# CRYPTOGRAPHIC KEYS MANAGEMENT FOR H.264 SCALABLE CODED VIDEO SECURITY

**Presented by:**

**Mamoona Asghar**

**PhD Scholar**

**Department of Computing & Electronic Systems**

**University of Essex, Colchester, United Kingdom. CO4 3SQ**

## ABSTRACT

- 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).
- 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.
- 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*

# INTRODUCTION

- 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. The bit stream components of SVC are encapsulated in network abstraction layer (NAL) units which are then arranged as access units.
- Cryptography is a conventional technique to provide security to the multimedia contents.
- The key generation and distribution is the critically tackled issue to enhance the security of any cipher algorithm.
- Reviewed researches have their own devised key management mechanisms but don't provide any reference to any standard key management protocol.

# INTRODUCTION (CONT.)

- For the hierarchical Scalable layers key generation/distribution, the standard Multimedia Internet Keying Protocol (MIKEY) protocol is implemented for SVC layer keys management.
- Advanced Encryption Standard (AES) block cipher used for encryption algorithm
- The research work incorporates the following DRM security processes.
  - Authentication key will be derived for the authentication of sender and receiver.
  - Encryption of Data with Cipher Algorithm
  - Key management with Standard Protocol

# Key Management Issues

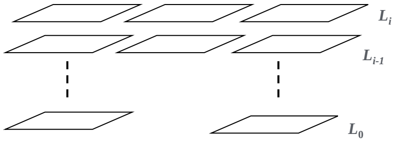


Figure1. Scalable Layers

TABLE I: Set of encryption keys should be held for each hierarchical layer

| Layers | Encryption Keys held for each Layer |
|---|---|
| $L_i$ | $eK_0, eK_1, eK_2, eK_3, \ldots, eK_{i-1}, eK_i$ |
| $L_{i-1}$ | $eK_0, eK_1, eK_2, eK_3, \ldots, eK_{i-1}$ |
| $L_3$ | $eK_0, eK_1, eK_2, eK_3$ |
| $L_2$ | $eK_0, eK_1, eK_2$ |
| $L_1$ | $eK_0, eK_1$ |
| $L_0$ | $eK_0$ |

# Multimedia Internet Keying Protocol (MIKEY)

TABLE II. Characteristics of MIKEY keys

| Keys | Key Length (bits) | Generation/ Distribution Methods & Parameters | MIKEY Constants | Key Life Time |
|---|---|---|---|---|
| **TGK (Master key)** | 128 | Diffie Hellman | DH prime & base values | 01 month |
| **TEK (Traffic Encryption key)** | 128 | HMAC-SHA1(TGK) | *0x2AD01C64* | Daily for 12 Hrs. |
| **Master Encryption key (*eK*)** | 128 | HMAC-SHA1(TEK) | *0x15798CEF* | For Session |
| **Authentication Key (*aK*)** | 160 | HMAC-SHA1(TEK) | *0x1B5C7973* | Unique for every User |
| **Salt Keys (*sK*)** | 112 | HMAC-SHA1(TEK) | *0x39A2C14B* | Daily for 12 Hrs. |

# Proposed Key Management Scheme (cont.)

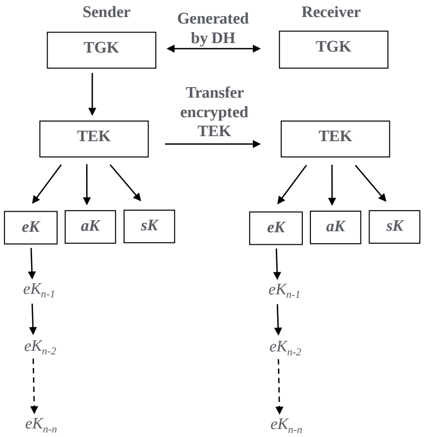


**Figure 2. Key Generation Mechanism**

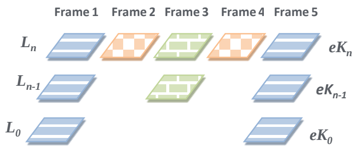


**Figure 3. Keys per scalable layer**

# Proposed Key Management Scheme (cont.)

There are five general equations for overall system keys generation:

