Features

- One of a Family of Devices with User Memory of 1 Kbit to 64 Kbits
- Contactless 13.56 MHz RF Communications Interface
  - ISO/IEC 14443-2:2001 Type B Compliant
  - ISO/IEC 14443-3:2001 Type B Compliant Anticollision Protocol
  - Command Set Optimized for Multicard RF Communications
  - Tolerant of Type A Signaling for Multiprotocol Applications
  - Operating Distance Up to 10 cm
- Integrated 82 pF Tuning Capacitor
- User EEPROM Memory
  - 2 Kbits Configured as Four 64-byte (512-bit) User Zones
  - Byte, Page, and Partial Page Write Modes
  - Self-timed Write Cycle
- 256-byte (2-Kbit) Configuration Zone
  - User-programmable Application Family Identifier (AFI)
  - User-defined Anticollision Polling Response
  - User-defined Keys and Passwords
- High-Security Features
  - 64-bit Mutual Authentication Protocol (under exclusive patent license from ELVA)
  - Encrypted Checksum
  - Stream Encryption
  - Four Key Sets for Authentication and Encryption
  - Eight Sets of Two 24-bit Passwords
  - Password and Authentication Attempts Counters
  - Selectable Access Rights by Zone
  - Write Lock Mode
  - Antitearing Function
  - Tamper Sensors
- High Reliability
  - Endurance: 100,000 Write Cycles
  - Data Retention: 10 Years
  - Operating Temperature: –40°C to +85°C

CryptoRF™ EEPROM Memory 2 Kbits

AT88SC0204CRF

Summary

Rev. 5022AS–CRRF–05/03

Note: This is a summary document. A complete document is available under NDA. For more information, please contact your local Atmel sales office.

Description

The CryptoRF™ family integrates a 13.56 Mhz RF interface into a CryptoMemory®, resulting in a contactless smart card with advanced security and cryptographic features. This device is optimized as a contactless secure memory, for multiapplication RF smart card markets, and secure identification for electronic data transfer, without the requirement of an internal microprocessor.

