INTERNATIONAL ORGANISATION FOR STANDARDISATION
ORGANISATION INTERNATIONALE DE NORMALISATION
ISO/IEC JTC1/SC29/WG11
CODING OF MOVING PICTURES AND AUDIO

ISO/IEC JTC1/SC29/WG11 MPEG2016/M41804
October 2017, Macao, China

Source **IETR/INSA Rennes, Thales Communication and Security and ParisTech**
Status **Input document**
Title **AVC and HEVC Selective Video Encryption: Decryption Challenge**
Author Wassim Hamidouche, Pierre-Loup Cabarat, Cyril Bergeron, Jean Le Feuvre

Abstract

This contribution provides information on how to generate and decode hevc bitstreams ciphered with the selective encryption method proposed in [1]. It also provides six ciphered AVC and HEVC bitstreams which can be used as reference for security evaluation of the selective encryption solution.

1 Introduction

Several ciphering methods have already been proposed for HEVC contents [3]. In this contribution we provide three HEVC and three AVC bitstreams which have been ciphered using the selective encryption method described in [1, 5] to test this method for robustness.
In this contribution we also provide some details on how to generate your own test sequences for HEVC selective encryption with real time encoder and decoder software. Kvazaar HEVC encoder and openHEVC HEVC decoder can be used as reference software to encrypt and decrypt these sequences. The process for installation and usage of openHEVC for decryption is provided in Section 3. The process for installation and usage of kvazaar for encryptions can be found in Section 4.

2 Description of contents

2.1 HEVC Bitstreams

We attached to this contribution two *.hevc files which correspond to conformant HEVC bitstreams ciphered using selective encryption on five HEVC *by-passed* syntax elements:

1. intra prediction modes,
2. motion vectors signs,
3. absolute motion vectors values,
4. transformed coefficients signs.
5. transformed coefficients absolute values.

These sequences are;

- ***drone_encry.hevc***
- ***kids_tiles2x4_encry.hevc***

Therefore, these two video bitsteams can be decoded with any standard HEVC decoder. The ***kids_tiles2x4_encry.hevc*** video sequence is encoded in 8 tiles and only two tiles are encrypted as described in [4]. More information about each bitstream can be found in the corresponding *.txt files.

2.2 AVC Bitstreams

The three AVC encrypted bitstreams are

- **testcypher.h264**
- **2160x3840ROI.h264**
- **image.avci**

All these bitstreams can be decoded with any standard AVC decoder. **2160x3840ROI.h264** and **image.avci** bitstreams are the same still picture encoded in AVC (only one Intra) in 3 Slices where only the second slice is encrypted as shown in Figure 1). **image.avci** is encapsulated as HEIF content, generated from the **2160x3840ROI.h264** content using GPAC's MP4Box [7], as described here: https://gpac.wp.imt.fr/2017/06/09/gpac-support-for-heif/

More information about each bitstream can be found in the corresponding *.txt files.

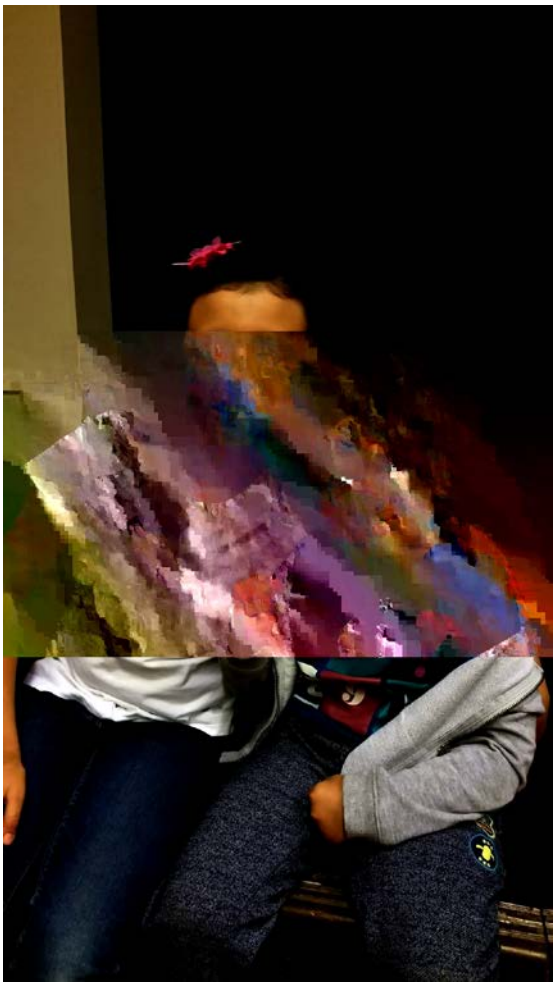

Figure 1 - image test "2160x3840ROI.h264" decoded without deciphering

The encryption algorithm encrypts all AVC syntax elements including : slice QP delta, Macroblock type, PCM sample Luma and Chroma, Macroblock QP Delta, Prediction Intra

