



Security IP-Cores

AES Encryption & decryption • RSA Public Key Crypto System • H-MAC SHA1 Authentication & Hashing



l e a d i n g t h e w a y

l e a d i n g t h e w a y

Secure your sensitive content, guarantee its integrity and protect it from piracy.

intoPIX provides a broad range of security IP-Cores dedicated to Broadcast, Video Transmission, Post-production, Archiving, Digital Cinema applications ...



IP-Cores that can secure your system integration

AES encryption & decryption
RSA Public Key Management
HMAC-SHA1 Authentication & Hashing

In order to offer the most complete solution to customers, intoPIX has developed a broad range of security IP-Cores.

These solutions perfectly complete the JPEG 2000 codec family in several domains and applications.

intoPIX specializes on highly efficient IP-Cores in the security and cryptography area. Whether you need key management or content protection, our solutions are usually the smallest, fastest, and most suitable choices on the market. These IP-Cores can also be perfectly combined with all intoPIX JPEG 2000 solutions and have been designed to be the most cost-effective in the market.



THE intoPIX PLUS

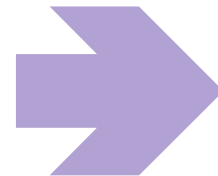
- Efficient FPGA footprint
- Flexible architecture
- Field upgradeable
- Customizable
- High Bitrate Capable





■ Security IP-Cores

IPX-AES: AES Symmetric Security Range



GENERAL DESCRIPTION

The family of IPX-AES IP-Cores provides an efficient FPGA implementation of the Advanced Encryption Standard (AES). Its flexibility allows the combination of several functions and operating modes for a very small FPGA footprint.

The family of IPX-AES IP-Cores is an encryptor / decryptor core range that efficiently implements in FPGA the Advanced Encryption Standard as specified in the Federal Information Processing publication FIPS-197 of the National Institute of Standards and Technology.

The IPX-AES module can be customized to ensure its optimization for a wide range of specific application fields with a design architecture that can be adapted to support from low up to very high bit-rates. Its flexibility allows combining several functions and operating modes on very small footprints.

FEATURES

KEY FEATURES

Multiple stream management
Renewable security

TECHNICAL DESCRIPTION

Functions

With addressing keys of 128, the IPX-AES cores execute decryption or encryption.

Data-stream handling

The IPX-AES cores can handle the data and secret keys in two different ways. The single stream option consists of a core capable of managing data with a single key, before a new update of this key. The multiple stream option is a feature capable of managing multiple ciphering processes together, each based on a different secret key.

Chaining modes

The inter-data-block chaining supports all existing modes that can be used separately or combined into a single design: ECB (Electronic Code-Book), CBC (Cipher Block Chaining), CTR (Counter). Other modes could be supported.

Data busses

The incoming, outgoing and key data are handled on either common or separate buses. Data bus width is 128 bits wide.

Clock

The processes use a single clock and can be reset asynchronously.

	OPTIONS	IPX-AES-MD	IPX-AES-M	IPX-AES-H
Functions	Encryptor	-	✓	✓
	Decryptor	✓	-	-
Throughput bit rate	2,5 Gbps	✓	✓	✓
	3,7 Gbps	-	✓	✓
	15 Gbps	-	-	✓
Data-stream handling	Single Stream	✓	✓	✓
	Up to 16 streams	✓	-	-
Operation modes	ECB	✓	✓	✓
	CBC	✓	-	-
	CTR	-	✓	✓
AES Data and Key Bus widths	128 bits	✓	✓	✓

APPLICATIONS

- Digital Cinema (DCI).
- Secure Content applications in Broadcast, Post-production, Archiving, Video Surveillance, Medical Imaging.
- Digital Right Management (DRM).



