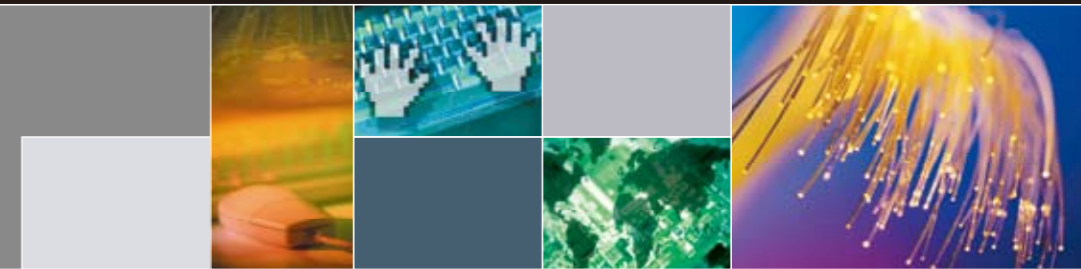


# High-Speed IPsec Processing Engine MB86978



## FUJITSU MICROELECTRONICS LIMITED

Shinjuku Dai-Ichi Seimei Bldg. 7-1, Nishishinjuku 2-chome, Shinjuku-ku,  
Tokyo 163-0722, Japan Tel: +81-3-5322-3347 Fax: +81-3-5322-3387  
<http://jp.fujitsu.com/fm/en/>

**North and South America**  
FUJITSU MICROELECTRONICS AMERICA, INC.  
1250 E. Arques Avenue, M/S 333  
Sunnyvale, CA 94085-5401, U.S.A.  
Tel: +1-408-737-5600 Fax: +1-408-737-5999  
<http://www.fma.fujitsu.com/>

**Europe**  
FUJITSU MICROELECTRONICS EUROPE GmbH  
Pittlerstrasse 47, 63225 Langen,  
Germany  
Tel: +49-6103-690-0 Fax: +49-6103-690-122  
<http://emea.fujitsu.com/microelectronics/>

**Korea**  
FUJITSU MICROELECTRONICS KOREA LTD.  
206 KOSMO TOWER, 1002 Daechi-Dong,  
Kangnam-Gu, Seoul 135-280 Korea  
Tel: +82-2-3484-7100 Fax: +82-2-3484-7111  
<http://www.fmk.fujitsu.com/>

**Asia Pacific**  
FUJITSU MICROELECTRONICS ASIA PTE LTD.  
151 Lorong Chuan, #05-08 New Tech Park  
Singapore 556741  
Tel: +65-6281-0770 Fax: +65-6281-0220  
<http://www.fujitsu.com/sg/services/micro/semiconductor/>

FUJITSU MICROELECTRONICS SHANGHAI CO., LTD.  
Rm. 3102, Bund Center, No.222 Yan An Road (E),  
Shanghai 200002, China  
Tel: +86-21-6335-1560 Fax: +86-21-6335-1605  
<http://cn.fujitsu.com/fmc>

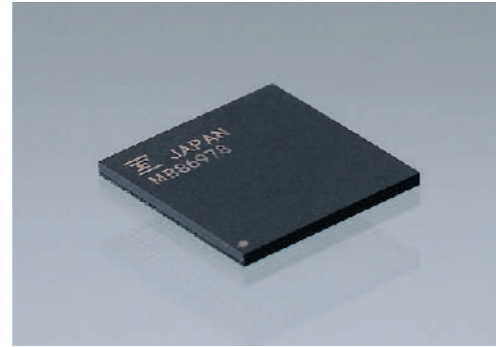
FUJITSU MICROELECTRONICS PACIFIC ASIA LTD.  
10/F, World Commerce Centre, 11 Canton Road  
Tsimshatsui, Kowloon  
Hong Kong  
<http://cn.fujitsu.com/fmc/tw>

Specifications are subject to change without notice. For further information please contact each office.