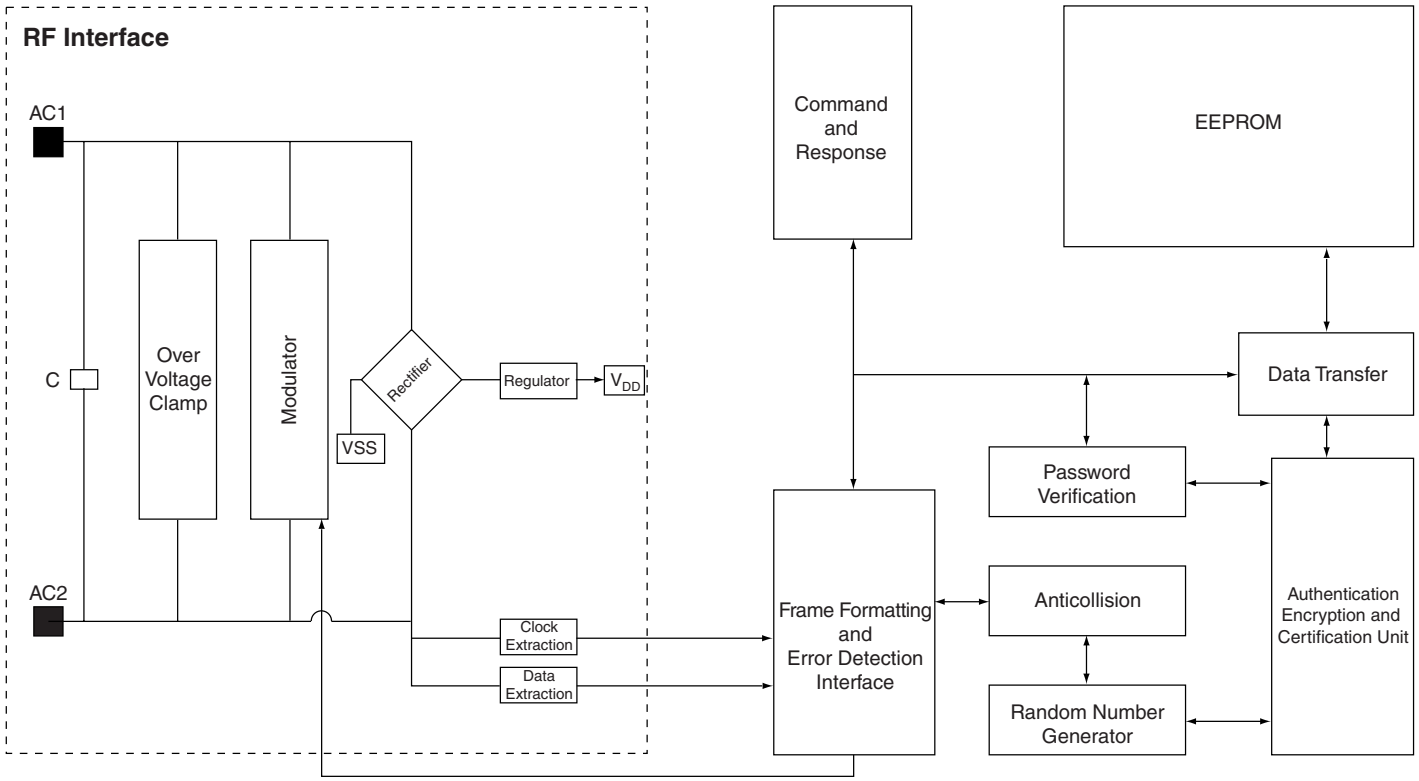
For communications, the RF interface utilizes the ISO 14443-2 and -3 Type B bit timing and signal modulation schemes, and the ISO 14443-3 Slot-MARKER Anticollision Protocol. Data is exchanged half duplex at a 106-kbit/s rate, with a two-byte CRC_B providing error detection capability. The maximum communication range between the reader antenna and contactless card is approximately 10 cm when used with an RFID reader that transmits the maximum ISO 14443-2 RF power level. The RF interface powers the other circuits; no battery is required. Full compliance with the ISO 14443-2 and -3 standards results in anticollision interoperability with the AT88RF020 2-Kbit RFID EEPROM product and provides both a proven RF communication interface and a robust anticollision protocol.

The AT88SC0204CRF contains 2 Kbits of user memory and 2 Kbits of system memory. The 2 Kbits of system zone memory contain eight sets of read/write passwords, four crypto key sets, security access registers for each user zone, and password/key registers for each zone. The features and functionality of the system zone are identical to those in the standard CryptoMemory.

The CryptoRF command set is optimized for a multicard RF communications environment and includes all of the functionality of the standard CryptoMemory commands. A programmable AFI register allows this IC to be used in numerous applications in the same geographic area with seamless discrimination of cards assigned to a particular application during the anticollision process.

Block Diagram

Figure 1. Block Diagram



Communications

All personalization and communication with this device is performed through the RF interface. The IC includes an integrated tuning capacitor, enabling it to operate with only the addition of a single external coil antenna.

The RF communications interface is fully compliant with the electrical signaling and RF power specifications in ISO/IEC 14443-2:2001 for Type B only. Anticollision operation and frame formatting are compliant with ISO/IEC 14443-3:2001 for Type B only.

ISO/IEC 14443 nomenclature is used in this specification where applicable. The following abbreviations are utilized throughout this document. Additional terms are defined in the section in which they are used.

- PCD – Proximity Coupling Device: the reader/writer and antenna.
- PICC – Proximity Integrated Circuit Card: the tag/card containing the IC and antenna.
- ETU – Elementary Time Unit: the time required to transmit or receive one data bit. One ETU is equal to 128 carrier cycles (9.439 microseconds).
- RFU – Reserved for Future Use: any feature, memory location, or bit that is held as reserved for future use
- $ xx – Hexadecimal Number: denotes a hex number “xx” (Most Significant Bit on left)
- xxxx b – Binary Number: denotes a binary number “xxxx” (Most Significant Bit on left)

Anticollision Protocol

When the PICC enters the 13.56 Mhz RF field of the host reader (PCD), it performs a power on reset (POR) function and waits silently for a valid Type B polling command. The CryptoRF PICC processes the antitearing registers as part of the POR process.

