Survey of commercially available cryptographic chips and IP cores implementing cryptographic algorithms
(December 2005)

P. Arora, M. Dugan, P. Gogte, GMU

Abstract— **The objective for this project is to analyze the cryptographic chips and IP cores that are commercially available today. This analysis includes a market survey and seeks out any published datasheets and implementations for these chips. From the published data, the project analysis includes a review of the advertised parameters and establishes evaluation criteria upon which a product comparison can be made. This project attempts to offer a "best of class" product based on the evaluation criteria.**

***Index Terms*—IP core, Cryptographic Chip, TPM, Security cores, Security Chip.**

I. Introduction

Due to an increasing demand for system security, a large computational burden is being placed on computing resources to perform cryptographic operations. To prevent these operations from affecting the overall system performance, a new breed of chips has emerged that handles all cryptographic and system security requirements. Although these new chips offer greater flexibility when designing a system, computer designers need to carefully consider the parameters of each product to ensure that all security needs are met.

The objective for this project is to analyze the cryptographic chips and IP cores that are commercially available today. This analysis includes a market survey and seeks out any published datasheets and implementations for these chips. From the published data, the project analysis includes a review of the advertised parameters and establishes evaluation criteria upon which a product comparison can be made. This project attempts to offer a "best of class" product based on the evaluation criteria

II. IP Cores

An IP (intellectual property) core is a block of logic or data that is used in making a field programmable gate array (FPGA) or application-specific integrated circuit (ASIC) for a product.

Manuscript received Dec 19, 2005.

P. Arora, and. Gogte are electrical engineering students at George Mason University under the supervision of Dr. Gaj (parora@gmu.edu, pgogte@gmu.edu)

M. Dugan is a computer engineering student at George Mason University under the supervision of Dr. Gaj. (mdugan@gmu.edu)

IP cores are a major part of the electronic design automation (EDA) industry trend which repeatedly uses previously designed components. An IP core is a design function with well-defined interfaces. Many IP cores can be considered as a block of design for a specific chip that handles a specific functionality, and then evolves to a standard block of functionality, which can be used in multiple chips. An IP core should be entirely portable i.e.: it can be easily used in any vendor technology or design.

The difference between a block on a single design (chip) and an IP core is that the signaling protocol and the clock definition can be significantly different between chips. An IP core needs to be flexible enough to handle these differences.

Some examples of IP cores are Universal Asynchronous Receiver/Transmitter (UART), central processing units (CPUs), Ethernet controllers, and PCI interfaces.

III. Need for IP Cores

In today's rapidly growing chip technology, the number of gates per chip can reach several millions. To overcome the design gap generated by such fast-growing capacity and lack of available manpower, reuse of the existing designs becomes a very important concept in design methodology. IC designers typically use pre designed modules to avoid redesigning the entire logic for every new product. Utilizing the pre designed modules accelerates the development of new products to meet today's time-to-market challenges. By practicing design-reuse techniques ie: by using blocks that have already been designed, and verified, various blocks of a large ASIC/SOC can be assembled quite rapidly. Another advantage of reusing the existing blocks is to reduce the possibility of failure based on design and verification of a block for the first time. These pre designed modules are commonly called *Intellectual Property (IP) cores.*

IV. Intellectual Property Categories

To provide various levels of flexibility for reuse and optimization, IP cores are classified into three different categories: hard cores, soft cores and firm cores.

Hard IP cores: Hard cores are physical manifestations of the IP design. They consist of hard layouts using particular physical design libraries and are delivered in masked-level designed blocks (GDSII format- a stream format that represents hexadecimal description in variable length records to describe graphical data). These cores offer optimized implementation and the highest performance for their chosen physical library. The integration of hard IP cores is simple and the core can be dropped into an SOC physical design with very little effort. However, hard cores are technology dependent and provide minimum flexibility and portability in reconfiguration and integration across multiple designs and technologies. They are best for plug-and-play applications.

Soft IP cores: They are delivered as RTL (Register transfer level) VHDL code to provide functional descriptions of IP cores. These cores offer maximum flexibility and re configurability to match the requirements of a specific design application, however they must be synthesized, optimized, and verified by their user before integration into designs. Being synthesizable, soft IP cores are compatible with the ASIC design flow. The SoC design can therefore be optimized for a specific silicon process and performance target. Therefore, the quality of a soft IP is highly dependent on the effort needed in the IP integration stage of SOC design.

Firm IP cores: These cores are a combination of advantages of both hard cores and soft cores and balance the high performance and optimization properties of hard IP cores with the flexibility of soft IP cores. These cores are delivered in the form of targeted netlists (a list of the logic gates and associated interconnections making up an integrated circuit) to specific physical libraries after going through synthesis without performing the physical layout. They have a higher level of optimization and are targeted for a specific device architecture. They are less portable than soft cores.

TABLE I
Comparison of IP formats

IP Format	Representation	Optimization technology	Reusability
Hard	GDSII	Very High Technology Dependent	Low
Soft	RTL	Low Technology Independent	Very high
Firm	Netlist	High Technology Generic	High

V. Commercially Available Cryptographic IP core Vendors (by Algorithm)

AES1- IP cores, Helion, Actel, Amphion, Cast

DES, 3DES - Actel, Helion, Amphion, Cast

MD5- Cast, Helion, Amphion

SHA-1- Cast, Helion, Amphion

SHA-256 - Cast, Helion, Amphion

VI. IP Core Comparison Parameters

- Throughput- It is the data throughput which is a product of clock frequency in MHz and the number of bits of data per the number of clock cycles (bits/cycles)
- Clock frequency (Master clock)- performance in MHz
- Number of clock cycles- Number of clock cycles of operation
- Core support for encryption and decryption- specifies whether the same core can be used for both encryption and decryption
- Area/Resources- Represents the total number of logic cells/slices/gates used for the design of the IP core
- Key size- Number of bits of the key
- Message digest output- Number of bits of the hash value (Message digest)
- Modes of operation- specifies the modes the core supports

VII. IP Core Comparison charts for different cryptographic algorithms

The comparison parameters for all the IP cores are only the ones that are most important from the survey point of view. Hence other parameters that are common for all the IP cores are not listed in the tables. Eg: Modes of operation which are more or less the same for all IP cores depending upon the algorithms. Also, some parameters for some cores are not listed in the tables, as not all information is provided in the datasheets.

