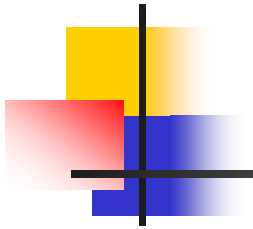
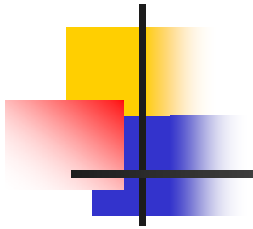


Hirotaka Yoshida, *HITACHI, Ltd., Systems Development Laboratory*

BIOGRAPHY

- Current position: Researcher at 7th Research Department
- Research field: Analysis and design of symmetric cryptographic primitives, especially hash functions
- 2004-2006: Research on analysis and design of hash functions
- 2003-2004: Visiting researcher with Prof. Bart Preneel at K.U.Leuven (ESAT, COSIC group), working on hash functions, Belgium.
- 2001-2003: Research on analysis and implementation of stream ciphers
- 1999-2001: Master studies in mathematics at Tokyo Institute of Technology



Hirotaka Yoshida, *HITACHI, Ltd., Systems Development Laboratory*

Conference talks:

- H. Yoshida, A. Biryukov, C. D. Canniere, J. Lano, and B. Preneel, “Non-randomness of the Full 4 and 5-pass HAVAL,” in SCN 2004.
- H. Yoshida and A. Biryukov, “Analysis of a SHA-256 Variant,” in SAC 2005.
- H. Yoshida, A. Biryukov, B. Preneel, “ Some Applications of the Biham-Chen Attack to SHA-like Hash Functions,” in CRYPTOGRAPHIC HASH WORKSHOP
- H. Yoshida, A. Biryukov, and Bart Preneel, “ Some applications of the Biham-Chen attack,” in Conference on Hash Functions.
- F. Mendel, B. Preneel, V. Rijmen, H. Yoshida, D. Watanabe,“ Update on Tiger, ” in INDOCRYPT 2006 to be appeared.