The PCD initiates the anticollision process by issuing an REQB or WUPB command. The WUPB command activates any card (PICC) in the field with a matching AFI code. The REQB command performs the same function but does not affect a PICC in the halt state. The REQB and WUPB commands contain an integer N indicating the number of slots assigned to the anticollision process. The CryptoRF command set is available only after the anticollision process has been completed.

CRC Error Detection

A two-byte CRC_B is required in each frame transmitted by the PICC or PCD to permit transmission error detection. The CRC_B is calculated on all of the command and data bytes in the frame. For encrypted data, the encryption is performed prior to CRC_B calculation. The SOF, EOF, start bits, stop bits, and EGT are not included in the CRC_B calculation. The two-byte CRC_B follows the data bytes in the frame.

Figure 2. Location of the Two CRC_B Bytes within a Frame

The CRC polynomial is defined in ISO/IEC 14443 and ISO/IEC 13239 as $x^{16} + x^{12} + x^5 + x^0$. This is a hex polynomial of $1021. The initial value of the register used for the CRC_B calculation is all ones ($FFFF). When receiving information from the reader, the PICC computes the CRC on the incoming command, data, and CRC bytes. After the last bit has been processed, the CRC register should contain $0000.

Type A Tolerance

The RF Interface is designed for use in multiprotocol applications. It will not latch or lock up if exposed to Type A signals and will not respond to them. The PICC may reset in the presence of Type A field modulation but is not damaged by exposure to Type A signals.

User Memory

The EEPROM user memory is divided into four user zones as shown in the memory map in Table 1. Multiple zones allow for different types of data or files to be stored in different zones. Access to the user zones is allowed only after security requirements have been met. These security requirements are defined by the user in the configuration zone during personalization of the device. If the same security requirements are selected for multiple zones, then these zones may be effectively accessed as one larger zone. The EEPROM memory page length is 16 bytes.

Table 1. Memory Map

Zone	$0	$1	$2	$3	$4	$5	$6	$7	
User 0									$00
	64 Bytes								–
									–
									$38
User 1									$00
	64 Bytes								–
									–
									$38
User 2									$00
	64 Bytes								–
									–
									$38
User 3									$00
	64 Bytes								–
									–
									$38

Configuration Memory

The configuration zone consists of 2048 bits of EEPROM memory used for storing system data, passwords, keys, codes, and security-level definitions for each user zone. Access rights to the configuration zone are defined in the control logic and may not be altered by the user. These access rights include the ability to program certain portions of the configuration zone and then lock the data written through use of the security fuses.

Security Fuses

There are three fuses on the device that must be blown during the device personalization process. Each fuse locks certain portions of the configuration zone as OTP memory. Fuses are designed for the module manufacturer, card manufacturer and card issuer and should be blown in sequence, although all programming of the device and blowing of the fuses may be performed at one final step.

Communication Security Modes

Communication between the PICC and reader operates in three basic modes. Standard mode is the default mode for the device after power-up and anticollision. Authentication mode is activated by a successful authentication sequence. Encryption mode is activated by a successful encryption activation, following a successful authentication.