TABLE IIA
AES comparison chart

Vendor	Key size (Bits)	Throughput
IP Cores	128	160, 320, 640, 1280 Mbps- data path width of 8, 16, 32, 64 bits
Actel	128	224 ,102,291 Mbps - Depending on the family
Altera	128	> 2.5 Gbps
Helion	128,192,256	Standard > 500 Mbps Fastest > 2 Gbps
Cast	128,192,256	157 183, 295,316,400 Mbps - depending on the family
Athena	128,192,256	> 1GBps
Vocal Technologies , Ltd.	128,192,256	>2.5 Gbps

* Support all AES modes like ECB, CBC, CFB, OFB, CTR

TABLE IIB
AES comparison chart

Vendor	Clock frequency (MHz)	Area/Resources
IP Cores	200	2948 gates / 639 LUT /236 SLICES
Actel	75, 35, 100	5193 cells (2597 Slices), 5555 (2777 Slices), 3112 (1556 Slices)
Altera	120.39, 118.47	6167 , 6784 Logic cells- APEX EP20K400E
Helion	> 200	Standard < 6K gates Fastest < 57K gates
Cast	54, 63, 102, 109, 138	450,425,365,244 Les (Logic Elements)
Athena	100	
Vocal Technologies, Ltd.		< 50k gates

TABLE III
DES comparison chart

Vendor	Throughput	Area	Clock frequency(MHz)
Actel	320 Mbps	1271 gates	80 ProASIC3/E family
Alliance core (Xilinx)	500 Mbps	286 slices- Spartan 2 family	63
Helion	> 1.25 Gbps	< 6K gates	> 180
Cast		438,438,355,568 LEs	83,84,97,190
Athena	> 500 Mbps		

* Support all DES modes like ECB, CBC, CFB, OFB

TABLE IV
Triple DES comparison chart

Vendor	Throughput	Clock frequency	Area
Actel	300 Mbps- ProASIC3/E	75 MHz- ProASIC3/E family	1413 cells/tiles (700 slices)
Algotronix		90 MHz	722 Slices (1444 cells)
Helion	> 460 Mbps	> 180 MHz	< 6K gates (maximum up to 500 slices)
Cast	240 Mbps at 180 MHz)	64, 82, 190 MHz	1720, 1699, 1757 LEs - family supported
Athena	> 500 Mbps		

TABLE V
MD5 comparison chart

Vendor	Through put	Clock cycles	Clock frequency	Area
Helion	1140 Mbps	65 per algorithm step + 1 clock loading per 512 bit block	145 MHz	16 K gates
Cast			25, 26, 39, 60, 69, 115 MHz	2262, 2261, 2285, 2290, 1527, 1259 LEs - Flex, Acex, Apex, Apex 2, Cyclone, Stratix 1, Stratix 2 families
Amphion		65 master cycles (1 clock per algorithm step + 1 clock load)	>212MHz	24-kgate design
Silicon designs International, Inc	400 Mbps	64 clocks to process single block (512 bits) of data	50 MHz	324 CLBs (1296 logic cells)

* 128 bit MD for all cores

TABLE VI
SHA-1 comparison chart

Vendor	Clock cycles/ 512 bit block	Through put	Clock freq	Area
Helion	82 cycles	937 Mbps 1810 Mbps Depends on family	150 MHz 290 MHz	approx 20 K approx gates 23 K
Cast	65 clock cycles	644 Mbps 676 Mbps 1156 Mbps	102 ,107 183MHz Depends on the family	1621, 1621 1445 LEs Cyclone, Stratix, Stratix 2 families
Amphion	81 master cycles (1 clock per algorithm step + 1 clock load)			
Silicon designs International , Inc	80 clocks	422.4 Mbps	66 MHz	579 Slices
Athena group, Inc		640 Mbps- 32 bits interface width		

* 160 bit MD for all cores

TABLE VII
SHA-256 comparison chart

Vendor	Throughput	Area	Clock cycles	Clock frequency
Helion	1163 Mbps 1963 Mbps	approx 23 K approx 26 K	66 cycles per 512 bit block	150 MHz 253 MHz
Cast	488.3 Mbps	980 Slices	49 clock cycles for 512 bit blocks	62 MHz- Spartan-3 family
Cadence	971 Mbps	21000 gates		133 MHz
HDL design use	363 Kbps, 1055 Kbps 1395 Kbps		65 clock cycles per 512 bit blocks	550 MHz- P3,Win 2000 professional, 440 MHz- Sun Sparc workstation,550 MHz- Red hat Linux V 7.1

* 256 bit MD for all cores

VIII. Best of Class IP Cores

The best of class IP cores are chosen on the basis of the various parameters like throughput which is the most important of the parameters and represents the efficiency of the IP core in terms of bits/sec. Tables VIII and IX list the AES IP cores with the throughput parameter. The higher the throughput, the efficient is the core.

