ST19 FAMILY

Smartcard MCU Family of Products

DATA BRIEFING

- 8 BIT ARCHITECTURE CPU
- FROM 32 KBytes OF USER ROM, WITH PARTITIONING
- SYSTEM ROM FOR LIBRARIES
- UP TO 2 KBytes OF RAM WITH PARTITIONING
- UP TO 64 KBytes OF EEPROM WITH PARTITIONING
  - Highly reliable submicron CMOS EEPROM technology
  - 10 year data retention
  - 100 000 Erase/Write cycle endurance
  - Separate Program and Erase cycles for fast “1” programming
  - 1 to 64 Bytes Erase or Program in 1 ms
- MODULAR ARITHMETIC PROCESSOR
  - Fast modular multiplication and squaring using Montgomery method
  - Software Crypto Libraries in separate ROM area for efficient algorithm coding using a set of advanced functions
  - Software selectable operand length (up to 2176 bits)
- SECURITY FIREWALLS FOR MAP AND MEMORIES
- VERY HIGH SECURITY FEATURES INCLUDING EEPROM FLASH PROGRAM AND RAM FLASH CLEAR
- POSSIBLE ADDITION OF CUSTOM LOGIC BLOCKS
- 8 BIT TIMER
- SERIAL ACCESS, ISO 7816-3 COMPATIBLE
- 3V ± 10% OR 5V ± 10% SUPPLY VOLTAGE
- STANDBY MODE FOR POWER SAVING
- UP TO 10 MHz INTERNAL OPERATING FREQUENCY
- CONTACT ASSIGNMENT COMPATIBLE ISO 7816-2
- ESD PROTECTION GREATER THAN 5000V
- 2 OPERATING CONFIGURATIONS
  - ISSUER
  - USER

Table 1 Features by Product

Feature	ST19SF64	ST19SF32	ST19SF16	ST19SF08	ST16KF16	ST19CF68
USER ROM	32K	32K	32K	32K	32K	23K
RAM	960	960	960	960	1984	960
EEPROM	64K	32K	16K	8K	16K	8K
MAP and Firmware	No	No	No	No	1088 bits	512 bits

DESCRIPTION

HARDWARE DESCRIPTION

All the products of the ST19 FAMILY are based on a STMicroelectronics 8 bit CPU core including on-chip memories: up to 2 KBytes of RAM, from 32 KBytes of USER ROM and up to 64 KBytes of EEPROM.

RAM, ROM and EEPROM memories can be configured into partitions. Access rules from any memory partition to any other partition are setup by the user defined Memory Access Control Logic.

They are manufactured using the highly reliable ST submicron CMOS EEPROM technology and are fully compatible with the ISO standards for Smartcard applications.

FAST CRYPTOGRAPHIC FUNCTIONS PROCESSING (5V ± 10%, 5MHz)

Function	MAP 512	MAP 1088
RSA 512 bits signature with CRT *	70 ms	20 ms
RSA 512 bits signature without CRT	200 ms	60 ms
RSA 512 bits verification (e=$10001)	6 ms	3 ms
RSA 1024 bits signature with CRT	400 ms	110 ms
RSA 1024 bits signature without CRT	N/A	380 ms
RSA 1024 bits verification (e=$10001)	150 ms	8 ms
RSA 2048 bits signature with CRT	N/A	800 ms
RSA 2048 bits verification	N/A	100 ms
EC 160 bits signature	N/A	250 ms
EC 160 bits verification	N/A	500 ms

Note * CRT: Chinese Remainder Theorem

MODULAR ARITHMETIC PROCESSOR

The internal Modular Arithmetic Processor is designed to speed up cryptographic calculations using Public Key Algorithms. Based on a 512 bit or 1088 architecture, it processes modular multiplication and squaring up to 2176 bit operands.

SOFTWARE SUPPORT

SOFTWARE DEVELOPMENT

Software development and firmware (ROM code/ options) generation are completed by the ST16-19HDS development system.

CRYPTO LIBRARIES

For an easy and efficient use of the Modular Arithmetic Processor (MAP), ST proposes a complete set of firmware subroutines. This library is located in a specific ROM area, leaving 32 KBytes minimum in the User ROM for the application software. This library saves the operating system designer from coding first layer functions and allows the designer to concentrate on algorithms and Public Key Cryptographic (PKC) protocol implementation.

This library contains firmware functions for:

– loading and unloading parameters and results to or from the MAP
– calculating Montgomery constants
– basic mathematics including modular squaring and multiplication for various lengths
– modular exponentiation or not using the Chinese Remainder Theorem (CRT),
– more elaborate functions such as RSA signatures and authentications for any modulo length up to 1024/2048 bits long or DSA signature and verification, elliptic curves.
– full internal key generation for signatures/authentications. This guarantees that the secret key will never be known outside the chip and contributes to overall system security.
– long random number generation
– sha-1

Figure 1 Block Diagram