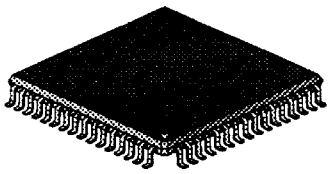
SGS-THOMSON MICROELECTRONICS

ST16xF74

CMOS CRYPTO-COMPUTER FAMILY

ADVANCE DATA

- 8 BIT ARCHITECTURE CPU
- 20K BYTES of ROM
- 608 BYTES oF RAM
- 4K BYTES of EEPROM SECTORS COMBINATIVE:
  - Highly reliable CMOS EEPROM Technology
  - 10 Years Data Retention
  - 100K Erase/Write Cycles Endurance
  - Protected one time programmable block (32 or 64 bytes)
  - Separate Write and Erase cycle for fast "1" programming
  - 1 to 32 bytes block Erase or Write single cycle programming
- SINGLE 5V ± 10% SUPPLY VOLTAGE
- SOPHISTICATED HIGH SECURITY FEATURES
- PROGRAMMABLE 8 BIT PARALLEL HOST BUS INTERFACE
- FIVE I/0 PORTS
  - Two 8 bit ports
  - One 4 bit port
  - Two serial ports
- MODULAR ARITHMETIC PROCESSOR
  - Fast modulo N addition, subtraction, multiplication, exponentiation and calculation of MONTGOMERY constants
  - Software selectable operand length (256/512 bit)
  - Double operand operation (1024 bit)
- REAL RANDOM NUMBER GENERATOR (can generate secret keys on board)
- OPTIONAL DES ACCELERATOR



PQFP64

- 64 PIN PQFP PACKAGE
- 512 BIT RSA SIGNATURES with 5MHz EXTERNAL CLOCK in 17ms

DESCRIPTION

The ST16xF74 is a family of safeguarded 8 bit MCU, especially designed for large volume and cost competitive smartcard terminals applications where high performance Public Key Algorithm are implemented, and Secret Keys are generated on board.

Its internal Modular Arithmetic Processor is designed to speed up cryptographic calculation using Public Key Algorithms. It can process modular addition, subtraction and exponentiation on 256/512 bit operands or 1024 bit double operand.

The optional DES Accelerator speeds up the necessary permutation specified by the NIST DEA standards.

The ST16xF74 is based on the SGS-THOMSON ST16XYZ family of 8 bit MCU.

Product Variance

ST16KF74	All features
ST16LF74	All features except DES accelerator
ST16MF74	All features except parallel I/O ports
ST16NF74	All features except DES accelerator and parallel I/O ports

DESCRIPTION (cont'd)

On-chip memories include: 608 bytes of RAM, 16K bytes of ROM and 4K bytes of EEPROM. The EEPROM can be configured into any of the following sector conbinations:

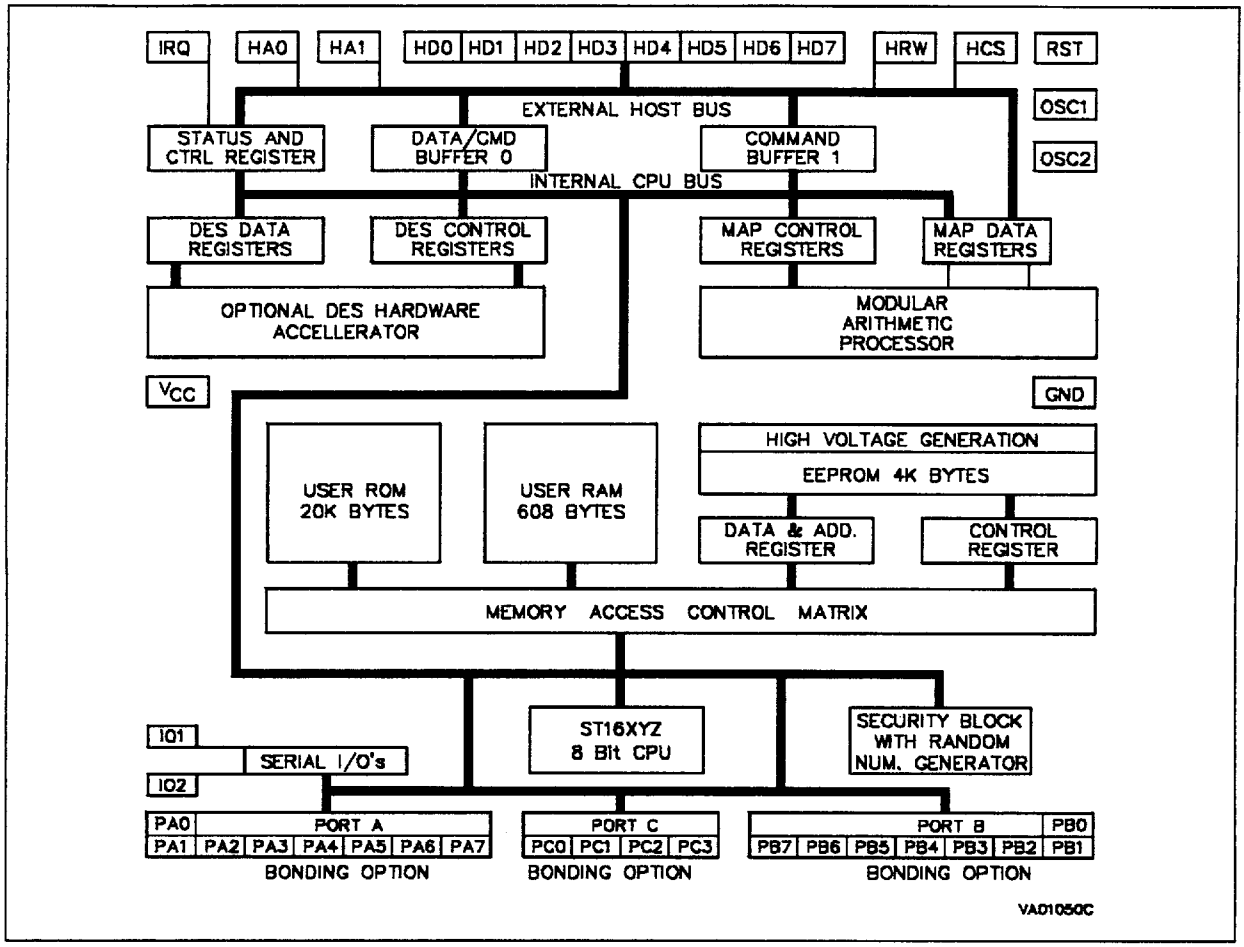
Sector A	Sector B
0	4096
512	3584
1024	3072
2048	2048