TABLE VIII
AES algorithm – Based on throughput with one key size = 128 bits

Vendor	Throughput
IPCores	80 Mbps
Actel	224 Mbps
Altera	> 2.5 Gbps

TABLE IX
AES algorithm- Based on throughput with varying key sizes of 128, 192, 256 bits

Vendor	Throughput
Helion	> 2 Gbps
Cast	400 Mbps
Athena	> 1 Gbps
Vocal Technologies	> 2.5 Gbps

The other parameter that could be important is the core support for both encryption and decryption and Table X lists the IP cores which support both encryption and decryption in the same core or different cores.

TABLE X
AES algorithm- Based on core support for both encryption and decryption

Vendor	Same core / separate core
IPCores	Same core for encryption and decryption
Actel	Same core for encryption and decryption
Altera	Separate core for encryption and decryption
Helion	Separate core for encryption and decryption
Cast	Same core for encryption and decryption
Athena	Same core for encryption and decryption

The third important parameter of comparison is the Area/ number of resources in the IP core. It is given in terms of number of gates or number of Slices/ Logic cells. Different vendors provide this parameter in different units. The conversion used is: 12 Logic cells = 1 Slice, 4 Logic cells = 1 CLB. Table XI lists the area of IP cores in terms of number of logic cells.

TABLE XI
AES algorithm- Based on the area/ number of resources

Vendor	Area in number of Logic cells
IPCores	472
Actel	3112
Altera	6117
Helion	500
Cast	300

The next important parameter of comparison is the clock frequency, which represents speed of the core in terms of Hz ie: the number of clock cycles in 1 sec. Table XII lists the IP cores and their corresponding frequency.

TABLE XII
AES algorithm- Based on the clock frequency

Vendor	Frequency (MHz)
IPCores	200
Actel	100
Altera	120
Helion	> 200
Cast	138
Athena	100

So the best of class IP core for each algorithm is chosen based on the best of all parameters.
So, based on these observations, the best of all AES cores is the Helion Technology AES core, the next best could be Actel AES core.

TABLE XIII
DES algorithm- Based on throughput

Vendor	Throughput
Actel	320 Mbps
Alliance	500 Mbps
Helion	> 1.25 Gbps
Athena	> 500 Mbps

Helion , Athena , Alliance have the top 3 DES throughputs.

TABLE XIV
DES algorithm- Based on clock frequency

Vendor	Frequency(MHz)
Actel	80
Alliance	63
Helion	> 180
Cast	190

So, based on these observations, the best of all DES cores is the Helion Technology DES core.

TABLE XV
Triple DES algorithm- Based on throughput

Vendor	Throughput
Actel	320 Mbps
Helion	> 460 Mbps
Cast	240 Mbps
Athena	> 500 Mbps
Xilinx	500 Mbps

Athena, Helion, Xilinx have the top 3 DES throughputs

TABLE XVI
Triple DES algorithm- Based on clock frequency

Vendor	Frequency (MHz)
Actel	75
Algotronix	90
Helion	> 180
Cast	190

Helion, Cast, Algotronix have the top3 3DES frequencies.

TABLE XVII
Triple DES algorithm- Based on area / resources

Vendor	Area in number of Logic cells
Actel	1413
Algotronix	1450
Helion	1000
Cast	1720

So, based on these observations, the best of all Triple DES cores is the Helion Technology Triple DES core.

TABLE XVIII
MD5 algorithm - Based on clock frequency

Vendor	Frequency (MHz)
Helion	145
Cast	115
Amphion	> 212

Silicon Design Itnl, Inc	50

Amphion, Helion, Cast have the top 3 MD5 frequencies.

TABLE XIX
MD5 algorithm - Based on area / resources

Vendor	Area in number of Logic cells
Helion	Approx 2500
Cast	Approx 4000
Amphion	2262
Silicon Design Itnl, Inc	1296

So, based on these observations, the best of all MD5 cores is the Amphion MD5 core and the next best is the Helion Technology MD5 core.

TABLE XX
SHA-1 algorithm - Based on throughput

Vendor	Throughput (Mbps)
Helion	1810
Cast	1156
Silicon Design Itnl, Inc	422.4
Athena	640

Helion, Cast, Athena have the top 3 SHA-1 throughputs.

TABLE XXI
SHA-1 algorithm - Based on frequency

Vendor	Frequency (MHz)
Helion	290
Cast	183
Silicon Design Itnl, Inc	66
Athena	100

Helion, Cast, Athena have the top 3 SHA-1 frequencies.

TABLE XXII
SHA-1 algorithm - Based on clock cycles

Vendor	Number of clock cycles for 512 bit data
Helion	82
Cast	65
Silicon Design Itnl, Inc	80
Amphion	82

So, based on these observations, the best of all SHA-1 cores is the Helion Technology SHA-1 core.

TABLE XXIII
SHA-256 algorithm - Based on throughput

Vendor	Throughput
Helion	1963 Mbps
Cast	488.3 Mbps
Cadence	971 Mbps
HDL Design	1395 Kbps(Red Hat Linux system)

* HDL design- Operated on different system like 550 MHz-P3,Win 2000 professional, 440 MHz- Sun Sparc workstation,550 MHz- Red hat Linux V 7.1

TABLE XXIV
SHA-256 algorithm - Based on frequency

Vendor	Frequency (MHz)
Helion	253
Cast	62
Cadence	133
HDL Design	550

HDL,Helion, Cadence have the top 3 SHA-256 frequencies
So, based on these observations, the best of all SHA-256 cores is the Helion Technology SHA-256 core.

