

Cryptography Edition

CONTENTS

TECHNICAL REPORTS

Overview	1
<i>by Kotaro Katsuyama</i>	
MISTY, KASUMI and Camellia Cipher Algorithm Development	2
<i>by Mitsuru Matsui and Toshio Tokita</i>	
Cryptanalysis Technique to Evaluate the Strength of Ciphers	9
<i>by Toshio Tokita, Yasuyuki Sakai and Katsuyuki Takashima</i>	
Cipher Algorithm Implementation	13
<i>by Junko Nakajima, Tetsuya Ichikawa and Tomomi Kasuya</i>	
Quantum Cryptography	18
<i>by Toshio Hasegawa and Tsuyoshi Nishioka</i>	
TURBOMISTY: A Tamper-Resistant Secure Board	23
<i>by Tetsuo Nakakawaji and Akira Takehara</i>	

Cover Story

Our cryptographic technology is not limited to our proprietary encryption algorithm development but also provides widespread support to industry standardization activity. There are two kinds of information security products in the front cover implementing our symmetric key cryptographic algorithm MISTY. The upper one is a typical cryptographic LSI and the lower one is the tamper-resistant secure board. Details of these and other products are provided in the articles of this special edition of *Advance*.

Editor-in-Chief

Kiyoshi Ide

Editorial Advisors

Futoshi Takahashi
Koji Kuwahara
Keizo Hama
Katsuto Nakajima
Masao Hataya
Hiroshi Muramatsu
Yoshimasa Ishino
Fuminobu Hidani
Yukio Kurohata
Hiroshi Yamaki
Kiyohide Tsutsumi
Osamu Matsumoto
Hiromasa Nakagawa

Vol. 100 Feature Articles Editor

Kotaro Katsuyama

Editorial Inquiries

Keizo Hama
Corporate Total Productivity Management
& Environmental Programs
Mitsubishi Electric Corporation
2-2-3 Marunouchi
Chiyoda-ku, Tokyo 100-8310, Japan
Fax 03-3218-2465

Product Inquiries

Planning & Coordination Dept.
Information Technology R&D Center
Mitsubishi Electric Corporation
misty@isl.melco.co.jp
<http://www.mitsubishielectric.co.jp/security/>

Mitsubishi Electric Advance is published on line quarterly (in March, June, September, and December) by Mitsubishi Electric Corporation.
Copyright © 2002 by Mitsubishi Electric Corporation; all rights reserved.
Printed in Japan.