARM Co., called AXI4 (Advanced eXtensible Interface 4).

So far, our approach has been verified using AES-GCM and ten arbitrarily selected CAESAR candidates, and the initial results are promising. However, a comprehensive discussion is needed in order to further optimize our approach and make it acceptable for other groups. We hope that our talk at CryptArchi 2015 will serve as an invitation for such a discussion and lead to multiple improvements and the wide adoption of our specification and the related open-source codes in the future implementations of CAESAR candidates and other authenticated ciphers.