IX. Cryptographic Chips

In contrast to IP cores, Cryptographic chips are fully implemented hardware chips that provide not only cryptographic logic but also all necessary interfaces and I/O connections to allow them to be embedded into a larger system design. The idea is that a given system can add security services by incorporating an "off-the-shelf" cryptographic chip into the design. An example would be a router manufacturer who decides to design a new product that includes security services. In this case the router designer would select an appropriate cryptographic chip (which meets the necessary performance parameters like clock frequency, throughput, etc) that will be embedded into the design. Cryptographic chips are used in many applications including security services for web servers, virtual private networks (VPNs), gateway routers, secure storage transfers, and many more. The purpose of this report is to conduct a survey of commercially available cryptographic chips and to compare them by their published parameters.

X. Need for Cryptographic chips

In some instances it is preferable for a system designer to choose a pre-manufactured chip as opposed to the Intellectual Property (IP core) for designing a chip. This affords the system designer freedom from cryptographic chip development. This is important to note because the appliance manufacturer needs only to account for their own development cycle rather than the development of a specific chip within the design.

XI. Commercially Available Cryptographic Chip Manufacturers

When conducting the market survey, there were a total of ten vendors found as listed in table XXVI. Between them, the market includes a total of 44 cryptographic chips. Additionally, among the various chips available, most of them included support for NIST approved algorithms. The entire list of supported algorithms found among the vendors can be seen below in table XXVI.

TABLE XXV
Vendors

Crytographic Chip Manufacturers
Atmel
Broadcom
Cavium
Harris
HIFN
IBM
Mykotronx

TABLE XXVI
Algorithms

Algorithms supported
AES (128, 192, 256)
Triple DES
DES
ARC-4 (RC-4)
RSA (1024, 2048 & 4096)
DSA
Diffie-Hellman Key

Philips
SafeNet
Sinosun

Agreement
MD5
SHA-1 & SHA-256
HMAC

Although not included in this table, there were two additional algorithms that were found (SKIPJACK and KEA) however these were only offered on the Mykotronx cryptographic chip which only supports older algorithms and therefore is not really a competitor among the other products. In addition to these algorithms several vendors advertised the capability to sustain communications that adhere to protocols like Internet Key Exchange (IKE), Secure Sockets Layer (SSL) and IPsec. It is interested to note that among all of the products surveyed, none mentioned support for Elliptic Curve Cryptography.

XII. Cryptographic Chip Comparison Parameters

When conducting the market survey there were several common parameters that most vendors advertised in their product briefs and data sheets. These parameters, shown in Table XXVII, are the basis upon which a product comparison can be made. Probably of most importance are the algorithms and protocols supported as well as the chip throughput, but a system designer also needs to be cognizant of several other parameters as well. These parameters may include the clock frequency, the presence (and speed) of a true random number generator, the package type (like TQFP or PBGA), chip dimensions, and supported interfaces (like PCI). Because of the importance of these parameters, this market survey sought to extract as much information as possible to provide the best comparison of parameters.

TABLE XXVII
Typical published parameters for Cryptographic chips

Encryption Algorithms (symmetric & public key) as well as Hash algorithms supported
Modes of Operation
RNG Speed and whether its HW or pseudo
Typical Applications for chip
Throughput for AES-128
Throughput for AES-192
Throughput for AES-256
Throughput for DES and Triple-DES
Throughput for IPSec-AES (with either HMAC-SHA-1 or HMAC-MD5)
Throughput for IPSec-3DES (with either HMAC-SHA-1 or HMAC-MD5)
Throughput for SSL
Supported RSA bit lengths (1024, 2048, etc)
RSA signatures/sec
RSA Operations/sec (assumed to be Signatures/sec) (1024-b)
RSA signature verifications/sec
RSA time to generate key pair
DSA signatures/sec
DSA Operations/sec (assumed to be Signatures/sec) (1024-b)
DSA verifications/sec
Diffie-Hellman keys/sec or transactions/sec
Processor core
Clock Freq (both core and interface)
Package type (TQFP, PBGA, etc)
Package dimensions
Interfaces (pci, pcix) as well as memory controllers
On-chip memory
Certification (FIPS, EAL, CC, etc)
Voltage (both signal and Vcc)

One of the more difficult aspects of doing a market comparison is that not all manufacturers publish the same information. A typical example of this is with comparing throughputs; some manufacturers will be specific on what algorithm, bit length, mode of operation, and protocol used, while others will give just a generic statement like "provides half-duplex encryption and decryption at throughput data rates of up to 5 Mbps." Additionally, not all parameters are addressed in each of the product briefs which hinders a fair comparison.

XIII. Complete List of Commercially Available Cryptographic Chips Sorted by Algorithm

Tables XXVIII through XXXII that follow provide a complete alphabetical listing of all cryptographic chips that are currently available. The entire list of chips is organized by algorithm and since most, if not all chips, provide support for multiple algorithms some chips are listed in multiple charts.

TABLE XXVIII
Complete listing of AES Crypto Chips

Crypto chip	**IPSec-AES (Mbps)**	**IPSec-3DES (Mbps)**	**RSA Sig/s (1024-b)**	**DSA Sig/s (1024-b)**
Broadcom BCM5812	**50**	50	65	50
Broadcom BCM5823		500	550	
Broadcom BCM5825		950	12000	
Broadcom BCM5841	**4800**			
Cavium Nitrox I	**3200**	4000	42000	
Cavium Nitrox II	**10000**	2000	40000	
Cavium Nitrox Lite	**100**	2000	900	
Harris Citadel II				
HIFN 7814		150		
HIFN 7815		250		
HIFN		500		