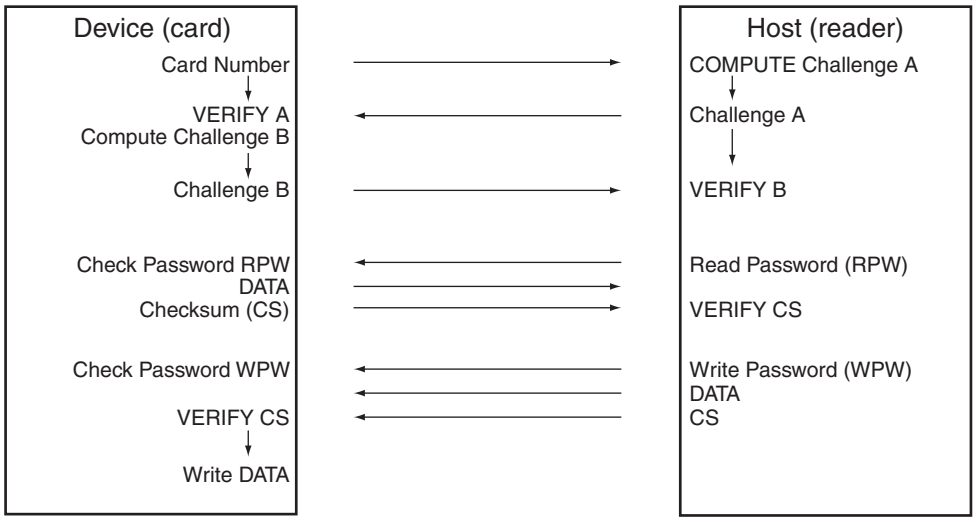
Table 2. Configuration Security Modes

Mode	Configuration Data[1]	User Data	Passwords	Data Integrity Check
Standard	clear	clear	clear	MDC[2]
Authentication	clear	clear	encrypted	MAC[3]
Encryption	clear	encrypted	encrypted	MAC[3]

Notes: 1. Configuration data includes the entire configuration zone except the passwords.
2. Modification Detection Code
3. Message Authentication Code

Security Methodology

Figure 3. Security Methodology



Memory Access

Depending on the device configuration, the host will carry out the authentication protocol and/or present different passwords for each operation: read or write. A bidirectional secure checksum may be used to certify data authenticity. Each user zone may be configured for free access for read and write or for password restricted access. To insure security between the different user zones (multiapplication card), each zone can use a different set of passwords. A specific attempts counter for each password and for the authentication provides protection against systematic attacks.

Security Operations

Antitearing

In the event of a power loss during a write cycle, the integrity of the device's stored data may be recovered. This function is optional: the host may choose to activate the antitearing function depending on application requirements. When antitearing is active, write commands take longer to execute since more write cycles are required to complete them. Data writes are limited to 8-byte pages when antitearing is active.

Data is written first to a buffer zone in EEPROM instead of to the intended destination address, but with the same access conditions. The data is then written to the required location. If this second write cycle is interrupted due to a power loss, the device will automatically recover the data from the system buffer zone at the next power-up.

Write Lock

If a user zone is configured in the write lock mode, then the user zone is effectively divided into 8-byte pages. The lowest address byte of each 8-byte page constitutes a write access control byte for the 8 bytes in that page.

Table 3. Example of the Write Lock Byte at $80 Controlling the Bytes from $80 to $87

$0	$1	$2	$3	$4	$5	$6	$7	Page
1101 1001 b	xxxx xxxx b locked	xxxx xxxx b locked	xxxx xxxx b	xxxx xxxx b	xxxx xxxx b locked	xxxx xxxx b	xxxx xxxx b	$80

The write lock byte may also be locked by writing its least significant (rightmost) bit to 0b. Moreover, the write lock byte can only be programmed, i.e., bits written to 0b cannot return to 1b.

In the write lock configuration, only one byte can be written at a time. If several bytes are received by the PICC, the command will be NACKed.

Password Verification

Passwords may be used to protect user zones' read and/or write access. When a password is presented using the Check Password command, it is memorized and active until power is removed unless a new password is presented or a valid DESELECT or IDLE command is received. Only one password is active at a time, but write passwords also give read access.

Authentication Protocol

The access to a user zone may be protected by an authentication protocol in addition to password dependent rights.

The authentication success is memorized and active as long as the chip is powered, unless a new authentication is initialized or a valid DESELECT or IDLE command is received. If the new authentication request is not validated, the card loses its previous authentication and it must be presented again. Only the last request is memorized.

Note: Authentication must be performed prior to the password check to insure password security. If the trial's limit has been reached (after four consecutive incorrect attempts), the password verification or authentication process will fail.

Encryption

The data exchanged between the card and the reader during Read, Write, and Check Password commands may be encrypted to ensure data confidentiality.

The issuer may choose to protect the access to a user zone with an encryption key by settings made in the configuration zone. In that case, activation of the encryption mode is required in order to read/write data in the zone.