### All Rights Reserved.

The contents of this document are subject to change without notice.  
Customers are advised to consult with sales representatives before ordering.  
The information, such as descriptions of function and application circuit examples, in this document are presented solely for the purpose of reference to show examples of operations and uses of FUJITSU MICROELECTRONICS device; FUJITSU MICROELECTRONICS does not warrant proper operation of the device with respect to use based on such information. When you develop equipment incorporating the device based on such information, you must assume any responsibility arising out of such use of the information. FUJITSU MICROELECTRONICS assumes no liability for any damages whatsoever arising out of the use of the information.  
Any information in this document, including descriptions of function and schematic diagrams, shall not be construed as license of the use or exercise of any intellectual property right, such as patent right or copyright, or any other right of FUJITSU MICROELECTRONICS or any third party or does FUJITSU MICROELECTRONICS warrant non-infringement of any third-party's intellectual property right or other right by using such information. FUJITSU MICROELECTRONICS assumes no liability for any infringement of the intellectual property rights or other rights of third parties which would result from the use of information contained herein.  
The products described in this document are designed, developed and manufactured as contemplated for general use, including without limitation, ordinary industrial use, general office use, personal use, and household use, but are not designed, developed and manufactured as contemplated (1) for use accompanying fatal risks or dangers that, unless extremely high safety is secured, could have a serious effect to the public, and could lead directly to death, personal injury, severe physical damage or other loss (i.e., nuclear reaction control in nuclear facility, aircraft flight control, air traffic control, mass transport control, medical life support system, missile launch control in weapon system), or (2) for use requiring extremely high reliability (i.e., submersible repeater and artificial satellite).  
Please note that FUJITSU MICROELECTRONICS will not be liable against you and/or any third party for any claims or damages arising in connection with above-mentioned uses of the products.  
Any semiconductor devices have an inherent chance of failure. You must protect against injury, damage or loss from such failures by incorporating safety design measures into your facility and equipment such as redundancy, fire protection, and prevention of over-current levels and other abnormal operating conditions.  
Exportation/release of any products described in this document may require necessary procedures in accordance with the regulations of the Foreign Exchange and Foreign Trade Control Law of Japan and/or US export control laws.  
The company names and brand names herein are the trademarks or registered trademarks of their respective owners.

## Full Wire Speed of 100 Mbps Bidirectionally



The MB86978 is an IPsec accelerator engine in the Inline Architecture. When configured appropriately, this LSI provides encryption and decryption at a full wire speed of 100 Mbps bidirectionally. Unlike conventional IPsec processing engines in a lookaside architecture, the MB86978 enables bidirectional transfer via IPsec at a full wire speed of 100 Mbps. The LSI is best suited for upcoming broadband VPN routers which require high-speed, low-delay, and low-fluctuation routing.

VPN : Virtual Private Network  
IPsec : Internet Protocol Security

### Features

- **Inline IPsec processing**  
The MB86978 provides the following features to perform IPsec processing at full wire speed.
  - (1) Full-wire encoding engine  
DES/3DES (CBC mode), AES (CBC mode, Key length 128/192/256bits)
  - (2) Full-wire authentication engine  
HMAC-SHA-1, HMAC-MD5
  - (3) SA (Security Association) database  
Available setting of up to 64 SAs (Encoding direction: 64, Decoding direction: 64)
- **IKE support**  
Incorporating a function block to boost IKE calculation.
- **Choice of tunnel and transport modes selectable**  
Supporting both of tunnel mode and transport mode. In tunnel mode, the LSI processes tunnel headers.
- **Applicable packets**  
Supporting IPv4/IPv6, PPPoE, VLAN, NAT-Traversal, etc.
- **Two ports for RMII/MII interface**  
Two 10/100BASE-T/TX interface ports: One on the Internet side and the other on the routing function side.
- **SA database extension**  
Capable of extending the SA database with an extended classifier LSI connected externally.

### Development Concept

As broadband networks have been spreading, broadband routers supporting IPsec as a VPN industry standard have been used at growing opportunities. Existing IPsec-VPN routers are not capable of achieving sufficient throughput.

Figure 1 shows a typical configuration of a current IPsec-VPN router and its device throughputs during static routing and IPsec routing.

As illustrated, it is difficult for the current architecture based on a PCI bus to achieve sufficient throughputs.

To solve this problem, Fujitsu has developed this IPsec engine LSI delivers full-wire-speed throughput Inline IPsec routing as shown in the Figure 2.

