

Multiple Algorithm Implementation Challenge

A major U.S. semiconductor manufacturer with a focus on communications applications was faced with the challenge of accelerating multiple cryptographic algorithms in a single system-on-chip (SoC).

Deployment of a faster central processing unit (CPU) could not deliver the requisite acceleration. Moreover, the cost and gate consumption of an additional processor precluded the multi-processor option which, in any case, did not deliver an acceleration that scaled with the hardware resources.

The manufacturer determined that the traditional alternative of implementing each algorithm in a dedicated fixed function hardware block could not meet the product's time to market, area consumption and re-usability objectives.

Application Coprocessor Solution

The manufacturer selected CriticalBlue's Cascade Application Coprocessor synthesis solution.

A Cascade-synthesized application coprocessor offers the programmability of a processor with the parallel processing performance of a fixed function hardware block. Consequently, it can be programmed to execute multiple algorithms, while optimizing cross-algorithm resource sharing to minimize gate consumption.

Before proceeding with such a multi-application coprocessor design, the manufacturer first wished to

understand how its acceleration and resource consumption compared with multiple coprocessors, each synthesized to execute a single algorithm.

The manufacturer therefore synthesized two single-algorithm coprocessors to execute two secure hash algorithms – the SHA-1 and MD5 algorithms. Each coprocessor was synthesized using compiled binary executable software code that had been developed for single CPU operation.

The SHA-1 coprocessor achieved an acceleration of 5x over the original CPU implementation with neither code optimization nor the use of custom functional units, while the MD5 coprocessor achieved an acceleration of 10x using both code optimization and custom functional units (see table 1).

The manufacturer then synthesized a coprocessor optimized to execute both algorithms, achieving an overall acceleration of 6.4x. The design used both code optimization and custom functional units. Very importantly, the multi-algorithm coprocessor consumed only 8% more gates than either of the two single-algorithm coprocessors.

In Only Seven Days

The entire project – encompassing the synthesis of three coprocessors and the design of custom functional units – required seven engineer-days of effort.

Algorithm	Single-Algorithm Coprocessors		Multi-Algorithm Coprocessor
	SHA-1	MD5	SHA-1 + MD5
Lines of Original Code	150	700	850
Code Optimized?	No	Yes	Same as MD5
Custom Functional Unit?	No	Yes	Same as MD5
Boost vs. CPU	5x	10x	6.4x
Effort (in days)	1	5	1 More Day

Table 1: Multi-Algorithm Coprocessor Synthesis