The encryption activation success is memorized and active as long as the chip is powered, unless a new initialization is initiated or a valid DESELECT or IDLE command is received. If the new encryption activation request is not validated, the card will no longer encrypt data during read operations nor will it decrypt data received during write or verify operations.

Checksum

The PICC implements a data validity check function in the form of a checksum. The checksum may function in standard or cryptographic mode.

In the standard mode, the checksum is optional and may be used for transmission error detection; however, communication error detection capability is already provided by the mandatory CRC and this capability is redundant. In standard mode, the host may read a checksum from the device to verify that the data sent was correctly written.

The cryptographic mode is more powerful since it provides data origin authentication capability in the form of a Message Authentication Code (MAC); only the host/device that carried out a valid authentication is capable of computing a valid MAC. The cryptographic mode is automatically activated when a successful authentication is carried out. To write data to the device, the host is required to compute a valid MAC and provide it to the device.

If after an ingoing command the device computes a MAC different from the MAC transmitted by the host, not only is the command abandoned but the cryptographic mode is also reset. A new authentication is required to reactivate the cryptographic mode.

Supervisor Mode

Enabling this feature allows the holder of one specific password to gain full access to all eight password sets, including the ability to change passwords.

Modify Forbidden

No write access is allowed in a user zone protected with this feature at any time. The user zone must be written during device personalization prior to blowing the security fuses.

Program Only

For a user zone protected by this feature, data within the zone may be changed from a “1” to a “0”, but never from a “0” to a “1”.

Tuning Capacitance

The capacitance between the coil pins AC1 and AC2 is 82 pF nominal and may vary over ±10% over temperature and process variation.

Reliability

Table 4. Reliability

Parameter	Min	Typ	Max	Units
Write endurance	100,000	–	–	Write Cycles
Data retention	10	–	–	Years

Mechanical

Engineering Samples

Engineering samples are available in Atmel’s RF modules or ISO7810 ID-1 plastic cards.

Atmel Corporation

2325 Orchard Parkway
San Jose, CA 95131
Tel: 1(408) 441-0311
Fax: 1(408) 487-2600

Regional Headquarters

Europe
Atmel Sarl
Route des Arsenaux 41
Case Postale 80
CH-1705 Fribourg
Switzerland
Tel: (41) 26-426-5555
Fax: (41) 26-426-5500

Asia
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimshatsui
East Kowloon
Hong Kong
Tel: (852) 2721-9778
Fax: (852) 2722-1369

Japan
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
Tel: (81) 3-3523-3551
Fax: (81) 3-3523-7581

Atmel Operations

Memory
2325 Orchard Parkway
San Jose, CA 95131
Tel: 1(408) 441-0311
Fax: 1(408) 436-4314

Microcontrollers
2325 Orchard Parkway
San Jose, CA 95131
Tel: 1(408) 441-0311
Fax: 1(408) 436-4314

La Chantrerie
BP 70602
44306 Nantes Cedex 3, France
Tel: (33) 2-40-18-18-18
Fax: (33) 2-40-18-19-60

ASIC/ASSP/Smart Cards
Zone Industrielle
13106 Rousset Cedex, France
Tel: (33) 4-42-53-60-00
Fax: (33) 4-42-53-60-01

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
Tel: 1(719) 576-3300
Fax: 1(719) 540-1759

Scottish Enterprise Technology Park
Maxwell Building
East Kilbride G75 0QR, Scotland
Tel: (44) 1355-803-000
Fax: (44) 1355-242-743

RF/Automotive
Theresienstrasse 2
Postfach 3535
74025 Heilbronn, Germany
Tel: (49) 71-31-67-0
Fax: (49) 71-31-67-2340

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
Tel: 1(719) 576-3300
Fax: 1(719) 540-1759

Biometrics/Imaging/Hi-Rel MPU/
High Speed Converters/RF Datacom
Avenue de Rochepleine
BP 123
38521 Saint-Egreve Cedex, France
Tel: (33) 4-76-58-30-00
Fax: (33) 4-76-58-34-80

e-mail
literature@atmel.com

Web Site
http://www.atmel.com

5022AS–CRRF–05/03 xM