

TURBOMISTY: A Tamper-Resistant Secure Board

by Tetsuo Nakakawaji and Akira Takehara*

There are limits to what can be done in software to ensure the secure control of private-key information, central to the safety of any security system. Mitsubishi Electric has developed specialty hardware to provide a secure private key-control function using a tamper-resistant unauthorized-access prevention structure, where the specialty hardware is equipped with a load-balancing function using multiple boards.

Development Goals

TURBOMISTY was developed primarily to provide secure control of private keys. The United States Government has provided the FIPS140-1 standard as the basis for security in encryption modules, and recently there have been more cases requiring the use of tamper-resistant hardware complying with this standard. Given this, TURBOMISTY was designed in compliance with FIPS140-1, Level 3.

The purpose of the encryption board is not just to control the private keys but also to provide high-performance symmetric ciphers such as TripleDES and MISTY to be used as an encryption engine.

In the balance between cost and performance, the objective was not simply to provide a single board with the highest possible performance; instead, the development project improved the total performance level by load balancing among multiple boards.

Features

Fig. 1 shows an outside view of the TURBOMISTY. It provides the following features:

1. The TURBOMISTY provides a high-level of security using a tamper-resistant function in compliance with FIPS140-1, Level 3.
 - Physical protection of secure information such as key information and authorization parameters using hardware.
 - Automatic protection of illegal access to the hardware itself, with automatic erasure of the information contained therein.
2. A software interface complying with the PKCS (Public Key Cryptography Standards) #11, which has become the industry standard, as the key control API, providing interoperability with PKCS #11 applications from other companies.
3. The use of multiple boards makes distributed load balancing possible using multiple boards that are transparent to the application.
4. Because the TURBOMISTY is installed in the form of PCI boards, it can be moved relatively easily to another platform.
5. Other encryption algorithms, such as elliptic-curve encryption, can be added at later dates using firmware updates.

Functions

TAMPER-RESISTANT FUNCTIONS. Attempts to make the forms of illegal access listed below will be detected automatically, resulting in the automatic erasure of all secret information contained within the TURBOMISTY.

- Removal of the board from the host equipment.
- Removal of the cover from the board, or destruction thereof.



Fig. 1 External appearance of the TURBOMISTY

*Tetsuo Nakakawaji and Akira Takehara are with the Information Technology R&D Center.

ASYMMETRIC CIPHER CALCULATIONS. RSA is used as the asymmetric cipher method, and, during calculations, all private-key information is concealed entirely within the board in the functions listed below in order to prevent any leakage to the outside:

- Public-key generation
- Private-key/public-key storage
- Private-key/public-key calculations
- Private-key backup

See below for more information about private-key backups.

SYMMETRIC CIPHER CALCULATIONS. Encryption and decryption calculation functions are provided using DES, Triple DES, and MISTY.

HARDWARE-BASED RANDOM NUMBER GENERATOR. It is possible to obtain better random numbers using hardware than it is with software-based generators.

DIGITAL CERTIFICATE STORAGE. This is based on X.509

MESSAGE DIGESTS. These are created using MD5 and SHA1.

SSL SERVER CONNECTIVITY. In the SSL protocol, which is used broadly as a secure communications protocol between browsers and web servers on the Internet, the control of the private keys for the SSL server is of critical importance. While at present most SSL servers store the private-key information on the disk drive, as is shown in Fig. 2, a combination of the TURBOMISTY and an SSL server makes it possible to control securely the private key in-

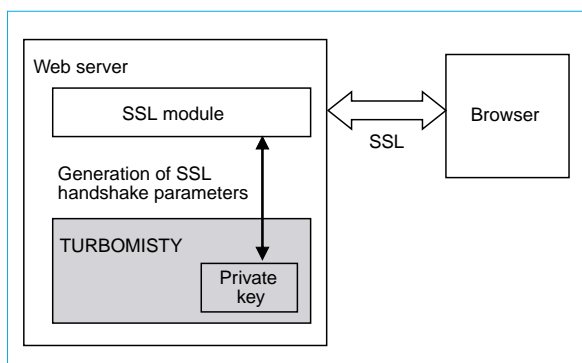


Fig. 2 Connections for an SSL server

formation for the SSL server, used when establishing an SSL connection.

