

SOFTWARE COPY PROTECTION BY USING MONOTONE DIGITAL SIGNATURES

ABHISHEK TRIPATHY¹ & SHIV SINGH SARANGDEVOT²

¹Department of Computer Science, NIMS, University, Jaipur, Rajasthan, India

²Department of Computer Science, JRN Rajasthan Vidyapeeth, Jaipur, Rajasthan, India

ABSTRACT

This paper aims at protection of the software piracy by using Monotone Digital Signatures. In settings where hard-copy materials (i.e. banknotes, legal documents and etc) which are not allowed to be reproduced by any means but are massively delivered to users security specialists distinguish a real threat which duplication and are even to be distributed over the internet.

One best way to figure out the problem of duplication and software piracy is the use of digital signatures. For this reason now a day's algorithms and advanced techniques of digital signatures are used to provide security or at least pretended to be secure. This security technique of digital signatures fragile if the secrecy of the key is compromised. In this paper the new digital signature scheme is introduced which is based on Rabin scheme. According to this idea the ID generation scheme is built which can be used in many situations where is needed such a level of security. And also this technique is applied in software piracy protection.

KEYWORDS: Monotone Digital Signature, Software Copy Protection, Rabin Scheme