World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:14, No:07, 2020

A Watermarking Signature Scheme with Hidden Watermarks and Constraint Functions in the Symmetric Key Setting

Authors : Yanmin Zhao, Siu Ming Yiu

Abstract : To claim the ownership for an executable program is a non-trivial task. An emerging direction is to add a watermark to the program such that the watermarked program preserves the original program’s functionality and removing the watermark would heavily destroy the functionality of the watermarked program. In this paper, the first watermarking signature scheme with the watermark and the constraint function hidden in the symmetric key setting is constructed. The scheme uses well-known techniques of lattice trapdoors and a lattice evaluation. The watermarking signature scheme is unforgeable under the Short Integer Solution (SIS) assumption and satisfies other security requirements such as the unremovability security property.

Keywords : short integer solution (SIS) problem, symmetric-key setting, watermarking schemes, watermarked signatures
Conference Title : ICCSCS 2020 : International Conference on Cryptography and Security in Computing Systems
Conference Location : Zurich, Switzerland
Conference Dates : July 27-28, 2020