Specifications for Citadel

General

- **Multiple Algorithms**
  Standard Harris proprietary high-grade algorithm
  Harris-configured customer unique algorithm
  Customer-configurable unique algorithm
- **Cryptographic Strengths**
  Configurable key lengths
  Proven secure against differential and linear cryptanalysis
  Third party verified
- **Multiple Cryptographic Modes**
  Block Cipher Feedback
  Self-Synchronizing Cipher Feedback
  Long Cycle or Minimum Error Propagation
  Codebook (Key processing only)
- **Cryptographic Keys**
  Traffic Encryption Key—
  Minimum 1.8 x 10^{19}
  Key Encryption Key—
  Minimum 1.8 x 10^{19}
- **Key Management**
  On-chip key storage for KEKs and TEKs
  Key Wrapping/Unwrapping
  Key Updating
  Deterministic Key Generation
  Non-deterministic Key Generation
- **Data Rate**
  Up to 5 Mbps
- **Package**
  80 pin TQFP
  16 mm x 16 mm (0.63 x 0.63inches)
- **Power**
  3.3 or 5 volt supply

Key Features

- Citadel encryption algorithm
- Half-duplex traffic
- Serial or Parallel Traffic Data interface available
- 5 Mbps data rate
- Processor-controlled or stand-alone operation
- Cryptographic modes: CFB, SELF SYNC and minimum error propagation
- Keys wrapped/covered with KEK for storage off chip
- Rewrap keys
- Generate keys
- Algorithm customization
- On chip state swapping
- Boundary scan
- Supply 3.0 V (min) to 5.5 V (max)
- Independent TRANSEC interface
- 80 pin TQFP

Additional Features

- Rapid State Swapping
- Message Authentication Code MAC) generation
- Provides for independent Transmission Security output
- Standard bus interface (control, data, status registers)
- Default and standalone modes
- Serial or parallel traffic modes
- Industrial temperature range: –40˚C to +85˚C

HARRIS

RF Communications Division | 1680 University Avenue | Rochester, NY USA 14610
www.harris.com 1-585-242-3667

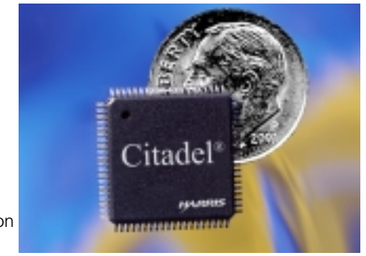
HARRIS

Communications Security Products

CITADEL®

CRYPTOGRAPHIC ENGINE

military-grade encryption for non-Type 1 applications



The Citadel® cryptographic engine provides high-grade protection for U.S. and international users and can be embedded into all modern communications media. It is approved for export with configurable key lengths and multiple algorithm options, making Citadel an ideal encryption solution for a broad range of communications products.

Citadel has three algorithm options: a standard Citadel high-grade algorithm, a Harris-configured customer unique Citadel algorithm, and a customer-configurable unique Citadel algorithm.

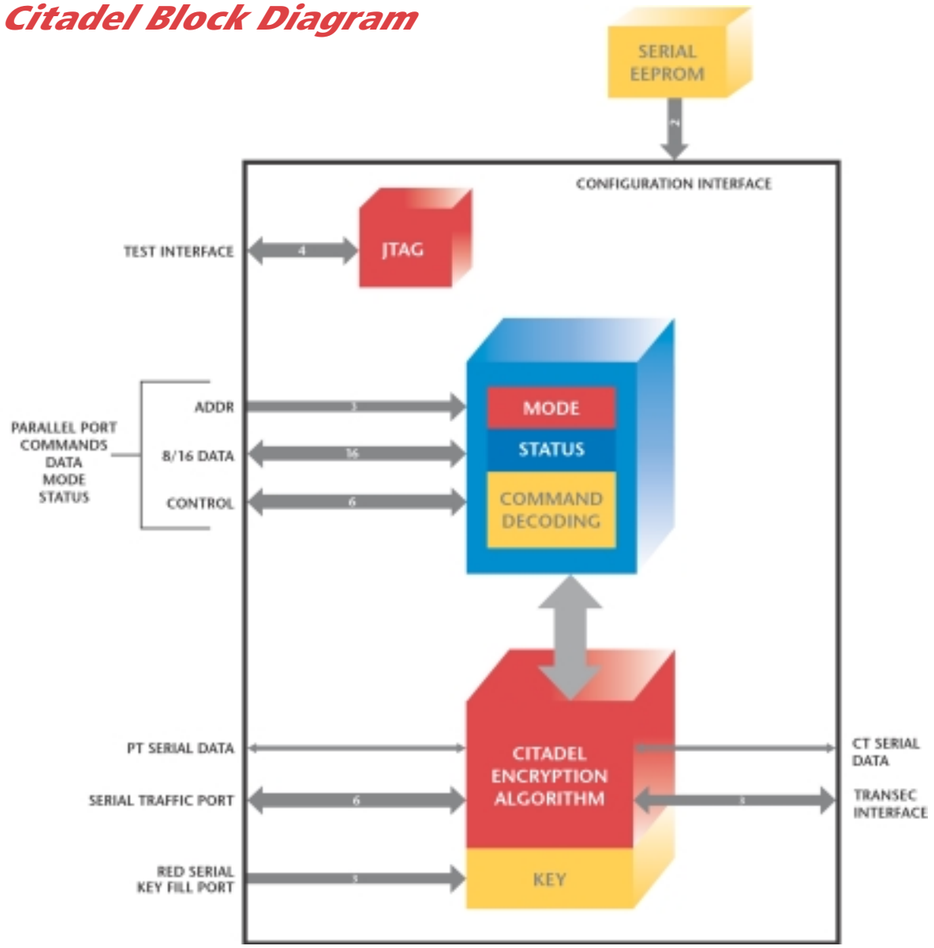
All Citadel cryptographic algorithms are based on a mixed-mode, arithmetic block cipher and support both communication security and transmission security functions. The algorithm has been analytically and field proven to withstand sophisticated cryptographic attacks.

