HASH-BASED COUNTER SCHEME FOR DIGITAL RIGHTS MANAGEMENT (WedPmOR6)

Author(s) :
Mikko Löytynoja (MediaTeam / University of Oulu, Finland)
Tapio Seppänen (MediaTeam / University of Oulu, Finland)

Abstract :
This paper describes a counter scheme that uses hash functions to count how many times the user is allowed to play protected content in a DRM-enabled player. The proposed basic scheme can be used in scenarios where the user cannot be assumed to have online connection. We discuss the weaknesses of the proposed scheme and present alternative to the basic scheme, which increases the security of the counter.