It is manufactured using the high reliable SGS-THOMSON 1µm CMOS EEPROM technology.

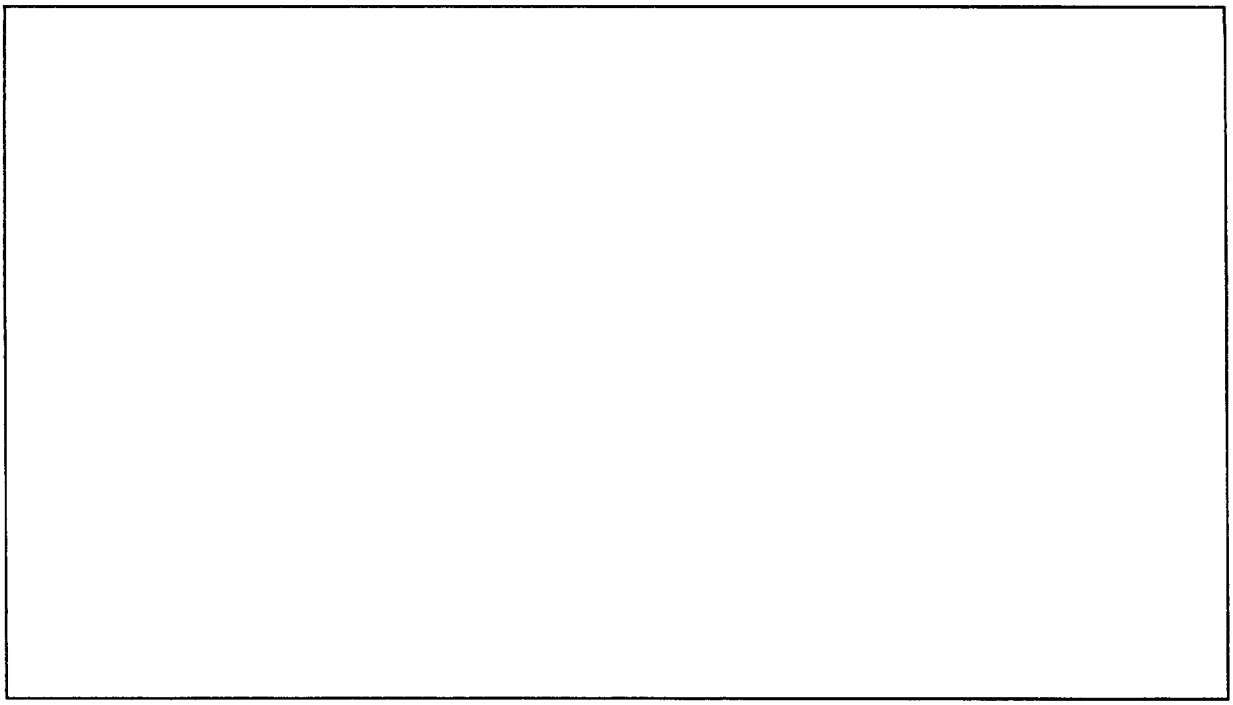
Software development and firmware (ROM code/options) generation can be done with the SGS-THOMSON ST16XYZ-EMU development system.

The ST16xF74 can be delivered in 64 pin PQFP.

Figure 1. Block Diagram



PQFP64 - 64 lead Plastic Quad Flatpack, 14 x 14mm



Drawing is out of scale