Crypto chip	IPSec-AES (Mbps)	IPSec-3DES (Mbps)	RSA Sig/s (1024-b)	DSA Sig/s (1024-b)
7851				
HIFN 7854		500		
HIFN 7855		650		
HIFN 7955		276	84	77
HIFN 7956		500	84	77
HIFN 8350	**4000**	4000	375	675
HIFN 4300	**2000**	2000	10	17
HIFN 4350	**4000**	4000	300	540
HIFN 7954		138	42	38
HIFN 8065		350		
HIFN 8154		2300		
HIFN 8300	**2000**	2000	250	437
IBM Otello			3300	
SafeXcel 1141	**268**	4000	58	55
SafeXcel 1741	**535**		119	112
SafeXcel 1840	**1300**		1220	833
SafeXcel 1841	**2000**		1220	1250
SafeXcel 1842	**3200**		1400	1440
SafeXcel 5140	**90**			
SafeXcel 5150	**100**		96	
SafeXcel 5160	**300**			

TABLE XXIX
Complete listing of Triple-DES Crypto Chips

Crypto chip	IPSec-AES (Mbps)	IPSec-3DES (Mbps)	RSA Sig/s (1024-b)	DSA Sig/s (1024-b)
Broadcom BCM5801		**200**	N/A	N/A
Broadcom BCM5802		**150**	20	50
Broadcom BCM5805		**200**	100	300
Broadcom BCM5812	50	**50**	65	50
Broadcom BCM5823		**500**	550	N/A
Broadcom BCM5825		**950**	12000	N/A
Broadcom BCM5840		**2400**	N/A	N/A
Broadcom BCM5841	4800			
Cavium Nitrox I	4000	**3200**	42000	
Cavium Nitrox II	10000		40000	
Cavium Nitrox Lite	100		900	
HIFN 7902		**66**	10	9
HIFN 7814		**150**		
HIFN 4300	2000	**2000**	10	17
HIFN 4350	4000	**4000**	300	540
HIFN 7815		**250**		
HIFN 7851		**500**		
HIFN 7854		**500**		
HIFN 7855		**650**		
HIFN 7951		**66**	10	9
HIFN 7954		**138**	42	38
HIFN 7955		**276**	84	77
HIFN 7956		**500**	84	77
HIFN 8065		**350**		
HIFN 8154		**2300**		
HIFN 8300	2000	**2000**	250	437
HIFN 8350	4000	**4000**	375	675
IBM Otello			3300	
SafeXcel 1141	268	**160**	58	55
SafeXcel 1741	535	**321**	119	112
SafeXcel 1840	1300		1220	1250
SafeXcel 1841	2000		1220	1250
SafeXcel 1842	3200		1400	1440
SafeXcel 2141		**155**		
SafeXcel 5140	90			
SafeXcel 5150	100		96	
SafeXcel 5160	300			

TABLE XXX
Complete listing of ARC-4 (RC4) Crypto Chips

Crypto chip	IPSec-AES (Mbps)	IPSec-3DES (Mbps)	RSA Sig/s (1024-b)	DSA Sig/s (1024-b)

Crypto chip	IPSec-AES (Mbps)	IPSec-3DES (Mbps)	RSA Sig/s (1024-b)	DSA Sig/s (1024-b)
Cavium Nitrox II	**10000**		40000	
Cavium Nitrox I	**4000**	**3200**	42000	
SafeXcel 1842	**3200**		1400	1440
SafeXcel 1841	**2000**		1220	1250
SafeXcel 1840	**1300**		1220	1250
Cavium Nitrox Lite	**100**		900	
Broadcom BCM5812	**50**	**50**	65	50
HIFN 8154		**2300**		
Broadcom BCM5825		**950**	12000	N/A
HIFN 7855		**650**		
HIFN 7956		**500**	84	77
HIFN 7851		**500**		
HIFN 7854		**500**		
Broadcom BCM5823		**500**	550	N/A
HIFN 8065		**350**		
HIFN 7955		**276**	84	77
HIFN 7815		**250**		
HIFN 7814		**150**		
HIFN 7954		**138**	42	38
HIFN 7951		**66**	10	9
HIFN 7902		**66**	10	9

TABLE XXXI
Complete Listing of DES Crypto Chips

Crypto chip	IPSec-AES (Mbps)	IPSec-3DES (Mbps)	RSA Sig/s (1024-b)	DSA Sig/s (1024-b)
Cavium Nitrox II	**10000**		40000	
Broadcom BCM5841	**4800**			
HIFN 8350	**4000**	**4000**	375	675
HIFN 4350	**4000**	**4000**	300	540
Cavium Nitrox I	**4000**	**3200**	42000	
SafeXcel 1842	**3200**		1400	1440
HIFN 8300	**2000**	**2000**	250	437
HIFN 4300	**2000**	**2000**	10	17

Crypto chip	IPSec-AES (Mbps)	IPSec-3DES (Mbps)	RSA Sig/s (1024-b)	DSA Sig/s (1024-b)
SafeXcel 1841	**2000**		1220	1250
SafeXcel 1840	**1300**		1220	1250
SafeXcel 1741	**535**	**321**	119	112
SafeXcel 5160	**300**			
SafeXcel 1141	**268**	**160**	58	55
Cavium Nitrox Lite	**100**		900	
SafeXcel 5150	**100**		96	
SafeXcel 5140	**90**			
Broadcom BCM5812	**50**	**50**	65	50
Broadcom BCM5840		**2400**	N/A	N/A
HIFN 8154		**2300**		
Broadcom BCM5825		**950**	12000	N/A
HIFN 7855		**650**		
HIFN 7956		**500**	84	77
HIFN 7851		**500**		
HIFN 7854		**500**		
Broadcom BCM5823		**500**	550	N/A
HIFN 8065		**350**		
HIFN 7955		**276**	84	77
HIFN 7815		**250**		
Broadcom BCM5801		**200**	N/A	N/A
Broadcom BCM5805		**200**	100	300
SafeXcel 2141		**155**		
HIFN 7814		**150**		
Broadcom BCM5802		**150**	20	50
HIFN 7954		**138**	42	38
HIFN 7951		**66**	10	9
HIFN 7902		**66**	10	9
IBM Otello			3300	
Phillips GCD-o				