RESOURCES

IPX-AES-MD 1Gbps Multi Assets Decryptor		
	Virtex-4	Virtex-5
Slices	1300 slices	800 slices
RAMBs	8	4
Work Frequency	200 Mhz	220 Mhz
Encryption/decryption cycle count	11 Clock Cycles	11 Clock Cycles
Encryption throughput	2,3 Gbit/s	2,5 Gbit/s
Key update cycle count	66 cycles	66 cycles

IPX-AES-M HD/ DC-2K- Link-Encryptor		
	Virtex-4	Virtex-5
Slices	750 slices	500 slices
RAMBs	8	0
Work Frequency	250 Mhz	320 Mhz
Encryption/decryption cycle count	11 Clock Cycles	11 Clock Cycles
Encryption throughput	3 Gbit/s	3,7 Gbit/s
Key update cycle count	On the fly	On the fly

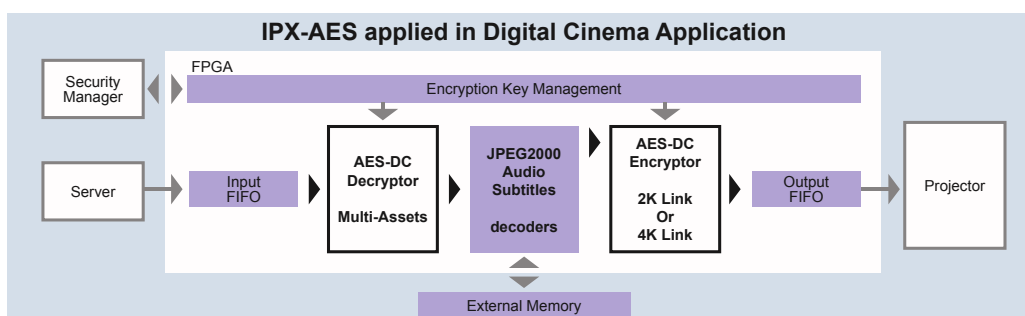
IPX-AES-H DC-4K-Link-Encryptor		
	Virtex-4	Virtex-5
Slices	3000 slices	2000 slices
RAMBs	32	0
Work Frequency	250 Mhz	320 Mhz
Encryption/decryption cycle count	11 Clock Cycles	11 Clock Cycles
Encryption throughput	12 Gbit/s	15 Gbit/s
Key update cycle count	On the fly	On the fly

EXAMPLE: A DIGITAL CINEMA APPLICATION

These three versions of the IPX-AES are designed specifically to meet Digital Cinema needs, and demonstrate how efficient the IPX-AES can be.

The modules specified are designed for Xilinx FPGAs and comply with the Digital Cinema Initiative requirement Specification V1.2.

The IPX-AES-MD Multi-Assets Decryptor can manage multiple assets together (video, audio and subtitles) without AES core updates. This core is also capable of bypassing the decryption process for non-encrypted data. The IPX-AES-M-2K and IPX-AES-H-4K Link Encryptors or the IPX-AES-H-4K-Link-Encryptor can be used to re-encrypt the uncompressed data between the mediablock and the projector.





IPX-RSA: RSA Public Key cryptography accelerator

GENERAL DESCRIPTION

The modular exponentiation accelerator IPX-RSA is an efficient arithmetic coprocessor for the RSA public-key cryptosystem. It performs the $A^e \text{ mod } M$ calculation and therefore offloads the most computer-intensive operation of RSA from the main processor. The RSA cryptosystem can be used for public key encryption, decryption and signature/authentication. It is currently the most deployed public key scheme and is used in well-known standards such as SSL/TLS secure internet access, IPsec Virtual Private Networks and S/MIME secure email.

The key advantage of the IPX-RSA IP-Core is its low footprint, thanks to an efficient balance between logic fabric and embedded RAMs and Multipliers.

Taking advantage of its high operating frequency, it is able of achieving a high throughput of modular exponentiations. As a result, this IP-Core provides a good compromise between processing time and resources compared to general purpose processors.

Other features of the IPX-RSA core are self-support and ease of use. The IP-core needs no interaction with the main processor during computation and requires no pre/post computation of the base and exponent (A and e). It is also accessed through a simple 32-bit processor bus.

KEY FEATURES

Low footprint

High throughput

2048-bit length inputs

Short exponent lengths
efficiently supported

No on-line pre/post computation

The IP-core targets the Xilinx Virtex-5 device. Performances on other Xilinx platforms can be provided on a request basis.

