



Achronix Taps Signal for 10/40/100 Gbps Encryption IP in World's Fastest FPGAs

128-bit key size AES cores designed for use in high-performance applications such as GPON (Gigabit-capable Passive Optical Network).

For More Information

Company Contacts:

Mark Konopacky
Signal Corp.
W. 408.476.0270
mark@signalcorp.com

Laurie Brunner
Achronix Semiconductor
W. 408.889.4144
lbrunner@achronix.com

San Jose, Calif. - Achronix Semiconductor, maker of the world's fastest field-programmable gate arrays (FPGAs), today announced the availability of new, high-performance Advanced Encryption Standard (AES) IP cores for its [Speedster™ 1.5 GHz family](#).

These high-performance 128-bit key size AES cores, from Portland, Oregon-based Signal Corp., are targeted at 10 Gbps, 40 Gbps, and 100 Gbps applications. They demonstrate the speed of the Speedster FGPA fabric, as well as the balance between throughput performance and resource minimization achieved by the Signal Cores.

"High-end 10/40/100G applications demand the highest-capability encryption engines to ensure security," said Ali Burney, SerDes and IP marketing manager for Achronix Semiconductor Corporation. "Signal's implementation with Achronix high performance FPGAs deliver peace of mind to system engineers while striking the right balance between resource allocation and performance."

The Achronix Speedster family, launched in September 2008 and offering three times the performance of conventional FPGAs, target traditional ASIC applications requiring high data throughput. Many of these also require increasingly sophisticated encryption algorithms to thwart hacking attempts from around the globe.

In order to achieve the performance and resource utilization targets, Signal implemented two configurations for the AES IP cores: a 16-bit core, aimed at 10 Gbps applications, features a pin-efficient 16-bit data path while a second, 128-bit data path core, targets 40 to 100 Gbps applications. Both cores use 128-bit keys and operate in CTR (counter) mode, designed for use in high-performance applications such as GPON (Gigabit-capable Passive Optical Network). The cores are provided in standard Verilog or VHDL RTL, together with simulation models, test benches and complete documentation.

"Information assurance is of major importance in many of the markets Achronix is serving, so our partnership is an ideal fit," said Mark Konopacky, responsible for business development for Signal. "Our expertise in design and implementation of



computationally efficient, complex algorithms, coupled with our innovative development methodology, enabled Signalali to quickly explore many different microarchitectures during our development work to find the one ideally suited for deployment on Achronix' Speedster."

Signalali uses its Quattro™ technology to transform high-level descriptions of data-intensive functions, such as AES, automatically into high-performance RTL. These tools allow very rapid algorithm and microarchitecture exploration at the design level, allowing the Signalali's designers to quickly choose the best solution for specific implementation platforms. Quattro enabled Signalali's engineers to maximize usage of the capabilities of the Achronix Speedster FPGA architecture.

About Signalali

Privately held Signalali Corp. provides custom IP cores targeted at complex mathematics, fixed-function DSP and cryptographic applications. Signalali is a commercial spin-out from Galois Inc., founded in 1999 to use functional programming and formal methods to address challenges in information assurance and other government and industry problems. Find out more at <http://www.signalicorp.com>.

About Achronix

Achronix Semiconductor is a privately held fabless corporation based in San Jose, Calif. Achronix builds the world's fastest field programmable gate arrays (FPGAs) capable of up to 1.5 GHz peak performance. Achronix has sales offices and representatives in the United States, Europe, China, Japan, and Korea, and has research and design offices in Boston, Mass., Ithaca, N.Y., and Bangalore, India. Find out more at <http://www.achronix.com>.