TABLE XXXII
Other miscellaneous Crypto Chips

Crypto chip	IPSec-AES (Mbps)	IPSec-3DES (Mbps)	RSA Sig/s (1024-b)	DSA Sig/s (1024-b)
Sinosun SSX35	N/A	N/A	8	
Atmel AT97SC3201 TPM	N/A	N/A	2	
Broadcom 6500	N/A	N/A	190	546
Mykotronx MYK-82A	N/A	N/A		25
Harris Citadel	N/A	N/A		

XIV. Best of Class Comparison for Cryptographic Chips

Once all of the parameters for each of the cryptographic chips were complied into a comprehensive listing some comparisons could be made. Since there were several parameters for which some vendors did not provide information, the "best of class" comparison had to be made only on the parameters for which the most information was available. As such, seven categories out of the entire list of parameters were chosen for rating. These included the highest throughputs for IPSec-AES & IPSec-3DES, the fastest implementations of RSA, DSA, & Diffie-Hellman, chips that provide support for the most algorithms, and the speed of the random number generator.

Throughput is probably the most important parameter that should be compared when surveying cryptographic chips because the system needs to be designed such that the security functions do not create a "bottleneck" for all communications. The five best chips for IPSec throughput (AES and Triple DES, respectively) are provided in tables XXXIII and XXXIV.

TABLE XXXIII
Top 5 highest throughputs for IPsec-AES

Crypto chip	Throughput IPSec-AES	Application
Cavium Nitrox II	**10 Gbps**	VPN Gateway, IPSEC & SSL Server connections, Server Load balancing, and Server backup
Broadcom BCM5841	**4.8 Gbps**	High performance, and can be used with multiple 5841's in an enterprise router
HIFN 8350 HIFN 4350 (tied for 3rd)	**4 Gbps**	Applications for High-end entrprise security services VPNs, Firewalls, Server security and secure storage
Cavium Nitrox & SafeXcel 1842 (tied for 4th)	**3.2 Gbps**	VPN Gateway, Router Gateways / Applications like Mid to high range VPN security devices
HIFN 8300 HIFN 4300 (tied for 5th)	**2 Gbps**	Applications for High-end entrprise security services VPNs, Firewalls, Server security and secure storage

TABLE XXXIV
Top 5 Highest Throughputs for IPsec-3DES

Crypto chip	Throughput IPSec-3DES	Application
Cavium Nitrox II	**10 Gbps**	VPN Gateway, IPSEC & SSL Server connections, Server Load balancing, and Server backup
HIFN 8350 HIFN 4350 (tied for 2nd)	**4 Gbps**	Applications for High-end entrprise security services VPNs, Firewalls, Server security and secure storage
Cavium Nitrox	**3.2 Gbps**	VPN Gateway, Router Gateways
Broadcom BCM5840	**2.4 Gbps**	High performance (wire speed) security applications. This would be connected to the NPU to create a secure solution for an enterprise router or layer 3 switch
HIFN 8154	**2.3 Gbps**	Applications for High-end entrprise security services in multi service appliances

Second to throughput, in importance, is the speed at which the cryptographic chip can processes Public Key (PK) operations. Public key operations are well known for requiring exceptional computing resources (especially as key sizes grow) therefore a chip that can rapidly process these operations is extremely beneficial. In PK cryptography, there are several operations that are processor-intensive. These include key generation, PK encryption & decryption, and signature generation & verification. Unfortunately very few vendors identify the performance of their products for each of these operations. In fact several vendors lump together the PK performance statistics and just list them by algorithm, like "RSA operations per second." When investigating the various products it appeared that the only common PK operation that's listed is Signatures Per Second. Therefore tables XXXV and XXXVI identify the five fastest chips for RSA and DSA signatures respectively.

TABLE XXXV
Top 5 most efficient RSA implementations

Crypto chip	Pub Key Algo's	RSA Sig per sec (1024-b)	Application
Cavium Nitrox I	RSA DH	**42000**	VPN Gateway, Router Gateways
Cavium Nitrox II	RSA DH	**40000**	VPN Gateway, IPSEC & SSL Server connections, Server Load balancing, and Server backup
Broadcom BCM5825	RSA DH	**12000**	High performance embedded VPN solutions
IBM Otello	RSA	**3300**	proprietary chip embedded in the PCIXXC board
SafeXcel 1842	RSA DSA DH	**1400**	Applications like Mid to high range VPN security devices

TABLE XXXVI
Top 5 most efficient DSA implementations

Crypto chip	Pub Key Algo's	DSA Sig per sec (1024-b)	Application
SafeXcel 1842	RSA DSA DH	1440	Applications like Mid to high range VPN security devices
SafeXcel 1841&1840 (tied for 2nd)	RSA DSA DH	1250	Applications like Mid to high range VPN security devices

Crypto chip	Pub Key Algo's	DSA Sig per sec (1024-b)	Application
HIFN 8350	RSA, DSA, DH	675	Applications for High-end entrprise security services VPNs, Firewalls, Server security
Broadcom 6500	RSA DSA DH	546	For VPN and secure electronic commerce devices
HIFN 4350	RSA, DSA, DH	540	For High-end (gigabit Ethernet) channels to secure storage and data repositories

In addition to RSA and DSA signatures, most vendors also implement the Diffie-Hellman key exchange algorithm and the five fastest products for this parameter are listed in table XXXVII.