- ***TGK***→ $g^{sr}$ *mod p* (Diffie Hellman) (1)
- *where* p=prime no., g=generator, sr=sender & receiver RAND values
- ***TEK*** → *HMAC (TGK, MIKEY Constant || RAND, TEK length)* (2)
- ***Master eK*** → *HMAC (TEK, eK Constant || RAND, eK length)* (3)
- ***aK*** → *HMAC (TEK, aK Constant || RAND, aK length)* (4)
- ***sK*** → *HMAC (TEK, sK Constant || RAND, sK length)* (5)

General equations for generation of encryption keys for lower SVC layers are:

- $\boldsymbol{eK_n}$ → *HMAC (TEK,* $eK_n$ *Constant || RAND,* $eK_n$ *length)* (6)
- $\boldsymbol{eK_{n-1}}$ → *HMAC (*$eK_n$*,* $eK_{n-1}$*Constant || RAND,* $eK_{n-1}$ *length)* (7)
- $\boldsymbol{eK_{n-2}}$ →*HMAC (*$eK_{n-1}$*,* $eK_{n-2}$*Constant || RAND,* $eK_{n-2}$ *length)* (8)

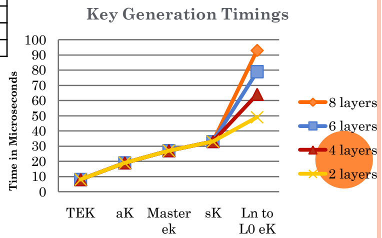
General equations for the bit streams encryption on all layers:

- $\boldsymbol{eK_n}$ *(encrypts)* → $L_n$ *Frames –* $L_{n-1}$ *Frames* (9)
- $\boldsymbol{eK_{n-1}}$ → $L_{n-1}$ *Frames –* $L_{n-2}$ *Frames* (10)

# Evaluation Results

| Sample CIF Timings (Sec.) | 30 Frames | 60 Frames | 90 Frames | 120 Frames | 150 Frames |
|---|---|---|---|---|---|
| **BUS** | | | | | |
| Encoding time | 23 | 47 | 70 | 93 | 116 |
| Encryption time | 0.012 | 0.019 | 0.027 | 0.039 | 0.043 |
| Decryption time | 0.021 | 0.028 | 0.032 | 0.042 | 0.047 |
| Decoding time | 0.977 | 1.879 | 2.678 | 3.544 | 4.278 |
| **FOOTBALL** | | | | | |
| Encoding time | 24 | 50 | 75 | 99 | 123 |
| Encryption time | 0.021 | 0.032 | 0.039 | 0.046 | 0.050 |
| Decryption time | 0.029 | 0.043 | 0.055 | 0.065 | 0.072 |
| Decoding time | 0.950 | 1.902 | 2.779 | 3.656 | 4.498 |
| **CREW** | | | | | |
| Encoding time | 22 | 43 | 66 | 100 | 113 |
| Encryption time | 0.010 | 0.016 | 0.020 | 0.031 | 0.038 |
| Decryption time | 0.012 | 0.027 | 0.031 | 0.037 | 0.054 |
| Decoding time | 0.877 | 1.776 | 2.623 | 3.440 | 4.312 |
| **FOREMAN** | | | | | |
| Encoding time | 21 | 41 | 62 | 83 | 104 |
| Encryption time | 0.010 | 0.012 | 0.017 | 0.021 | 0.038 |
| Decryption time | 0.016 | 0.020 | 0.027 | 0.038 | 0.040 |
| Decoding time | 0.863 | 1.711 | 2.582 | 3.380 | 4.164 |

**TABLE III. Timings of sample CIF**



# Conclusions

- This paper has proposed a compact key management and distribution system which is very efficient and greatly enhances the security of transmission.
- After the detailed analysis of key management protocol, the strength of cipher algorithm, and the encryption of layered data, it is expected that the proposed security scheme will be a desirable contribution for the security of scalable video coding especially its part of flexible hierarchical key management for all layers (top to bottom).
- The significance of the proposed method is that subscriber of each layer has only one encryption key to use, but this key can open the doors of all layers below.
- This cryptographic hierarchical key management scheme is suitable for the secure video distribution to users who have subscribed to a different video quality.