

TMPR4926 Triple Data Encryption Standard (3DES) Application

Highlights

- Toshiba's new 64-Bit MIPS-based RISC microprocessor (MPU) brings a high level of security to data transmissions in all high-performance packet-processing applications.
- The device supports the triple data encryption standard (3DES) algorithm, the most widely used encryption standard, and achieves highly secure data transfers in various networking and communications applications.

Description

The new TMPR4926XB-200 microprocessor is based on the TX49/H2 core, which operates at 200 MHz. Its design integrates Toshiba's TMPR4925XB-200 CPU with a dedicated DES and 3DES algorithm in a single chip allowing use of the TMPR4925XB-200's software and development environment. The MPU supports a wide range of applications with built-in controllers for peripheral component interconnect (PCI), direct memory access (DMA), and NAND flash memory.

Toshiba's TMPR4926XB-200 processor provides a complete system solution for networking and communications equipment. A high-performance 64-Bit MIPS RISC core has been coupled with carefully selected peripherals to meet these system requirements. The high-performance DES/3DES engine provides hardware encryption and decryption without loading the central processing unit with software emulation overhead. This is a key system performance advantage.

As broadband Internet connections become prevalent, more and more companies are promoting private data networks as a vehicle for electronic business. Virtual Private Networks (VPNs) use the public telecommunications infrastructure but maintain privacy by using a tunneling protocol and security procedures. This approach necessitates high-level encryption, a requirement that Toshiba's new processor meets.

Secure data transmission first encrypts data to be transmitted, turning it into unintelligible code, and on receipt decrypts it into its original form. In such a system, security depends on the key used to encode and decode the data. Although the encryption algorithm specified in the 3DES algorithm is common, a unique key for each transaction protects the security of data. Encrypted data can be deciphered only by using a key identical to that used to encipher the data. Even if unauthorized recipients of enciphered data have access to the 3DES algorithm, they cannot access original data without the correct key.

Features

- The built-in DES/3DES engine supports both Electronic Code Book (ECB) operation mode and Cipher Block Chain (CBC) operation mode.
- The DES/3DES engine is compliant with Federal Information Processing Standards (FIPS) PUB 46-3 and is also the FIPS-approved Symmetric Encryption Algorithm of choice. The DES/3DES algorithm uses Symmetric Block Cipher, and the block size is 64 bits.
- The key length is 64 bits for DES and 192 bits for 3DES. In the 64-Bit DES key, 56 bits are randomly generated and used directly by the algorithm, and the remaining 8 bits are for error detection. A 3DES key consists of three DES keys. The DES/3DES algorithm uses the same key for encryption and decryption.
- The performance of the DES/3DES engine is 22 Mbps for DES and 19 Mbps for 3DES per 1024-byte package (compared to 2.2 Mbps software 3DES running on the same TMPR4926 microprocessor). Using a

TAEC Regional Sales Offices

NORTHWEST

San Jose, CA

TEL: (408) 526-2400

FAX: (408) 526-8910

Portland, OR

TEL: (503) 629-0818

FAX: (503) 629-0827

SOUTHWEST

Irvine, CA

TEL: (949) 455-2000

FAX: (949) 707-5576

Richardson, TX

TEL: (972) 480-0470

FAX: (972) 235-4114

CENTRAL

Deerfield, IL

TEL: (847) 945-1500

FAX: (847) 945-2902

NORTHEAST

Wakefield, MA

TEL: (781) 224-0074

FAX: (781) 224-1096

Edison, NJ

TEL: (732) 248-8070

FAX: (732) 248-8030

SOUTHEAST

Duluth, GA

TEL: (770) 931-3363

FAX: (770) 931-7602

hardware 3DES engine delivers key performance advantages over software 3DES emulation.

- The built-in DES/3DES engine of the TMPR4926XB-200 contains a Direct Memory Access Controller (DMAC) for high performance of data transfer. The DMAC can transfer data from TMPR4926XB-200 memory to the DES/3DES computational block for encryption or decryption; the result can then be transferred back to TMPR4926XB-200 memory. The DMAC encodes/decodes the data package with sizes larger than 8 bytes.
- Our DES/3DES also supports chain operation: DMAC uses the linked-list chaining method to minimize the time from the completion of one command to the beginning of another.

Supported Product Families

In the TX Series MPU, only the TMPR4926XB-200 currently has a built-in DES/3DES calculator.

Specifications

- TMPR4926XB-200 DES supports Electronic Code Book (ECB) mode and Cipher Block Chain (CBC) mode. The block size of TMPR4926XB-200 DES is 64 bits.
- In ECB mode, each block of plain text encrypts to a block of cipher text. Since the same block of plain text will encrypt with the same key into the same block of cipher text, it is possible to build a code book of all possible cipher texts for a known plain text. If we know that an IP datagram was encrypted, we know that the first 20 bytes of cipher text represent the IP header and can use that knowledge with a code book to determine the key. Therefore, due to this security reason, the ECB mode has little or no practical use.

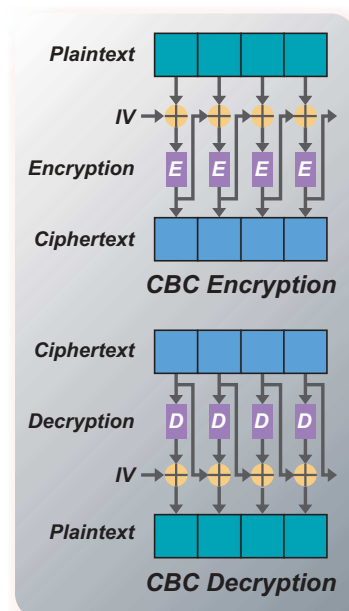
- CBC mode takes the previous block of cipher text and XORs it with the next block of plain text prior to encryption. The first block is XORed with an Initialization Vector (IV). The IV must have strong pseudo-random properties to ensure that identical plain text will not produce identical cipher text. Decryption is the opposite of encryption: Each block is decrypted and XORed with the previous block prior to decryption. The first block is decrypted and XORed with the IV. CBC mode has higher security; therefore, all ciphers currently defined for use in IPsec are block ciphers operating in CBC mode.

Related Tools and Systems Available

- DES API
- DES Linux driver
- DES vxWorks driver for Tornado 2.2/MIPS

Block Diagram

The following diagram explains the CBC eEncryption/dDecryption operation:



www.Toshiba.com/taec

The technical data may be controlled under U.S. Export Administration Regulations and may be subject to the approval of the U.S. Department of Commerce prior to export. Any export or re-export directly or indirectly, in contravention of the U.S. Export Administration regulations, is strictly prohibited.

TOSHIBA

TOSHIBA AMERICA ELECTRONICS COMPONENTS, INC.

TMPR4926 Triple Data Encryption Standard (3DES) Application

All trademarks are of their respective manufacturer and may be registered in certain jurisdictions.

© Copyright 3/2002 TAEC