TABLE XXXVII
Top 5 most efficient DH implementations

Crypto chip	Pub Key Algo's	D-H Key Gen/sec	Application
Cavium Nitrox I	RSA DH	72000	VPN Gateway, Router Gateways
Cavium Nitrox II	RSA DH	60000	VPN Gateway, IPSEC & SSL Server connections, Server Load balancing, and Server backup
Broadcom BCM5825	RSA DH	12000	High performance embedded VPN solutions
Cavium Nitrox Lite	RSA DH	1500	SOHO-VPN gateways and routers
SafeXcel 1842	RSA DSA DH	1425	Applications like Mid to high range VPN security devices

The parameters listed thus far provide a good comparison between the various vendors' and their respective products, however there are a few other considerations that a system designer should take into account. One important consideration is the number of algorithms supported by the chip. Table XXXVIII lists the products which implement the most algorithms. It is interesting to note that a majority of the chips surveyed implement multiple algorithms.

TABLE XXXVIII
The Manufacturers/chips that support the most Algorithms

Crypto chips	Models	Algorithms supported
SafeXcel	1840	DES, 3-DES, AES, ARC4, MD5, SHA-1, HMAC, DH, RSA, DSA
	1841	
	1842	
	1741	DES, 3-DES, AES (ECB, CBC, OFB, CFB), DH, RSA, DSA, SHA-1, MD5, HMAC
	1141	
	5150	IPSec, DES, 3-DES, (ECB, CBC), AES, (ECB, CBC, CTR, GCM), MD5-SHA-1, SHA-256, HMAC,
Broadcom	5812	3DES, AES, RSA, DSA, DH, SHA-1, MD5, HMCA-SHA-1, HMAC-MD5, ARCFOUR
	5823	
	5825	
HIFN	7954	DES, 3DES, ARC4, AES(128,192,256-bit), RSA, DSA, DH
	7955	
	7956	
	7814	
	7815	
	7851	
	7854	
	7855	
	8065	
	8054	
Cavium	Nitro x Lite	RSA, DH, DES, 3DES, AES (128, 192, 256), ARC4, modes=ECB, CBC, OFB, CFB, MD5, SHA-1, HMAC-MD5. HMAC-SHA-1
	Nitro x	RSA(up to 4096), DH (groups 1, 2, 5), DES, 3DES, AES (128, 192, 256), ARC4, MD5, SHA-1, HMAC-MD5. HMAC-SHA-1
	Nitro x II	RSA, DH, DES, 3DES, AES, ARC4, MD5, SHA-1, HMAC-MD5, HMAC-SHA-1

Another important attribute for cryptographic chips to have is a random number generator. There are two major types of random number generators (RNGs), pseudo-random (PRNGs) and true-random (TRNGs). Pseudo-random number generators are designed using algorithms that generate numbers or bit streams that appear to be random. In most cases the output from these RNGs are random enough to pass basic statistical testing, but given that this method employs a deterministic approach that is initialized with a seed, it is debatable whether this category can be considered genuinely random. True Random Number Generators (TRNGs), on the other hand, capitalize on naturally occurring random phenomena and generate nearly perfect statistical randomness without the need for seed initialization. For this reason, system designers should strongly consider the use of cryptographic chips that implement a TRNG. Additionally, the random number generator needs to be able to sustain throughput speeds that can support the overall chip design. As such the five crypto chips that employ the fastest number generators are listed in table XXXIX.

TABLE XXXIX
Top 5 fastest on-chip random number generators.

Crypto chips	RNG Speed	True RNG	Application
Cavium Nitrox II	320 Mbps	Y	VPN Gateway, IPSEC & SSL Server connections, Server Load balancing, and Server backup
Cavium Nitrox I	200 Mbps	Y	VPN Gateway, Router Gateways
Cavium Nitrox Lite	100 Mbps	**	SOHO-VPN gateways and routers
SafeXcel 1840 1841 1842	20 Mbps	Y	Applications like Mid to high range VPN security devices
SafeXcel 1741	1Mbps	Y	Applications like low to Mid range VPN security devices

** The datasheet did not specify

While there are strong arguments for the use of TRNGs it is interesting that NIST currently only endorses pseudo random number generators on their website.

Although not included as a comparison parameter, the system designer may also be interested in knowing which crypto chip manufacturers offer the most products. The benefit of this attribute may be a little less tangible than the other factors but it may be something that influences the decision to choose a particular vendor. One example might be a change in the system design that requires the designer to look for a smaller chip or different package type. In this case it would be convenient if the chosen manufacturer offered a similar chip but implemented with a different package. In table XXXX, it's clear to see that HIFN Inc dominates the market of cryptographic processors.

TABLE XXXX
Vendors with the most market offerings

Manufacturer	Models
HIFN	16
Broadcom	10
SafeNet	9

Lastly, table XXXXI, is provided in an effort to emphasize that cryptographic chips are available in several different package forms. This fact is important because it means that regardless of the type of product that is being designed, there is most likely a cryptographic chip that can be implemented.

TABLE XXXXI
Various Chip Packages & Pin Count

Package	Various Pin Sizes			
BGA	144	502	1096	
TBGA	256	480	576	
FPBGA	256			
LBGA	324			
PBGA	256	400	456	480
TSBGA	600			
TQFP	80	128	144	
LQFP	128			
MQFP	208			
DQFP	144			
FBGA	198			
TSSOP	28			
MLF	40			
HQFP	160			

In looking at the seven comparison categories, there are a few chips that frequently show up in the top five. These chips represent the "Best-of-Class" products which should be considered first when designing a system. These chips are ranked in table XXXXII.