Figure 1 Current IPsec-Oriented VPN Router

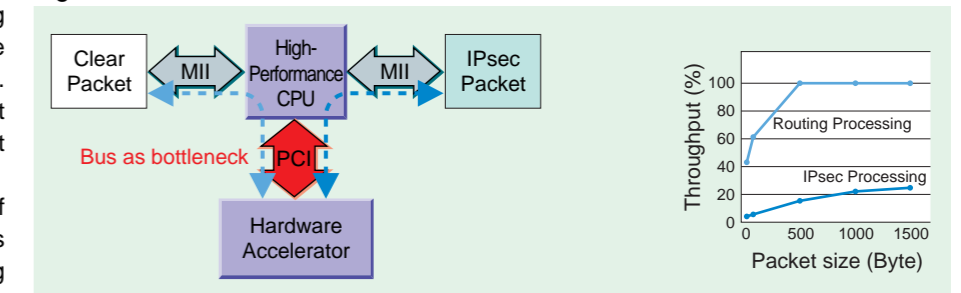
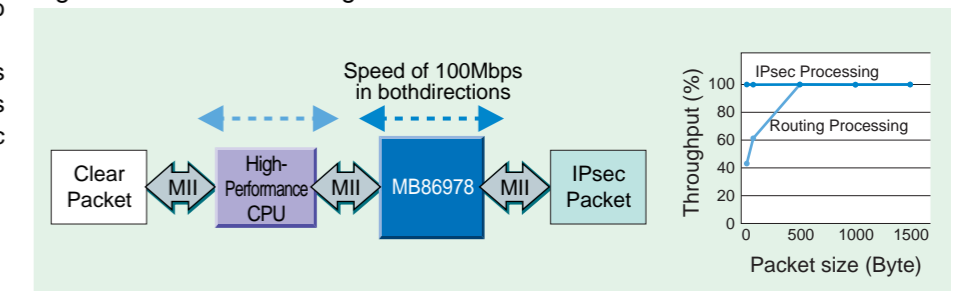


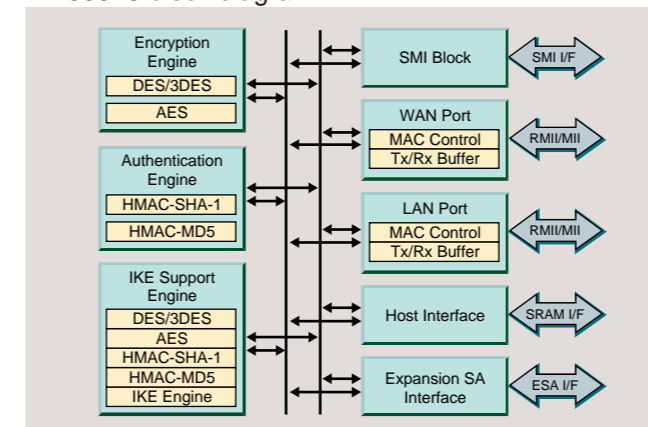
Figure 2 VPN Router Using MB86978



### Specifications and Configuration

- Encryption function : DES/3DES, AES
- Authentication function : HMAC-SHA-1, HMAC-MD5
- IKE support : IKE Engine
- Number of tunnels : 64 (Encoding direction: 64, Decoding direction: 64)
- Host interface : 16/32bits SRAM interface
- MAC block : Conformed to IEEE802.3 (DIX type), MII/RMII I/F of a WAN/LAN one port each
- Supply voltage : Dual power supplies at 1.8V and 3.3V
- Operating frequency : MAX 66MHz
- Package : FBGA337 (13mm x 13mm x 1.15mm)
- Manufacturing process : 0.18μm Manufacturing process

MB86978 block diagram

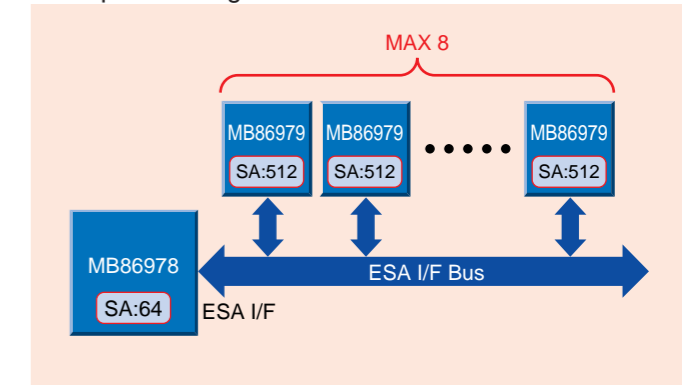


### Enhancements

Connecting the extended classifier LSI (MB86979) to the ESA interface of the MB86978 dramatically increases the number of tunnels.

One extended classifier LSI provides 512 tunnels and up to eight can be connected to the MB86978, where the maximum number of tunnels is 4096.

Example of Using Extended classifier LSIs



### Evaluation/Development Board

An evaluation/development board is available for supporting the development of MB86978-based products. Fujitsu will also provide one for use on the Linux platform.