Luma, Prediction Intra Chroma, Motion prediction reference, Trailing ones, Level Suffix, Total zeros, Run Before.
Note that some constraints were applied on those different codewords. If you wanted more information on code-words containing bits ‘selected for encryption’ see Annex A in [6].

3 Installation and usage of kvazaar software for ciphering

We only provide information using Ubuntu 16.04 linux distribution, since its he easiest way to obtain a working build.

Install Kvazaar dependencies autogen libcryptopp9v5
sudo apt-get install libcrytptopp9v5 && sudo apt-get install autogen

Retrieve Kvazaar source code by cloning its git repository:
git clone https://github.com/ultravideo/kvazaar

Use autogen to generate a configuration script for your computer
./autogen.sh

Run the configuration script with selective encryption enabled:
./configure --with-cryptopp

Compile kvazaar source code
make

Install kvazaar
sudo make install

Encode a raw video using selective encryption:

kvazaar --input <RAW_VIDEO_INPUT_FILE> --input-res=<WxH> --crypto=”on" --key <KEY> --output <OUTPUT_HEVC_BITSTREAM> --no-wpp

Note: It is necessary to disable wavefront parallel processing by providing the parameter *–no-wpp*. It is currently not supported when selective encryption is on.

4 Installation and usage of openHEVC software for deciphering

We only provide information using Ubuntu 16.04 linux distribution, since its he easiest way to obtain a working build

Install openHEVC dependencies (SDL and libcryptopp9v5)
sudo apt-get install libsdl && sudo apt-get install libcrytptopp9v5

Retrieve openHEVC source code by cloning its git repository:
git clone https://github.com/OpenHEVC/openHEVC

Go into openHEVC repository
cd openHEVC

Checkout onto openHEVC-2.0 tag
git checkout openhevc-2.0

Run configure with selective encryption feature enabled:
./configure --enable-encryption

Compile openHEVC source code
make

Install openHEVC
sudo make install

You might need to run ldconfig in order to update your library linking path.
sudo ldconfig

Running openHEVC with selective encryption mode enabled:
ohplay -i <FILE> --crypto on --key <KEY> -o <RAW_VIDEO_OUTPUT_FILE>

5 References

[1] Wassim Hamidouche, Mousa Farajallah, Naty Ould Sidaty, Safwan El Assad, Olivier Déforges: *Real-time selective video encryption based on the chaos system in scalable HEVC extension*. Sig. Proc.: Image Comm. 58: 73-86 (2017)

[2] Cyril Bergeron, Naty Sidaty, Wassim Hamidouche, Benoit Boyadjis, Jean Le Feuvre, Lim Youngkwon, *Real-Time Selective Encryption Solution based on ROI for MPEG-A Visual Identity Management AF*, Digital Signal Processing (DSP2017), Aug 2017, London, UK

[3] Zafar Shahid and William Puech, *Visual Protection of HEVC Video by Selective Encryption of CABAC Binstrings*, IEEE Transactions on Multimedia, vol. 16, no. 1, pp. 24-36, 2013.

[4] Mousa Farajallah, Wassim Hamidouche, Olivier Déforges, Safwan El Assad, *ROI encryption for the HEVC coded video contents*, IEEE Interbation Confernce on Image Processing, ICIP2015.

[5] Benoit Boyadjis, Cyril Bergeron, Béatrice Pesquet-Popescu, Frédéric Dufaux: *Extended Selective Encryption of H.264/AVC (CABAC)- and HEVC-Encoded Video Streams*. IEEE Trans. Circuits Syst. Video Techn. 27(4): 892-906 (2017).

[6] Cyril Bergeron, Wassim Hamidouche, Youngkwon Lim, WD of ISO/IEC 23000-21 Visual Identity Management AF, output MPEG document w16956, July 2017, Torino, Italy

[7] J. Le Feuvre, C. Concolato and J.-C. Moissinac, GPAC: *Open Source Multimedia Framework*, Proceedings of the 15th ACM International Conference on Multimedia, no. 4, pp. 1009-1012, New York, 2007.