TABLE XXXXII
Best Cryptographic chips

Rank	Cryptographic Chip
1st	Cavium Nitrox II
2nd	Cavium Nitrox 1
3rd	SafeXcel 1842
4th	HIFN 8350
5th	HIFN 4350

XV. Conclusion

The goal for this project was to conduct a market survey for both IP cores and cryptographic chips, determine common parameters among each and for an evaluation for the "Best of Class." As noted in section VIII the best cryptographic IP cores are from Helion technology for all algorithms and as identified in the tables above, the best cryptographic chip is the Cavium Nitrox II. The information obtained in this report can serve as a guide for system designers that need to implement either IP core logic or an actual cryptographic chip.

Lastly, it should be noted that the Linley Group has produced a 175-page document titled "A Guide to Security and Content Processors, Fourth Edition" which includes a comprehensive market survey of cryptographic chips and security devices. For the inquisitive (and well funded) reader, this document may be purchased for $2495.00 online

References

[1] http://www.silicon-designs.com/Intellectual_Prop.asp#
[2] http://www.m-sys.com/site/en-US/Products/SecurityIP/SecurityIP/Crypto_Cores.htm
[3] http://Whatis.techtarget.com
[4] http://www.ipcores.com/
[5] http://www.hdl-dh.com/products/products.htm
[6] http://www.conexant.com/products/entry.jsp?id=320
[7] http://www.heliontech.com/core.html
[8] http://www.cast-inc.com/cores/
[9] http://www.pittsburghsolutions.com/eresearch-news.htm
[10] Atmel Corp Data sheet for AT97SC3201 Trusted Platform Module
[11] Atmel Inc Data sheet for AT97SC3203 TPM
[12] Broadcom Corp data sheet for BCM5801 Cryptographic Processor
[13] Broadcom Corp data sheet for BCM5802 Security Processor
[14] Broadcom Corp data sheet for BCM5805 Security Processor
[15] Broadcom Corp data sheet for BCM5812 Security Processor
[16] Broadcom Corp data sheet for BCM5823 Security Processor
[17] Broadcom Corp data sheet for BCM5825 Hi performance Security Processor
[18] Broadcom Corp data sheet for BCM5840 Gigabit Security Processor
[19] Broadcom Corp data sheet for BCM5841 Multi-Gigabit Security Processor
[20] Harris Corp Data sheet for Citadel Cryptographic Engine
[21] Harris Corp Data sheet for Citadel II Cryptographic Engine
[22] HIFN Inc Data sheet for 4300 Storage Security Processor
[23] HIFN Inc Data sheet for 4350 Storage Security Processor
[24] HIFN Inc Data sheet for 6500 Public Key Processor
[25] HIFN Inc Data sheet for 7711 Security Processor
[26] HIFN Inc Data sheet for 7811 Security Processor
[27] HIFN Inc Data sheet for 7814 Network Security Processor
[28] HIFN Inc Data sheet for 7815 Security Processor
[29] HIFN Inc Data sheet for 7851 Security Processor
[30] HIFN Inc Data sheet for 7855 Network Security Processor
[31] HIFN Inc Data sheet for 7902 Network Security Processor
[32] HIFN Inc Data sheet for 7951 Network Security Processor
[33] HIFN Inc Data sheet for 7954 Security Processor
[34] HIFN Inc Data sheet for 7955 Security Processor
[35] HIFN Inc Data sheet for 7956 Security Processor

[36] HIFN Inc Data sheet for 8154 Security Processor
[37] HIFN Inc Data sheet for 8155 Security Processor
[38] HIFN Inc Data sheet for 8300 Security Processor
[39] HIFN Inc Data sheet for 8350 Security Processor
[40] HIFN Inc Product Comparison matrix
[41] Cavium Networks Product Brief for Nitrox Lite Security Processor
[42] Cavium Networks Product Brief for Nitrox Security Processor
[43] Cavium Networks Product Brief for Nitrox II Security Processor
[44] Philips Inc Data sheet for GCD-Φ 2000 General Crypto Device
[45] Mykotronix Inc, Data sheet for MYK-82A Cryptographic Processor
[46] SafeNet Inc Data sheet for SafeXcel 1141 security co-processor
[47] SafeNet Inc Data sheet for SafeXcel 1741 security co-processor
[48] SafeNet Inc Data sheet for SafeXcel 1840 security co-processor
[49] SafeNet Inc Data sheet for SafeXcel 1841 security co-processor
[50] SafeNet Inc Data sheet for SafeXcel 1842 security co-processor
[51] SafeNet Inc Data sheet for SafeXcel 2141 security-system-on-a-chip
[52] SafeNet Inc Data sheet for SafeXcel 5140 Enterprise Security Processor
[53] SafeNet Inc Data sheet for SafeXcel 5150 Enterprise Security Processor
[54] SafeNet Inc Data sheet for SafeXcel 5160 Enterprise Security Processor
[55] Sinosun Technology Ltd Data sheet for SSX35 Trusted Platform Module
[56] T. W. Arnold and L. P. Van Doorn, "The IBM PCIXCC: A new cryptographic coprocessor for the IBM eServer," IBM Journal of Research and Development, Vol. 48 No. 3/4 May/July 2004

P. Arora completed her Bachelor of Engineering in Electronics and Telecommunication Engineering at Rajiv Gandhi Institute of Technology, Mumbai University, in May 2005

M. Dugan received his bachelor of science in mechanical engineering at Penn State University, State College, PA in 1997. Since then he has been working as contractor for the US Navy on the hull and mechanical design of AEGIS destroyers in Washington DC.

P. Gogte received her Bachelor's degree in Electronics & Telecommunications in 2002, from Pune, India and she's currently working towards a Master's in EE with Communications & Networking as a major concentration area