SPC5-CRYP-LIB

SPC5 Software Cryptography Library

Features

The SPC5 Software Cryptography Library supports the following algorithms:

- **AES-128, AES-192, AES-256 bits.** Supported modes are:
  - ECB (Electronic Codebook Mode)
  - CBC (Cipher-Block Chaining) with support for ciphertext stealing
  - CTR (CounTer Mode)
  - CCM (Counter with CBC-MAC)
  - GCM (Galois Counter Mode)
  - CMAC
  - KEY WRAP
- **ARC4**
- **DES, TripleDES.** Supported modes are:
  - ECB (Electronic Codebook Mode)
  - CBC (Cipher-Block Chaining)
- **HASH functions with HMAC support**:
  - MD5
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512
- **Random engine based on DRBG-AES-128**
- **SHA-512**
- Random engine based on DRBG-AES-128
- **RSA signature functions with PKCS#1v1.5**
- **ECC (Elliptic Curve Cryptography):**
  - Key generation
  - Scalar multiplication (the base for ECDH)
  - ECDSA

Description


The software library can run on the whole SPC5 microcontroller family.

On SPC564B/EC MCU’s, AES-128 ECB/CBC Encryption/Decryption, CMAC Message Authentication, Keys access lock/unlock, secure Key loading/update and Random Number Generation are implemented by an hardware dedicated peripheral (CSE accelerator) to guarantee minimum CPU load and maximum security level (a complete set of software drivers are available as part of SPC5Studio suite www.st.com/spc5studio).

For the other members of SPC5 family implementation is fully based on software routines.

### Table 1. Order code

<table>
<thead>
<tr>
<th>Order code</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPC5-CRYP-LIB</td>
<td>SPC5 Software Cryptography Library</td>
</tr>
</tbody>
</table>
Contents

1 Supported algorithms ......................................................... 3
  1.1 DES and Triple-DES algorithms ........................................ 3
  1.2 AES algorithm ............................................................. 3
  1.3 ARC4 algorithm ............................................................ 3
  1.4 RNG algorithm ............................................................. 4
  1.5 HASH algorithm ............................................................ 4
  1.6 RSA algorithm ............................................................. 4
  1.7 ECC algorithm ............................................................. 4

2 Revision history ................................................................. 6
1 Supported algorithms

1.1 DES and Triple-DES algorithms

The data encryption standard (DES) is a symmetric cipher algorithm that can process datablocks of 64 bits under the control of a 64-bit key. The DES core algorithm uses 56 bits for enciphering and deciphering, and 8 bits for parity, so the DES cipher key size is 56 bits.

The DES cipher key size has become insufficient to guarantee algorithm security, thus the Triple-DES (TDES) has been devised to expand the key from 56 bits to 168 bits (56 ÷ 3) while keeping the same algorithm core.

The Triple-DES is a suite of three DES in series, making three DES encryptions with three different keys.

The SPC5 Software Cryptography Library includes the functions required to support DES and Triple-DES modules to perform encryption and decryption using the following modes:

- ECB (Electronic Codebook Mode)
- CBC (Cipher-Block Chaining)

1.2 AES algorithm

The advanced encryption standard (AES), is a symmetric cipher algorithm that can process data blocks of 128 bits, using a key with a length of 128, 192 or 256 bits.

The SPC56 cryptographic library includes AES 128-bit, 192-bit and 256-bit modules to perform encryption and decryption in the following modes:

- ECB (Electronic Codebook mode)
- CBC (Cipher-Block Chaining) with support for Ciphertext Stealing
- CTR (Counter mode)
- CCM (Counter with CBC-MAC)
- GCM (Galois Counter mode)
- CMAC
- KEY WRAP

1.3 ARC4 algorithm

The ARC4 (also known as RC4) encryption algorithm was designed by Ronald Rivest of RSA. It is used identically for encryption and decryption as the data stream is simply XORed with the generated key sequence. The algorithm is serial as it requires successive exchanges of state entries based on the key sequence.

The SPC5 Software Cryptography Library includes functions required to support ARC4, a module to perform encryption and decryption.
1.4 **RNG algorithm**

The security of cryptographic algorithms relies on the impossibility of guessing the key. The key has to be a random number, otherwise the attacker can guess it.

Random number generation (RNG) is used to generate an unpredictable series of numbers. The random engine is implemented in software using a CTR_ DRBG based on AES-128, while a True RNG is done entirely by the hardware peripheral.

The SPC5 Software Cryptography Library includes functions required to support the RNG module to generate a random number.

1.5 **HASH algorithm**

This algorithm provides a way to guarantee the integrity of information, verify digital signatures and message authentication codes. It is based on a one-way hash function that processes a message to produce a small length / condensed message called a message digest.

The SSPC5 Software Cryptography Library includes functions required to support HASH/HMAC modules to guarantee the integrity of information using the following modes:

- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

1.6 **RSA algorithm**

RSA algorithm is a public key cryptographic algorithm designed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA labs specified some public key cryptographic standards leveraging it.

The SPC5 Software Cryptography Library includes functions required to generate and verify digital signatures and encryption / decryption using PKCS#1v1.5 standard, as well as RSA low level computation functions:

- RSA_PKCS1v15_Sign
- RSA_PKCS1v15_Verify
- RSA_PKCS1v15_Encrypt
- RSA_PKCS1v15_Decrypt
- RSASP1
- RSAVP1

1.7 **ECC algorithm**

SPC5 Software Cryptography Library supports ECC Elliptic Curve Cryptography (ECC) operations for elliptic curves defined over prime fields.
Supported functionalities includes ECC key pair generation, ECDSA (Elliptic Curve Digital Signature Algorithm), which can be used to generate and verify digital signatures, and Scalar Multiplication which is the Elliptic Curve operation required by ECDH (Elliptic Curve Diffie-Hellman protocol) that can be used to securely establish a shared key between two peers.
2  Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>27-May-2014</td>
<td>1</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>