Cryptographic Hash Workshop
October 31 – November 1, 2005

Orr Dunkelman, *Computer Science Dept., Technion*
orrd@cs.technion.ac.il

BIOGRAPHY:

Orr Dunkelman is about to finish his Ph.D. at the Technion (Israel) under the supervision of Prof. Eli Biham. His main research interests are cryptanalysis of symmetric key primitives (block ciphers, stream ciphers, and hash functions). He has authored and co-authored 15 scientific publications in which he improved cryptanalytic techniques, such as the amplified boomerang attack (improved into the rectangle attack), and introduced new attacks (such as the related-key rectangle attack). Using the new techniques he presented attacks on several reduced versions of block ciphers such as AES, Serpent, IDEA, and SHACAL-1 (SHA-1 in encryption mode). Orr presented the first (related-key) attack on the full KASUMI (3GPP block cipher).
Orr has been active in the cryptanalysis community for the past years, and participated in program committees, including Fast Software Encryption 2006 and ASIACRYPT 2005. He has took part in the Technion's effort during the NESSIE project (New European Schemes for Signatures, Integrity, and Encryption). During this project Orr worked on the security analysis of symmetric primitives.