



algotronix™

The core of  
your security





Data is moving from cables and private networks to wireless networks and the public internet. New paradigms such as 'Software as a Service' and 'Grid Computing' require that sensitive data is moved from the user's own computer systems onto third party servers accessed via the internet. Corporations are demanding that their media content is protected from consumers - and consumers are demanding that their personal data are protected from corporations.





Today, the walls around a home or office can no longer protect sensitive information. Your customers need strong encryption and you need Algotronix IP Cores.

# Algotronix<sup>®</sup> IP: because the world needs strong encryption



# AES is everywhere

The Advanced Encryption Standard (AES) standardised by NIST in 2001 and approved by NSA for classified data is at the heart of almost all modern data security protocols. Algotronix is the leading vendor of AES IP cores for FPGA chips.

	AES	Algotronix implementation of AES as specified in FIPS 197 and SP800-38A secures video data in transit over point to point microwave links
	AES Keywrap	Algotronix encryption cores are designed into communications system used by four NATO countries. The AES Keywrap algorithm protects sensitive key information in transit to mobile systems
	AES	Algotronix encryption cores are providing security for computerised casino gaming machines
	AES - CCM	Algotronix implementation of the Counter with CBC MAC mode provides the security for wireless networking standards including 802.11 WiFi and 802.15 WiMax
	AES - LRW	Algotronix implementation of the new IEEE1619 draft standard secures data in place on storage systems.
	AES - GCM	Algotronix implementation of the Galois Counter Mode according to NIST Draft Special Publication 800-38D protects very high speed communication networks based on IEEE 802.1AE MAC security.

Choosing encryption IP is about more than technical performance: it is about trust. Confidence in an IP core can be based on confidence in the supplier, independent certification of the product and on source code reviews.

Algotronix is a well established company based in Edinburgh, in the United Kingdom. It was founded in 1998 as a spin-out from Xilinx the leading vendor of FPGA chips. Algotronix' clients include multinational defence companies, government agencies and financial institutions. Algotronix has strong links to the leading FPGA research group at Imperial College in London and to the System on Chip design expertise of the Institute for System Level Integration (ISLI) in Scotland.

Algotronix' G2 AES core has been certified by NIST as a true implementation of AES and is designed into military communications equipment used by several NATO countries. Algotronix has a policy of obtaining NIST certification for all algorithms where this is available.

Many applications require a source code review of the encryption software before use. This is the only way to be certain that the core does not contain malicious 'Trojan Horse' functionality. Even when this is not done it makes sense to archive the source code of the encryption IP so that it could be analysed 'after the fact' if the system security was compromised.

Recognising this, Algotronix offers particularly competitive pricing on source code licences to its IP.

# Flexible Licensing for flexible IP



Algotronix makes evaluating its IP easy through the use of a one page 'NDA Style' evaluation agreement. The final licence is based on the Xilinx 'Sign Once' template and can be customised to meet the requirements of individual customers.

Algotronix offers a range of product licence options from netlist to source code and from single project to unlimited project licences. With an unlimited project licence the highly configurable G3 core offers an ideal organization wide solution.

Algotronix AES cores are configured using VHDL generic parameters to generate a wide range of implementation options allowing you to evaluate area and performance tradeoffs and select a final configuration late in the design cycle.

The cores support all the standard AES modes: ECB, CBC, OFB, CFB1, CFB8, CFB128 and CTR as well as 128, 192 or 256 bit key length and key-schedule generation in hardware or software. Although the cores are written in VHDL it is straightforward to integrate them in a Verilog design flow using a simple wrapper around the top level design unit.

The G3 core can be configured from ultra small, micropower 8 bit implementations delivering around 100Mbit/sec up to 10 Gigabit implementations with multiple 128 bit datapaths operating in parallel. Algotronix also offers cost effective unlimited project licences making it easy for an organisation to

standardise on G3 for every project that needs AES. The cores can be targetted at FPGAs from Xilinx, Altera and Actel as well as ASIC or even CPLD implementations. They are supplied with a 'Getting Started' application note which demonstrates the cores working on low cost vendor evaluation boards.

	Data Path	Benefits
<b>AES G2</b>	32 bits	NIST Certification Moderate priced access to source code. Good price / performance for typical applications
<b>AES G3</b>	8, 16, 32, 64 or 128 bits	Most complete implementation of AES available with very wide range of application. Unrivalled performance and density.

"The Algotronix AES IP core is at the heart of the security system in the QX-10 platform. We selected it because it offered an unrivalled level of performance and efficiency. Design integration was assisted by the expert support we received from Algotronix at every stage."

Jon Jayal, Design Engineer, Quixant Ltd.

# www.algotronix.com

algotronix ltd PO Box 23116 Edinburgh EH8 8YB United Kingdom +44 131 556 9242