Session Code: **CX**	Title: **Information Hiding**	
Paper Code: **310**	Thu, September 15, 2011	Time: 15 – 15:20

Cryptographic Keys Management for H.264 Scalable Coded Video Security

Mamoona Asghar
School of Computing and Electronic Systems
University of Essex, Colchester, CO4 3SQ
Essex, United Kingdom
masghaa@essex.ac.uk

Mohammad Ghanbari, Fellow IEEE
School of Computing and Electronic Systems
University of Essex, Colchester, CO4 3SQ
Essex, United Kingdom
ghan@essex.ac.uk

Abstract: Scalable multi-layered coded video requires its individual layer security, as every layer has its own characteristics i.e. bit-rate, frame rate, resolution and quality. We investigate a problem of individual layer cryptographic key management issues in scalable video coding (H.264/SVC) and propose a top down hierarchical keys generation and distribution system by using a standard key management protocol MIKEY (Multimedia Internet Keying Protocol). The research goal is to enhance the security, while reducing the multiple encryption keys overhead for scalable video content retrieval, and derive a mechanism in which every entitled user needs to hold single encryption key to watch his subscribed layer data, but this key can open the doors of all layers below. The timing results are calculated for SVC bit-stream encryption/decryption and hierarchical keys generation to prove the suitability of the proposed scheme. We combine a standard protocol with the DRM (Digital Rights Management) techniques to accomplish the security demands of scalable video content on the application level.

Keywords: H.264/SVC; MIKEY; DRM; Cryptographic keys; AES encryption; security