The load on the CPU can also be reduced by performing in the TURBOMISTY the processes that are involved in encryption.

LOAD BALANCING. Load balancing among multiple boards is possible.

ADDITION OF NEW ALGORITHMS. Algorithms can be added by performing firmware updates for the TURBOMISTY.

Hardware Configuration

As is shown in Fig. 3, the TURBOMISTY is installed as a set of PCI boards. In order to prevent unauthorized access to key information or data from the circuits on the board during the calculations, the boards are structured with the circuits mounted on one side, with covers provided to cover the circuit-sides of the boards.

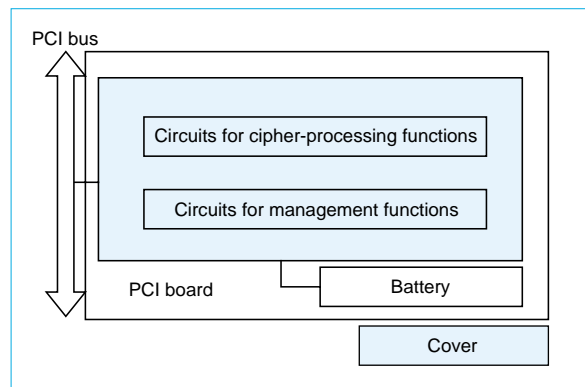


Fig. 3 Hardware configuration

A battery is provided outside the cover to maintain the key information when the host device is turned off, but all other components involved in the encryption processing and in managing keys are housed inside the cover.

Software Specifications

The PKCS #11, which has become the global standard for encryption module interfaces, is provided as the software interface.

In the TURBOMISTY, a single board has eight logical slots. So, for example, it can manage private keys from multiple certificate authorities (CAs). Furthermore, a maximum of four boards can be installed, meaning that up to 32 slots can be used. The relationships between the logi-

cal slots and the boards is managed within the PKCS #11 library.

As is shown in Fig. 4, non-exclusive control of the multiple ports that are fitted is performed within the PKCS #11 library, enabling processing to be distributed over multiple boards in a multi-thread/multi-processing environment without the need for any modifications to the applications.

Private Key Backups

TURBOMISTY's tamper-resistant mechanism prevents the leakage of key information by erasing automatically private keys stored within it. This function requires that the private keys be backed up against the possibility of a loss of security information due to attempted illegal access, damaged boards, etc., during operation.

Although the backup data is stored outside of the TURBOMISTY, the security is increased by internally encrypting the private keys and then dividing them up using a secret sharing procedure and then distributing components of the encrypted code to multiple users, thereby making it impossible to decode the original private key from the backup data outside of the TURBOMISTY.

In order to restore the private keys to the TURBOMISTY, the multiple backup segments that were indicated when the backup was made must be reassembled, preventing any individual from restoring the private keys working alone. The backup segments can be stored on floppy

disks or IC cards. By storing the backup segments on IC cards, it is possible to prevent copying of the backup segments, making control even securer.

Performance

In addition to the advantage of security, the secure boards also provide enhanced performance. Conventionally, encryption processing and, in particular, private-key processing as part of an asymmetric cipher system, has consumed a large portion of CPU resources in multi-word calculations. By performing the encryption processes within the secure board, the load on the host CPU is reduced. The TURBOMISTY is able to perform RSA 1024-bit key signature calculations at a rate of six per second, and can perform RSA 2048-bit key signature calculations at a rate of about one per second.

In addition, when the signature generation is distributed among multiple boards, the performance increases essentially in direct proportion to the number of boards, thus making it possible to obtain a full load-balancing effect.