RESOURCES

	Virtex-4	Virtex-5
Slices	520 slices	280 slices
RAMBs	2 x 18 kb bRAMs	2 x 18 kb bRAMs
DSPs	2	2
Frequency	320 Mhz	350 Mhz
Throughput (2048-bit inputs)	6.6 op./s (13.5 kb/s)	7.2 op./s (14.8 kb/s)

IPX-HMAC-SHA1: Authentication & Hashing function

GENERAL DESCRIPTION

IPX-HMAC-SHA-1 IP-Core is the hashing function required for the content integrity check and content identification as specified in DCI document v1.2. It is designed for Xilinx Virtex-4 or Virtex-5 devices.

IPX-HMAC-SHA-1 is an implementation of the Key Hashed Message Authentication Code standard, which describes a mechanism for message authentication using cryptographic hash functions. It enables computation of the keyed-

hash message authentication code (HMAC) for audio and video assets.

This HMAC module uses the SHA1 core in combination with a secret key and the text message provided by the user in order to generate a fixed length MAC value.

The key advantages of the IPX-HMAC-SHA-1 IP-Core are its high throughput and low latency. Its interface can handle a frequency of at least 125 MHz, which is highly suitable for applications like Gigabit Ethernet.



KEY FEATURES

High operating frequency supported

Low footprint

Compatible with

Gigabit Ethernet data throughput

Ideal for Digital Cinema applications (DCI)

RESOURCES

	Virtex-4	Virtex-5
Slices	1130	700
RAMBs	0	0
DSPs	0	0
Frequency	125 MHz (and 250 MHz for internal core)	140 MHz
Throughput	512/88*250 MHz = 1.454 Gb/s	512/88*280 MHz = 1.629 Gb/s
Data	Split into groups of 128-bit	Split into groups of 128-bit



Security IP-Cores Matrix



		Xilinx Virtex 4 - FPGA Reference				Xilinx Virtex 5 - FPGA Reference				
		Slices	RAMBs	DSPs	Frequency	Slices	RAMBs	DSPs	Frequency	
Security IP-cores	IPX-AES-MD	1Gbps-Multi-Assets Decryptor	1300	8	0	200	800	4	0	220
	IPX-AES-M	HD/ DC-2K- Link-Encryptor	750	8	0	250	450	5	0	320
	IPX-AES-H	DC-4K-Link-Encryptor	3000	32	0	250	2000	0	0	320
	IPX-RSA	RSA Public Key cryptography accelerator	520	2	2	320	280	2	2	350
	IPX-HMAC- SHA1	HMAC-SHA1 Authentication & Hashing function	1130	0	0	125	700	0	0	140

l e a d i n g t h e w a y

About intoPIX

intoPIX develops and commercializes high-end image processing and security tools in large data streams with high intrinsic value. The applications are aimed especially at pictures having demanding requirements in quality, security and authoring rights. Based in Louvain-la-Neuve (Belgium), intoPIX was established in 2005, quickly becoming the international reference for hardware JPEG 2000 coding solutions.

intoPIX's world leading expertise includes FPGA and software engineering, JPEG 2000 image compression and symmetric-asymmetric security.

intoPIX's solutions are dedicated to the Digital Cinema, Digital Archiving, Camera, Field Recorder, Video Server, Broadcast contribution and Wireless transmission areas.

intoPIX efficiently combines on-chip hardware and software operations for an optimal co-design repartition of the coding blocks, it also provides a unique post-deployment core renewability for field upgrade and update. intoPIX IP-cores are especially targeting image and video applications.

More information

Ask intoPIX how to bring your JPEG 2000 requirements to life!

Email : sales@intopix.com

Information provided is accurate at the time of publication, however, no responsibility is assumed by intoPIX for its use, nor for any infringements of patents or other rights of third parties that may result from its use. Specifications Subject to change without notice. No license is granted by implication or otherwise under any patent or patents rights of intoPIX. Trademarks and registered trademarks are the property of their respective owner.



intoPIX s.a.
Place de l'Université 16
B-1348 Louvain-la-Neuve
Tel.: +32 10 23 84 70
Fax: +32 10 23 84 71

www.intopix.com