Citadel provides half-duplex encryption and decryption at throughput data rates of up to 5 Mbps. It processes serial or parallel unencrypted [plain text-(PT)] data and serial or parallel encrypted [cipher text-(CT)] data. Key management commands are included in the IC's command set to provide flexibility to meet the user's requirements. All interfaces are 3.3V and 5V CMOS compatible.

The purpose of the IC is to encrypt and decrypt digital communications: data and digitized analog. Encrypting a signal containing sensitive information allows the resulting signal to be transmitted over normal communication channels without jeopardizing the security of the sensitive information. Decrypting the signal recovers the sensitive information in its original plain text form.

The ability to customize the algorithm provides the user with the ability to change the security without physically modifying the equipment.

Citadel Block Diagram



- The Parallel Port is a bi-directional interface used to control the chip's operation. Commands, status, bytes, and command data are passed via this port in 8- or 16-bit format. Encryption and de-cryption can be processed via the Parallel Port in either 8-bit or 16-bit format.
- The Power Port is compatible with 5V or 3.3V DC power.
- The Serial Traffic Port contains all the data and control lines necessary for encryption and decryption. PT and CT data are on different pins to provide red and black data separation.
- Keys are loaded via the Red Serial Key Fill Port.
- User-unique configuration information for the IC can be read from a serial EEROM by the Configuration Interface or loaded via the Parallel Port.
- The Housekeeping Port contains the **/RESET, /ZERO, STAND_ALONE, CONFIG/DE** signals.
- The Test Port contains the Test Access Port (TAP) interface for Boundary Scan.

	Designation	I/O	Name	Pin #'s (TQFP 80)
Serial Traffic Port	DECRYPT_REQ	I	Decryption request	43
	ENCRYPT_ REQ	I	Encryption Request	44
	TRAF_OUT_EN	O	Traffic Output Enable in serial mode	45
	OUT_BUF_FULL	O	Output Buffer full in parallel mode	49
	CT	Bidir	Cipher Text Traffic In or Out	21
	TRAF_CLK	I	Traffic Clock	51
	CRYPTO_RDY	O	Crypto Ready in serial mode	52
	TRAF_IN_EN	I Serial	Traffic Input Enable	53
	IN_BUF_EMP	O Parallel	Input buffer Empty in parallel mode	56
	PT	Bidir	Plain Text Traffic In or Out	80
TRANSEC Interface	TRANS_EN	I	TRANSEC Enable	59
	TRANS_KS_OUT	O	TRANSEC Key Stream Out	58
	TRANS_CLK	I	TRANSEC Clock	57
Red Serial Key Fill Port	R_KEY_IN	I	Red Key Data Input	63
	KEY_CLK	I	Key Clock	64
	R_KEY_EN	I	Enable for Red key Input Data	65
	STAND_ALONE	I	Stand-Alone mode	68
	CONFIG/DE	I	Configuration/Default	69
	/ZERO	I	Zeroize	41
Test Port	TCK	I	Test Clock	70
	TMS	I	Test Mode Select	71
	TDI	I	Test Data In	72
	TDO	O	Test Data Out	73
Configuration Interface	SCL	O	Serial Clock	76
	SDA	I/O	Serial Data	77
	ERR	O	Error	32
	VDD	I	Supply Voltage	6, 15, 20, 26, 35, 40, 46, 50, 55, 60, 66, 75, 78, 79
	GND	I	Ground	1, 7, 14, 22, 27, 34, 42, 47, 48, 54, 62, 67, 74
	CLK	I	Chip Clock	33
	/RESET	I	Reset	61
Parallel Port	/CS	I	Chip Select	8
	/WR	I	Write	9
	/RD	I	Read	10
	BUSY	O	Busy	11
	DR	O	Data Request	12
	DA	O	Data Available	13
	A2	I	Address for Parallel Port Registers	31
	A1	I	Addr	30
	A0	I	Addr	29
	D15	Bidir	Addr	39
	D14	Bidir	Data	38
	D13	Bidir	Data	37
	D12	Bidir	Data	36
	D11	Bidir	Data	28
	D10	Bidir	Data	25
	D9	Bidir	Data	24
	D8	Bidir	Data	23
	D7	Bidir	Data	19
	D6	Bidir	Data	18
	D5	Bidir	Data	17
	D4	Bidir	Data	16
	D3	Bidir	Data	5
	D2	Bidir	Data	4
	D1	Bidir	Data	3
	D0	Bidir	Data	2