Managing Operations in the TURBOMISTY

The operation of the TURBOMISTY can be managed using the control tools on the host machine. The primary functions of the control tools are as follows:

- Board status display
- Board initialization/setup of parameters such as PINs

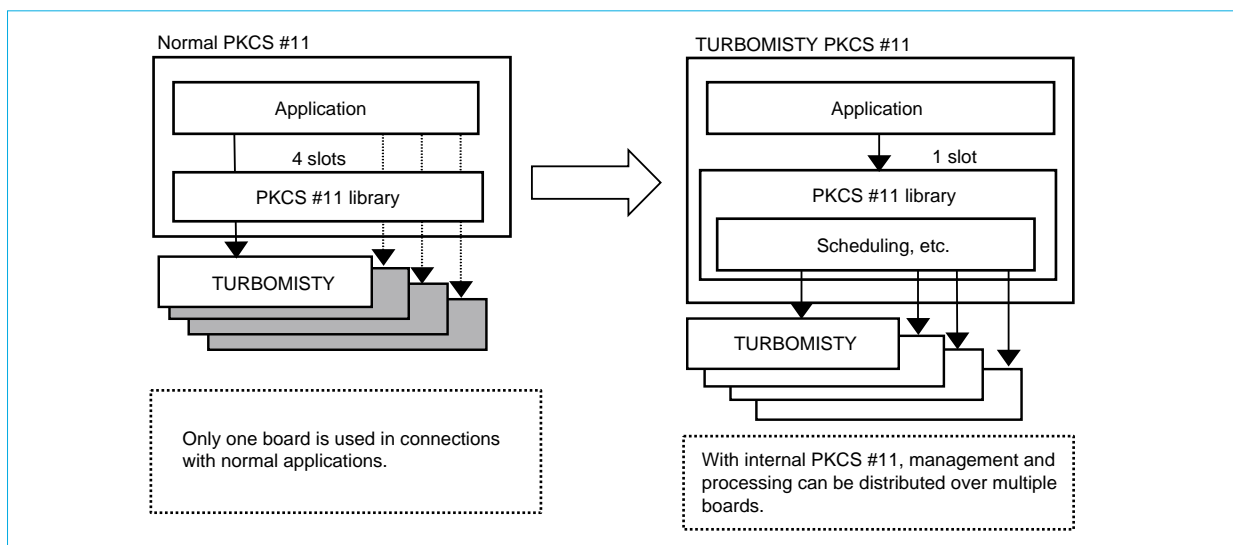


Fig. 4 Distributed processing using PKCS #11 library

- Display of lists of keys/digital certificates
- Backup/restore of private keys

Specifications

The primary specifications of the TURBOMISTY are given in Table 1.

As electronic transaction systems and e-business become ubiquitous, hardware by which to control the keys that are central to the security of systems is expected to become increasingly important. The corporation is committed to remaining in the forefront of all such efforts. □

Table 1 TURBOMISTY Specifications

PCI bus	32bit, 33MHz synchronous bus to PCI 2.1 standards
Size (W x Dmm)	Full-size PCI board 106.7 x 312
Compatible with FIPS 140-1	Level 3
Interface	PKCS #11 Ver. 2.01
Slots per board	8
Max. number of boards (slots)	4 (32)
Private keys per board	32
Certificates per board	64
Algorithms	RSA (512~2048) MISTY, DES, Triple DES MD5, SHA-1
Random number generator	Hardware
Compatible OS	Windows NT/2000 Solaris 7 HP-UX11.0 (planned)

Connectivity

At present, connectivity and interoperability of the TURBOMISTY has been verified for the following products:

ASSURETRANSACTION. AssureTransaction is the digital signature messaging system (DSMS) of Entegriy Corp., and is authorized as one component of the Identrus Financial System Certification System.

Connectivity between TURBOMISTY and AssureTransaction has been confirmed, certifying TURBOMISTY as an Entegriy Corp. certified hardware security module (HSM) along with products of foreign vendors such as Chrysalis Corp. and nCipher Corp.

IPLANET WEB SERVER. The iPlanet Web Server private key can be controlled by TURBOMISTY through storing them in the TURBOMISTY PKCS #11 library.