

Difference between SELF-evaluation reports for MULTI-S01

24/9/2001
HITACHI, LTD.

In this documentation we list the modifications and updates on the previous "self-evaluation report of multi-s01."

Difference.

- [1] Every page: on foot note,
All rights reserved. → All rights reserved.
The page number is added.
- [2] Page 3.
The URL where the latest information is available was added.
- [3]Page 16.
The first paragraph of Section 3:
The recent result that the Panama hash mode is not collision free, was treated
(also the reference was added).
Two typos are corrected: cryptanalysis → cryptanalysis
- [4]Page 17.
The implementation results on Intel Pentium III processor and Hitachi MAP1000
were added.
- [5]page 25.
The reference for the recent analysis of panama hash mode was added.
- [6]overall.
For every registered trademark or service mark, it is specified clearly.

- ☐ Pentium is a registered trademark of Intel Corporation.
- ☐ All other names are trademarks, registered trademarks or service marks of their respective companies.